Cisco Secure Firewall Threat Defense syslog メッセージ

初版：2018 年 3 月 30 日

最終更新：2022 年 7 月 6 日

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

このマニュアルについて

ここでは、このガイドを使用する方法について説明します。

各リリースでの変更点

セキュリティイベントの Syslog メッセージ

次のイベントタイプの syslog メッセージに対する変更については、「セキュリティイベントの Syslog メッセージの履歴 （26 ページ）」を参照してください。

- 侵入イベント
- 接続イベント
- セキュリティ インテリジェンス イベント
- ファイル イベント
- マルウェア イベント

その他のすべての Syslog メッセージ

この項では、次の Secure Firewall Threat Defense リリースで追加、変更、および廃止された syslog メッセージを示します。Syslog メッセージの詳細な説明については、それぞれ対応する章を参照してください。

- 表 1 : バージョン 7.2 で追加、変更、および廃止された Syslog メッセージ
- 表 2 : バージョン 7.1 で追加、変更、および廃止された Syslog メッセージ
- 表 3 : バージョン 7.0 で追加、変更、および廃止された Syslog メッセージ

表 *1* : バージョン *7.2* で追加、変更、および廃止された *Syslog* メッセージ

追加された Syslog メッセージ	新しい syslog メッセージは追加されませんでした。
変更された Syslog メッセージ（ドキュメント）	なし
変更された syslog メッセージ（コード）	なし
廃止された Syslog メッセージ	なし

表 *2* : バージョン *7.1* で追加、変更、および廃止された *Syslog* メッセージ

追加された Syslog メッセージ	709009、709010、709011、709012、709013
変更された Syslog メッセージ（ドキュメント）	なし
変更された syslog メッセージ（コード）	なし
廃止された Syslog メッセージ	なし

表 *3* : バージョン *7.0* で追加、変更、および廃止された *Syslog* メッセージ

追加された Syslog メッセージ	なし
変更された syslog メッセージ（ドキュメント）	717009
変更された syslog メッセージ（コード）	なし
廃止された Syslog メッセージ	なし

表 *4* : バージョン *6.7* で追加、変更、および廃止された *Syslog* メッセージ

追加された Syslog メッセージ	106029
変更された syslog メッセージ（ドキュメント）	105042、105003、105004、105043、305006、414004
変更された syslog メッセージ（コード）	302013、302014
廃止された Syslog メッセージ	なし

表 *5 :* バージョン *6.6* で追加、変更、および廃止された *Syslog* メッセージ

追加された Syslog メッセージ	209006

表 *6 :* バージョン *6.5* で追加、変更、および廃止された *Syslog* メッセージ

追加された Syslog メッセージ	748011、748012、302311、747042、747043、747044、769007、769009、852001、852002
変更された Syslog メッセージ	302014
廃止された Syslog メッセージ	

表 *7 :* バージョン *6.4* で追加、変更、および廃止された *Syslog* メッセージ

追加された Syslog メッセージ	セキュリティイベント：430004、430005 その他：305017、308003、308004、408101、408102、409014、409015、409016、409017、419004、419005、419006、503002、503003、503004、503005、737038、737200-737206,737400-737407、747042、747043、747044、768003、768004
変更された Syslog メッセージ	737001 ～ 737019、737031 ～ 737036
廃止された Syslog メッセージ	

すべての Syslog メッセージ

表 *8 :* バージョン *6.3* の *Syslog* メッセージの変更

タイムスタンプロギング	バージョン 6.3 以降、Secure Firewall Threat Defense は、イベントの syslog で RFC 5424 に従ってタイムスタンプを有効にするオプションを提供します。このオプションを有効にすると、Syslog メッセージのすべてのタイムスタンプには、RFC 5424 形式に従って時刻が表示されます。次に、RFC 5424 形式の出力例を示します。 `<166>2018-06-27T12:17:46Z firepower : %FTD-6-110002: Failed to locate egress interface for protocol from src interface :src IP/src port to dest IP/dest port` （注） 上記の例では、PRI 値 <166> は、ファシリティとアラートの重大度の両方を表すプライオリティ値です。RFC5424 形式の Syslog メッセージには、通常 PRI が表示されます。ただし、Management Center が管理する Threat Defense の場合、Management Center プラットフォーム設定を使用して EMBLEM 形式でのロギングを有効にした場合にのみ、PRI 値が syslog メッセージに表示されます。EMBLEM 形式を有効にする方法については、「Cisco Secure Firewall Management Center アドミニストレーション ガイド」を参照してください。PRI の詳細については、「RFC5424」を参照してください。
Syslog のプレフィックスの形式	Threat Defense オペレーティングシステムは、syslog ユーティリティを含む ASA オペレーティングシステムの一部を使用していました。したがって、この共有ユーティリティのため、Threat Defense の syslog メッセージはすべて「%ASA」から始まっていました。リリース 6.3 以降、Threat Defense の syslog メッセージは「%FTD」から始まります。

Secure Firewall Threat Defense Syslog メッセージについて

（注） このトピックの情報は、セキュリティイベントに関連するメッセージには適用されません。

次の表に、メッセージのクラスおよび各クラスに関連付けられているメッセージ ID の範囲を示します。メッセージ ID の有効な範囲は 100000 ～ 999999 です。

（注） 番号が連番から抜けている場合、そのメッセージは Threat Defense デバイスコードにはありません。

ほとんどの ISAKMP メッセージには、トンネルの識別に役立つ追加オブジェクトの共通セットがあります。これらのオブジェクトは、使用可能なときに、メッセージの説明テキストの前に付加されます。メッセージの生成時にオブジェクトが未知の場合、特定の **heading = value** の対は表示されません。

これらのオブジェクトは次の形式で追加されます。

Group = **groupname**, Username = **user**, IP = **IP_address**,...

ここで、Group はトンネル グループを特定し、username はローカル データベースまたは AAA サーバーのユーザー名、IP アドレスはリモート アクセス クライアントまたは L2L ピアのパブリック IP アドレスです。

通常、Syslog メッセージのトラフィックセッションに各フローの接続番号/ID が表示されます。ただし、一部の接続については、接続 ID は増加しますが、Syslog メッセージには ID が表示されません。そのため、後続のメッセージの接続 ID でシーケンス番号の欠落が見られる場合があります。たとえば、TCP トラフィックフローで、Syslog メッセージに各フローの接続 ID が 201、202、203、204 と表示されたとします。ICMP フローが開始されると、接続 ID は内部的に 205 および 206 に増えますが、Syslog メッセージには番号が表示されません。別の TCP フローが続くと、その接続番号は 207、208 などと表示され、シーケンスをスキップしているように見えます。

表 *9 : syslog* メッセージのクラスおよび関連付けられているメッセージ *ID* 番号

ロギング クラス	定義	Syslog メッセージ ID 番号
auth	User Authentication	109、113
—	アクセス リスト	106
—	アプリケーション ファイアウォール	415
bridge	トランスペアレント ファイアウォール	110、220
ca	PKI 認証局	717
citrix	Citrix Client	723
—	クラスタ	747
—	カード管理	323
config	コマンド インターフェイス	111、112、208、308
csd	Secure Desktop	724
cts	Cisco TrustSec	776
dap	ダイナミック アクセス ポリシー	734
eap、eapoudp	ネットワーク アドミッション コントロールの EAP または EAPoUDP	333、334

ロギング クラス	定義	Syslog メッセージ ID 番号
eigrp	EIGRP ルーティング	336
email	電子メール プロキシ	719
—	環境モニタリング	735
ha	フェールオーバー	101、102、103、104、105、210、311、709、727
—	Identity-Based ファイアウォール	746
ids	侵入検知システム	400、733
—	IKEv2 ツールキット	750、751、752
ip	IP スタック	209、215、313、317、408
ipaa	IP アドレス割り当て	735
ips	侵入防御システム	400、401、420
—	IPv6	325
—	ブロックリスト、許可リスト、およびグレーリスト	338
—	ライセンス	444
mdm-proxy	MDM プロキシ	802
nac	ネットワーク アドミッション コントロール	731、732
nacpolicy	NAC ポリシー	731
nacsettings	NAC ポリシーを適用する NAC 設定	732
—	ネットワーク アクセス ポイント	713
np	ネットワーク プロセッサ	319
—	NP SSL	725
ospf	OSPF ルーティング	318、409、503、613
—	パスワードの暗号化	742
—	電話プロキシ	337
rip	RIP ルーティング	107、312
rm	Resource Manager	321

ロギング クラス	定義	Syslog メッセージ ID 番号
—	セキュリティ イベント （このトピックの情報は、これらのイベントには適用されません）	430
—	Smart Call Home	120
session	ユーザ セッション	106、108、201、202、204、302、303、304、305、314、405、406、407、500、502、607、608、609、616、620、703、710
snmp	SNMP	212
—	ScanSafe	775
ssl	SSL スタック	725
svc	SSL VPN クライアント	722
sys	システム	199、211、214、216、306、307、315、414、604、605、606、610、612、614、615、701、711、741
—	脅威の検出	733
tre	トランザクション ルール エンジン	780
—	UC-IME	339
tag-switching	サービス タグ スイッチング	779
vm	VLAN マッピング	730
vpdn	PPTP および L2TP セッション	213、403、603
vpn	IKE および IPsec	316、320、402、404、501、602、702、713、714、715
vpnc	VPN クライアント	611
vpnfo	VPN フェールオーバー	720
vpnlb	VPN ロード バランシング	718
—	VXLAN	778
webfo	WebVPN フェールオーバー	721

ロギング クラス	定義	Syslog メッセージ ID 番号
webvpn	WebVPN と AnyConnect Client	716
—	NAT および PAT	305

Syslog メッセージを送信するためのシステムの設定

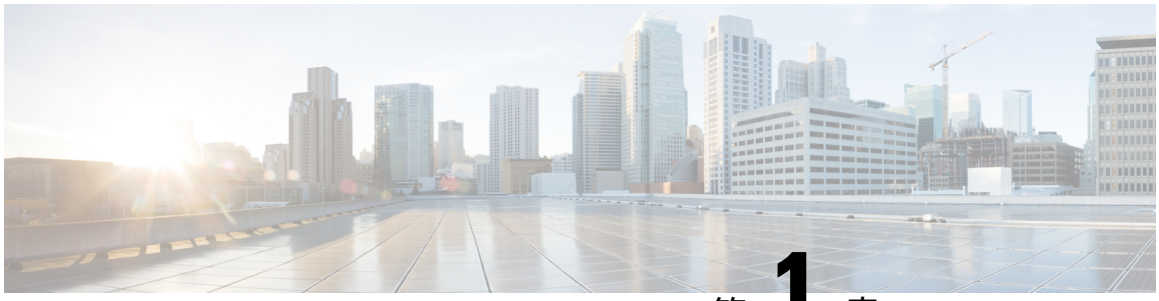
トリガーするイベントが発生するとすぐに、syslog が生成されます。Threat Defense が syslog メッセージを送信できる最大レートは、syslog のレベルと使用可能な CPU リソースによって異なります。Management Center に保存できるイベントの数はモデルによって異なります。システムパフォーマンスを向上させるために、イベント生成制限、しきい値制限を構成でき、一部のイベントタイプのストレージを無効にすることもできます。外部の syslog、SNMP トラップサーバー、またはその他の外部ツールにイベントを記録することもできます。これらのシステムロギング設定の詳細については、ご使用のリリースの『Cisco Secure Firewall Management Center デバイス構成ガイド』または『Cisco Secure Firewall Device Manager Configuration Guide』を参照してください。

通信、サービス、およびその他の情報

- シスコからタイムリーな関連情報を受け取るには、Cisco Profile Manager でサインアップしてください。
- 重要な技術によりビジネスに必要な影響を与えるには、シスコ サービスにアクセスしてください。
- サービス リクエストを送信するには、シスコ サポートにアクセスしてください。
- 安全で検証済みのエンタープライズクラスのアプリケーション、製品、ソリューション、およびサービスを探して参照するには、Cisco Marketplace にアクセスしてください。
- 一般的なネットワーク、トレーニング、認定関連の出版物を入手するには、Cisco Press にアクセスしてください。
- 特定の製品または製品ファミリの保証情報を探すには、Cisco Warranty Finder にアクセスしてください。

Cisco バグ検索ツール

Cisco バグ検索ツール（BST）は、シスコ製品とソフトウェアの障害と脆弱性の包括的なリストを管理する Cisco バグ追跡システムへのゲートウェイとして機能する、Web ベースのツールです。BST は、製品とソフトウェアに関する詳細な障害情報を提供します。



第 1 章

セキュリティイベントの Syslog メッセージ

セキュリティイベントの Syslog メッセージの ID

- 430001：侵入イベント

  この ID はリリース 6.3 で導入されました。

- 430002：接続の開始時に記録された接続イベント

  この ID はリリース 6.3 で導入されました。

- 430003：接続の終了時に記録された接続イベント

  この ID はリリース 6.3 で導入されました。

- 430004：ファイルイベント

  これらのイベントの Syslog サポートはリリース 6.4 で導入されました。

- 430005：ファイルマルウェアイベント

  これらのイベントの Syslog サポートはリリース 6.4 で導入されました。

侵入イベントのフィールドの説明

（注） リリース 6.3 以降、空の値または不明な値を持つフィールドは Syslog メッセージに含まれません。

AccessControlRuleName

このフィールドはリリース 6.5 以降の該当する侵入イベントの Syslog メッセージに含まれます。

イベントを生成した侵入ルールを呼び出したアクセス コントロール ルール。[デフォルト アクション（Default Action）] は、ルールが有効化されている侵入ポリシーが特定のアクセス コントロール ルールに関連付けられておらず、代わりに、アクセス コントロール ポリシーのデフォルト アクションとして設定されていることを示しています。

次の場合、このフィールドは空になります（または、syslog メッセージの場合は省略されます）。

- 関連ルール/デフォルトアクションなし：侵入インスペクションは、アクセス制御ルールにもデフォルトアクションにも関連付けられていません。たとえば、システムが適用するルールを決定する前に通過する必要があるパケットを処理するために指定された侵入ポリシーによってパケットが検査された場合が該当します。(このポリシーは、アクセス制御ポリシーの [詳細（Advanced）] タブで指定されます。)
- [関連付けられている接続イベントなし（No associated connection event）]：セッションに記録された接続イベントがデータベースから消去されている場合。たとえば、接続イベントに侵入イベントよりも高いターンオーバーがある場合などです。

ACPolicy

イベントを生成した侵入ルール、プリプロセッサ ルール、またはデコーダ ルールが有効になっている侵入ポリシーに関連付けられているアクセス コントロール ポリシー。

ApplicationProtocol

（使用可能な場合）侵入イベントをトリガーとして使用したトラフィックで検出されたホスト間の通信を表す、アプリケーション プロトコル。

Classification

イベントを生成したルールが属する分類。

Client

（使用可能な場合）侵入イベントをトリガーとして使用したトラフィックで検出されたモニター対象のホストで実行されているソフトウェアを表す、クライアント アプリケーション。

このフィールドはリリース 6.5 で追加されました。

ある接続と別の同時接続を区別するカウンタ。このフィールドは、それ自体には意味がありません。

DeviceUUID、First Packet Time、Connection Instance ID、および Connection Counter フィールドの情報を総合すると、特定の侵入イベントに関連付けられた接続イベントを識別できます。

このフィールドはリリース 6.5 で追加されました。

接続イベントを処理した Snort インスタンス。このフィールドは、それ自体には意味がありません。

[DeviceUUID]、[First Packet Time]、[Connection Instance ID]、および [Connection Counter] フィールドの情報を総合すると、特定の侵入イベントに関連付けられた接続イベントを識別できます。

DeviceUUID

このフィールドはリリース 6.5 で追加されました。

イベントを生成したデバイスの一意の識別子。

DeviceUUID、First Packet Time、Connection Instance ID、および Connection Counter フィールドの情報を総合すると、特定の侵入イベントに関連付けられた接続イベントを識別できます。

DstIP

侵入イベントに関連する受信ホストが使用する IP アドレス。

DstPort

トラフィックを受信するホストのポート番号。ICMP トラフィックの場合は、ポート番号がないため、このフィールドには ICMP コードが表示されます。

EgressInterface

イベントをトリガーとして使用したパケットの出力インターフェイス。パッシブインターフェイスの場合、このインターフェイスの列には入力されません。

EgressZone

イベントをトリガーとして使用したパケットの出力セキュリティゾーン。パッシブ展開環境では、このセキュリティ ゾーンのフィールドには入力されません。

（FirstPacketSecond）

このフィールドはリリース 6.5 で追加されました。

システムが最初のパケットを検出した時間。

DeviceUUID、First Packet Time、Connection Instance ID、および Connection Counter フィールドの情報を総合すると、特定の侵入イベントに関連付けられた接続イベントを識別できます。

GID

ジェネレータ ID。イベントを生成したコンポーネントの ID。

HTTPResponse

イベントをトリガーした接続を介してクライアントの HTTP 要求に応答して送信される HTTP ステータス コード。HTTP 要求の成功と失敗の理由を示します。

ICMPCode

「**DstPort**」を参照してください。

ICMPType

「**SrcPort**」を参照してください。

IngressInterface

イベントをトリガーとして使用したパケットの入力インターフェイス。パッシブインターフェイスの場合、このインターフェイスの列だけに入力されます。

IngressZone

イベントをトリガーとして使用したパケットの入力セキュリティ ゾーンまたはトンネル ゾーン。パッシブ展開環境では、このセキュリティ ゾーン フィールドだけに入力されます。

InlineResult

このフィールドはバージョン 6.3 で Syslog を介して使用できるようになりました。

（注） このフィールドは、IPS ルールが「ドロップして生成する」に設定されている場合にのみ使用できます。

このフィールドは次の値を持ちます。

- **Dropped**：インライン展開環境でパケットがドロップされる場合
- **Would have dropped**：インライン展開環境でパケットをドロップするように侵入ポリシーが設定されていればパケットがドロップされた場合

パッシブ展開では、侵入ポリシーのルールの状態やインライン ドロップ動作に関係なく、インライン インターフェイスがタップ モードの場合を含めて、システムはパケットをドロップしません。

IntrusionPolicy

このフィールドはバージョン 6.4 で Syslog を介して使用できるようになりました。

イベントを生成した侵入ルール、プリプロセッサ ルール、またはデコーダ ルールが有効にされた侵入ポリシー。アクセス コントロール ポリシーのデフォルト アクションとして侵入ポリシーを選択するか、アクセス コントロール ルールと侵入ポリシーを関連付けることができます。

MPLS_Label

このフィールドはバージョン 6.3 で追加されました。

侵入イベントをトリガーしたパケットと関連付けられているマルチプロトコル ラベル スイッチング ラベル。

メッセージ

イベントを説明するテキスト。ルールベースの侵入イベントの場合、イベントメッセージはルールから取得されます。デコーダベースおよびプリプロセッサベースのイベントの場合は、イベント メッセージはハードコーディングされています。

ジェネレータおよび Snort ID（GID と SID）と SID バージョン（改訂）はカッコで囲んだコロン区切りの数字形式で各メッセージの末尾に付加されます（GID:SID:version）。例：`(1:36330:2)`。

NAPPolicy

イベントの生成に関連付けられているネットワーク分析ポリシー（ある場合）。

このフィールドには、取得された URI の最初の 50 文字が表示されます。省略 URI の表示部分にポインタを合わせると、最大 2048 バイトまでの完全な URI を表示することができます。また、最大 2048 バイトまでの完全な URI をパケット ビューに表示することもできます。

NumIOC

侵入イベントをトリガーとして使用したトラフィックが、接続に関係するホストに対する侵入の痕跡（IOC）もトリガーとして使用したかどうか。

Priority

Cisco Talos Intelligence Group（Talos） で指定されたイベントの優先度。優先度は、`priority` キーワードの値または `classtype` キーワードの値に対応します。その他の侵入イベントの場合、プライオリティはデコーダまたはプリプロセッサによって決定されます。有効な値は、[高（high）]、[中（medium）]、および [低（low）] です。

Protocol

http://www.iana.org/assignments/protocol-numbers に一覧表示されている、接続で使用するトランスポートプロトコルの名前または番号。これは、送信元および宛先ポート/ICMP の列と関連付けられたプロトコルです。

Revision

イベントの生成に使用された署名のバージョン。

SID

イベントを生成したルールの署名 ID（Snort ID ともいう）

SSLActualAction

システムが暗号化されたトラフィックに適用したアクション。

SrcIP

侵入イベントに関連する送信ホストが使用する IP アドレス。

SrcPort

送信元ホストのポート番号。ICMP トラフィックの場合は、ポート番号がないため、このフィールドには ICMP タイプが表示されます。

User

接続を開始したホストの IP アドレスに関連付けられたユーザー名。エクスプロイトの送信元ホストである場合とそうでない場合があります。このユーザー値は、通常、ネットワーク上のユーザーだけに知らされます。

リリース 6.5 以降： 該当する場合、ユーザー名の前には `<realm>\` が付いています。

VLAN_ID

このフィールドはバージョン 6.3 で追加されました。

侵入イベントをトリガーとして使用したパケットと関連付けられた最内部 VLAN ID。

WebApplication

侵入イベントをトリガーとして使用したトラフィックで検出された HTTP トラフィックの内容または要求された URL を表す、Web アプリケーション。

システムが HTTP のアプリケーション プロトコルを検出し、特定の Web アプリケーションを検出できなかった場合、システムは代わりに一般的な Web ブラウジング指定を提供します。

接続およびセキュリティ インテリジェンス イベントのフィールドの説明

（注） リリース 6.3 以降、空の値または不明な値を持つフィールドは Syslog メッセージに含まれません。

AccessControlRuleAction

接続をロギングした設定に関連付けられているアクション。

セキュリティインテリジェンスによってモニターされている接続の場合、そのアクションは、接続によってトリガーされる最初のモニター以外のアクセス コントロール ルールのアクションであるか、またはデフォルト アクションです。同様に、モニター ルールに一致するトラフィックは常に後続のルールまたはデフォルトアクションによって処理されるため、モニター ルールによってロギングされた接続と関連付けられたアクションが [モニター（Monitor）] になることはありません。ただし、モニタ ルールに一致する接続の相関ポリシー違反をトリガーする可能性があります。

アクション	説明
許可（Allow）	アクセス コントロールによって明示的に許可された、またはユーザーがインタラクティブ ブロックをバイパスしたために許可された接続。

アクション	説明
ブロック（Block）、リセットしてブロック（Block with reset）	次を含むブロックされた接続： • プレフィルタ ポリシーによってブロックされたトンネルおよびその他の接続 • セキュリティ インテリジェンスによってブロックされた接続 • SSL ポリシーによってブロックされた暗号化接続 • 侵入ポリシーによってエクスプロイトがブロックされた接続 • ファイル ポリシーによってファイル（マルウェアを含む）がブロックされた接続。 システムが侵入またはファイルをブロックする接続では、アクセス コントロールの許可ルールを使用してディープ インスペクションを呼び出す場合にも、システムはブロックを表示します。
高速パス（Fastpath）	プレフィルタ ポリシーによって高速パスが適用された暗号化されていないトンネルおよびその他の接続。
インタラクティブ ブロック（Interactive Block）、リセット付きインタラクティブ ブロック（Interactive Block with reset）	システムがインタラクティブ ブロック ルールを使用してユーザーの HTTP 要求を最初にブロックしたときにログに記録された接続。システムにより表示される警告ページでユーザーがクリックスルーすると、そのセッションでログに記録されるその後の接続に許可アクションが付きます。
信頼（Trust）	アクセス コントロールによって信頼された接続。デバイス モデルに応じて、システムは信頼された TCP 接続を別にログに記録します。
デフォルト アクション（Default Action）	アクセス コントロール ポリシーのデフォルト アクションによって処理される接続。
（空白/空）	ルールに一致するのに十分なパケットが渡される前に接続が閉じられました。 侵入防御などのアクセス制御以外の機能によって接続がログに記録される場合にのみ発生します。

AccessControlRuleName

接続を処理したアクセス コントロール ルールまたはデフォルト アクションと、その接続に一致した最大 8 つのモニター ルール。

接続が 1 つのモニター ルールに一致した場合、Secure Firewall Management Center は接続を処理したルールの名前を表示し、その後にモニター ルール名を表示します。接続が複数のモニター ルールに一致した場合、一致するモニター ルールの数が表示されます（`Default Action + 2 Monitor Rules` など）。

AccessControlRuleReason

接続がロギングされた 1 つまたは複数の原因（使用可能な場合）。

IP ブロック、DNS ブロック、および URL ブロックの理由による接続には、固有のイニシエータ レスポンダ ペアごとに 15 秒のしきい値があります。システムがこれらのいずれかの接続をブロックした後、イベントを生成した時点から 15 秒の間、この 2 つのホスト間で接続がブロックされたとしても、ポートやプロトコルの違いに関わらず、接続イベントを生成しません。

ACPolicy

接続をモニターしたアクセス コントロール ポリシー。

ApplicationProtocol

接続で検出された、ホスト間の通信を表すアプリケーション プロトコル。

Client

接続で検出されたクライアント アプリケーション。

接続に使用されている特定のクライアントをシステムが特定できなかった場合、このフィールドは汎用的な名称としてアプリケーション プロトコル名の後に「client」という語を付加して FTP client などと表示します。

ClientVersion

接続で検出されたクライアント アプリケーションのバージョン（使用可能な場合）。

このフィールドはリリース 6.5 で追加されました。

ある接続と別の同時接続を区別するカウンタ。このフィールドは、それ自体には意味がありません。

[DeviceUUID]、[First Packet Time]、[Connection Instance ID]、および [Connection Counter] フィールドの情報を総合すると、接続イベントを識別できます。

このフィールドはリリース 6.5 で追加されました。

接続イベントを処理した Snort インスタンス。このフィールドは、それ自体には意味がありません。

[DeviceUUID]、[First Packet Time]、[Connection Instance ID]、および [Connection Counter] フィールドの情報を総合すると、接続イベントを識別できます。

ConnectionDuration

このフィールドはバージョン 6.3 で導入されました。

このフィールドは、接続の最後にロギングが発生した場合にのみ、値が備わっています。接続開始の syslog メッセージでは、このフィールドは出力されません。その時点では不明であるためです。

接続終了の syslog メッセージでは、このフィールどは最初のパケットと最後のパケットまでの秒数が表示されます。短時間の接続ではゼロになることがあります。たとえば、syslog のタイムスタンプが 12:34:56 で ConnectionDuration が 5 の場合、最初のパケットは 12:34:51 に検出されました。

DestinationSecurityGroup

このフィールドはリリース 6.5 で導入されました。

接続に関係する宛先のセキュリティグループ。

このフィールドには、 **Destinationsecuritygrouptag**（使用可能な場合）の数値に関連付けられているテキスト値が保持されます。グループ名をテキスト値として使用できない場合、このフィールドには、[DestinationSecurityGroupTag] フィールドと同じ整数値が含まれます。

DestinationSecurityGroupTag

このフィールドはリリース 6.5 で導入されました。

接続に関係する宛先のセキュリティグループタグ（SGT）数値属性。

リリース 6.6 では、この値は [DestinationSecurityGroupType] フィールドで指定されたソースから取得されます。

リリース 6.5 では、この値は ISE（SXP またはユーザーセッションのいずれか）から取得されます。

「**SourceSecurityGroupTag**」も参照してください。

このフィールドはリリース 6.6 で導入されました。

このフィールドには、セキュリティグループタグを取得した送信元が表示されます。

値	説明
インライン	送信元 SGT 値はパケットからのものです
Session Directory	送信元 SGT 値は、セッション ディレクトリ トピックによる ISE からのものです
SXP	送信元 SGT 値は SXP トピックによる ISE からのものです

DeviceUUID

このフィールドはリリース 6.5 で追加されました。

イベントを生成したデバイスの一意の識別子。

[DeviceUUID]、[First Packet Time]、[Connection Instance ID]、および [Connection Counter] フィールドの情報を総合すると、接続イベントを識別できます。

DNS_Sinkhole

システムが接続をリダイレクトしたシンクホール サーバーの名前。

DNS_TTL

DNS サーバーが DNS リソース レコードをキャッシュする秒数。

DNSQuery

ドメイン名を検索するために接続でネーム サーバーに送信された DNS クエリ。

リリース 6.7 以降（実験段階の機能として）：

このフィールドには、DNS フィルタリングが有効になっている場合の URL フィルタリング一致のドメイン名も保持できます。この場合、[URL] フィールドは空白になり、[URL Category] フィールドと [URL Reputation] フィールドにはドメインに関連付けられた値が含まれます。

DNSRecordType

接続で送信された DNS クエリを解決するために使用された DNS リソース レコードのタイプ。

DNSResponseType

問い合わせ時に接続でネーム サーバーに返された DNS レスポンス。

DNSSICategory

「**URLSICategory**」を参照してください。

DstIP

セッションレスポンダの IP アドレス（宛先 IP アドレス）（および DNS 解決が有効化されている場合はホスト名）。

プレフィルタポリシーによってブロックされるか、または高速パスが適用されたプレーンテキストのパススルートンネルでは、イニシエータとレスポンダの IP アドレスはトンネルエンドポイント（トンネルの両側のネットワークデバイスのルーテッドインターフェイス）を表します。

DstPort

セッション レスポンダが使用するポート。

EgressInterface

接続に関連付けられた出力インターフェイス。展開に非対称のルーティング設定が含まれている場合は、入力と出力のインターフェイスが同じインラインペアに属する場合があります。

EgressVRF

このフィールドのサポートはバージョン 6.6 で追加されました。

仮想ルーティングおよびフォワーディングを使用するネットワークでは、トラフィックがネットワークから出るときに通過する仮想ルータの名前。

EgressZone

接続に関連付けられた出力セキュリティ ゾーン。

再ゾーン化されたカプセル化接続の場合、出力フィールドは空白になります。

Endpoint Profile

ISE で指定されたユーザーのエンドポイント デバイス タイプ。

このフィールドはリリース 6.5 で追加されました。

接続イベントが優先度の高いイベントであるかどうか。高優先度（`High`）のイベントは、侵入、セキュリティインテリジェンス、ファイル、またはマルウェアイベントに関連付けられた接続イベントです。他のすべてのイベントは低優先度（`Low`）イベントです。

FileCount

1 つ以上のファイルイベントに関連付けられている接続で検出またはブロックされたファイル（マルウェア ファイルを含む）の数。

このフィールドはリリース 6.5 で追加されました。

システムが最初のパケットを検出した時間。

[DeviceUUID]、[First Packet Time]、[Connection Instance ID]、および [Connection Counter] フィールドの情報を総合すると、接続イベントを識別できます。

HTTPReferer

接続で検出された HTTP トラフィックの要求 URL の参照元を示す HTTP 参照元（他の URL へのリンクを提供した Web サイト、他の URL からリンクをインポートした Web サイトなど）。

HTTPResponse

クライアントからの接続経由の HTTP 要求に応じて送信される HTTP ステータス コード。ステータスコードは、HTTP 要求の成功や失敗の理由を示します。

HTTP レスポンスコードの詳細については、RFC 2616（HTTP）の「Section 10」を参照してください。

ICMPCode

セッションレスポンダが使用する ICMP コード。

ICMPType

セッションイニシエータが使用する ICMP タイプ。

IngressInterface

接続に関連付けられた入力インターフェイス。展開に非対称のルーティング設定が含まれている場合は、入力と出力のインターフェイスが同じインラインペアに属する場合があります。

Ingressvrf

このフィールドのサポートはバージョン 6.6 で追加されました。

仮想ルーティングおよびフォワーディングを使用するネットワークでは、トラフィックがネットワークに入るときに通過する仮想ルータの名前。

IngressZone

接続に関連付けられた入力セキュリティ ゾーン。

再区分されたカプセル化接続では、元の入力セキュリティ ゾーンの代わりに、割り当てたトンネル ゾーンが入力フィールドに表示されます。

InitiatorBytes

セッション イニシエータが送信した合計バイト数。

InitiatorPackets

セッション イニシエータが送信した合計パケット数。

, IPReputationSICategory

「**URLSICategory**」を参照してください。

IPSCount

接続に関連付けられた侵入イベント（ある場合）の数。

NAPPolicy

イベントの生成に関連付けられているネットワーク分析ポリシー（NAP）（ある場合）。

NAT_InitiatorIP, NAT_ResponderIP

このフィールドのサポートはバージョン 7.1 で追加されました。

セッションのイニシエータまたはレスポンダの NAT 変換後の IP アドレス。

NAT_InitiatorPort, NAT_ResponderPort

このフィールドのサポートはバージョン 7.1 で追加されました。

セッションのイニシエータまたはレスポンダの NAT 変換後のポート。

NetBIOSDomain

セッションで使用された NetBIOS ドメイン。

originalClientSrcIP

X-Forwarded-For（XFF）、True-Client-IP、またはカスタム定義の HTTP ヘッダーからの、元のクライアント IP アドレス。このフィールドに入力するには、元のクライアントに基づいてプロキシ トラフィックを処理するアクセス コントロール ルールを有効にする必要があります。

Prefilter Policy

接続を処理したプレフィルタ ポリシー。

Protocol

接続に使用されるトランスポートプロトコルです。特定のプロトコルを検索するには、名前を使用するか、http://www.iana.org/assignments/protocol-numbers に記載されたプロトコルの番号を指定します。

ReferencedHost

接続のプロトコルが HTTP または HTTPS の場合、このフィールドにはそれぞれのプロトコルが使用していたホスト名が表示されます。

ResponderBytes

セッションレスポンダが受信した合計バイト数。

ResponderPackets

セッションレスポンダが受信した合計パケット数。

SecIntMatchingIP

どの IP アドレスが一致しているか。

有効な値：**None**、**Destination**、または**Source**。

セキュリティ グループ（Security Group）

リリース 6.5 では、このフィールドが **SourceSecurityGroupTag** フィールドに置き換えられ、**SourceSecurityGroup**、**DestinationSecurityGroupTag**、および **DestinationSecurityGroup** の新しいフィールドが導入されました。

接続に関係するパケットのセキュリティ グループ タグ（SGT）属性。SGT は、信頼ネットワーク内での、トラフィックの送信元の権限を指定します。セキュリティ グループ アクセス（Cisco TrustSec と Cisco ISE の両方に共通の機能）は、パケットがネットワークに入るときに属性を適用します。

SourceSecurityGroup

このフィールドはリリース 6.5 で導入されました。

接続に関係する送信元のセキュリティグループ。

このフィールドには、[SourceSecurityGroupTag]（使用可能な場合）の数値に関連付けられているテキスト値が保持されます。グループ名をテキスト値として使用できない場合、このフィールドには、[SourceSecurityGroupTag] フィールドと同じ整数値が含まれます。タグは、インラインデバイス（送信元SGT名が指定されていない）またはISE（送信元を指定している）から取得できます。

SourceSecurityGroupTag

リリース 6.5 では、**Security Group** フィールドがこのフィールドに置き換えられました。

接続に関係するパケットのセキュリティグループタグ（SGT）属性の数値表現。SGTは、信頼ネットワーク内での、トラフィックの送信元の権限を指定します。セキュリティ グループ アクセス（Cisco TrustSec と Cisco ISE の両方に共通の機能）は、パケットがネットワークに入るときに属性を適用します。

「**DestinationSecurityGroupTag**」も参加してください。

SourceSecurityGroupType

このフィールドはリリース 6.6 で導入されました。

このフィールドには、セキュリティグループタグを取得した送信元が表示されます。

値	説明
インライン	送信元 SGT 値はパケットからのものです
Session Directory	送信元 SGT 値は、セッション ディレクトリ トピックによる ISE からのものです
SXP	送信元 SGT 値は、SXP トピックによる ISE からのものです

SrcIP

セッションイニシエータ の IP アドレス（送信元 IP アドレス）（および DNS 解決が有効化されている場合はホスト名）。

プレフィルタポリシーによってブロックされるか、または高速パスが適用されたプレーンテキストのパススルートンネルでは、イニシエータとレスポンダの IP アドレスはトンネルエンドポイント（トンネルの両側のネットワークデバイスのルーテッドインターフェイス）を表します。

SrcPort

セッション イニシエータが使用するポート。

SSLActualAction

システムが SSL ポリシーの暗号化トラフィックに適用したアクション。

アクション	説明
ブロック/リセット付きブロック（Block/Block with reset）	ブロックされた暗号化接続を表します。
[復号（再署名）（Decrypt (Resign)）]	再署名サーバー証明書を使用して復号された発信接続を表します。
[復号（キーの交換）（Decrypt (Replace Key)）]	置き換えられた公開キーと自己署名サーバー証明書を使用して復号化された発信接続を表します。

アクション	説明
[復号（既知のキー）（Decrypt (Known Key)）]	既知の秘密キーを使用して復号化された着信接続を表します。
[デフォルトアクション（Default Action）]	接続がデフォルト アクションによって処理されたことを示します。
[復号しない（Do not Decrypt）]	システムが復号化しなかった接続を表します。

SSLCertificate

トラフィックを暗号化するための公開キー証明書に保存される次の情報：

- サブジェクト/発行元共通名（Subject/Issuer Common Name）
- サブジェクト/発行元組織（Subject/Issuer Organization）
- サブジェクト/発行元組織単位（Subject/Issuer Organization Unit）
- 有効期間の開始/終了（Not Valid Before/After）
- シリアル番号（Serial Number）
- 証明書フィンガープリント（Certificate Fingerprint）
- 公開キー フィンガープリント（Public Key Fingerprint）

SSLExpectedAction

有効なSSLルールで指定された、暗号化トラフィックに適用されると予想されるアクション。

SSLFlowStatus

システムが暗号化されたトラフィックの復号化に失敗した理由。

- 不明
- No Match
- Success
- Uncached Session
- 不明な暗号スイート
- サポートされていない暗号スイート

- Unsupported SSL Version
- SSL Compression Used
- Session Undecryptable in Passive Mode
- Handshake Error
- Decryption Error
- Pending Server Name Category Lookup
- Pending Common Name Category Lookup
- Internal Error
- Network Parameters Unavailable
- Invalid Server Certificate Handle
- Server Certificate Fingerprint Unavailable
- Cannot Cache Subject DN
- Cannot Cache Issuer DN
- Unknown SSL Version
- External Certificate List Unavailable
- External Certificate Fingerprint Unavailable
- Internal Certificate List Invalid
- Internal Certificate List Unavailable
- Internal Certificate Unavailable
- Internal Certificate Fingerprint Unavailable
- Server Certificate Validation Unavailable
- Server Certificate Validation Failure
- 無効なアクション（Invalid Action）

SSLPolicy

接続を処理した SSL ポリシー。

リリース 6.7 以降： アクセス コントロール ポリシーの詳細設定で TLS サーバーのアイデンティティ検出が有効になっている場合で、そのアクセス コントロール ポリシーに関連付けられている SSL ポリシーがない場合、このフィールドにはどの SSL イベントについても何も保持されません。

SSLRuleName

接続を処理した SSL ルールまたはデフォルト アクションと、その接続に一致した最初のモニター ルール。接続がモニター ルールに一致した場合、フィールドには接続を処理したルールの名前が表示され、その後にモニター ルール名が表示されます。

SSLServerCertStatus

これは、認証ステータスの SSL ルール条件が設定されている場合にのみ適用されます。暗号化されたトラフィックが SSL ルールに一致すると、このフィールドに次のサーバーの証明書のステータス値の 1 つ以上が表示されます。

- [自署（Self Signed）]
- Valid
- Invalid Signature
- Invalid Issuer
- Expired
- Unknown
- Not Valid Yet
- [失効（Revoked）]

復号できないトラフィックが SSL ルールと一致する場合、このフィールドには [未チェック（Not Checked）] と表示されます。

SSLServerName

クライアントが暗号化された接続を確立した相手側サーバーのホスト名。

SSLSessionID

TLS/SSL ハンドシェイク時にクライアントとサーバー間でネゴシエートされた 16 進数セッション ID。

SSLTicketID

TLS/SSL ハンドシェイク時に送信されたセッション チケット情報の 16 進数のハッシュ値。

SSLURLCategory

暗号化接続でアクセスされた URL の URL カテゴリ

システムが TLS/SSL アプリケーションを識別またはブロックする場合、要求された URL は暗号化トラフィック内にあるため、システムは、SSL 証明書に基づいてトラフィックを識別します。したがって TLS/SSL アプリケーションの場合、このフィールドは証明書に含まれる一般名を表示します。

SSLVersion

接続の暗号化に使用された TLS/SSL プロトコル バージョン。

- 不明
- SSLv2.0
- SSLv3.0
- TLSv1.0

- TLSv1.1
- TLSv1.2

SSSLCipherSuite

接続を暗号化するのに使用される暗号スイートを表すマクロ値。暗号スイート値の指定については、www.iana.org/assignments/tls-parameters/tls-parameters.xhtml を参照してください。

TCPFlags

NetFlow データから生成された接続において、接続で検出された TCP フラグ。

Tunnel または Prefilter Rule

トンネル ルール、プレフィルタ ルール、または接続を処理したプレフィルタ ポリシーのデフォルト アクション。

URL

セッション中にモニター対象のホストによって要求された URL。

リリース 6.7 以降（実験段階の機能として）：

[URL] 列が空で、DNS フィルタリングが有効になっている場合、[DNS Query] フィールドにドメインが表示され、[URL Category] と [URL Reputation] の値がドメインに適用されます。

URLCategory

セッション中にモニター対象ホストによって要求された URL のカテゴリ（使用可能な場合）。

リリース 6.7 以降（実験段階の機能として）：

[URL] 列が空で、DNS フィルタリングが有効になっている場合、[DNS Query] フィールドにドメインが表示され、[URL Category] と [URL Reputation] の値がドメインに適用されます。

URLReputation

セッション中にモニター対象ホストによって要求された URL のレピュテーション（使用可能な場合）。

リリース 6.7 以降（実験段階の機能として）：

[URL] 列が空で、DNS フィルタリングが有効になっている場合、[DNS Query] フィールドにドメインが表示され、[URL Category] と [URL Reputation] の値がドメインに適用されます。

URLSICategory、DNSSICategory、, IPReputationSICategory

接続でブロックされた URL、ドメイン、または IP アドレスを表すか、またはそれを含むオブジェクトの名前。セキュリティ インテリジェンスのカテゴリは、ネットワークオブジェクトまたはグループ、ブロックリスト、カスタム セキュリティ インテリジェンスのリストまたはフィード、監視に関連する TID カテゴリ、またはインテリジェンスフィードのカテゴリのいずれかの名前にすることができます。

User

セッションイニシエータにログインしていたユーザー。このフィールドに[認証なし（No Authentication）] が入力されている場合、ユーザー トラフィックは次のようになります。

- 関連付けられたアイデンティティ ポリシーがないアクセス コントロール ポリシーに一致しました。
- アイデンティティ ポリシーのいずれのルールにも一致しませんでした。

リリース 6.5 以降： 該当する場合、ユーザー名の前には `<realm>\` が付いています。

UserAgent

接続で検出された HTTP トラフィックから取得したユーザー エージェント文字列アプリケーションの情報。

VLAN_ID

このフィールドはバージョン 6.3 で Syslog を介して使用できるようになりました。

接続をトリガーしたパケットに関連付けられている最内部 VLAN ID。

WebApplication

接続で検出された HTTP トラフィックの内容または要求された URL を表す Web アプリケーション。

Web アプリケーションがイベントの URL に一致しない場合、そのトラフィックは通常、参照先のトラフィックです（アドバタイズメントのトラフィックなど）。システムは、参照先のトラフィックを検出すると、参照元のアプリケーションを保存し（可能な場合）、そのアプリケーションを Web アプリケーションとして表示します。

HTTP トラフィックに含まれる特定の Web アプリケーションをシステムが特定できなかった場合、このフィールドには [Web ブランジング（Web Browsing）] と表示されます。

ファイルおよびマルウェアイベントのフィールドの説明

ファイルおよびマルウェアイベントの Syslog メッセージはリリース 6.4 で使用できるようになりました。

（注）

- 空の値または不明な値を持つフィールドはセキュリティイベントの Syslog メッセージに含まれません。ただし、「Unknown」または類似の値を持つ判定はファイルおよびマルウェアイベントのメッセージに含まれます。
- ファイルおよびマルウェアイベントのステータスフィールドの値には、初期ステータスのみが反映します。これらのフィールドは更新されません。

ApplicationProtocol

管理対象デバイスがファイルを検出したトラフィックで使用されるアプリケーションプロトコル。

ArchiveDepth

アーカイブ ファイル内でファイルがネストされたレベル（存在する場合）。

ArchiveFileName

マルウェア ファイルが含まれていたアーカイブ ファイル（ある場合）の名前。

ArchiveFileStatus

調査中のアーカイブのステータス。次のいずれかの値になります。

- [保留中（Pending）]：アーカイブは調査中です
- [取得済み（Extracted）]：調査が問題なく正常に実行されました
- [失敗（Failed）]：システムのリソース不足のため調査に失敗しました。
- [深度の超過（Depth Exceeded）]：調査は正常に実行されましたが、アーカイブがネストされた調査の深度を超過しました
- [暗号化（Encrypted）]：部分的に正常に実行されましたが、アーカイブが暗号化されているか、暗号化されたアーカイブが含まれています
- [調査できませんでした（Not Inspectable）]：部分的に正常に実行されましたが、ファイルは形式が不正であるか破損しています

ArchiveSHA256

マルウェア ファイルを含むアーカイブ ファイル（ある場合）の SHA-256 ハッシュ値。

Client

1 つのホストで実行され、ファイルを送信するためにサーバーに依存するクライアントアプリケーション。

このフィールドはリリース 6.5 で追加されました。

ある接続と別の同時接続を区別するカウンタ。このフィールドは、それ自体には意味がありません。

[DeviceUUID]、[First Packet Time]、[Connection Instance ID]、および [Connection Counter] フィールドの情報を総合すると、特定のファイルまたはマルウェアイベントに関連付けられた接続イベントを一意に識別できます。

このフィールドはリリース 6.5 で追加されました。

接続イベントを処理した Snort インスタンス。このフィールドは、それ自体には意味がありません。

[DeviceUUID]、[First Packet Time]、[Connection Instance ID]、および [Connection Counter] フィールドの情報を総合すると、特定のファイルまたはマルウェアイベントに関連付けられた接続イベントを一意に識別できます。

DeviceUUID

このフィールドはリリース 6.5 で追加されました。

イベントを生成したデバイスの一意の識別子。

[DeviceUUID]、[First Packet Time]、[Connection Instance ID]、および [Connection Counter] フィールドの情報を総合すると、特定のファイルまたはマルウェアイベントに関連付けられた接続イベントを一意に識別できます。

DstIP

接続に応答したホストの IP アドレス。これは、FileDirection フィールドの値によってファイルの送信者または受信者の IP アドレスとなる場合があります。

FileDirection が **`Upload`** の場合、これはファイル受信者の IP アドレスです。

FileDirection が **`Download`** の場合、これはファイル送信者の IP アドレスです。

SrcIP も参照してください。

DstPort

DstIP で説明されている接続で使用されるポート。

FileAction

ファイルを検出したファイル ポリシー ルールに関連したアクション、および関連するファイル アクション オプション。

FileDirection

接続中にファイルがダウンロードされたか、またはアップロードされたか。値は次のとおりです。

- Download：ファイルは DstIP から SrcIP に転送されました。
- Upload：ファイルは SrcIP から DstIP に転送されました。

FileName

ファイルの名前。

FilePolicy

ファイルを検出したファイル ポリシー。

FileSandboxStatus

ファイルが動的分析のために送信されたかとその場合のステータスを示します。

FileSHA256

ファイルの SHA-256 ハッシュ値。

SHA256 値を得るには、ファイルが次のいずれかによって処理されている必要があります。

- [ファイルの保存（Store files）] が有効になっているファイル検出ファイル ルール。
- [ファイルの保存（Store files）] が有効になっているファイル ブロック ファイル ルール。
- マルウェア クラウド ルックアップ ファイル ルール
- マルウェア ブロック ファイル ルール

FileSize

The size of the file, in bytes.

ファイルが完全に受信される前にシステムがファイルのタイプを特定した場合は、ファイル サイズが計算されない場合があります。

FileStorageStatus

イベントに関連付けられたファイルのストレージ ステータス：

Stored

関連するファイルが現在保存されているすべてのイベントを返します。

Stored in connection

関連するファイルが現在保存されているかどうかに関係なく、関連するファイルをシステムがキャプチャおよび保存したすべてのイベントを返します。

Failed

関連するファイルをシステムが保存できなかったすべてのイベントを返します。

syslog フィールドには、初期のステータスのみが含まれています。これらのステータスは変更後のステータスを反映するようには更新されません。

FileType

ファイルのタイプ（HTML や MSEXE など）。

システムが最初のパケットを検出した時間。

[DeviceUUID]、[First Packet Time]、[Connection Instance ID]、および [Connection Counter] フィールドの情報を総合すると、特定のファイルまたはマルウェアイベントに関連付けられた接続イベントを一意に識別できます。

FirstPacketSecond

ファイルのダウンロード フローまたはアップロード フローが開始された時刻。

イベントが発生した時刻がメッセージ ヘッダーのタイムスタンプにキャプチャされます。

Protocol

接続に使用されたプロトコル（TCP や UDP など）。

SHA_Disposition

ファイルの性質：

[クリーン（Clean）]

AMP クラウドでそのファイルがクリーンとして分類されているか、ユーザがファイルをクリーン リストに追加したことを示します。クリーンのファイルがマルウェア テーブルに含められるのは、そのファイルがクリーンに変更された場合だけです。

Custom Detection

ユーザがカスタム検出リストにファイルを追加したことを示します。

Malware

AMP クラウドでそのファイルがマルウェアとして分類された、ローカル マルウェア分析でマルウェアとして識別された、またはファイル ポリシーで定義されたマルウェアしきい値をファイルの脅威スコアが超えたことを示します。

Unavailable

システムがAMPクラウドに問い合わせできなかったことを示します。この性質に関するイベントが、わずかながら存在する可能性があります。これは予期された動作です。

[不明（Unknown）]

システムが AMP クラウドに問い合わせましたが、ファイルの性質が割り当てられていませんでした。言い換えると、AMP クラウドがファイルを正しく分類していませんでした。

ファイルの後処理は、システムが AMP クラウドにクエリを実行したファイルについてのみ表示されます。

syslog フィールドには最初の後処理のみが反映されます。レトロスペクティブな判定を反映するようには更新されません。

SperoDisposition

SPERO 署名がファイル分析で使用されたかどうかを示します。有効な値：

- ファイルで実行された Spero の検出
- ファイルで実行されなかった Spero の検出

SrcIP

接続を開始したホストの IP アドレス。これは、FileDirection フィールドの値によってファイルの送信者または受信者の IP アドレスとなる場合があります。

FileDirection が **`Upload`** の場合、これはファイル送信者の IP アドレスです。

FileDirection が **`Download`** の場合、これはファイル受信者の IP アドレスです。

DstIP も参照してください。

SrcPort

SrcIP で説明されている接続で使用されるポート。

SSLActualAction

システムが暗号化されたトラフィックに適用したアクション。

Block または Block with reset

ブロックされた暗号化接続を表します。

[復号（再署名）（Decrypt (Resign)）]

再署名サーバー証明書を使用して復号された発信接続を表します。

[復号（キーの交換）（Decrypt (Replace Key)）]

置き換えられた公開キーと自己署名サーバー証明書を使用して復号化された発信接続を表します。

[復号（既知のキー）（Decrypt (Known Key)）]

既知の秘密キーを使用して復号化された着信接続を表します。

[デフォルトアクション（Default Action）]

接続がデフォルト アクションによって処理されたことを示します。

[復号しない（Do not Decrypt）]

システムが復号化しなかった接続を表します。

SSLCertificate

TLS/SSL サーバーの証明書のフィンガープリント。

SSLFlowStatus

システムが暗号化されたトラフィックの復号化に失敗した理由。

- 不明
- No Match
- Success
- Uncached Session

- 不明な暗号スイート
- サポートされていない暗号スイート
- Unsupported SSL Version
- SSL Compression Used
- Session Undecryptable in Passive Mode
- Handshake Error
- Decryption Error
- Pending Server Name Category Lookup
- Pending Common Name Category Lookup
- Internal Error
- Network Parameters Unavailable
- Invalid Server Certificate Handle
- Server Certificate Fingerprint Unavailable
- Cannot Cache Subject DN
- Cannot Cache Issuer DN
- Unknown SSL Version
- External Certificate List Unavailable
- External Certificate Fingerprint Unavailable
- Internal Certificate List Invalid
- Internal Certificate List Unavailable
- Internal Certificate Unavailable
- Internal Certificate Fingerprint Unavailable
- Server Certificate Validation Unavailable
- Server Certificate Validation Failure
- 無効なアクション（Invalid Action）

ThreatName

検出されたマルウェアの名前。

ThreatScore

このファイルに関連付けられている最新の脅威スコア。これは、動的分析中に観察された悪意がある可能性がある動作に基づいた 0 ～ 100 の値です。

URI

ファイルトランザクションに関連付けられている接続のURI。たとえば、ユーザーがファイルをダウンロードした URL など。

User

接続を開始した IP アドレスに関連付けられているユーザー名。この IP アドレスがネットワークの外部にある場合、関連付けられているユーザー名は通常不明です。

リリース 6.5 以降： 該当する場合、ユーザー名の前には `<realm>\` が付いています。

ファイルイベントおよび Firepower デバイスによって生成されたマルウェアイベントの場合、このフィールドには、ID ポリシーまたは権限のあるログインによって決定されたユーザー名が表示されます。ID ポリシーがない場合、認証は必要ありませんと表示されます。

WebApplication

接続で検出されたHTTP トラフィックについて、内容を表すまたはURL を要求したアプリケーション。

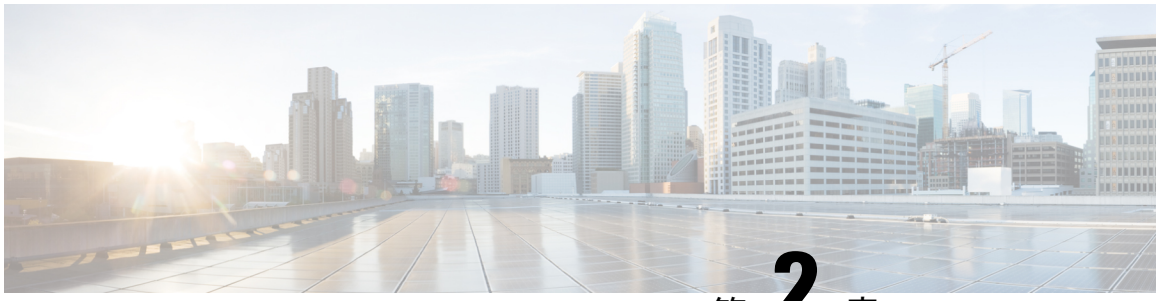
セキュリティイベントの Syslog メッセージの履歴

機能	バージョン	詳細
DNS フィルタ処理の更新	7.0 6.7（実験段階の機能）	DNS フィルタ処理が有効な場合： • DNSQuery フィールドは、一致する DNS フィルタ処理に関連付けられたドメインを保留できます。 • URL フィールドが空で、DNSQuery、URLCategory、および URLReputation には値がある場合、イベントは DNS フィルタ処理機能によって生成され、カテゴリとレピュテーションが DNSQuery で指定されたドメインに適用されます。 • 詳細については、Management Center オンラインヘルプで DNS フィルタ処理とイベントに関する情報を参照してください。

機能	バージョン	詳細
SGT と VRF の新しい接続イベントフィールド	6.6	新しいセキュリティグループのフィールド： • DestinationSecurityGroupType • SourceSecurityGroupType 仮想ルーティングおよびフォーワディングフィールド： • IngressVRF • EgressVRF
SGT の新しい接続イベントフィールド	6.5	新しいセキュリティグループのフィールド： • SourceSecurityGroup • SourceSecurityGroupTag （Security Group フィールドがこれに置き換えられます） • [DestinationSecurityGroup] • [DestinationSecurityGroupTag]
新しい接続イベントフィールド：Event Priority	6.5	Event Priority フィールドが導入されました。
Syslog の接続イベントの固有識別子	6.5	Syslog の [DeviceUUID]、[First Packet Time]、[Connection Instance ID]、および [Connection Counter] フィールドの情報を総合すると、接続イベントを識別できます。これらのフィールドは、侵入、ファイル、およびマルウェアイベントの Syslog にも含まれます。
ファイルとマルウェアのイベントの syslog サポート	6.4	ファイルおよびマルウェアイベントのフィールドを Syslog を介して使用できるようになりました。 詳細については、セキュリティイベントの Syslog メッセージの ID （1 ページ） および ファイルおよびマルウェアイベントのフィールドの説明 （19 ページ） を参照してください。

機能	バージョン	詳細
侵入イベントのフィールドのリストに追加された IntrusionPolicy フィールド	6.4	侵入イベントの syslog が、イベントをトリガーした侵入ポリシーを指定するようになりました。
接続および侵入イベントのサポートが改善された	6.3	接続イベント、セキュリティインテリジェンスイベント、および侵入イベントは、完全修飾イベントとして使用できるようになりました。
セキュリティイベントのイベントタイプ ID	6.3	接続、セキュリティ インテリジェンス、および侵入イベントのメッセージには、メッセージヘッダーにイベントタイプ ID が含まれています。 詳細については、セキュリティイベントの Syslog メッセージの ID （1 ページ）を参照してください。
セキュリティ イベント メッセージに含まれる空の値と不明な値の省略	6.3	空の値または不明な値を持つフィールドは、接続、セキュリティ インテリジェンス、および侵入イベントの Syslog メッセージから省略されます。
ドキュメンテーションの改善	6.3	接続、セキュリティ インテリジェンス、および侵入イベントに関する Syslog フィールド名と説明の追加ドキュメント （この機能は、このリリースでは新規ではありません。）

機能	バージョン	詳細
Firepower（SFIMS）イベントログ形式	6.2.2	Apr 30 04:33:28 192.168.1.1 Apr 30 13:57:38 firepower SFIMS: Protocol: ICMP, SrcIP: 172.16.10.10, OriginalClientIP: ::, DstIP: 172.16.20.10, ICMPType: Echo Request, ICMPCode: 0, TCPFlags: 0x0, IngressInterface: inside, EgressInterface: outside, DE: Primary Detection Engine (e357206c-a9b0-11eb-93fe-a690508a381d), Policy: Default Allow All Traffic, ConnectType: Start, AccessControlRuleName: test, AccessControlRuleAction: Allow, Prefilter Policy: Unknown, UserName: No Authentication Required, Client: ICMP client, ApplicationProtocol: ICMP, InitiatorPackets: 1, ResponderPackets: 0, InitiatorBytes: 74, ResponderBytes: 0, NAPPolicy: Balanced Security and Connectivity, DNSResponseType: No Error, Sinkhole: Unknown, URLCategory: Unknown, URLReputation: Risk unknown
Firepower（NULL）イベントログ形式	6.6.3	Apr 30 02:07:02 192.168.1.1 2021-04-30T11:31:19Z firepower (null) %NGIPS-1-430002: EventPriority: Low, DeviceUUID: b2433c5c-a6a1-11eb-a6e7-be0b9833091f, InstanceID: 2, FirstPacketSecond: 2021-04-30T11:31:19Z, ConnectionID: 4, AccessControlRuleAction: Allow, SrcIP: 172.16.10.10, DstIP: 172.16.20.10, ICMPType: Echo Request, ICMPCode: No Code, Protocol: icmp, IngressInterface: inside, EgressInterface: outside, ACPolicy: Default Allow All Traffic, AccessControlRuleName: test, Client: ICMP client, ApplicationProtocol: ICMP, InitiatorPackets: 1, ResponderPackets: 0, InitiatorBytes: 74, ResponderBytes: 0, NAPPolicy: Balanced Security and Connectivity



第 2 章

Syslog メッセージ 101001 ～ 199021

この章は、次の項で構成されています。

メッセージ 101001 ～ 109213

この項では、101001 から 109213 までのメッセージについて説明します。

101001

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

説明フェールオーバー ケーブルが接続され、正常に機能しています。Primary は、セカンダリ装置の場合は Secondary と示されることもあります。

推奨アクション 不要。

101002

エラーメッセージ `%Threat Defense-1-101002: (Primary) Bad failover cable.`

説明フェールオーバー ケーブルが接続されていますが、正常に機能していません。Primaryは、セカンダリ装置の場合は Secondary と示されることもあります。

推奨アクション フェールオーバー ケーブルを交換します。

101003、101004

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

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

説明フェールオーバー モードがイネーブルになっていますが、フェールオーバー ケーブルがフェールオーバー ペアの一方の装置に接続されていません。Primary は、セカンダリ装置の場合は Secondary と示されることもあります。

推奨アクション フェールオーバー ケーブルをフェールオーバー ペアの両方の装置に接続します。

101005

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

説明フェールオーバー ケーブルが接続されていますが、プライマリ装置が自分のステータスを判断できません。

推奨アクション ケーブルを交換します。

103001

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

説明プライマリ装置がフェールオーバー ケーブル経由でセカンダリ装置と通信できません。Primary は、セカンダリ装置の場合は Secondary と示されることもあります。次の表に、フェールオーバーが発生した原因を判断するための原因コードおよび説明を示します。

原因コード	説明
1	ローカル装置が、LAN フェールオーバーが発生した場合はフェールオーバー LAN インターフェイス上で、シリアルフェールオーバーが発生した場合はシリアルフェールオーバーケーブル上で、hello パケットを受信しておらず、ピアがダウンしたと宣言しています。

原因コード	説明
2	インターフェイスが 4 つのフェールオーバー テストのうちのいずれか 1 つを通過させませんでした。4つのテストは、1）Link Up、2）Monitor for Network Traffic、3）ARP、および 4）Broadcast Ping です。
3	シリアル ケーブルでコマンドが送信された後 15 秒以上適切な ACK が受信されません。
4	フェールオーバー LAN インターフェイスがダウンし、他のデータ インターフェイスは、別のインターフェイスのテストに応答していません。また、ローカル装置はピアがダウンしていることを宣言しています。
5	コンフィギュレーション同期化プロセス中に、スタンバイ ピアがダウンしました。
6	複製が完了していません。フェールオーバー ユニットは同期されません。

推奨アクション フェールオーバー ケーブルが正しく接続され、両方の装置が同じハードウェア、ソフトウェア、およびコンフィギュレーションになっ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。

103002

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

説明セカンダリ装置のネットワーク インターフェイスが正常であることをプライマリ装置が検出しました。Primary は、セカンダリ装置の場合は Secondary と示されることもあります。

推奨アクション 不要。

103003

エラーメッセージ `%Threat Defense-1-103003: (Primary) Other firewall network interface interface_number failed.`

説明セカンダリ装置に不良ネットワーク インターフェイスをプライマリ装置が検出しました。Primary は、セカンダリ装置の場合は Secondary と示されることもあります。

推奨アクション セカンダリ装置のネットワーク接続とネットワーク ハブ接続を確認します。必要に応じて、障害の発生したネットワーク インターフェイスを交換します。

103004

エラーメッセージ `%Threat Defense-1-103004: (Primary) Other firewall reports this firewall failed. Reason: reason-string`

説明プライマリ装置に障害が発生していることを示すメッセージをプライマリ装置がセカンダリ装置から受信しました。Primaryは、セカンダリ装置の場合はSecondaryと示されることもあります。理由は、次のいずれかになります。

- フェールオーバー コマンド インターフェイスのポーリング パケット失敗がしきい値を超過しました。
- LAN フェールオーバー インターフェイスが失敗しました。
- ピアが Standby Ready 状態への移行に失敗しました。
- コンフィギュレーションの完全なレプリケーションに失敗しました。このファイアウォールのコンフィギュレーションが同期していない可能性があります。
- フェールオーバー メッセージの送信に失敗し、受信使用状態の ACK が受信されません。

推奨アクション プライマリ装置のステータスを確認します。

103005

エラーメッセージ `%Threat Defense-1-103005: (Primary) Other firewall reporting failure. Reason: SSM card failure`

説明 セカンダリ装置がプライマリ装置にSSMカードの障害を報告しました。Primaryは、セカンダリ装置の場合はSecondaryと示されることもあります。

推奨アクション セカンダリ装置のステータスを確認します。

103006

エラーメッセージ `%Threat Defense-1-103006: (Primary|Secondary) Mate version ver_num is not compatible with ours ver_num`

説明 ローカル装置と異なるバージョンを実行している、HA Hitless Upgrade機能と互換性がないピア装置をSecure Firewall Threat Defenseデバイス が検出しました。

- *ver_num*：バージョン番号

推奨アクション 両方の装置に、同じバージョンまたは互換性のあるバージョンのイメージをインストールします。

103007

エラーメッセージ `%Threat Defense-1-103007: (Primary|Secondary) Mate version ver_num is not identical with ours ver_num`

説明 ピア装置で実行されているバージョンがローカル装置と異なるが、Hitless Upgradeをサポートしており、ローカル装置と互換性があることをSecure Firewall Threat Defenseデバイス が検出しました。イメージのバージョンが異なるために、システムのパフォーマンスが低下するおそれがあります。また、異なるイメージを長期間実行すると、Secure Firewall Threat Defenseデバイス で安定性の問題が発生する可能性があります。

- **ver_num**：バージョン番号

推奨アクション できるだけ早く、両方の装置に同じバージョンのイメージをインストールします。

103008

エラーメッセージ `%Threat Defense-1-103008: Mate hwdib index is not compatible`

説明 アクティブ装置とスタンバイ装置のインターフェイス数が同じではありません。

推奨アクション ユニット間のインターフェイスの数が同じであることを確認します。場合によって、追加のインターフェイスモジュールを取り付けるか、または別のデバイスを使用する必要があります。物理インターフェイスが一致したら、HAを一時停止してから再開することで、設定の同期を強制します。

104001、104002

エラーメッセージ `%Threat Defense-1-104001: (Primary) Switching to ACTIVE (cause: string).`

エラーメッセージ `%Threat Defense-1-104002: (Primary) Switching to STANDBY (cause: string ).`

説明スタンバイ装置で**failover active** コマンドを入力するか、またはアクティブ装置で**no failover active** コマンドを入力することによって強制的にフェールオーバー ペアの役割が切り替えられました。Primary は、セカンダリ装置の場合は Secondary と示されることもあります。string 変数の値は次のとおりです。

- state check
- bad/incomplete config
- ifc [interface] check, mate is healthier
- the other side wants me to standby
- in failed state, cannot be active
- switch to failed state
- other unit set to active by CLI config command fail active

推奨アクション 手作業による介入が原因でメッセージが表示される場合は、処置は不要です。それ以外の場合は、セカンダリ装置から報告された原因を使用して、ペアの装置両方のステータスを確認します。

104003

エラーメッセージ `%Threat Defense-1-104003: (Primary) Switching to FAILED.`

説明プライマリ装置に障害が発生しました。

推奨アクションプライマリ装置のメッセージを確認して、問題の内容を示す表示がないかどうかを調べます（メッセージ 104001 を参照）。Primary は、セカンダリ装置の場合は Secondary と示されることもあります。

104004

エラーメッセージ `%Threat Defense-1-104004: (Primary) Switching to OK.`

説明前に障害になった装置が再び動作していると報告しました。Primary は、セカンダリ装置の場合は Secondary と示されることもあります。

推奨アクション 不要。

105001

エラーメッセージ `%Threat Defense-1-105001: (Primary) Disabling failover.`

説明バージョン 7.x 以降では、このメッセージは、モードのミスマッチ（シングルまたはマルチ）、ライセンスのミスマッチ（暗号化またはコンテキスト）、またはハードウェアの相違（一方の装置には IPS SSM がインストールされ、そのピアには CSC SSM がインストールされている）が原因でフェールオーバーが自動的にディセーブルになったことを示す場合があります。Primary は、セカンダリ装置の場合は Secondary と示されることもあります。

推奨アクション 不要。

105002

エラーメッセージ `%Threat Defense-1-105002: (Primary) Enabling failover.`

説明これまでフェールオーバーをディセーブルにしていたコンソールで引数を指定せずに **failover** コマンドが使用されました。Primary は、セカンダリ装置の場合は Secondary と示されることもあります。

推奨アクション 不要。

105003

エラーメッセージ `%Threat Defense-1-105003: (Primary) Monitoring on interface interface_name waiting`

説明 Secure Firewall Threat Defense デバイスが指定されたネットワーク インターフェイス（フェールオーバー ペアの相手装置とのインターフェイス）をテストしています。Primary は、セカンダリ装置の場合は Secondary と示されることもあります。

（注） 実際のステータスの変化と比較すると、syslog のロギングに遅延が生じる可能性があります。この遅延は、インターフェイスモニターリング用に設定されたポーリング時間とホールド時間によるものです。

推奨アクション 不要。Secure Firewall Threat Defense デバイス は、正常動作中に自分のネットワーク インターフェイスを頻繁にモニターします。

105004

エラーメッセージ `%Threat Defense-1-105004: (Primary) Monitoring on interface interface_name normal`

説明指定されたネットワーク インターフェイスのテストが成功しました。Primary は、セカンダリ装置の場合は Secondary と示されることもあります。

（注） 実際のステータスの変化と比較すると、syslog のロギングに遅延が生じる可能性があります。この遅延は、インターフェイスモニターリング用に設定されたポーリング時間とホールド時間によるものです。

推奨アクション 不要。

105005

エラーメッセージ `%Threat Defense-1-105005: (Primary) Lost Failover communications with mate on interface interface_name.`

説明フェールオーバーペアの一方の装置がペアの相手装置と通信できなくなりました。Primary は、セカンダリ装置の場合は Secondary と示されることもあります。

推奨アクション指定されたインターフェイスに接続されているネットワークが正しく機能していることを確認します。

105006、105007

エラーメッセージ`%Threat Defense-1-105006: (Primary) Link status Up on interface interface_name.`

エラーメッセージ `%Threat Defense-1-105007: (Primary) Link status Down on interface interface_name.`

説明指定されたインターフェイスのリンク ステータスのモニタリング結果が報告されました。Primary は、セカンダリ装置の場合は Secondary と示されることもあります。

推奨アクション リンク ステータスがダウンである場合は、指定されたインターフェイスに接続されているネットワークが正しく動作していることを確認します。

105008

エラーメッセージ `%FTD-1-105008: (Primary) Testing interface interface_name.`

説明指定されたネットワーク インターフェイスのテストが行われました。このテストは、想定された間隔後にSecure Firewall Threat Defense デバイスがそのインターフェイス上でスタンバイ装置からメッセージを受け取ることができなかった場合に限って実行されます。Primary は、セカンダリ装置の場合は Secondary と示されることもあります。

推奨アクション 不要。

105009

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

説明前のインターフェイス テストの結果（Passed または Failed）が報告されました。Primary は、セカンダリ装置の場合は Secondary と示されることもあります。

推奨アクション結果が Passed であれば不要です。結果が Failed の場合は、両方のフェールオーバー装置へのネットワーク ケーブル接続、およびネットワーク自体が正しく機能していることをチェックし、スタンバイ装置のステータスを確認します。

105010

エラーメッセージ `%Threat Defense-3-105010: (Primary) Failover message block alloc failed.`

説明ブロック メモリが枯渇しました。これは一時メッセージで、Secure Firewall Threat Defense デバイスは回復する必要があります。Primaryは、セカンダリ装置の場合はSecondaryと示されることもあります。

推奨アクション show blocks コマンドを使用して、現在のブロック メモリをモニターします。

105011

エラーメッセージ `%Threat Defense-1-105011: (Primary) Failover cable communication failure`

説明フェールオーバー ケーブルがプライマリ装置とセカンダリ装置間の通信を許可していません。Primary は、セカンダリ装置の場合は Secondary と示されることもあります。

推奨アクション ケーブルが正しく接続されていることを確認します。

105020

エラーメッセージ `%Threat Defense-1-105020: (Primary) Incomplete/slow config replication`

説明フェールオーバーが発生すると、アクティブな Secure Firewall Threat Defense デバイス はメモリ内の不完全なコンフィギュレーションを検出します。通常、これは複製サービスの中断が原因となっています。Primaryは、セカンダリ装置の場合はSecondaryと示されることもあります。

推奨アクション Secure Firewall Threat Defense デバイス がフェールオーバーを検出した後、Secure Firewall Threat Defense デバイス は自動的にリブートして、フラッシュ メモリからコンフィギュレーションをロードするか、または別の Secure Firewall Threat Defense デバイス と再同期化します（両方行うこともあります）。フェールオーバーが引き続き発生する場合は、フェールオーバー コンフィギュレーションを調べて、両方の Secure Firewall Threat Defense デバイス 装置が互いに通信できることを確認します。

105021

エラーメッセージ `%Threat Defense-1-105021: (failover_unit ) Standby unit failed to sync due to a locked context_name config. Lock held by lock_owner_name`

説明コンフィギュレーションの同期化中に、他の何らかのプロセスが 5 分を超えてコンフィギュレーションをロックして、フェールオーバープロセスが新しいコンフィギュレーションを適用するのを妨げている場合、スタンバイ装置は自分自身をリロードします。これは、コンフィギュレーション同期化の進行中に、管理者がスタンバイ装置で実行コンフィギュレーションに目を通している場合に発生することがあります。コマンドリファレンスガイドで、特権 EXEC モードの **show running-config** コマンドと、グローバル コンフィギュレーション モードの **pager lines num** コマンドも参照してください。

推奨アクションスタンバイ装置が最初にブートし、アクティブ装置とのフェールオーバー接続を確立している間は、スタンバイ装置でコンフィギュレーションを表示または修正しないでください。

105022

エラーメッセージ `%FTD-1-105022: (host) Config replication failed with reason = (reason)`

説明 高可用性レプリケーションが失敗すると、このメッセージが生成されます。それぞれの説明は次のとおりです。

- *host*：現在のフェールオーバーユニット、つまりプライマリまたはセカンダリを示します。
- *reason*：フェールオーバー コンフィギュレーション レプリケーション終了のタイムアウト期限の理由。
  - CFG_SYNC_TIMEOUT：アクティブからスタンバイへの設定の複製時に 60 秒のタイマーが経過したため、デバイスの再起動が開始されます。
  - CFG_PROGRESSION_TIMEOUT：高可用性構成の複製を管理する 6 時間のタイマーが経過しました。

推奨アクション なし。

105031

エラーメッセージ `%Threat Defense-1-105031: Failover LAN interface is up`

説明 LAN フェールオーバー インターフェイス リンクがアップしています。

推奨アクション 不要。

105032

エラーメッセージ `%Threat Defense-1-105032: LAN Failover interface is down`

説明 LAN フェールオーバー インターフェイス リンクがダウンしています。

推奨アクション LAN のフェールオーバー インターフェイスの接続を確認します。速度または二重通信の設定が正しいことを確認します。

105033

エラーメッセージ `%Threat Defense-1-105033: LAN FO cmd Iface down and up again`

説明 フェールオーバーの LAN インターフェイスがダウンしました。

推奨アクション フェールオーバー リンクを確認します。通信の問題の可能性があります。

105034

エラーメッセージ `%Threat Defense-1-105034: Receive a LAN_FAILOVER_UP message from peer.`

説明 ピアがブートされて、初期コンタクト メッセージが送信されました。

推奨アクション 不要。

105035

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

説明ピア LAN フェールオーバー インターフェイス リンクがダウンしています。装置がスタンバイ モードになっている場合、アクティブ モードに切り替わります。

推奨アクション ピア LAN のフェールオーバー インターフェイスの接続を確認します。

105036

エラーメッセージ `%Threat Defense-1-105036: dropped a LAN Failover command message.`

説明 Secure Firewall Threat Defense デバイス は無応答の LAN フェールオーバー コマンド メッセージを廃棄しました。これは LAN フェールオーバー インターフェイスに接続障害が存在することを示します。

推奨アクション LAN インターフェイス ケーブルが接続されていることを確認します。

105037

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

説明プライマリ装置およびスタンバイ装置がアクティブ装置として交互に切り替わっています。これは、LAN フェールオーバー接続障害またはソフトウェアのバグが存在することを示します。

推奨アクション LAN インターフェイス ケーブルが接続されていることを確認します。

105038

エラーメッセージ `%Threat Defense-1-105038: (Primary) Interface count mismatch`

説明フェールオーバーが発生すると、アクティブな Secure Firewall Threat Defense デバイス はメモリ内の不完全なコンフィギュレーションを検出します。通常、これは複製サービスの中断が原因となっています。Primary は、セカンダリ装置の場合は Secondary と示されることもあります。

推奨アクション Secure Firewall Threat Defense デバイス によってフェールオーバーが検出されると、Secure Firewall Threat Defense デバイス は自動的にリブートして、フラッシュ メモリからコンフィギュレーションをロードするか、または別の Secure Firewall Threat Defense デバイスと再同期化します（両方行うこともあります）。フェールオーバーが引き続き発生する場合は、フェールオーバー コンフィギュレーションを調べて、両方の Secure Firewall Threat Defense デバイス 装置が互いに通信できることを確認します。

105039

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

説明 フェールオーバーは最初にプライマリおよびセカンダリの Secure Firewall Threat Defense デバイス で設定されているインターフェイスの数が同じであることを確認します。このメッセージは、セカンダリのSecure Firewall Threat Defense デバイスで設定されているインターフェイスの数をプライマリのSecure Firewall Threat Defense デバイスが確認できないことを示します。このメッセージは、プライマリ Secure Firewall Threat Defense デバイス がフェールオーバーインターフェイス経由でセカンダリ Secure Firewall Threat Defense デバイス と通信できないことを示します。Primary は、セカンダリ装置の場合は Secondary と示されることもあります。

推奨アクション プライマリおよびセカンダリの Secure Firewall Threat Defense デバイス のフェールオーバー LAN、インターフェイス設定、ステータスを確認します。セカンダリの Secure Firewall Threat Defense デバイス が Secure Firewall Threat Defense デバイス アプリケーションを実行しており、フェールオーバーがイネーブルであることを確認します。

105040

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

説明 プライマリおよびセカンダリの Secure Firewall Threat Defense デバイス は、フェールオーバー ペアとして動作するために同じフェールオーバー ソフトウェアのバージョンを実行する必要があります。このメッセージは、セカンダリのSecure Firewall Threat Defense デバイス フェールオーバー ソフトウェアのバージョンがプライマリのSecure Firewall Threat Defense デバイスと互換性がないことを示します。フェールオーバーがプライマリのSecure Firewall Threat Defense デバイスでディセーブルになっています。Primary は、セカンダリの Secure Firewall Threat Defense デバイス の場合は Secondary と示されることもあります。

推奨アクション フェールオーバーをイネーブルにするために、プライマリおよびセカンダリの Secure Firewall Threat Defense デバイス 間で一致したソフトウェア バージョンを使用します。

105041

エラーメッセージ `%Threat Defense-1-105041: cmd failed during sync`

説明 アクティブ装置とスタンバイ装置のインターフェイス数が同じではないため、nameif コマンドの複製に失敗しました。

推奨アクション ユニット間のインターフェイスの数が同じであることを確認します。場合によって、追加のインターフェイス モジュールを取り付けるか、または別のデバイスを使用する必要があります。物理インターフェイスが一致したら、HA を一時停止してから再開することで、設定の同期を強制します。

105042

エラーメッセージ `%Threat Defense-1-105042: (Primary) Failover interface OK`

説明 フェールオーバーメッセージを送信するインターフェイスは、フェールオーバーリンクの物理ステータスがダウンしている場合、またはフェールオーバーピア間の L2 接続が失われ、その結果 ARP パケットがドロップされる場合にダウンする可能性があります。このメッセージは、L2 ARP 接続を復元した後に生成されます。

推奨アクション 不要。

105043

エラーメッセージ `%Threat Defense-1-105043: (Primary) Failover interface failed`

説明 この Syslog は、フェールオーバーリンクの物理ステータスがダウンしている場合、またはフェールオーバーピア間の L2 接続が失われた場合に生成されます。切断すると、ユニット間の ARP パケットが失われます。

推奨処置

- フェールオーバーリンクの物理ステータスを確認し、物理ステータスと動作ステータスが機能していることを確認します。
- ARP パケットがフェールオーバーペア間のフェールオーバーリンクの中継パスを通過することを確認します。

105044

エラーメッセージ `%Threat Defense-1-105044: (Primary) Mate operational mode mode is not compatible with my mode mode.`

説明動作モード（シングルまたはマルチ）がフェールオーバー ピア間で一致しない場合、フェールオーバーはディセーブルになります。

推奨アクション 同じ動作モードになるようにフェールオーバー ピアを設定してから、フェールオーバーを再度イネーブルにします。

105045

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

説明フィーチャ ライセンスがフェールオーバー ピア間で一致しない場合、フェールオーバーはディセーブルになります。

推奨アクション 同じフィーチャ ライセンスになるようにフェールオーバー ピアを設定してから、フェールオーバーを再度イネーブルにします。

105046

エラーメッセージ `%Threat Defense-1-105046: (Primary|Secondary) Mate has a different chassis`

説明 2つのフェールオーバー装置が異なるタイプのシャーシを持っています。たとえば、一方が 3 スロットのシャーシを持ち、もう一方が 6 スロットのシャーシを持つ場合です。

推奨アクション 2 つのフェールオーバー装置が同じであることを確認します。

105047

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

説明 2つのフェールオーバー装置は、対応するスロットに異なるタイプのカードが実装されています。

推奨アクション フェールオーバー装置のカード コンフィギュレーションが同じであることを確認します。

105048

エラーメッセージ `%Threat Defense-1-105048: (unit ) Mate's service module (application ) is different from mine (application )`

説明 アクティブ装置とスタンバイ装置のサービスモジュールで異なるアプリケーションが動作していることをフェールオーバー プロセスが検出しました。異なるサービス モジュールが使用されている場合、2 つのフェールオーバー装置は互換性がありません。

- **unit**：プライマリまたはセカンダリ
- **application**：アプリケーションの名前（たとえば、InterScan Security Card）

推奨アクション フェールオーバーを再度イネーブルにする前に、両方の装置が同じサービス モジュールを装備していることを確認します。

105050

エラーメッセージ `%Threat Defense-3-105050: ASAv ethernet interface mismatch`

説明 スタンバイ装置のイーサネット インターフェイスの数がアクティブ装置のイーサネット インターフェイスの数より少ないです。

推奨アクション インターフェイスの数が同じ Secure Firewall Threat Defense デバイス を互いにペアにしてください。装置のインターフェイスの数が同じであることを確認します。場合によって、追加のインターフェイス モジュールを取り付けるか、または別のデバイスを使用する必要があります。物理インターフェイスが一致したら、HA を一時停止してから再開することで、設定の同期を強制します。

106001

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

説明内部アドレスへの接続の試行が、指定されたトラフィック タイプに定義されたセキュリティ ポリシーによって拒否されました。表示される IP アドレスは、NAT によって表示される IP アドレスではなく実際の IP アドレスです。表示される tcp_flags 値は、接続が拒否されたときに存在していた TCP ヘッダーのフラグに対応します。たとえば、Secure Firewall Threat Defense デバイスに接続状態が存在しない TCP パケットが到着し、それが廃棄された場合です。このパケットの tcp_flags は FIN および ACK です。

tcp_flags を次に示します。

- ACK：肯定応答番号が受信されました。
- FIN：データが送信されました。
- PSH：受信者がデータをアプリケーションに渡しました。
- RST：接続がリセットされました。
- SYN：シーケンス番号が接続を開始するために同期化されました。
- URG：緊急ポインタが有効であると宣言されました。

推奨アクション 不要。

106002

エラーメッセージ `%Threat Defense-2-106002: protocol Connection denied by outbound list acl_ID src inside_address dest outside_address`

説明指定された接続は、**outbound deny** コマンドが原因で失敗しました。**protocol** 変数は ICMP、TCP、または UDP になります。

推奨アクション show outbound コマンドを使用して、発信リストを確認します。

106006

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

説明着信 UDP パケットが、指定されたトラフィック タイプに定義されているセキュリティ ポリシーによって拒否されました。

推奨アクション 不要。

106007

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

説明 DNS クエリーまたは応答を含む UDP パケットが拒否されました。

推奨アクション 内部ポート番号が 53 の場合、内部ホストはキャッシング ネーム サーバーとして設定されていると考えられます。**access-list** コマンド文を追加して、UDP ポート 53 のトラフィックおよび内部ホストの変換エントリを許可します。外部ポート番号が 53 の場合、DNS サーバーの応答が遅かったため、クエリーには別のサーバーが応答したと考えられます。

106010

エラーメッセージ `%Threat Defense-3-106010: Deny inbound protocol src [interface_name : source_address/source_port ] [([idfw_user | FQDN_string ], sg_info )] dst [interface_name : dest_address /dest_port ][([idfw_user | FQDN_string ], sg_info )]`

説明 着信接続は、セキュリティ ポリシーによって拒否されました。

推奨アクション トラフィックを許可する必要がある場合は、セキュリティ ポリシーを修正します。このメッセージが繰り返し表示される場合は、リモート ピアの管理者にお問い合わせください。

106011

エラーメッセージ `%Threat Defense-3-106011: Deny inbound (No xlate) protocol src Interface:IP/port dst Interface-nameif:IP/port`

説明 このメッセージは、Web ブラウザ経由でインターネットにアクセスしている内部ユーザーがいる場合、通常のトラフィック条件で表示されます。接続がリセットされた場合は常に、Secure Firewall Threat Defense デバイス が接続リセットを受信した後にその接続の端にあるホストがパケットを送信すると、このメッセージが表示されます。これは通常、無視してかまいません。

推奨アクション **no logging message 106011** コマンドを入力して、このメッセージが syslog サーバーに記録されないようにします。

106012

エラーメッセージ `%Threat Defense-6-106012: Deny IP from IP_address to IP_address , IP options hex.`

説明 IP パケットが IP オプションとともに表示されました。IP オプションはセキュリティ リスクと見なされるので、パケットは廃棄されました。

推奨アクション リモート ホスト システムの管理者に問い合わせて、問題を判別します。ローカル サイトを確認して、あいまいなソース ルーティングや厳密なソース ルーティングがないかどうかを調べます。

106013

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

説明 Secure Firewall Threat Defense デバイス は、PAT グローバル アドレスに対応する宛先アドレスを持つ着信 ICMP エコー要求パケットを廃棄しました。着信パケットは、そのパケットを受信するべき PAT ホストを指定できないので廃棄されます。

推奨アクション 不要。

106014

エラーメッセージ `%Threat Defense-3-106014: Deny inbound icmp src interface_name : IP_address [([idfw_user | FQDN_string ], sg_info )] dst interface_name : IP_address [([idfw_user | FQDN_string ], sg_info )] (type dec , code dec )`

説明 Secure Firewall Threat Defense デバイス は、着信 ICMP パケット アクセスをすべて拒否しました。デフォルトで、ICMP パケットはすべて、特に許可されている場合を除き、アクセスを拒否されます。

推奨アクション 不要。

106015

エラーメッセージ `%Threat Defense-6-106015: Deny TCP (no connection) from IP_address /port to IP_address /port flags tcp_flags on interface interface_name.`

説明 Secure Firewall Threat Defense デバイス は、関連付けられている接続が Secure Firewall Threat Defense 接続テーブルにない TCP パケットを廃棄しました。Secure Firewall Threat Defense デバイス は、新しい接続の確立要求を示す SYN フラグをパケットで探します。SYN フラグがセットされておらず、既存の接続がない場合、Secure Firewall Threat Defense デバイス はそのパケットを廃棄します。

推奨アクション Secure Firewall Threat Defense デバイス がこれらの無効な TCP パケットを大量に受信する場合を除き、不要です。大量に受信する場合は、パケットを送信元までトレースして、これらのパケットが送信された原因を判別します。

106016

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

説明宛先 IP アドレスが 0.0.0.0 で、宛先 MAC アドレスが Secure Firewall Threat Defense インターフェイスのアドレスのパケットが Secure Firewall Threat Defense インターフェイスに到着しました。また、このメッセージは、Secure Firewall Threat Defense デバイス が無効な送信元アドレス（たとえば、次に示すアドレスなどの無効アドレス）を持つパケットを廃棄した場合にも生成されます。

- ループバック ネットワーク（127.0.0.0）
- ブロードキャスト（limited、net-directed、subnet-directed、および all-subnets-directed）
- 宛先ホスト（land.c）

スプーフィング パケット検出をさらに強化するには、**icmp** コマンドを使用して、内部ネットワークに属する送信元アドレスを持つパケットを廃棄するように Secure Firewall Threat Defense デバイス を設定します。現在、**access-list** コマンドは推奨されておらず、正しく動作することも保証されていません。

推奨アクション外部ユーザーが保護されているネットワークを危険にさらそうとしていないかどうかを判別します。設定に誤りのあるクライアントをチェックします。

106017

エラーメッセージ `%Threat Defense-2-106017: Deny IP due to Land Attack from IP_address to IP_address`

説明 IP 送信元アドレスと IP 宛先が同一で、かつ宛先ポートと送信元ポートが同一のパケットを Secure Firewall Threat Defense デバイス が受信しました。このメッセージは、システムの攻撃を目的としてスプーフィングされたパケットを示します。この攻撃は、Land 攻撃と呼ばれます。

推奨アクションこのメッセージが引き続き表示される場合は、攻撃が進行中である可能性があります。パケットは、攻撃の起点を決定するのに十分な情報を提供しません。

106018

エラーメッセージ `%Threat Defense-2-106018: ICMP packet type ICMP_type denied by outbound list acl_ID src inside_address dest outside_address`

説明ローカル ホスト（inside_address）から外部ホスト（outside_address）への発信 ICMP パケット（指定された ICMP のパケット）が発信 ACL リストによって拒否されました。

推奨アクション 不要。

106020

エラーメッセージ `%Threat Defense-2-106020: Deny IP teardrop fragment (size = number, offset = number) from IP_address to IP_address`

説明 Secure Firewall Threat Defense デバイス が、小さなオフセットまたはフラグメントの重複が含まれる teardrop シグニチャを持つ IP パケットを廃棄しました。これは、Secure Firewall Threat Defense デバイス または侵入検知システムを欺く敵対イベントです。

推奨アクション リモート ピアの管理者に連絡するか、またはセキュリティ ポリシーに従ってこの問題の危険度を高くします。

106021

エラーメッセージ `%Threat Defense-1-106021: Deny protocol reverse path check from source_address to dest_address on interface interface_name`

説明攻撃が進行中です。インバウンド接続上の IP アドレスのスプーフィングが試みられています。逆ルート ルックアップとも呼ばれる Unicast RPF は、ルートによって表される送信元アドレスを持たないパケットを検出し、そのパケットをSecure Firewall Threat Defense デバイスへの攻撃の一部であると想定します。

このメッセージは、ip verify reverse-path コマンドで Unicast RPF をイネーブルにしている場合に表示されます。この機能は、インターフェイスに入力されるパケットについて動作します。外側で設定されている場合、Secure Firewall Threat Defense デバイスは、外部から到達するパケットを確認します。

Secure Firewall Threat Defense デバイスは、source_address に基づいてルートを検索します。エントリが検出されず、ルートが定義されない場合は、このメッセージが表示され、接続は廃棄されます。

ルートがある場合、Secure Firewall Threat Defense デバイスは対応するインターフェイスを確認します。パケットが別のインターフェイスに到達している場合、スプーフィングであるか、または宛先への複数パスが存在する非対称ルーティング環境であるかのどちらかです。Secure Firewall Threat Defense デバイスは、非対称ルーティングをサポートしていません。

Secure Firewall Threat Defense デバイス は内部インターフェイスに設定されている場合、スタティック ルート コマンド文または RIP をチェックします。source_address が見つからない場合、内部ユーザーはアドレスをスプーフィングしています。

推奨アクション攻撃が進行中であっても、この機能がイネーブルになっていれば、ユーザーによる処置は不要です。Secure Firewall Threat Defense デバイス により、攻撃が阻止されます。

106022

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

説明接続と一致するパケットが、その接続が開始されたインターフェイスとは異なるインターフェイスに到着しました。また、ip verify reverse-path コマンドが設定されていません。

たとえば、ユーザーが内部インターフェイスで接続を開始したが、Secure Firewall Threat Defense デバイスが境界インターフェイスに到着する同じ接続を検出する場合、Secure Firewall Threat Defense デバイスは宛先へのパスを複数持っていることになります。これは非対称ルーティングと呼ばれ、Secure Firewall Threat Defense デバイスではサポートされていません。

攻撃者は、Secure Firewall Threat Defense デバイスに侵入する方法として、1 つの接続から別の接続にパケットを付加しようと試みることもあります。どちらの場合も、Secure Firewall Threat Defense デバイス はこのメッセージを表示して、接続を廃棄します。

推奨アクション ルーティングが非対称でないことを確認します。

106023

エラーメッセージ`%Threat Defense-4-106023: Deny protocol src [`*interface_name* `:`*source_address* `/`*source_port* `] [([`*idfw_user* `|`*FQDN_string* `], `*sg_info* `)] dst `*interface_name*

:*dest_address /dest_port* [([*idfw_user* |*FQDN_string*], *sg_info*)] [type {*string* }, code {*code* }] by *access_group acl_ID* [0x8ed66b60, 0xf8852875]

説明 ACL により実 IP パケットが拒否されました。このメッセージは、ACL に対して **log** オプションをイネーブルにしていない場合でも表示されます。IP アドレスは、NAT によって表示される値ではなく実際の IP アドレスです。一致するものが見つかった場合、IP アドレスに対応するユーザー ID 情報と FQDN 情報の両方が出力されます。Secure Firewall Threat Defense デバイス は、識別情報（ドメイン\ユーザー）または FQDN（ユーザー名が使用できない場合）のいずれかをログに記録します。識別情報または FQDN が使用可能な場合、Secure Firewall Threat Defense デバイス は、この情報を送信元と宛先の両方のログに記録します。

推奨アクション同じ送信元アドレスからのメッセージが引き続き表示される場合は、フットプリンティングまたはポート スキャンが行われている可能性があります。リモート ホストの管理者にお問い合わせください。

106024

エラーメッセージ `%Threat Defense-2-106024: Access rules memory exhausted`

説明アクセス リストのコンパイル プロセスで、メモリが不足しています。最後の正常なアクセス リスト以降に追加されたコンフィギュレーション情報はすべて、Secure Firewall Threat Defense デバイス から削除されました。最新のコンパイル済みアクセス リストのセットが引き続き使用されます。

推奨アクション Access Lists、AAA、ICMP、SSH、Telnet、および他の規則タイプは、アクセス リストの規則タイプとして格納され、コンパイルされます。これらの規則タイプの一部を削除して、他の規則タイプを追加できるようにします。

106025、106026

エラーメッセージ `%Threat Defense-6-106025: Failed to determine the security context for the packet:sourceVlan:source_address dest_address source_port dest_port protocol`

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

説明マルチコンテキスト モードのパケットのセキュリティ コンテキストを判定できません。どちらのメッセージも、ルータまたはトランスペアレント モードで廃棄される IP パケットに対して生成されることがあります。

推奨アクション 不要。

106027

エラーメッセージ `%Threat Defense-4-106027:acl_ID: Deny src [source address] dst [destination address] by access-group "access-list name"`

説明 ACL により非 IP パケットが拒否されました。このメッセージは、たとえ拡張 ACL に対して log オプションがイネーブルになっていない場合でも表示されます。

推奨アクション同じ送信元アドレスからのメッセージが引き続き表示される場合は、フットプリンティングまたはポート スキャンが行われようとしていることを示している可能性があります。リモート ホストの管理者にお問い合わせください。

106100

エラーメッセージ`%Threat Defense-6-106100: access-list acl_ID {permitted | denied | est-allowed} protocol interface_name /source_address (source_port ) (idfw_user , sg_info ) interface_name /dest_address (dest_port ) (idfw_user , sg_info ) hit-cnt number ({first hit | number -second interval}) hash codes`

説明最初の出現か、またはある期間の合計出現数を示します。このメッセージは、拒否されたパケットだけを記録して、ヒット数も設定可能なレベルも含まないメッセージ 106023 よりも多くの情報を提供します。

アクセス リストの行に *log* 引数が含まれている場合、非同期パケットが Secure Firewall Threat Defense デバイスに到達し、アクセス リストによって評価されることによって、このメッセージ ID がトリガーされる可能性があると想定されます。たとえば、Secure Firewall Threat Defense デバイス で（接続テーブルに TCP 接続が存在しない）ACK パケットを受信した場合、Secure Firewall Threat Defense デバイス によってメッセージ 106100 が生成される可能性があります。このメッセージは、パケットは許可されたが、一致する接続が存在しないために後で正しく廃棄されることを示します。

メッセージの値は次のとおりです。

- permitted | denied | est-allowed：これらの値は、パケットが ACL によって許可されたか拒否されたかを指摘します。値が est-allowed の場合、パケットは ACL によって拒否されましたが、すでに確立されているセッションで許可されました（たとえば、内部ユーザーがインターネットへのアクセスを許可され、通常は ACL によって拒否される応答パケットが許可されます）。
- *protocol*：TCP、UDP、ICMP、または IP プロトコル番号。
- *interface_name*：ログ フローの送信元または宛先のインターフェイス名。VLAN インターフェイスがサポートされています。
- *source_address*：ログ フローの送信元 IP アドレス。IP アドレスは、NAT によって表示される値ではなく実際の IP アドレスです。
- *dest_address*：ログ フローの宛先 IP アドレス。IP アドレスは、NAT によって表示される値ではなく実際の IP アドレスです。
- *source_port*：ログ フローの送信元ポート（TCP または UDP）。ICMP の場合、送信元ポートの後の数字は、メッセージ タイプです。
- *idfw_user*：Secure Firewall Threat Defense デバイス が当該 IP アドレスのユーザー名を見つけた場合に既存の syslog に追加される、ドメイン名を含むユーザー識別用ユーザー名。
- *sg_info*：Secure Firewall Threat Defense デバイス によって当該 IP アドレスのセキュリティ グループ タグが検出された場合に syslog に追加されるセキュリティ グループ タグ。セキュリティ グループ名は、セキュリティ グループ タグがあればそれとともに表示されます。
- *dest_port*：ログ フローの宛先ポート（TCP または UDP）。ICMP の場合、宛先ポートの後の数字は ICMP メッセージ コードです。これは一部のメッセージ タイプに使用可能です。

タイプ 8 の場合、これは常に 0 です。ICMP メッセージ タイプのリストについては、次の URL を参照してください。http://www.iana.org/assignments/icmp-parameters/icmp-parameters.xml

- hit-cnt *number*：設定した期間に、このフローが ACL エントリによって許可または拒否された回数。Secure Firewall Threat Defense デバイス がこのフローに対して最初のメッセージを生成するときの値は 1 です。
- first hit：このフローに対して生成された最初のメッセージ。
- *number*-second interval：ヒット数を累算する対象期間。この期間は、**access-list** コマンドで **interval** オプションを使用して設定します。
- hash codes：オブジェクト グループ ACE および構成要素の通常の ACE には、必ず 2 が表示されます。値は、パケットがヒットする ACE 上で決定されます。これらのハッシュ コードを表示するには **show-access list** コマンドを入力します。

推奨アクション 不要。

106101

エラーメッセージ `%Threat Defense-1-106101 Number of cached deny-flows for ACL log has reached limit (number ).`

説明 ACL **deny** 文（**access-list** *id* **deny** コマンド）に **log** オプションを設定してあり、トラフィック フローが ACL 文と一致する場合、Secure Firewall Threat Defense デバイス はフロー情報をキャッシュします。このメッセージは、Secure Firewall Threat Defense デバイスでキャッシュされる一致フローの数がユーザーが設定した制限（**access-list deny-flow-max** コマンドを使用）を超えたことを示します。このメッセージは、サービス拒絶（DoS）攻撃の結果生成される可能性があります。

- *number*：**access-list deny-flow-max** コマンドを使用して設定された制限

推奨アクション 不要。

106102

エラーメッセージ `%Threat Defense-6-106102: access-list acl_ID {permitted|denied} protocol for user username interface_name /source_address source_port interface_name /dest_address dest_port hit-cnt number {first hit|number -second interval} hash codes`

説明 VPN フィルタを通じて適用されるアクセス リストによってパケットが許可または拒否されました。このメッセージは、メッセージ 106100 に相当する VPN/AAA フィルタのメッセージです。

推奨アクション 不要。

106103

エラーメッセージ `%Threat Defense-4-106103: access-list acl_ID denied protocol for user username interface_name /source_address source_port interface_name /dest_address dest_port hit-cnt number first hit hash codes`

説明 VPN フィルタを通じて適用されるアクセス リストによってパケットが拒否されました。このメッセージは、メッセージ 106023 に相当する VPN/AAA フィルタのメッセージです。

推奨アクション 不要。

107001

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

説明 Secure Firewall Threat Defense デバイス は不正な認証を持つ RIP 応答メッセージを受信しました。このメッセージは、ルータまたはSecure Firewall Threat Defense デバイスの設定の誤り、またはSecure Firewall Threat Defense デバイスのルーティング テーブルへの攻撃の失敗が原因となることもあります。

推奨アクション このメッセージは攻撃の可能性を示しているため、モニターする必要があります。このメッセージに示されている送信元 IP アドレスを熟知していない場合は、信頼できるエンティティ間でRIP認証キーを交換します。攻撃者が既存のキーを判別しようと試みている可能性もあります。

109011

エラーメッセージ `%Threat Defense-2-109011: Authen Session Start: user 'user ', sid number`

説明認証セッションがホストと Secure Firewall Threat Defense デバイス の間で開始されましたが、まだ完了していません。

推奨アクション 不要。

109012

エラーメッセージ `%Threat Defense-5-109012: Authen Session End: user 'user', sid number, elapsed number seconds`

説明認証キャッシュがタイムアウトになっています。ユーザーは、次の接続で再認証が必要になります。timeout uauth コマンドを使用して、このタイマーのタイムアウト時間を変更できます。

推奨アクション 不要。

109013

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

説明ユーザーは、サービスを使用する前に認証を受ける必要があります。

推奨アクション サービスを使用する前に FTP、Telnet、または HTTP を使用して認証します。

109016

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

説明このユーザーの AAA サーバーで指定された ACL が、Secure Firewall Threat Defense デバイスに存在しません。このエラーは、Secure Firewall Threat Defense デバイスを設定する前に AAA サーバーを設定した場合に発生することがあります。AAA サーバーでベンダー固有の属性（VSA）が次の値のいずれかになっている可能性があります。

- acl=acl_ID
- shell:acl=acl_ID
- ACS:CiscoSecured-Defined-ACL=acl_ID

推奨アクション Secure Firewall Threat Defense デバイス に ACL を追加し、AAA サーバーで指定したものと同じ名前を必ず使用します。

109018

エラーメッセージ `%Threat Defense-3-109018: Downloaded ACL acl_ID is empty`

説明ダウンロードされた認可に ACE がありません。この状況は、属性文字列 *ip:inacl#* のつづりの誤り、または access-list コマンドの省略が原因となっている可能性があります。

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

推奨アクション 指摘されたエラーのある ACL コンポーネントを AAA サーバー上で修正します。

109019

エラーメッセージ `%Threat Defense-3-109019: Downloaded ACL acl_ID has parsing error; ACE string`

説明ダウンロードした認可の属性文字列 ip:inacl#NNN= のシーケンス番号 NNN を解析中にエラーが発生しました。= の欠落、数字以外の文字やスペース以外の文字が # と = の間にある、NNN が 999999999 より大きい、などの原因が考えられます。

```
ip:inacl# 1 permit tcp any any
ip:inacl# 1junk2=permit tcp any any
ip:inacl# 1000000000=permit tcp any any
```

推奨アクション 指摘されたエラーのある ACL コンポーネントを AAA サーバー上で修正します。

109020

エラーメッセージ `%Threat Defense-3-109020: Downloaded ACL has config error; ACE`

説明ダウンロードされた認可のコンポーネントの 1 つにコンフィギュレーション エラーがあります。要素のテキスト全体がメッセージに含まれています。このメッセージは通常、無効な access-list コマンド文が原因となっています。

推奨アクション 指摘されたエラーのある ACL コンポーネントを AAA サーバー上で修正します。

109026

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

説明 AAA サーバーからの応答を検証できません。設定されたサーバー キーが誤っている可能性があります。このメッセージは、RADIUS サーバーまたは TACACS+ サーバーとのトランザクション中に生成されることがあります。

aaa-server コマンドを使用して設定されたサーバー キーが正しいことを確認します。

109027

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

説明 AAA サーバーからの応答を検証できません。設定されたサーバー キーが誤っている可能性があります。このメッセージは、RADIUS サーバーまたは TACACS+ サーバーとのトランザクション中に表示されることがあります。server_IP_address は、関連する AAA サーバーの IP アドレスです。user は、接続に関連付けられているユーザー名です。

推奨アクション aaa-server コマンドを使用して設定されたサーバー キーが正しいことを確認します。

109029

エラーメッセージ `%Threat Defense-5-109029: Parsing downloaded ACL: string`

説明ユーザー認証中に RADIUS サーバーからダウンロードされたアクセス リストを解析している間に構文エラーが発生しました。

- *string*：アクセス リストの正しい解析を妨げた構文エラーを詳述するエラー メッセージ

推奨アクションこのメッセージに提示されている情報を使用して、RADIUS サーバー コンフィギュレーション内のアクセス リスト定義にある構文エラーを特定し、訂正します。

109030

エラーメッセージ `%Threat Defense-4-109030: Autodetect ACL convert wildcard did not convert ACL access_list source |dest netmask netmask .`

説明 RADIUS サーバーで設定されたダイナミック ACL が、ワイルドカード ネットマスクを自動的に検出するメカニズムによって変換されませんでした。問題は、ネットマスクがワイルド

カードであるか、通常のネットマスクであるかをこのメカニズムが判別できないために発生します。

- **access_list**：変換できないアクセス リスト
- **source**：送信元 IP アドレス
- **dest**：宛先 IP アドレス
- **netmask**：宛先アドレスまたは送信元アドレスに対する 10 進数表記のサブネット マスク

推奨アクション RADIUS サーバーのアクセス リスト ネットマスクを確認して、ワイルドカードコンフィギュレーションがないかどうかを調べます。ネットマスクをワイルドカードにする予定の場合、およびそのサーバーのアクセス リスト ネットマスクすべてがワイルドカードである場合、AAA サーバーの **acl-netmask-convert** に wildcard 設定を使用します。それ以外の場合は、ネットマスクを通常のネットマスクまたはホールを含まないワイルドカードネットマスクに変更します（つまり、ネットマスクは連続する 2 進数の 1 を提示します。たとえば、00000000.00000000.00011111.11111111 または 16 進数の 0.0.31.255 のようになります）。マスクを通常にする予定の場合、およびそのサーバーのすべてのアクセス リスト ネットマスクが通常である場合、AAA サーバーの **acl-netmask-convert** に normal 設定を使用します。

109032

エラーメッセージ `%Threat Defense-3-109032: Unable to install ACL access_list , downloaded for user username ; Error in ACE: ace .`

説明 Secure Firewall Threat Defense デバイス は、ユーザー接続に適用するアクセス コントロール リストを RADIUS サーバーから受信しましたが、リストのエントリに構文エラーが含まれています。エラーが含まれるリストを使用すると、セキュリティ ポリシー違反になる可能性があるため、Secure Firewall Threat Defense デバイス はユーザーを認証できませんでした。

- *access_list*：**show access-list** コマンドの出力に表示されるダイナミック アクセス リストに割り当てられている名前
- *username*：その接続がこのアクセス リストの制御を受けるユーザーの名前
- *ace*：エラーが検出されたときに処理されていたアクセス リストのエントリ

推奨アクション RADIUS サーバーのコンフィギュレーションのアクセス リスト定義を訂正します。

109033

エラーメッセージ `%Threat Defense-4-109033: Authentication failed for admin user user from src_IP . Interactive challenge processing is not supported for protocol connections`

説明管理接続の認証中に AAA チャレンジ処理がトリガーされましたが、Secure Firewall Threat Defense デバイス はそのクライアント アプリケーションでの対話型チャレンジ処理を開始できません。このような場合は、認証試行が拒否され、接続が拒否されます。

- *user*：認証対象のユーザーの名前
- *src_IP*：クライアント ホストの IP アドレス。
- *protocol*：クライアント接続プロトコル（SSH v1 または管理 HTTP）

推奨アクションこれらの接続タイプに対してチャレンジ処理が発生しないように AAA を再設定します。これは、通常、RSA SecurID サーバー、またはRADIUS経由のトークンベースAAAサーバーに対して、これらの接続タイプの認証を避けることを意味します。

109034

エラーメッセージ `%Threat Defense-4-109034: Authentication failed for network user user from src_IP/port to dst_IP/port . Interactive challenge processing is not supported for protocol connections`

説明ネットワーク接続の認証中にAAAチャレンジ処理がトリガーされましたが、Secure Firewall Threat Defense デバイス はそのクライアント アプリケーションでの対話型チャレンジ処理を開始できません。このような場合は、認証試行が拒否され、接続が拒否されます。

- *user*：認証対象のユーザーの名前
- *src_IP/port*：クライアント ホストの IP アドレスおよびポート。
- *dst_IP/port*：クライアントが接続しようとしているサーバーの IP アドレスおよびポート。
- *protocol*：クライアント接続プロトコル（たとえば、FTP）

推奨アクションこれらの接続タイプに対してチャレンジ処理が発生しないように AAA を再設定します。これは、通常、RSA SecurID サーバー、またはRADIUS経由のトークンベースAAAサーバーに対して、これらの接続タイプの認証を避けることを意味します。

109035

エラーメッセージ `%Threat Defense-3-109035: Exceeded maximum number (<max_num>) of DAP attribute instances for user <user>`

説明このログは、RADIUS サーバーから受信した DAP 属性の数が、指定されたユーザーの接続の認証中に許可されている最大数を超えた場合に生成されます。

推奨アクション DAP 属性のコンフィギュレーションを変更してログで指定されている許可最大数以下に DAP 属性の数を削減し、指定したユーザーが接続できるようにします。

109036

エラーメッセージ `%Threat Defense-6-109036: Exceeded 1000 attribute values for the attribute name attribute for user username .`

説明 LDAP 応答メッセージに、1000 を超える値を持つ属性が含まれています。

- *attribute_name*：LDAP 属性名
- *username*：ログイン時のユーザー名

推奨アクション 不要。

109037

エラーメッセージ `%Threat Defense-3-109037: Exceeded 5000 attribute values for the attribute name attribute for user username .`

説明 Secure Firewall Threat Defense デバイス では、AAA サーバーから同じ属性の複数の値を受信することがサポートされています。AAA サーバーから同じ属性に関して 5000 を超える値を含む応答が送信されてきた場合、Secure Firewall Threat Defense デバイス ではこの応答メッセージを形式誤りとして処理し、認証を拒否します。このような状況は、特殊なテストツールを使用するラボ環境でだけ確認されています。実際の実稼働ネットワークで発生する可能性はまずありません。

- *attribute_name*：LDAP 属性名
- *username*：ログイン時のユーザー名

推奨アクション プロトコル スニファ（WireShark など）を使用して Secure Firewall Threat Defense デバイス と AAA サーバー間の認証トラフィックを取り込み、トレース ファイルを Cisco TAC に転送して分析を依頼してください。

109038

エラーメッセージ `%Threat Defense-3-109038: Attribute internal-attribute-name value string-from-server from AAA server could not be parsed as a type internal-attribute-name string representation of the attribute name`

説明 AAA サブシステムが AAA サーバーからの属性を内部表現へと解析しようとして失敗しました。

- *string-from-server*：AAA サーバーから受信した文字列。40 文字に切り捨てられます。
- *type*：指定された属性のタイプ

推奨アクション 属性が AAA サーバー上に正しく生成されていることを確認します。詳細については、**debug ldap** コマンドおよび **debug radius** コマンドを使用します。

109039

エラーメッセージ `%Threat Defense-5-109039: AAA Authentication:Dropping an unsupported IPv6/IP46/IP64 packet from lifc :laddr to fifc :faddr`

説明 NAT によって IPv6 アドレスに変換される IPv6 アドレスまたは IPv4 アドレスを含むパケットには、AAA の認証または承認が必要です。AAA の認証および承認は IPv6 アドレスをサポートしません。パケットはドロップされます。

- *lifc*：入力インターフェイス
- *laddr*：送信元 IP アドレス
- *fifc*：出力インターフェイス
- *faddr*：NAT 変換後の宛先 IP アドレス（存在する場合）

推奨アクション 不要。

109100

エラーメッセージ `%Threat Defense-6-109100: Received CoA update from coa-source-ip for user username , with session ID: audit-session-id , changing authorization attributes`

説明 Secure Firewall Threat Defense デバイス は、セッション ID *audit-session-id* を持つユーザー *username* の *coa-source-ip* からの CoA ポリシー更新要求を正常に処理しました。この Syslog メッセージは、認可変更ポリシーの更新を Secure Firewall Threat Defense デバイス が受け取り、検証および適用した後に生成されます。エラーがない場合、認可変更を受け取って処理するときに生成されるのはこの Syslog メッセージのみです。

- *coa-source-ip*：許可要求の変更の発信 IP アドレス
- *username*：変更するセッションのユーザー
- *audit-session-id*：変更されるセッションのグローバル ID

推奨アクション 不要。

109101

エラーメッセージ `%Threat Defense-6-109101: Received CoA disconnect request from coa-source-ip for user username , with audit-session-id: audit-session-id`

説明 Secure Firewall Threat Defense デバイス は、アクティブな VPN セッションに対して正しくフォーマットされた Disconnect-Request を受信し、接続を正常に終了しました。

- *coa-source-ip*：許可要求の変更の発信 IP アドレス
- *username*：変更するセッションのユーザー
- *audit-session-id*：変更されるセッションのグローバル ID

推奨アクション 不要。

109102

エラーメッセージ `%Threat Defense-4-109102: Received CoA action-type from coa-source-ip , but cannot find named session audit-session-id`

説明 Secure Firewall Threat Defense デバイス は有効な認可変更要求を受信しましたが、要求で指定されたセッション ID が Secure Firewall Threat Defense デバイス 上のアクティブなセッションと一致しません。これは、ユーザーがすでに閉じたセッション上の認可変更をサーバーが発行しようとした結果である可能性があります。

- *action-type*：要求された認可変更アクション（update または disconnect）
- *coa-source-ip*：許可要求の変更の発信 IP アドレス
- *audit-session-id*：変更されるセッションのグローバル ID

推奨アクション 不要。

109103

エラーメッセージ `%Threat Defense-3-109103: CoA action-type from coa-source-ip failed for user username , with session ID: audit-session-id .`

説明 Secure Firewall Threat Defense デバイス は正しくフォーマットされた認可変更要求を受信しましたが、正常に処理できませんでした。

- *action-type*：要求された認可変更アクション（update または disconnect）
- *coa-source-ip*：許可要求の変更の発信 IP アドレス
- *username*：変更するセッションのユーザー
- *audit-session-id*：変更されるセッションのグローバル ID

推奨アクション 関連するVPNサブシステムのログを調査し、更新された属性を提供できなかった理由、またはセッションを終了できなかった理由を判断します。

109104

エラーメッセージ `%Threat Defense-3-109104: CoA action-type from coa-source-ip failed for user username , session ID: audit-session-id . Action not supported.`

説明 Secure Firewall Threat Defense デバイス は認可変更を正しい形式で受け取りましたが、指定されたアクションが Secure Firewall Threat Defense デバイス でサポートされていないために処理しませんでした。

- *action-type*：要求された認可変更アクション（update または disconnect）
- *coa-source-ip*：許可要求の変更の発信 IP アドレス
- *username*：変更するセッションのユーザー
- *audit-session-id*：変更されるセッションのグローバル ID

推奨アクション 不要。

109105

エラーメッセージ `%FTD-3-109105: Failed to determine the egress interface for locally generated traffic destined to <protocol> <IP>:<port>.`

説明インターフェイスがBVIであれば、ルートが存在しない場合、Secure Firewall Threat Defense デバイス は syslog をログに記録する必要があります。デフォルト ルートが存在し、正しいインターフェイスにパケットをルーティングしない場合は追跡できなくなります。 Secure Firewall Threat Defense の場合は、データインターフェイスの次にまず管理ルートが検索されます。このためデフォルトルートが異なる宛先にパケットをルーティングする場合は、追跡が難しくなります。

推奨アクション 正しい宛先のデフォルト ルートを追加するか、スタティック ルートを追加することを強くお勧めします。

109201

エラーメッセージ `%FTD-5-109201: UAUTH Session session, User username, Assigned IP IP Address, Succeeded adding entry.`

説明 VPN ユーザーが正常に追加されると、このメッセージが生成されます。

推奨アクションなし。

109202

エラーメッセージ `%Threat Defense-6-109202: UAUTH Session session, User username, Assigned IP IP Address, Succeeded incrementing entry use.`

説明 VPN ユーザーアカウントはすでに存在し、参照カウントは正常に増分されました。

推奨アクションなし。

109203

エラーメッセージ `%Threat Defense-3-109203: UAUTH Session session, User username, Assigned IP IP Address, Failed adding entry.`

説明 このメッセージは、デバイスが新しく作成されたユーザーエントリに ACL ルールを適用できなかった場合に生成されます。

推奨アクション 再接続を試みます。

109204

エラーメッセージ `%Threat Defense-5-109204: UAUTH Session session, User username, Assigned IP IP Address, Succeeded applying filter.`

説明 このメッセージは、デバイスが新しく作成されたユーザーエントリに ACL ルールを適用できなかった場合に生成されます。

推奨アクションなし。

109205

エラーメッセージ `%Threat Defense-3-109205: UAUTH Session session, User username, Assigned IP IP Address, Failed applying filter.`

説明 このメッセージは、ユーザーエントリがすでに存在し、インターフェイス上のセッションに新しいルールを適用できなかった場合に生成されます。

推奨アクション 再接続を試みます。

109206

エラーメッセージ %Threat Defense-3-109206: UAUTH Session *session*, User *username*, Assigned IP *IP Address*, Removing stale entry added *hours* ago.

説明 このメッセージは、デバイスがコリジョンのためにユーザーエントリの追加に失敗し、古いエントリを削除した場合に生成されます。

推奨アクション 再接続を試みます。

109207

エラーメッセージ %Threat Defense-5-109207: UAUTH Session *session*, User *username*, Assigned IP *IP Address*, Succeeded updating entry.

説明 このメッセージは、デバイスがインターフェイス上のユーザーのルールを正常に適用したときに生成されます。

推奨アクションなし。

109208

エラーメッセージ %Threat Defense-3-109208: UAUTH Session *session*, User *username*, Assigned IP *IP Address*, Failed updating entry - no entry.

説明 このメッセージは、デバイスがユーザーエントリを新しいルールで更新できなかった場合に生成されます。

推奨アクション 再接続を試みます。

109209

エラーメッセージ %Threat Defense-3-109209: UAUTH Session *session*, User *username*, Assigned IP *IP Address*, Failed updating filter for entry.

説明 このメッセージは、デバイスがコリジョンのためにユーザーエントリのルールを更新できなかった場合に生成されます。

推奨アクション 再接続を試みます。

109210

エラーメッセージ %Threat Defense-5-109210: UAUTH Session *session*, User *username*, Assigned IP *IP Address*, Successfully removed the rules for user during tunnel torn down.

説明 このメッセージは、トンネルの切断中にデバイスがユーザーのルールを正常に削除した場合に生成されます。

推奨アクションなし。

109211

エラーメッセージ `%Threat Defense-6-109211: UAUTH Session session, User username, Assigned IP IP Address, Successfully removed the rules for user during tunnel torn down.`

説明 このメッセージは、トンネルの削除後に参照カウントが正常に減少した場合に生成されます。

推奨アクションなし。

109212

エラーメッセージ `%Threat Defense-3-109212: UAUTH Session session, User username, Assigned IP IP Address, Failed removing entry.`

説明 このメッセージは、無効なアドレスまたは不正なエントリが原因でデバイスの削除に失敗した場合に生成されます。

推奨アクション 再度接続の切断を試みます。

109213

エラーメッセージ `%Threat Defense-3-109213: UAUTH Session session, User username, Assigned IP IP Address, Failed removing entry.`

説明 このメッセージは、ユーザーエントリのコリジョンが原因でデバイスの削除に失敗した場合に生成されます。

推奨アクション 再度接続の切断を試みます。

メッセージ 110002 ～ 113045

この項では、110002 ～ 113045 のメッセージについて説明します。

110002

エラーメッセージ `%Threat Defense-6-110002: Failed to locate egress interface for protocol from src interface :src IP/src port to dest IP/dest port`

説明パケットの送信に使用するインターフェイスを Secure Firewall Threat Defense デバイス が検出しようとしたときに、エラーが発生しました。

- *protocol*：パケットのプロトコル
- *src interface*：パケットの送信元インターフェイス
- *src IP*：パケットの送信元 IP アドレス
- *src port*：送信元ポート番号
- *dest IP*：パケットの宛先 IP アドレス
- *dest port*：宛先ポート番号

推奨アクション エラー メッセージ、設定、およびエラーの原因となったイベントの詳細をコピーし、Cisco TAC にお問い合わせください。

110003

エラーメッセージ `%Threat Defense-6-110003: Routing failed to locate next-hop for protocol from src interface :src IP/src port to dest interface :dest IP/dest port`

説明インターフェイス ルーティング テーブル上のネクスト ホップを Secure Firewall Threat Defense デバイス が検出しようとしたときに、エラーが発生しました。

- *protocol*：パケットのプロトコル
- *src interface*：パケットの送信元インターフェイス
- *src IP*：パケットの送信元 IP アドレス
- *src port*：送信元ポート番号
- *dest IP*：パケットの宛先 IP アドレス
- *dest port*：宛先ポート番号

推奨アクション エラー メッセージ、設定、およびエラーの原因となったイベントの詳細をコピーし、Cisco TAC にお問い合わせください。デバッグ時にルーティング テーブルの詳細を表示するには、**show asp table routing** コマンドを使用します。

110004

エラーメッセージ `%Threat Defense-6-110004: Egress interface changed from old_active_ifc to new_active_ifc on ip_protocol connection conn_id for outside_zone /parent_outside_ifc :outside_addr /outside_port (mapped_addr /mapped_port) to inside_zone /parent_inside_ifc :inside_addr /inside_port (mapped_addr /mapped_port)`

説明出力インターフェイスでフローが変更されました。

推奨アクション 不要。

111001

エラーメッセージ `%Threat Defense-5-111001: Begin configuration: IP_address writing to device`

説明コンフィギュレーションをデバイス（フロッピーディスク、フラッシュ メモリ、TFTP、フェールオーバー スタンバイ装置、またはコンソール端末のいずれか）に格納する **write** コマンドを入力しました。**IP_address** は、ログインがコンソール ポートで行われたか、または Telnet 接続で行われたかを示します。

推奨アクション 不要。

111002

エラーメッセージ `%Threat Defense-5-111002: Begin configuration: IP_address reading from device`

説明コンフィギュレーションをデバイス（フロッピーディスク、フラッシュ メモリ、TFTP、フェールオーバー スタンバイ装置、またはコンソール端末のいずれか）から読み取る **read** コマンドを入力しました。**IP_address** は、ログインがコンソール ポートで行われたか、または Telnet 接続で行われたかを示します。

推奨アクション 不要。

111003

エラーメッセージ `%Threat Defense-5-111003: IP_address Erase configuration`

説明コンソールで **write erase** コマンドを入力してフラッシュ メモリの内容を消去しました。**IP_address** の値は、ログインがコンソール ポートで行われたか、または Telnet 接続で行われたかを示します。

推奨アクションコンフィギュレーションを消去した後、Secure Firewall Threat Defense デバイスを再設定して新しいコンフィギュレーションを保存します。または、フロッピーディスクまたはネットワークの他の場所にある TFTP サーバーに以前保存してあるコンフィギュレーションから情報を復元できます。

111004

エラーメッセージ `%Threat Defense-5-111004: IP_address end configuration: {FAILED|OK}`

説明 config floppy/memory/ network コマンドまたは **write floppy/memory/network/standby** コマンドを入力しました。**IP_address** の値は、ログインがコンソール ポートで行われたか、または Telnet 接続で行われたかを示します。

推奨アクションメッセージが OK で終われば不要です。このメッセージでエラーが表示された場合は、問題を解決します。たとえば、フロッピーディスクに書き込む場合は、フロッピーディスクが書き込み禁止になっていないことを確認します。TFTP サーバーに書き込む場合は、サーバーが動作していることを確認します。

111005

エラーメッセージ `%Threat Defense-5-111005: IP_address end configuration: OK`

説明コンフィギュレーション モードを終了しました。**IP_address** の値は、ログインがコンソール ポートで行われたか、または Telnet 接続で行われたかを示します。

推奨アクション 不要。

111007

エラーメッセージ `%Threat Defense-5-111007: Begin configuration: IP_address reading from device.`

説明 **reload** コマンドまたは **configure** コマンドを入力してコンフィギュレーションを読み込みました。deviceテキストは、フロッピーディスク、メモリ、ネット、スタンバイ、または端末になります。**IP_address** の値は、ログインがコンソール ポートで行われたか、または Telnet 接続で行われたかを示します。

推奨アクション 不要。

111008

エラーメッセージ `%Threat Defense-5-111008: User user executed the command string`

説明ユーザーが **show** コマンド以外の任意のコマンドを入力しました。

推奨アクション 不要。

111009

エラーメッセージ `%Threat Defense-7-111009:User user executed cmd:string`

説明ユーザーにより、コンフィギュレーションが変更されないコマンドが入力されました。このメッセージは、**show** コマンドに限り表示されます。

推奨アクション 不要。

111010

エラーメッセージ `%Threat Defense-5-111010: User username , running application-name from IP ip addr , executed cmd`

説明ユーザーが設定変更を行いました。

- *username*：設定変更を行ったユーザー
- *application-name*：ユーザーが実行しているアプリケーション
- *ip addr*：管理ステーションの IP アドレス
- *cmd*：ユーザーが実行したコマンド

推奨アクション 不要。

111111

エラーメッセージ `% Threat Defense-1-111111 error_message`

説明システム エラーまたはインフラストラクチャ エラーが発生しました。

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

112001

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

説明モジュール コンフィギュレーションを消去する要求が完了しました。ソース ファイルおよび行番号が特定されます。

推奨アクション 不要。

113001

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

説明 AAA リソースが使用できないために、IPSec トンネルまたは WebVPN 接続で AAA 動作を実行できません。**limit** 値は、同時 AAA トランザクションの最大数を示します。

推奨アクション 可能であれば、AAA リソースの要求を減らします。

113003

エラーメッセージ `%Threat Defense-6-113003: AAA group policy for user user is being set to policy_name .`

説明トンネル グループに関連付けられているグループ ポリシーが、ユーザー固有のポリシー *policy_name* で上書きされます。*policy_name* は、LOCAL 認証の設定時に **username** コマンドを使用して指定されており、RADIUS 認証の設定時に RADIUS CLASS 属性で返されます。

推奨アクション 不要。

113004

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

説明 IPSec または WebVPN 接続に対する AAA 操作が正常に完了しました。AAA タイプは、認証、許可、またはアカウンティングです。**server_IP_address** は、関連する AAA サーバーの IP アドレスです。**user** は、接続に関連付けられているユーザー名です。

推奨アクション 不要。

113005

エラーメッセージ `%Threat Defense-6-113005: AAA user authentication Rejected: reason = AAA failure: server = ip_addr : user = *****: user IP = ip_addr`

説明接続で AAA 認証に失敗しました。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。

推奨アクション 認証を再試行してください。

113005

エラーメッセージ `%Threat Defense-6-113005: AAA user authentication Rejected: reason = AAA failure: server = ip_addr : user = *****: user IP = ip_addr`

説明接続で AAA 認証に失敗しました。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。

推奨アクション 認証を再試行してください。

113006

エラーメッセージ `%Threat Defense-6-113006: User user locked out on exceeding number successive failed authentication attempts`

説明ローカルに設定されているユーザーがロックアウトされています。このメッセージは、このユーザーについて認証失敗が連続して設定回数だけ発生したときに現れ、今後このユーザーが認証を受けようとしても、管理者が **clear aaa local user lockout** コマンドを使用してユーザーをアンロックするまでは、すべて拒否されることを示します。**user** は現在ロックされているユーザーであり、**number** は **aaa local authentication attempts max-fail** コマンドを使用して設定されている連続失敗しきい値です。

推奨アクション clear_aaa_local_user_lockout コマンドを使用してユーザーをアンロックするか、許容される連続認証失敗の最大数を調整します。

113007

エラーメッセージ `%Threat Defense-6-113007: User user unlocked by administrator`

説明ローカルに設定されたユーザーが、**aaa local authentication attempts max-fail** コマンドを使用して設定された連続認証失敗の最大数を超えたためロックアウトされた後、表示されている管理者によってアンロックされました。

推奨アクション 不要。

113008

エラーメッセージ `%Threat Defense-6-113008: AAA transaction status ACCEPT: user = user`

説明 IPSec 接続または WebVPN 接続に関連付けられているユーザーの AAA トランザクションが正常に完了しました。user は、接続に関連付けられているユーザー名です。

推奨アクション 不要。

113009

エラーメッセージ `%Threat Defense-6-113009: AAA retrieved default group policy policy for user user`

説明 IPSec 接続または WebVPN 接続の認証または認可が行われました。**tunnel-group** コマンドまたは **webvpn** コマンドで指定されたグループ ポリシーの属性が取得されました。

推奨アクション 不要。

113010

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

説明 SecurID サーバーを使用した IPSec 接続の認証が行われました。ユーザーは、認証に先立って詳細情報を入力するよう求められます。

- **user**：接続に関連付けられているユーザー名
- **server _IP_address**：関連する AAA サーバーの IP アドレス

推奨アクション 不要。

113011

エラーメッセージ `%Threat Defense-6-113011: AAA retrieved user specific group policy policy for user user`

説明 IPSec 接続または WebVPN 接続の認証または認可が行われました。**tunnel-group** コマンドまたは **webvpn** コマンドで指定されたグループ ポリシーの属性が取得されました。

推奨アクション 不要。

113012

エラーメッセージ `%Threat Defense-6-113012: AAA user authentication Successful: local database: user = user`

説明 IPSec 接続または WebVPN 接続に関連付けられているユーザーが、ローカル ユーザー データベースに正常に認証されました。

- **user**：接続に関連付けられているユーザー名

推奨アクション 不要。

113013

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

説明 IPSec 接続または WebVPN 接続に関連付けられているユーザーの AAA トランザクションが、エラーにより失敗したか、またはポリシー違反により拒否されました。

- **reason**：理由の詳細
- **user**：接続に関連付けられているユーザー名

推奨アクション 不要。

113014

エラーメッセージ `%Threat Defense-6-113014: AAA authentication server not accessible: server = server_IP_address : user = user`

説明デバイスが、IPSec 接続または WebVPN 接続に関連付けられている AAA トランザクション中に設定済み AAA サーバーと通信できませんでした。このため、ユーザーが接続しようとしたとき、**aaa-server** グループに設定されているバックアップ サーバーおよびそのサーバーのアベイラビリティ次第で、接続に失敗する場合も、失敗しない場合もあります。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。

推奨アクション 設定済みの AAA サーバーとの接続を確認します。

113015

エラーメッセージ `%Threat Defense-6-113015: AAA user authentication Rejected: reason = reason : local database: user = user: user IP = xxx.xxx.xxx.xxx`

説明 IPSec 接続または WebVPN 接続に関連付けられているユーザーのローカル ユーザー データベースへの認証要求が拒否されました。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。

- **reason**：要求が拒否された理由の詳細
- **user**：接続に関連付けられているユーザー名
- **user_ip**：認証または認証要求を開始したユーザーの IP アドレス<915CLI>

推奨アクション 不要。

113016

エラーメッセージ `%Threat Defense-6-113016: AAA credentials rejected: reason = reason : server = server_IP_address : user = user<915CLI>: user IP = xxx.xxx.xxx.xxx`

説明 IPSec 接続または WebVPN 接続に関連付けられているユーザーの AAA トランザクションが、エラーにより失敗したか、またはポリシー違反により拒否されました。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。

- **reason**：要求が拒否された理由の詳細

- **server_IP_address**：関連する AAA サーバーの IP アドレス
- **user**：接続に関連付けられているユーザー名
- *<915CLI>user_ip*：認証または認証要求を開始したユーザーの IP アドレス

推奨アクション 不要。

113017

エラーメッセージ `%Threat Defense-6-113017: AAA credentials rejected: reason = reason : local database: user = user: user IP = xxx.xxx.xxx.xxx`

説明 IPSec 接続または WebVPN 接続に関連付けられているユーザーの AAA トランザクションが、エラーにより失敗したか、またはポリシー違反により拒否されました。このイベントが表示されるのは、AAA トランザクションが外部 AAA サーバーではなくローカル ユーザー データベースと行われる場合だけです。

- **reason**：要求が拒否された理由の詳細
- **user**：接続に関連付けられているユーザー名
- **user_ip**：認証または認証要求を開始したユーザーの IP アドレス

推奨アクション 不要。

113018

エラーメッセージ `%Threat Defense-3-113018: User: user , Unsupported downloaded ACL Entry: ACL_entry , Action: action`

説明サポートされていないフォーマットの ACL エントリが認証サーバーからダウンロードされました。メッセージの値は次のとおりです。

- **user**：ログインを試行しているユーザー
- **ACL_entry**：認証サーバーからダウンロードされたサポートされていない ACL エントリ
- **action**：サポートされていない ACL エントリに対して実行するアクション

推奨アクション 認証サーバーの ACL エントリは、サポートされている ACL エントリ フォーマットに適合するように管理者が変更する必要があります。

113019

エラーメッセージ `%Threat Defense-4-113019: Group = group , Username = username , IP = peer_address , Session disconnected. Session Type: type , Duration: duration , Bytes xmt: count , Bytes rcv: count , Reason: reason`

説明最大アイドル ユーザーが切断されたタイミングとその理由を示します。

- **group**：グループ名
- **username**：ユーザー名
- **IP**：ピア アドレス
- **Session Type**：セッション タイプ（たとえば IPSec または UDP）

- **duration**：接続期間（時間、分、および秒）
- **Bytes xmt**：送信されたバイト数
- *Bytes rcv*：受信されたバイト数
- **reason**：切断原因

ユーザーから要求された

搬送が失われた

サービスが失われた

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

接続が切り替えられた。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。

ポートが中断された

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

SA が期限切れ

IKE の削除

帯域幅の管理エラー

証明書が期限切れ

フェーズ 2 の不一致

ファイアウォールの不一致

ピア アドレスの変更

ACL 解析エラー

フェーズ 2 エラー

設定エラー

ピアの再接続

内部エラー

クリプト マップ ポリシーが見つからない

L2TP 開始

VLAN マッピング エラー

NAC ポリシー エラー

ダイナミック アクセス ポリシーの終了

サポートされていないクライアント タイプ

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。

113020

エラーメッセージ `%Threat Defense-3-113020: Kerberos error: Clock skew with server ip_address greater than 300 seconds`

説明 Kerberos サーバー経由の IPSec または WebVPN のユーザーの認証が、Secure Firewall Threat Defense デバイス のクロックとそのサーバーのクロックが 5 分（300 秒）以上ずれているために失敗しました。この失敗が起こったときは、接続しようとしても拒否されます。

- *ip_address*：Kerberos サーバーの IP アドレス

推奨アクション Secure Firewall Threat Defense デバイス サーバーと Kerberos サーバーのクロックを同期させます。

113021

エラーメッセージ `%Threat Defense-3-113021 : Attempted console login failed. User username did NOT have appropriate Admin Rights.`

説明ユーザーが管理コンソールにアクセスしようとしましたが、拒否されました。

- *username*：ユーザーが入力したユーザー名

推奨アクション 新しく追加された admin 権限ユーザーの場合は、そのユーザーのサービス タイプ（LOCAL または RADIUS 認証サーバー）が次のようなアクセスを許可するように設定されていることを確認します。

- nas-prompt：コンソールへのログインおよび要求されたレベルの EXEC 特権を許可しますが、イネーブル（コンフィギュレーション修正）アクセスは許可しません。
- admin：すべてのアクセスを許可します。コマンド特権によって制約できます。

上記以外のユーザーの場合は、そのユーザーが管理コンソールへの不適切なアクセスを試みています。実行されるアクションは、このような問題に関する社内のポリシーに適合している必要があります。

113022

エラーメッセージ `%Threat Defense-2-113022: AAA Marking RADIUS server servername in aaa-server group AAA-Using-DNS as FAILED`

説明 Secure Firewall Threat Defense デバイス が AAA サーバーに認証、許可、またはアカウンティングの要求を試みましたが、設定されているタイムアウト期間内に応答を受信しませんでした。この AAA サーバーには失敗のマークが付けられます。この AAA サーバーは、サービスから削除されました。

- *protocol*：次のいずれかのタイプの認証プロトコル

- RADIUS

- TACACS+

- NT

- RSA SecurID

- Kerberos

- LDAP

- *ip-addr*：AAA サーバーの IP アドレス
- *tag*：サーバー グループ名

推奨アクション AAA サーバーがオンラインで、Secure Firewall Threat Defense デバイス からアクセスできることを確認します。

113023

エラーメッセージ `%Threat Defense-2-113023: AAA Marking protocol server ip-addr in server group tag as ACTIVE`

説明以前失敗のマークを付けられた AAA サーバーが、Secure Firewall Threat Defense デバイスによって再びアクティブにされました。AAA 要求の処理に、この AAA サーバーを使用できるようになりました。

- *protocol*：次のいずれかのタイプの認証プロトコル

- RADIUS

- TACACS+

- NT

- RSA SecurID

- Kerberos

- LDAP

- *ip-addr*：AAA サーバーの IP アドレス
- *tag*：サーバー グループ名

推奨アクション 不要。

113024

エラーメッセージ `%Threat Defense-5-113024: Group tg : Authenticating type connection from ip with username, user_name , from client certificate`

説明ユーザー名の事前入力機能によって、AAA 用にクライアント証明書から抽出されたユーザー名で元のユーザー名が上書きされました。

- *tg*：トンネル グループ
- *type*：接続のタイプ（SSL クライアントまたはクライアントレス）
- *ip*：接続しているユーザーの IP アドレス
- *user_name*：AAA 用にクライアント証明書から抽出された名前

推奨アクション 不要。

113025

エラーメッセージ `%Threat Defense-5-113025: Group tg : fields  Could not authenticate connection type connection from ip`

説明証明書からユーザー名を正常に抽出できませんでした。

- *tg*：トンネル グループ
- *fields*：検索対象の DN フィールド
- *connection type*：接続のタイプ（SSL クライアントまたはクライアントレス）
- *ip*：接続しているユーザーの IP アドレス

推奨アクション 管理者は、**authentication aaa certificate**、**ssl certificate-authentication**、および **authorization-dn-attributes** の各キーワードが正しく設定されていることを確認する必要があります。

113026

エラーメッセージ `%Threat Defense-4-113026: Error error while executing Lua script for group tunnel group`

説明 AAA 用にクライアント証明書からユーザー名を抽出中に、エラーが発生しました。このメッセージは、username-from-certificate use-script オプションが有効な場合にだけ生成されます。

- *error*：Lua 環境から返されたエラー文字列
- *tunnel group*：証明書からユーザー名を抽出しようとしたトンネル グループ

推奨アクション username-from-certificate use-script オプションで使用されているスクリプトにエラーがないかどうかを調べます。

113027

エラーメッセージ `%Threat Defense-2-113027: Error activating tunnel-group scripts`

説明スクリプト ファイルを正常にロードできません。username-from-certificate use-script オプションを使用するトンネル グループが正しく動作していません。

推奨アクション 管理者は、ASDM を使用して、スクリプト ファイルにエラーがないかどうかを確認する必要があります。**debug aaa** コマンドを使用して詳細なエラー メッセージを取得すると役立ちます。

113028

エラーメッセージ `%Threat Defense-7-113028: Extraction of username from VPN client certificate has` *`string`*`. [Request` *`num`* `]`

説明証明書のユーザー名の処理要求は、実行中であるか、終了しました。

- *num*：要求の ID（ファイバへのポインタの値）。単調に増加する番号です。
- *string*：次のいずれかのステータス メッセージ。
  - 「been requested（要求済み）」
  - 「started（開始）」
  - 「finished with error（エラーで終了）」
  - 「finished successfully（正常に終了）」
  - 「completed（完了）」

推奨アクション 不要。

113029

エラーメッセージ `%Threat Defense-4-113029: Group` *`group`* `User` *`user`* `IP` *`ipaddr`* `Session could not be established: session limit of` *`num`* `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。

113030

エラーメッセージ `%Threat Defense-4-113030: Group` *`group`* `User` *`user`* `IP` *`ipaddr`* `User ACL` *`acl`* `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**：グループの名前
- **user**：ユーザーの名前

- **ipaddr**：IP アドレス
- **acl**：ACL 名

推奨アクション コンフィギュレーションを変更して、指定された ACL を追加するか、ACL の名前を修正します。

113031

エラーメッセージ `%Threat Defense-4-113031: Group group User user IP ipaddr AnyConnect vpn-filter filter is an IPv6 ACL; ACL not applied.`

説明 適用される ACL のタイプが誤っています。**vpn-filter** コマンドによって、IPv6 ACL が IPv4 ACL として設定されています。

- *group*：ユーザーのグループ ポリシー名
- *user*：ユーザー名
- *ipaddr*：ユーザーのパブリック（割り当てられていない）IP アドレス
- *filter*：VPN フィルタの名前

推奨アクション Secure Firewall Threat Defense デバイス の VPN フィルタと IPv6 VPN フィルタの設定、および AAA（RADIUS）サーバーのフィルタ パラメータを検証します。正しいタイプの ACL が指定されていることを確認します。

113032

エラーメッセージ `%Threat Defense-4-113032: Group group User user IP ipaddr AnyConnect ipv6-vpn-filter filter is an IPv4 ACL; ACL not applied.`

説明 適用する ACL のタイプが誤っています。**ipv6-vpn-filter** コマンドによって、IPv4 ACL が IPv6 ACL として設定されています。

- *group*：ユーザーのグループ ポリシー名
- *user*：ユーザー名
- *ipaddr*：ユーザーのパブリック（割り当てられていない）IP アドレス
- *filter*：VPN フィルタの名前

推奨アクション Secure Firewall Threat Defense デバイス の VPN フィルタと IPv6 VPN フィルタの設定、および AAA（RADIUS）サーバーのフィルタ パラメータを検証します。正しいタイプの ACL が指定されていることを確認します。

113033

エラーメッセージ `%Threat Defense-6-113033: Group group User user IP ipaddr AnyConnect session not allowed. 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。

- *group*：ユーザーのグループ ポリシー名
- *user*：ユーザー名
- *ipaddr*：ユーザーのパブリック（割り当てられていない）IP アドレス

推奨アクション WebVPN ACL を修正します。

113034

エラーメッセージ `%Threat Defense-4-113034: Group group User user IP ipaddr User ACL acl 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**：グループの名前
- **user**：ユーザーの名前
- **ipaddr**：IP アドレス
- **acl**：ACL 名

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。

113035

エラーメッセージ `%Threat Defense-4-113035: Group group User user IP ipaddr Session terminated: AnyConnect not enabled or invalid AnyConnect image on the ASA.`

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

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

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

113036

エラーメッセージ `%Threat Defense-4-113036: Group group User user IP ipaddr AAA parameter 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**：グループの名前
- **user**：ユーザーの名前
- **ipadddr**：IP アドレス
- **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。

113037

エラーメッセージ `%Threat Defense-6-113037: 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。

推奨アクション 不要。

113038

エラーメッセージ `%Threat Defense-4-113038: Group group User user IP ipaddr Unable to create AnyConnect parent session.`

説明リソースの問題のため、指定されたグループ内のユーザーに対して AnyConnect 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。

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

推奨アクション 不要。

113039

エラーメッセージ `%Threat Defense-6-113039: Group group User user IP ipaddr AnyConnect parent 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 AnyConnect セッションが開始されました。ユーザーが AnyConnect ログイン ページを介してログインすると、AnyConnect セッションが開始されます。

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

推奨アクション 不要。

113040

エラーメッセージ `%Threat Defense-4-113040: Terminating the VPN connection attempt from attempted group . Reason: This connection is group locked to locked group.`

説明 接続が試行されるトンネル グループは、グループ ロックに設定されているトンネル グループと同じではありません。

- *attempted group*：接続が着信するトンネル グループ
- *locked group*：接続がロックまたは制限されているトンネル グループ

推奨アクション グループ ポリシーまたはユーザー属性のグループロック値を確認します。

113041

エラーメッセージ `%Threat Defense-4-113041: Redirect ACL configured for assigned IP does not exist on the device.`

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

- *assigned-ip*：クライアントに割り当てられる IP アドレス

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

113042

エラーメッセージ `%Threat Defense-4-113042: CoA: Non-HTTP connection from src_if :src_ip /src_port to dest_if :dest_ip /dest_port for user username at client_IP denied by redirect filter; only HTTP connections are supported for redirection.`

説明 CoA 機能の場合、リダイレクト ACL フィルタは、リダイレクト処理中に一致する非 HTTP トラフィックをドロップし、終了したトラフィック フローに関する情報を提供します。

- *src_if*、*src_ip*、*src_port*：フローの送信元インターフェイス、IP アドレス、ポート
- *dest_if*、*dest_ip*、*dest_port*：フローの宛先インターフェイス、IP アドレス、ポート
- *username*：ユーザーの名前
- *client_IP*：クライアントの IP アドレス

推奨アクション Secure Firewall Threat Defense デバイス のリダイレクト ACL の設定を検証します。リダイレクトするトラフィックに正しく一致し、通過を許可するフローが間違ってブロックされることがないように適正なフィルタを使用してください。

メッセージ 114001 ～ 199027

この項では、114001 から 199027 までのメッセージについて説明します。

114001

エラーメッセージ `%Threat Defense-1-114001: Failed to initialize 4GE SSM I/O card (error error_string ).`

説明 I2C エラーまたはスイッチ初期化エラーのためにシステムが 4GE SSM I/O カードを初期化できませんでした。

- *syslog_id*：メッセージ識別子

- >*error_string*：I2C シリアル バス エラーまたはスイッチ アクセス エラー（10 進数のエラー コード）。I2C シリアル バス エラーは次のとおりです。
  - I2C_BUS_TRANSACTION_ERROR
  - I2C_CHKSUM_ERROR
  - I2C_TIMEOUT_ERROR
  - I2C_BUS_COLLISION_ERROR
  - I2C_HOST_BUSY_ERROR
  - I2C_UNPOPULATED_ERROR
  - I2C_SMBUS_UNSUPPORT
  - I2C_BYTE_COUNT_ERROR
  - I2C_DATA_PTR_ERROR

推奨アクション次の手順を実行します。

1. イベントに関連付けられているメッセージとエラーを記録して確認します。
2. Secure Firewall Threat Defense デバイスで実行しているソフトウェアをリブートします。
3. デバイスの電源を一度切ってから再投入します。電源を切った後、必ず数秒待ってから電源を入れます。
4. 問題が解決しない場合、Cisco TAC にお問い合わせください。

114002

エラーメッセージ `%Threat Defense-1-114002: Failed to initialize SFP in 4GE SSM I/O card (error error_string ).`

説明 I2C エラーまたはスイッチ初期化エラーのためにシステムが 4GE SSM I/O カードの SFP コネクタを初期化できませんでした。

- >*syslog_id*：メッセージ識別子
- >*error_string*：I2C シリアル バス エラーまたはスイッチ アクセス エラー（10 進数のエラー コード）。I2C シリアル バス エラーは次のとおりです。
  - I2C_BUS_TRANSACTION_ERROR
  - I2C_CHKSUM_ERROR
  - I2C_TIMEOUT_ERROR
  - I2C_BUS_COLLISION_ERROR
  - I2C_HOST_BUSY_ERROR
  - I2C_UNPOPULATED_ERROR
  - I2C_SMBUS_UNSUPPORT
  - I2C_BYTE_COUNT_ERROR
  - I2C_DATA_PTR_ERROR

推奨アクション次の手順を実行します。

1. イベントに関連付けられているメッセージとエラーを記録して確認します。
2. Secure Firewall Threat Defense デバイスで実行しているソフトウェアをリブートします。

3. デバイスの電源を一度切ってから再投入します。電源を切った後、必ず数秒待ってから電源を入れます。
4. 問題が解決しない場合、Cisco TAC にお問い合わせください。

114003

エラーメッセージ `%Threat Defense-1-114003: Failed to run cached commands in 4GE SSM I/O card (error error_string ).`

説明 I2C エラーまたはスイッチ初期化エラーのためにシステムが 4GE SSM I/O カードにキャッシュされたコマンドを実行できませんでした。

- >*syslog_id*：メッセージ識別子
- >*error_string*：I2C シリアル バス エラーまたはスイッチ アクセス エラー（10 進数のエラーコード）。I2C シリアル バス エラーは次のとおりです。
  - I2C_BUS_TRANSACTION_ERROR
  - I2C_CHKSUM_ERROR
  - I2C_TIMEOUT_ERROR
  - I2C_BUS_COLLISION_ERROR
  - I2C_HOST_BUSY_ERROR
  - I2C_UNPOPULATED_ERROR
  - I2C_SMBUS_UNSUPPORT
  - I2C_BYTE_COUNT_ERROR
  - I2C_DATA_PTR_ERROR

推奨アクション次の手順を実行します。

1. イベントに関連付けられているメッセージとエラーを記録して確認します。
2. Secure Firewall Threat Defense デバイスで実行しているソフトウェアをリブートします。
3. デバイスの電源を一度切ってから再投入します。電源を切った後、必ず数秒待ってから電源を入れます。
4. 問題が解決しない場合、Cisco TAC にお問い合わせください。

114004

エラーメッセージ `%Threat Defense-6-114004: 4GE SSM I/O Initialization start.`

説明 4GE SSM I/O の初期化が開始されていることがユーザーに通知されました。

- >*syslog_id*：メッセージ識別子

推奨アクション 不要。

114005

エラーメッセージ `%Threat Defense-6-114005: 4GE SSM I/O Initialization end.`

説明 4GE SSM I/O の初期化が終了したことがユーザーに通知されました。

- >*syslog_id*：メッセージ識別子

推奨アクション 不要。

114006

エラーメッセージ `%Threat Defense-3-114006: Failed to get port statistics in 4GE SSM I/O card (error error_string ).`

説明 I2C エラーまたはスイッチ初期化エラーのために Secure Firewall Threat Defense デバイスが 4GE SSM I/O カードのポート統計情報を取得できませんでした。

- >*syslog_id*：メッセージ識別子
- >*error_string*：I2C シリアル バス エラーまたはスイッチ アクセス エラー（10 進数のエラーコード）。I2C シリアル バス エラーは次のとおりです。
  - I2C_BUS_TRANSACTION_ERROR
  - I2C_CHKSUM_ERROR
  - I2C_TIMEOUT_ERROR
  - I2C_BUS_COLLISION_ERROR
  - I2C_HOST_BUSY_ERROR
  - I2C_UNPOPULATED_ERROR
  - I2C_SMBUS_UNSUPPORT
  - I2C_BYTE_COUNT_ERROR
  - I2C_DATA_PTR_ERROR

推奨アクション次の手順を実行します。

1. イベントに関連付けられているメッセージとエラーを記録して確認します。
2. Secure Firewall Threat Defense デバイスで実行しているソフトウェアをリブートします。
3. デバイスの電源を一度切ってから再投入します。電源を切った後、必ず数秒待ってから電源を入れます。
4. 問題が解決しない場合、Cisco TAC にお問い合わせください。

114007

エラーメッセージ `%Threat Defense-3-114007: Failed to get current msr in 4GE SSM I/O card (error error_string ).`

説明 I2C エラーまたはスイッチ初期化エラーのために Secure Firewall Threat Defense デバイスが 4GE SSM I/O カードの現在のモジュール ステータス レジスタ情報を取得できませんでした。

- >*syslog_id*：メッセージ識別子
- >*error_string*：I2C シリアル バス エラーまたはスイッチ アクセス エラー（10 進数のエラーコード）。I2C シリアル バス エラーは次のとおりです。
  - I2C_BUS_TRANSACTION_ERROR
  - I2C_CHKSUM_ERROR
  - I2C_TIMEOUT_ERROR

- I2C_BUS_COLLISION_ERROR
- I2C_HOST_BUSY_ERROR
- I2C_UNPOPULATED_ERROR
- I2C_SMBUS_UNSUPPORT
- I2C_BYTE_COUNT_ERROR
- I2C_DATA_PTR_ERROR

推奨アクション次の手順を実行します。

1. イベントに関連付けられているメッセージとエラーを記録して確認します。
2. Secure Firewall Threat Defense デバイスで実行しているソフトウェアをリブートします。
3. デバイスの電源を一度切ってから再投入します。電源を切った後、必ず数秒待ってから電源を入れます。
4. 問題が解決しない場合、Cisco TAC にお問い合わせください。

114008

エラーメッセージ `%Threat Defense-3-114008: Failed to enable port after link is up in 4GE SSM I/O card due to either I2C serial bus access error or switch access error.`

説明 I2C シリアル バス アクセス エラーまたはスイッチ アクセス エラーのために、Up 状態へのリンク移行が 4GE SSM I/O カードで検出された後に Secure Firewall Threat Defense デバイスがポートをイネーブルにできませんでした。

- >*syslog_id*：メッセージ識別子
- >*error_string*：I2C シリアル バス エラーまたはスイッチ アクセス エラー（10 進数のエラーコード）。I2C シリアル バス エラーは次のとおりです。
  - I2C_BUS_TRANSACTION_ERROR
  - I2C_CHKSUM_ERROR
  - I2C_TIMEOUT_ERROR
  - I2C_BUS_COLLISION_ERROR
  - I2C_HOST_BUSY_ERROR
  - I2C_UNPOPULATED_ERROR
  - I2C_SMBUS_UNSUPPORT
  - I2C_BYTE_COUNT_ERROR
  - I2C_DATA_PTR_ERROR

推奨アクション次の手順を実行します。

1. イベントに関連付けられているメッセージとエラーを記録して確認します。
2. Secure Firewall Threat Defense デバイスで実行しているソフトウェアをリブートします。
3. デバイスの電源を一度切ってから再投入します。電源を切った後、必ず数秒待ってから電源を入れます。
4. 問題が解決しない場合、Cisco TAC にお問い合わせください。

114009

エラーメッセージ `%Threat Defense-3-114009: Failed to set multicast address in 4GE SSM I/O card (error error_string ).`

説明 I2C エラーまたはスイッチ初期化エラーのために Secure Firewall Threat Defense デバイスが 4GE SSM I/O カードのマルチキャスト アドレスを設定できませんでした。

- >*syslog_id*：メッセージ識別子
- >*error_string*：I2C シリアル バス エラーまたはスイッチ アクセス エラー（10 進数のエラーコード）。I2C シリアル バス エラーは次のとおりです。
  - I2C_BUS_TRANSACTION_ERROR
  - I2C_CHKSUM_ERROR
  - I2C_TIMEOUT_ERROR
  - I2C_BUS_COLLISION_ERROR
  - I2C_HOST_BUSY_ERROR
  - I2C_UNPOPULATED_ERROR
  - I2C_SMBUS_UNSUPPORT
  - I2C_BYTE_COUNT_ERROR
  - I2C_DATA_PTR_ERROR

推奨アクション次の手順を実行します。

1. イベントに関連付けられているメッセージとエラーを記録して確認します。
2. Secure Firewall Threat Defense デバイスで実行しているソフトウェアをリブートします。
3. デバイスの電源を一度切ってから再投入します。電源を切った後、必ず数秒待ってから電源を入れます。
4. 問題が解決しない場合、Cisco TAC にお問い合わせください。

114010

エラーメッセージ `%Threat Defense-3-114010: Failed to set multicast hardware address in 4GE SSM I/O card (error error_string ).`

説明 I2C エラーまたはスイッチ初期化エラーのために Secure Firewall Threat Defense デバイスが 4GE SSM I/O カードのマルチキャスト ハードウェア アドレスを設定できませんでした。

- >*syslog_id*：メッセージ識別子
- >*error_string*：I2C シリアル バス エラーまたはスイッチ アクセス エラー（10 進数のエラーコード）。I2C シリアル バス エラーは次のとおりです。
  - I2C_BUS_TRANSACTION_ERROR
  - I2C_CHKSUM_ERROR
  - I2C_TIMEOUT_ERROR
  - I2C_BUS_COLLISION_ERROR
  - I2C_HOST_BUSY_ERROR
  - I2C_UNPOPULATED_ERROR
  - I2C_SMBUS_UNSUPPORT

- I2C_BYTE_COUNT_ERROR
- I2C_DATA_PTR_ERROR
- I2C_DATA_PTR_ERROR

推奨アクション次の手順を実行します。

1. イベントに関連付けられているメッセージとエラーを記録して確認します。
2. Secure Firewall Threat Defense デバイスで実行しているソフトウェアをリブートします。
3. デバイスの電源を一度切ってから再投入します。電源を切った後、必ず数秒待ってから電源を入れます。
4. 問題が解決しない場合、Cisco TAC にお問い合わせください。

114011

エラーメッセージ `%Threat Defense-3-114011: Failed to delete multicast address in 4GE SSM I/O card (error error_string ).`

説明 I2C エラーまたはスイッチ初期化エラーのために Secure Firewall Threat Defense デバイスが 4GE SSM I/O カードのマルチキャスト アドレスを削除できませんでした。

- >*syslog_id*：メッセージ識別子
- >*error_string*：I2C シリアル バス エラーまたはスイッチ アクセス エラー（10 進数のエラーコード）。I2C シリアル バス エラーは次のとおりです。
  - I2C_BUS_TRANSACTION_ERROR
  - I2C_CHKSUM_ERROR
  - I2C_TIMEOUT_ERROR
  - I2C_BUS_COLLISION_ERROR
  - I2C_HOST_BUSY_ERROR
  - I2C_UNPOPULATED_ERROR
  - I2C_SMBUS_UNSUPPORT
  - I2C_BYTE_COUNT_ERROR
  - I2C_DATA_PTR_ERROR

推奨アクション次の手順を実行します。

1. イベントに関連付けられているメッセージとエラーを記録して確認します。
2. Secure Firewall Threat Defense デバイスで実行しているソフトウェアをリブートします。
3. デバイスの電源を一度切ってから再投入します。電源を切った後、必ず数秒待ってから電源を入れます。
4. 問題が解決しない場合、Cisco TAC にお問い合わせください。

114012

エラーメッセージ `%Threat Defense-3-114012: Failed to delete multicast hardware address in 4GE SSM I/O card (error error_string ).`

説明 I2C エラーまたはスイッチ初期化エラーのために Secure Firewall Threat Defense デバイスが 4GE SSM I/O カードのマルチキャスト ハードウェア アドレスを削除できませんでした。

- >*syslog_id*：メッセージ識別子
- >*error_string*：I2C シリアル バス エラーまたはスイッチ アクセス エラー（10 進数のエラーコード）。I2C シリアル バス エラーは次のとおりです。
  - I2C_BUS_TRANSACTION_ERROR
  - I2C_CHKSUM_ERROR
  - I2C_TIMEOUT_ERROR
  - I2C_BUS_COLLISION_ERROR
  - I2C_HOST_BUSY_ERROR
  - I2C_UNPOPULATED_ERROR
  - I2C_SMBUS_UNSUPPORT
  - I2C_BYTE_COUNT_ERROR
  - I2C_DATA_PTR_ERROR

推奨アクション次の手順を実行します。

1. イベントに関連付けられているメッセージとエラーを記録して確認します。
2. Secure Firewall Threat Defense デバイスで実行しているソフトウェアをリブートします。
3. デバイスの電源を一度切ってから再投入します。電源を切った後、必ず数秒待ってから電源を入れます。
4. 問題が解決しない場合、Cisco TAC にお問い合わせください。

114013

エラーメッセージ `%Threat Defense-3-114013: Failed to set mac address table in 4GE SSM I/O card (error error_string ).`

説明 I2C エラーまたはスイッチ初期化エラーのために Secure Firewall Threat Defense デバイスが 4GE SSM I/O カードの MAC アドレス テーブルを設定できませんでした。

- >*syslog_id*：メッセージ識別子
- >*error_string*：I2C シリアル バス エラーまたはスイッチ アクセス エラー（10 進数のエラーコード）。I2C シリアル バス エラーは次のとおりです。

- I2C_BUS_TRANSACTION_ERROR

- I2C_CHKSUM_ERROR

- I2C_TIMEOUT_ERROR

- I2C_BUS_COLLISION_ERROR

- I2C_HOST_BUSY_ERROR

- I2C_UNPOPULATED_ERROR

- I2C_SMBUS_UNSUPPORT

- I2C_BYTE_COUNT_ERROR

- I2C_DATA_PTR_ERROR

推奨アクション次の手順を実行します。

1. イベントに関連付けられているメッセージとエラーを記録して確認します。
2. Secure Firewall Threat Defense デバイスで実行しているソフトウェアをリブートします。
3. デバイスの電源を一度切ってから再投入します。電源を切った後、必ず数秒待ってから電源を入れます。
4. 問題が解決しない場合、Cisco TAC にお問い合わせください。

114014

エラーメッセージ `%Threat Defense-3-114014: Failed to set mac address in 4GE SSM I/O card (error error_string ).`

説明 I2C エラーまたはスイッチ初期化エラーのために Secure Firewall Threat Defense デバイスが 4GE SSM I/O カードの MAC アドレスを設定できませんでした。

- >*syslog_id*：メッセージ識別子
- >*error_string*：I2C シリアル バス エラーまたはスイッチ アクセス エラー（10 進数のエラーコード）。I2C シリアル バス エラーは次のとおりです。

- I2C_BUS_TRANSACTION_ERROR

- I2C_CHKSUM_ERROR

- I2C_TIMEOUT_ERROR

- I2C_BUS_COLLISION_ERROR

- I2C_HOST_BUSY_ERROR

- I2C_UNPOPULATED_ERROR

- I2C_SMBUS_UNSUPPORT

- I2C_BYTE_COUNT_ERROR

- I2C_DATA_PTR_ERROR

推奨アクション次の手順を実行します。

1. イベントに関連付けられているメッセージとエラーを記録して確認します。
2. Secure Firewall Threat Defense デバイスで実行しているソフトウェアをリブートします。
3. デバイスの電源を一度切ってから再投入します。電源を切った後、必ず数秒待ってから電源を入れます。
4. 問題が解決しない場合、Cisco TAC にお問い合わせください。

114015

エラーメッセージ `%Threat Defense-3-114015: Failed to set mode in 4GE SSM I/O card (error error_string ).`

説明 I2C エラーまたはスイッチ初期化エラーのために Secure Firewall Threat Defense デバイスが 4GE SSM I/O カードの個々のモードまたは無差別モードを設定できませんでした。

- >*syslog_id*：メッセージ識別子
- >*error_string*：I2C シリアル バス エラーまたはスイッチ アクセス エラー（10 進数のエラー コード）。I2C シリアル バス エラーは次のとおりです。

- I2C_BUS_TRANSACTION_ERROR
- I2C_CHKSUM_ERROR
- I2C_TIMEOUT_ERROR
- I2C_BUS_COLLISION_ERROR
- I2C_HOST_BUSY_ERROR
- I2C_UNPOPULATED_ERROR
- I2C_SMBUS_UNSUPPORT
- I2C_BYTE_COUNT_ERROR
- I2C_DATA_PTR_ERROR

推奨アクション次の手順を実行します。

1. イベントに関連付けられているメッセージとエラーを記録して確認します。
2. Secure Firewall Threat Defense デバイスで実行しているソフトウェアをリブートします。
3. デバイスの電源を一度切ってから再投入します。電源を切った後、必ず数秒待ってから電源を入れます。
4. 問題が解決しない場合、Cisco TAC にお問い合わせください。

114016

エラーメッセージ `%Threat Defense-3-114016: Failed to set multicast mode in 4GE SSM I/O card (error error_string ).`

説明 I2C エラーまたはスイッチ初期化エラーのために Secure Firewall Threat Defense デバイスが 4GE SSM I/O カードのマルチキャスト モードを設定できませんでした。

- >*syslog_id*：メッセージ識別子
- >*error_string*：I2C シリアル バス エラーまたはスイッチ アクセス エラー（10 進数のエラー コード）。I2C シリアル バス エラーは次のとおりです。

- I2C_BUS_TRANSACTION_ERROR
- I2C_CHKSUM_ERROR
- I2C_TIMEOUT_ERROR
- I2C_BUS_COLLISION_ERROR
- I2C_HOST_BUSY_ERROR
- I2C_UNPOPULATED_ERROR
- I2C_SMBUS_UNSUPPORT
- I2C_BYTE_COUNT_ERROR
- I2C_DATA_PTR_ERROR

推奨アクション次の手順を実行します。

1. イベントに関連付けられているメッセージとエラーを記録して確認します。
2. Secure Firewall Threat Defense デバイスで実行しているソフトウェアをリブートします。
3. デバイスの電源を一度切ってから再投入します。電源を切った後、必ず数秒待ってから電源を入れます。
4. 問題が解決しない場合、Cisco TAC にお問い合わせください。

114017

エラーメッセージ `%Threat Defense-3-114017: Failed to get link status in 4GE SSM I/O card (error error_string ).`

説明 I2C シリアル バス アクセス エラーまたはスイッチ アクセス エラーのために Secure Firewall Threat Defense デバイス が 4GE SSM I/O カードのリンク ステータスを取得できませんでした。

- >*syslog_id*：メッセージ識別子
- >*error_string*：I2C シリアル バス エラーまたはスイッチ アクセス エラー（10 進数のエラー コード）。I2C シリアル バス エラーは次のとおりです。

- I2C_BUS_TRANSACTION_ERROR

- I2C_CHKSUM_ERROR

- I2C_TIMEOUT_ERROR

- I2C_BUS_COLLISION_ERROR

- I2C_HOST_BUSY_ERROR

- I2C_UNPOPULATED_ERROR

- I2C_SMBUS_UNSUPPORT

- I2C_BYTE_COUNT_ERROR

- I2C_DATA_PTR_ERROR

推奨アクション：次のステップを実行します。

1. システム管理者に通知します。
2. イベントに関連付けられているメッセージとエラーを記録して確認します。
3. Secure Firewall Threat Defense デバイスで実行しているソフトウェアをリブートします。
4. デバイスの電源を一度切ってから再投入します。電源を切った後、必ず数秒待ってから電源を入れます。
5. 問題が解決しない場合、Cisco TAC にお問い合わせください。

114018

エラーメッセージ `%Threat Defense-3-114018: Failed to set port speed in 4GE SSM I/O card (error error_string ).`

説明 I2C エラーまたはスイッチ初期化エラーのために Secure Firewall Threat Defense デバイスが 4GE SSM I/O カードのポート速度を設定できませんでした。

- >*syslog_id*：メッセージ識別子
- >*error_string*：I2C シリアル バス エラーまたはスイッチ アクセス エラー（10 進数のエラーコード）。I2C シリアル バス エラーは次のとおりです。

- I2C_BUS_TRANSACTION_ERROR

- I2C_CHKSUM_ERROR

- I2C_TIMEOUT_ERROR

- I2C_BUS_COLLISION_ERROR

- I2C_HOST_BUSY_ERROR

- I2C_UNPOPULATED_ERROR

- I2C_SMBUS_UNSUPPORT

- I2C_BYTE_COUNT_ERROR

- I2C_DATA_PTR_ERROR

推奨アクション次の手順を実行します。

1. イベントに関連付けられているメッセージとエラーを記録して確認します。
2. Secure Firewall Threat Defense デバイスで実行しているソフトウェアをリブートします。
3. デバイスの電源を一度切ってから再投入します。電源を切った後、必ず数秒待ってから電源を入れます。
4. 問題が解決しない場合、Cisco TAC にお問い合わせください。

114019

エラーメッセージ `%Threat Defense-3-114019: Failed to set media type in 4GE SSM I/O card (error error_string ).`

説明 I2C エラーまたはスイッチ初期化エラーのために Secure Firewall Threat Defense デバイスが 4GE SSM I/O カードのメディア タイプを設定できませんでした。

- >*syslog_id*：メッセージ識別子
- >*error_string*：I2C シリアル バス エラーまたはスイッチ アクセス エラー（10 進数のエラーコード）。I2C シリアル バス エラーは次のとおりです。

- I2C_BUS_TRANSACTION_ERROR

- I2C_CHKSUM_ERROR

- I2C_TIMEOUT_ERROR

- I2C_BUS_COLLISION_ERROR

- I2C_HOST_BUSY_ERROR

- I2C_UNPOPULATED_ERROR

- I2C_SMBUS_UNSUPPORT

- I2C_BYTE_COUNT_ERROR

- I2C_DATA_PTR_ERROR

推奨アクション次の手順を実行します。

1. イベントに関連付けられているメッセージとエラーを記録して確認します。
2. Secure Firewall Threat Defense デバイスで実行しているソフトウェアをリブートします。
3. デバイスの電源を一度切ってから再投入します。電源を切った後、必ず数秒待ってから電源を入れます。
4. 問題が解決しない場合、Cisco TAC にお問い合わせください。

114020

エラーメッセージ `%Threat Defense-3-114020: Port link speed is unknown in 4GE SSM I/O card.`

説明 Secure Firewall Threat Defense デバイス が 4GE SSM I/O カードのポート リンク速度を検出できません。

推奨アクション：次のステップを実行します。

1. イベントに関連付けられているメッセージを記録して確認します。
2. 4GE SSM I/O カードをリセットし、ソフトウェアがイベントから自動的に回復するかどうかを観察します。
3. ソフトウェアが自動的に回復しない場合は、デバイスの電源を一度切ってから再投入します。電源を切った後、必ず数秒待ってから電源を入れます。
4. 問題が解決しない場合、Cisco TAC にお問い合わせください。

114021

エラーメッセージ `%Threat Defense-3-114021: Failed to set multicast address table in 4GE SSM I/O card due to` *`error`* `.`

説明 I2C シリアル バス アクセス エラーまたはスイッチ アクセス エラーのために Secure Firewall Threat Defense デバイス が 4GE SSM I/O カードのマルチキャスト アドレス テーブルを設定できませんでした。

- **error**：スイッチ アクセス エラー（10 進数のエラー コード）または I2C シリアル バス エラー。考えられる I2C シリアル バス エラーは次のとおりです。

- I2C_BUS_TRANSACTION_ERROR

- I2C_CHKSUM_ERROR

- I2C_TIMEOUT_ERROR

- I2C_BUS_COLLISION_ERROR

- I2C_HOST_BUSY_ERROR

- I2C_UNPOPULATED_ERROR

- I2C_SMBUS_UNSUPPORT

- I2C_BYTE_COUNT_ERROR

- I2C_DATA_PTR_ERROR

推奨アクション：次のステップを実行します。

1. イベントに関連付けられているメッセージを記録して確認します。
2. Secure Firewall Threat Defense デバイスのリブートを試みます。
3. ソフトウェアが自動的に回復しない場合は、デバイスの電源を一度切ってから再投入します。電源を切った後、必ず数秒待ってから電源を入れます。
4. 問題が解決しない場合、Cisco TAC にお問い合わせください。

114022

エラーメッセージ `%Threat Defense-3-114022: Failed to pass broadcast traffic in 4GE SSM I/O card due to error_string`

説明スイッチ アクセス エラーが原因で Secure Firewall Threat Defense デバイス が 4GE SSM I/O カードでブロードキャスト トラフィックを渡すことができませんでした。

- *error_string*：10 進エラー コードであるスイッチ アクセス エラー

推奨アクション：次のステップを実行します。

1. イベントが含まれているメッセージとエラーを記録します。
2. ssm4ge_dump ファイルをコンパクト フラッシュから取得し、Cisco TAC に送信します。
3. 手順 1 および 2 で収集した情報を Cisco TAC に連絡します。

（注） 4GE SSM が自動的にリセットされ回復します。

114023

エラーメッセージ `%Threat Defense-3-114023: Failed to cache/flush mac table in 4GE SSM I/O card due to error_string .`

説明 I2C シリアル バス アクセス エラーまたはスイッチ アクセス エラーが原因で、4GE SSM I/O カードで MAC テーブルをキャッシュまたはフラッシュできませんでした。このメッセージが表示されるのは稀です。

- **error_string**：I2C シリアル バス エラー（可能な値については、2 番めの項目を参照）またはスイッチ アクセス エラー（10 進エラー コード）。
- I2C シリアル バス エラーは次のとおりです。

I2C_BUS_TRANSACTION_ERROR

I2C_CHKSUM_ERROR

I2C_TIMEOUT_ERROR

I2C_BUS_COLLISION_ERROR

I2C_HOST_BUSY_ERROR

I2C_UNPOPULATED_ERROR

I2C_SMBUS_UNSUPPORT

I2C_BYTE_COUNT_ERROR

I2C_DATA_PTR_ERROR

推奨アクション次の手順を実行します。

1. イベントが含まれている syslog メッセージとエラーを記録します。
2. Secure Firewall Threat Defense デバイス のソフトウェア リブートを試みます。
3. Secure Firewall Threat Defense デバイス の電源を一度切ってから再投入します。

（注） 電源を切った後、必ず数秒待ってから電源を入れます。手順 1 ～ 3 を完了した後、問題が解決しない場合は、Cisco TAC に連絡して、手順 1 の情報を提供します。Secure Firewall Threat Defense デバイス の RMA が必要になる場合があります。

115000

エラーメッセージ `%Threat Defense-2-115000: Critical assertion in process: process name fiber: fiber name , component: component name , subcomponent: subcomponent name , file: filename , line: line number , cond: condition`

説明重要なアサーションが失敗しました。このメッセージは、チェック ビルドでの開発時にだけ使用され、実稼働ビルドでは使用されません。

- **process name**：プロセスの名前
- *fiber name*：ファイバの名前
- *component name*：指定したコンポーネントの名前
- *subcomponent name*：指定したサブコンポーネントの名前
- *filename*：指定したファイルの名前
- *line number*：指定した行の行番号
- *condition*：指摘された状態

推奨アクション優先度の高い障害を記録として残し、アサーションの原因を調査し、問題を修正する必要があります。

115001

エラーメッセージ `%Threat Defense-3-115001: Error in process: process name fiber: fiber name , component: component name , subcomponent: subcomponent name , file: filename , line: line number , cond: condition`

説明エラー アサーションが失敗しました。このメッセージは、チェック ビルドでの開発時にだけ使用され、実稼働ビルドでは使用されません。

- **process name**：プロセスの名前
- *fiber name*：ファイバの名前
- *component name*：指定したコンポーネントの名前
- *subcomponent name*：指定したサブコンポーネントの名前
- *filename*：指定したファイルの名前
- *line number*：指定した行の行番号
- *condition*：指摘された状態

推奨アクション障害を記録として残し、アサーションの原因を調査し、問題を修正する必要があります。

115002

エラーメッセージ `%Threat Defense-4-115002: Warning in process: process name fiber: fiber name , component: component name , subcomponent: subcomponent name , file: filename , line: line number , cond: condition`

説明警告アサーションが失敗しました。このメッセージは、チェック ビルドでの開発時にだけ使用され、実稼働ビルドでは使用されません。

- **process name**：プロセスの名前
- *fiber name*：ファイバの名前
- *component name*：指定したコンポーネントの名前
- *subcomponent name*：指定したサブコンポーネントの名前
- *filename*：指定したファイルの名前
- *line number*：指定した行の行番号
- *condition*：指摘された状態

推奨アクションアサーションの原因を調査し、問題が見つかった場合は、障害を記録として残し、問題を修正する必要があります。

199001

エラーメッセージ `%Threat Defense-5-199001: Reload command executed from Telnet (remote IP_address ).`

説明 reload コマンドで Secure Firewall Threat Defense デバイス のリブートを開始するホストのアドレスが記録されました。

推奨アクション 不要。

199002

エラーメッセージ `%Threat Defense-6-199002: startup completed. Beginning operation.`

説明 Secure Firewall Threat Defense デバイス が、その初期ブートおよびフラッシュ メモリ読み取りシーケンスを完了し、正常動作を開始する準備が整いました。

（注） このメッセージは、no logging message コマンドを使用してもブロックできません。

推奨アクション 不要。

199003

エラーメッセージ `%Threat Defense-6-199003: Reducing link MTU dec .`

説明 Secure Firewall Threat Defense デバイス が、内部ネットワークよりも大きい MTU を使用している外部ネットワークからパケットを受信しました。その後Secure Firewall Threat Defense デバイスは、適切な MTU をネゴシエートするため、ICMP メッセージをその外部ホストに送信しました。ログ メッセージには、ICMP メッセージのシーケンス番号が含まれています。

推奨アクション 不要。

199005

エラーメッセージ `%Threat Defense-6-199005: Startup begin`

説明 Secure Firewall Threat Defense デバイス が開始されました。

推奨アクション 不要。

199010

エラーメッセージ `%Threat Defense-1-199010: Signal 11 caught in process/fiber(rtcli async executor process)/(rtcli async executor) at address 0xf132e03b, corrective action at 0xca1961a0`

説明システムは重大なエラーから回復しました。

推奨アクション Cisco TAC にお問い合わせください。

199011

エラーメッセージ `%Threat Defense-2-199011: Close on bad channel in process/fiber process/fiber , channel ID p , channel state s process/fiber  name of the process/fiber that caused the bad channel close operation.`

説明予期しないチャネル クローズ状態が検出されました。

- **p**：チャネル ID
- *process/fiber*：不正なチャネル クローズ動作の原因となったプロセス/ファイバの名前
- **s**：チャネル状態

推奨アクション Cisco TAC にお問い合わせください。その際はログ ファイルを添付してください。

199012

エラーメッセージ `%FTD-1-1199012: Stack overflow during new_stack_call in process/fiber` *`process/fiber`* `, call target` *`f`* `, stack size` *`s`* `,` *`process/fiber`* `name of the process/fiber that caused the stack overflow`

説明 スタックオーバーフロー状態が検出されました。

- **f**：new_stack_call のターゲット
- *process/fiber*：スタックオーバーフローの原因となったプロセス/ファイバの名前
- **s**：new_stack_call で指定されている新しいスタック サイズ

推奨アクション Cisco TAC にお問い合わせください。その際はログファイルを添付してください。

199013

エラーメッセージ `%Threat Defense-1-199013:` *`syslog`*

説明変数 syslog が補助的なプロセスによって生成されました。

- **syslog**：アラート syslog が外部プロセスから verbatim を渡しました

推奨アクション Cisco TAC にお問い合わせください。

199014

エラーメッセージ `%Threat Defense-2-199014:` *`syslog`*

説明変数 syslog が補助的なプロセスによって生成されました。

- **syslog**：重大な syslog が外部プロセスから verbatim を渡しました

推奨アクション Cisco TAC にお問い合わせください。

199015

エラーメッセージ `%Threat Defense-3-199015:` *`syslog`*

説明変数 syslog が補助的なプロセスによって生成されました。

- **syslog**：エラー syslog が外部プロセスから verbatim を渡しました

推奨アクション Cisco TAC にお問い合わせください。

199016

エラーメッセージ `%Threat Defense-4-199016:` *syslog*

説明変数 syslog が補助的なプロセスによって生成されました。

- **syslog**：警告 syslog が外部プロセスから verbatim を渡しました

推奨アクション Cisco TAC にお問い合わせください。

199017

エラーメッセージ `%Threat Defense-5-199017: syslog`

説明変数 syslog が補助的なプロセスによって生成されました。

- **syslog**：通知 syslog が外部プロセスから verbatim を渡しました

推奨アクション 不要。

199018

エラーメッセージ `%Threat Defense-6-199018: syslog`

説明変数 syslog が補助的なプロセスによって生成されました。

- **syslog**：情報 syslog が外部プロセスから verbatim を渡しました

推奨アクション 不要。

199019

エラーメッセージ `%Threat Defense-7-199019: syslog`

説明変数 syslog が補助的なプロセスによって生成されました。

- **syslog**：デバッグ syslog が外部プロセスから verbatim を渡しました

推奨アクション 不要。

199020

エラーメッセージ `%Threat Defense-2-199020: System memory utilization has reached X %. System will reload if memory usage reaches the configured trigger level of Y %.`

説明システム メモリの使用率がシステム メモリのウォッチドッグ機能の設定値の 80% に達しました。

推奨アクショントラフィック負荷を軽減し、トラフィック インスペクションを削除し、ACL エントリの数を減らすなどして、システム メモリの使用率を減らしてください。メモリ リークが疑われる場合は、Cisco TAC にお問い合わせください。

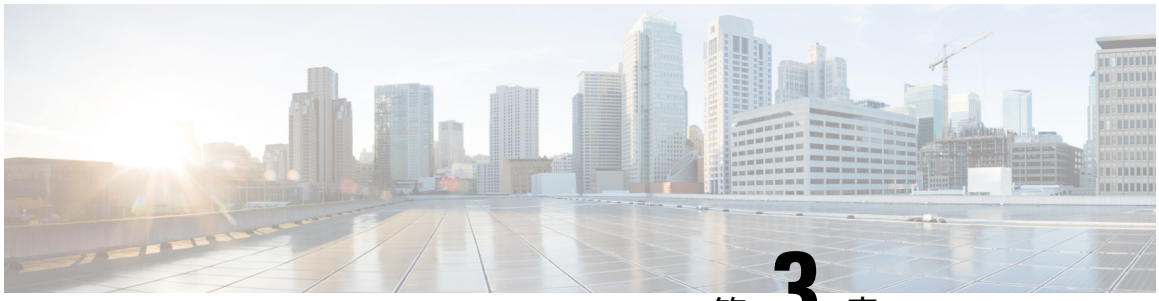
199021

エラーメッセージ `%Threat Defense-1-199021: System memory utilization has reached the configured watchdog trigger level of Y %. System will now reload`

説明 システム メモリの使用率がシステム メモリのウォッチドッグ機能の設定値の 100% に達しました。システムは自動的にリロードされます。

推奨アクション トラフィック負荷を軽減し、トラフィック インスペクションを削除し、ACL エントリの数を減らすなどして、システム メモリの使用率を減らしてください。メモリ リークが疑われる場合は、Cisco TAC にお問い合わせください。

199021



第 3 章

Syslog メッセージ 201002 ～ 219002

この章は、次の項で構成されています。

メッセージ 201002 ～ 210022

この章では、201002 から 210022 までのメッセージについて説明します。

201002

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

説明指定されたグローバル アドレスへの TCP 接続が最大数を超えました。

- econns：初期接続の最大数
- nconns：静的または xlate グローバル アドレスに許可される最大接続数

推奨アクション show static コマンドまたは show nat コマンドを使用して、スタティック アドレスへの接続に課されている制限を確認します。制限は設定可能です。

201003

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

説明指定されたスタティック グローバル アドレスを持つ、指定された外部アドレスから指定されたローカル アドレスへの初期接続の数が初期接続の制限を超えました。Secure Firewall Threat Defense デバイスへの初期接続の制限に達すると、Secure Firewall Threat Defense デバイスは何としても受け入れようと試みますが、その接続に時間制限を課します。この状況により、たとえSecure Firewall Threat Defense デバイスがビジー状態であっても、一部の接続が成功することがあります。このメッセージは、メッセージ 201002 より重大なオーバーロードを示

しています。このオーバーロードは、SYN攻撃、または正規のトラフィックの非常に重い負荷が原因で発生します。

- nconns：受信した最大初期接続数
- *elimit*：static コマンドまたは nat コマンドで指定された最大初期接続数

推奨アクション show static コマンドを使用して、スタティック アドレスへの初期接続に課されている制限を確認します。

201004

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

説明 指定されたグローバル アドレスへの UDP 接続が最大数を超えました。

- udp conn limit：静的アドレスまたは変換に許可される UDP 接続の最大数

推奨アクション show static コマンドまたは show nat コマンドを使用して、静的アドレスへの接続に課されている制限を確認します。制限は設定可能です。

201005

エラーメッセージ `%Threat Defense-3-201005: FTP data connection failed for IP_address IP_address`

説明 Secure Firewall Threat Defense デバイス が、メモリ不足のため FTP のデータ接続を追跡するための構造を割り当てることができません。

推奨アクション メモリ使用量を減らすか、または増設メモリを購入します。

201006

エラーメッセージ `%Threat Defense-3-201006: RCMD backconnection failed for IP_address/port.`

説明 メモリ不足のため Secure Firewall Threat Defense デバイス が **rsh** コマンドに対する着信標準出力のための接続を事前割り当てできません。

推奨アクション rsh クライアント バージョンを確認します。Secure Firewall Threat Defense デバイス がサポートしているのは Berkeley **rsh** クライアント バージョンだけです。メモリ使用量を減らすか、または増設メモリを購入することもできます。

201008

エラーメッセージ `%Threat Defense-3-201008: Disallowing new connections.`

説明 TCP システム ログ メッセージングをイネーブルにしていても syslog サーバーに到達できません。

推奨アクション TCP syslog メッセージングをディセーブルにします。さらに、syslog サーバーが動作しており、Secure Firewall Threat Defense コンソールからそのホストに ping できることを確認します。次に、TCP システム メッセージ ロギングを再開してトラフィックを許可します。

201009

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

説明指定されたスタティック アドレスへの接続が最大数を超えました。

- number：ホストに許可されている接続の最大数
- **IP_address**：ホスト IP アドレス
- *interface_name*：ホストの接続先インターフェイスの名前

推奨アクション show static コマンドまたは show nat コマンドを使用して、アドレスへの接続に課されている制限を確認します。制限は設定可能です。

201010

エラーメッセージ `%Threat Defense-6-201010: Embryonic connection limit exceeded econns/limit for dir packet from source_address/source_port to dest_address/dest_port on interface interface_name`

説明 TCP 接続を確立しようとしたが、トラフィック クラスに対して **set connection embryonic-conn-max** MPC コマンドで設定されている初期接続の制限を超えたために失敗しました。

ASA のさまざまな管理インターフェイスおよびプロトコルへの異常な着信トラフィックの影響を軽減するために、インターフェイスはデフォルトの初期制限 100 に設定されます。この syslog メッセージは、ASA インターフェイスへの初期接続数が 100 を超えると表示されます。このデフォルト値は変更または無効にできません。

- **econns**：設定したトラフィック クラスに関連付けられている初期接続の現在の数
- **limit**：設定した初期接続のトラフィック クラスの制限
- **dir**：input（接続を開始した最初のパケットはインターフェイス **interface_name** 上の入力パケットです）または output（接続を開始した最初のパケットはインターフェイス **interface_name** 上の出力パケットです）
- *source_address/source_port*：接続を開始しているパケットの送信元の実際の IP アドレスと送信元ポート
- *dest_address/dest_port*：接続を開始しているパケットの宛先の実際の IP アドレスと宛先ポート
- **interface_name**：ポリシー制限が強制されているインターフェイスの名前

推奨アクション 不要。

201011

エラーメッセージ `%Threat Defense-3-201011: Connection limit exceeded cnt /limit for dir packet from sip /sport to dip /dport on interface if_name .`

説明 Secure Firewall Threat Defense デバイス 経由の新しい接続により、少なくとも 1 つの設定済み最大接続制限を超えました。このメッセージは、**static** コマンドを使用して設定された接続制限にも、Cisco Modular Policy Framework を使用して設定された接続制限にも適用されます。既存の接続のいずれかが切断されて現在の接続数が設定済みの最大値を下回るまで、Secure Firewall Threat Defense デバイス 経由の新しい接続は許可されません。

- *cnt*：現在の接続数
- *limit*：設定されている接続制限
- *dir*：トラフィックの方向（着信または発信）
- *sip*：送信元の実際の IP アドレス
- *sport*：送信元ポート
- *dip*：宛先の実際の IP アドレス
- *dport*：宛先ポート
- *if_name*：トラフィックを受信したインターフェイスの名前

推奨アクション 不要。

201012

エラーメッセージ `%Threat Defense-6-201012: Per-client embryonic connection limit exceeded curr num /limit for [input|output] packet from IP_address / port to ip /port on interface interface_name`

説明 TCP 接続を確立しようとしましたが、クライアントごとの初期接続制限を超えたために失敗しました。デフォルトでは、このメッセージは 10 秒に 1 回しか表示されないように制限されています。

- **curr num**：現在の数
- **limit**：設定されている制限
- [input|output]：インターフェイス **interface_name** 上の入力パケットまたは出力パケット
- **IP_address**：実際の IP アドレス
- **port**：TCP ポートまたは UDP ポート
- **interface_name**：ポリシーが適用されているインターフェイスの名前

推奨アクション 制限に達すると、SYN フラッド アタックを防止するために、それ以降の接続要求はすべて Secure Firewall Threat Defense デバイス によってプロキシされます。クライアントが 3 ウェイ ハンドシェイクを終了できる場合に限り、Secure Firewall Threat Defense デバイスはサーバーに接続します。これは、通常、エンドユーザーにもアプリケーションにも影響しません。ただし、正当に多数の初期接続を必要とするアプリケーションに問題が生じる場合は、**set connection per-client-embryonic-max** コマンドを入力して設定を調整できます。

201013

エラーメッセージ `%Threat Defense-3-201013: Per-client connection limit exceeded curr num /limit for [input|output] packet from ip /port to ip /port on interface interface_name`

説明クライアントごとの接続制限を超えたため、接続が拒否されました。

- **curr num**：現在の数
- **limit**：設定されている制限
- [input|output]：インターフェイス **interface_name** 上の入力パケットまたは出力パケット
- **ip**：実際の IP アドレス
- **port**：TCP ポートまたは UDP ポート
- **interface_name**：ポリシーが適用されているインターフェイスの名前

推奨アクション制限に達すると、それ以降の接続要求はすべて警告なしで廃棄されます。通常は、アプリケーションで接続が再試行されるため、遅延が発生します。再試行がすべて失敗した場合にはタイムアウトも発生します。アプリケーションが正当に多数の同時接続を必要とする場合は、**set connection per-client-max** コマンドを入力して設定を調整できます。

202010

エラーメッセージ `%Threat Defense-3-202010: [NAT | PAT] pool exhausted for pool-name , port range [1-511 | 512-1023 | 1024-65535]. Unable to create protocol connection from in-interface :src-ip /src-port to out-interface :dst-ip /dst-port`

説明

- *pool-name*：NAT または PAT プール名
- *protocol*：接続を作成するために使用されるプロトコル
- *in-interface*：入力インターフェイス
- *src-ip*：送信元 IP アドレス
- *src-port*：送信元ポート
- *out-interface*：出力インターフェイス
- *dest-ip*：宛先 IP アドレス
- *dst-port*：宛先ポート

Secure Firewall Threat Defense デバイス に使用可能なアドレス変換プールがなくなりました。

推奨アクション プール内のすべてのアドレスとポートを使い果たした原因を特定するには、**show nat pool** および **show nat detail** コマンドを使用します。これが通常の状態で発生している場合は、NAT/PAT プールに IP アドレスを追加します。

202016

エラーメッセージ `%Threat Defense-3-202016: "%d: Unable to pre-allocate SIP %s secondary channel for message" \ "from %s:%A/%d to %s:%A/%d with PAT and missing port information.\n"`

説明

SIP アプリケーションがメディア ポートを 0 に設定して SDP ペイロードを生成する場合、このような無効なポート要求に PAT xlate を割り当てることはできないため、この Syslog を生成してパケットを廃棄します。

推奨アクション なし。これはアプリケーション固有の問題です。

208005

エラーメッセージ `%Threat Defense-3-208005: (function:line_num) clear command return code`

説明 Secure Firewall Threat Defense デバイス が、フラッシュ メモリ内のコンフィギュレーションを消去しようとしたときに非ゼロ値（内部エラー）を受信しました。このメッセージには、報告サブルーチンのファイル名および行番号が含まれています。

推奨アクション パフォーマンス上の理由から、エンド ホストは IP フラグメントを投入しないように設定する必要があります。このコンフィギュレーションの変更は、NFS が原因と考えられます。読み取りサイズおよび書き込みサイズを NFS のインターフェイス MTU と等しく設定します。

209003

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

説明現在リアセンブリを待っている IP フラグメントが多すぎます。デフォルトでは、フラグメントの最大数は200です（最大値を大きくするには、コマンドリファレンスガイドの**fragment size** コマンドを参照してください）。Secure Firewall Threat Defense デバイスは、同時にリアセンブリできる IP フラグメントの数を制限します。この制約により、異常なネットワーク条件下でSecure Firewall Threat Defense デバイスのメモリが枯渇するのが防止されます。一般に、フラグメント化されたトラフィックは、混合トラフィック全体のわずかな割合に抑える必要があります。例外は、ほとんどがフラグメント化されたトラフィックである NFS over UDP のネットワーク環境の場合です。Secure Firewall Threat Defense デバイスこのタイプのトラフィックが経由で中継される場合、その代わりに NFS over TCP の使用を検討します。フラグメント化を防ぐには、コマンドリファレンス ガイドの **sysopt connection tcpmss bytes** コマンドを参照してください。

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

209004

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

説明 IP フラグメントの形式が誤っています。リアセンブリ済み IP パケットの合計サイズが、最大可能サイズの 65,535 バイトを超えています。

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

209005

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

説明 Secure Firewall Threat Defense デバイス は、24 よりも多くのフラグメントにフラグメント化されている IP パケットを拒否します。詳細については、コマンド リファレンス ガイドの **fragment** コマンドを参照してください。

推奨アクション侵入イベントが進行している可能性があります。このメッセージが引き続き表示される場合は、リモート ピアの管理者またはアップストリームのプロバイダーにお問い合わせください。**fragment chain xxx interface_name** コマンドを使用して、パケットあたりのフラグメントの数を変更できます。

209006

エラーメッセージ `%Threat Defense-4-209006: Fragment queue threshold exceeded, dropped` *`protocol`* `fragment from IP address/port to IP address/port on outside interface.`

説明 Secure Firewall Threat Defense デバイス は、フラグメントデータベースのしきい値（インターフェイスあたりのキューサイズの 2/3）を超過すると、フラグメントパケットをドロップします。

推奨アクション 不要。

210001

エラーメッセージ `%Threat Defense-3-210001: LU` *`sw_module_name`* `error =` *`number`*

説明ステートフル フェールオーバー エラーが発生しました。

推奨アクション Secure Firewall Threat Defense デバイス 経由のトラフィックが減少した後もこのエラーが引き続き表示される場合は、Cisco TAC にこのエラーを報告してください。

210002

エラーメッセージ `%Threat Defense-3-210002: LU allocate block (`*`bytes`*` ) failed.`

説明ステートフル フェールオーバーが、ステートフル情報をスタンバイ Secure Firewall Threat Defense デバイス に送信するためのメモリのブロックを割り当てることができません。

推奨アクション show interface コマンドを使用してフェールオーバー インターフェイスを調べて、その送信が正常であることを確認します。さらに、**show block** コマンドを使用して、現在のブロック メモリを調べます。現在使用可能なカウントが 0 になっているメモリのブロックが

あれば、Secure Firewall Threat Defense ソフトウェアをリロードして失われたメモリのブロックを回復します。

210003

エラーメッセージ `%Threat Defense-3-210003: Unknown LU Object number`

説明ステートフル フェールオーバーが、サポートされていない Logical Update オブジェクトを受信し、そのオブジェクトを処理できませんでした。これは、破損したメモリ、LAN 伝送、または他のイベントが原因となっている可能性があります。

推奨アクションこのエラーがまれにしか表示されない場合、処置は不要です。このエラーが頻繁に発生する場合は、ステートフル フェールオーバー リンク LAN 接続を確認します。エラーが不適切なフェールオーバー リンク LAN 接続のためでない場合は、外部ユーザーが保護されているネットワークを危険にさらそうとしていないかどうかを判別します。また、誤って設定したクライアントがないかどうかも確認します。

210005

エラーメッセージ `%Threat Defense-3-210005: LU allocate secondary (optional ) connection failed for protocol [TCP |UDP ] connection from ingress interface name :Real IP Address /Real Port to egress interface name :Real IP Address /Real Port`

説明ステートフル フェールオーバーが新しい接続をスタンバイ装置に割り当てることができません。これは、Secure Firewall Threat Defense デバイス内の利用可能な RAM メモリがほとんどないか、またはまったくないことが原因となっている可能性があります。

（注） Syslog メッセージの *secondary* フィールドはオプションであり、接続がセカンダリ接続である場合にのみ表示されます。

推奨アクション **show memory** コマンドを使用して Secure Firewall Threat Defense デバイス の空きメモリをチェックし、利用可能なメモリを確認します。利用可能なメモリがない場合は、さらに物理メモリをSecure Firewall Threat Defense デバイスに追加します。

210006

エラーメッセージ `%Threat Defense-3-210006: LU look NAT for IP_address failed`

説明ステートフル フェールオーバーが、スタンバイ装置上で IP アドレス用の NAT グループを検出できませんでした。アクティブおよびスタンバイの Secure Firewall Threat Defense デバイスが相互に同期していない可能性があります。

推奨アクションアクティブ装置で **write standby** コマンドを使用し、システム メモリをスタンバイ装置と同期させます。

210007

エラーメッセージ `%Threat Defense-3-210007: LU allocate xlate failed for type [static | dynamic]-[NAT | PAT] secondary(optional) protocol translation from ingress interface name :Real IP Address /real port (Mapped IP Address /Mapped Port) to egress interface name :Real IP Address /Real Port (Mapped IP Address /Mapped Port)`

説明ステートフル フェールオーバーが変換スロット レコードの割り当てに失敗しました。

推奨アクション show memory コマンドを使用して Secure Firewall Threat Defense デバイス の空きメモリをチェックし、利用可能なメモリを確認します。利用可能なメモリがない場合は、さらに物理メモリを追加します。

210008

エラーメッセージ `%Threat Defense-3-210008: LU no xlate for inside_address /inside_port outside_address /outside_port`

説明 Secure Firewall Threat Defense デバイス でステートフル フェールオーバー接続の変換スロットレコードを検出できません。そのため、Secure Firewall Threat Defense デバイス で接続情報を処理できません。

推奨アクション アクティブなユニットで **write standby** コマンドを使用し、システム メモリをアクティブ ユニットとスタンバイ ユニットの間で同期させます。

210010

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

説明ステートフル フェールオーバーが、UDP 接続に新しいレコードを割り当てることができませんでした。

推奨アクション show memory コマンドを使用して Secure Firewall Threat Defense デバイス の空きメモリをチェックし、利用可能なメモリを確認します。利用可能なメモリがない場合は、さらに物理メモリを追加します。

210020

エラーメッセージ `%Threat Defense-3-210020: LU PAT port port reserve failed`

説明ステートフル フェールオーバーが、使用中の特定の PAT アドレスを割り当てることができません。

推奨アクション アクティブなユニットで **write standby** コマンドを使用し、システム メモリをアクティブ ユニットとスタンバイ ユニットの間で同期させます。

210021

エラーメッセージ `%Threat Defense-3-210021: LU create static xlate global_address ifc interface_name failed`

説明ステートフル フェールオーバーが変換スロットを作成できません。

推奨アクション アクティブ装置で **write standby** コマンドを入力し、システム メモリをアクティブ装置とスタンバイ装置の間で同期させます。

210022

エラーメッセージ `%Threat Defense-6-210022: LU missed number updates`

説明ステートフルフェールオーバーは、スタンバイ装置に送信された各レコードにシーケンス番号を割り当てます。受信したレコードのシーケンス番号が最後にアップデートされたレコードと一致していない場合、その間の情報が失われたものと見なされ、その結果、このエラーメッセージが送信されます。

推奨アクション LAN の中断が発生しない場合、両方の Secure Firewall Threat Defense 装置の利用可能なメモリをチェックして、ステートフル情報を処理するのに十分なメモリがあることを確認します。**show failover** コマンドを使用して、ステートフル情報のアップデートの品質をモニターします。

メッセージ 211001 ～ 219002

この章では、211001 ～ 219002 のメッセージについて説明します。

211001

エラーメッセージ `%Threat Defense-3-211001: Memory allocation Error`

説明 Secure Firewall Threat Defense デバイス は RAM システム メモリの割り当てに失敗しました。

推奨アクションこのメッセージが定期的に表示される場合は、無視できます。頻繁に繰り返される場合は、Cisco TAC にお問い合わせください。

211003

エラーメッセージ `%Threat Defense-3-211003: Error in computed percentage CPU usage value`

説明 CPU 使用率が 100 %を超えています。

推奨アクションこのメッセージが定期的に表示される場合は、無視できます。頻繁に繰り返される場合は、Cisco TAC にお問い合わせください。

211004

エラーメッセージ `%Threat Defense-1-211004: WARNING: Minimum Memory Requirement for ASA version ver not met for ASA image. min MB required, actual MB found.`

説明 Secure Firewall Threat Defense デバイス がこのバージョンの最小メモリ要件を満たしていません。

- **ver**：実行イメージのバージョン番号
- **min**：インストールされたイメージを実行するために必要な RAM の最小容量
- **actual**：現在システムに搭載されているメモリの量

推奨アクション 必要な量の RAM を搭載します。

212001

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

説明 Secure Firewall Threat Defense デバイス は、このインターフェイス上にある SNMP 管理ステーションから Secure Firewall Threat Defense デバイス 宛ての SNMP 要求を受信できません。任意のインターフェイス上で Secure Firewall Threat Defense デバイス を通過する SNMP トラフィックは影響を受けません。エラー コードは次のとおりです。

- エラー コード -1 は、Secure Firewall Threat Defense デバイス がそのインターフェイスに対して SNMP トランスポートを開けないことを示します。このエラーは、SNMP がクエリーを受け入れるポートを別の機能ですでに使われているポートに変更しようとした場合に発生する可能性があります。この場合、SNMP が使用するポートは、着信 SNMP クエリー用のデフォルト ポート（UDP 161）にリセットされます。
- エラー コード -2 は、Secure Firewall Threat Defense デバイス がそのインターフェイスに対して SNMP トランスポートをバインドできないことを示します。

推奨アクション トラフィック量が少ないときに Secure Firewall Threat Defense デバイス リソースの一部を再要求してから、対象となるインターフェイスに対して snmp-server host コマンドを再入力します。

212002

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

説明 Secure Firewall Threat Defense デバイス は、Secure Firewall Threat Defense デバイス からこのインターフェイス上にある SNMP 管理ステーションに自分の SNMP トラップを送信できません。任意のインターフェイス上で Secure Firewall Threat Defense デバイス を通過する SNMP トラフィックは影響を受けません。エラー コードは次のとおりです。

- エラー コード -1 は、Secure Firewall Threat Defense デバイス がそのインターフェイスに対して SNMP トラップ トランスポートを開けないことを示します。

- エラー コード -2 は、Secure Firewall Threat Defense デバイス がそのインターフェイスに対して SNMP トラップ トランスポートをバインドできないことを示します。
- エラー コード -3 は、Secure Firewall Threat Defense デバイス がトラップ チャネルを書き込み専用として設定できないことを示します。

推奨アクション トラフィック量が少ないときに Secure Firewall Threat Defense デバイス リソースの一部を再要求してから、対象となるインターフェイスに対して snmp-server host コマンドを再入力します。

212003

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

説明指定されたインターフェイス上で Secure Firewall Threat Defense デバイス 宛ての SNMP 要求を受信する際に内部エラーが発生しました。エラー コードは次のとおりです。

- エラー コード -1 は、Secure Firewall Threat Defense デバイス がインターフェイスに対してサポートされているトランスポート タイプを検出できないことを示します。
- エラー コード -5 は、Secure Firewall Threat Defense デバイスがインターフェイスの UDP チャネルからデータを受信しなかったことを示します。
- エラー コード -7 は、Secure Firewall Threat Defense デバイスがサポートされているバッファ サイズを超える着信要求を受信したことを示します。
- エラー コード -14 は、Secure Firewall Threat Defense デバイス が UDP チャネルからの送信元 IP アドレスを判別できないことを示します。
- エラー コード -22 は、Secure Firewall Threat Defense デバイスが無効なパラメータを受信したことを示します。

推奨アクション 不要。Secure Firewall Threat Defense SNMP エージェントは元に戻って次の SNMP 要求を待ちます。

212004

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

説明指定されたインターフェイス上の指定されたホストに Secure Firewall Threat Defense デバイス から SNMP 応答を送信する際に内部エラーが発生しました。エラー コードは次のとおりです。

- エラー コード -1 は、Secure Firewall Threat Defense デバイス がインターフェイスに対してサポートされているトランスポート タイプを検出できないことを示します。
- エラー コード -2 は、Secure Firewall Threat Defense デバイスが無効なパラメータを送信したことを示します。
- エラー コード -3 は、Secure Firewall Threat Defense デバイスが UDP チャネルに宛先 IP アドレスを設定できなかったことを示します。

- エラー コード -4 は、Secure Firewall Threat Defense デバイスがサポートされている UDP セグメント サイズを超える PDU 長を送信したことを示します。
- エラー コード -5 は、Secure Firewall Threat Defense デバイスが PDU 構築用のシステム ブロックを割り当てることができなかったことを示します。

推奨アクション 不要。

212005

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

説明 Secure Firewall Threat Defense デバイス 宛ての着信 SNMP 要求の長さが、内部処理中に要求を格納するために使用される内部データ バッファのサイズ（512 バイト）を超えています。Secure Firewall Threat Defense デバイスはこの要求を処理できません。任意のインターフェイス上で Secure Firewall Threat Defense デバイス を通過する SNMP トラフィックは影響を受けません。

推奨アクション SNMP 管理ステーションに長さの短い要求を再送信させます。たとえば、1 つの要求で複数の MIB 変数にクエリーを実行するのではなく、1 つの要求で 1 つの MIB 変数だけにクエリーを実行するようにします。SNMP マネージャ ソフトウェアのコンフィギュレーションの修正が必要になる可能性もあります。

212006

エラーメッセージ `%Threat Defense-3-212006: Dropping SNMP request from src_addr /src_port to ifc :dst_addr /dst_port because: reason username`

説明 Secure Firewall Threat Defense デバイス が次の理由により自分宛ての SNMP 要求を処理できません。

- user not found：ユーザー名がローカル SNMP ユーザー データベース内に見つかりません。
- username exceeds maximum length：PDU に埋め込まれているユーザー名が SNMP RFC で許可されている最大長を超えています。
- authentication algorithm failure：無効なパスワードにより認証が失敗したか、またはパケットが不適切なアルゴリズムで認証されました。
- privacy algorithm failure：無効なパスワードによりプライバシー障害が発生したか、またはパケットが不適切なアルゴリズムで暗号化されました。
- error decrypting request：ユーザー要求を復号化するプラットフォーム暗号モジュールでエラーが発生しました。
- error encrypting response：ユーザー応答またはトラップ通知を暗号化するプラットフォーム暗号モジュールでエラーが発生しました。
- engineBoots has reached maximum value：engineBoots 変数が最大許容値に達しました。詳細については、メッセージ 212011 を参照してください。

（注） 上記の各理由の後にユーザー名が表示されます。

推奨アクション Secure Firewall Threat Defense SNMP サーバー設定をチェックし、NMS コンフィギュレーションで想定どおりのユーザー、認証、および暗号化設定が使用されていることを確認します。プラットフォーム暗号モジュールのエラーを分離するには、**show crypto accelerator statistics** コマンドを入力します。

212009

エラーメッセージ `%Threat Defense-5-212009: Configuration request for SNMP group groupname failed. User username , reason .`

説明 ユーザーが SNMP サーバーのグループ コンフィギュレーションを変更しようとしました。グループを参照する 1 人または複数のユーザーの設定が不十分であるため、要求されたグループの変更に応じることができません。

- **groupname**：グループ名を表す文字列
- *username*：ユーザー名を表す文字列
- **reason**：次のいずれかの原因を表す文字列

- *missing auth-password*：ユーザーがグループに認証を追加しようとしましたが、その際、認証パスワードを指定しませんでした。

- *missing priv-password*：ユーザーがグループにプライバシーを追加しようとしましたが、その際、暗号化パスワードを指定しませんでした。

- *reference group intended for removal*：ユーザーが、所属ユーザーが存在するグループを削除しようとしました。

推奨アクション ユーザーは、グループを変更したり、指摘されたユーザーを削除したりする前に、指摘されたユーザーのコンフィギュレーションをアップデートする必要があります。その後で、グループを変更し、ユーザーを追加し直します。

212010

エラーメッセージ `%Threat Defense-3-212010: Configuration request for SNMP user %s failed. Host %s reason .`

説明 ユーザーが SNMP サーバーのユーザー コンフィギュレーションを変更しようとしました。つまり、対象のユーザーを参照する 1 つまたは複数のホストを削除しようとしました。ホストごとに 1 つのメッセージが生成されます。

- **%s**：ユーザー名またはホスト名を表す文字列
- *reason*：次の原因を表す文字列

- *references user intended for removal*：ユーザー名がホストから削除されようとしました。

推奨アクション ユーザーは、ユーザーを変更したり、指摘されたホストを削除したりする前に、指摘されたホストのコンフィギュレーションをアップデートする必要があります。その後で、ユーザーを変更し、ホストを追加し直します。

212011

エラーメッセージ `%Threat Defense-3-212011: SNMP engineBoots is set to maximum value.`*`Reason`*`: %s User intervention necessary.`

次に例を示します。

```
%Threat Defense-3-212011: SNMP engineBoots is set to maximum value. Reason: error accessing
 persistent data. User intervention necessary.
```

説明 デバイスが 214783647 回（engineBoots 変数の最大許容値）リブートされたか、またはフラッシュ メモリから固定値を読み取り中にエラーが発生しました。engineBoots 値は、フラッシュ メモリ内の flash:/snmp/*ctx-name* ファイルに格納されます。ここで、*ctx-name* はコンテキストの名前です。シングル モードの場合、このファイルの名前は flash:/snmp/single_vf です。マルチモードの場合、管理コンテキスト用のファイルの名前は flash:/snmp/admin です。リブート時にデバイスでファイルの読み書きができない場合、engineBoots 値は最大値に設定されます。

- **%s**：engineBoots 値が最大許容値に設定されている原因を表す文字列。有効な文字列は「device reboots」および「error accessing persistent data」の 2 つです。

推奨アクション 1 つ目の文字列の場合、管理者は、すべての SNMP バージョン 3 ユーザーを削除してから追加し直すことで、engineBoots 変数を 1 にリセットする必要があります。それ以降のすべてのバージョン 3 クエリーは、すべてのユーザーが削除されるまで失敗します。2 つ目の文字列の場合、管理者は、コンテキスト固有のファイルを削除し、すべての SNMP バージョン ユーザーを削除してから追加し直すことで、engineBoots 変数を 1 にリセットする必要があります。それ以降のすべてのバージョン3 クエリーは、すべてのユーザーが削除されるまで失敗します。

212012

エラーメッセージ `%Threat Defense-3-212012: Unable to write SNMP engine data to persistent storage.`

説明 SNMP エンジン データはファイル flash:/snmp/*context-name* に書き込まれます。たとえば、シングルモードでは、データは flash:/snmp/single_vf ファイルに書き込まれます。マルチモードの管理コンテキストでは、ファイルはディレクトリ flash:/snmp/admin に書き込まれます。flash:/snmp ディレクトリの作成または flash:/snmp/*context-name* ファイルの作成に失敗すると、エラーが発生する可能性があります。また、ファイルへの書き込みに失敗した場合も、エラーが発生する可能性があります。

推奨アクション システム管理者は、flash:/snmp/*context-name* ファイルを削除し、すべての SNMP バージョン 3 ユーザーを削除してから追加し直す必要があります。この手順により、flash:/snmp/*context-name* ファイルが再作成されるはずです。問題が解決しない場合、システム管理者はフラッシュの再フォーマットを試みる必要があります。

214001

エラーメッセージ `%Threat Defense-2-214001: Terminating manager session from IP_address on interface interface_name . Reason: incoming encrypted data (number bytes) longer than number bytes`

説明 Secure Firewall Threat Defense 管理ポート宛ての着信暗号化データ パケットは、指定された上限をパケット長が超えていることを示します。これは敵対イベントの場合があります。Secure Firewall Threat Defense デバイスは、ただちにこの管理接続を終了します。

推奨アクション 管理接続が Cisco Secure Policy Manager によって開始されたことを確認します。

215001

エラーメッセージ `%Threat Defense-2-215001:Bad route_compress() call, sdb = number`

説明内部ソフトウェア エラーが発生しました。

推奨アクション Cisco TAC にお問い合わせください。

216001

エラーメッセージ `%Threat Defense-n-216001: internal error in: function : message`

説明正常動作中に発生してはならないさまざまな内部エラーが発生しました。重大度は、メッセージの原因によって異なります。

- **n**：メッセージの重大度
- **function**：影響を受けたコンポーネント
- **message**：問題の原因を説明するメッセージ

推奨アクション Bug Toolkit で特定のテキスト メッセージを検索します。また、アウトプット インタープリタを使用して問題の解決を試みます。問題が解決しない場合、Cisco TAC にお問い合わせください。

216002

エラーメッセージ `%Threat Defense-3-216002: Unexpected event (major: major_id , minor: minor_id ) received by task_string in function at line: line_num`

説明タスクがイベント通知に登録したが、そのタスクが特定のイベントを処理できません。監視できるイベントには、キュー、ブーリアン、タイマー サービスに関連付けられているイベントが含まれます。登録されているイベントのいずれかが発生した場合、スケジューラはタスクを再起動してイベントを処理します。このメッセージは、予期しないイベントがタスクを再起動したが、タスクがそのイベントの処理方法を認識していない場合に生成されます。

イベントが未処理のままになっている場合、そのイベントが頻繁にタスクを再起動して処理されていることを確認しますが、これは正常状態では発生してはならないことです。このメッセージが表示される場合、必ずしもデバイスが使用できないという意味ではなく、問題が発生し、調査する必要があることを意味しています。

- *major_id*：イベント識別子
- *minor_id*：イベント識別子
- *task_string*：タスクが自分自身を認識するために通過させたカスタム文字列
- *function*：予期しないイベントを受信した機能
- *line_num*：コード中の行番号

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。

216003

エラーメッセージ `%Threat Defense-3-216003: Unrecognized timer timer_ptr , timer_id received by task_string in function at line: line_num`

説明予期しないタイマーイベントがタスクを再起動したが、タスクがそのイベントの処理方法を認識していません。タスクは、一連のタイマーサービスをスケジューラに登録できます。タイマーのいずれかが期限満了になった場合、スケジューラはタスクを再起動してアクションを実行します。このメッセージは、認識できないタイマーイベントによってタスクが再起動された場合に生成されます。

期限満了になったタイマーは、タスクが未処理のままになっている場合、途切れることなくタスクを再起動して処理されていることを確認しますが、これは望ましいことではありません。これは正常状態では発生してはならないことです。このメッセージが表示される場合、必ずしもデバイスが使用できないという意味ではなく、問題が発生し、調査する必要があることを意味しています。

- *timer_ptr*：タイマーへのポインタ
- *timer_id*：タイマー識別子
- *task_string*：タスクが自分自身を認識するために通過させたカスタム文字列
- *function*：予期しないイベントを受信した機能
- *line_num*：コード中の行番号

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。

216004

エラーメッセージ `%Threat Defense-4-216004:prevented: error in function at file (line ) - stack trace`

説明内部ロジック エラーが発生しました。このエラーは、正常動作中に発生してはならないものです。

- *error*：内部ロジック エラー。考えられるエラーは、次のとおりです。

- 例外

- ヌル ポインタの逆参照

- 範囲外の配列インデックス

- 無効なバッファ サイズ

- 入力からの書き込み

- 送信元と宛先の重複

- 無効な日付

- 配列インデックスからのアクセス オフセット

  - *function*：エラーを生成した呼び出し機能
  - *file(line)*：エラーを生成したファイルと行番号
  - *stack trace*：完全なコール スタック トレースバック。呼び出し機能から開始します。たとえば、("0x001010a4 0x00304e58 0x00670060 0x00130b04") です。

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

217001

エラーメッセージ `%Threat Defense-2-217001: No memory for string in string`

説明メモリ不足が原因で動作が失敗しました。

推奨アクション 十分なメモリが存在する場合は、エラー メッセージ、コンフィギュレーション、およびこのエラーの発端になったイベントの詳細を、Cisco TAC に送付してください。

218001

エラーメッセージ `%Threat Defense-2-218001: Failed Identification Test in slot# [fail #/res ].`

説明 Secure Firewall Threat Defense デバイス の **slot#** のモジュールが、シスコ純正製品として識別できません。シスコの保証およびサポートプログラムは、シスコ純正製品だけに適用されます。シスコは、サポート問題の原因がシスコ製以外のメモリ、SSMモジュール、SSCモジュールなどのモジュールに関連していると判断した場合、現在の保証またはシスコ サポート プログラム（SmartNet など）の下でのサポートを拒否することがあります。

推奨アクションこのメッセージが繰り返し表示される場合は、コンソールまたはシステム ログに表示されたとおりに、メッセージをコピーします。アウトプットインタープリタを使用してエラーの詳細を調べて解決してください。Bug Toolkitでの検索も行います。問題が解決しない場合、Cisco TAC にお問い合わせください。

218002

エラーメッセージ `%Threat Defense-2-218002: Module (slot# ) is a registered proto-type for Cisco Lab use only, and not certified for live network operation.`

説明指摘された場所のハードウェアが、シスコのラボで製造されたプロトタイプモジュールです。

推奨アクション このメッセージが繰り返し表示される場合は、コンソールまたはシステム ログに表示されているとおりにメッセージをコピーします。アウトプットインタープリタを使用

してエラーの詳細を調べて解決してください。Bug Toolkit での検索も行います。問題が解決しない場合、Cisco TAC にお問い合わせください。

218003

エラーメッセージ `%Threat Defense-2-218003: Module Version in slot# is obsolete. The module in slot = slot# is obsolete and must be returned via RMA to Cisco Manufacturing. If it is a lab unit, it must be returned to Proto Services for upgrade.`

説明 古いハードウェアが検出されたか、**show module** コマンドがモジュールに対して実行されました。このメッセージは、最初に表示された後 1 分ごとに生成されます。

推奨アクションこのメッセージが繰り返し表示される場合は、コンソールまたはシステム ログに表示されたとおりに、メッセージをコピーします。アウトプット インタープリタを使用してエラーの詳細を調べて解決してください。Bug Toolkit での検索も行います。問題が解決しない場合、Cisco TAC にお問い合わせください。

218004

エラーメッセージ `%Threat Defense-2-218004: Failed Identification Test in slot# [fail# /res ]`

説明指定された場所のハードウェアを特定する際に問題が発生しました。

推奨アクションこのメッセージが繰り返し表示される場合は、コンソールまたはシステム ログに表示されたとおりに、メッセージをコピーします。アウトプット インタープリタを使用してエラーの詳細を調べて解決してください。Bug Toolkit での検索も行います。問題が解決しない場合、Cisco TAC にお問い合わせください。

218005

エラーメッセージ `%Threat Defense-2-218005: Inconsistency detected in the system information programmed in non-volatile memory`

説明不揮発性メモリにプログラムされたシステム情報が一貫していません。この Syslog は、Secure Firewall Threat Defense デバイス が IDPROM の内容と ACT2 EEPROM の内容が異なることを検出すると、ブートアップ時に生成されます。IDPROM と ACT2 EEPROM は製造時にまったく同じ内容でプログラムされているため、これは製造時のエラーまたは IDPROM の内容が不正に変更されたことが原因となって生じます。

推奨アクション メッセージが再発する場合は、show tech-support コマンドの出力を収集し、Cisco TAC に連絡します。

219002

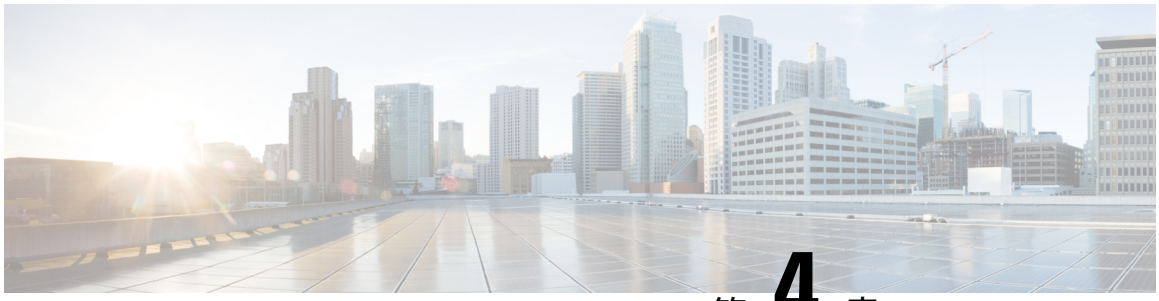
エラーメッセージ `%Threat Defense-3-219002: I2C_API_name error, slot = slot_number , device = device_number , address = address , byte count = count . Reason: reason_string`

説明 ハードウェアまたはソフトウェアの問題が原因で I2C シリアル バス API が失敗しました。

- *I2C_API_name*：失敗した I2C API。次のいずれかです。
  - I2C_read_byte_w_wait()
  - I2C_read_word_w_wait()
  - I2C_read_block_w_wait()
  - I2C_write_byte_w_wait()
  - I2C_write_word_w_wait()
  - I2C_write_block_w_wait()
  - I2C_read_byte_w_suspend()
  - I2C_read_word_w_suspend()
  - I2C_read_block_w_suspend()
  - I2C_write_byte_w_suspend()
  - I2C_write_word_w_suspend()
  - I2C_write_block_w_suspend()
- *slot_number*：このメッセージを生成した I/O 動作が行われたスロットの番号（16 進数）。スロット番号は、シャーシ内のスロットとして一意でないことがあります。シャーシによっては、2 つの異なるスロットが同じ I2C スロット番号を持つことがあります。また、値は必ずしもスロット数以下ではありません。値は、I2C ハードウェアがどのように配線されているかによって異なります。
- *device_number*：I/O 動作が行われたスロット上のデバイスの番号（16 進数）。
- *address*：I/O 動作が行われたデバイスのアドレス（16 進数）。
- *byte_count*：I/O 動作のバイト数（10 進数形式）。
- *error_string*：エラーの原因。次のいずれかです。
  - I2C_BUS_TRANSACTION_ERROR
  - I2C_CHKSUM_ERROR
  - I2C_TIMEOUT_ERROR
  - I2C_BUS_COLLISION_ERROR
  - I2C_HOST_BUSY_ERROR
  - I2C_UNPOPULATED_ERROR
  - I2C_SMBUS_UNSUPPORT
  - I2C_BYTE_COUNT_ERROR
  - I2C_DATA_PTR_ERROR

推奨アクション次の手順を実行します。

1. イベントに関連付けられているメッセージとエラーを記録して確認します。このメッセージが継続的に表示されず、数分後に表示されなくなる場合は、I2C シリアル バスのビジー状態が原因である可能性があります。
2. Secure Firewall Threat Defense デバイスで実行しているソフトウェアをリブートします。
3. デバイスの電源を一度切ってから再投入します。電源を切った後、必ず数秒待ってから電源を入れます。
4. 問題が解決しない場合、Cisco TAC にお問い合わせください。



第 4 章

Syslog メッセージ 302003 ～ 341011

この章は、次の項で構成されています。

メッセージ 302003 ～ 319004

この章には、メッセージ 302003 ～ 319004 を示します。

302003

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

説明 H.245 接続が **outside_address** から **inside_address** に向けて開始されました。Secure Firewall Threat Defense デバイス は、Intel Internet Phone の使用を検出しました。外部ポート（*outside_port*）は、Secure Firewall Threat Defense デバイス 外部からの接続にしか表示されません。ローカル ポート値（*inside_port*）は、内部インターフェイスで開始された接続にしか表示されません。

推奨アクション 不要。

302004

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

説明 H.323 UDP バック接続がローカル アドレス（**inside_address**）から外部アドレス（**outside_address**）に事前割り当てされました。Secure Firewall Threat Defense デバイス は、Intel Internet Phone の使用を検出しました。外部ポート（**outside_port**）は、Secure Firewall Threat Defense デバイス外部からの接続にしか表示されません。ローカル ポート値（**inside_port**）は、内部インターフェイスで開始された接続にしか表示されません。

推奨アクション 不要。

302010

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

説明使用中の接続数と最も使用されている接続数に関する情報を提供します。

- **connections**：接続数

推奨アクション 不要。

302012

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

説明 H.225 二次チャネルは事前割り当て済みです。

推奨アクション 不要。

302013

エラーメッセージ`%FTD-6-302013: Built {inbound|outbound} [Probe] TCP connection_id for interface :real-address /real-port (mapped-address/mapped-port ) [(idfw_user )] to interface :real-address /real-port (mapped-address/mapped-port ) [(idfw_user )] [(user )]`

説明 2 つのホスト間に TCP 接続スロットが作成されました。

- **probe**：TCP 接続がプローブ接続であることを示します
- **connection_id**：一意の識別子
- **interface**、**real-address**、**real-port**：実際のソケット
- **mapped-address**、**mapped-port**：マッピングされたソケット
- **user**：ユーザーの AAA の名前
- **idfw_user**：アイデンティティ ファイアウォールのユーザー名

inbound が表示されている場合、元の制御接続は外部から開始されています。たとえば、FTP の場合、元の制御チャネルが着信であれば、すべてのデータ転送チャネルは着信です。outbound が表示されている場合、元の制御接続は内部から開始されています。

推奨アクション 不要。

302014

エラーメッセージ `%FTD-6-302014: Teardown [Probe] TCP connection id for interface :real-address /real-port [(idfw_user )] to interface :real-address /real-port [(idfw_user )] duration hh:mm:ss bytes bytes [reason [from teardown-initiator]] [(user )]`

説明 2 つのホスト間の TCP 接続が削除されました。メッセージの値は次のとおりです。

- **probe**：TCP 接続がプローブ接続であることを示します

- **id** ：一意の識別子
- **interface**、**real-address**、**real-port**：実際のソケット
- **duration**：接続のライフタイム
- **bytes**：接続中のデータ転送量
- **User**：ユーザーの AAA の名前
- **idfw_user**：アイデンティティ ファイアウォールのユーザーの名前
- **reason**：接続終了の原因となったアクション**reason** 変数には、次の表に示されている TCP 終了の原因の 1 つが設定されています。
- **teardown-initiator**：ティアダウンを開始した側のインターフェイス名。

表 *10 : TCP* 終了の原因

理由	説明
Conn-timeout	非アクティビティ タイマーの期限切れのため、フローが終了したときに接続が終了しました。
Deny Terminate	フローは、アプリケーション インスペクションによって終了されました。
Failover primary closed	アクティブ装置から受信したメッセージが原因で、フェールオーバー ペアのスタンバイ装置が接続を削除しました。
FIN Timeout	最終 ACK を 10 分間待機した後、またはハーフクローズ タイムアウト後の強制終了です。
Flow closed by inspection	フローは、検査機能によって終了されました。
Flow terminated by IPS	フローは、IPS によって終了されました。
Flow reset by IPS	フローは、IPS によってリセットされました。
Flow terminated by TCP Intercept	フローは、TCP 代行受信によって終了されました。
Flow timed out	フローがタイムアウトしました。
Flow timed out with reset	フローがタイムアウトしましたが、リセットされました。
Flow is a loopback	フローはループバックです。
Free the flow created as result of packet injection	Packet Tracer 機能によって Secure Firewall Threat Defense デバイスを介してシミュレートパケットが送信されたため、接続が確立されました。
Invalid SYN	SYN パケットが無効でした。

理由	説明
IPS fail-close	フローは、IPS カードのダウンのため終了されました。
ゾーンに関連付けられているインターフェイスがありません。	“no nameif” または “no zone-member” の実行後、ゾーンに関連付けられているインターフェイス メンバーがなくなったため、フローは切断されました。
No valid adjacency	Secure Firewall Threat Defense デバイスが隣接情報を取得しようとしましたが、ネクスト ホップの MAC アドレスを取得できなかった場合、このカウンタが増分します。パケットはドロップされます。
Pinhole Timeout	Secure Firewall Threat Defense デバイス がセカンダリ フローを開始しましたが、タイムアウト間隔内にこのフローにパケットが渡されなかったためにフローが削除されたことを報告するため、このカウンタが増分します。セカンダリ フローの例としては、FTP コントロール チャネル上でネゴシエーションの成功後に作成される FTP データ チャネルがあります。
再送信のプローブの最大再試行回数を超えました	TCP パケットが再送信の最大プローブ再試行回数を超えたため、接続が切断されました。
プローブの最大再送信時間経過	TCP パケットの最大プローブ時間が経過したため、接続が切断されました。
プローブによる RST の受信	プローブ接続がサーバーから RST を受信したため、接続が切断されました。
プローブによる FN の受信	プローブ接続はサーバーから FIN を受信し、完全な FIN 終了プロセスが完了したため、接続が切断されました。
プローブの完了	プローブ接続が成功しました。
Route change	Secure Firewall Threat Defense デバイス が低コスト（より良いメトリック）ルートを追加した場合、着信パケットが新しいルートに一致すると、ユーザー設定のタイムアウト値（floating-conn）後に既存の接続が切断されます。後続のパケットは、良好なメトリックを持つインターフェイスから接続を再構築します。コストが小さいルートの追加がアクティブ フローに影響を与えることを防ぐため、floating-conn 設定タイムアウト値を 0:0:0 に設定できます。
SYN Control	バック チャネル開始が誤った側から発生しました。
SYN Timeout	3 ウェイ ハンドシェイクの完了を 30 秒間待機した後の強制終了です。
TCP bad retransmission	不良 TCP 再送が原因で接続は終了しました。

理由	説明
TCP FINs	正常なクローズダウン シーケンスが発生しました。
TCP Invalid SYN	無効な TCP SYN パケットです。
TCP Reset - APPLIANCE	フローは、Secure Firewall Threat Defense デバイス によって TCP リセットが生成された場合に終了します。
TCP Reset - I	内部からリセットされました。
TCP Reset - O	外部からリセットされました。
TCP segment partial overlap	部分的に重複するセグメントが検出されました。
TCP unexpected window size variation	TCP ウィンドウ サイズに変動があるため接続は終了しました。
Tunnel has been torn down	トンネルがダウンしているため、フローは終了しました。
Unauth Deny	許可は、URL フィルタによって拒否されました。
不明（Unknown）	不明なエラーが発生しました。
Xlate Clear	コマンド ラインが削除されました。

推奨アクション 不要。

302015

エラーメッセージ `%FTD-6-302015: Built {inbound|outbound} UDP connection number for interface_name :real_address /real_port (mapped_address /mapped_port ) [(idfw_user )] to interface_name :real_address /real_port (mapped_address /mapped_port )[(idfw_user )] [(user )]`

説明 2 つのホスト間に UDP 接続スロットが作成されました。メッセージの値は次のとおりです。

- **number**：一意の識別子
- **interface、real_address、real_port**：実際のソケット
- **mapped_address、mapped_port**：マッピングされたソケット
- **user**：ユーザーの AAA の名前
- *idfw_user*：アイデンティティ ファイアウォールのユーザーの名前

inbound が表示されている場合、元の制御接続は外部から開始されています。たとえば、UDP の場合、元の制御チャネルが着信であれば、すべてのデータ転送チャネルは着信です。outbound が表示されている場合、元の制御接続は内部から開始されています。

推奨アクション 不要。

302016

エラーメッセージ `%FTD-6-302016: Teardown UDP connection number for interface :real-address /real-port [(idfw_user )] to interface :real-address /real-port [(idfw_user )] duration hh :mm :ss bytes bytes [(user )]`

説明 2 つのホスト間の UDP 接続スロットが削除されました。メッセージの値は次のとおりです。

- **number**：一意の識別子
- **interface、real_address、real_port**：実際のソケット
- **time**：接続のライフタイム
- **bytes**：接続中のデータ転送量
- **id**：一意の識別子
- **interface、real-address、real-port**：実際のソケット
- **duration**：接続のライフタイム
- **bytes**：接続中のデータ転送量
- **user**：ユーザーの AAA の名前
- *idfw_user*：アイデンティティ ファイアウォールのユーザーの名前

推奨アクション 不要。

302017

エラーメッセージ `%FTD-6-302017: Built {inbound|outbound} GRE connection id from interface :real_address (translated_address ) [(idfw_user )] to interface :real_address /real_cid (translated_address /translated_cid ) [(idfw_user )] [(user )`

説明 2 つのホスト間に GRE 接続スロットが作成されました。**id** は、一意の識別子です。**interface、real_address、real_cid** タプルは、2 つのシンプレックス PPTP GRE ストリームのうちの 1 つを示します。カッコ付きの **translated_address**、**translated_cid** タプルは、ネットワーク アドレス変換（NAT）で変換された値を示します。inbound が表示されている場合、接続は着信だけに使用できます。outboundが表示されている場合、接続は発信だけに使用できます。メッセージの値は次のとおりです。

- **id**：接続を識別するための一意の番号
- **inbound**：制御接続は着信 PPTP GRE フロー用
- **outbound**：制御接続は発信 PPTP GRE フロー用
- **interface_name**：インターフェイス名
- **real_address**：実際のホストの IP アドレス
- **real_cid**：接続の変換前のコール ID
- **translated_address**：変換後の IP アドレス
- **translated_cid**：変換後のコール
- **user**：AAA ユーザー名
- *idfw_user*：アイデンティティ ファイアウォールのユーザーの名前

推奨アクション 不要。

302018

エラーメッセージ `%FTD-6-302018: Teardown GRE connection id from interface :real_address (translated_address ) [(idfw_user )] to interface :real_address /real_cid (translated_address /translated_cid ) [(idfw_user )] duration hh :mm :ss bytes bytes [(user )]`

説明 2 つのホスト間の GRE 接続スロットが削除されました。**interface、real_address、real_port** タプルは、実際のソケットを示します。**Duration** は、接続のライフタイムを示します。メッセージの値は次のとおりです。

- **id**：接続を識別するための一意の番号
- **interface**：インターフェイス名
- **real_address**：実際のホストの IP アドレス
- **real_port**：実際のホストのポート番号
- **hh:mm:ss**：時:分:秒の形式の時間
- **bytes**：GRE セッションで転送された PPP バイトの数
- **reason**：接続が終了された原因
- **user**：AAA ユーザー名
- *idfw_user*：アイデンティティ ファイアウォールのユーザーの名前

推奨アクション 不要。

302019

エラーメッセージ `%FTD-3-302019: H.323 library_name ASN Library failed to initialize, error code number`

説明 指摘された ASN ライブラリ（Secure Firewall Threat Defense デバイス が H.323 メッセージのデコードに使用するライブラリ）の初期化に失敗しました。Secure Firewall Threat Defense デバイスは到着する H.323 パケットのデコードも検査もできません。Secure Firewall Threat Defense デバイスは、何も修正を加えずに H.323 パケットが通過できるようにします。次の H.323 メッセージが到着すると、Secure Firewall Threat Defense デバイスはライブラリを再度初期化しようとします。

推奨アクション このメッセージが特定のライブラリに対して始終生成される場合は、Cisco TAC にお問い合わせのうえ、すべてのログ メッセージ（タイムスタンプ付きが望ましい）を送付してください。

302020

エラーメッセージ `%FTD-6-302020: Built {in | out} bound ICMP connection for faddr {faddr | icmp_seq_num } [(idfw_user )] gaddr {gaddr | icmp_type } laddr laddr [(idfw_user )] type {type } code {code }`

説明 このメッセージは、高速パスで ICMP セッションが確立されたときに生成されます。メッセージの値は次のとおりです。

- *faddr*：外部ホストの IP アドレスを指定します
- *gaddr*：グローバル ホストの IP アドレスを指定します。
- *laddr*：ローカル ホストの IP アドレスを指定します
- *idfw_user*：アイデンティティ ファイアウォールのユーザーの名前
- *user*：接続が開始されたホストに関連付けられているユーザー名
- *type*：ICMP タイプを指定します。
- *code*：ICMP コードを指定します。

推奨アクション 不要。

302021

エラーメッセージ `%FTD-6-302021: Teardown ICMP connection for faddr {faddr | icmp_seq_num } [(idfw_user )] gaddr {gaddr | icmp_type } laddr laddr [(idfw_user )] type {type } code {code }`

説明 このメッセージは、高速パスでICMPセッションが削除されたときに生成されます。メッセージの値は次のとおりです。

- *faddr*：外部ホストの IP アドレスを指定します
- *gaddr*：グローバル ホストの IP アドレスを指定します。
- *laddr*：ローカル ホストの IP アドレスを指定します
- *idfw_user*：アイデンティティ ファイアウォールのユーザーの名前
- *user*：接続が開始されたホストに関連付けられているユーザー名
- *type*：ICMP タイプを指定します。
- *code*：ICMP コードを指定します。

推奨アクション 不要。

302022

エラーメッセージ `%FTD-6-302022: Built role stub TCP connection for interface :real-address /real-port (mapped-address /mapped-port ) to interface :real-address /real-port (mapped-address /mapped-port)`

説明 TCP ディレクタ/バックアップ/フォワーダ フローが作成されました。

推奨アクション 不要。

302023

エラーメッセージ `%FTD-6-302023: Teardown stub TCP connection for interface :real-address /real-port to interface :real-address /real-port duration hh:mm:ss forwarded bytes bytes reason`

説明 TCP ディレクタ/バックアップ/フォワーダ フローが切断されました。

推奨アクション 不要。

302024

エラーメッセージ `%FTD-6-302024: Built role stub UDP connection for interface :real-address /real-port (mapped-address /mapped-port ) to interface :real-address /real-port (mapped-address /mapped-port )`

説明 UDP ディレクタ/バックアップ/フォワーダ フローが作成されました。

推奨アクション 不要。

302025

エラーメッセージ `%FTD-6-302025: Teardown stub UDP connection for interface :real-address /real-port to interface :real-address /real-port duration hh:mm:ss forwarded bytes bytes reason`

説明 UDP ディレクタ/バックアップ/フォワーダ フローが切断されました。

推奨アクション 不要。

302026

エラーメッセージ `%FTD-6-302026: Built role stub ICMP connection for interface :real-address /real-port (mapped-address ) to interface :real-address /real-port (mapped-address )`

説明 ICMP ディレクタ/バックアップ/フォワーダ フローが作成されました。

推奨アクション 不要。

302027

エラーメッセージ `%FTD-6-302027: Teardown stub ICMP connection for interface :real-address /real-port to interface :real-address /real-port duration hh:mm:ss forwarded bytes bytes reason`

説明 ICMP ディレクタ/バックアップ/フォワーダ フローが切断されました。

推奨アクション 不要。

302033

エラーメッセージ `%FTD-6-302033:Pre-allocated H323 GUP Connection for faddr interface :foreign address /foreign-port to laddr interface :local-address /local-port`

説明GUP接続は外部アドレスからローカルアドレスに開始されました。外部ポートは、セキュリティ デバイスの外部からの接続にしか表示されません。ローカル ポート値（内部ポート）は、内部インターフェイスで開始された接続にしか表示されません。

- **interface**：インターフェイス名
- *foreign-address*：外部ホストの IP アドレス
- *foreign-port*：外部ホストのポート番号

- *local-address*：ローカル ホストの IP アドレス
- *local-port*：ローカル ホストのポート番号

推奨アクション 不要。

302034

エラーメッセージ `%FTD-4-302034: Unable to pre-allocate H323 GUP Connection for faddr interface :foreign address /foreign-port to laddr interface :local-address /local-port`

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

- **interface**：インターフェイス名
- *foreign-address*：外部ホストの IP アドレス
- *foreign-port*：外部ホストのポート番号
- *local-address*：ローカル ホストの IP アドレス
- *local-port*：ローカル ホストのポート番号

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

302302

エラーメッセージ `%FTD-3-302302: ACL = deny; no sa created`

説明 IPSec プロキシのミスマッチが発生しました。ネゴシエートした SA のプロキシ ホストは、deny access-list コマンド ポリシーに対応します。

推奨アクション コンフィギュレーションの access-list コマンド文を確認します。ピアの管理者にお問い合わせください。

302303

エラーメッセージ `%FTD-6-302303: Built TCP state-bypass connection conn_id from initiator_interface :real_ip /real_port (mapped_ip /mapped_port ) to responder_interface :real_ip /real_port (mapped_ip /mapped_port )`

説明新しい TCP 接続が作成されました。この接続は、TCP 状態バイパス接続です。このタイプの接続では、すべての TCP 状態チェックと追加のセキュリティ チェックおよび検査がバイパスされます。

推奨アクション標準的なすべての TCP 状態チェックと他のすべてのセキュリティ チェックおよび検査によって TCP トラフィックを保護する必要がある場合は、**no set connection advanced-options tcp-state-bypass** コマンドを使用して、TCP トラフィックに対してこの機能をディセーブルにできます。

302304

エラーメッセージ `%FTD-6-302304: Teardown TCP state-bypass connection conn_id from initiator_interface :ip/port to responder_interface :ip/port duration , bytes , teardown reason .`

説明新しい TCP 接続が切断されました。この接続は、TCP 状態バイパス接続です。このタイプの接続では、すべての TCP 状態チェックと追加のセキュリティ チェックおよび検査がバイパスされます。

- *duration*：TCP 接続の期間
- *bytes*：TCP 接続で転送された合計バイト数
- *teardown reason*：TCP 接続の切断原因

推奨アクション 標準的なすべての TCP 状態チェックと他のすべてのセキュリティ チェックおよびインスペクションによって TCP トラフィックを保護する必要がある場合は、**no set connection advanced-options tcp-state-bypass** コマンドを使用し、TCP トラフィックに対してこの機能を無効にすることができます。

302311

エラーメッセージ `%FTD-4-302311: Failed to create a new protocol connection from ingress interface:source IP/source port to egress interface:destination IP/destination port due to application cache memory allocation failure. The app-cache memory threshold level is threshold% and threshold check is enabled/disabled.`

説明アプリケーション キャッシュ メモリ割り当てに失敗したために、新しい接続を作成できませんでした。この障害は、システムのメモリ不足またはシステムがアプリケーション キャッシュ メモリしきい値を超えたことが原因である可能性があります。

- protocol：接続を作成するために使用されるプロトコルの名前
- ingress interface：インターフェイス名
- source IP：送信元 IP アドレス
- source port：送信元ポート番号
- egress interface：インターフェイス名
- destination IP：宛先アドレス
- destination port：宛先ポート番号
- threshold%：メモリしきい値のパーセンテージ値
- enabled/disabled：アプリケーション キャッシュ メモリしきい値機能の有効化/無効化

推奨アクションデバイスでメモリを大量に消費する機能を無効にするか、through-the-box 接続の数を減らします。

303002

エラーメッセージ `%FTD-6-303002: FTP connection from src_ifc :src_ip /src_port to dst_ifc :dst_ip /dst_port , user username action file filename`

説明 クライアントは、FTP サーバーとの間でファイルをアップロードまたはダウンロードしました。

- **src_ifc**：クライアントが存在するインターフェイス。
- **src_ip**：クライアントの IP アドレス。
- **src_port**：クライアント ポート。
- **dst_ifc**：サーバーが存在するインターフェイス。
- **dst_ip**：FTP サーバーの IP アドレス。
- **dst_port**：サーバー ポート。
- **username**：FTP ユーザー名。
- **action**：保存または取得されたアクション。
- **filename**：保存または取得したファイル。

推奨アクション 不要。

303004

エラーメッセージ `%FTD-5-303004: FTP cmd_string command unsupported - failed strict inspection, terminating connection from source_interface :source_address /source_port to dest_interface :dest_address/dest_interface`

説明 FTP トラフィックの厳密な FTP 検査が使用された、または FTP 要求メッセージに、デバイスに認識されないコマンドが含まれています。

推奨アクション 不要。

303005

エラーメッセージ `%FTD-5-303005: Strict FTP inspection matched match_string in policy-map policy-name , action_string from src_ifc :sip /sport to dest_ifc :dip /dport`

説明 FTP 検査で、設定済みの値（ファイル名、ファイル タイプ、要求コマンド、サーバー、ユーザー名）のいずれかと一致した場合、このメッセージの *action_string* で指定されたアクションが実行されます。

- *match_string*：ポリシー マップ内の match 節
- **policy-name**：一致したポリシー マップ
- **action_string**：実行するアクション（たとえば、Reset Connection）
- **src_ifc**：送信元インターフェイス名
- **sip**：送信元 IP アドレス
- **sport**：送信元ポート
- **dest_ifc**：宛先インターフェイス名

- **dip**：宛先 IP アドレス
- **dport**：宛先ポート

推奨アクション 不要。

305006

エラーメッセージ `%FTD-3-305006: {outbound static|identity|portmap|regular) translation creation failed for protocol src interface_name:source_address/source_port [(idfw_user )] dst interface_name:dest_address/dest_port [(idfw_user )]`

説明 ICMP エラーインスペクションが有効になり、次の条件が満たされました。

- プロトコルの異なる順方向フローと逆方向フローを使用したデバイスを介して確立された接続がありました。（順方向のフローが UDP または TCP で、逆方向のフローが ICMP である場合など）。プロトコルの切り替えは、受信者またはパス内の中間デバイスのいずれかが ICMP エラーメッセージ（タイプ 3 コード 3 など）を返したときに発生します。
- デバイスがすべての ICMP メッセージタイプに PAT を適用しないため、リバースフローのパケットに一致し、外部ヘッダーの IP アドレスの変換に失敗した動的 NAT/PAT ステートメントがありました。PAT ICMP エコーおよびエコー応答パケット（タイプ 8 および 0）のみを適用します。

推奨アクション 不要。

305009

エラーメッセージ `%FTD-6-305009: Built {dynamic|static} translation from interface_name [(acl-name)]:real_address [(idfw_user )] to interface_name :mapped_address`

説明アドレス変換スロットが作成されました。スロットは、送信元アドレスをローカル側からグローバル側に変換します。また、逆方向では、宛先アドレスをグローバル側からローカル側に変換します。

推奨アクション 不要。

305010

エラーメッセージ `%FTD-6-305010: Teardown {dynamic|static} translation from interface_name :real_address [(idfw_user )] to interface_name :mapped_address duration time`

説明アドレス変換スロットが削除されました。

推奨アクション 不要。

305011

エラーメッセージ %FTD-6-305011: Built {dynamic|static} {TCP|UDP|ICMP} translation from *interface_name* :*real_address*/*real_port* [(*idfw_user*)] to *interface_name* :*mapped_address*/*mapped_port*

説明 TCP、UDP、またはICMPアドレス変換スロットが作成されました。スロットは、ローカル側からグローバル側に送信元ソケットを変換します。逆に、スロットは、グローバル側からローカル側に宛先ソケットを変換します。

推奨アクション 不要。

305012

エラーメッセージ %FTD-6-305012: Teardown {dynamic|static} {TCP|UDP|ICMP} translation from *interface_name* [(*acl-name*)]:*real_address* /{*real_port* |*real_ICMP_ID* } [(*idfw_user*)] to *interface_name* :*mapped_address* /{*mapped_port* |*mapped_ICMP_ID* } duration *time*

説明 アドレス変換スロットが削除されました。

推奨アクション 不要。

305013

エラーメッセージ %FTD-5-305013: Asymmetric NAT rules matched for forward and reverse flows; Connection *protocol* src *interface_name* :*source_address* /*source_port* [(*idfw_user*)] dst *interface_name* :*dst_address* /*dst_port* [(*idfw_user*)] denied due to NAT reverse path failure.

説明 実際のアドレスを使用して、マップされたホストへの接続を試みましたが、拒否されました。

推奨アクション NAT を使用するホストと同じインターフェイス上にないホストに接続する場合は、実際のアドレスではなく、マップされたアドレスを使用します。また、アプリケーションに IP アドレスが埋め込まれている場合は、**inspect** コマンドをイネーブルにします。

305014

エラーメッセージ % FTD -6-305014: アロケート block of ports for translation from *real_interface* :*real_host_ip* /*real_source_port* to *real_dest_interface* :*real_dest_ip* /*real_dest_port*.

説明 CGNAT の「block-allocation」が設定されている場合、この syslog は新しいポート ブロックの割り当て時に生成されます。

推奨アクション なし。

305015

エラーメッセージ %Threat Defense-6-305015: Released block of ports for translation from *real_interface* :*real_host_ip* /*real_source_port* to *real_dest_interface* :*real_dest_ip* /*real_dest_port*.

説明 CGNAT の「block-allocation」が設定されている場合、この syslog は割り当てられたポートブロックのリリース時に生成されます。

推奨アクションなし。

305016

エラーメッセージ %FTD-3-305016: Unable to create *protocol* connection from *real_interface* :*real_host_ip* /*real_source_port* to *real_dest_interface* :*real_dest_ip* /*real_dest_port* due to *reason* .

説明ホストごとの最大ポート ブロックの制限数に達しているか、またはポート ブロックが枯渇しています。

- *reason*：以下のいずれかになります。
  - ホストあたりの PAT ポート ブロックの制限である *value* に達している
  - PAT プール内のポート ブロックを使い果たしている

推奨アクション ホストあたりの PAT ポート ブロックの制限に達している場合は、次のコマンドを入力し、ホストあたりの最大ブロックの制限を確認します。

```
xlate block-allocation maximum-per-host 4
```

PAT プール内のポート ブロックを使い果たしている場合は、ポート サイズを増やすことをお勧めします。また、次のコマンドを入力し、ブロック サイズを確認してください。

```
xlate block-allocation size 512
```

305017

エラーメッセージ %FTD-3-305017: Pba-interim-logging: Active ICMP block of ports for translation from *<source device IP>* to *<destination device IP>*/*<Active Port Block>*

説明 CGNAT 一時ロギング機能がオンになっている場合、この Syslog により、特定のソース IP アドレスからその時点の宛先 IP アドレスへのアクティブポートブロックが示されます。

推奨処置なし。

308001

エラーメッセージ %Threat Defense-6-308001: console enable password incorrect for *number* tries (from *IP_address*)

説明これは Secure Firewall Threat Defense 管理メッセージです。このメッセージは、特権モードに入るためにユーザーがパスワードを指摘された回数だけ誤って入力した後に表示されます。最大試行回数は 3 回です。

推奨アクション パスワードを確認し、再度試行します。

308002

エラーメッセージ `%Threat Defense-4-308002: static global_address inside_address netmask netmask overlapped with global_address inside_address`

説明 1 つまたは複数の static コマンド文の IP アドレスが重複しています。**global_address** は低セキュリティ レベルのインターフェイス上のアドレスであるグローバル アドレスであり、**inside_address** は高セキュリティ レベルのインターフェイス上のアドレスであるローカル アドレスです。

推奨アクション show static コマンドを使用してコンフィギュレーションの static コマンド文を表示し、重複しているコマンドを修正します。最も一般的な重複は、10.1.1.0 などのネットワーク アドレスを指定して、別の static コマンドで 10.1.1.5 などその範囲内にあるホストを指定する場合に発生します。

311001

エラーメッセージ `%Threat Defense-6-311001: LU loading standby start`

説明スタンバイ Secure Firewall Threat Defense デバイス が最初にオンラインになるときに、ステートフル フェールオーバー アップデート情報がスタンバイ Secure Firewall Threat Defense デバイス に送信されました。

推奨アクション 不要。

311002

エラーメッセージ `%Threat Defense-6-311002: LU loading standby end`

説明ステートフル フェールオーバー アップデート情報が、スタンバイ Secure Firewall Threat Defense デバイス への送信を停止しました。

推奨アクション 不要。

311003

エラーメッセージ `%Threat Defense-6-311003: LU recv thread up`

説明アップデート肯定応答がスタンバイ Secure Firewall Threat Defense デバイス から受信されました。

推奨アクション 不要。

311004

エラーメッセージ `%Threat Defense-6-311004: LU xmit thread up`

説明ステートフル フェールオーバー アップデート情報が、スタンバイ Secure Firewall Threat Defense デバイス に送信されました。

推奨アクション 不要。

312001

エラーメッセージ `%Threat Defense-6-312001: RIP hdr failed from IP_address : cmd=string , version=number domain=string on interface interface_name`

説明 Secure Firewall Threat Defense デバイス が応答以外のオペレーション コードを持つ RIP メッセージを受信し、メッセージはこのインターフェイスで予想されるバージョン番号とは異なる番号を持ち、ルーティング ドメインのエントリは非ゼロでした。別の RIP デバイスは Secure Firewall Threat Defense デバイス と通信するように正しく設定されていない可能性があります。

推奨アクション 不要。

313001

エラーメッセージ `%Threat Defense-3-313001: Denied ICMP type=number , code=code from IP_address on interface interface_name`

説明 icmp コマンドをアクセス リストとともに使用している場合、最初に一致したエントリが許可エントリであれば、ICMP パケットは処理を続行します。最初に一致したエントリが拒否エントリの場合、またはエントリが一致しなかった場合、Secure Firewall Threat Defense デバイスは ICMP パケットを廃棄し、このメッセージを生成します。**icmp** コマンドは、インターフェイスへの ping をイネーブルまたはディセーブルにします。ping の実行がディセーブルの場合、Secure Firewall Threat Defense デバイスはネットワーク上で検出できません。この機能は、設定可能なプロキシ ping とも呼ばれます。

推奨アクション ピア デバイスの管理者にお問い合わせください。

313004

エラーメッセージ `%Threat Defense-4-313004:Denied ICMP type=icmp_type , from source_address on interface interface_name to dest_address :no matching session`

説明ステートフル ICMP 機能で追加されたセキュリティ チェックのため、ICMP パケットが Secure Firewall Threat Defense デバイス によって廃棄されました。通常、これに該当するのは、すでに Secure Firewall Threat Defense デバイス を通過した有効なエコー要求を含まない ICMP エコー応答、またはすでに Secure Firewall Threat Defense デバイス で確立されている TCP、UDP、または ICMP セッションに関連しない ICMP エラー メッセージのいずれかです。

推奨アクション 不要。

313005

エラーメッセージ `%Threat Defense-4-313005: No matching connection for ICMP error message: icmp_msg_info on interface_name interface. Original IP payload: embedded_frame_info icmp_msg_info = icmp src src_interface_name :src_address [([idfw_user | FQDN_string], sg_info)] dst dest_interface_name :dest_address [([idfw_user | FQDN_string], sg_info)] (type icmp_type, code icmp_code) embedded_frame_info = prot src source_address /source_port [([idfw_user | FQDN_string], sg_info)] dst dest_address /dest_port [(idfw_user |FQDN_string), sg_info]`

説明 ICMP エラー メッセージが Secure Firewall Threat Defense デバイス ですでに確立されているどのセッションとも関連しないため、ICMP エラー パケットが Secure Firewall Threat Defense デバイス によって廃棄されました。

推奨アクション 原因が攻撃にある場合は、ACL を使用してホストを拒否することができます。

313008

エラーメッセージ `%Threat Defense-3-313008: Denied ICMPv6 type=number , code=code from IP_address on interface interface_name`

説明 icmp コマンドをアクセス リストとともに使用している場合、最初に一致したエントリが許可エントリであれば、ICMPv6 パケットは処理を続行します。最初に一致したエントリが拒否エントリの場合、またはエントリが一致しなかった場合、Secure Firewall Threat Defense デバイス は ICMPv6 パケットを廃棄し、このメッセージを生成します。

icmp コマンドは、インターフェイスへの ping をイネーブルまたはディセーブルにします。ping をディセーブルにすると、Secure Firewall Threat Defense デバイスがネットワーク上で検出できなくなります。この機能は、「設定可能なプロキシ ping」とも呼ばれます。

推奨アクション ピア デバイスの管理者にお問い合わせください。

313009

エラーメッセージ `%Threat Defense-4-313009: Denied invalid ICMP code icmp-code , for src-ifc :src-address /src-port (mapped-src-address/mapped-src-port) to dest-ifc :dest-address /dest-port (mapped-dest-address/mapped-dest-port) [user ], ICMP id icmp-id , ICMP type icmp-type`

説明 コードが不正な（ゼロ以外）ICMP エコー要求または応答パケットを受信しました。

推奨アクション 断続的なイベントの場合は、対処不要です。原因が攻撃にある場合、ACL を使用してホストを拒否することができます。

314001

エラーメッセージ `%Threat Defense-6-314001: Pre-allocated RTSP UDP backconnection for src_intf :src_IP to dst_intf :dst_IP /dst_port.`

説明 Secure Firewall Threat Defense デバイス が、サーバーからデータを受信していた RTSP クライアントに対して UDP メディア チャネルを開きました。

- *src_intf*：送信元インターフェイス名
- *src_IP*：送信元インターフェイス IP アドレス
- *dst_intf*：宛先インターフェイス名
- *dst_IP*：宛先 IP アドレス
- *dst_port*：宛先ポート

推奨アクション 不要。

314002

エラーメッセージ `%Threat Defense-6-314002: RTSP failed to allocate UDP media connection from src_intf :src_IP to dst_intf :dst_IP /dst_port : reason_string.`

説明 Secure Firewall Threat Defense デバイス がメディア チャネルに対して新しいピンホールを開くことができません。

- *src_intf*：送信元インターフェイス名
- *src_IP*：送信元インターフェイス IP アドレス
- *dst_intf*：宛先インターフェイス名
- *dst_IP*：宛先 IP アドレス
- *dst_port*：宛先ポート
- *reason_string*：Pinhole already exists または Unknown

推奨アクション 原因が不明な場合は、Secure Firewall Threat Defense デバイス のメモリが不足しているため、**show memory** コマンドを実行して利用可能な空きメモリを確認するか、または **show conn** コマンドを実行して使用されている接続数を確認します。

316001

エラーメッセージ `%Threat Defense-3-316001: Denied new tunnel to IP_address . VPN peer limit (platform_vpn_peer_limit) exceeded`

説明プラットフォーム VPN ピアの上限でサポートされているよりも多くの VPN トンネル（ISAKMP/IPSec）を同時に確立しようとした場合、過剰なトンネルは打ち切られます。

推奨アクション 不要。

316002

エラーメッセージ `%Threat Defense-3-316002: VPN Handle error: protocol=protocol , src in_if_num :src_addr , dst out_if_num :dst_addr`

説明 VPN ハンドルがすでに存在するため、Secure Firewall Threat Defense デバイス は VPN ハンドルを作成できません。

- *protocol*：VPN フローのプロトコル

- *in_if_num*：VPN フローの入力インターフェイス番号
- *src_addr*：VPN フローの送信元 IP アドレス
- *out_if_num*：VPN フローの出力インターフェイス番号
- *dst_addr*：VPN フローの宛先 IP アドレス

推奨アクションこのメッセージは、正常動作中に発生することもあります。ただし、メッセージが繰り返し表示され、VPNベースのアプリケーションに深刻な誤動作が発生する場合は、ソフトウェア障害が原因となっている可能性があります。次のコマンドを入力して詳細な情報を収集し、Cisco TAC に問題の調査を依頼してください。

```
capture
 name
 type asp-drop vpn-handle-error
show asp table classify crypto detail
show asp table vpn-context
```

317001

エラーメッセージ `%Threat Defense-3-317001: No memory available for limit_slow`

説明メモリが低下している状態のため、要求された操作が失敗しました。

推奨アクション 他のシステム アクティビティを減らして、メモリを解放します。状況に応じて、より大容量のメモリ構成にアップグレードしてください。

317002

エラーメッセージ `%Threat Defense-3-317002: Bad path index of number for IP_address , number max`

説明ソフトウェアのエラーが発生しました。

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

317003

エラーメッセージ `%Threat Defense-3-317003: IP routing table creation failure - reason`

説明内部ソフトウェア エラーが発生したため、新しい IP ルーティング テーブルの作成が妨げられました。

推奨アクション 表示されているとおりにエラー メッセージをコピーして、Cisco TAC に報告してください。

317004

エラーメッセージ `%Threat Defense-3-317004: IP routing table limit warning`

説明名前付き IP ルーティング テーブル内のルート数が、設定された警告制限に到達しました。

推奨アクション テーブルのルート数を減らすか、制限を設定し直します。

317005

エラーメッセージ `%Threat Defense-3-317005: IP routing table limit exceeded - reason , IP_address netmask`

説明追加のルートがテーブルに追加されます。

推奨アクション テーブルのルート数を減らすか、制限を設定し直します。

317006

エラーメッセージ `%Threat Defense-3-317006: Pdb index error pdb , pdb_index , pdb_type`

説明 PDB に対するインデックスが範囲外です。

- **pdb**：Protocol Descriptor Block（PDB インデックス エラーの記述子）
- **pdb_index**：PDB インデックス識別子
- **pdb_type**：PDB インデックス エラーのタイプ

推奨アクション 問題が解決しない場合、コンソールまたはシステム ログに表示されるエラー メッセージをそのままコピーし、Cisco TAC にお問い合わせのうえ、TAC の担当者に収集した情報をご提供ください。

317007

エラーメッセージ `%Threat Defense-6-317007: Added route_type route dest_address netmask via gateway_address [distance /metric ] on interface_name route_type`

説明新しいルートがルーティング テーブルに追加されました。

ルーティング プロトコルのタイプ：

C：接続、S：スタティック、I：IGRP、R：RIP、M：モバイル

B：BGP、D：EIGRP、EX：EIGRP 外部、O：OSPF

IA：OSPF 内部エリア、N1：OSPF NSSA 外部タイプ 1

N2：OSPF NSSA 外部タイプ 2、E1：OSPF 外部タイプ 1

E2：OSPF 外部タイプ 2、E：EGP、i：IS-IS、L1：IS-IS レベル 1

L2：IS-IS レベル 2、ia：IS-IS 内部エリア

- *dest_address*：このルートの宛先ネットワーク
- *netmask*：宛先ネットワークのネットマスク
- *gateway_address*：宛先ネットワークに到達するために使用するゲートウェイのアドレス
- *distance*：このルートのアドミニストレーティブ ディスタンス
- *metric*：このルートのメトリック
- *interface_name*：トラフィックがルーティングされるネットワーク インターフェイス名

推奨アクション 不要。

317008

エラーメッセージ `%Threat Defense-6-317008: Community list check with bad list list_number`

説明 範囲外のコミュニティリストが識別されると、このメッセージがリスト番号とともに生成されます。

推奨アクション 不要。

317012

エラーメッセージ `%Threat Defense-3-317012: Interface IP route counter negative - nameif-string-value`

説明 インターフェイス ルートの数が負の値であることを示します。

- nameif-string-value：nameif command で指定したインターフェイス名

推奨アクション 不要。

318001

エラーメッセージ `%Threat Defense-3-318001: Internal error: reason`

説明 内部ソフトウェア エラーが発生しました。このメッセージは 5 秒ごとに表示されます。

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

318002

エラーメッセージ `%Threat Defense-3-318002: Flagged as being an ABR without a backbone area`

説明 ルータは、ルータにバックボーンエリアが設定されていないエリア境界ルータとしてフラグが立てられました。このメッセージは 5 秒ごとに表示されます。

推奨アクション OSPF プロセスを再起動します。

318003

エラーメッセージ `%Threat Defense-3-318003: Reached unknow n state in neighbor state machine`

説明 内部ソフトウェア エラーが発生しました。このメッセージは 5 秒ごとに表示されます。

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

318004

エラーメッセージ `%Threat Defense-3-318004: area string lsid IP_address mask netmask adv IP_address type number`

説明 OSPF プロセスでリンクステートアドバタイズメントの検出に問題が生じました。これはメモリ リークにつながる可能性があります。

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

318005

エラーメッセージ `%Threat Defense-3-318005: lsid ip_address adv IP_address type number gateway gateway_address metric number network IP_address mask netmask protocol hex attr hex net-metric number`

説明 OSPF で、そのデータベースと IP ルーティング テーブル間に不整合が検出されました。

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

318006

エラーメッセージ `%Threat Defense-3-318006: if interface_name if_state number`

説明 内部エラーが発生しました。

推奨アクション 表示されているとおりにメッセージをコピーして、Cisco TAC に報告してください。

318007

エラーメッセージ `%Threat Defense-3-318007: OSPF is enabled on interface_name during idb initialization`

説明 内部エラーが発生しました。

推奨アクション 表示されているとおりにメッセージをコピーして、Cisco TAC に報告してください。

318008

エラーメッセージ `%Threat Defense-3-318008: OSPF process number is changing router-id. Reconfigure virtual link neighbors with our new router-id`

説明 OSPF プロセスがリセット中で、新しいルータ ID を選択しようとしています。このアクションによってすべての仮想リンクが停止させられます。

推奨アクション すべての隣接仮想リンクの仮想リンク コンフィギュレーションを、新しいルータ ID を反映するように変更します。

318009

エラーメッセージ `%Threat Defense-3-318009: OSPF: Attempted reference of stale data encountered in function , line: line_num`

説明 OSPF が動作中で、他の場所で削除された一部の関連データ構造を参照しようとしました。インターフェイスおよびルータのコンフィギュレーションを消去すると、問題が解決する可能性があります。しかし、このメッセージが表示される場合は、シーケンスの一部のステップによってデータ構造の早期削除が生じているので、調査する必要があります。

- *function*：予期しないイベントを受信した機能
- *line_num*：コード中の行番号

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。

318101

エラーメッセージ `%Threat Defense-3-318101: Internal error: REASON`

説明内部ソフトウェア エラーが発生しました。

- *REASON*：イベントの詳細な原因

推奨アクション 不要。

318102

エラーメッセージ `%Threat Defense-3-318102: Flagged as being an ABR without a backbone area`

説明ルータ内のバックボーン領域なしに、ルータが Area Border Router（ABR）としてフラグが設定されました。

推奨アクション OSPF プロセスを再起動します。

318103

エラーメッセージ `%Threat Defense-3-318103: Reached unknown state in neighbor state machine`

説明内部ソフトウェア エラーが発生しました。

推奨アクション 不要。

318104

エラーメッセージ `%Threat Defense-3-318104: DB already exist: area AREA_ID_STR lsid i adv i type 0x x`

説明 OSPF で LSA を見つけることができないため、メモリのリークが発生する可能性があります。

- *AREA_ID_STR*：領域を表す文字列
- *i*：整数値
- *x*：整数値の 16 進表記

推奨アクション 不要。

318105

エラーメッセージ `%Threat Defense-3-318105: lsid i adv i type 0x x gateway i metric d network i mask i protocol #x attr #x net-metric d`

説明 OSPF で、そのデータベースと IP ルーティング テーブル間に不整合が検出されました。

- *i*：整数値
- *x*：整数値の 16 進表記
- *d*：数値

推奨アクション 不要。

318106

エラーメッセージ `%Threat Defense-3-318106: if IF_NAME if_state d`

説明内部エラーが発生しました。

- *IF_NAME*：影響を受けるインターフェイスの名前
- *d*：数値

推奨アクション 不要。

318107

エラーメッセージ `%Threat Defense-3-318107: OSPF is enabled on IF_NAME during idb initialization`

説明内部エラーが発生しました。

- *IF_NAME*：影響を受けるインターフェイスの名前

推奨アクション 不要。

318108

エラーメッセージ `%Threat Defense-3-318108: OSPF process d is changing router-id. Reconfigure virtual link neighbors with our new router-id`

説明 OSPF プロセスがリセット中で、新しいルータ ID を選択しようとしています。これにより、すべての仮想リンクがダウンします。再び動作させるには、すべての仮想リンク ネイバー上の仮想リンク設定を変更する必要があります。

- *d*：プロセス ID を表す番号

推奨アクションすべての隣接仮想リンクの仮想リンク コンフィギュレーションを、新しいルータ ID を含むように変更します。

318109

エラーメッセージ `%Threat Defense-3-318109: OSPFv3 has received an unexpected message: 0x / 0x`

説明 OSPFv3 が予期しないプロセス間メッセージを受信しました。

- *x*：整数値の 16 進表記

推奨アクション 不要。

318110

エラーメッセージ `%Threat Defense-3-318110: Invalid encrypted key s .`

説明指定された暗号キーが無効です。

- *s*：暗号キーを表す文字列

推奨アクション クリア テキストのキーを指定し、**service password-encryption** コマンドを入力して暗号化するか、または指定した暗号キーが有効であることを確認します。指定された暗号キーが無効な場合は、システム設定時にエラー メッセージが表示されます。

318111

エラーメッセージ `%Threat Defense-3-318111: SPI u is already in use with ospf process d`

説明すでに使用されている SPI を使用しようとしました。

- *u*：SPI を表す番号
- *d*：プロセス ID を表す番号

推奨アクション 別の SPI を選択します。

318112

エラーメッセージ `%Threat Defense-3-318112: SPI u is already in use by a process other than ospf process d .`

説明すでに使用されている SPI を使用しようとしました。

- *u*：SPI を表す番号
- *d*：プロセス ID を表す番号

推奨アクション別の SPI を選択します。すでに使用されている SPI のリストを表示するには、**show crypto ipv6 ipsec sa** コマンドを入力します。

318113

エラーメッセージ `%Threat Defense-3-318113: s s is already configured with SPI u .`

説明すでに使用されている SPI を使用しようとしました。

- *s*：インターフェイスを表す文字列
- *u*：SPI を表す番号

推奨アクション 最初に SPI を設定解除するか、別の SPI を選択します。

318114

エラーメッセージ `%Threat Defense-3-318114: The key length used with SPI u is not valid`

説明キーの長さが間違っています。

- *u*：SPI を表す番号

推奨アクション 有効な IPsec キーを選択します。IPsec 認証キーは 32 桁（MD5）または 40 桁（SHA-1）の 16 進数値である必要があります。

318115

エラーメッセージ `%Threat Defense-3-318115: s error occured when attempting to create an IPsec policy for SPI u`

説明 IPsec API（内部）エラーが発生しました。

- *s*：エラーを表す文字列
- *u*：SPI を表す番号

推奨アクション 不要。

318116

エラーメッセージ `%Threat Defense-3-318116: SPI u is not being used by ospf process d .`

説明 OSPFv3 で使用されていない SPI を設定解除しようとしました。

- *u*：SPI を表す番号
- *d*：プロセス ID を表す番号

推奨アクションOSPFv3 によって使用されている SPI を確認するには、**show** コマンドを入力します。

318117

エラーメッセージ `%Threat Defense-3-318117: The policy for SPI u could not be removed because it is in use.`

説明表示された SPI のポリシーを削除しようとしましたが、そのポリシーがまだセキュア ソケットにより使用されていました。

- *u*：SPI を表す番号

推奨アクション 不要。

318118

エラーメッセージ `%Threat Defense-3-318118: s error occured when attemtping to remove the IPsec policy with SPI u`

説明 IPsec API（内部）エラーが発生しました。

- *s*：指定されたエラーを表す文字列
- *u*：SPI を表す番号

推奨アクション 不要。

318119

エラーメッセージ `%Threat Defense-3-318119: Unable to close secure socket with SPI u on interface s`

説明 IPsec API（内部）エラーが発生しました。

- *u*：SPI を表す番号
- *s*：指定されたインターフェイスを表す文字列

推奨アクション 不要。

318120

エラーメッセージ `%Threat Defense-3-318120: OSPFv3 was unable to register with IPsec`

説明内部エラーが発生しました。

推奨アクション 不要。

318121

エラーメッセージ `%Threat Defense-3-318121: IPsec reported a GENERAL ERROR: message s , count d`

説明内部エラーが発生しました。

- *s*：指定したメッセージを表す文字列
- *d*：生成メッセージの総数を表す数値

推奨アクション 不要。

318122

エラーメッセージ `%Threat Defense-3-318122: IPsec sent a s message s to OSPFv3 for interface s . Recovery attempt d`

説明内部エラーが発生しました。システムがセキュアなソケットの再オープンと復旧を試みています。

- *s*：指定されたメッセージと指定されたインターフェイスを表す文字列
- *d*：リカバリ試行回数を表す数値

推奨アクション 不要。

318123

エラーメッセージ `%Threat Defense-3-318123: IPsec sent a s message s to OSPFv3 for interface IF_NAME . Recovery aborted`

説明 内部エラーが発生しました。リカバリの試行の最大数を超えました。

- *s*：指定したメッセージを表す文字列
- *IF_NAME*：指定したインターフェイス

推奨アクション 不要。

318125

エラーメッセージ `%Threat Defense-3-318125: Init failed for interface IF_NAME`

説明インターフェイスの初期化に失敗しました。考えられる原因は、次のとおりです。

- インターフェイスの接続先となる領域が削除されています。
- リンク スコープのデータベースを作成できませんでした。
- ローカル ルータのネイバー データブロックを作成できませんでした。

推奨アクション インターフェイスを初期設定するコンフィギュレーション コマンドを削除して、再試行します。

318126

エラーメッセージ `%Threat Defense-3-318126: Interface IF_NAME is attached to more than one area`

説明インターフェイスが、インターフェイスのリンク先以外の領域のインターフェイス リストに含まれています。

- *IF_NAME*：指定したインターフェイス

推奨アクション 不要。

318127

エラーメッセージ `%Threat Defense-3-318127: Could not allocate or find the neighbor`

説明内部エラーが発生しました。

推奨アクション 不要。

メッセージ 320001 ～ 341011

この章では、320001 から 341011 までのメッセージについて説明します。

320001

エラーメッセージ `%Threat Defense-3-320001: The subject name of the peer cert is not allowed for connection`

説明 Secure Firewall Threat Defense デバイス が簡単な VPN リモート デバイスまたはサーバーである場合、ピア証明書には **ca verifycertdn** コマンドの出力と一致しないサブジェクト名が含まれています。中間者攻撃が発生している可能性もあります。これは、デバイスがピア IP アドレスをスプーフィングし、Secure Firewall Threat Defense デバイス から VPN 接続を代行受信しようとするものです。

推奨アクション 不要。

321001

エラーメッセージ `%FTD-5-321001: Resource var1 limit of var2 reached.`

説明指摘されたリソースの設定使用率またはレート制限に達しました。

推奨アクションプラットフォームの最大接続数に達した場合、メモリを再割り当てしてシステムメモリを解放するのに時間がかかり、トラフィックに障害が発生します。メモリスペースが解放された後、デバイスをリロードする必要があります。その他の支援については、TAC にお問い合わせください。

321002

エラーメッセージ `%FTD-5-321002: Resource var1 rate limit of var2 reached.`

説明指摘されたリソースの設定使用率またはレート制限に達しました。

推奨アクションプラットフォームの最大接続数に達した場合、メモリを再割り当てしてシステムメモリを解放するのに時間がかかり、トラフィックに障害が発生します。メモリスペースが解放された後、デバイスをリロードする必要があります。その他の支援については、TAC にお問い合わせください。

321003

エラーメッセージ `%Threat Defense-6-321003: Resource var1 log level of var2 reached.`

説明指摘されたリソースの設定リソース使用率またはレート ログ レベルに達しました。

推奨アクション 不要。

321004

エラーメッセージ `%Threat Defense-6-321004: Resource var1 rate log level of var2 reached`

説明指摘されたリソースの設定リソース使用率またはレート ログ レベルに達しました。

推奨アクション 不要。

321005

エラーメッセージ `%Threat Defense-2-321005: System CPU utilization reached utilization %`

説明システムの CPU 使用率が 95% 以上に到達し、5 分間このレベルにとどまっています。

- *utilization %*：使用されている CPU のパーセンテージ

推奨アクションこのメッセージが定期的に表示される場合は、無視できます。頻繁に繰り返される場合は、**show cpu** コマンドの出力を確認し、CPU 使用率を確認します。これが高い場合は、Cisco TAC にお問い合わせください。

321006

エラーメッセージ `%Threat Defense-2-321006: System memory usage reached utilization %`

説明システムのメモリ使用率が 80% 以上に到達し、5 分間このレベルにとどまっています。

- *utilization %*：使用されている CPU のパーセンテージ

推奨アクションこのメッセージが定期的に表示される場合は、無視できます。頻繁に繰り返される場合は、**show memory** コマンドの出力を確認し、メモリ使用率を確認します。これが高い場合は、Cisco TAC にお問い合わせください。

321007

エラーメッセージ `%Threat Defense-3-321007: System is low on free memory blocks of size block_size (free_blocks CNT out of max_blocks MAX)`

説明システムでメモリの空きブロックが不足しています。ブロックが不足すると、トラフィックの中断が発生する可能性があります。

- *block_size*：メモリのブロック サイズ（たとえば、4、1550、8192）
- *free_blocks*：空きブロック数。**show blocks** コマンドの使用後に CNT カラムに示される

- *max_blocks*：システムが割り当てることができるブロックの最大数。**show blocks** コマンドの使用後 MAX カラムに示される

推奨アクション 表示されたブロック サイズの出力の CNT カラムにある空きブロックの量をモニターするには、**show blocks** コマンドを使用します。CNT カラムが長時間にわたってゼロかそれに非常に近いままになる場合、Secure Firewall Threat Defense デバイス がオーバーロードになっているか、追加調査が必要な別の問題が発生している可能性があります。

322001

エラーメッセージ `%Threat Defense-3-322001: Deny MAC address MAC_address, possible spoof attempt on interface interface`

説明 Secure Firewall Threat Defense デバイス が、疑わしい MAC アドレスからのパケットを指定のインターフェイス上で受信しましたが、そのパケットの送信元 MAC アドレスは、コンフィギュレーションでは別のインターフェイスにスタティックにバインドされています。MAC スプーフィング攻撃または設定ミスが原因である可能性があります。

推奨アクション コンフィギュレーションを調べ、攻撃ホストを突き止めるか、またはコンフィギュレーションを訂正して適切な処置を行います。

322002

エラーメッセージ `%Threat Defense-3-322002: ARP inspection check failed for arp {request|response} received from host MAC_address on interface interface . This host is advertising MAC Address MAC_address_1 for IP Address IP_address , which is {statically|dynamically} bound to MAC Address MAC_address_2 .`

説明 ARP 検査モジュールは、イネーブルになっている場合、パケット内でアドバタイズされる新しいARPエントリが、静的に設定されたIP-MACアドレスまたは動的に取得されたIP-MACアドレスのバインディングに従っているかどうかをチェックしてから、Secure Firewall Threat Defense デバイス を介して ARP パケットを転送します。このチェックが失敗した場合、ARP インスペクション モジュールは ARP パケットを廃棄し、このメッセージを生成します。ネットワーク上で ARP スプーフィング攻撃が発生しているか、またはコンフィギュレーション（IP-MAC バインディング）が無効である可能性があります。

推奨アクション 原因が攻撃にある場合は、ACL を使用してホストを拒否することができます。原因が無効なコンフィギュレーションにある場合、バインディングを修正します。

322003

エラーメッセージ `%Threat Defense-3-322003:ARP inspection check failed for arp {request|response} received from host MAC_address on interface interface . This host is advertising MAC Address MAC_address_1 for IP Address IP_address , which is not bound to any MAC Address.`

説明 ARP 検査モジュールは、イネーブルになっている場合、パケット内でアドバタイズされる新しい ARP エントリが、静的に設定された IP-MAC アドレスのバインディングに従っているかどうかをチェックしてから、Secure Firewall Threat Defense デバイス を介して ARP パケッ

トを転送します。このチェックが失敗した場合、ARP インスペクション モジュールは ARP パケットを廃棄し、このメッセージを生成します。ネットワーク上で ARP スプーフィング攻撃が発生しているか、またはコンフィギュレーション（IP-MAC バインディング）が無効である可能性があります。

推奨アクション原因が攻撃にある場合は、ACL を使用してホストを拒否することができます。原因が無効なコンフィギュレーションにある場合、バインディングを修正します。

322004

エラーメッセージ `%Threat Defense-6-322004: No management IP address configured for transparent firewall. Dropping protocol protocol packet from interface_in :source_address /source_port to interface_out :dest_address /dest_port`

説明管理 IP アドレスがトランスペアレント モードで設定されていないため、Secure Firewall Threat Defense デバイス がパケットを廃棄しました。

- **protocol**：プロトコルの文字列または値
- **interface_in**：入力インターフェイス名
- **source_address**：パケットの送信元 IP アドレス
- **source_port**：パケットの送信元ポート
- **interface_out**：出力インターフェイス名
- **dest_address**：パケットの宛先 IP アドレス
- **dest_port**：パケットの宛先ポート

推奨アクション デバイスに管理 IP アドレスとマスクの値を設定します。

323001

エラーメッセージ `%Threat Defense-3-323001: Module module_id experienced a control channel communications failure.`

`%Threat Defense-3-323001: Module in slot slot_num experienced a control channel communications failure.`

説明 Secure Firewall Threat Defense デバイス が、制御チャネルを介して、指定されたスロットに設置されているモジュールと通信できません。

- **module_id**：ソフトウェア サービスのモジュールの場合、サービス モジュールの名前を指定します。
- **slot_num**：ハードウェアのサービス モジュールの場合、障害が発生したスロットを指定します。スロット 0 はシステムのメイン ボードを示し、スロット 1 は拡張スロットに設置されているモジュールを示します。

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。

323002

エラーメッセージ `%Threat Defense-3-323002: Module module_id is not able to shut down, shut down request not answered.`

`%Threat Defense-3-323002: Module in slot slot_num is not able to shut down, shut down request not answered.`

説明設置されているモジュールが、シャットダウン要求に応答しませんでした。

- **module_id**：ソフトウェア サービスのモジュールの場合、サービス モジュールの名前を指定します。
- **slot_num**：ハードウェアのサービス モジュールの場合、障害が発生したスロットを指定します。スロット 0 はシステムのメイン ボードを示し、スロット 1 は拡張スロットに設置されているモジュールを示します。

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。

323003

エラーメッセージ `%Threat Defense-3-323003: Module module_id is not able to reload, reload request not answered.`

`%Threat Defense-3-323003: Module in slot slotnum is not able to reload, reload request not answered.`

説明設置されているモジュールが、リロード要求に応答しませんでした。

- **module_id**：ソフトウェア サービスのモジュールの場合、サービス モジュールの名前を指定します。
- **slot_num**：ハードウェアのサービス モジュールの場合、障害が発生したスロットを指定します。スロット 0 はシステムのメイン ボードを示し、スロット 1 は拡張スロットに設置されているモジュールを示します。

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。

323004

エラーメッセージ `%Threat Defense-3-323004: Module string one failed to write software newver (currently ver ), reason . Hw-module reset is required before further use.`

説明 モジュールがソフトウェア バージョンに対応できませんでした。UNRESPONSIVE 状態に移行します。モジュールは、ソフトウェアがアップデートされるまで使用できません。

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

- write failure

- failed to create a thread to write the image

推奨アクション モジュール ソフトウェアは、アップデートできない場合、使用できなくなります。問題が解決しない場合、Cisco TAC にお問い合わせください。

323005

エラーメッセージ `%Threat Defense-3-323005: Module module_id can not be started completely`

`%Threat Defense-3-323005: Module in slot slot_num  cannot be started completely`

説明このメッセージは、モジュールが完全に起動できないことを示します。モジュールは、この状態が修正されるまで、UNRESPONSIVE 状態のままになります。最も可能性が高い原因として、モジュールがスロットに正しく取り付けられていないことが考えられます。

- **module_id**：ソフトウェア サービスのモジュールの場合、サービス モジュールの名前を指定します。
- **slot_num**：ハードウェアのサービス モジュールの場合、モジュールが装着されているスロット番号を指定します。

推奨アクションモジュールが正しく取り付けられていることを確認し、モジュールのステータス LED が点灯しているかどうかをチェックします。モジュールを正しく取り付け直した後、モジュールが電源投入されたことを Secure Firewall Threat Defense デバイス が認識するまで数分かかることがあります。モジュールが取り付けられていることを確認し、**sw-module module** *service-module-name* **reset** コマンドまたは **hw-module module** *slotnum* **reset** コマンドを使用してモジュールをリセットした後もこのメッセージが表示される場合は、Cisco TAC にお問い合わせください。

323006

エラーメッセージ `%Threat Defense-1-323006: Module ips  experienced a data channel communication failure, data channel is DOWN.`

説明データ チャネル通信障害が発生し、Secure Firewall Threat Defense デバイス がサービス モジュールにトラフィックを転送できませんでした。この障害が HA コンフィギュレーションのアクティブ Secure Firewall Threat Defense デバイス で発生した場合は、フェールオーバーがトリガーされます。また、この障害によって、通常はサービスモジュールに送信されるトラフィックに、設定済みのフェール オープン ポリシーまたはフェール クローズ ポリシーが適用されます。このメッセージは、システム モジュールとサービス モジュールの間で Secure Firewall Threat Defense デバイス のデータプレーンを介した通信上の問題が発生すると必ず生成されます。このような問題は、サービスモジュールが停止、リセット、取り外し、またはディセーブルにされた場合に発生する可能性があります。

推奨アクション IPS などのソフトウェア サービスモジュールの場合、**sw-module module ips recover** コマンドを使用してモジュールを回復します。ハードウェア サービス モジュールの場合、このメッセージが SSM のリロードまたはリセットの結果として生成されたのではなく、

SSM が UP 状態に戻った後に、対応する syslog メッセージ 505010 が表示されない場合は、**hw-module module 1 reset** コマンドを使用してモジュールをリセットします。

323007

エラーメッセージ `%Threat Defense-3-323007: Module in slot slot experienced a firware failure and the recovery is in progress.`

説明 4GE-SSM が装着された Secure Firewall Threat Defense デバイス で、短い電力サージが発生し、その後リブートされました。その結果、4GE-SSM は、無応答状態でオンラインになっている可能性があります。Secure Firewall Threat Defense デバイス は、4GE-SSM が無応答であることを検出し、自動的に 4GE-SSM を再起動します。

推奨アクション 不要。

325001

エラーメッセージ `%Threat Defense-3-325001: Router ipv6_address on interface has conflicting ND (Neighbor Discovery) settings`

説明 リンク上の別のルータが、矛盾するパラメータを持つルータ アドバタイズメントを送信しました。

- **ipv6_address**：相手側ルータの IPv6 アドレス
- **interface**：相手側ルータとのリンクのインターフェイス名

推奨アクション リンク上の IPv6 ルータがすべて、**hop_limit**、**managed_config_flag**、**other_config_flag**、**reachable_time**、および **ns_interval** についてルータ アドバタイズメントに同じパラメータを持つことを確認し、複数のルータによってアドバタイズされる、同じプレフィックスの優先される有効なライフタイムが同じであることを確認します。インターフェイスごとにパラメータを示すには、**show ipv6 interface** コマンドを入力します。

325002

エラーメッセージ `%Threat Defense-4-325002: Duplicate address ipv6_address/MAC_address on interface`

説明 別のシステムが IPv6 アドレスを使用しています。

- **ipv6_address**：相手側ルータの IPv6 アドレス
- **MAC_address**：既知の場合は相手側システムの MAC アドレス、それ以外の場合は unknown
- **interface**：相手側システムとのリンクのインターフェイス名

推奨アクション 2 つのシステムのうちの 1 つの IPv6 アドレスを変更します。

326001

エラーメッセージ `%Threat Defense-3-326001: Unexpected error in the timer library: error_message`

説明管理対象タイマーイベントが、コンテキストも正しいタイプもなしで受信されたか、あるいはハンドラがありません。または、キューに入るイベントの数がシステム制限を超えると、後で処理が試行されます。

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

326002

エラーメッセージ `%Threat Defense-3-326002: Error in error_message : error_message`

説明 IGMP プロセスが要求に応じてシャットダウンできませんでした。このシャットダウンに備えて実行されるイベントが同期していない可能性があります。

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

326004

エラーメッセージ `%Threat Defense-3-326004: An internal error occurred while processing a packet queue`

説明 IGMP パケット キューがパケットを持たない信号を受信しました。

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。

326005

エラーメッセージ `%Threat Defense-3-326005: Mrib notification failed for (IP_address, IP_address )`

説明データ駆動型イベントをトリガーするパケットが受信され、MRIB を通知する試行が失敗しました。

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。

326006

エラーメッセージ `%Threat Defense-3-326006: Entry-creation failed for (IP_address, IP_address )`

説明 MFIB は MRIB からエントリのアップデートを受信しましたが、表示されるアドレスに関連するエントリを作成できませんでした。メモリ不足が原因として考えられます。

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

326007

エラーメッセージ `%Threat Defense-3-326007: Entry-update failed for (IP_address, IP_address )`

説明 MFIB が MRIB からインターフェイスのアップデートを受信しましたが、表示されるアドレスに関連するインターフェイスを作成できませんでした。メモリ不足が原因として考えられます。

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

326008

エラーメッセージ `%Threat Defense-3-326008: MRIB registration failed`

説明 MFIB が MRIB に登録できませんでした。

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

326009

エラーメッセージ `%Threat Defense-3-326009: MRIB connection-open failed`

説明 MFIB が MRIB への接続を開けませんでした。

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

326010

エラーメッセージ `%Threat Defense-3-326010: MRIB unbind failed`

説明 MFIB が MRIB からアンバインドできませんでした。

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

326011

エラーメッセージ `%Threat Defense-3-326011: MRIB table deletion failed`

説明 MFIB が削除されるはずだったテーブルを取得できませんでした。

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

326012

エラーメッセージ `%Threat Defense-3-326012: Initialization of` *`string`* `functionality failed`

説明指摘された機能の初期化が失敗しました。このコンポーネントは引き続き、機能なしでも動作する可能性があります。

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

326013

エラーメッセージ `%Threat Defense-3-326013: Internal error: string in string line %d (%s)`

説明 MRIB で基本エラーが発生しました。

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

326014

エラーメッセージ `%Threat Defense-3-326014: Initialization failed: error_message error_message`

説明 MRIB が初期化できませんでした。

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

326015

エラーメッセージ `%Threat Defense-3-326015: Communication error: error_message error_message`

説明 MRIB が形式が誤っているアップデートを受信しました。

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。

326016

エラーメッセージ `%Threat Defense-3-326016: Failed to set un-numbered interface for interface_name (string )`

説明 PIM トンネルが送信元アドレスがないため使用できません。この状況は、番号付きインターフェイスが見つからないため、または内部エラーが原因で発生します。

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。

326017

エラーメッセージ `%Threat Defense-3-326017: Interface Manager error - string in string : string`

説明 PIM トンネル インターフェイスを作成中に、エラーが発生しました。

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

326019

エラーメッセージ `%Threat Defense-3-326019: string in string : string`

説明 PIM RP トンネル インターフェイスを作成中に、エラーが発生しました。

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

326020

エラーメッセージ `%Threat Defense-3-326020: List error in string : string`

説明 PIM インターフェイス リストを処理中に、エラーが発生しました。

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

326021

エラーメッセージ `%Threat Defense-3-326021: Error in string : string`

説明 PIM トンネル インターフェイスの SRC を設定中に、エラーが発生しました。

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

326022

エラーメッセージ `%Threat Defense-3-326022: Error in string : string`

説明 PIM プロセスが要求に応じてシャットダウンできませんでした。このシャットダウンに備えて実行されるイベントが同期していない可能性があります。

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

326023

エラーメッセージ `%Threat Defense-3-326023: string - IP_address : string`

説明 PIM グループ範囲を処理中に、エラーが発生しました。

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

326024

エラーメッセージ `%Threat Defense-3-326024: An internal error occurred while processing a packet queue.`

説明 PIM パケット キューがパケットを持たない信号を受信しました。

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。

326025

エラーメッセージ `%Threat Defense-3-326025: string`

説明メッセージ送信の試行中に、内部エラーが発生しました。PIM トンネル IDB の削除など、メッセージの受信時に発生するようスケジュールされたイベントが発生しない可能性があります。

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

326026

エラーメッセージ `%Threat Defense-3-326026: Server unexpected error: error_message`

説明 MRIB がクライアントを登録できませんでした。

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

326027

エラーメッセージ `%Threat Defense-3-326027: Corrupted update: error_message`

説明 MRIB が破損したアップデートを受信しました。

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。

326028

エラーメッセージ `%Threat Defense-3-326028: Asynchronous error: error_message`

説明 MRIB API で未処理の非同期エラーが発生しました。

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

327001

エラーメッセージ `%Threat Defense-3-327001: IP SLA Monitor: Cannot create a new process`

説明 IP SLA モニターが新しいプロセスを開始できませんでした。

推奨アクション システム メモリを確認します。メモリが不足している場合は、それが原因である可能性があります。メモリが利用可能になったときに、コマンドを再入力してみます。問題が解決しない場合、Cisco TAC にお問い合わせください。

327002

エラーメッセージ `%Threat Defense-3-327002: IP SLA Monitor: Failed to initialize, IP SLA Monitor functionality will not work`

説明 IP SLA モニターが初期化に失敗しました。この状態は、タイマー ホイール機能が初期化に失敗した場合、またはプロセスが作成されなかった場合に発生します。タスクを完了するために利用できるメモリが十分でない可能性があります。

推奨アクション システム メモリを確認します。メモリが不足している場合は、それが原因である可能性があります。メモリが利用可能になったときに、コマンドを再入力してみます。問題が解決しない場合、Cisco TAC にお問い合わせください。

327003

エラーメッセージ `%Threat Defense-3-327003: IP SLA Monitor: Generic Timer wheel timer functionality failed to initialize`

説明 IP SLA モニターがタイマー ホイールを初期化できません。

推奨アクション システム メモリを確認します。メモリが不足している場合は、そのためにタイマー ホイール機能が初期化されませんでした。メモリが利用可能になったときに、コマンドを再入力してみます。問題が解決しない場合、Cisco TAC にお問い合わせください。

328001

エラーメッセージ `%Threat Defense-3-328001: Attempt made to overwrite a set stub function in string .`

説明 レジストリ チェック付きスタブが起動されたときのコールバックとして、1 つの機能を設定できます。コールバック機能がすでに設定されていたため、新しいコールバックの設定試行が失敗しました。

- **string**：機能の名前

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。

328002

エラーメッセージ `%Threat Defense-3-328002: Attempt made in string to register with out of bounds key`

説明 FASTCASE レジストリでは、レジストリが作成されたときに指定されたサイズよりもキーが小さくなければなりません。限界を超えたキーを登録しようとしました。

推奨アクション 表示されているとおりにエラー メッセージをコピーして、Cisco TAC に報告してください。

329001

エラーメッセージ `%Threat Defense-3-329001: The string0 subblock named string1 was not removed`

説明 ソフトウェアのエラーが発生しました。IDB サブブロックを削除できません。

- *string0*：SWIDB または HWIDB
- *string1*：サブブロックの名前

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。

331001

エラーメッセージ `%Threat Defense-3-331001: Dynamic DNS Update for 'fqdn_name ' = ip_address failed`

説明ダイナミック DNS サブシステムが DNS サーバー上のリソース レコードをアップデートできませんでした。この障害は、Secure Firewall Threat Defense デバイス が DNS サーバーにアクセスできない場合、または対象のシステム上で DNS サービスが動作していない場合に発生する可能性があります。

- *fqdn_name*：DNS アップデートが試行された完全修飾ドメイン名
- *ip_address*：DNS アップデートの IP アドレス

推奨アクション DNS サーバーが設定されており、Secure Firewall Threat Defense デバイス から到達可能であることを確認します。問題が解決しない場合、Cisco TAC にお問い合わせください。

331002

エラーメッセージ `%Threat Defense-5-331002: Dynamic DNS type RR for ('fqdn_name ' - ip_address | ip_address - 'fqdn_name ') successfully updated in DNS server dns_server_ip`

説明 DNS サーバーでダイナミック DNS アップデートが成功しました。

- *type*：リソース レコードのタイプ（A または PTR）
- *fqdn_name*：DNS アップデートが試行された完全修飾ドメイン名
- *ip_address*：DNS アップデートの IP アドレス
- *dns_server_ip*：DNS サーバーの IP アドレス

推奨アクション 不要。

332001

エラーメッセージ `%Threat Defense-3-332001: Unable to open cache discovery socket, WCCP V2 closing down.`

説明内部エラーです。WCCP プロセスが、キャッシュからのプロトコル メッセージのリッスンに使用される UDP ソケットを開くことができなかったことを示しています。

推奨アクション IP コンフィギュレーションが正しいこと、および少なくとも 1 つの IP アドレスが設定されていることを確認します。

332002

エラーメッセージ `%Threat Defense-3-332002: Unable to allocate message buffer, WCCP V2 closing down.`

説明内部エラーです。WCCP プロセスが、着信プロトコル メッセージを保持するためのメモリを割り当てることができなかったことを示しています。

推奨アクション すべてのプロセスに利用可能な十分なメモリがあることを確認します。

332003

エラーメッセージ `%Threat Defense-5-332003: Web Cache IP_address /service_ID acquired`

説明 Secure Firewall Threat Defense デバイス の Web キャッシュからのサービスが取得されました。

- **IP_address**：Web キャッシュの IP アドレス
- **service_ID**：WCCP サービス識別子

推奨アクション 不要。

332004

エラーメッセージ `%Threat Defense-1-332004: Web Cache IP_address /service_ID lost`

説明 Secure Firewall Threat Defense デバイス の Web キャッシュからのサービスが失われました。

- **IP_address**：Web キャッシュの IP アドレス
- **service_ID**：WCCP サービス識別子

推奨アクション 指摘された Web キャッシュの動作を確認します。

333001

エラーメッセージ `%Threat Defense-6-333001: EAP association initiated - context: EAP-context`

説明リモート ホストとの EAP アソシエーションが開始されました。

- *EAP-context*：EAP セッションの一意の識別子。8 桁の 16 進数として表示されます（たとえば、0x2D890AE0）。

推奨アクション 不要。

333002

エラーメッセージ `%Threat Defense-5-333002: Timeout waiting for EAP response - context:EAP-context`

説明 EAP 応答を待っている間にタイムアウトが発生しました。

- *EAP-context*：EAP セッションの一意の識別子。8 桁の 16 進数として表示されます（たとえば、0x2D890AE0）。

推奨アクション 不要。

333003

エラーメッセージ `%Threat Defense-6-333003: EAP association terminated - context:EAP-context`

説明リモート ホストとの EAP アソシエーションが終了しました。

- *EAP-context*：EAP セッションの一意の識別子。8 桁の 16 進数として表示されます（たとえば、0x2D890AE0）。

推奨アクション 不要。

333004

エラーメッセージ `%Threat Defense-7-333004: EAP-SQ response invalid - context:EAP-context`

説明 EAP ステータス クエリーの応答が、基本的なパケット検証に失敗しました。

- *EAP-context*：EAP セッションの一意の識別子。8 桁の 16 進数として表示されます（たとえば、0x2D890AE0）。

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。

333005

エラーメッセージ `%Threat Defense-7-333005: EAP-SQ response contains invalid TLV(s) - context:EAP-context`

説明 EAP ステータス クエリーの応答に、1 つまたは複数の無効な TLV が含まれています。

- *EAP-context*：EAP セッションの一意の識別子。8 桁の 16 進数として表示されます（たとえば、0x2D890AE0）。

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。

333006

エラーメッセージ `%Threat Defense-7-333006: EAP-SQ response with missing TLV(s) - context:EAP-context`

説明 EAP ステータス クエリーの応答に、1 つまたは複数の必須 TLV がありません。

- *EAP-context*：EAP セッションの一意の識別子。8 桁の 16 進数として表示されます（たとえば、0x2D890AE0）。

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。

333007

エラーメッセージ `%Threat Defense-7-333007: EAP-SQ response TLV has invalid length - context:EAP-context`

説明 EAP ステータス クエリーの応答に、無効な長さの TLV が含まれています。

- *EAP-context*：EAP セッションの一意の識別子。8 桁の 16 進数として表示されます（たとえば、0x2D890AE0）。

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。

333008

エラーメッセージ `%Threat Defense-7-333008: EAP-SQ response has invalid nonce TLV - context:EAP-context`

説明 EAP ステータス クエリーの応答に、無効なナンス TLV が含まれています。

- *EAP-context*：EAP セッションの一意の識別子。8 桁の 16 進数として表示されます（たとえば、0x2D890AE0）。

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。

333009

エラーメッセージ `%Threat Defense-6-333009: EAP-SQ response MAC TLV is invalid - context:EAP-context`

説明 EAP ステータス クエリーの応答に、計算された MAC と一致しない MAC が含まれています。

- *EAP-context*：EAP セッションの一意の識別子。8 桁の 16 進数として表示されます（たとえば、0x2D890AE0）。

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。

333010

エラーメッセージ `%Threat Defense-5-333010: EAP-SQ response Validation Flags TLV indicates PV request - context:EAP-context`

説明 EAP ステータス クエリーの応答に、ピアが完全なポスチャ検証を要求したことを示す検証フラグ TLV が含まれています。

推奨アクション 不要。

334001

エラーメッセージ `%Threat Defense-6-334001: EAPoUDP association initiated - host-address`

説明 リモート ホストとの EAPoUDP アソシエーションが開始されました。

- *host-address*：ホストの IP アドレス。ドット付き 10 進表記で示されます（たとえば、10.86.7.101）。

推奨アクション 不要。

334002

エラーメッセージ `%Threat Defense-5-334002: EAPoUDP association successfully established - host-address`

説明ホストとの EAPoUDP アソシエーションが正常に確立されました。

- *host-address*：ホストの IP アドレス。ドット付き 10 進表記で示されます（たとえば、10.86.7.101）。

推奨アクション 不要。

334003

エラーメッセージ `%Threat Defense-5-334003: EAPoUDP association failed to establish - host-address`

説明ホストとの EAPoUDP アソシエーションを確立できませんでした。

- *host-address*：ホストの IP アドレス。ドット付き 10 進表記で示されます（たとえば、10.86.7.101）

推奨アクション Cisco Secure Access Control Server の設定を確認します。

334004

エラーメッセージ `%Threat Defense-6-334004: Authentication request for NAC Clientless host - host-address`

説明 NAC クライアントレス ホストの認証要求が行われました。

- *host-address*：ホストの IP アドレス。ドット付き 10 進表記で示されます（たとえば、10.86.7.101）。

推奨アクション 不要。

334005

エラーメッセージ `%Threat Defense-5-334005: Host put into NAC Hold state - host-address`

説明ホストの NAC セッションが Hold 状態になりました。

- *host-address*：ホストの IP アドレス。ドット付き 10 進表記で示されます（たとえば、10.86.7.101）。

推奨アクション 不要。

334006

エラーメッセージ `%Threat Defense-5-334006: EAPoUDP failed to get a response from host - host-address`

説明ホストから EAPoUDP 応答を受信しませんでした。

- *host-address*：ホストの IP アドレス。ドット付き 10 進表記で示されます（たとえば、10.86.7.101）。

推奨アクション 不要。

334007

エラーメッセージ `%Threat Defense-6-334007: EAPoUDP association terminated - host-address`

説明ホストとの EAPoUDP アソシエーションが終了しました。

- *host-address*：ホストの IP アドレス。ドット付き 10 進表記で示されます（たとえば、10.86.7.101）。

推奨アクション 不要。

334008

エラーメッセージ `%Threat Defense-6-334008: NAC EAP association initiated - host-address , EAP context: EAP-context`

説明 EAPoUDP がホストとの EAP を開始しました。

- *host-address*：ホストの IP アドレス。ドット付き 10 進表記で示されます（たとえば、10.86.7.101）。
- *EAP-context*：EAP セッションの一意の識別子。8 桁の 16 進数として表示されます（たとえば、0x2D890AE0）。

推奨アクション 不要。

334009

エラーメッセージ `%Threat Defense-6-334009: Audit request for NAC Clientless host - Assigned_IP.`

説明指摘された割り当て済み IP アドレスの監査要求が送信されています。

- *Assigned_IP*：クライアントに割り当てられている IP アドレス

推奨アクション 不要。

336001

エラーメッセージ `%Threat Defense-3-336001 Route desination_network stuck-in-active state in EIGRP-ddb_name as_num. Cleaning up`

説明 SIA 状態とは、EIGRP ルータが指定された時間（約 3 分）以内に 1 つ以上の隣接ルータからクエリーに対する応答を受信できなかったことを意味します。この状態が発生した場合、

EIGRP は、応答を送信しなかった隣接ルータとの隣接関係を解消し、アクティブになったルートに関するエラー メッセージをログに記録します。

- *destination_network*：アクティブになったルート
- *ddb_name*：IPv4
- *as_num*：EIGRP ルータ

推奨アクション ルータが一部の隣接ルータから応答を受信しなかった原因、およびルートが消失した原因を確認します。

336002

エラーメッセージ `%Threat Defense-3-336002: Handle handle_id is not allocated in pool.`

説明 EIGRP ルータは、ネクスト ホップのハンドルを見つけることができません。

- *handle_id*：見つからないハンドルの ID

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。

336003

エラーメッセージ `%Threat Defense-3-336003: No buffers available for bytes byte packet`

説明 DUAL ソフトウェアが、パケット バッファを割り当てることができませんでした。Secure Firewall Threat Defense デバイス のメモリが不足している可能性があります。

- *bytes*：パケット内のバイト数

推奨アクション **show mem** または **show tech** コマンドを入力して、Secure Firewall Threat Defense デバイス のメモリが不足しているかどうかを確認します。問題が解決しない場合、Cisco TAC にお問い合わせください。

336004

エラーメッセージ `%Threat Defense-3-336004: Negative refcount in pakdesc pakdesc.`

説明 リファレンス カウントのパケット カウントが負になりました。

- *pakdesc*：パケット識別子

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。

336005

エラーメッセージ `%Threat Defense-3-336005: Flow control error, error , on interface_name.`

説明 インターフェイスでマルチキャストのフロー ブロックが発生しています。Qelm はキュー要素で、この場合は、この特定のインターフェイスのキューにある最後のマルチキャスト パケットです。

- *error*：エラー文：Qelm on flow ready
- *interface_name*：エラーが発生したインターフェイスの名前

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。

336006

エラーメッセージ `%Threat Defense-3-336006: num peers exist on IIDB interface_name.`

説明 EIGRP の IDB のクリーンアップ中またはクリーンアップ後、特定のインターフェイス上にピアがまだ存在しています。

- *num*：ピアの数
- *interface_name*：インターフェイス名

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

336007

エラーメッセージ `%Threat Defense-3-336007: Anchor count negative`

説明エラーが発生し、アンカーの解放時にアンカー カウントが負になりました。

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。

336008

エラーメッセージ `%Threat Defense-3-336008: Lingering DRDB deleting IIDB, dest network, nexthop address (interface), origin origin_str`

説明インターフェイスが削除されており、長期の DRDB が存在します。

- network：宛先ネットワーク
- address：ネクストホップ アドレス
- interface：ネクストホップ インターフェイス
- origin_str：発生元を定義する文字列

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

336009

エラーメッセージ `%Threat Defense-3-336009 ddb_name as_id: Internal Error`

説明内部エラーが発生しました。

- *ddb_name*：PDM 名（たとえば、IPv4 PDM）
- *as_id*：自律システム ID

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。

336010

エラーメッセージ `%Threat Defense-5-336010 EIGRP-ddb_name tableid as_id: Neighbor address (%interface) is event_msg: msg`

説明隣接ルータがアップまたはダウンしました。

- *ddb_name*：IPv4
- *tableid*：RIB の内部 ID
- *as_id*：自律システム ID
- *address*：隣接ルータの IP アドレス
- *interface*：インターフェイスの名前
- *event_msg*：隣接ルータで発生しているイベント（つまり、up または down）
- *msg*：イベントの原因。*event_msg* と *msg* の値ペアには次のものがあります。

- resync: peer graceful-restart

- down: holding timer expired

- up: new adjacency

- down: Auth failure

- down: Stuck in Active

- down: Interface PEER-TERMINATION received

- down: K-value mismatch

- down: Peer Termination received

- down: stuck in INIT state

- down: peer info changed

- down: summary configured

- down: Max hopcount changed

- down: metric changed

- down: [No reason]

推奨アクション隣接ルータのリンクがダウンまたはフラッピングしている原因を確認します。これは、問題の兆候である可能性があります。または、これが原因で問題が発生する可能性があります。

336011

エラーメッセージ `%Threat Defense-6-336011: event event`

説明デュアル イベントが発生しました。イベントは次のいずれかです。

- Redist rt change
- SIA Query while Active

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。

336012

エラーメッセージ `%Threat Defense-3-336012: Interface interface_names going down and neighbor_links links exist`

説明インターフェイスがダウンしているか、または IGRP 経由でルーティングから削除されていますが、すべてのリンク（ネイバー）がトポロジテーブルから削除されたわけではありません。

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

336013

エラーメッセージ `%Threat Defense-3-336013: Route iproute, iproute_successors successors, db_successors rdbs`

説明ハードウェアまたはソフトウェアのエラーが発生しました。

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

336014

エラーメッセージ `%Threat Defense-3-336014: "EIGRP_PDM_Process_name, event_log"`

説明ハードウェアまたはソフトウェアのエラーが発生しました。

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

336015

エラーメッセージ `%Threat Defense-3-336015: "Unable to open socket for AS as_number"`

説明ハードウェアまたはソフトウェアのエラーが発生しました。

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

336016

エラーメッセージ `%Threat Defense-3-336016: Unknown timer type timer_type expiration`

説明ハードウェアまたはソフトウェアのエラーが発生しました。

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

336019

エラーメッセージ `%Threat Defense-3-336019: process_name as_number: prefix_source threshold prefix level (prefix_threshold) reached`

説明トポロジデータベース内のプレフィックス数が、設定されたしきい値レベルまたはデフォルトのしきい値レベルに達しました。プレフィックスのソースは次のいずれかになります。

- Neighbor
- Redistributed
- Aggregate

推奨アクション **show eigrp accounting** コマンドを使用して、プレフィックスのソースの詳細情報を取得し、是正措置を実施します。

337000

エラーメッセージ `%Threat Defense-6-337000: Created BFD session with local discriminator <id> on <real_interface> with neighbor <real_host_ip>`

説明 この syslog メッセージは、BFD アクティブ セッションが作成されたことを示します。

- id：特定の BFD セッションのローカル識別子の値を示す数値フィールド
- real_interface：BFD セッションを実行しているインターフェイスの nameif
- real_host_ip：BFD セッションが確立されたネイバーの IP アドレス

推奨アクション なし。

337001

エラーメッセージ `%Threat Defense-6-337001: Terminated BFD session with local discriminator <id> on <real_interface> with neighbor <real_host_ip> due to <failure_reason>`

説明 この syslog メッセージは、アクティブな BFD セッションが終了したことを示します。

- id：特定の BFD セッションのローカル識別子の値を示す数値フィールド
- real_interface：BFD セッションを実行しているインターフェイスの nameif
- real_host_ip：BFD セッションが確立されたネイバーの IP アドレス
- failure_reason：次に示す障害の理由のいずれか：ピア側の BFD がダウンしている、ピア側の BFD 設定が削除されている、検出タイマーの期限切れ、エコー機能の障害、ピアまでのパスがダウンしている、ローカルの BFD 設定が削除されている、BFD クライアント設定が削除されている

推奨アクション なし。

337005

エラーメッセージ `%Threat Defense-4-337005: Phone Proxy SRTP: Media session not found for media_term_ip/media_term_port for packet from in_ifc:src_ip/src_port to out_ifc:dest_ip/dest_port`

説明 適応型セキュリティ アプライアンスでメディア終端 IP アドレスおよびポートを宛先とした SRTP/RTP パケットを受信したが、このパケットを処理するための対応するメディア セッションが見つかりませんでした。

- in_ifc：入力インターフェイス
- src_ip：パケットの送信元 IP アドレス

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

推奨アクション このメッセージがコールの最後に生成された場合、正常であると考えられます。シグナリング メッセージによりメディア セッションは解放された可能性がありますが、エンドポイントでは引き続きいくつかの SRTP または RTP パケットが送信されているためです。このメッセージが奇数のメディア終端ポートに対して生成された場合、エンドポイントではRTCPが送信されており、それをCUCMからディセーブルにする必要があります。このメッセージがコールに対して継続的に生成される場合は、電話プロキシ デバッグ コマンドまたは取り込みコマンドを使用してシグナリング メッセージ トランザクションをデバッグし、シグナリング メッセージがメディア終端 IP アドレスおよびポートで変更されているかどうかを確認します。

339006

エラーメッセージ `%Threat Defense-3-339006: Umbrella resolver current resolver ipv46 is reachable, resuming Umbrella redirect.`

説明 Umbrella が開くことに失敗し、リゾルバが到達不能でした。現時点では、レゾルバが到達可能になっており、サービスが再開されています。

推奨処置なし。

339007

エラーメッセージ `%Threat Defense-3-339007: Umbrella resolver current resolver ipv46 is unreachable, moving to fail-open. Starting probe to resolver.`

説明 Umbrella フェールオープンが設定されており、リゾルバの到達不能が検出されました。

推奨アクションUmbrella リゾルバへの到達可能性に関してネットワーク設定を確認します。

339008

エラーメッセージ `%Threat Defense-3-339008: Umbrella resolver current resolver ipv46 is unreachable, moving to fail-close.`

説明 Umbrella フェールオープンが設定されて「おらず」、リゾルバの到達不能が検出されました。

推奨アクションUmbrella リゾルバへの到達可能性に関してネットワーク設定を確認します。

340001

エラーメッセージ `%Threat Defense-3-340001: Loopback-proxy error: error_string context id context_id , context type = version /request_type /address_type client socket`

(internal)= *client_address_internal* /*client_port_internal* server socket (internal)= *server_address_internal* /*server_port_internal* server socket (external)= *server_address_external* /*server_port_external* remote socket (external)= *remote_address_external* /*remote_port_external*

説明ループ バック プロキシは、Secure Firewall Threat Defense デバイス で実行されているサードパーティ製アプリケーションがネットワークにアクセスすることを可能にします。ループバック プロキシでエラーが発生しました。

- *context_id*：各ループバック クライアント プロキシ要求に対して生成される一意の 32 ビット コンテキスト ID
- *version*：プロトコル バージョン
- *request_type*：要求タイプ。TC（TCP 接続）、TB（TCP バインド）、または UA（UDP アソシエーション）のいずれかです。
- *address_type*：アドレス タイプ、IP4（IPv4）、IP6（IPv6）、または DNS（ドメイン名サービス）のいずれかです。
- *client_address_internal*/*server_address_internal*：ループバック クライアントおよびループバック サーバーが通信に使用するアドレス
- *client_port_internal*/*server_port_internal*：ループバック クライアントおよびループバック サーバーが通信に使用するポート
- *server_address_external*/*remote_address_external*：ループバック サーバーとリモート ホストが通信に使用するアドレス
- *server_port_external*/*remote_port_external*：ループバック サーバーとリモート ホストが通信に使用するポート
- *error_string*：問題の解決に役立つエラー文字列

推奨アクション syslog メッセージをコピーし、Cisco TAC にお問い合わせください。

340002

エラーメッセージ %Threat Defense-6-340002: Loopback-proxy info: *error_string* context id *context_id* , context type = *version* /*request_type* /*address_type* client socket (internal)= *client_address_internal* /*client_port_internal* server socket (internal)= *server_address_internal* /*server_port_internal* server socket (external)= *server_address_external* /*server_port_external* remote socket (external)= *remote_address_external* /*remote_port_external*

説明ループ バック プロキシは、Secure Firewall Threat Defense デバイス で実行されているサードパーティ製アプリケーションがネットワークにアクセスすることを可能にします。ループバック プロキシは、トラブルシューティングで使用するデバッグ情報を生成しました。

- *context_id*：各ループバック クライアント プロキシ要求に対して生成される一意の 32 ビット コンテキスト ID
- *version*：プロトコル バージョン
- *request_type*：要求タイプ。TC（TCP 接続）、TB（TCP バインド）、または UA（UDP アソシエーション）のいずれかです。

- *address_type*：アドレス タイプ、IP4（IPv4）、IP6（IPv6）、またはDNS（ドメイン名サービス）のいずれかです。
- *client_address_internal/server_address_internal*：ループバック クライアントおよびループバック サーバーが通信に使用するアドレス
- *client_port_internal*/*server_port_internal*：ループバック クライアントおよびループバック サーバーが通信に使用するポート
- *server_address_external*/*remote_address_external*：ループバック サーバーとリモート ホストが通信に使用するアドレス
- *server_port_external*/*remote_port_external*：ループバック サーバーとリモート ホストが通信に使用するポート
- *error_string*：問題の解決に役立つエラー文字列

推奨アクション syslog メッセージをコピーし、Cisco TAC にお問い合わせください。

341001

エラーメッセージ `%Threat Defense-6-341001: Policy Agent started successfully for VNMC` *`vnmc_ip_addr`*

説明ポリシー エージェント プロセス（DME、ducatiAG および commonAG）が正常に開始されました。

- *vnmc_ip_addr*：VNMC サーバーの IP アドレス

推奨アクション なし。

341002

エラーメッセージ `%Threat Defense-6-341002: Policy Agent stopped successfully for VNMC` *`vnmc_ip_addr`*

説明ポリシー エージェント プロセス（DME、ducatiAG および commonAG）が停止しました。

- *vnmc_ip_addr*：VNMC サーバーの IP アドレス

推奨アクション なし。

341003

エラーメッセージ `%Threat Defense-3-341003: Policy Agent failed to start for VNMC` *`vnmc_ip_addr`*

説明ポリシー エージェントの開始に失敗しました。

- *vnmc_ip_addr*：VNMC サーバーの IP アドレス

推奨アクション コンソールの履歴やエラー メッセージの disk0:/pa/log/vnm_pa_error_status をチェックします。ポリシー エージェントの開始を再試行するには、**registration host** コマンドを再実行します。

341004

エラーメッセージ `%Threat Defense-3-341004: Storage device not available: Attempt to shutdown module %s failed.`

説明すべての SSD が失敗したか、アップ状態のシステムから削除されました。システムがソフトウェア モジュールをシャット ダウンしようとしましたが、失敗しました。

- *%s*：ソフトウェア モジュール（cxsc など）

推奨アクション削除されたか、障害が発生したドライブを交換し、Secure Firewall Threat Defense デバイス をリロードします。

341005

エラーメッセージ `%Threat Defense-3-341005: Storage device not available. Shutdown issued for module %s .`

説明すべての SSD が失敗したか、アップ状態のシステムから削除されました。システムがソフトウェア モジュールをシャット ダウンしています。

- *%s*：ソフトウェア モジュール（cxsc など）

推奨アクション 削除されたか、障害が発生したドライブを交換し、ソフトウェア モジュールをリロードします。

341006

Error Message `%Threat Defense-3-341006: Storage device not available. Failed to stop recovery of module %s .`

説明すべての SSD が失敗したか、リカバリ状態のシステムから削除されました。システムがリカバリを停止しようとしましたが、失敗しました。

- *%s*：ソフトウェア モジュール（cxsc など）

推奨アクション削除されたか、障害が発生したドライブを交換し、Secure Firewall Threat Defense デバイス をリロードします。

341007

エラーメッセージ `%Threat Defense-3-341007: Storage device not available. Further recovery of module %s was stopped. This may take several minutes to complete.`

説明 すべての SSD に障害が発生したか、リカバリ状態のシステムから削除されました。システムはソフトウェア モジュールのリカバリを中断します。

- *%s*：ソフトウェア モジュール（cxsc など）

推奨アクション 削除されたか、障害が発生したドライブを交換し、ソフトウェア モジュールをリロードします。

341008

エラーメッセージ `%Threat Defense-3-341008: Storage device not found. Auto-boot of module %s cancelled. Install drive and reload to try again.`

説明 システムをアップ状態にした後、すべての SSD に障害が発生したか、システムをリロードする前に削除されました。ブート中のデフォルト動作ではソフトウェア モジュールが自動ブートされますが、利用可能なストレージ デバイスがないため、その動作がブロックされます。

推奨アクション 削除されたか、障害が発生したドライブを交換し、ソフトウェア モジュールをリロードします。

341010

エラーメッセージ `%Threat Defense-6-341010: Storage device with serial number ser_no [inserted into | removed from] bay bay_no`

説明 Secure Firewall Threat Defense デバイス が挿入または削除のイベントを検出し、この syslog メッセージをすぐに生成します。

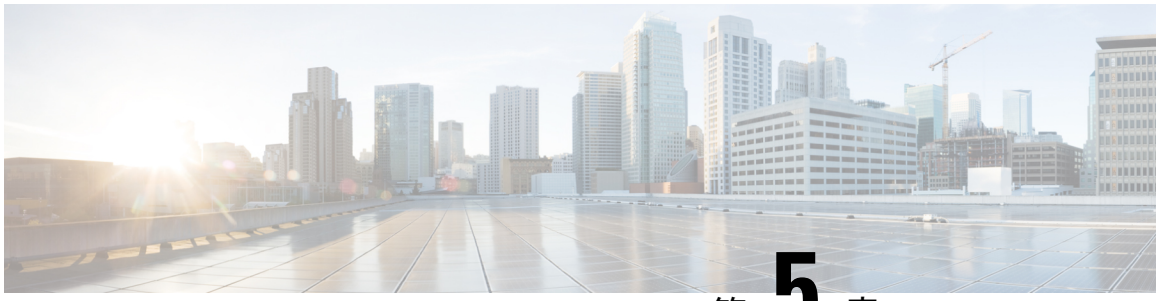
推奨アクション 不要。

341011

エラーメッセージ `%Threat Defense-3-341011: Storage device with serial number ser_no in bay bay_no faulty.`

説明 Secure Firewall Threat Defense デバイス は 10 分ごとにハード ディスク ドライブ（HDD）のヘルス ステータスをポーリングし、HDD が障害状態の場合は、この syslog メッセージを生成します。

推奨アクション 不要。



第 5 章

Syslog メッセージ 401001 ～ 450001

この章は、次の項で構成されています。

メッセージ 401001 ～ 409128

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

401001

エラーメッセージ `%Threat Defense-4-401001: Shuns cleared`

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

推奨アクション 不要。

401002

エラーメッセージ `%Threat Defense-4-401002: Shun added: IP_address` *IP_address* `port` *port*

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

推奨アクション 不要。

401003

エラーメッセージ `%Threat Defense-4-401003: Shun deleted:` *IP_address*

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

推奨アクション 不要。

401004

エラーメッセージ `%Threat Defense-4-401004: Shunned packet: IP_address = IP_address on interface interface_name`

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

推奨アクション必要なし。

401005

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

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

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

402114

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

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

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

推奨アクション ローカル SA が消去されたことを、ピアは認識していないことがあります。新しい接続がローカル ルータから確立された場合、2 つのピアが正常に接続を再度確立すること

があります。あるいは、問題の発生が短期間にとどまらない場合は、接続を新規に確立してみるか、またはピアの管理者に問い合わせます。

402115

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

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

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

推奨アクション ピアの管理者にお問い合わせください。

402116

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

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

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

- id_saddr>：リモート プロキシ IP アドレス
- id_smask>：リモート プロキシ IP サブネット マスク
- id_sprot>：リモート プロキシ トランスポート プロトコル
- id_sport>：リモート プロキシ ポート

推奨アクション ピアの管理者に問い合わせて、ポリシーの設定を比較します。

402117

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

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

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

推奨アクション ピアの管理者に問い合わせて、ポリシーの設定を比較します。

402118

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

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

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

- local_IP>：トンネルのローカル エンドポイントの IP アドレス
- frag_len>：IP フラグメント長
- frag_offset>：IP フラグメント オフセット（バイト）

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

402119

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

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

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

推奨アクション ピアの管理者にお問い合わせください。

402120

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

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

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

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

402121

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

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

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

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

402122

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

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

- *src_addr* >：送信元 IP アドレス
- *dest_addr* >：宛先 > IP アドレス
- drop_reason>：パケットがドロップされた原因

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。

402123

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

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

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

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

402124

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

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

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

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

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

402125

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

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

- >*ring*：IPSEC リングまたは Admin リング
- *parameters* >：次のとおり

- Desc>：記述子アドレス

- CtrlStat>：制御/ステータス値

- ResultP>：成功ポインタ

- ResultVal>：成功値

- Cmd>：暗号コマンド

- CmdSize>：コマンド サイズ

- Param>：コマンド パラメータ

- Dlen>：データ長

- DataP>：データ ポインタ

- CtxtP>：VPN コンテキスト ポインタ

- SWReset>：ブート後の暗号チップ リセット回数

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

402126

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

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

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

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

402127

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

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

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

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

402128

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

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

- *size*：割り当てられているメモリ ブロックのサイズ
- *limit*：許容割り当てメモリの最大サイズ

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

402129

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

説明内部ソフトウェア エラーが発生しました。

- *address*：解放されようとしたアドレス

推奨アクション Cisco TAC に連絡してサポートを受けてください。

402130

エラーメッセージ `%Threat Defense-6-402130: CRYPTO: Received an ESP packet (SPI = xxxxxxxxxx, sequence number=xxxx) from 172.16.0.1 (user=user) to 192.168.0.2 with incorrect IPsec padding.`

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

- *SPI*：パケットに関連付けられている SPI
- *sequence number*：パケットに関連付けられているシーケンス番号

- *user*：ユーザー名文字列
- *padding*：パケットからの埋め込みデータ

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

402131

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

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

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

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

402140

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

説明 RSA 公開キー ペアの生成時にエラーが発生しました。

- *len*：ビット単位で示したプライム モジュラスの長さ

推奨アクション Cisco TAC に連絡してサポートを受けてください。

402141

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

説明 RSA 公開キー ペアの生成時にエラーが発生しました。

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

推奨アクション Cisco TAC に連絡してサポートを受けてください。

402142

エラーメッセージ `%Threat Defense-3-402142: CRYPTO: Bulk data op error: algorithm alg , mode mode`

説明対称キー操作中にエラーが発生しました。

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

推奨アクション Cisco TAC に連絡してサポートを受けてください。

402143

エラーメッセージ `%Threat Defense-3-402143: CRYPTO: alg type key op`

説明非対称キー操作中にエラーが発生しました。

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

推奨アクション Cisco TAC に連絡してサポートを受けてください。

402144

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

説明デジタル署名の生成中にエラーが発生しました。

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

推奨アクション Cisco TAC に連絡してサポートを受けてください。

402145

エラーメッセージ `%Threat Defense-3-402145: CRYPTO: Hash generation error: algorithm hash`

説明ハッシュ生成エラーが発生しました。

- *hash*：ハッシュ アルゴリズム。MD5、SHA1、SHA256、SHA384、SHA512 のいずれかです。

推奨アクション Cisco TAC に連絡してサポートを受けてください。

402146

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

説明キー付きハッシュ生成エラーが発生しました。

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

推奨アクション Cisco TAC に連絡してサポートを受けてください。

402147

エラーメッセージ `%Threat Defense-3-402147: CRYPTO: HMAC generation error: algorithm alg`

説明 HMAC の生成エラーが発生しました。

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

推奨アクション Cisco TAC に連絡してサポートを受けてください。

402148

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

説明乱数ジェネレータ エラーが発生しました。

推奨アクション Cisco TAC に連絡してサポートを受けてください。

402149

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

説明 Secure Firewall Threat Defense デバイス は 2048 ビット未満の RSA キー、または DH グループ 1、2、5 を使おうとしました。

- *encryption type*：暗号化のタイプ
- *length*：RSA キーの長さ、または DH グループの番号

推奨アクション 2048 ビット以上の RSA キーを使うように、または 1、2、5 以外の DH グループを設定するように Secure Firewall Threat Defense デバイス または外部アプリケーションを設定します。

402150

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

説明 デジタル証明書の署名、または FIPS 140-2 認証の検証に、受け入れられないハッシュ アルゴリズムが使われました。

- *operation*：署名または検証
- *hash alg*：受け入れられないハッシュ アルゴリズムの名前

推奨アクション 少なくともデジタル証明書の署名または FIPS 140-2 認証の検証には受け入れられるハッシュ アルゴリズムを使っていることを確認します。これらには、SHA-256、SHA-384、SHA-512 があります。

403500

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

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

推奨アクション 不要。

403501

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

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

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

403502

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

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

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

403503

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

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

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

403504

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

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

次に例を示します。

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

推奨アクション PPPoE 用の VPDN グループを設定します。

403505

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

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

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

403506

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

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

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

403507

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

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

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

推奨アクション：次のステップを実行します。

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

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

405001

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

説明 Secure Firewall Threat Defense デバイス が ARP パケットを受信しましたが、パケットの MAC アドレスが ARP キャッシュ エントリと異なっています。

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

405002

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

説明 このパケットは、次のどちらかの条件の場合に表示されます。

- Secure Firewall Threat Defense デバイスは IP アドレスが同じだが、MAC アドレスがその uauth エントリの 1 つとは異なるパケットを受信しました。
- Secure Firewall Threat Defense デバイス に **vpnclient mac-exempt** コマンドを設定しました。除外 MAC アドレスを持つが、対応する uauth エントリとは異なる IP アドレスを持つパケットが Secure Firewall Threat Defense デバイス によって受信されました。

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

405003

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

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

推奨アクション クライアントの IP アドレスを変更します。

405101

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

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

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

405102

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

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

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

405103

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

説明 Secure Firewall Threat Defense デバイス はプロトコル識別子 0x08 を予測していますが、0x08 以外の識別子を受信しました。エンドポイントから不良パケットが送信されているか、または最初のセグメント以外のメッセージセグメントを受信した可能性があります。パケットの通過は許可されます。

推奨アクション 不要。

405104

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

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

推奨アクション 不要。

405105

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

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

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

406001

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

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

推奨アクション 不要。

406002

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

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

推奨アクション 不要。

407001

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

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

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

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

表 *11* : タイムアウトおよび推奨値

タイムアウト	推奨値
xlate	00:05:00（5 分）
conn	00:01:00（1 時間）
uauth	00:05:00（5 分）

407002

エラーメッセージ `%Threat Defense-4-407002: Embryonic limit nconns /elimit for through connections exceeded.outside_address /outside_port to global_address (inside_address )/inside_port on interface interface_name`

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

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

407003

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

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

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

408001

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

説明 IP ルート カウンタを負の値に減少しようとしましたが失敗しました。

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

408002

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

説明既存のルートよりも適切なメトリックを持つ同じ距離の別のインターフェイスからネットワークアップデートを受信しました。新規のルートによって、別のインターフェイスを使用してインストールされた既存のルートが上書きされます。新規のルートは冗長目的に限り使用され、ネットワーク内でパスが移動されたことを意味します。この変更は、トポロジと再配布を使用して制御する必要があります。この変更の影響を受ける既存の接続は、ディセーブルにされる可能性があり、タイムアウトになります。このパスの移動は、パス冗長をサポートするようにネットワークトポロジが特に設計されている場合（このケースが予測されます）に限り発生します。

推奨アクション 不要。

408003

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

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

- *hex*：メモリ内の変数値またはアドレスを示す 16 進値

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

408101

エラーメッセージ `%Threat Defense-4-408101: KEYMAN : Type encrption_type encryption unknown. Interpreting keystring as literal.`

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

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

408102

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

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

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

409001

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

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

推奨アクション 不要。

409002

エラーメッセージ `%Threat Defense-4-409002: db_free: external LSA IP_address netmask`

説明内部ソフトウェア エラーが発生しました。

推奨アクション 不要。

409003

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

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

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

409004

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

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

推奨アクション 不要。

409005

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

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

推奨アクション 隣接アドレスから問題のルータを特定しリブートします。

409006

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

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

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

409007

エラーメッセージ `%Threat Defense-4-409007: Found LSA with the same host bit set but using different mask LSA ID IP_address netmask New: Destination IP_address netmask`

説明 内部ソフトウェア エラーが発生しました。

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

409008

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

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

推奨アクション 表示されているとおりにメッセージをコピーして、Cisco TAC に報告してください。

409009

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

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

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

409010

エラーメッセージ `%Threat Defense-4-409010: Virtual link information found in non-backbone area: string`

説明 内部エラーが発生しました。

推奨アクション 表示されているとおりにメッセージをコピーして、Cisco TAC に報告してください。

409011

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

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

推奨アクション OSPF ルータ ID を固有のものにしてください。隣接ルータのルータ ID を変更します。

409012

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

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

推奨アクション OSPF ルータ ID を固有のものにしてください。隣接ルータのルータ ID を変更します。

409013

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

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

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

409014

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

説明 インターフェイスで設定されている認証キーが無効です。

推奨アクション 新しいキーを設定します。

409015

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

説明 設定されたキーチェーンで ID が見つかりません。

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

409016

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

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

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

409017

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

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

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

409023

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

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

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

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

409101

エラーメッセージ `%Threat Defense-4-409101: Received invalid packet: s from P , s`

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

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

409102

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

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

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

409103

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

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

推奨アクション 不要。

409104

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

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

推奨アクション 不要。

409105

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

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

推奨アクション 隣接アドレスから、問題のルータを特定し以下を実行します。

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

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

409106

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

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

推奨アクション 不要。

409107

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

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

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

409108

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

説明内部エラーが発生しました。

推奨アクション 不要。

409109

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

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

推奨アクション ネイバー ルータ ID を変更します。

409110

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

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

推奨アクション ネイバー ルータ ID を変更します。

409111

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

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

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

409112

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

説明 内部エラーが発生しました。

推奨アクション 不要。

409113

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

説明 内部エラーが発生しました。

推奨アクション 不要。

409114

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

説明 内部エラーが発生しました。

推奨アクション 不要。

409115

エラーメッセージ `%Threat Defense-4-409115: Unrecognized timer d in OSPF s`

説明 内部エラーが発生しました。

推奨アクション 不要。

409116

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

説明内部エラーが発生しました。

推奨アクション 不要。

409117

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

説明内部エラーが発生しました。

推奨アクション 不要。

409118

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

説明内部エラーが発生しました。

推奨アクション 不要。

409119

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

説明内部エラーが発生しました。

推奨アクション必要なし。

409120

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

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

推奨アクション 1 つのプロセスに対して別のルータ ID を設定します。

409121

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

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

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

409122

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

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

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

409123

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

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

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

409125

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

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

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

409128

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

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

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

メッセージ 410001 ～ 450001

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

410001

エラーメッセージ `%Threat Defense-4-410001: UDP DNS request from source_interface :source_address /source_port to dest_interface :dest_address /dest_port ; (label length | domain-name length) 52 bytes exceeds remaining packet length of 44 bytes.`

説明 UDP DNS パケットのドメイン名の長さが、255 バイトを超えています。詳細については、RFC 1035 の 3.1 項を参照してください。

推奨アクション 不要。

411001

エラーメッセージ `%Threat Defense-4-411001: Line protocol on interface interface_name changed state to up`

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

推奨アクション 不要。

411002

エラーメッセージ `%Threat Defense-4-411002:Line protocol on interface interface_name changed state to down`

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

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

411003

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

説明インターフェイスのコンフィギュレーション ステータスが、ダウンからアップに変更されました。

推奨アクション これが予期しないイベントの場合、物理回線を確認します。

411004

エラーメッセージ `%Threat Defense-4-411004: Configuration status on interface interface_name changed state to up`

説明インターフェイスのコンフィギュレーション ステータスが、ダウンからアップに変更されました。

推奨アクション 不要。

411005

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

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

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

推奨アクション 不要。

412001

エラーメッセージ `%Threat Defense-4-412001:MAC MAC_address moved from interface_1 to interface_2`

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

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

412002

エラーメッセージ `%Threat Defense-4-412002:Detected bridge table full while inserting MAC MAC_address on interface interface . Number of entries = num`

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

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

413001

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

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

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

413002

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

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

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

413003

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

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

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

413004

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

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

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

- write failure

- failed to create a thread to write the image

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

413005

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

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

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

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

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

413006

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

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

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

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

414001

エラーメッセージ `%Threat Defense-3-414001: Failed to save logging buffer using file name filename to FTP server ftp_server_address on interface interface_name : [fail_reason ]`

説明ロギング モジュールによる外部 FTP サーバーへのロギング バッファの保存が失敗しました。

推奨アクション 失敗した原因に基づいて適切な処置を行います。

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

414002

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

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

推奨アクション十分な領域がないために失敗した場合は、フラッシュの空き領域をチェックして、**logging flash-size** コマンドの設定制限が正しく設定されていることを確認します。エラーが、フラッシュ ファイル システムの I/O エラーの場合は、Cisco TAC に問い合わせてサポートを受けてください。

414003

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

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

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

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

414005

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

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

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

推奨アクション 不要。

414006

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

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

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

415020

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

説明非 ASCII 文字が見つかりました。

- **matched_string**：次のいずれかの一致文字列

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

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

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

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

417001

エラーメッセージ `%Threat Defense-4-417001: Unexpected event received: number`

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

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

417004

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

説明クライアントが、自分が所有していないルート属性を修正しようとしました。

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。

417006

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

説明メモリ不足のために動作が失敗しましたが、別のメカニズムで処理されます。

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

418001

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

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

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

推奨アクション このようなパケットを生成している個人と理由を特定します。

419001

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

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

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

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

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

419002

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

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

- **in_interface**：入力インターフェイス
- **src_address**：パケットの送信元 IP アドレス

- **src_port**：パケットの送信元ポート
- **out_interface**：出力インターフェイス
- **dest_address**：パケットの宛先 IP アドレス
- **dest_port**：パケットの宛先ポート

推奨アクション 不要。

419003

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

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

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

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

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

説明この syslog は、緊急フラグまたは tcp パケットの緊急ポインタがクリアされたときに表示されます。これは、ユーザー コンフィギュレーション（tcp-map）が原因で生じるか、または TCP パケットに緊急ポインタの値は設定されているが緊急フラグは設定されていない場合に生じることがあります。

推奨アクション tcp-map コンフィギュレーションで、緊急フラグをクリアするように設定されているかどうか確認します。

419004

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

説明

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

推奨アクションなし。

419005

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

説明

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

推奨アクションなし。

419006

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

説明

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

推奨アクションなし。

421005

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

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

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

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

421007

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

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

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

- **application**：CSC SSM

推奨アクション サービス モジュールで問題を特定します。

422004

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

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

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

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

422005

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

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

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

422006

エラーメッセージ `%Threat Defense-4-422006: IP SLA Monitor Probe number : string`

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

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

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

424001

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

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

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

推奨アクション 拒否されたパケットの送信元を特定します。

424002

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

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

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

推奨アクション 拒否されたパケットの送信元を特定します。

425001

エラーメッセージ `%Threat Defense-6-425001 Redundant interface redundant _interface_name created.`

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

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

推奨アクション 不要。

425002

エラーメッセージ `%Threat Defense-6-425002 Redundant interface redundant _interface_name removed.`

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

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

推奨アクション 不要。

425003

エラーメッセージ `%Threat Defense-6-425003 Interface interface_name added into redundant interface redundant _interface_name .`

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

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

推奨アクション 不要。

425004

エラーメッセージ `%Threat Defense-6-425004 Interface interface_name removed from redundant interface redundant _interface_name .`

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

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

推奨アクション 不要。

425005

エラーメッセージ `%Threat Defense-5-425005 Interface interface_name become active in redundant interface redundant _interface_name`

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

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

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

推奨アクション メンバー インターフェイスのステータスを確認します。

425006

エラーメッセージ `%Threat Defense-3-425006 Redundant interface redundant _interface_name switch active member to interface_name failed.`

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

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

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

426001

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

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

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

推奨アクション 不要。

426002

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

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

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

推奨アクション 不要。

426003

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

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

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

推奨アクション 不要。

426004

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

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

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

- *ifc_name*：ポート チャネルに追加しようとしているインターフェイス
- *ifc name1*：ポート チャネル中にすでに存在しバンドル状態になっているインターフェイス

推奨アクション 次のいずれかを実行します。

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

426101

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

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

推奨アクション 不要。

426102

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

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

推奨アクション 不要。

426103

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

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

推奨アクション 不要。

426104

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

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

推奨アクション 不要。

428002

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

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

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

429008

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

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

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

推奨アクション 不要。

430001

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

これとその他のセキュリティイベントに関するメッセージの詳細については、セキュリティイベントの Syslog メッセージ （1 ページ）を参照してください。

430002

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

これとその他のセキュリティイベントに関するメッセージの詳細については、セキュリティイベントの Syslog メッセージ （1 ページ）を参照してください。

430003

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

これとその他のセキュリティイベントに関するメッセージの詳細については、セキュリティイベントの Syslog メッセージ （1 ページ）を参照してください。

430004

このメッセージ番号はリリース 6.4 で導入されました。これによってファイルイベントが識別されます。ファイルマルウェアイベントについては、430005 （225 ページ）も参照してください。

これとその他のセキュリティイベントに関するメッセージの詳細については、セキュリティイベントの Syslog メッセージ （1 ページ）を参照してください。

430005

このメッセージ番号はリリース 6.4 で導入されました。これによってマルウェアイベントが識別されます。ファイルイベントについては、430004 （224 ページ）も参照してください。

これとその他のセキュリティイベントに関するメッセージの詳細については、セキュリティイベントの Syslog メッセージ （1 ページ）を参照してください。

4302310

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

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

- **packet init/init-ack**：hostname パラメータを含んでいるメッセージ
- **src-ifc**：入力インターフェイスを示す
- **src-ip/src-port**：パケットの送信元 IP とポートを示す
- **dst-ifc**：出力インターフェイスを示す
- **dst_ip/dst_port**：パケットの宛先 IP とポートを示す

推奨アクションホスト名ではなく、エンドポイントの実際の IP アドレスを使用します。hostname パラメータをディセーブルにします。

434001

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

説明 モジュールのフェールクローズ設定のためにパケットがドロップされました。fail-close 設定はモジュールがダウンしている場合にすべてのフローを廃棄するように設計されているため、モジュールにフローをリダイレクトすることで、すべてのフローの接続が失われます。

推奨アクション障害の理由を理解し、サービスを復元してください。また、カードがすぐに回復しない場合は、fail-open オプションを使用できます。fail-open 設定では、カードのステータスがダウンの場合、モジュールに送られるパケットがすべてバイパスされます。

434004

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

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

推奨アクション 不要。

446003

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

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

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

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

447001

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

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

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

推奨アクション キューがいっぱいの状態は、CP に対する負荷が CP 処理能力を超えていることを示します。これは、一時的な状態の場合もあれば、そうでない場合もあります。このメッセージが繰り返し表示される場合は、CP に対する機能負荷を軽減することを検討してください。**show asp event dp-cp** コマンドを使用して、イベント キューの負荷に最も影響を及ぼしている機能を特定できます。

448001

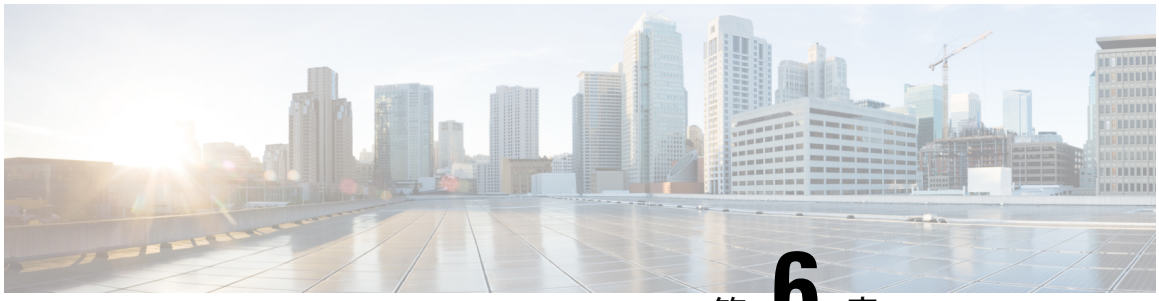
エラーメッセージ `%Threat Defense-4-448001: Denied SRTP crypto session setup on flow from src_int :src_ip /src_port to dst_int :dst_ip /dst_port , licensed K8 SRTP crypto session of limit exceeded`

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

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

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

448001



第 6 章

Syslog メッセージ 500001 ～ 520025

この章は、次の項で構成されています。

メッセージ 500001 ～ 504002

この章では、500001 ～ 504002 のメッセージについて説明します。

500001

エラーメッセージ `%FTD>-5-500001: ActiveX content in java script is modified: src` *`src ip`* `dest` *`dest ip`* `on interface` *`interface name`*

説明ポリシー（Java のフィルタ（または）ActiveX のフィルタ）が Secure Firewall Threat Defense デバイス で有効になっているときに Java スクリプトに存在する Java/ActiveX コンテンツを確実にブロックします。

推奨アクション 不要。

500002

エラーメッセージ `%FTD>-5-500002: Java content in java script is modified: src` *`src ip`* `dest` *`dest ip`* `on interface` *`interface name`*

説明ポリシー（Java のフィルタ（または）ActiveX のフィルタ）が Secure Firewall Threat Defense デバイス で有効になっているときに Java スクリプトに存在する Java/ActiveX コンテンツを確実にブロックします。

推奨アクション 不要。

500003

エラーメッセージ `%FTD>-5-500003: Bad TCP hdr length (hdrlen=bytes , pktlen=bytes ) from source_address /source_port to dest_address /dest_port , flags: tcp_flags , on interface interface_name`

説明 TCP 内のヘッダー長に誤りがありました。一部のオペレーティング システムは、ディセーブル状態のソケットへの接続要求に応答するときに、TCP リセット（RST）を正しく処理しません。クライアントがSecure Firewall Threat Defense デバイスの外側にある FTP サーバーに接続しようとしたときに、FTP サーバーがリスニングしていない場合、FTP サーバーは RST を送信します。一部のオペレーティング システムは誤った TCP ヘッダー長を送信します。このために、問題が発生します。UDP は、ICMP ポート到達不能メッセージを使用します。

TCP ヘッダー長は、パケット長よりも長いことを示す場合があります。このために、負のバイト数が転送されます。負の数値は、メッセージでは符号なし数値として表示されます。このために、正常の場合よりも非常に大きな値が表示されます。たとえば、1 秒に 4 GB 転送されたことを示す場合があります。このメッセージは、まれに発生します。

推奨アクション 不要。

500004

エラーメッセージ `%FTD>-4-500004: Invalid transport field for protocol=protocol , from source_address /source_port to dest_address /dest_port`

説明 無効なトランスポート番号が使用されました。この場合、プロトコルの送信元または宛先のポート番号はゼロです。**protocol** 値は、TCP の場合は 6、UDP の場合は 17 です。

推奨アクション メッセージがその後も表示される場合は、ピアの管理者にお問い合わせください。

500005

エラーメッセージ `%FTD>-3-500005: connection terminated for protocol from in_ifc_name :src_adddress /src_port to out_ifc_name :dest_address /dest_port due to invalid combination of inspections on same flow. Inspect inspect_name is not compatible with filter filter_name .`

説明 接続が 1 つまたは複数の検査と一致したか、または同じ接続には適用できない 1 つまたは複数のフィルタ機能と一致しました（あるいはその両方と一致しました）。

- *protocol*：接続で使用されていたプロトコル
- *in_ifc_name*：入力インターフェイス名
- *src_address*：接続の送信元 IP アドレス
- *src_port*：接続の送信元ポート
- *out_ifc_name*：出力インターフェイス名
- *dest_address*：接続の宛先 IP アドレス
- *dest_port*：パケットの宛先ポート
- *inspect_name*：検査またはフィルタ機能名

• *filter_name*：フィルタ機能名

推奨アクション接続に対して一致する、対象の検査またはフィルタ機能（あるいはその両方）の要因となる **class-map**、**policy-map**、**service-policy**、または **filter** コマンドの組み合わせのコンフィギュレーションを確認します。接続に対する検査およびフィルタ機能の組み合わせの規則は次のとおりです。

- • **inspect http [http-policy-map]**、**filter url**、**filter java**、または **filter activex** コマンドの任意の組み合わせは有効です。
  • **inspect ftp [ftp-policy-map]** または **filter ftp** コマンド、あるいはその組み合わせは有効です。
  • **filter https** コマンドと他の **inspect** コマンドまたは **filter** コマンドの組み合わせは無効です。

上記の組み合わせ以外の他の検査またはフィルタ機能の組み合わせはすべて無効です。

501101

エラーメッセージ `%FTD>-5-501101: User transitioning priv level`

説明コマンドの特権レベルが変更されました。

推奨アクション 不要。

502101

エラーメッセージ `%FTD>-5-502101: New user added to local dbase: Uname: user Priv: privilege_level Encpass: string`

説明ユーザー名、特権レベル、および暗号化されたパスワードを含む新しいユーザー名レコードが作成されました。

推奨アクション 不要。

502102

エラーメッセージ `%FTD>-5-502102: User deleted from local dbase: Uname: user Priv: privilege_level Encpass: string`

説明ユーザー名、特権レベル、および暗号化されたパスワードを含むユーザー名レコードが削除されました。

推奨アクション 不要。

502103

エラーメッセージ `%FTD>-5-502103: User priv level changed: Uname: user From: privilege_level To: privilege_level`

説明ユーザーの特権レベルが変更されました。

推奨アクション 不要。

502111

エラーメッセージ `%FTD>-5-502111: New group policy added: name: policy_name Type: policy_type`

説明 **group-policy** CLI コマンドを使用してグループ ポリシーが設定されました。

- **policy_name**：グループ ポリシーの名前
- **policy_type**：internal または external

推奨アクション 不要。

502112

エラーメッセージ `%FTD>-5-502112: Group policy deleted: name: policy_name Type: policy_type`

説明 **group-policy** CLI コマンドを使用してグループ ポリシーが削除されました。

- **policy_name**：グループ ポリシーの名前
- **policy_type**：internal または external

推奨アクション 不要。

503001

エラーメッセージ `%FTD-5-503001: Process number, Nbr IP_address on interface_name from string to string , reason`

説明 OSPFv2 ネイバーの状態が変化しました。このメッセージには、変更およびその理由が記述されています。このメッセージは、OSPF プロセスに **log-adjacency-changes** コマンドが設定された場合にだけ表示されます。

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

503002

エラーメッセージ `%FTD-5-503002: The last key has expired for interface nameif, packets sent using last valid key.`

説明 現在のシステム時間を含むライフタイムを持つセキュリティ アソシエーションはありません。

推奨アクション 新しいセキュリティ アソシエーションを設定するか、現在のセキュリティ アソシエーションのライフタイムを変更します。

503003

エラーメッセージ `%FTD-5-503003: Packet sent | received on interface nameif with expired Key ID key-id.`

説明 インターフェイスで設定されたキー ID の有効期限が切れました。

推奨アクション 新しいキーを設定します。

503004

エラーメッセージ `%FTD-5-503004: Key ID key-id in key chain key-chain-name does not have a key.`

説明 OSPF は暗号化認証を使用するように設定されていますが、キーまたはパスワードが設定されていません。

推奨アクション 新しいセキュリティ アソシエーションを設定するか、現在のセキュリティ アソシエーションのライフタイムを変更します。

503005

エラーメッセージ `%FTD-5-503005: Key ID key-id in key chain key-chain-name does not have a cryptographic algorithm.`

説明 OSPF は暗号化認証を使用するように設定されていますが、アルゴリズムが設定されていません。

推奨アクション セキュリティ アソシエーションの暗号化アルゴリズムを設定します。

503101

エラーメッセージ `%FTD>-5-503101: Process d , Nbr i on s from s to s , s`

説明 OSPFv3 ネイバーの状態が変化しました。このメッセージには、変更およびその理由が記述されています。このメッセージは、OSPF プロセスに **log-adjacency-changes** コマンドが設定された場合にだけ表示されます。

推奨アクション 不要。

504001

エラーメッセージ `%FTD>-5-504001: Security context context_name was added to the system`

説明セキュリティ コンテンツが Secure Firewall Threat Defense デバイス に正常に追加されました。

推奨アクション 不要。

504002

エラーメッセージ `%FTD>-5-504002: Security context context_name was removed from the system`

説明セキュリティ コンテンツが Secure Firewall Threat Defense デバイス から正常に削除されました。

推奨アクション 不要。

メッセージ 505001 ～ 520025

この章では、505001 ～ 520025 のメッセージについて説明します。

505001

エラーメッセージ `%FTD>-5-505001: Module string one is shutting down. Please wait...`

説明 モジュールをシャット ダウンしています。

推奨アクション 不要。

505002

エラーメッセージ `%FTD>-5-505002: Module ips is reloading. Please wait...`

説明 IPS モジュールをリロードしています。

推奨アクション 不要。

505003

エラーメッセージ `%FTD>-5-505003: Module string one is resetting. Please wait...`

説明 モジュールはリセットされます。

推奨アクション 不要。

505004

エラーメッセージ `%FTD>-5-505004: Module string one shutdown is complete.`

説明モジュールはシャット ダウンされました。

推奨アクション 不要。

505005

エラーメッセージ `%FTD>-5-505005: Module module_name is initializing control communication. Please wait...`

説明 モジュールが検出され、そのモジュールとの制御チャネルの通信を Secure Firewall Threat Defense デバイス が初期化しています。

推奨アクション 不要。

505006

エラーメッセージ `%FTD>-5-505006: Module string one is Up.`

説明モジュールが制御チャネルの初期化を完了して、UP 状態です。

推奨アクション 不要。

505007

エラーメッセージ `%FTD>-5-505007: Module module_id is recovering. Please wait...`

エラーメッセージ `%FTD>-5-505007: Module prod_id in slot slot_num is recovering. Please wait...`

説明 **sw-module module** *service-module-name* **recover boot** コマンドを使用してソフトウェア モジュールを回復中であるか、**hw-module module** *slotnum* **recover boot** コマンドを使用してハードウェア モジュールを回復中です。

- **module_id**：ソフトウェア サービス モジュールの名前。
- **prod_id**：製品 ID 文字列。
- *slot_num*：ハードウェア サービス モジュールが搭載されているスロット。スロット 0 はシステムのメイン ボードを示し、スロット 1 は拡張スロットに設置されているモジュールを示します。

推奨アクション 不要。

505008

エラーメッセージ `%FTD>-5-505008: Module module_id software is being updated to newver (currently ver )`

エラーメッセージ `%FTD>-5-505008: Module` *module_id* in slot *slot_num* software is being updated to *newver* (currently *ver*)

説明サービス モジュール ソフトウェアのアップグレード中です。アップデートは正常に進行中です。

- *module_id*：ソフトウェア サービス モジュールの名前
- *slot_num*：ハードウェア サービス モジュールが搭載されているスロット番号

- >*newver*：モジュールへの書き込みが正常に終了しなかったソフトウェアの新しいバージョン番号（1.0(1)0 など）
- >*ver*：モジュール上のソフトウェアの現在のバージョン番号（1.0(1)0 など）

推奨アクション 不要。

505009

エラーメッセージ `%FTD>-5-505009: Module string one software was updated to newver`

説明 4GE SSM モジュール ソフトウェアは正常にアップグレードされました。

- *string one*：モジュールを示すテキスト文字列
- *newver*：モジュールへの書き込みが正常に終了しなかったソフトウェアの新しいバージョン番号（1.0(1)0 など）
- *ver*：モジュール上のソフトウェアの現在のバージョン番号（1.0(1)0 など）

推奨アクション 不要。

505010

エラーメッセージ `%FTD>-5-505010: Module in slot slot removed.`

説明 SSM が Secure Firewall Threat Defense デバイス のシャーシから削除されました。

- **slot**：SSM が取り外されたスロット

推奨アクション 不要。

505011

エラーメッセージ `%FTD>-1-505011: Module ips , data channel communication is UP.`

説明データ チャネル通信がダウン状態から回復しました。

推奨アクション 不要。

505012

エラーメッセージ `%FTD>-5-505012: Module module_id , application stopped application , version version`

エラーメッセージ `%FTD>-5-505012: Module prod_id in slot slot_num , application stopped application , version version`

説明アプリケーションが停止するか、サービスモジュールから削除されました。これは、サービス モジュールがアプリケーションをアップグレードした場合、あるいはサービス モジュール上のアプリケーションが停止またはアンインストールされた場合に発生する可能性があります。

- **module_id**：ソフトウェア サービス モジュールの名前

- *prod_id*：ハードウェア サービス モジュールに搭載されているデバイスの製品 ID 文字列
- *slot_num*：アプリケーションが停止したスロット
- **application**：停止したアプリケーションの名前
- **version**：停止したアプリケーションのバージョン

推奨アクション 4GE SSM でアップグレードが行われていなかった場合、あるいはアプリケーションの停止やアンインストールが意図的なものではなかった場合は、4GE SSM のログを調べて、アプリケーションが停止した原因を確認します。

505013

エラーメッセージ `%FTD>-5-505013: Module module_id application changed from: application version version to: newapplication version newversion .`

エラーメッセージ `%FTD>-5-505013: Module prod_id in slot slot_nunm application changed from: application version version to: newapplication version newversion .`

説明アップグレード後などにアプリケーションのバージョンが変わりました。サービスモジュール上のアプリケーションのソフトウェア アップデートが完了しました。

- **module_id**：ソフトウェア サービス モジュールの名前
- **application**：アップグレードされたアプリケーションの名前。
- **version**：アップグレードされたアプリケーションのバージョン
- **prod_id**：ハードウェア サービス モジュールに搭載されているデバイスの製品 ID 文字列
- **slot_num**：アプリケーションがアップグレードされたスロット
- **application**：アップグレードされたアプリケーションの名前。
- **version**：アップグレードされたアプリケーションのバージョン
- **newapplication**：新しいアプリケーションの名前
- **newversion**：新しいアプリケーションのバージョン

推奨アクションアップグレードが予期されていたこと、および新しいバージョンが正しいことを確認します。

505014

エラーメッセージ `%FTD>-1-505014: Module module_id , application down name , version version reason`

エラーメッセージ `%FTD>-1-505014: Module prod_id in slot slot_num , application down name , version version reason`

説明モジュール上で動作するアプリケーションがディセーブルになっています。

- **module_id**：ソフトウェア サービス モジュールの名前
- **prod_id**：ハードウェア サービス モジュールに搭載されているデバイスの製品 ID 文字列
- *slot_num*：アプリケーションがディセーブルにされたスロット。スロット 0 はシステムのメイン ボードを示し、スロット 1 は拡張スロットに設置されているモジュールを示します。

- **name**：アプリケーションの名前（文字列）。
- **application**：アップグレードされたアプリケーションの名前。
- **version**：アプリケーションのバージョン（文字列）。
- **reason**：障害の原因（文字列）。

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

505015

エラーメッセージ `%FTD>-1-505015: Module module_id , application up application , version version`

エラーメッセージ `%FTD>-1-505015: Module prod_id in slot slot_num , application up application , version version`

説明スロット *slot_num* の SSM 上のアプリケーションがアップして、動作しています。

- **module_id**：ソフトウェア サービス モジュールの名前
- **prod_id**：ハードウェア サービス モジュールに搭載されているデバイスの製品 ID 文字列
- *slot_num*：アプリケーションが動作しているスロット。スロット 0 はシステムのメイン ボードを示し、スロット 1 は拡張スロットに設置されているモジュールを示します。
- **application**：アプリケーションの名前（文字列）。
- **version**：アプリケーションのバージョン（文字列）。

推奨アクション 不要。

505016

エラーメッセージ `%FTD>-3-505016: Module module_id application changed from: name version version state state to: name version state state .`

エラーメッセージ `%FTD>-3-505016: Module` *prod_id* in slot *slot_num* application changed from: *name* version *version* state *state* to: *name version* state *state* .

説明アプリケーションのバージョンまたは名前の変更が検出されました。

- **module_id**：ソフトウェア サービス モジュールの名前
- **prod_id**：ハードウェア サービス モジュールに搭載されているデバイスの製品 ID 文字列
- *slot_num*：アプリケーションが変更されたスロット。スロット 0 はシステムのメイン ボードを示し、スロット 1 は拡張スロットに設置されているモジュールを示します。
- **name**：アプリケーションの名前（文字列）。
- **version**：アプリケーションのバージョン（文字列）。
- **state**：アプリケーションの状態（文字列）。
- **application**：変更されたアプリケーションの名前

推奨アクション変更が予期されていたこと、および新しいバージョンが正しいことを確認します。

506001

エラーメッセージ `%FTD>-5-506001: event_source_string event_string`

説明ファイル システムのステータスが変更されました。ファイル システムを利用可能または利用不可にしたイベントおよびイベントのソースが表示されます。ファイルシステムのステータスを変更させるソースおよびイベントの例には、次のものがあります。

- 外部 CompactFlash が除去された。
- 外部 CompactFlash が挿入された。
- 外部 CompactFlash の不明イベント。

推奨アクション 不要。

507001

エラーメッセージ `%FTD>-5-507001: Terminating TCP-Proxy connection from interface_inside:source_address/source_port to interface_outside :dest_address /dest_port - reassembly limit of limit bytes exceeded`

説明 TCP セグメントの再構築中にアセンブリ バッファ制限を超過しました。

- **source_address/source_port**：接続を開始しているパケットの送信元 IP アドレスと送信元ポート
- **dest_address/dest_port**：接続を開始しているパケットの宛先 IP アドレスと宛先ポート
- **interface_inside**：接続を開始したパケットが到着するインターフェイスの名前
- **interface_outside**：接続を開始したパケットを外部に送信するインターフェイスの名前
- **limit**：設定した初期接続のトラフィック クラスの制限

推奨アクション 不要。

507002

エラーメッセージ `%FTD>-4-507002: Data copy in proxy-mode exceeded the buffer limit`

説明フラグメント化された TCP メッセージの処理中に動作エラーが発生しました。

推奨アクション 不要。

507003

エラーメッセージ `%FTD>-3-507003: The flow of type protocol from the originating interface: src_ip /src_port to dest_if :dest_ip /dest_port terminated by inspection engine, reason-`

説明 TCP プロキシまたはセッション API が、メッセージで示されるさまざまな理由で接続を終了しました。

- **protocol**：フローのプロトコル。
- **src_ip**：フローの送信元 IP アドレス。
- *src_port*：フローの送信元ポートの名前

- *dest_if*：フローの宛先インターフェイス
- *dest_ip*：フローの宛先 IP アドレス
- *dest_port*：フローの宛先ポート
- *reason*：フローがインスペクションエンジンによって終了された原因の説明有効な原因は次のとおりです。

- フローの作成失敗

- セッション API の初期化失敗

- インストール済/一致したフィルタ規則の互換性なし

- 新しいバッファ データと元のデータとの結合失敗

- 無条件のリセット

- “service reset inbound” コンフィギュレーションに基づいたリセット

- 切断、パケットの廃棄

- パケット長の変更

- 送信者へのリセット反映

- プロキシ インスペクタの無条件のリセット

- プロキシ インスペクタのドロップ リセット

- プロキシ インスペクタの FIN 後のデータ受信

- プロキシ インスペクタの切断、パケットの廃棄

- インスペクタの無条件のリセット

- インスペクタのドロップ リセット

- インスペクタの FIN 後のデータ受信

- インスペクタの切断、パケットの廃棄

- 未処理データのバッファ失敗

- セッション API プロキシの転送失敗

- インスペクト データからセッション データへの変換失敗

- TLS プロキシの SSL チャネルのクローズ

推奨アクション 不要。

509001

エラーメッセージ `%FTD>-5-509001: Connection attempt from src_intf :src_ip /src_port [([idfw_user | FQDN_string ], sg_info )] to dst_intf :dst_ip /dst_port [([idfw_user | FQDN_string ], sg_info )] was prevented by "no forward" command.`

説明 このメッセージで指摘された送信元インターフェイスから宛先インターフェイスへのトラフィックをブロックするために、**no forward interface** コマンドが入力されました。このコマン

ドは、ライセンス制限を超えたインターフェイスの作成を可能にするためにローエンドプラットフォームで必要となります。

- **src_intf**：**no forward interface** コマンドの制限が適用される送信元インターフェイス名
- **dst_intf**：**no forward interface** コマンドの制限が適用される宛先インターフェイス名
- *sg_info*：指定した IP アドレスのセキュリティ グループ名またはタグ

推奨アクション このコマンドをローエンド プラットフォームで使用しなくて済むようにライセンスをアップグレードし、このコマンドをコンフィギュレーションから削除します。

520001

エラーメッセージ `%FTD>-3-520001: error_string`

説明 ID Manager で malloc 障害が発生しました。エラー文字列は次のいずれかになります。

- Malloc failure—id_reserve
- Malloc failure—id_get

推奨アクション Cisco TAC にお問い合わせください。

520002

エラーメッセージ `%FTD>-3-520002: bad new ID table size`

説明 ID Manager への新しい不正なテーブル要求が発生しました。

推奨アクション Cisco TAC にお問い合わせください。

520003

エラーメッセージ `%FTD>-3-520003: bad id in error_string (id: 0xid_num)`

説明 ID Manager のエラーが発生しました。エラー文字列は次のいずれかになります。

- id_create_new_table (no more entries allowed)
- id_destroy_table (bad table ID)
- id_reserve
- id_reserve (bad ID)
- id_reserve: ID out of range
- id_reserve (unassigned table ID)
- id_get (bad table ID)
- id_get (unassigned table ID)
- id_get (out of IDs!)
- id_to_ptr
- id_to_ptr (bad ID)
- id_to_ptr (bad table ID)
- id_get_next_id_ptr (bad table ID)
- id_delete
- id_delete (bad ID)

- id_delete (bad table key)

推奨アクション Cisco TAC にお問い合わせください。

520004

エラーメッセージ `%FTD>-3-520004: error_string`

説明 id_get が割り込みレベルで試行されました。

推奨アクション Cisco TAC にお問い合わせください。

520005

エラーメッセージ `%FTD>-3-520005: error_string`

説明 内部エラーが ID Manager で発生しました。

推奨アクション Cisco TAC にお問い合わせください。

520010

エラーメッセージ `%FTD>-3-520010: Bad queue elem - qelem_ptr : flink flink_ptr , blink blink_ptr , flink-blink flink_blink_ptr , blink-flink blink_flink_ptr`

説明内部ソフトウェア エラーが発生しました。次のいずれかになります。

- *qelem_ptr*：キュー データ構造へのポインタ
- *flink_ptr*：キュー データ構造の次の要素へのポインタ
- *blink_ptr*：キュー データ構造の前の要素へのポインタ
- *flink_blink_ptr*：キュー データ構造の次の要素の前のポインタへのポインタ
- *blink_flink_ptr*：キュー データ構造の前の要素の次のポインタへのポインタ

推奨アクション Cisco TAC にお問い合わせください。

520011

エラーメッセージ `%FTD>-3-520011: Null queue elem`

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 Cisco TAC にお問い合わせください。

520013

エラーメッセージ `%FTD>-3-520013: Regular expression access check with bad list acl_ID`

説明アクセス リストへのポインタが無効です。

推奨アクションこのメッセージを引き起こしたイベントは発生すべきではありません。1つ以上のデータ構造が上書きされたことを意味します。このメッセージが繰り返され、TACの担当

者に報告する場合は、メッセージのテキストを表示されているとおりにコピーして、関連のスタック トレースを含めてください。アクセス リストが破損している可能性があるため、TAC 担当者はアクセス リストが正しく機能していることを確認する必要があります。

520020

エラーメッセージ `%FTD>-3-520020: No memory available`

説明システムのメモリが不足しています。

推奨アクション 問題を修正するために、次のアクションのいずれかを試行してください。

- このルータによって受け入れるルートの数を減らす。
- ハードウェアをアップグレードする。
- run-from-RAM プラットフォームではより小さなサブセット イメージを使用する。

520021

エラーメッセージ `%FTD>-3-520021: Error deleting trie entry, error_message`

説明ソフトウェア プログラミング エラーが発生しました。エラー メッセージは次のいずれかになります。

- Inconsistent annotation
- Couldn't find our annotation
- Couldn't find deletion target

推奨アクション 表示されているとおりにエラー メッセージをコピーして、Cisco TAC に報告してください。

520022

エラーメッセージ `%FTD>-3-520022: Error adding mask entry, error_message`

説明ソフトウェアまたはハードウェア エラーが発生しました。エラー メッセージは次のいずれかになります。

- Mask already in tree
- Mask for route not entered
- Non-unique normal route, mask not entered

推奨アクション 表示されているとおりにエラー メッセージをコピーして、Cisco TAC に報告してください。

520023

エラーメッセージ `%FTD>-3-520023: Invalid pointer to head of tree, 0x radix_node_ptr`

説明ソフトウェア プログラミング エラーが発生しました。

推奨アクション 表示されているとおりにエラー メッセージをコピーして、Cisco TAC に報告してください。

520024

エラーメッセージ `%FTD>-3-520024: Orphaned mask #radix_mask_ptr, refcount= radix_mask_ptr's ref count at #radix_node_address, next= #radix_node_nxt`

説明 ソフトウェア プログラミング エラーが発生しました。

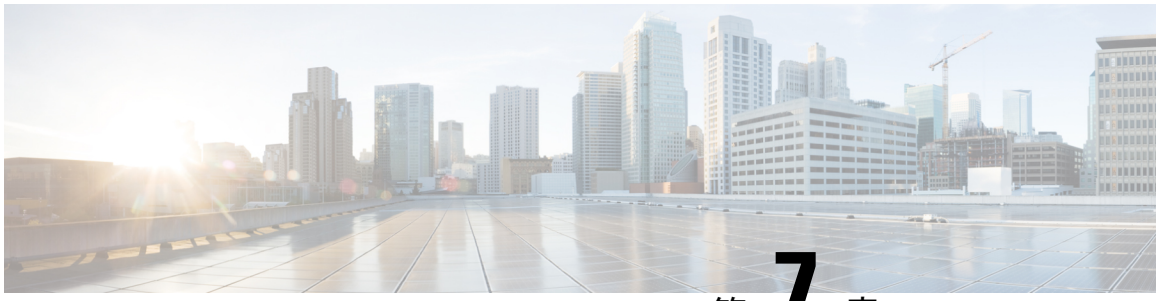
推奨アクション 表示されているとおりにエラー メッセージをコピーして、Cisco TAC に報告してください。

520025

エラーメッセージ `%FTD>-3-520025: No memory for radix initialization: err_msg`

説明 初期化中にシステムのメモリが不足しました。これは既存のダイナミック メモリに対してイメージが大きすぎる場合にのみ発生します。エラー メッセージは、Initializing leaf nodes と Mask housekeeping のいずれかになります。

推奨アクション より小さなサブセット イメージを使うか、ハードウェアをアップグレードします。



第 7 章

Syslog メッセージ 602101 ～ 622102

この章は、次の項で構成されています。

メッセージ 602101 ～ 609002

この項では、602101 から 609002 までのメッセージについて説明します。

602101

エラーメッセージ `%Threat Defense-6-602101: PMTU-D packet number bytes greater than effective mtu number dest_addr=dest_address , src_addr=source_address , prot=protocol`

説明 Secure Firewall Threat Defense デバイス が ICMP 宛先到達不能メッセージを送信し、フラグメンテーションが必要です。

推奨アクション データが正しく送信されることを確認します。

602103

エラーメッセージ `%FTD-6-602103: IPSEC: Received an ICMP Destination Unreachable from src_addr with suggested PMTU of rcvd_mtu; PMTU updated for SA with peer peer_addr, SPI spi, tunnel name username, old PMTU old_mtu, new PMTU new_mtu.`

説明 SA の MTU が変更されました。IPSec トンネル用のパケットを受信すると、対応する SA が特定され、ICMP パケットで推奨されている MTU に基づいて MTU がアップデートされます。推奨された MTU が 0 より大きく 256 未満の場合、新規 MTU は 256 に設定されます。推奨された MTU が 0 の場合、前の MTU から 256 を引いた値または 256 のどちらか大きい値に設定されます。推奨された MTU が 256 より大きい場合、新規 MTU は推奨された値に設定されます。

- src_addr：PMTU 送信側の IP アドレス
- rcvd_mtu：PMTU メッセージで受信した推奨 MTU

- peer_addr：IPSec ピアの IP アドレス
- spi：IPSec のセキュリティ パラメータ インデックス
- username：IPSec トンネルに関連付けられているユーザー名
- old_mtu：IPSec トンネルに関連付けられている前の MTU
- new_mtu：IPSec トンネルに関連付けられている新規 MTU

推奨アクション 不要。

602104

エラーメッセージ `%FTD-6-602104: IPSEC: Received an ICMP Destination Unreachable from src_addr , PMTU is unchanged because suggested PMTU of rcvd_mtu is equal to or greater than the current PMTU of curr_mtu , for SA with peer peer_addr , SPI spi , tunnel name username .`

説明 IPSec トンネル経由で送信されたパケットがパス MTU を超えたことを示す ICMP メッセージを受信し、推奨 MTU が現行 MTU 以上でした。MTU 値はすでに訂正されているので、MTU の調整は行われません。これは、さまざまな中間ステーションから複数の PMTU メッセージが受信され、現在の PMTU メッセージが処理される前に MTU が調整された場合に発生します。

- **src_addr**：PMTU 送信側の IP アドレス
- **rcvd_mtu**：PMTU メッセージで受信した推奨 MTU
- **curr_mtu**：IPSec トンネルに関連付けられている現行 MTU
- **peer_addr**：IPSec ピアの IP アドレス
- **spi**：IPSec のセキュリティ パラメータ インデックス
- *username*：IPSec トンネルに関連付けられているユーザー名

推奨アクション 不要。

602303

エラーメッセージ `%FTD-6-602303: IPSEC: An direction tunnel_type SA (SPI=spi ) between local_IP and remote_IP (username ) has been created.`

説明 新しい SA が作成されました。

- direction：SA の方向（インバウンドまたはアウトバウンド）
- tunnel_type：SA のタイプ（リモート アクセスまたは L2L）
- spi：IPSec のセキュリティ パラメータ インデックス
- local_IP：トンネルのローカル エンドポイントの IP アドレス
- remote_IP：トンネルのリモート エンドポイントの IP アドレス
- >*username*：IPSec トンネルに関連付けられているユーザー名

推奨アクション 不要。

602304

エラーメッセージ `%Threat Defense-6-602304: IPSEC: An direction tunnel_type SA (SPI=spi ) between local_IP and remote_IP (username ) has been deleted.`

説明 SA が削除されました。

- direction：SA の方向（インバウンドまたはアウトバウンド）
- tunnel_type：SA のタイプ（リモート アクセスまたは L2L）
- spi：IPSec のセキュリティ パラメータ インデックス
- local_IP：トンネルのローカル エンドポイントの IP アドレス
- remote_IP：トンネルのリモート エンドポイントの IP アドレス
- >*username*：IPSec トンネルに関連付けられているユーザー名

推奨アクション 不要。

602305

エラーメッセージ `%Threat Defense-3-602305: IPSEC: SA creation error, source source address , destination destination address , reason error string`

説明 IPSec セキュリティ アソシエーションの作成中に、エラーが発生しました。

推奨アクション通常、これは一時的なエラー状態です。このメッセージが連続して発生する場合は、Cisco TAC にお問い合わせください。

602306

エラーメッセージ `%Threat Defense-3-602306: IPSEC: SA change peer IP error, SPI: IPsec SPI, (src {original src IP address | original src port}, dest {original dest IP address| original dest port} => src {new src IP address | new src port}, dest: {new dest IP address | new dest port}), reason failure reason`

説明モバイル IKE の IPsec トンネルのピア アドレスを更新中にエラーが発生し、ピア アドレスを変更できませんでした。

推奨アクション通常、これは一時的なエラー状態です。このメッセージが連続して発生する場合は、Cisco TAC にお問い合わせください。

604101

エラーメッセージ `%Threat Defense-6-604101: DHCP client interface interface_name : Allocated ip = IP_address , mask = netmask , gw = gateway_address`

説明 Secure Firewall Threat Defense DHCP クライアントが DHCP サーバーから IP アドレスを正常に取得しました。dhcpc コマンド文によって、Secure Firewall Threat Defense デバイス は、ネットワーク インターフェイスの IP アドレスおよびネットワーク マスクを DHCP サーバーから取得でき、またデフォルト ルートを取得できます。デフォルト ルート文では、ゲートウェイ アドレスがデフォルト ルータのアドレスとして使用されます。

推奨アクション 不要。

604102

エラーメッセージ `%Threat Defense-6-604102: DHCP client interface interface_name : address released`

説明 Secure Firewall Threat Defense DHCP クライアントが、割り当てられた IP アドレスを解放して DHCP サーバーに戻しました。

推奨アクション 不要。

604103

エラーメッセージ `%Threat Defense-6-604103: DHCP daemon interface interface_name : address granted MAC_address (IP_address )`

説明 Secure Firewall Threat Defense DHCP サーバーによって、IP アドレスが外部クライアントに付与されました。

推奨アクション 不要。

604104

エラーメッセージ `%Threat Defense-6-604104: DHCP daemon interface interface_name : address released build_number (IP_address )`

説明外部クライアントが、IP アドレスを解放して Secure Firewall Threat Defense DHCP サーバーに戻しました。

推奨アクション 不要。

604105

エラーメッセージ `%Threat Defense-4-604105: DHCPD: Unable to send DHCP reply to client hardware_address on interface interface_name . Reply exceeds options field size (options_field_size ) by number_of_octets octets.`

説明管理者は、DHCP クライアントに返す DHCP オプションを設定できます。DHCP クライアントが要求するオプションに応じて、オファーの DHCP オプションはメッセージの長さの制限を超える場合があります。DHCP オファーは、メッセージの制限内に収まらないため、送信できません。

- *hardware_address*：要求元クライアントのハードウェア アドレス
- *interface_name*：サーバー メッセージを送受信するインターフェイス
- *options_field_size*：オプション フィールドの最大長。デフォルトは 312 オクテットであり、終端のための 4 オクテットを含みます。
- *number_of_octets*：超過したオクテット数

推奨アクション 設定されている DHCP オプションのサイズまたは数を減らします。

604201

エラーメッセージ `%Threat Defense-6-604201: DHCPv6 PD client on interface <pd-client-iface> received delegated prefix <prefix> from DHCPv6 PD server <server-address> with preferred lifetime <in-seconds> seconds and valid lifetime <in-seconds> seconds.`

説明この syslog は、最初の 4 ウェイ交換の一部として、PD サーバーから委任されたプレフィックスを使用して DHCPv6 PD クライアントが受信されると表示されます。複数のプレフィックスの場合は、プレフィックスごとに syslog が表示されます。

- *pd-client-iface*：DHCPv6 PD クライアントが有効になっているインターフェイス名。
- *prefix*：DHCPv6 PD サーバーから受信したプレフィックス。
- *server-address*：DHCPv6 PD サーバー アドレス。
- *in-seconds*：委任されたプレフィックスに関連付けられている優先される有効期間（秒単位）。

推奨アクション なし。

604202

エラーメッセージ `%Threat Defense-6-604202: DHCPv6 PD client on interface <pd-client-iface> releasing delegated prefix <prefix> received from DHCPv6 PD server <server-address>.`

説明この syslog は、無設定時に DHCPv6 PD クライアントが PD サーバーから受信した委任されたプレフィックスを解放している場合に表示されます。複数のプレフィックスの場合は、プレフィックスごとに syslog が表示されます。

- *pd-client-iface*：DHCPv6 PD クライアントが有効になっているインターフェイス名。
- *prefix*：DHCPv6 PD サーバーから受信したプレフィックス。
- *server-address*：DHCPv6 PD サーバー アドレス。

推奨アクション なし。

604203

エラーメッセージ `%Threat Defense-6-604203: DHCPv6 PD client on interface <pd-client-iface> renewed delegated prefix <prefix> from DHCPv6 PD server <server-address> with preferred lifetime <in-seconds> seconds and valid lifetime <in-seconds> seconds.`

説明この syslog は、DHCPv6 PD クライアントが以前に割り当てられた委任されたプレフィックスの更新を PD サーバーから開始し、成功した場合に表示されます。複数のプレフィックスの場合は、プレフィックスごとに syslog が表示されます。

- *pd-client-iface*：DHCPv6 PD クライアントが有効になっているインターフェイス名。
- *prefix*：DHCPv6 PD サーバーから受信したプレフィックス。
- *server-address*：DHCPv6 PD サーバー アドレス。
- *in-seconds*：委任されたプレフィックスに関連付けられている優先される有効期間（秒単位）。

推奨アクション なし。

604204

エラーメッセージ `%Threat Defense-6-604204: DHCPv6 delegated prefix <delegated prefix> got expired on interface <pd-client-iface>, received from DHCPv6 PD server <server-address>.`

説明この syslog は、DHCPv6 PD クライアントが受信した委任されたプレフィックスが期限切れになっている場合に表示されます。

- *pd-client-iface*：DHCPv6 PD クライアントが有効になっているインターフェイス名。
- *prefix*：DHCPv6 PD サーバーから受信したプレフィックス。
- *delegated prefix*：DHCPv6 PD サーバーから受信した委任プレフィックス。

推奨アクション なし。

604205

エラーメッセージ `%Threat Defense-6-604205: DHCPv6 client on interface <client-iface> allocated address <ipv6-address> from DHCPv6 server <server-address> with preferred lifetime <in-seconds> seconds and valid lifetime <in-seconds> seconds`

説明この syslog は、最初の 4 ウェイ交換の一部として DHCPv6 クライアント アドレスが DHCPv6 サーバーから受信され、有効な場合に表示されます。アドレスが複数の場合は、受け取ったアドレスごとに syslog が表示されます。

- *client-iface*：DHCPv6 クライアント アドレスがイネーブルになっているインターフェイス名。
- *ipv6-address*：DHCPv6 サーバーから受信した IPv6 アドレス。
- *server-address*：DHCPv6 サーバー アドレス。
- *in-seconds*：クライアントアドレスに関連付けられている優先される有効期間（秒単位）。

推奨アクション なし。

604207

エラーメッセージ `%Threat Defense-6-604207: DHCPv6 client on interface <client-iface> renewed address <ipv6-address> from DHCPv6 server <server-address> with preferred lifetime <in-seconds> seconds and valid lifetime <in-seconds> seconds.`

説明この syslog は、DHCPv6 クライアントが DHCPv6 サーバーから以前に割り当てられたアドレスの更新を開始すると表示されます。アドレスが複数の場合は、更新したアドレスごとに syslog が表示されます。

- *client-iface*：DHCPv6 クライアント アドレスがイネーブルになっているインターフェイス名。
- *ipv6-address*：DHCPv6 サーバーから受信した IPv6 アドレス。
- *server-address*：DHCPv6 サーバー アドレス。

• *in-seconds*：クライアントアドレスに関連付けられている優先される有効期間（秒単位）。

推奨アクション なし。

604206

エラーメッセージ `%Threat Defense-6-604206: DHCPv6 client on interface <client-iface> releasing address <ipv6-address> received from DHCPv6 server <server-address>.`

説明 DHCPv6 クライアントアドレスのコンフィギュレーションが実行されない場合、DHCPv6 クライアントは受信したクライアントアドレスを解放しています。アドレスが複数の場合は、アドレスごとに syslog が表示されます。

• *client-iface*：DHCPv6 クライアント アドレスが有効になっているインターフェイス名。
• *ipv6-address*：DHCPv6 サーバーから受信した IPv6 アドレス。
• *server-address*：DHCPv6 サーバー アドレス。

推奨アクション なし。

604208

エラーメッセージ `%Threat Defense-6-604208: DHCPv6 client address <ipv6-address> got expired on interface <client-iface>, received from DHCPv6 server <server-address>`

説明 この syslog は、DHCPv6 クライアントが受信したアドレスが期限切れになっている場合に表示されます。

• *client-iface*：DHCPv6 クライアント アドレスがイネーブルになっているインターフェイス名。
• *ipv6-address*：DHCPv6 サーバーから受信した IPv6 アドレス。
• *server-address*：DHCPv6 サーバー アドレス。

推奨アクション なし。

605004

エラーメッセージ `%Threat Defense-6-605004: Login denied from source-address/source-port to interface:destination/service for user "username "`

説明 ユーザーがコンソールにログインしようとすると、次の形式のメッセージが表示されます。

```
Login denied from serial to console for user "username"
```

Secure Firewall Threat Defense デバイス への誤ったログインの試行、またはログインの失敗が発生しました。すべてのログインに対して、セッションあたり 3 回の試行が許容され、不正な試行が 3 回行われると、そのセッションは終了します。SSH ログインおよび Telnet ログインの場合、このメッセージは、3 回目の試行の失敗後、または 1 回以上の試行の失敗後に TCP セッションが終了したときに、生成されます。他のタイプの管理セッションの場合、このメッセージは試行に失敗するたびに生成されます。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。

- *source-address*：ログイン試行の送信元アドレス
- *source-port*：ログイン試行の送信元ポート
- *interface*：宛先管理インターフェイス
- *destination*：宛先 IP アドレス
- *service*：宛先サービス
- *username*：宛先管理インターフェイス

推奨アクション このメッセージの表示頻度が少ない場合、処置は不要です。このメッセージが頻繁に表示される場合は、攻撃を示すことがあります。ユーザーと通信して、ユーザー名とパスワードを確認します。

605005

エラーメッセージ `%Threat Defense-6-605005: Login permitted from source-address /source-port to interface:destination /service for user "username "`

ユーザーがコンソールにログインすると、次の形式のメッセージが表示されます。

```
Login permitted from serial to console for user "username"
```

説明 ユーザーは認証に成功し、管理セッションが開始されました。

- *source-address*：ログイン試行の送信元アドレス
- *source-port*：ログイン試行の送信元ポート
- *interface*：宛先管理インターフェイス
- *destination*：宛先 IP アドレス
- *service*：宛先サービス
- *username*：宛先管理インターフェイス

推奨アクション 不要。

607001

エラーメッセージ `%Threat Defense-6-607001: Pre-allocate SIP connection_type secondary channel for interface_name:IP_address/port to interface_name:IP_address from string message`

説明 SIP メッセージの検査後、**fixup sip** コマンドによって SIP 接続が割り当て済みでした。**connection_type** は、次の文字列のいずれかです。

- SIGNALLING UDP
- SIGNALLING TCP
- SUBSCRIBE UDP
- SUBSCRIBE TCP
- Via UDP
- Route

- RTP
- RTCP

推奨アクション 不要。

608001

エラーメッセージ `%Threat Defense-6-608001: Pre-allocate Skinny connection_type secondary channel for interface_name:IP_address to interface_name:IP_address from string message`

接続 Skinny メッセージの検査後、**inspect skinny** コマンドによって Skinny 接続が割り当て済みでした。**connection_type** は、次の文字列のいずれかです。

- SIGNALLING UDP
- SIGNALLING TCP
- SUBSCRIBE UDP
- SUBSCRIBE TCP
- Via UDP
- Route
- RTP
- RTCP

推奨アクション 不要。

608002

エラーメッセージ `%Threat Defense-4-608002: Dropping Skinny message for in_ifc :src_ip /src_port to out_ifc :dest_ip /dest_port , SCCP Prefix length value too small`

説明設定済みの最小長より短い SCCP プレフィックス長を持つ Skinny（SSCP）メッセージを受信しました。

- *in_ifc*：入力インターフェイス
- *src_ip*：パケットの送信元 IP アドレス
- *src_port*：パケットの送信元ポート
- *out_ifc*：出力インターフェイス
- *dest_ip*：パケットの宛先 IP アドレス
- *dest_port*：パケットの宛先ポート
- *value*：パケットの SCCP プレフィックス長

推奨アクション SCCP メッセージが有効である場合は、Skinny ポリシー マップをカスタマイズして、SSCP プレフィックスの最小長の値を大きくします。

608003

エラーメッセージ `%Threat Defense-4-608003: Dropping Skinny message for in_ifc :src_ip /src_port to out_ifc :dest_ip /dest_port , SCCP Prefix length value too large`

説明設定済みの最大長より長い SCCP プレフィックス長を持つ Skinny（SSCP）メッセージを受信しました。

- *in_ifc*：入力インターフェイス
- *src_ip*：パケットの送信元 IP アドレス
- *src_port*：パケットの送信元ポート
- *out_ifc*：出力インターフェイス
- *dest_ip*：パケットの宛先 IP アドレス
- *dest_port*：パケットの宛先ポート
- *value*：パケットの SCCP プレフィックス長

推奨アクション SCCP メッセージが有効である場合は、Skinny ポリシー マップをカスタマイズして、SCCP プレフィックスの最大長の値を大きくします。

609001

エラーメッセージ `%Threat Defense-7-609001: Built local-host zone-name/* :ip-address`

説明ネットワーク状態コンテナは、ゾーン *zone-name* に接続されたホスト **ip-address** 用に予約済みでした。zone-name/* パラメータは、ホストが作成されているインターフェイスがゾーンの一部である場合に使用されます。ホストはいずれのインターフェイスにも属していないため、アスタリスクはすべてのインターフェイスを表します。

推奨アクション 不要。

609002

エラーメッセージ `%Threat Defense-7-609002: Teardown local-host zone-name/* :ip-address duration time`

説明ゾーン **zone-name** に接続されたホスト **ip-address** 用のネットワーク状態コンテナが削除されました。zone-name/* パラメータは、ホストが作成されているインターフェイスがゾーンの一部である場合に使用されます。ホストはいずれのインターフェイスにも属していないため、アスタリスクはすべてのインターフェイスを表します。

推奨アクション 不要。

メッセージ 610101 ～ 622102

この項では、610101 から 622102 までのメッセージについて説明します。

611101

エラーメッセージ `%Threat Defense-6-611101: User authentication succeeded: IP, IP address : Uname: user`

説明 Secure Firewall Threat Defense デバイス へのアクセス時にユーザー認証が成功しました。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。

- *IP address*：ユーザー認証に成功したクライアントの IP アドレス
- *user*：認証されたユーザー

推奨アクション 不要。

611102

エラーメッセージ `%Threat Defense-6-611102: User authentication failed: IP = IP address, Uname: user`

説明 Secure Firewall Threat Defense デバイス にアクセスしようとしたときに、ユーザー認証に失敗しました。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。

- *IP address*：ユーザー認証に失敗したクライアントの IP アドレス
- *user*：認証されたユーザー

推奨アクション 不要。

611103

エラーメッセージ `%Threat Defense-5-611103: User logged out: Uname: user`

説明指定されたユーザーがログアウトしました。

推奨アクション 不要。

611104

エラーメッセージ `%Threat Defense-5-611104: Serial console idle timeout exceeded`

説明ユーザー アクティビティがなかったために、Secure Firewall Threat Defense のシリアル コンソールに設定されたアイドル タイムアウトを超えました。

推奨アクション 不要。

611301

エラーメッセージ `%Threat Defense-6-611301: VPNClient: NAT configured for Client Mode with no split tunneling: NAT address: mapped_address`

説明スプリット トンネリングなしでクライアント モード用の VPN クライアント ポリシーがインストールされました。

推奨アクション 不要。

611302

エラーメッセージ `%Threat Defense-6-611302: VPNClient: NAT exemption configured for Network Extension Mode with no split tunneling`

説明スプリット トンネリングなしでネットワーク拡張モード用の VPN クライアント ポリシーがインストールされました。

推奨アクション 不要。

611303

エラーメッセージ `%Threat Defense-6-611303: VPNClient: NAT configured for Client Mode with split tunneling: NAT address: mapped_address Split Tunnel Networks: IP_address/netmask IP_address/netmask`

説明スプリット トンネリング付きでクライアント モード用の VPN クライアント ポリシーがインストールされました。

推奨アクション 不要。

611304

エラーメッセージ `%Threat Defense-6-611304: VPNClient: NAT exemption configured for Network Extension Mode with split tunneling: Split Tunnel Networks: IP_address/netmask IP_address/netmask`

説明スプリット トンネリング付きでネットワーク拡張モード用の VPN クライアント ポリシーがインストールされました。

推奨アクション 不要。

611305

エラーメッセージ `%Threat Defense-6-611305: VPNClient: DHCP Policy installed: Primary DNS: IP_address Secondary DNS: IP_address Primary WINS: IP_address Secondary WINS: IP_address`

説明 DHCP 用の VPN クライアント ポリシーがインストールされました。

推奨アクション 不要。

611306

エラーメッセージ `%Threat Defense-6-611306: VPNClient: Perfect Forward Secrecy Policy installed`

説明 VPN クライアント ダウンロード ポリシーの一部として、完全転送秘密が設定されました。

推奨アクション 不要。

611307

エラーメッセージ `%Threat Defense-6-611307: VPNClient: Head end: IP_address`

説明 VPN クライアントが、指摘されたヘッドエンドに接続されています。

推奨アクション 不要。

611308

エラーメッセージ `%Threat Defense-6-611308: VPNClient: Split DNS Policy installed: List of domains: string string`

説明 VPN クライアント ダウンロード ポリシーの一部として、スプリット DNS ポリシーがインストールされました。

推奨アクション 不要。

611309

エラーメッセージ `%Threat Defense-6-611309: VPNClient: Disconnecting from head end and uninstalling previously downloaded policy: Head End: IP_address`

説明 VPN クライアントが、前にインストールされたポリシーを切断しアンインストールしています。

推奨アクション 不要。

611310

エラーメッセージ `%Threat Defense-6-611310: VNPClient: XAUTH Succeeded: Peer: IP_address`

説明 VPN クライアント Xauth が、指摘されたヘッドエンドで成功しました。

推奨アクション 不要。

611311

エラーメッセージ `%Threat Defense-6-611311: VNPClient: XAUTH Failed: Peer: IP_address`

説明 VPN クライアント Xauth が、指摘されたヘッドエンドで失敗しました。

推奨アクション 不要。

611312

エラーメッセージ `%Threat Defense-6-611312: VPNClient: Backup Server List: reason`

説明 Secure Firewall Threat Defense デバイス が Easy VPN リモート デバイスの場合、Easy VPN サーバーがバックアップ サーバーのリストを Secure Firewall Threat Defense デバイス にダウンロードしました。このリストによって、ローカルで設定済みのバックアップ サーバーはすべて

上書きされます。ダウンロードされたリストが空の場合、Secure Firewall Threat Defense デバイスはバックアップ サーバーを使用しません。**reason** は、次のメッセージのどちらかです。

- A list of backup server IP addresses
- Received NULL list. Deleting current backup servers

推奨アクション 不要。

611313

エラーメッセージ `%Threat Defense-3-611313: VPNClient: Backup Server List Error: reason`

説明 Secure Firewall Threat Defense デバイス が Easy VPN リモート デバイスであり、Easy VPN サーバーがバックアップ サーバーのリストを Secure Firewall Threat Defense デバイス にダウンロードする場合、リストに無効な IP アドレスまたはホスト名が含まれています。Secure Firewall Threat Defense デバイスは、DNS はサポートしません。したがって、**name** コマンドを使用して名前を IP アドレスに手動でマッピングしない限り、サーバーのホスト名はサポートされません。

推奨アクション Easy VPN サーバー上で、サーバーの IP アドレスが正しいことを確認して、ホスト名ではなく IP アドレスでサーバーを設定します。サーバーでホスト名を使用する必要がある場合は、Easy VPN リモート デバイスで **name** コマンドを使用して IP アドレスを名前にマッピングします。

611314

エラーメッセージ `%Threat Defense-6-611314: VPNClient: Load Balancing Cluster with Virtual IP: IP_address has redirected the to server IP_address`

説明 Secure Firewall Threat Defense デバイス が Easy VPN リモートデバイスの場合、ロードバランシンググループのディレクタサーバーによって、Secure Firewall Threat Defense デバイス が特定のサーバーに接続するようにリダイレクトされました。

推奨アクション 不要。

611315

エラーメッセージ `%Threat Defense-6-611315: VPNClient: Disconnecting from Load Balancing Cluster member IP_address`

説明 Secure Firewall Threat Defense デバイス が Easy VPN リモート デバイスの場合、ロード バランシング クラスタ サーバーから切断しました。

推奨アクション 不要。

611316

エラーメッセージ `%Threat Defense-6-611316: VPNClient: Secure Unit Authentication Enabled`

説明 Secure Firewall Threat Defense デバイスが Easy VPN リモート デバイスの場合、ダウンロードされた VPN ポリシーによって SUA がイネーブルにされました。

推奨アクション 不要。

611317

エラーメッセージ `%Threat Defense-6-611317: VPNClient: Secure Unit Authentication Disabled`

説明 Secure Firewall Threat Defense デバイスが Easy VPN リモート デバイスの場合、ダウンロードされた VPN ポリシーによって SUA がディセーブルにされました。

推奨アクション 不要。

611318

エラーメッセージ `%Threat Defense-6-611318: VPNClient: User Authentication Enabled: Auth Server IP: IP_address Auth Server Port: port Idle Timeout: time`

説明 Secure Firewall Threat Defense デバイスが Easy VPN リモート デバイスの場合、ダウンロードされた VPN ポリシーによって、ネットワーク内側の Secure Firewall Threat Defense デバイス上のユーザーに対して IUA がイネーブルにされました。

- **IP_address**：Secure Firewall Threat Defense デバイスから認証要求が送信されるサーバーの IP アドレス
- **port**：Secure Firewall Threat Defense デバイスから認証要求が送信されるサーバーのポート
- **time**：認証クレデンシャルのアイドル タイムアウト値

推奨アクション 不要。

611319

エラーメッセージ `%Threat Defense-6-611319: VPNClient: User Authentication Disabled`

説明 Secure Firewall Threat Defense デバイスが Easy VPN リモート デバイスの場合、ダウンロードされた VPN ポリシーによって、ネットワーク内側の Secure Firewall Threat Defense 上のユーザーに対して IUA がディセーブルにされました。

推奨アクション 不要。

611320

エラーメッセージ `%Threat Defense-6-611320: VPNClient: Device Pass Thru Enabled`

説明 Secure Firewall Threat Defense デバイスが Easy VPN リモート デバイスの場合、ダウンロードされた VPN ポリシーによってデバイス パススルーがイネーブルにされました。デバイス パススルー機能によって、認証を実行できないデバイス（IP 電話など）は、IUA がイネーブルの場合、認証が免除されます。Easy VPN サーバーによってこの機能がイネーブルにされている

場合、Secure Firewall Threat Defense デバイス で **vpnclient mac-exempt** コマンドを使用して、認証（IUA）を免除するデバイスを指定できます。

推奨アクション 不要。

611321

エラーメッセージ `%Threat Defense-6-611321: VPNClient: Device Pass Thru Disabled`

説明 Secure Firewall Threat Defense デバイス が Easy VPN リモート デバイスの場合、ダウンロードされた VPN ポリシーによってデバイス パススルーがディセーブルにされました。

推奨アクション 不要。

611322

エラーメッセージ `%Threat Defense-6-611322: VPNClient: Extended XAUTH conversation initiated when SUA disabled`

説明 Secure Firewall Threat Defense デバイス が Easy VPN リモート デバイスであり、ダウンロードされた VPN ポリシーによって SUA がディセーブルにされている場合、Easy VPN サーバーは 2 要素/SecurID/cryptocard ベースの認証メカニズムで、XAUTH を使用している Secure Firewall Threat Defense デバイス を認証します。

推奨アクション 2 要素/SecurID/cryptocard ベースの認証メカニズムを使用して Easy VPN リモート デバイスを認証する場合は、サーバー上の SUA をイネーブルにします。

611323

エラーメッセージ `%Threat Defense-6-611323: VPNClient: Duplicate split nw entry`

説明 Secure Firewall Threat Defense デバイス が Easy VPN リモート デバイスの場合、ダウンロードされた VPN ポリシーに重複したスプリット ネットワーク エントリが含まれていました。エントリは、ネットワーク アドレスとネットワーク マスクの両方に一致する場合、重複と見なされます。

推奨アクション Easy VPN サーバー上の VPN ポリシーから重複したスプリット ネットワーク エントリを削除します。

612001

エラーメッセージ `%Threat Defense-5-612001: Auto Update succeeded:`*`filename`*` , version:`*`number`*

説明 Auto Update Server からのアップデートが成功しました。**filename** 変数は、image、ASDM file、または configuration です。**version number** 変数は、アップデートのバージョン番号です。

推奨アクション 不要。

612002

エラーメッセージ `%Threat Defense-4-612002: Auto Update failed:filename , version:number , reason:reason`

説明 Auto Update Server からのアップデートが失敗しました。

- **filename**：イメージ ファイル、ASDM ファイル、またはコンフィギュレーション ファイル。
- **number**：アップデートのバージョン番号。
- **reason**：失敗の原因。次のいずれかの可能性があります。

- フェールオーバー モジュールがストリーム バッファを開くことができなかった。

- フェールオーバー モジュールがストリーム バッファにデータを書き込むことができなかった。

- フェールオーバー モジュールがストリーム バッファに対して制御動作を行うことができなかった。

- フェールオーバー モジュールがフラッシュ ファイルを開くことができなかった。

- フェールオーバー モジュールがフラッシュにデータを書き込むことができなかった。

- フェールオーバー モジュールの動作のタイムアウト。

- フェールオーバー コマンド リンクがダウンしている。

- フェールオーバー リソースを使用できない。

- 相手装置の無効なフェールオーバー状態。

- フェールオーバー モジュールがファイル転送データの破損を検出した。

- フェールオーバー アクティブ状態の変更。

- フェールオーバー コマンドの EXEC に失敗した。

- イメージは、現在のシステムで動作できない。

- サポートされていないファイル タイプ。

推奨アクション Auto Update Server の設定を確認します。スタンバイ装置が障害状態であるかどうかを確認します。Auto Update Server が正しく設定されており、スタンバイ装置が障害状態でない場合は、Cisco TAC にお問い合わせください。

612003

エラーメッセージ `%Threat Defense-4-612003:Auto Update failed to contact:url , reason:reason`

説明 Auto Update デーモンが指摘された URL **url** にアクセスできませんでした。これは、Auto Update Server の URL、または Auto Update Server から返されたファイル サーバー URL の 1 つである場合があります。**reason** フィールドには、接続が失敗した原因が記述されています。考

えられる失敗の原因としては、サーバーからの応答がない、認証の失敗、またはファイルが見つからないことが挙げられます。

推奨アクション Auto Update Server の設定を確認します。

613001

エラーメッセージ `%Threat Defense-6-613001: Checksum Failure in database in area string Link State Id IP_address Old Checksum number New Checksum number`

説明メモリ破損のために、OSPF がデータベースでチェックサム エラーを検出しました。

推奨アクション OSPF プロセスを再起動します。

613002

エラーメッセージ `%Threat Defense-6-613002: interface interface_name has zero bandwidth`

説明このインターフェイスの帯域幅がゼロと報告されました。

推奨アクション 表示されているとおりにメッセージをコピーして、Cisco TAC に報告してください。

613003

エラーメッセージ `%Threat Defense-6-613003: IP_address netmask changed from area string to area string`

説明 OSPF コンフィギュレーションの変更によって、ネットワーク範囲のエリアが変更されました。

推奨アクション 正しいネットワーク範囲で OSPF を再設定します。

613004

エラーメッセージ `%Threat Defense-3-613004: Internal error: memory allocation failure`

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 表示されているとおりにエラー メッセージをコピーして、Cisco TAC に報告してください。

613005

エラーメッセージ `%Threat Defense-3-613005: Flagged as being an ABR without a backbone area`

説明ルータ内のバックボーン領域なしに、ルータが Area Border Router（ABR）としてフラグが設定されました。

推奨アクション OSPF プロセスを再起動します。

613006

エラーメッセージ `%Threat Defense-3-613006: Reached unknown state in neighbor state machine`

説明このルータ内の内部ソフトウェアエラーにより、データベース交換中に無効なネイバー状態が発生しました。

推奨アクション エラー メッセージ、設定、およびこのエラーの原因となったイベントの詳細をコピーし、Cisco TAC に提出してください。

613007

エラーメッセージ `%Threat Defense-3-613007: area string lsid IP_address mask netmask type number`

説明 OSPF がデータベースに既存の LSA を追加しようとしています。

推奨アクション エラー メッセージ、設定、およびこのエラーの原因となったイベントの詳細をコピーし、Cisco TAC に提出してください。

613008

エラーメッセージ `%Threat Defense-3-613008: if inside if_state number`

説明内部エラーが発生しました。

推奨アクション エラー メッセージ、設定、およびこのエラーの原因となったイベントの詳細をコピーし、Cisco TAC に提出してください。

613011

エラーメッセージ `%Threat Defense-3-613011: OSPF process number is changing router-id. Reconfigure virtual link neighbors with our new router-id`

説明 OSPF プロセスがリセット中で、新しいルータ ID を選択しようとしています。このアクションによってすべての仮想リンクが停止します。再び動作させるには、すべての仮想リンク ネイバー上の仮想リンク設定を変更する必要があります。

推奨アクションすべての仮想リンク ネイバーの仮想リンク コンフィギュレーションを変更し、新しいルータ ID を反映させます。

613013

エラーメッセージ `%Threat Defense-3-613013: OSPF LSID IP_address adv IP_address type number gateway IP_address metric number forwarding addr route IP_address/mask type number has no corresponding LSA`

説明 OSPF で、そのデータベースと IP ルーティング テーブル間に不整合が検出されました。

推奨アクション エラー メッセージ、設定、およびこのエラーの原因となったイベントの詳細をコピーし、Cisco TAC に提出してください。

613014

エラーメッセージ `%Threat Defense-6-613014: Base topology enabled on interface string attached to MTR compatible mode area string`

説明 MTR に互換性がある OSPF エリアに接続された OSPF インターフェイスでは、基本トポロジを有効にする必要があります。

推奨アクション なし。

613015

エラーメッセージ `%Threat Defense-4-613015: Process 1 flushes LSA ID IP_address type-number adv-rtr IP_address in area mask`

説明ルータは、このエラーメッセージによって報告されたLSAを広範囲に再発信またはフラッシュしています。

推奨アクション このルータがネットワーク LSA をフラッシュしている場合は、ルータのいずれかのインターフェイスの IP アドレスと LSA ID が衝突しているネットワーク LSA をルータが受信し、ネットワークの外部にLSAをフラッシュしたことを意味します。OSPF が正しく機能するためには、中継ネットワークの IP アドレスが一意であることが必要です。衝突しているルータは、このエラー メッセージを報告しているルータとこのメッセージで adv-rtr として報告された OSPF ルータ ID を持つルータです。このルータが LSA を再発信している場合は、他のルータがネットワークの外部にこの LSA をフラッシュしている可能性が高くなります。そのルータを見つけて衝突を解消してください。タイプ 2 LSA での衝突は、LSA ID の重複が原因の可能性があります。タイプ 5 LSA の場合、このエラー メッセージを報告しているルータと異なる領域に接続されているルータでルータ ID が重複している可能性があります。不安定なネットワークでは、このメッセージはその他の何らかの理由で LSA が広く再発信されていることを警告している場合もあります。このタイプのケースを調査するには、Cisco TAC にお問い合わせください。

613016

エラーメッセージ `%Threat Defense-3-613016: Area string router-LSA of length number bytes plus update overhead bytes is too large to flood.`

説明ルータは、特大システム バッファ サイズまたは OSPF プロトコルに課された最大サイズより大きいルータ LSA を構築しようとしました。

推奨アクション 報告されたトータル長（LSA サイズ + オーバーヘッド）が Huge システム バッファ サイズを超えていても、65535 バイト未満の場合は（OSPF プロトコルが指定する最大長）、Huge システム バッファ サイズを増やすことができます。報告されたトータル長が 65535 より大きい場合は、報告された領域の OSPF インターフェイスの数を削減する必要があります。

613017

エラーメッセージ `%Threat Defense-4-613017: Bad LSA mask: Type number, LSID IP_address Mask mask from IP_address`

説明 LSA 発信元の設定が不正であるため、ルータが無効な LSA マスクを持つ LSA を受信しました。結果として、このルートはルーティング テーブルにインストールされていません。

推奨アクション 不正なマスクとともに LSA 発信元ルータを探し、その LSA のネットワークの不良構成を修正します。詳しいデバッグについては、Cisco TAC に問い合わせてください。

613018

エラーメッセージ `%Threat Defense-4-613018: Maximum number of non self-generated LSA has been exceeded “OSPF number” - number LSAs`

説明非自己生成 LSA の最大数を超えました。

推奨アクション ネットワーク内のルータが誤設定の結果として大量の LSA を生成しているかどうかを確認します。

613019

エラーメッセージ `%Threat Defense-4-613019: Threshold for maximum number of non self-generated LSA has been reached "OSPF number" - number LSAs`

説明非自己生成 LSA の最大数のしきい値に達しました。

推奨アクション ネットワーク内のルータが誤設定の結果として大量の LSA を生成しているかどうかを確認します。

613021

エラーメッセージ `%Threat Defense-4-613021: Packet not written to the output queue`

説明内部エラーが発生しました。

推奨アクション エラー メッセージ、設定、およびこのエラーの原因となったイベントの詳細をコピーし、Cisco TAC に提出してください。

613022

エラーメッセージ `%Threat Defense-4-613022: Doubly linked list linkage is NULL`

説明内部エラーが発生しました。

推奨アクション エラー メッセージ、設定、およびこのエラーの原因となったイベントの詳細をコピーし、Cisco TAC に提出してください。

613023

エラーメッセージ `%Threat Defense-4-613023: Doubly linked list prev linkage is NULL number`

説明内部エラーが発生しました。

推奨アクション エラー メッセージ、コンフィギュレーション、およびエラーの原因となったイベントの詳細をコピーし、Cisco TAC に提出してください。

613024

エラーメッセージ `%Threat Defense-4-613024: Unrecognized timer number in OSPF string`

説明内部エラーが発生しました。

推奨アクション エラー メッセージ、コンフィギュレーション、およびエラーの原因となったイベントの詳細をコピーし、Cisco TAC に提出してください。

613025

エラーメッセージ `%Threat Defense-4-613025: Invalid build flag number for LSA IP_address, type number`

説明内部エラーが発生しました。

推奨アクション エラー メッセージ、設定、およびこのエラーの原因となったイベントの詳細をコピーし、Cisco TAC に提出してください。

613026

エラーメッセージ `%Threat Defense-4-613026: Can not allocate memory for area structure`

説明内部エラーが発生しました。

推奨アクション エラー メッセージ、コンフィギュレーション、およびエラーの原因となったイベントの詳細をコピーし、Cisco TAC に提出してください。

613027

エラーメッセージ `%Threat Defense-6-613027: OSPF process number removed from interface interface_name`

説明 IP VRF が理由で、OSPF プロセスがインターフェイスから削除されました。

推奨アクション なし。

613028

エラーメッセージ `%Threat Defense-6-613028: Unrecognized virtual interface intetface_name. Treat it as loopback stub route`

説明 仮想インターフェイス タイプが OSPF によって認識されなかったため、ループバック インターフェイスのスタブ ルートとして扱われます。

推奨アクション なし。

613029

エラーメッセージ `%Threat Defense-3-613029: Router-ID IP_address is in use by ospf process number`

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

推奨アクション プロセスの 1 つに別のルータ ID を設定します。

613030

エラーメッセージ `%Threat Defense-4-613030: Router is currently an ASBR while having only one area which is a stub area`

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

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

613031

エラーメッセージ `%Threat Defense-4-613031: No IP address for interface inside`

説明インターフェイスはポイントツーポイントではなく、番号が付けられていません。

推奨アクション インターフェイス タイプを変更するか、またはインターフェイスに IP アドレスを指定します。

613032

エラーメッセージ `%Threat Defense-3-613032: Init failed for interface inside, area is being deleted. Try again.`

説明 インターフェイスの初期化に失敗しました。考えられる原因は次のとおりです。

- インターフェイスの接続先となる領域が削除されています。
- ローカル ルータのネイバー データブロックを作成できませんでした。

推奨アクション インターフェイスに関係するコンフィギュレーション コマンドを削除して、再試行します。

613033

エラーメッセージ `%Threat Defense-3-613033: Interface inside is attached to more than one area`

説明インターフェイスが、インターフェイスのリンク先以外の領域のインターフェイス リストに含まれています。

推奨アクション エラー メッセージ、設定、およびこのエラーの原因となったイベントの詳細をコピーし、Cisco TAC に提出してください。

613034

エラーメッセージ `%Threat Defense-3-613034: Neighbor IP_address not configured`

説明設定されたネイバー オプションが有効ではありません。

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

613035

エラーメッセージ `%Threat Defense-3-613035: Could not allocate or find neighbor IP_address`

説明内部エラーが発生しました。

推奨アクション 表示されているとおりにエラー メッセージをコピーして、Cisco TAC に報告してください。

613036

エラーメッセージ `%Threat Defense-4-613036: Can not use configured neighbor: cost and database-filter options are allowed only for a point-to-multipoint network`

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

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

613037

エラーメッセージ `%Threat Defense-4-613037: Can not use configured neighbor: poll and priority options are allowed only for a NBMA network`

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

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

613038

エラーメッセージ `%Threat Defense-4-613038: Can not use configured neighbor: cost or database-filter option is required for point-to-multipoint broadcast network`

説明設定されたネイバーが、ポイントツーマルチポイント ブロードキャスト ネットワーク上で検出されました。**cost** または **database-filter** オプションのいずれかを設定する必要があります。

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

613039

エラーメッセージ `%Threat Defense-4-613039: Can not use configured neighbor: neighbor command is allowed only on NBMA and point-to-multipoint networks`

説明ネットワーク タイプが NBMA でもポイントツーマルチポイントでもないネットワーク上で、設定されたネイバーが検出されました。

推奨アクション なし。

613040

エラーメッセージ `%Threat Defense-4-613040: OSPF-1 Area string: Router IP_address originating invalid type number LSA, ID IP_address, Metric number on Link ID IP_address Link Type number`

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

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

613041

エラーメッセージ `%Threat Defense-6-613041: OSPF-100 Areav string: LSA ID IP_address, Type number, Adv-rtr IP_address, LSA counter DoNotAge`

説明内部エラーが修正されました。このエラーメッセージに関連する動作への影響はありません。

推奨アクション システム メモリを確認します。メモリが不足している場合は、そのためにタイマー ホイール機能が初期化されませんでした。メモリが利用可能になったときに、コマンドを再入力してみます。メモリが十分ある場合は、Cisco TAC に連絡し、**show memory** コマンド、**show processes** コマンド、および **show tech-support ospf** コマンドの出力を提供してください。

613042

エラーメッセージ `%Threat Defense-4-613042: OSPF process number lacks forwarding address for type 7 LSA IP_address in NSSA string - P-bit cleared`

説明 NSSA エリアに実行可能な転送先アドレスがありません。結果として、P ビットをクリアする必要があります。NSSA トランスレータはタイプ 7 LSA をタイプ 5 LSA に変換しません。RFC 3101 を参照してください。

推奨アクション アドバタイズされた IP アドレスで、少なくとも 1 つのインターフェイスを NSSA に設定します。アドバタイズメントは下位レイヤ 2 の状態に依存しないため、ループバックを選ぶようにしてください。

613043

エラーメッセージ `%Threat Defense-6-613043:`

説明負のデータベース リファレンス カウントが発生しました。

推奨アクション システム メモリを確認します。メモリが不足している場合は、そのためにタイマー ホイール機能が初期化されませんでした。メモリが利用可能になったときに、コマンドを再入力してみます。メモリが十分ある場合は、Cisco TAC に連絡し、**show memory** コマンド、**show processes** コマンド、および **show tech-support ospf** コマンドの出力を提供してください。

613101

エラーメッセージ `%Threat Defense-6-613101: Checksum Failure in database in area s Link State Id i Old Checksum #x New Checksum #x`

説明メモリ破損のために、OSPF がデータベースでチェックサム エラーを検出しました。

推奨アクション OSPF プロセスを再起動します。

613102

エラーメッセージ `%Threat Defense-6-613102: interface s has zero bandwidth`

説明このインターフェイスの帯域幅がゼロと報告されています。

推奨アクション 不要。

613103

エラーメッセージ `%Threat Defense-6-613103: i m changed from area AREA_ID_STR to area AREA_ID_STR`

説明 OSPF コンフィギュレーションの変更によって、ネットワーク範囲のエリアが変更されました。

推奨アクション 不要。

613104

エラーメッセージ `%Threat Defense-6-613104: Unrecognized virtual interface IF_NAME .`

説明仮想インターフェイス タイプが OSPFv3 によって認識されなかったため、ループバック インターフェイスのスタブ ルートとして扱われます。

推奨アクション 不要。

614001

エラーメッセージ `%Threat Defense-6-614001: Split DNS: request patched from server: IP_address to server: IP_address`

説明スプリット DNS によって、DNS クエリーが元の宛先サーバーから企業のプライマリ DNS サーバーにリダイレクトされています。

推奨アクション 不要。

614002

エラーメッセージ `%Threat Defense-6-614002: Split DNS: reply from server:IP_address reverse patched back to original server:IP_address`

説明スプリット DNS によって、DNS クエリーが企業の DNS サーバーから元の宛先サーバーにリダイレクトされています。

推奨アクション 不要。

615001

エラーメッセージ `%Threat Defense-6-615001: vlan number not available for firewall interface`

説明スイッチによって、VLAN が Secure Firewall Threat Defense デバイス から削除されました。

推奨アクション 不要。

615002

エラーメッセージ `%Threat Defense-6-615002: vlan number available for firewall interface`

説明スイッチによって、VLAN が Secure Firewall Threat Defense デバイス に追加されました。

推奨アクション 不要。

621001

エラーメッセージ `%Threat Defense-6-621001: Interface` *interface_name* does not support multicast, not enabled

説明マルチキャストをサポートしていないインターフェイス上の PIM をイネーブルにしようとしました。

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。

621002

エラーメッセージ `%Threat Defense-6-621002: Interface` *interface_name* does not support multicast, not enabled

説明マルチキャストをサポートしていないインターフェイス上の IGMP をイネーブルにしようとしました。

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。

621003

エラーメッセージ `%Threat Defense-6-621003: The event queue size has exceeded` *number*

説明作成されたイベント マネージャ数が想定された数を超えました。

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。

621006

エラーメッセージ `%Threat Defense-6-621006: Mrib disconnected`, (*IP_address* ,*IP_address*) event cancelled

説明データ駆動イベントを起動するパケットを受信したが、MRIB への接続がダウンしました。通知はキャンセルされました。

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

621007

エラーメッセージ `%Threat Defense-6-621007: Bad register from` *interface_name* :*IP_address* to *IP_address* for (*IP_address* , *IP_address*)

説明 PIM ルータが、ランデブー ポイントとして設定されている場合、または NAT で別の PIM ルータから PIM レジスタ パケットを受信した場合に表示されます。このパケット内のカプセル化されたデータは無効です。

推奨アクション 送信ルータが誤って RFC 以外のレジスタを送信しています。送信側のルータをアップグレードします。

622001

エラーメッセージ `%Threat Defense-6-622001`: *string* tracked route *network mask address* , distance *number* , table *string* , on interface *interface-name*

説明追跡対象ルートがルーティングテーブルに対して追加または削除されました。これは、追跡対象オブジェクトの状態がアップまたはダウンから変わったことを意味します。

- *string*：Adding または Removing
- *network*：ネットワーク アドレス
- *mask*：ネットワーク マスク
- *address*：ゲートウェイ アドレス
- *number*：ルート アドミニストレーティブ ディスタンス
- *string*：ルーティング テーブル名
- *interface-name*：**nameif** コマンドで指定されたインターフェイス名

推奨アクション 不要。

622101

エラーメッセージ `%Threat Defense-6-622101`: Starting regex table compilation for *match_command* ; table entries = *regex_num* entries

説明正規表現コンパイルのバックグラウンド アクティビティに関する情報が表示されます。

- *match_command*：正規表現テーブルが関連付けられている match コマンド
- *regex_num*：コンパイルされる正規表現エントリの数

推奨アクション 不要。

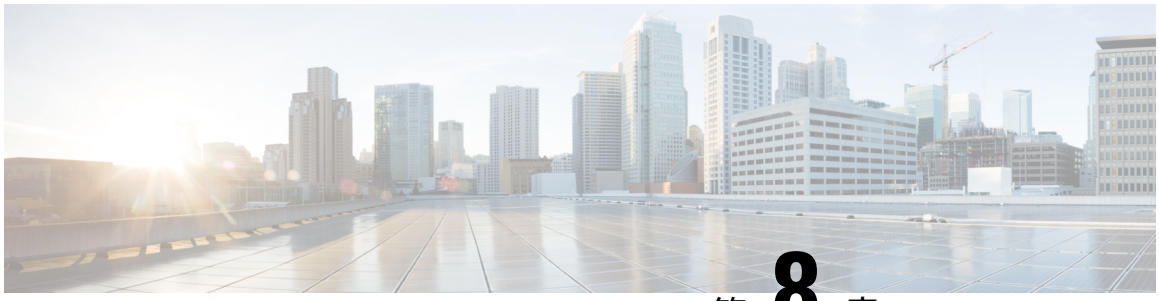
622102

エラーメッセージ `%Threat Defense-6-622102`: Completed regex table compilation for *match_command* ; table size = *num* bytes

説明正規表現コンパイルのバックグラウンド アクティビティに関する情報が表示されます。

- *match_command*：正規表現テーブルが関連付けられている match コマンド
- *num*：コンパイルされたテーブルのサイズ（バイト単位）

推奨アクション 不要。



第 8 章

Syslog メッセージ 701001 ～ 714011

この章は、次の項で構成されています。

メッセージ 701001 ～ 713109

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

701001

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

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

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

701002

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

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

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

703001

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

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

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

703002

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

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

推奨アクション 不要。

703008

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

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

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

709001、709002

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

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

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

推奨アクション 不要。

709003

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

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

推奨アクション 不要。

709004

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

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

推奨アクション 不要。

709005

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

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

推奨アクション 不要。

709006

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

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

推奨アクション 不要。

709007

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

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

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

709008

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

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

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

推奨アクション なし。

709009

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

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

推奨アクションなし。

709010

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

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

推奨アクションなし。

709011

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

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

推奨アクションなし。

709012

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

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

推奨アクションなし。

709013

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

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

推奨アクションなし。

710001

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

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

推奨アクション 不要。

710002

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

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

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

推奨アクション 不要。

710003

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

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

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

次に例を示します。

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

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

710004

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

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

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

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

710005

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

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

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

710006

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

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

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

710007

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

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

推奨アクション 不要。

711001

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

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

推奨アクション 不要。

711002

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

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

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

推奨アクション 不要。

711003

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

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

- *vpifnum*：インターフェイスに対応する 32 ビット値

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

711004

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

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

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

推奨アクション 不要。

711005

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

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

- *call_stack*：コール スタックの EIP

推奨アクション Cisco TAC にお問い合わせください。

711006

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

説明 CPU プロファイリングが開始されました。

- *n-samples*：CPU プロファイリング サンプルの指定数

• *reason-string*：次のうちどれかです。

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

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

推奨アクション 「指定なし」

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

713004

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

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

推奨アクション 不要。

713201

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

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

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

推奨アクション ネットワークのパフォーマンス、または接続を確認します。

713202

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

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

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

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

713006

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

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

推奨アクション 不要。

713008

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

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

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

713009

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

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

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

713010

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

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

この問題が解決しない場合は、ピアを調査します。

713012

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

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

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

713014

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

説明ピアから受信した ISAKMP DOI がサポートされていません。

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

713016

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

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

推奨アクション ヘッドエンドとピアのコンフィギュレーションを確認します。

713017

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

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

推奨アクション ヘッドエンドとピアのコンフィギュレーションを確認します。

713018

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

説明内部ソフトウェア エラーが発生しました。

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

713020

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

説明内部ソフトウェア エラーが発生しました。

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

713022

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

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

推奨アクション ピアのコンフィギュレーションを確認します。

713024

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

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

推奨アクション 不要。

713025

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

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

推奨アクション 不要。

713028

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

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

推奨アクション 不要。

713029

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

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

推奨アクション 不要。

713032

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

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

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

713033

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

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

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

713034

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

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

推奨アクション 不要。

713035

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

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

推奨アクション 不要。

713039

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

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

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

713040

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

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

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

713041

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

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

推奨アクション 不要。

713042

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

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

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

713043

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

説明元のトンネルが進行中に、IKE が再度起動されました。

推奨アクション 不要。

713048

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

説明処理できなかったペイロードでパケットが受信されました。

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

713049

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

説明 IPSec トンネルが開始されました。

推奨アクション 不要。

713050

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

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

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

推奨アクション 不要。

713052

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

説明リモート アクセス ユーザーが認証されました。

推奨アクション 不要。

713056

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

説明 IPSec SA が見つかりませんでした。

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

713060

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

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

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

713061

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

説明 Secure Firewall Threat Defense デバイス が、メッセージに示されているプライベート ネットワークまたはホストのセキュリティ ポリシー情報を検出できませんでした。これらのネットワークまたはホストは、発信側によって送信され、Secure Firewall Threat Defense デバイス のどの暗号 ACL とも一致しません。多くの場合、これはコンフィギュレーションの誤りです。

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

713062

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

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

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

713063

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

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

推奨アクション L2L 設定を確認します。

713065

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

説明内部ソフトウェア エラーが発生しました。

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

713066

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

説明ピアの暗号ポリシーが設定されています。

推奨アクション 不要。

713068

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

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

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

713072

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

説明ユーザーのパスワードが長すぎます。

推奨アクション 認証サーバーでパスワードの長さを訂正します。

713073

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

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

推奨アクション 不要。

713074

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

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

推奨アクション 不要。

713075

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

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

推奨アクション 不要。

713076

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

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

推奨アクション 不要。

713078

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

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

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

713081

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

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

推奨アクション デジタル証明書およびトラストポイントの設定を確認します。

713082

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

説明このトンネルの ID 証明書が見つかりません。

推奨アクション デジタル証明書およびトラストポイントの設定を確認します。

713083

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

説明このトンネルの ID 証明書が見つかりません。

推奨アクション デジタル証明書およびトラストポイントの設定を確認します。

713084

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

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

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

713085

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

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

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

713086

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

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

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

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

713088

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

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

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

713092

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

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

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

713094

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

説明 内部ソフトウェア エラーが発生しました。

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

713098

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

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

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

713099

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

説明内部ソフトウェア エラーが発生しました。

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

713102

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

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

推奨アクション 不要。

713103

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

説明内部ソフトウェア エラーが発生しました。

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

713104

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

説明内部ソフトウェア エラーが発生しました。

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

713105

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

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

推奨アクション ピアのコンフィギュレーションを確認します。

713107

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

説明内部ソフトウェア エラーが発生しました。

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

713109

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

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

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

メッセージ 713112 ～ 714011

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

713112

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

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

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

713113

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

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

推奨アクション 不要。エラー リカバリは組み込まれています。

713114

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

説明内部ソフトウェア エラーが発生しました。

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

713115

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

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

推奨アクション ヘッドエンドとピアのコンフィギュレーションを確認します。

713117

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

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

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

713118

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

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

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

713119

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

説明 IKE フェーズ 1 が正常終了しました。

推奨アクション 不要。

713120

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

説明 IKE フェーズ 2 が正常終了しました。

推奨アクション 不要。

713121

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

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

推奨アクション 不要。

713122

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

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

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

713123

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

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

推奨アクション 不要。

713124

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

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

推奨アクション 不要。

713127

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

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

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

713128

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

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

推奨アクション 不要。

713129

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

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

推奨アクション ピア間でコンフィギュレーションを確認します。

713130

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

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

推奨アクション 不要。

713131

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

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

推奨アクション 不要。

713132

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

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

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

713133

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

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

推奨アクション 不要。

713134

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

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

推奨アクション 不要。

713135

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

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

推奨アクション 不要。

713136

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

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

推奨アクション 不要。

713137

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

説明内部ソフトウェア エラーが発生しました。

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

713138

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

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

推奨アクション 事前共有キーのコンフィギュレーションを確認します。

713139

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

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

推奨アクション 不要。

713140

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

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

推奨アクション ACL のコンフィギュレーションを確認します。

713141

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

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

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

713142

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

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

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

713143

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

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

推奨アクション 不要。

713144

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

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

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

713145

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

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

推奨アクション 不要。

713146

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

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

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

713147

エラーメッセージ `%Threat Defense-6-713147: Terminating tunnel to Hardware Client in network extension mode, deleting static route for address: IP_address , mask: netmask`

説明ネットワーク拡張モードのハードウェア クライアントへのトンネルが除去され、ハードウェア クライアントの背後でプライベート ネットワーク用のスタティック ルートが削除されています。

推奨アクション 不要。

713148

エラーメッセージ `%Threat Defense-5-713148: Terminating tunnel to Hardware Client in network extension mode, unable to delete static route for address: IP_address , mask: netmask`

説明ネットワーク拡張モードのハードウェア クライアントへのトンネルを除去しているときに、ハードウェア クライアントの背後にあるプライベート ネットワークへのルートを削除できません。これは、アドレッシングまたはソフトウェアの問題を意味する場合があります。

推奨アクションルーティング テーブルを調べて、ルートがそこにないことを確認します。ルートがある場合は、手動で削除する必要がありますが、ハードウェア クライアントへのトンネルが完全に削除された場合に限り行います。

713149

エラーメッセージ `%Threat Defense-3-713149: Hardware client security attribute attribute_name was enabled but not requested.`

説明ヘッドエンドの Secure Firewall Threat Defense デバイス で指摘されたハードウェア クライアント セキュリティ属性がイネーブルになっているが、VPN 3002 ハードウェア クライアントによって属性が要求されませんでした。

推奨アクション ハードウェア クライアントでコンフィギュレーションを確認します。

713152

エラーメッセージ `%Threat Defense-3-713152: Unable to obtain any rules from filter ACL_tag to send to client for CPP, terminating connection.`

説明クライアントで CPP を使用してその Secure Firewall Threat Defense デバイス をプロビジョニングする必要があるが、ヘッドエンド デバイスがクライアントへ送信する ACL を取得できませんでした。原因として、設定の誤りが考えられます。

推奨アクション クライアントのグループ ポリシーで CPP に対して指定された ACL を確認します。

713154

エラーメッセージ `%Threat Defense-4-713154: DNS lookup for peer_description Server [server_name ] failed!`

説明このメッセージは、指摘されたサーバーに対する DNS ルックアップが解決されなかった場合に表示されます。

推奨アクション Secure Firewall Threat Defense デバイス 上の DNS サーバー コンフィギュレーションを確認します。また、DNS サーバーがオプションになっていることと、IP アドレス マッピングへのホスト名を持っていることを確認します。

713155

エラーメッセージ `%Threat Defense-5-713155: DNS lookup for Primary VPN Server [server_name ] successfully resolved after a previous failure. Resetting any Backup Server init.`

説明 プライマリ サーバーに対する以前の DNS ルックアップの失敗によって、Secure Firewall Threat Defense デバイス がバックアップ ピアを初期化した可能性があります。このメッセージは、プライマリ サーバーでの後の DNS ルックアップが最終的に成功し、バックアップ サーバーの初期化をリセットしていることを示しています。このポイントより後に初期化されたトンネルは、プライマリ サーバーに向けられます。

推奨アクション 不要。

713156

エラーメッセージ `%Threat Defense-5-713156: Initializing Backup Server [server_name or IP_address ]`

説明クライアントがバックアップ サーバーにフェールオーバーしているか、プライマリ サーバーに対する DNS ルックアップが失敗したことにより Secure Firewall Threat Defense デバイスがバックアップ サーバーを初期化しました。このポイントより後に初期化されたトンネルは、指摘されたバックアップ サーバーに向けられます。

推奨アクション 不要。

713157

エラーメッセージ `%Threat Defense-4-713157: Timed out on initial contact to server [server_name or IP_address ] Tunnel could not be established.`

説明クライアントが IKE MSG1 を送信してトンネルを初期化しようとしたが、相手側の Secure Firewall Threat Defense デバイス から応答を受信しませんでした。バックアップ サーバーを使用できる場合、クライアントはそれらのいずれかに接続しようとします。

推奨アクションヘッドエンドの Secure Firewall Threat Defense デバイス への接続を確認します。

713158

エラーメッセージ `%Threat Defense-5-713158: Client rejected NAT enabled IPsec Over UDP request, falling back to IPsec Over TCP`

説明クライアントが IPSec over TCP を使用するよう設定されています。Secure Firewall Threat Defense デバイスが IPSec over UDP を使用しようとする試みがクライアントによって拒否されました。

推奨アクション TCP を希望する場合、処置は不要です。それ以外の場合は、クライアント コンフィギュレーションを確認します。

713159

エラーメッセージ `%Threat Defense-3-713159: TCP Connection to Firewall Server has been lost, restricted tunnels are now allowed full network access`

説明 Secure Firewall Threat Defense サーバーへの TCP 接続が特定の原因により失われました。原因としては、サーバーがリブートした、ネットワークの問題が発生した、SSL のミスマッチが発生した、などがあります。

推奨アクション 初期接続が確立された後にサーバーの接続が失われた場合は、サーバーとネットワークの接続を確認する必要があります。初期接続がすぐに失われた場合、これは SSL 認証の問題を意味することがあります。

713160

エラーメッセージ `%Threat Defense-7-713160: Remote user (session Id - id ) has been granted access by the Firewall Server`

説明 Secure Firewall Threat Defense サーバーへのリモート ユーザーの通常の認証が実行されました。

推奨アクション 不要。

713161

エラーメッセージ `%Threat Defense-3-713161: Remote user (session Id - id ) network access has been restricted by the Firewall Server`

説明 Secure Firewall Threat Defense サーバーは、ユーザーを制限する必要があることを示すメッセージを Secure Firewall Threat Defense デバイス に送信しました。これには、Secure Firewall Threat Defense ソフトウェアのアップグレードや許可の変更など、いくつかの理由があります。Secure Firewall Threat Defense サーバーは、処理が完了するとすぐに、ユーザーを完全アクセス モードに移行します。

推奨アクション ユーザーが完全アクセス モードに移行されない限り、処置は不要です。これが実行されない場合、実行中の処理の詳細およびリモート マシンで実行中の Secure Firewall Threat Defense ソフトウェアの状態については、Secure Firewall Threat Defense サーバーを参照します。

713162

エラーメッセージ `%Threat Defense-3-713162: Remote user (session Id - id ) has been rejected by the Firewall Server`

説明 Secure Firewall Threat Defense サーバーは、このユーザーを拒否しました。

推奨アクション Secure Firewall Threat Defense サーバーにおけるポリシー情報で、ユーザーが正しく設定されていることを確認します。

713163

エラーメッセージ `%Threat Defense-3-713163: Remote user (session Id - id ) has been terminated by the Firewall Server`

説明 Secure Firewall Threat Defense サーバーがこのユーザー セッションを終了しました。これは、整合性エージェントがクライアント マシンで動作を停止した場合や、セキュリティ ポリシーがリモート ユーザーによって何らかの方法で変更された場合に発生します。

推奨アクション Secure Firewall Threat Defense ソフトウェアがクライアント マシンで動作を続けていることと、ポリシーが正しいことを確認します。

713164

エラーメッセージ `%Threat Defense-7-713164: The Firewall Server has requested a list of active user sessions`

説明 Secure Firewall Threat Defense サーバーが、古いデータがあることを検出した場合や（リブートにより）セッション データを失った場合に、セッション情報を要求します。

推奨アクション 不要。

713165

エラーメッセージ `%Threat Defense-3-713165: Client IKE Auth mode differs from the group's configured Auth mode`

説明デジタル証明書を使用するよう設定されているポリシーをトンネル グループが指しているときに、クライアントが事前共有キーとネゴシエートしました。

推奨アクション クライアント設定を確認します。

713166

エラーメッセージ `%Threat Defense-3-713166: Headend security gateway has failed our user authentication attempt - check configured username and password`

説明ハードウェア クライアントが拡張認証に失敗しました。これはおそらく、ユーザー名とパスワードの問題または認証サーバーの問題です。

推奨アクション設定したユーザー名とパスワードの値が各側で一致することを確認します。また、ヘッドエンドの認証サーバーが動作していることを確認します。

713167

エラーメッセージ `%Threat Defense-3-713167: Remote peer has failed user authentication - check configured username and password`

説明リモート ユーザーが認証の拡張に失敗しました。これはおそらく、ユーザー名とパスワードの問題または認証サーバーの問題です。

推奨アクション設定したユーザー名とパスワードの値が各側で一致することを確認します。また、リモートユーザーの認証に使用している認証サーバーが動作していることも確認します。

713168

エラーメッセージ `%Threat Defense-3-713168: Re-auth enabled, but tunnel must be authenticated interactively!`

説明キー再生成の再認証がイネーブルになっているが、トンネル認証で手動による介入が必要です。

推奨アクション手動による介入を希望する場合、処置は不要です。それ以外の場合は、対話型の認証コンフィギュレーションを確認します。

713169

エラーメッセージ `%Threat Defense-7-713169: IKE Received delete for rekeyed SA IKE peer: IP_address , SA address: internal_SA_address , tunnelCnt: tunnel_count`

説明キー再生成が完了した後に古い IKE SA を削除するために、IKE がリモート ピアから削除メッセージを受信しました。

推奨アクション 不要。

713170

エラーメッセージ `%Threat Defense-7-713170: Group group IP ip IKE Received delete for rekeyed centry IKE peer: IP_address , centry address: internal_address , msgid: id`

説明 IKE は、フェーズ 2 キー再生成が完了した後に古い centry を削除するために、リモート ピアから削除メッセージを受信しました。

推奨アクション 不要。

713171

エラーメッセージ `%Threat Defense-7-713171: NAT-Traversal sending NAT-Original-Address payload`

説明 UDP-Encapsulated-Transport が、フェーズ 2 中に提案または選択されました。この場合、NAT-Traversal 用にこのペイロードを送信します。

推奨アクション 不要。

713172

エラーメッセージ `%Threat Defense-6-713172: Automatic NAT Detection Status: Remote end is |is not behind a NAT device This end is |is not behind a NAT device`

説明 NAT-Traversal が NAT を自動検出しました。

推奨アクション 不要。

713174

エラーメッセージ `%Threat Defense-3-713174: Hardware Client connection rejected! Network Extension Mode is not allowed for this group!`

説明 ハードウェア クライアントがネットワーク拡張モードを使用してトンネルを試行しましたが、ネットワーク拡張モードは許可されていません。

推奨アクション ネットワーク拡張モードと PAT モードのコンフィギュレーションを対比して確認します。

713176

エラーメッセージ `%Threat Defense-2-713176: Device_type memory resources are critical, IKE key acquire message on interface interface_number , for Peer IP_address ignored`

説明 Secure Firewall Threat Defense デバイス が、示されたピアへの IPSec トンネルをトリガーするためのデータを処理しています。メモリ リソースは重大な状態なので、トンネルをそれ以上開始していません。データ パケットは無視され、廃棄されました。

推奨アクション 状態が解決しない場合は、Secure Firewall Threat Defense デバイス が効率的に設定されていることを確認します。このアプリケーションでは、Secure Firewall Threat Defense デバイス のメモリを増やす必要がある可能性があります。

713177

エラーメッセージ `%Threat Defense-6-713177: Received remote Proxy Host FQDN in ID Payload: Host Name: host_name Address IP_address , Protocol protocol , Port port`

説明 FQDN を含むフェーズ 2 ID ペイロードがピアから受信されました。

推奨アクション 不要。

713178

エラーメッセージ `%Threat Defense-5-713178: IKE Initiator received a packet from its peer without a Responder cookie`

説明内部ソフトウェア エラーが発生しました。

推奨アクション 問題が解決しない場合は、Cisco TAC にお問い合わせください。

713179

エラーメッセージ `%Threat Defense-5-713179: IKE AM Initiator received a packet from its peer without a payload_type payload`

説明内部ソフトウェア エラーが発生しました。

推奨アクション 問題が解決しない場合は、Cisco TAC にお問い合わせください。

713182

エラーメッセージ `%Threat Defense-3-713182: IKE could not recognize the version of the client! IPsec Fragmentation Policy will be ignored for this connection!`

説明内部ソフトウェア エラーが発生しました。

推奨アクション 問題が解決しない場合は、Cisco TAC にお問い合わせください。

713184

エラーメッセージ `%Threat Defense-6-713184: Client Type: Client_type Client Application Version: Application_version_string`

説明クライアントのオペレーティング システムとアプリケーションのバージョンが表示されます。情報を入手できない場合は、N/A が示されます。

推奨アクション 不要。

713185

エラーメッセージ `%Threat Defense-3-713185: Error: Username too long - connection aborted`

説明クライアントが無効な長さのユーザー名を戻し、トンネルが切断されました。

推奨アクション ユーザー名を確認し、必要に応じて変更します。

713186

エラーメッセージ `%Threat Defense-3-713186: Invalid secondary domain name list received from the authentication server. List Received: list_text Character index (value ) is illegal`

説明無効なセカンダリ ドメイン名リストが外部 RADIUS 認証サーバーから受信されました。スプリット トンネルが使用されている場合、このリストは、クライアントがトンネルで解決すべきドメインを示します。

推奨アクション RADIUS サーバーで Secondary-Domain-Name-List 属性（ベンダー固有の属性 29）の指定を訂正します。リストは、カンマ区切りのドメイン名のリストとして指定する必要があります。ドメイン名には英数字、ハイフン、下線、ピリオドだけ含めることができます。

713187

エラーメッセージ `%Threat Defense-7-713187: Tunnel Rejected: IKE peer does not match remote peer as defined in L2L policy IKE peer address: IP_address , Remote peer address: IP_address`

説明このトンネルを開始しようとしている IKE ピアは、受信されたリモート サブネットにバインドされた ISAKMP コンフィギュレーション内で設定された IKE ピアではありません。

推奨アクション ヘッドエンドとピアの L2L 設定が正しいことを確認します。

713189

エラーメッセージ `%Threat Defense-3-713189: Attempted to assign network or broadcast IP_address , removing ( IP_address ) from pool.`

説明プールからの IP アドレスは、このサブネットのネットワークまたはブロードキャスト アドレスです。このアドレスには、使用不可のマークが付けられます。

推奨アクション 通常、これは問題のないエラーですが、IP アドレス プール コンフィギュレーションを確認する必要があります。

713190

エラーメッセージ `%Threat Defense-7-713190: Got bad refCnt ( ref_count_value ) assigning IP_address ( IP_address )`

説明この SA のリファレンス カウンタは無効です。

推奨アクション 不要。

713191

エラーメッセージ `%Threat Defense-3-713191: Maximum concurrent IKE negotiations exceeded!`

説明 CPU に負荷のかかる暗号化計算を最小限にするため、Secure Firewall Threat Defense デバイスは処理中の接続ネゴシエーションの数を制限しています。新しいネゴシエーションが要求されたとき、Secure Firewall Threat Defense デバイス がすでに制限値に達している場合、新しいネゴシエーションは拒否されます。既存の接続ネゴシエーションが完了すると、新しい接続ネゴシエーションが再び許可されます。

推奨アクション crypto ikev1 limit max-in-negotiation-sa コマンドを参照してください。制限値を大きくすると、パフォーマンスが低下する可能性があります。

713193

エラーメッセージ `%Threat Defense-3-713193: Received packet with missing payload, Expected payload: payload_id`

説明 Secure Firewall Threat Defense デバイス が、1 つまたは複数の欠落ペイロードを持つ特定の交換タイプの暗号化または暗号解除されたパケットを受信しました。通常、これはピアに問題があることを意味します。

推奨アクション ピアが有効な IKE メッセージを送信していることを確認します。

713194

エラーメッセージ `%Threat Defense-3-713194: Sending IKE |IPsec Delete With Reason message: termination_reason`

説明終了原因コードを持つ削除メッセージが受信されました。

推奨アクション 不要。

713195

エラーメッセージ `%Threat Defense-3-713195: Tunnel rejected: Originate-Only: Cannot accept incoming tunnel yet!`

説明 originate-only ピアが着信接続を受け入れることができるのは、最初の P2 トンネルを作成した後だけです。その時点で、どの方向からでもデータは追加のフェーズ2トンネルを開始できます。

推奨アクション別の動作を希望する場合は、originate-only コンフィギュレーションを見直す必要があります。

713196

エラーメッセージ `%Threat Defense-5-713196: Remote L2L Peer IP_address initiated a tunnel with same outer and inner addresses. Peer could be Originate Only - Possible misconfiguration!`

説明 リモート L2L ピアが Public-Public トンネルを開始しました。リモート L2L ピアは、もう一方のピアからの応答を期待しますが、その応答を受信しません。設定が誤っている可能性があります。

推奨アクション 両方の終端で L2L コンフィギュレーションを確認します。

713197

エラーメッセージ `%Threat Defense-5-713197: The configured Confidence Interval of number seconds is invalid for this tunnel_type connection. Enforcing the second default.`

説明 グループ内の設定済み Confidence Interval が有効な範囲外です。

推奨アクション グループ内の信頼度の設定が有効な範囲内であることを確認します。

713198

エラーメッセージ `%Threat Defense-3-713198: User Authorization failed: user User authorization failed. Username could not be found in the certificate`

説明証明書内にユーザー名が見つからないことを示す原因文字列が表示されます。

推奨アクション グループ コンフィギュレーションとクライアント認可を確認します。

713199

エラーメッセージ `%Threat Defense-5-713199: Reaper corrected an SA that has not decremented the concurrent IKE negotiations counter ( counter_value )!`

説明リーパーによって内部ソフトウェア エラーが訂正されました。

推奨アクション 問題が解決しない場合は、Cisco TAC にお問い合わせください。

713203

エラーメッセージ `%Threat Defense-3-713203: IKE Receiver: Error reading from socket.`

説明受信したIKEパケットの読み取り中にエラーが発生しました。通常、これは内部エラーであり、ソフトウェアの問題を示している可能性があります。

推奨アクション 通常、これは問題のない状態であり、システムによって自動的に訂正されます。問題が解決しない場合、Cisco TAC にお問い合わせください。

713204

エラーメッセージ `%Threat Defense-7-713204: Adding static route for client address: IP_address`

説明このメッセージは、ピアが割り当てたアドレスへのルートまたはハードウェア クライアントによって保護されたネットワークへのルートがルーティング テーブルに追加されたことを示しています。

推奨アクション 不要。

713205

エラーメッセージ `%Threat Defense-3-713205: Could not add static route for client address: IP_address`

説明クライアントが割り当てたアドレスへのルートまたはハードウェア クライアントによって保護されたネットワークへのルートを追加する試みが失敗しました。これは、ルーティング テーブルまたは破損したネットワーク アドレスでのルートの重複を意味している場合もあります。ルートの重複は、ルートが正しくクリーンアップされていないか、複数のクライアントがネットワークまたはアドレスを共有していることによって発生します。

推奨アクション IP ローカル プール コンフィギュレーション、およびその他の使用中の IP アドレス割り当てメカニズム（DHCP や RADIUS など）をチェックします。ルーティング テーブルからルートが消去されていることを確認します。また、ピアにおけるネットワークやアドレスのコンフィギュレーションも確認します。

713206

エラーメッセージ `%Threat Defense-3-713206: Tunnel Rejected: Conflicting protocols specified by tunnel-group and group-policy`

説明 グループ ポリシーで指定された許可済みのトンネルが、トンネル グループの設定内の許可済みのトンネルと異なっていたために、トンネルが切断されました。

推奨アクション トンネル グループとグループ ポリシーの設定をチェックします。

713207

エラーメッセージ `%Threat Defense-4-713207: Terminating connection: IKE Initiator and tunnel group specifies L2TP Over IPSec`

説明 この Syslog は、GW が発信側でトンネルグループタイプが L2TP over IPSEC の場合に、接続を終了している ikev1 に対して表示されます。

推奨アクション 不要。

713208

エラーメッセージ `%Threat Defense-3-713208: Cannot create dynamic rule for Backup L2L entry rule rule_id`

説明 IKE をトリガーして IPSec データを適切に処理する ACL の作成時に障害が発生しました。この障害はバックアップ L2L コンフィギュレーションに固有です。これは、コンフィギュレーション エラー、キャパシティ エラー、または内部ソフトウェア エラーを示していることがあります。

推奨アクション 最大数の接続および最大数の VPN トンネルを使用して Secure Firewall Threat Defense デバイス が実行されている場合は、メモリの問題の可能性があります。それ以外の場合、バックアップ L2L およびクリプト マップ コンフィギュレーション（特にクリプト マップと関連付けられている ACL）を確認します。

713209

エラーメッセージ `%Threat Defense-3-713209: Cannot delete dynamic rule for Backup L2L entry rule id`

説明 IKE をトリガーして IPSec データを正しく処理する ACL の削除時に障害が発生しました。この障害はバックアップ L2L コンフィギュレーションに固有です。これは、内部ソフトウェア エラーが存在する可能性があることを示しています。

推奨アクション 問題が解決しない場合は、Cisco TAC にお問い合わせください。

713210

エラーメッセージ `%Threat Defense-3-713210: Cannot create dynamic map for Backup L2L entry rule_id`

説明バックアップ L2L コンフィギュレーションに関連するダイナミック クリプト マップの実行時インストールの作成時に障害が発生しました。これは、コンフィギュレーションエラー、キャパシティ エラー、または内部ソフトウェア エラーを示していることがあります。

推奨アクション 最大数の接続および最大数の VPN トンネルを使用して Secure Firewall Threat Defense デバイス が実行されている場合は、メモリの問題の可能性があります。それ以外の場合、バックアップ L2L およびクリプト マップ コンフィギュレーション（特にクリプト マップと関連付けられている ACL）を確認します。

713212

エラーメッセージ `%Threat Defense-3-713212`: Could not add route for L2L peer coming in on a dynamic map. address: *IP_address* , mask: *netmask*

説明 Secure Firewall Threat Defense デバイス がピアのプライベート アドレスまたはネットワーク用のルートを追加しようとして失敗しました。この場合、ピアはアドレスが不明なクライアントまたはL2L ピアのいずれかです。これらの場合ではいずれも、トンネルを通過するのにダイナミック クリプト マップを使用します。これは、ルートの重複か、ルーティング テーブルがいっぱいになっているか、前に使用したルートを Secure Firewall Threat Defense デバイス が削除していないことを意味している場合があります。

ルーティングテーブルに追加ルートのためのスペースがあることと、古いルートが存在しないことを確認します。テーブルがいっぱいになっている場合や古いルートが含まれている場合は、ルートを削除して再試行します。問題が解決しない場合、Cisco TAC にお問い合わせください。

713213

エラーメッセージ `%Threat Defense-6-713213: Deleting static route for L2L peer that came in on a dynamic map. address: IP_address , mask: netmask`

説明 Secure Firewall Threat Defense デバイス がピアのプライベート アドレスまたはネットワーク用のルートを削除しています。この場合、ピアはアドレスが不明なクライアントまたはL2L ピアのいずれかです。これらの場合ではいずれも、トンネルを通過するのにダイナミック クリプト マップを使用します。

推奨アクション 不要。

713214

エラーメッセージ `%Threat Defense-3-713214: Could not delete route for L2L peer that came in on a dynamic map. address: IP_address , mask: netmask`

説明 Secure Firewall Threat Defense デバイス がピアのプライベート アドレスまたはネットワーク用のルートを削除しようとしたときに障害が発生しました。この場合、ピアはアドレスが不明なクライアントまたはL2L ピアのいずれかです。これらの場合ではいずれも、トンネルを通過するのにダイナミック クリプト マップを使用します。ルートがすでに削除されているか、内部ソフトウェア エラーが発生しました。

推奨アクションルートがすでに削除されている場合は、問題のない状態であり、デバイスは正常に機能します。問題が解決しない場合、または VPN トンネルでルーティングの問題にリンクできる場合は、VPN L2L コンフィギュレーションのルーティング部分とアドレッシング部分を確認します。逆ルートの注入と、適切なクリプト マップに関連する ACL を確認します。問題が解決しない場合、Cisco TAC にお問い合わせください。

713215

エラーメッセージ `%Threat Defense-6-713215: No match against Client Type and Version rules. Client: type version is /is not allowed by default`

説明クライアントのタイプとクライアントのバージョンが Secure Firewall Threat Defense デバイス で設定された規則と一致しませんでした。デフォルトのアクションが表示されます。

推奨アクション デフォルトのアクションと配置要件を決定し、適切な変更を加えます。

713216

エラーメッセージ `%Threat Defense-5-713216: Rule: action [Client type]: version Client: type version allowed/not allowed`

説明クライアントのタイプとクライアントのバージョンが規則の 1 つと一致しました。一致の結果と規則が表示されます。

推奨アクション 配置要件を決定し、適切な変更を加えます。

713217

エラーメッセージ `%Threat Defense-3-713217: Skipping unrecognized rule: action: action client type: client_type client version: client_version`

説明形式が誤っているクライアント タイプとバージョン規則が存在します。必要な形式は、action client type | client version action ですclient type と client version の許可または拒否が、Session Management の下に表示されます。サポートされるワイルドカード（*）はパラメータごとに 1 つだけです。

推奨アクション 規則を修正します。

713218

エラーメッセージ `%Threat Defense-3-713218: Tunnel Rejected: Client Type or Version not allowed.`

設定された規則に従ってクライアントによるアクセスが拒否されました。

対処は不要です。

713219

エラーメッセージ `%Threat Defense-6-713219: Queuing KEY-ACQUIRE messages to be processed when P1 SA is complete.`

説明フェーズ 1 の完了後にフェーズ 2 のメッセージがキューイングされています。

推奨アクション 不要。

713220

エラーメッセージ `%Threat Defense-6-713220: De-queuing KEY-ACQUIRE messages that were left pending.`

説明キューに入れられたフェーズ 2 メッセージが処理されています。

推奨アクション 不要。

713221

エラーメッセージ `%Threat Defense-7-713221: Static Crypto Map check, checking map = crypto_map_tag , seq = seq_number...`

説明 Secure Firewall Threat Defense デバイスがクリプトマップで繰り返しコンフィギュレーション情報を探しています。

推奨アクション 不要。

713222

エラーメッセージ `%Threat Defense-7-713222: Group group Username username IP ip Static Crypto Map check, map = crypto_map_tag , seq = seq_number , ACL does not match proxy IDs src:source_address dst:dest_address`

説明設定されたクリプトマップで反復しているときに、Secure Firewall Threat Defense デバイスが関連する ACL と一致できません。通常、これは ACL の設定が誤っていることを意味します。

推奨アクション このトンネルピアに関連する ACL を調べ、VPN トンネルの両端から適切なプライベート ネットワークが指定されていることを確認します。

713223

エラーメッセージ `%Threat Defense-7-713223: Static Crypto Map check, map = crypto_map_tag , seq = seq_number , no ACL configured`

説明このピアに関連するクリプト マップが ACL にリンクされていません。

推奨アクション このクリプト マップに関連する ACL があることと、ACL に VPN トンネルの両側の適切なプライベート アドレスまたはネットワークが含まれていることを確認します。

713224

エラーメッセージ `%Threat Defense-7-713224: Static Crypto Map Check by-passed: Crypto map entry incomplete!`

説明この VPN トンネルに関連するクリプト マップで重要な情報が欠落しています。

推奨アクション VPN ピア、トランスフォーム セット、関連する ACL すべてでクリプト マップが正しく設定されていることを確認します。

713225

エラーメッセージ `%Threat Defense-7-713225: [IKEv1], Static Crypto Map check, map` *`map_name`* `, seq =` *`sequence_number`* `is a successful match`

説明 Secure Firewall Threat Defense デバイス がこの VPN トンネルに対して一致する有効なクリプト マップを検出しました。

推奨アクション 不要。

713226

エラーメッセージ `%Threat Defense-3-713226: Connection failed with peer` *`IP_address`* `, no trust-point defined in tunnel-group` *`tunnel_group`*

説明デバイスがデジタル証明書を使用するように設定されている場合は、コンフィギュレーションでトラストポイントを指定する必要があります。トラストポイントがコンフィギュレーションから欠落している場合は、このメッセージが生成され、エラーのフラグが立てられます。

- **IP_address**：ピアの IP アドレス
- **tunnel_group**：コンフィギュレーションでトラストポイントが欠落しているトンネル グループ

推奨アクションデバイスの管理者は、コンフィギュレーションでトラストポイントを指定する必要があります。

713227

エラーメッセージ `%Threat Defense-3-713227: Rejecting new IPsec SA negotiation for peer` *`Peer_address`* `. A negotiation was already in progress for local Proxy` *`Local_address /Local_netmask`* `, remote Proxy` *`Remote_address /Remote_netmask`*

説明フェーズ SA を確立するとき、Secure Firewall Threat Defense デバイス はこのプロキシに一致する新しいフェーズ 2 を拒否します。

推奨アクション 不要。

713228

エラーメッセージ `%Threat Defense-6-713228: Group = group , Username = uname , IP = remote_IP_address Assigned private IP address assigned_private_IP to remote user`

説明 IKE が DHCP またはアドレス プールからクライアントのプライベート IP アドレスを取得しました。

- *group*：グループの名前
- *uname*：ユーザーの名前
- *remote_IP_address*：リモート クライアントの IP アドレス
- *assigned_private_IP*：DHCP によって、またはローカル アドレス プールから割り当てられるクライアント IP アドレス

推奨アクション 不要。

713229

エラーメッセージ `%Threat Defense-5-713229: Auto Update - Notification to client client_ip of update string: message_string .`

説明アップデートされたソフトウェアをダウンロードできることが VPN リモート アクセス クライアントに通知されました。リモート クライアントユーザーには、クライアント アクセス ソフトウェアのアップデートを選択する責任があります。

- **client_ip**：リモート クライアントの IP アドレス
- **message_string**：リモート クライアントに送信されたメッセージ テキスト

推奨アクション 不要。

713230

エラーメッセージ `%Threat Defense-3-713230 Internal Error, ike_lock trying to lock bit that is already locked for type type`

説明内部エラーが発生しました。これは、IKEサブシステムがすでにロックされているメモリをロックしようとしていることを報告しています。これは、IKE SA のメモリ違反を保護するために使用するセマフォにエラーがあることを示します。このメッセージは、重大な誤りがないことを示しています。ただし、予期しないイベントが発生し、自動的に回復されました。

- >*type*：ロックの問題を持つセマフォのタイプを説明する文字列

推奨アクション 問題が解決しない場合は、Cisco TAC にお問い合わせください。

713231

エラーメッセージ `%Threat Defense-3-713231 Internal Error, ike_lock trying to unlock bit that is not locked for type type`

説明内部エラーが発生しました。IKEサブシステムが現在ロックされていないメモリをロック解除しようとしていることを報告しています。これは、IKE SA のメモリ違反を保護するために使用するセマフォにエラーがあることを示します。このメッセージは、重大な誤りがないことを示しています。ただし、予期しないイベントが発生し、自動的に回復されました。

- *type*：ロックの問題を持つセマフォのタイプを説明する文字列

推奨アクション 問題が解決しない場合は、Cisco TAC にお問い合わせください。

713232

エラーメッセージ `%Threat Defense-3-713232 SA lock refCnt = value , bitmask = hexvalue , p1_decrypt_cb = value , qm_decrypt_cb = value , qm_hash_cb = value , qm_spi_ok_cb = value , qm_dh_cb = value , qm_secret_key_cb = value , qm_encrypt_cb = value`

説明すべてのIKE SAがロックされ、発生する可能性のあるエラーが検出されました。このメッセージは、IKE SA のメモリ違反を保護するために使用するセマフォにエラーがあることを報告します。

- >*value*：10 進数値
- >*hexvalue*：16 進数値

推奨アクション 問題が解決しない場合は、Cisco TAC にお問い合わせください。

713233

エラーメッセージ `%Threat Defense-7-713233: (VPN-unit ) Remote network (remote network ) validated for network extension mode.`

説明フェーズ2ネゴシエーション中に受信されたリモートネットワークが検証されました。このメッセージは、ネットワーク拡張モード クライアントのフェーズ 2 ネゴシエーションでリモート ネットワーク チェックの結果を示します。これは、ユーザーがハードウェア クライアント ネットワークの設定を誤らないようにするための既存の機能の一部です（複数のクライアントでの重複するネットワークや同じネットワークの設定など）。

- *remote network*：フェーズ 2 のプロキシのサブネット アドレスおよびサブネット マスク

推奨アクション 不要。

713234

エラーメッセージ `%Threat Defense-7-713234: (VPN-unit) Remote network (remote network ) from network extension mode client mismatches AAA configuration (aaa network ).`

説明フェーズ2ネゴシエーション中に受信されたリモートネットワークが、このセッションのAAA サーバーから戻された framed-ip-address および framed-subnet-mask と一致しません。

- *remote network*：フェーズ 2 のプロキシのサブネット アドレスおよびサブネット マスク
- *aaa network*：AAA で設定されたサブネット アドレスおよびサブネット マスク

推奨アクション 次のいずれかを実行します。

- このユーザーとグループのアドレス割り当てをチェックし、HW クライアントのネットワーク コンフィギュレーションを確認して、不整合をすべて修正します。
- このユーザーおよびグループのアドレス割り当てをディセーブルにします。

713235

エラーメッセージ `%Threat Defense-6-713235: Attempt to send an IKE packet from standby unit. Dropping the packet!`

説明 通常、IKE パケットをスタンバイ装置からリモート ピアへ送信することはありません。このような試みがされた場合、内部ロジック エラーが発生している可能性があります。保護コードのため、パケットはスタンバイ装置から離れません。このメッセージは、デバッグを促進します。

推奨アクション 不要。

713236

エラーメッセージ `%Threat Defense-7-713236: IKE_DECODE tx/rx Message (msgid=msgid) with payloads:payload1 (payload1_len) + payload2 (payload2_len)...total length: tlen`

説明 IKE はさまざまなメッセージを送信または受信しました。

次の例に、IKE が 8 バイトのハッシュ ペイロード、11 バイトの通知ペイロード、および 2 つの 13 バイトのベンダー固有ペイロードを含むメッセージを受信した場合の出力を示します。

```
%Threat Defense-7-713236: IKE_DECODE RECEIVED Message msgid=0) with payloads: HDR + HASH
 (8) + NOTIFY (11) + VENDOR (13) + VENDOR (13) + NONE (0)
```

推奨アクション 不要。

713237

エラーメッセージ `%Threat Defense-5-713237: ACL update (access_list ) received during re-key re-authentication will not be applied to the tunnel.`

説明次の条件で、リモート アクセス IPSec トンネルのフェーズ 1 のキー再生成が表示されます。

- トンネルは、トンネルのキー再生成時にユーザーを再認証するよう設定されています。
- RADIUS サーバーは、アクセス リストまたはリファレンスを、ローカルで設定されたアクセス リストに戻します。これは、トンネルが最初に確立されたときに戻されたアクセス リストとは異なります。

推奨アクション これらの条件下では、Secure Firewall Threat Defense デバイス は新しいアクセス リストを無視し、このメッセージを生成します。

- >*access_list*：**show access-list** コマンドの出力に表示されるスタティックまたはダイナミック アクセス リストに関連付けられた名前

IPSec ユーザーは、ユーザー指定のアクセス リストを有効にするため、再接続する必要があります。

713238

エラーメッセージ `%Threat Defense-3-713238: Invalid source proxy address: 0.0.0.0! Check private address on remote client`

説明 ネットワーク拡張モード クライアントのプライベート側のアドレスが 0.0.0.0 です。通常、これは、ハードウェア クライアントのプライベート インターフェイスで IP アドレスが設定されていなかったことを示します。

推奨アクション リモート クライアントのコンフィギュレーションを確認します。

713239

エラーメッセージ `%Threat Defense-4-713239: IP_Address : Tunnel Rejected: The maximum tunnel count allowed has been reached`

説明 トンネルの最大許容数に達した後に、トンネル作成が試行されました。

- **IP_Address**：ピアの IP アドレス

推奨アクション 不要。

713240

エラーメッセージ `%Threat Defense-4-713240: Received DH key with bad length: received length=rlength expected length=elength`

説明 誤った長さの Diffie-Hellman キーをピアから受信しました。

- rlength：受信した DH キーの長さ
- elength：予期された長さ（DH キー サイズに基づく）

推奨アクション 不要。

713241

エラーメッセージ `%Threat Defense-4-713241: IE Browser Proxy Method setting_number is Invalid`

説明 ModeCfg の処理中に無効なプロキシ設定が見つかりました。P1 ネゴシエーションは失敗します。

推奨アクション **msie-proxy method** コマンド設定（**group-policy** コマンドのサブコマンド）を確認します。[**auto-detect** | **no-modify** | **no-proxy** | **use-server**] のいずれかが設定されているはずです。他の値が設定されている場合や値がない場合は、誤っています。**msie-proxy method** コ

マンドの設定をやり直してみてください。問題が解決しない場合、Cisco TAC にお問い合わせください。

713242

エラーメッセージ `%Threat Defense-4-713242: Remote user is authenticated using Hybrid Authentication. Not starting IKE rekey.`

説明 Secure Firewall Threat Defense デバイス が、ハイブリッド Xauth を使用するように設定されたトンネルに対する IKE キー再生成の開始要求を検出しましたが、キー再生成が開始されませんでした。Secure Firewall Threat Defense デバイスは、クライアントが IKE キー再生成を検出して開始するまで待ちます。

推奨アクション 不要。

713243

エラーメッセージ `%Threat Defense-4-713243: META-DATA Unable to find the requested certificate`

説明 IKE ピアが cert-req ペイロードで証明書を要求しました。しかし、要求した DN によって発行された有効な ID 証明書が見つかりませんでした。

推奨アクション：次のステップを実行します。

1. ID 証明書を確認します。
2. 必要な証明書を登録またはインポートします。
3. 詳細情報を得るために、証明書のデバッグをイネーブルにします。

713244

エラーメッセージ `%Threat Defense-4-713244: META-DATA Received Legacy Authentication Method(LAM) type type is different from the last type received type .`

説明受信した LAM 属性タイプが、最後に受信したタイプと異なります。タイプは、ユーザー認証プロセス全体で同じである必要があります。ユーザー認証プロセスを続行できず、VPN 接続が確立されません。

- **type**：LAM タイプ

推奨アクション 問題が解決しない場合は、Cisco TAC にお問い合わせください。

713245

エラーメッセージ `%Threat Defense-4-713245: META-DATA Unknown Legacy Authentication Method(LAM) type type received.`

説明 CRACK チャレンジまたは応答ユーザー認証プロセス中に、サポートされていない LAM タイプを受信しました。ユーザー認証プロセスを続行できず、VPN 接続が確立されません。

• **type**：LAM タイプ

推奨アクション 問題が解決しない場合は、Cisco TAC にお問い合わせください。

713246

エラーメッセージ `%Threat Defense-4-713246: META-DATA Unknown Legacy Authentication Method(LAM) attribute type type received.`

説明 Secure Firewall Threat Defense デバイス が、未知の LAM 属性タイプを受信しました。これは、接続の問題にはなりませんが、ピアの機能に影響する場合があります。

• **type**：LAM 属性タイプ

推奨アクション 不要。

713247

エラーメッセージ `%Threat Defense-4-713247: META-DATA Unexpected error: in Next Card Code mode while not doing SDI.`

説明状態処理中に予期しないエラーが発生しました。

推奨アクション 問題が解決しない場合は、Cisco TAC にお問い合わせください。

713248

エラーメッセージ `%Threat Defense-5-713248: META-DATA Rekey initiation is being disabled during CRACK authentication.`

説明 CRACK 認証方式による IKE SA のネゴシエート中、正常なキー再生成前にヘッドエンドのフェーズ 1 SA キー再生成タイマーが期限切れになりました。CRACK 認証方式を使用する場合は、リモートクライアントが必ず交換の発信側になるため、ヘッドエンドはキー再生成を開始しません。IKE SA が期限切れになる前にリモートピアが正常なキー再生成を開始しないと、IKE SA の期限切れで接続がダウンします。

推奨アクション 不要。

713249

エラーメッセージ `%Threat Defense-4-713249: META-DATA Received unsupported authentication results: result`

説明 CRACK 認証方式による IKE SA のネゴシエート中、IKE サブシステムが CRACK 認証時にサポートされていない結果を認証サブシステムから受信しました。ユーザー認証は失敗し、VPN 接続は切断されます。

• *result*：認証サブシステムから返された結果

推奨アクション 問題が解決しない場合は、Cisco TAC にお問い合わせください。

713250

エラーメッセージ `%Threat Defense-5-713250: META-DATA Received unknown Internal Address attribute: attribute`

説明 Secure Firewall Threat Defense デバイス が、認識できない内部アドレス属性の要求を受信しました。属性は有効であっても、現在サポートされていないか、ピアが不正な値を送信している可能性があります。これは、接続の問題にはなりませんが、ピアの機能に影響する場合があります。

推奨アクション 不要。

713251

エラーメッセージ `%Threat Defense-4-713251: META-DATA Received authentication failure message`

説明 CRACK 認証方式による IKE SA のネゴシエート中、Secure Firewall Threat Defense デバイス が認証の失敗を示す通知メッセージを受信しました。接続は切断されます。

推奨アクション 不要。

713252

エラーメッセージ `%Threat Defense-5-713252: Group = group , Username = user , IP = ip , Integrity Firewall Server is not available. VPN Tunnel creation rejected for client.`

説明 クライアントに Zonelab Integrity Server での認証を要求するようにグループ ポリシーが設定されている場合、設定されている失敗ポリシーによっては、サーバーがコンセントレータに接続する必要があります。失敗ポリシーによってクライアント接続が拒否される場合、クライアントの接続時に Zonelab Integrity Server が Secure Firewall Threat Defense デバイス に接続されていないと、このメッセージが生成されます。

- *group*：リモート アクセス ユーザーが接続しているトンネル グループ
- *user*：リモート アクセス ユーザー
- *ip*：リモート アクセス ユーザーの IP アドレス

推奨アクション コンセントレータと Zonelab Integrity Server のコンフィギュレーションが一致することを確認します。その後、コンセントレータと Zonelab Integrity Server の間に通信が存在することを確認します。

713253

エラーメッセージ `%Threat Defense-5-713253: Group = group , Username = user , IP = ip , Integrity Firewall Server is not available. Entering ALLOW mode. VPN Tunnel created for client.`

説明 クライアントに Zonelab Integrity Server での認証を要求するようにグループ ポリシーが設定されている場合、設定されている失敗ポリシーによっては、サーバーがコンセントレータに

接続する必要があります。失敗ポリシーによってクライアント接続が受け入れられ、無制限のネットワーク アクセスが提供される場合、クライアントの接続時に Zonelab Integrity Server が Secure Firewall Threat Defense デバイス に接続されていないと、このメッセージが生成されます。

- *group*：リモート アクセス ユーザーが接続しているトンネル グループ
- *user*：リモート アクセス ユーザー
- *ip*：リモート アクセス ユーザーの IP アドレス

推奨アクション Secure Firewall Threat Defense デバイス と Zonelab Integrity Server のコンフィギュレーションが一致することを確認し、Secure Firewall Threat Defense デバイス と Zonelab Integrity Server の間に通信が存在することを確認します。

713254

エラーメッセージ `%Threat Defense-3-713254: Group = groupname , Username = username , IP = peerip , Invalid IPsec/UDP port = portnum , valid range is minport - maxport , except port 4500, which is reserved for IPsec/NAT-T`

説明 UDP ポート 4500 は IPSec または NAT-T 接続用に予約されているため、IPSec/UDP 接続には使用できません。CLI では、ローカル グループに対してこのコンフィギュレーションが許可されません。このメッセージは、外部で定義されたグループに限り発生します。

- *groupname*：ユーザー グループの名前
- *username*：ユーザーの名前
- *peerip*：クライアントの IP アドレス
- *portnum*：外部サーバー上の IPSec/UDP ポート番号
- *minport*：ユーザーが設定可能なポートの最小有効ポート番号（4001）
- *maxport*：ユーザーが設定可能なポートの最大有効ポート番号（49151）

推奨アクション 外部サーバー上の IPSec または UDP ポート番号を別のポート番号に変更します。有効なポート番号は 4001 ～ 49151 です。

713255

エラーメッセージ `%Threat Defense-4-713255: IP = peer-IP , Received ISAKMP Aggressive Mode message 1 with unknown tunnel group name group-name`

説明 ISAKMP アグレッシブ モードのメッセージ 1 で不明なトンネル グループが指定されました。

- *peer-ip*：ピアのアドレス
- *group-name*：ピアによって指定されたグループ名

推奨アクション トンネル グループとクライアント コンフィギュレーションが有効であることを確認します。

713256

エラーメッセージ `%Threat Defense-6-713256: IP = peer-IP , Sending spoofed ISAKMP Aggressive Mode message 2 due to receipt of unknown tunnel group. Aborting connection.`

説明 ピアによって無効なトンネル グループが指定されると、Secure Firewall Threat Defense デバイス は引き続きメッセージ 2 を送信して、ピアでトンネル グループ情報が収集されるのを防止します。

- *peer-ip*：ピアのアドレス

推奨アクション 不要。

713257

エラーメッセージ `%Threat Defense-5-713257: Phase var1 failure: Mismatched attribute types for class var2 : Rcv'd: var3 Cfg'd: var4`

説明 Secure Firewall Threat Defense デバイス が、LAN-to-LAN 接続で応答側として動作しました。これは、Secure Firewall Threat Defense の暗号コンフィギュレーションが発信側のコンフィギュレーションと一致しないことを示しています。このメッセージでは、ミスマッチが発生したフェーズ、および応答側と発信側の両方が持つ属性のうち一致しない属性が指摘されます。

- *var1*：ミスマッチが発生したフェーズ
- *var2*：一致しない属性が属するクラス
- *var3*：発信側から受信した属性
- *var4*：設定されている属性

推奨アクション 両方の LAN-to-LAN デバイスで暗号コンフィギュレーションの不整合を確認します。特に、UDP-Tunnel（NAT-T）と他のデバイスとの間のミスマッチが報告された場合は、クリプトマップを確認してください。一方のコンフィギュレーションの一致したクリプトマップで NAT-T がディセーブルになっており、もう一方ではディセーブルになっていない場合、障害の原因となります。

713258

エラーメッセージ `%Threat Defense-3-713258: IP = var1 , Attempting to establish a phase2 tunnel on var2 interface but phase1 tunnel is on var3 interface. Tearing down old phase1 tunnel due to a potential routing change.`

説明 Secure Firewall Threat Defense デバイス がインターフェイスでフェーズ 2 トンネルを確立しようとしたときに、別のインターフェイスにフェーズ 1 トンネルがすでに存在しています。既存のフェーズ 1 トンネルは切断され、新しいインターフェイスで新しいトンネルを確立できるようになります。

- *var1*：ピアの IP アドレス
- *var2*：Secure Firewall Threat Defense デバイス がフェーズ 2 トンネルを確立しようとしているインターフェイス
- *var3*：フェーズ 1 トンネルが存在するインターフェイス

推奨アクション ピアのルートが変更されていないかどうかを確認します。ルートが変更されていない場合は、コンフィギュレーションが誤っている可能性があります。

713259

エラーメッセージ `%Threat Defense-5-713259: Group = groupname , Username = username , IP = peerIP , Session is being torn down. Reason: reason`

説明 ISAKMP セッションの終了原因が表示されます。これは、セッション管理によってセッションが切断された場合に発生します。

- *groupname*：終了されるセッションのトンネル グループ。
- *username*：終了されるセッションのユーザー名。
- *peerIP*：終了されるセッションのピア アドレス。
- *reason*：終了されるセッションの RADIUS 終了原因。原因は次のとおりです。

- ポートが切り替えられた（同時ログイン）

- アイドル タイムアウト

- 最大時間を超過した

- 管理者がリセットした

推奨アクション 不要。

713260

エラーメッセージ `%Threat Defense-3-713260: Output interface %d to peer was not found`

説明 フェーズ 1 SA を作成しようとしたときに、そのインターフェイス ID のインターフェイス データベースが見つかりませんでした

推奨アクション 問題が解決しない場合は、Cisco TAC にお問い合わせください。

713261

エラーメッセージ `%Threat Defense-3-713261: IPV6 address on output interface %d was not found`

説明 フェーズ 1 SA を作成しようとしたときに、IPv6 アドレスがローカル インターフェイスで指定されていません。

推奨アクション 目的のインターフェイスの IPv6 アドレスを設定する方法の詳細については、『CLI 構成ガイド』の「Configuring IPv6 Addressing」セクションを参照してください。

713262

エラーメッセージ `%Threat Defense-3-713262: Rejecting new IPSec SA negotiation for peer Peer_address . A negotiation was already in progress for local Proxy Local_address /Local_prefix_len , remote Proxy Remote_address /Remote_prefix_len`

説明フェーズ SA を確立するとき、Secure Firewall Threat Defense デバイス はこのプロキシに一致する新しいフェーズ 2 SA を拒否します。

- *Peer_address*：既存のネゴシエーションと一致するプロキシでフェーズ 2 を開始しようとしている新しいアドレス
- *Local_address*：現在フェーズ2をネゴシエートしている、以前のローカル ピアのアドレス
- *Local_prefix_len*：CIDR 表記に従ったサブネット プレフィックス長
- *Remote_address*：プロキシのアドレス
- *Remote_prefix_len*：CIDR 表記に従ったサブネット プレフィックス長

推奨アクション 不要。

713263

エラーメッセージ `%Threat Defense-7-713263: Received local IP Proxy Subnet data in ID Payload: Address IP_address , Mask /prefix_len , Protocol protocol , Port port`

説明 Secure Firewall Threat Defense デバイス がピアのプライベート アドレスまたはネットワーク用のルートを追加しています。この場合、ピアはアドレスが不明なクライアントまたはL2Lピアのいずれかです。これらの場合ではいずれも、トンネルを通過するのにダイナミック クリプト マップを使用します。

- *IP_address*：ピアの宛先ネットワークのベース IP アドレス
- *prefix_len*：CIDR 表記に従ったサブネット プレフィックス長
- *protocol*：プロキシ プロトコル
- *port*：プロキシ ポート

推奨アクション 不要。

713264

エラーメッセージ `%Threat Defense-7-713264: Received local IP Proxy Subnet data in ID Payload: Address IP_address , Mask/prefix_len , Protocol protocol , Port port {"Received remote IP Proxy Subnet data in ID Payload: Address %a , Mask/%d , Protocol %u , Port %u "}`

説明 Secure Firewall Threat Defense デバイス がピアのプライベート アドレスまたはネットワーク用のルートを追加しています。この場合、ピアはアドレスが不明なクライアントまたはL2Lピアのいずれかです。これらの場合ではいずれも、トンネルを通過するのにダイナミック クリプト マップを使用します。

- *IP_address*：ピアの宛先ネットワークのベース IP アドレス
- *prefix_len*：CIDR 表記に従ったサブネット プレフィックス長
- *protocol*：プロキシ プロトコル
- *port*：プロキシ ポート

推奨アクション 不要。

713265

エラーメッセージ `%Threat Defense-6-713265: Adding static route for L2L peer coming in on a dynamic map. address: IP_address , mask: /prefix_len`

説明 Secure Firewall Threat Defense デバイス がピアのプライベート アドレスまたはネットワーク用のルートを追加しています。この場合、ピアはアドレスが不明なクライアントまたはL2Lピアのいずれかです。これらの場合ではいずれも、トンネルを通過するのにダイナミック クリプト マップを使用します。

- *IP_address*：ピアの宛先ネットワークのベース IP アドレス
- *prefix_len*：CIDR 表記に従ったサブネット プレフィックス長

推奨アクション 不要。

713266

エラーメッセージ `%Threat Defense-3-713266: Could not add route for L2L peer coming in on a dynamic map. address: IP_address , mask: /prefix_len`

説明 Secure Firewall Threat Defense デバイス がピアのプライベート アドレスまたはネットワーク用のルートを追加しようとして失敗しました。この場合、ピアはアドレスが不明なクライアントまたはL2Lピアのいずれかです。これらの場合ではいずれも、トンネルを通過するのにダイナミック クリプト マップを使用します。これは、ルートの重複か、IPv6 ルーティング テーブルがいっぱいになっているか、前に使用したルートを Secure Firewall Threat Defense デバイスが削除していないことを意味している場合があります。

- *IP_address*：ピアの宛先ネットワークのベース IP アドレス
- *prefix_len*：CIDR 表記に従ったサブネット プレフィックス長

推奨アクション IPv6 ルーティング テーブルに追加ルートのためのスペースがあることと、古いルートが存在しないことを確認します。テーブルがいっぱいになっている場合や古いルートが含まれている場合は、ルートを削除して再試行します。問題が解決しない場合、Cisco TAC にお問い合わせください。

713267

エラーメッセージ `%Threat Defense-6-713267: Deleting static route for L2L peer that came in on a dynamic map. address: IP_address , mask: /prefix_len`

説明 Secure Firewall Threat Defense デバイス がピアのプライベート アドレスまたはネットワーク用のルートを追加しようとして失敗しました。この場合、ピアはアドレスが不明なクライアントまたはL2Lピアのいずれかです。これらの場合ではいずれも、トンネルを通過するのにダイナミック クリプト マップを使用します。

- *IP_address*：ピアの宛先ネットワークのベース IP アドレス
- *prefix_len*：CIDR 表記に従ったサブネット プレフィックス長

推奨アクション 不要。

713268

エラーメッセージ `%Threat Defense-3-713268: Could not delete route for L2L peer that came in on a dynamic map. address: IP_address , mask: /prefix_len`

説明 Secure Firewall Threat Defense デバイス がピアのプライベート アドレスまたはネットワーク用のルートを削除しようとしたときに障害が発生しました。この場合、ピアはアドレスが不明なクライアントまたはL2L ピアのいずれかです。これらの場合ではいずれも、トンネルを通過するのにダイナミック クリプト マップを使用します。ルートがすでに削除されているか、内部ソフトウェア エラーが発生しました。

- *IP_address*：ピアの宛先ネットワークのベース IP アドレス
- *prefix_len*：CIDR 表記に従ったサブネット プレフィックス長

推奨アクション ルートがすでに削除されている場合は、問題のない状態であり、デバイスは正常に機能します。問題が解決しない場合、または VPN トンネルでルーティングの問題にリンクできる場合は、VPN L2L コンフィギュレーションのルーティング部分とアドレッシング部分を確認します。また、逆ルートの注入と、適切なクリプト マップに関連する ACL も確認します。問題が解決しない場合、Cisco TAC にお問い合わせください。

713269

エラーメッセージ `%Threat Defense-6-713269: Detected Hardware Client in network extension mode, adding static route for address: IP_address , mask: /prefix_len`

説明 ネットワーク拡張モードのハードウェア クライアントを持つトンネルがネゴシエートされ、ハードウェア クライアントの背後にあるプライベート ネットワーク用にスタティック ルートが追加されています。この設定によって、Secure Firewall Threat Defense デバイス は、ヘッドエンドのプライベート側にあるすべてのルータにリモート ネットワークを知らせることができます。

- *IP_address*：ピアの宛先ネットワークのベース IP アドレス
- *prefix_len*：CIDR 表記に従ったサブネット プレフィックス長

推奨アクション 不要。

713270

エラーメッセージ `%Threat Defense-3-713270: Could not add route for Hardware Client in network extension mode, address: IP_address , mask: /prefix_len`

説明 内部ソフトウェア エラーが発生しました。ネットワーク拡張モードのハードウェア クライアントを持つトンネルがネゴシエートされ、ハードウェア クライアントの背後にあるプライベート ネットワーク用にスタティック ルートを追加する試みが失敗しました。IPv6 ルーティング テーブルがいっぱいになっているか、アドレッシング エラーが発生した可能性があります。

- *IP_address*：ピアの宛先ネットワークのベース IP アドレス
- *prefix_len*：CIDR 表記に従ったサブネット プレフィックス長

推奨アクション 問題が解決しない場合は、Cisco TAC にお問い合わせください。

713271

エラーメッセージ `%Threat Defense-6-713271: Terminating tunnel to Hardware Client in network extension mode, deleting static route for address: IP_address , mask:/prefix_len`

説明 ネットワーク拡張モードのハードウェア クライアントへのトンネルが除去され、ハードウェア クライアントの背後でプライベート ネットワーク用のスタティック ルートが削除されています。

- *IP_address*：ピアの宛先ネットワークのベース IP アドレス
- *prefix_len*：CIDR 表記に従ったサブネット プレフィックス長

推奨アクション 不要。

713272

エラーメッセージ `%Threat Defense-3-713272: Terminating tunnel to Hardware Client in network extension mode, unable to delete static route for address: IP_address , mask: /prefix_len`

説明 ネットワーク拡張モードのハードウェア クライアントへのトンネルを除去しているときに、ハードウェア クライアントの背後にあるプライベート ネットワークへのルートを削除できません。これは、アドレッシングまたはソフトウェアの問題を意味する場合があります。

- *IP_address*：ピアの宛先ネットワークのベース IP アドレス
- *prefix_len*：CIDR 表記に従ったサブネット プレフィックス長

推奨アクション IPv6 ルーティング テーブルを調べて、ルートがそこにないことを確認します。ルートがある場合は、手動で削除する必要がありますが、ハードウェア クライアントへのトンネルが完全に削除された場合に限り行います。

713273

エラーメッセージ `%Threat Defense-7-713273: Deleting static route for client address: IP_Address IP_Address address of client whose route is being removed`

説明 ピアが割り当てたアドレスへのルートまたはハードウェア クライアントによって保護されたネットワークへのルートがルーティング テーブルから削除されました。

推奨アクション 不要。

713274

エラーメッセージ `%Threat Defense-3-713274: Could not delete static route for client address: IP_Address IP_Address address of client whose route is being removed`

説明 IPSec クライアントへのトンネルが削除されたときに、ルーティング テーブル中のそのエントリを削除できませんでした。この状態は、ネットワーキングまたはソフトウェアの問題を示している場合があります。

推奨アクション ルーティング テーブルにルートがないことを確認します。ルートが存在する場合、トンネルが正常にクローズされた場合だけ、ルートを手動で削除する必要があります。

713275

エラーメッセージ `%Threat Defense-3-713275: IKEv1 Unsupported certificate keytype %s found at trustpoint %s`

説明 証明書のキー タイプが ECDSA でない場合、この syslog が ikev1 に対して表示されます。必ず、有効なキー タイプの証明書を GW にインストールします。

推奨アクション 不要。

713276

エラーメッセージ `%Threat Defense-3-713276: Dropping new negotiation - IKEv1 in-negotiation context limit of %u reached`

説明 ネゴシエーションの上限に達した場合、この Syslog メッセージがマルチコンテキストで ikev1 に対して表示されます。

推奨アクション 必要なし。

713900

エラーメッセージ `%Threat Defense-1-713900: Descriptive_event_string.`

説明 重大なイベントまたは障害が発生しました。たとえば、Secure Firewall Threat Defense デバイス がフェーズ 2 削除を生成しようとしたが、SPI が既存のどのフェーズ 2 SA とも一致しませんでした。

推奨アクション 上記の例では、両方のピアが同時にフェーズ 2 SA を削除しています。この場合、問題のないエラーであるため、無視してかまいません。エラーが引き続き表示され、トンネルの廃棄やデバイスのリブートなどの副作用が生じる場合は、ソフトウェア障害を示している可能性があります。その場合、コンソールまたはシステム ログに表示されるエラー メッセージをそのままコピーし、Cisco TAC に問い合わせてサポートを受けてください。

713901

エラーメッセージ `%Threat Defense-2-713901: Descriptive_event_string .`

説明 エラーが発生しました。これは、ヘッドエンドまたはリモート アクセス クライアントにおけるコンフィギュレーション エラーの結果である可能性があります。イベント文字列は、発生したエラーの詳細を提供します。

推奨アクション 場合によっては、エラーの原因を判別するためメッセージをトラブルシューティングする必要があります。両方のピアで、ISAKMP およびクリプト マップ コンフィギュレーションを確認します。

713902

エラーメッセージ `% Threat Defense-3-713902: Descriptive_event_string.`

説明エラーが発生しました。これは、ヘッドエンドまたはリモート アクセス クライアントにおけるコンフィギュレーション エラーの結果である可能性があります。

推奨アクション場合によっては、エラーの原因を判別するためコンフィギュレーションをトラブルシューティングする必要があります。両方のピアで、ISAKMP およびクリプト マップ コンフィギュレーションを確認します。

713903

エラーメッセージ `%Threat Defense-4-713903: IKE error message reason reason.`

説明 この Syslog ID は、複数の他の Syslog を表示できる IKE 警告メッセージに使用されます。

推奨アクション必要なし。

次に、例を示します。

`%Threat Defense-4-713903: Group = group policy , Username = user name , IP = remote IP , ERROR: Failed to install Redirect URL: redirect URL Redirect ACL: non_exist for assigned IP`

`%Threat Defense-4-713903: IKE Receiver: Runt ISAKMP packet discarded on Port Port_Number from Source_URL`

`%Threat Defense-4-713903: IP = IP address, Header invalid, missing SA payload! (next payload = x)`

`%Threat Defense-4-713903: Group = DefaultRAGroup, IP = IP address, Error: Unable to remove PeerTblEntry`

713904

エラーメッセージ `%Threat Defense-5-713904: Descriptive_event_string .`

説明発生したイベントを追跡するために使用される通知ステータス情報が表示されます。

推奨アクション 不要。

713905

エラーメッセージ `%Threat Defense-6-713905: Descriptive_event_string.`

説明発生したイベントを追跡するために使用される情報ステータスの詳細が表示されます。

例

```
%Threat Defense-6-713905: IKE successfully unreserved UDP port 27910 on interface outside
```

推奨アクション必要なし。

713906

エラーメッセージ `%Threat Defense-7-713906: Descriptive_event_string .`

説明発生したイベントを追跡するために使用されるデバッグのステータス情報が表示されます。

推奨アクション 不要。

714001

エラーメッセージ `%Threat Defense-7-714001: description_of_event_or_packet`

説明 IKE プロトコル イベントまたはパケットの説明が示されます。

推奨アクション 不要。

714002

エラーメッセージ `%Threat Defense-7-714002: IKE Initiator starting QM: msg id = message_number`

説明 Secure Firewall Threat Defense デバイス が、フェーズ 2 発信側としてクイック モード交換の最初のパケットを送信しました。

推奨アクション 不要。

714003

エラーメッセージ `%Threat Defense-7-714003: IKE Responder starting QM: msg id = message_number`

説明 Secure Firewall Threat Defense デバイス が、フェーズ 2 応答側としてクイック モード交換の最初のパケットを受信しました。

推奨アクション 不要。

714004

エラーメッセージ `%Threat Defense-7-714004: IKE Initiator sending 1st QM pkt: msg id = message_number`

説明最初のクイック モード パケットのプロトコルがデコードされました。

推奨アクション 不要。

714005

エラーメッセージ `%Threat Defense-7-714005: IKE Responder sending 2nd QM pkt: msg id = message_number`

説明 2 番目のクイック モード パケットのプロトコルがデコードされました。

推奨アクション 不要。

714006

エラーメッセージ `%Threat Defense-7-714006: IKE Initiator sending 3rd QM pkt: msg id = message_number`

説明 3 番目のクイック モード パケットのプロトコルがデコードされました。

推奨アクション 不要。

714007

エラーメッセージ `%Threat Defense-7-714007: IKE Initiator sending Initial Contact`

説明 Secure Firewall Threat Defense デバイス は、最初のコンタクト ペイロードを構築および送信しています。

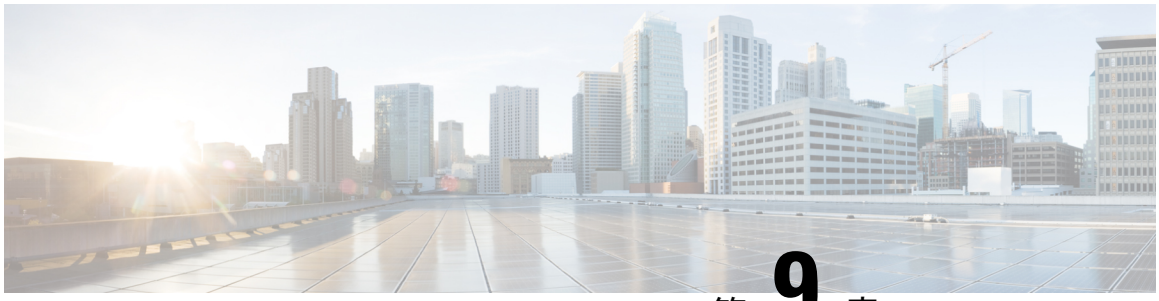
推奨アクション 不要。

714011

エラーメッセージ `%Threat Defense-7-714011: Description of received ID values`

説明 Secure Firewall Threat Defense デバイス が、ネゴシエーション中に、表示された ID 情報を受信しました。

推奨アクション 不要。



第 9 章

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。

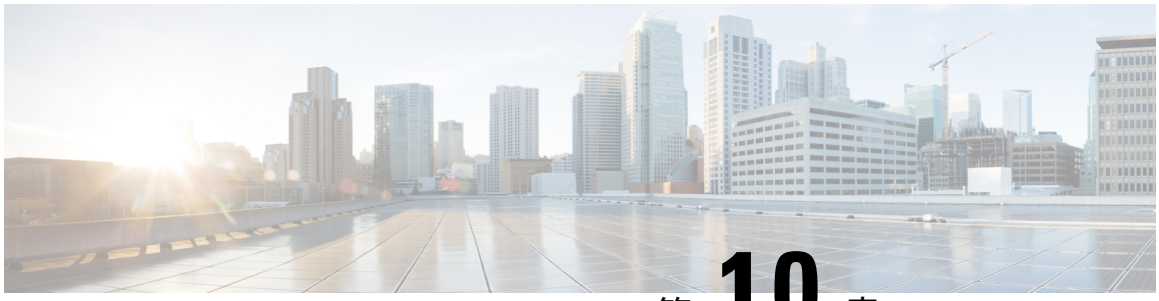
721019

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。



第 10 章

Syslog メッセージ 722001 ～ 776254

この章は、次の項で構成されています。

メッセージ 722001 ～ 722056

この項では、722001 から 722056 までのメッセージについて説明します。

722001

エラーメッセージ `%Threat Defense-4-722001: IP IP_address Error parsing SVC connect request.`

説明 SVC からの要求が無効でした。

説明 必要に応じて調査を実施し、このエラーの原因が SVC の障害であるか、互換性のない SVC バージョンであるか、デバイスに対する攻撃であるかを確認します。

722002

エラーメッセージ `%Threat Defense-4-722002: IP IP_address Error consolidating SVC connect request.`

説明アクションを実行するための十分なメモリがありません。

推奨アクション増設メモリを購入するか、デバイスをアップグレードするか、デバイスの負荷を減らします。

722003

エラーメッセージ `%Threat Defense-4-722003: IP IP_address Error authenticating SVC connect request.`

説明ユーザーがダウンロードおよび接続にかける時間が長すぎました。

推奨アクションセッションのアイドルタイムアウトおよび最大接続時間の値を大きくします。

722004

エラーメッセージ `%Threat Defense-4-722004: Group group User user-name IP IP_address Error responding to SVC connect request.`

説明アクションを実行するための十分なメモリがありません。

推奨アクション増設メモリを購入するか、デバイスをアップグレードするか、デバイスの負荷を減らします。

722005

エラーメッセージ `%Threat Defense-5-722005: Group group User user-name IP IP_address Unable to update session information for SVC connection.`

説明アクションを実行するための十分なメモリがありません。

推奨アクション増設メモリを購入するか、デバイスをアップグレードするか、デバイスの負荷を減らします。

722006

エラーメッセージ `%Threat Defense-5-722006: Group group User user-name IP IP_address Invalid address IP_address assigned to SVC connection.`

説明無効なアドレスがユーザーに割り当てられました。

推奨アクション可能であれば、アドレスの割り当てを確認し、修正します。そうでなければ、ネットワーク管理者に連絡するか、またはセキュリティポリシーに従ってこの問題の解決を依頼します。さらにサポートが必要な場合は、Cisco TAC にお問い合わせください。

722007

エラーメッセージ `%Threat Defense-3-722007: Group group User user-name IP IP_address SVC Message: type-num /ERROR: message`

説明 SVC がメッセージを発行しました。

- **type-num**：メッセージ タイプを示す 0 ～ 31 の番号。メッセージ タイプは次のとおりです。

- 0：正常

- 16：ログアウト

- 17：エラーによるクローズ

- 18：キー再生成によるクローズ

- 1 ～ 15、19 ～ 31：予約済みで未使用

• **message**：SVC からのテキスト メッセージ

推奨アクション 不要。

722008

エラーメッセージ `%Threat Defense-3-722008: Group group User user-name IP IP_address SVC Message: type-num /ERROR: message`

説明 SVC がメッセージを発行しました。

• **type-num**：メッセージ タイプを示す 0 ～ 31 の番号。メッセージ タイプは次のとおりです。

- 0：正常

- 16：ログアウト

- 17：エラーによるクローズ

- 18：キー再生成によるクローズ

- 1 ～ 15、19 ～ 31：予約済みで未使用

• **message**：SVC からのテキスト メッセージ

推奨アクション 不要。

722009

エラーメッセージ `%Threat Defense-3-722009: Group group User user-name IP IP_address SVC Message: type-num /ERROR: message`

説明 SVC がメッセージを発行しました。

• **type-num**：メッセージ タイプを示す 0 ～ 31 の番号。メッセージ タイプは次のとおりです。

- 0：正常

- 16：ログアウト

- 17：エラーによるクローズ

- 18：キー再生成によるクローズ

- 1 ～ 15、19 ～ 31：予約済みで未使用

• **message**：SVC からのテキスト メッセージ

推奨アクション 不要。

722010

エラーメッセージ `%Threat Defense-5-722010: Group group User user-name IP IP_address SVC Message: type-num /NOTICE: message`

説明 SVC がメッセージを発行しました。

- **type-num**：メッセージ タイプを示す 0 ～ 31 の番号。メッセージ タイプは次のとおりです。

- 0：正常

- 16：ログアウト

- 17：エラーによるクローズ

- 18：キー再生成によるクローズ

- 1 ～ 15、19 ～ 31：予約済みで未使用

- **message**：SVC からのテキスト メッセージ

推奨アクション 不要。

722011

エラーメッセージ `%Threat Defense-5-722011: Group group User user-name IP IP_address SVC Message: type-num /NOTICE: message`

説明 SVC がメッセージを発行しました。

- **type-num**：メッセージ タイプを示す 0 ～ 31 の番号。メッセージ タイプは次のとおりです。

- 0：正常

- 16：ログアウト

- 17：エラーによるクローズ

- 18：キー再生成によるクローズ

- 1 ～ 15、19 ～ 31：予約済みで未使用

- **message**：SVC からのテキスト メッセージ

推奨アクション 不要。

722012

エラーメッセージ `%Threat Defense-5-722012: Group group User user-name IP IP_address SVC Message: type-num /INFO: message`

説明 SVC がメッセージを発行しました。

- **type-num**：メッセージ タイプを示す 0 ～ 31 の番号。メッセージ タイプは次のとおりです。

- 0：正常

- 16：ログアウト

- 17：エラーによるクローズ

- 18：キー再生成によるクローズ

- 1 ～ 15、19 ～ 31：予約済みで未使用

- **message**：SVC からのテキスト メッセージ

推奨アクション 不要。

722013

エラーメッセージ `%Threat Defense-6-722013: Group group User user-name IP IP_address SVC Message: type-num /INFO: message`

説明 SVC がメッセージを発行しました。

- **type-num**：メッセージ タイプを示す 0 ～ 31 の番号。メッセージ タイプは次のとおりです。

- 0：正常

- 16：ログアウト

- 17：エラーによるクローズ

- 18：キー再生成によるクローズ

- 1 ～ 15、19 ～ 31：予約済みで未使用

- **message**：SVC からのテキスト メッセージ

推奨アクション 不要。

722014

エラーメッセージ `%Threat Defense-6-722014: Group group User user-name IP IP_address SVC Message: type-num /INFO: message`

説明 SVC がメッセージを発行しました。

- **type-num**：メッセージ タイプを示す 0 ～ 31 の番号。メッセージ タイプは次のとおりです。

- 0：正常

- 16：ログアウト

- 17：エラーによるクローズ

- 18：キー再生成によるクローズ

- 1 ～ 15、19 ～ 31：予約済みで未使用

• **message**：SVC からのテキスト メッセージ

推奨アクション 不要。

722015

エラーメッセージ `%Threat Defense-4-722015: Group group User user-name IP IP_address Unknown SVC frame type: type-num`

説明 SVC が、無効なフレーム タイプをデバイスに送信しました。これは、SVC のバージョンの非互換性が原因となっている可能性があります。

• **type-num**：フレーム タイプの ID 番号

推奨アクション SVC のバージョンを確認します。

722016

エラーメッセージ `%Threat Defense-4-722016: Group group User user-name IP IP_address Bad SVC frame length: length expected: expected-length`

説明 SVC から、予期された量のデータを入手できませんでした。これは、SVC のバージョンの非互換性が原因となっている可能性があります。

推奨アクション SVC のバージョンを確認します。

722017

エラーメッセージ `%Threat Defense-4-722017: Group group User user-name IP IP_address Bad SVC framing: 525446, reserved: 0`

説明 SVC が、正しくフレーム化されていないデータグラムを送信しました。これは、SVC のバージョンの非互換性が原因となっている可能性があります。

推奨アクション SVC のバージョンを確認します。

722018

エラーメッセージ `%Threat Defense-4-722018: Group group User user-name IP IP_address Bad SVC protocol version: version , expected: expected-version`

説明 SVC が、デバイスに未知のバージョンを送信しました。これは、SVC のバージョンの非互換性が原因となっている可能性があります。

推奨アクション SVC のバージョンを確認します。

722019

エラーメッセージ `%Threat Defense-4-722019: Group group User user-name IP IP_address Not enough data for an SVC header: length`

説明 SVC から、予期された量のデータを入手できませんでした。これは、SVC のバージョンの非互換性が原因となっている可能性があります。

推奨アクション SVC のバージョンを確認します。

722020

エラーメッセージ `%Threat Defense-3-722020: TunnelGroup tunnel_group GroupPolicy group_policy User user-name IP IP_address No address available for SVC connection`

説明 AnyConnect セッションに対するアドレスの割り当てに失敗しました。使用できる IP アドレスがありません。

- **tunnel_group**：ユーザーが割り当てられているか、ログインに使用されたトンネル グループの名前
- *group_policy*：ユーザーが割り当てられているグループ ポリシーの名前
- *user-name*：このメッセージが関連付けられているユーザー名
- *IP_address*：クライアント マシンのパブリック IP（インターネット）アドレス

推奨アクション ip local ip コマンドで表示されるコンフィギュレーションを参照し、トンネル グループとグループ ポリシーに割り当てられているプールに十分なアドレスが存在するかどうかを確認します。DHCP の設定およびステータスを確認します。アドレス割り当てコンフィギュレーションを確認します。AnyConnect クライアントが IP アドレスを取得できない理由を特定するため、IPAA の syslog メッセージをイネーブルにします。

722028

エラーメッセージ `%Threat Defense-5-722028: Group group User user-name IP IP_address Stale SVC connection closed.`

説明未使用の SVC 接続が閉じられました。

推奨アクション不要。ただし、複数の接続が確立されている場合は、クライアントに接続の問題が発生している可能性があります。SVC のログを調べる必要があります。

722029

エラーメッセージ `%Threat Defense-7-722029: Group group User user-name IP IP_address SVC Session Termination: Conns: connections , DPD Conns: DPD_conns , Comp resets: compression_resets , Dcmp resets: decompression_resets`

説明行われた接続、再接続、およびリセットの数が報告されます。**connections** が 1 より大きい場合、または **DPD_conns**、**compression_resets**、**decompression_resets** のいずれかが 0 より大きい場合は、Secure Firewall Threat Defense の管理者が制御できない、ネットワークの信頼性の問

題を示している可能性があります。接続数または DPD 接続数が多い場合は、ユーザーに接続の問題が発生していて、パフォーマンスが低下している可能性があります。

- **connections**：このセッション中の接続の総数（1 が正常）
- **DPD_conns**：DPD による再接続の数
- **compression_resets**：圧縮履歴のリセット数
- **decompression_resets**：圧縮解除履歴のリセット数

推奨アクション SVC のログを調べる必要があります。考えられるネットワーク信頼性問題を解決するための調査と適切な処置が必要になる場合もあります。

722030

エラーメッセージ `%Threat Defense-7-722030: Group group User user-name IP IP_address SVC Session Termination: In: data_bytes (+ctrl_bytes ) bytes, data_pkts (+ctrl_pkts ) packets, drop_pkts drops`

説明セッション終了時の統計情報が記録されています。

- **data_bytes**：（SVC からの）着信データ バイト数
- **ctrl_bytes**：着信制御バイト数
- **data_pkts**：着信データ パケット数
- **ctrl_pkts**：着信制御パケット数
- **drop_pkts**：廃棄された着信パケット数

推奨アクション 不要。

722031

エラーメッセージ `%Threat Defense-7-722031: Group group User user-name IP IP_address SVC Session Termination: Out: data_bytes (+ctrl_bytes ) bytes, data_pkts (+ctrl_pkts ) packets, drop_pkts drops.`

説明セッション終了時の統計情報が記録されています。統計には、データバイト、制御パケットバイト、データパケット、制御パケット、およびドロップされたパケットが含まれます。

- **data_bytes**：（SVC への）発信データ バイト数
- **ctrl_bytes**：発信制御バイト数
- **data_pkts**：発信データ パケット数
- **ctrl_pkts**：発信制御パケット数
- **drop_pkts**：ドロップされた発信パケット数

場合によっては、このsyslogがドロップされたパケットの内訳を提供しないため、ドロップされたパケットの数はデータおよび制御パケット全体よりも多くなります。インスタンスの例：

```
2020-09-30T09:06:09.254798+00:00 local4.err pg122d-vpn116 %ASA-3-722031: Group <GP_1>
User <xxxxxxxxxxxx.xxxxxxxxxx@intel.com> IP <x.x.x.x> SVC Session Termination: Out:
800808 (+32) bytes, 1957 (+4) packets, 3358 drops.

2020-09-30T08:53:11.359833+00:00 local4.err srr10c-vpn103 %ASA-3-722031: Group <GP_2>
User <xxxxxxxxxxxx.xxxxxxxxxx@intel.com> IP <x.x.x.x> SVC Session Termination: Out:
413194 (+32) bytes, 1540 (+4) packets, 2059 drops.

2020-09-30T08:37:59.287415+00:00 local4.err srr10c-vpn115 %ASA-3-722031: Group <GP_3>
User <xxxxxxxxxxxx.xxxxxxxxxx@intel.com> IP <x.x.x.x> SVC Session Termination: Out:
571473 (+48) bytes, 1283 (+6) packets, 1323 drops.

2020-09-30T08:31:48.105943+00:00 local4.err srr10c-vpn114 %ASA-3-722031: Group <GP_4>
User <xxxxxxxxxxxx.xxxxxxxxxx@intel.com> IP <x.x.x.x> SVC Session Termination: Out:
131566 (+0) bytes, 283 (+0) packets, 320 drops.

2020-09-30T08:28:38.053003+00:00 local4.err pg122d-vpn117 %ASA-3-722031: Group <GP_5>
User <xxxxxxxxxxxx.xxxxxxxxxx@intel.com> IP <x.x.x.x> SVC Session Termination: Out:
497446 (+23) bytes, 1048 (+1) packets, 1128 drops.

2020-09-30T07:45:43.044373+00:00 local4.err srr10c-vpn114 %ASA-3-722031: Group <GP_6>
User <xxxxxxxxxxxx.xxxxxxxxxx@intel.com> IP <x.x.x.x> SVC Session Termination: Out:
153165 (+16) bytes, 398 (+2) packets, 1045 drops.
```

推奨アクション 不要。

722032

エラーメッセージ `%Threat Defense-5-722032: Group group User user-name IP IP_address New SVC connection replacing old connection.`

説明既存の SVC 接続から新しい SVC 接続に切り替えられようとしています。接続の問題が発生している可能性があります。

推奨アクション SVC ログを確認します。

722033

エラーメッセージ `%Threat Defense-5-722033: Group group User user-name IP IP_address First SVC connection established for SVC session.`

説明 SVC セッションの最初の SVC 接続が確立されました。

推奨アクション 不要。

722034

エラーメッセージ `%Threat Defense-5-722034: Group group User user-name IP IP_address New SVC connection, no existing connection.`

説明再接続が試行されました。すでに閉じられた接続から新しい SVC 接続に切り替えられようとしています。SVC またはSecure Firewall Threat Defense デバイスによって接続がすでに廃棄

されたため、このセッションには既存の接続がありません。接続の問題が発生している可能性があります。

推奨アクション Secure Firewall Threat Defense デバイス のログと SVC のログを調べます。

722035

エラーメッセージ `%Threat Defense-3-722035: Group group User user-name IP IP_address Received large packet length (threshold num ).`

説明大きなパケットがクライアントから受信されました。

- **length**：大きなパケットの長さ
- **num**：しきい値

推奨アクション Secure Firewall Threat Defense デバイスに、DF ビットが設定されて着信するパケットのフラグメント化を許可するには、グループ ポリシーの下で **anyconnect ssl df-bit-ignore enable** コマンドを入力します。

722036

エラーメッセージ `%Threat Defense-3-722036: Group group User user-name IP IP_address Transmitting large packet length (threshold num ).`

説明大きなパケットがクライアントに送信されました。パケットの送信元がクライアントの MTU を認識していない可能性があります。また、圧縮できないデータを圧縮したことが原因の可能性もあります。

- **length**：大きなパケットの長さ
- **num**：しきい値

推奨アクション SVC 圧縮をオフにします。オフになっている場合は、アクションを取る必要はありません。

722037

エラーメッセージ `%Threat Defense-5-722037: Group group User user-name IP IP_address SVC closing connection: reason .`

説明指摘された理由で SVC 接続が終了しました。この動作は正常である場合もあれば、接続の問題が発生している場合もあります。

- **reason**：SVC 接続が終了した理由

推奨アクション SVC ログを調べます。

722038

エラーメッセージ `%Threat Defense-5-722038: Group group-name User user-name IP IP_address SVC terminating session: reason .`

説明指摘された理由でSVCセッションが終了しました。この動作は正常である場合もあれば、接続の問題が発生している場合もあります。

- **reason**：SVC セッションが終了した理由

推奨アクション 終了の理由が予期しないものである場合は、SVC のログを調べます。

722041

エラーメッセージ `%Threat Defense-4-722041: TunnelGroup tunnel_group GroupPolicy group_policy User username IP peer_address No IPv6 address available for SVC connection.`

説明リモート SVC クライアントへの割り当てに使用できる IPv6 アドレスがありませんでした。

- *n*：SVC 接続識別子

推奨アクション 必要に応じて、IPv6 アドレス プールを拡大または作成します。

722042

エラーメッセージ `%Threat Defense-4-722042: Group group User user IP ip Invalid Cisco SSL Tunneling Protocol version.`

説明無効な SVC クライアントまたは AnyConnect クライアントが接続しようとしています。

- *group*：ユーザーの接続試行時に適用するグループ ポリシーの名前
- *user*：接続を試行しているユーザーの名前
- *ip*：接続を試行しているユーザーの IP アドレス

推奨アクション SVC クライアントまたは AnyConnect クライアントが Secure Firewall Threat Defense デバイス と互換性があることを検証します。

722043

エラーメッセージ `%Threat Defense-5-722043: Group group User user IP ip DTLS disabled: unable to negotiate cipher.`

説明 DTLS（UDP トランスポート）を確立できません。SSL 暗号化コンフィギュレーションが変更された可能性があります。

- *group*：ユーザーの接続試行時に適用するグループ ポリシーの名前
- *user*：接続を試行しているユーザーの名前
- *ip*：接続を試行しているユーザーの IP アドレス

推奨アクション SSL暗号化設定を元に戻します。SSL 暗号化コンフィギュレーションに少なくとも 1 つのブロック暗号（AES、DES、または 3DES）が含まれていることを確認します。

722044

エラーメッセージ `%Threat Defense-5-722044: Group group User user IP ip Unable to request ver address for SSL tunnel.`

説明 Secure Firewall Threat Defense デバイス のメモリ不足が原因で、IP アドレスを要求できません。

- *group*：ユーザーの接続試行時に適用するグループ ポリシーの名前
- *user*：接続を試行しているユーザーの名前
- *ip*：接続を試行しているユーザーの IP アドレス
- *ver*：IPv4 または IPv6（要求されている IP アドレスのバージョンに基づく）

推奨アクション Secure Firewall Threat Defense デバイスの負荷を減らすか、または増設メモリを追加します。

722045

エラーメッセージ `%Threat Defense-3-722045: Connection terminated: no SSL tunnel initialization data.`

説明接続を確立するためのデータが欠落しています。これは、Secure Firewall Threat Defense ソフトウェアの障害です。

推奨アクション Cisco TAC に連絡して、サポートを受けてください。

722046

エラーメッセージ `%Threat Defense-3-722046: Group group User user IP ip Session terminated: unable to establish tunnel.`

説明 Secure Firewall Threat Defense デバイス で接続パラメータを設定できません。これは、Secure Firewall Threat Defense ソフトウェアの障害です。

- *group*：ユーザーの接続試行時に適用するグループ ポリシーの名前
- *user*：接続を試行しているユーザーの名前
- *ip*：接続を試行しているユーザーの IP アドレス

推奨アクション Cisco TAC に連絡してサポートを受けてください。

722047

エラーメッセージ `%Threat Defense-4-722047: Group group User user IP ip Tunnel terminated: SVC not enabled or invalid SVC image on the ASA.`

説明ユーザーが Web ブラウザを使用してログインし、SVC または AnyConnect クライアントを起動しようとしました。SVC サービスがグローバルにイネーブルになっていないか、または SVCイメージが無効か破損しています。トンネル接続は終了されましたが、クライアントレス接続は維持されています。

- *group*：ユーザーの接続試行時に適用するグループ ポリシーの名前
- *user*：接続を試行しているユーザーの名前
- *ip*：接続を試行しているユーザーの IP アドレス

推奨アクション **svc enable** コマンドを使用して、SVC をグローバルにイネーブルにします。**svc image** コマンドを使用して新しいイメージをリロードすることで、SVC イメージのバージョンの整合性を検証します。

722048

エラーメッセージ `%Threat Defense-4-722048: Group group User user IP ip Tunnel terminated: SVC not enabled for the user.`

説明 ユーザーが Web ブラウザを使用してログインし、SVC または AnyConnect クライアントを起動しようとしました。このユーザーに対して SVC サービスがイネーブルになっていません。トンネル接続は終了されましたが、クライアントレス接続は維持されています。

- *group*：ユーザーの接続試行時に適用するグループ ポリシーの名前
- *user*：接続を試行しているユーザーの名前
- *ip*：接続を試行しているユーザーの IP アドレス

推奨アクション **group-policy** コマンドと **username** コマンドを使用して、このユーザーに対してサービスを有効にします。

722049

エラーメッセージ `%Threat Defense-4-722049: Group group User user IP ip Session terminated: SVC not enabled or invalid image on the ASA.`

説明 ユーザーが AnyConnect クライアントを使用してログインしました。SVC サービスがグローバルにイネーブルになっていないか、または SVC イメージが無効か破損しています。セッション接続が終了されました。

- *group*：ユーザーの接続試行時に適用するグループ ポリシーの名前
- *user*：接続を試行しているユーザーの名前
- *ip*：接続を試行しているユーザーの IP アドレス

推奨アクション **svc-enable** コマンドを使用して、SVC をグローバルにイネーブルにします。**svc image** コマンドを使用して新しいイメージをリロードすることで、SVC イメージの整合性とバージョンを検証します。

722050

エラーメッセージ `%Threat Defense-4-722050: Group group User user IP ip Session terminated: SVC not enabled for the user.`

説明 ユーザーが AnyConnect クライアントを使用してログインしました。このユーザーに対して SVC サービスがイネーブルになっていません。セッション接続が終了されました。

- *group*：ユーザーの接続試行時に適用するグループ ポリシーの名前
- *user*：接続を試行しているユーザーの名前
- *ip*：接続を試行しているユーザーの IP アドレス

推奨アクション group-policy コマンドと **username** コマンドを使用して、このユーザーに対してサービスを有効にします。

722051

エラーメッセージ `%Threat Defense-6-722051: Group group-policy User username IP public-ip IPv4 Address assigned-ip IPv6 Address assigned-ip  assigned to session`

説明指摘されたアドレスが、指摘されたユーザーに割り当てられました。

- *group-policy*：ユーザーに対してアクセスを許可したグループ ポリシー
- *username*：ユーザーの名前
- *public-ip*：接続されたクライアントのパブリック IP アドレス
- *assigned-ip*：クライアントに割り当てられた IPv4 アドレスまたは IPv6 アドレス

推奨アクション 不要。

722053

エラーメッセージ `%Threat Defense-6-722053: Group g User u IP ip Unknown client user-agent connection.`

説明未知またはサポート対象外の SSL VPN クライアントが Secure Firewall Threat Defense デバイス に接続しました。旧式のクライアントには、Cisco SVC とバージョン 2.3.1 よりも前の Cisco AnyConnect クライアントが含まれます。

- *g*：ユーザーのログイン時に適用されたグループ ポリシー
- *u*：ユーザーの名前
- *ip*：クライアントの IP アドレス
- *user-agent*：クライアントから受信したユーザー エージェント（通常、バージョンを含む）

推奨アクション サポートされている Cisco SSL VPN クライアントにアップグレードします。

722054

エラーメッセージ `%Threat Defense-4-722054: Group group policy User user name IP remote IP SVC terminating connection: Failed to install Redirect URL: redirect URL Redirect ACL: non_exist for assigned IP`

説明リダイレクト URL がインストールされ、ACL が ISE から受信されたが、リダイレクト ACL が Secure Firewall Threat Defense デバイス に存在しない場合に、AnyConnect VPN 接続でエラーが発生しました。

- *group policy*：ユーザーに対してアクセスを許可したグループ ポリシー
- *user name*：リモート アクセスの要求者のユーザー名

- *remote IP*：接続要求の発信元であるリモート IP アドレス
- *redirect URL*：HTTP トラフィック リダイレクションの URL
- *assigned IP*：ユーザーに割り当てられる IP アドレス

推奨アクション Secure Firewall Threat Defense デバイス にリダイレクト ACL を設定します。

722055

エラーメッセージ `%Threat Defense-6-722055: Group group-policy User username IP public-ip Client Type: user-agent`

説明指摘されたユーザーが指摘されたユーザー エージェントに接続しようとしています。

- *group-policy*：ユーザーに対してアクセスを許可したグループ ポリシー
- *username*：ユーザーの名前
- *public-ip*：接続されたクライアントのパブリック IP アドレス
- *user-agent*：接続クライアントによって指定されたユーザーエージェント文字列。通常、AnyConnect クライアントのバージョンと、AnyConnect クライアントのホストオペレーティングシステムが含まれています。

推奨アクション 不要。

722056

エラーメッセージ `%Threat Defense-4-722055: Unsupported AnyConnect client connection rejected from ip address. Client info: user-agent string. Reason: reason`

説明 この syslog は AnyConnect クライアント接続が拒否されたことを示します。この理由は、クライアント情報とともに syslog に示されます。

- *ip address*：古いクライアントとの接続が試行された IP アドレス。
- *user- agent string*：クライアント要求内のユーザーエージェント ヘッダー通常、AnyConnect クライアントのバージョンと、AnyConnect クライアントのホストオペレーティングシステムが含まれています。
- *reason*：拒否の理由。

推奨アクション syslog に示されたクライアント情報と理由を使用して問題を解決します。

メッセージ 723001 ～ 736001

この項では、723001 ～ 736001 のメッセージについて説明します。

723001

エラーメッセージ `%Threat Defense-6-723001: Group group-name , User user-name , IP IP_address : WebVPN Citrix ICA connection connection is up.`

説明 Citrix 接続がアップしています。

- **group-name**：Citrix グループの名前
- **user-name**：Citrix ユーザーの名前
- **IP_address**：Citrix ユーザーの IP アドレス
- **connection**：Citrix 接続識別子

推奨アクション 不要。

723002

エラーメッセージ `%Threat Defense-6-723002: Group group-name , User user-name , IP IP_address : WebVPN Citrix ICA connection connection is down.`

説明 Citrix 接続がダウンしています。

- **group-name**：Citrix グループの名前
- **user-name**：Citrix ユーザーの名前
- **IP_address**：Citrix ユーザーの IP アドレス
- **connection**：Citrix 接続識別子

推奨アクション Citrix ICA 接続がクライアント、サーバー、または Secure Firewall Threat Defense の管理者によって意図的に終了された場合、処置は不要です。それ以外の場合は、Citrix ICA 接続がセットアップされている WebVPN セッションがアクティブであることを確認します。WebVPN セッションが非アクティブである場合、このメッセージの受信は正常です。WebVPN セッションがアクティブである場合は、ICA クライアントと Citrix サーバーの両方が正常に動作すること、およびエラーが表示されていないことを確認します。どちらか一方または両方が正常に動作しない場合、あるいはエラーが表示されている場合は、どちらか一方または両方を起動するか、エラーに対処します。それでもこのメッセージを受信する場合は、Cisco TAC にお問い合わせのうえ、次の情報をご提供ください。

- ネットワーク トポロジ
- 遅延およびパケット損失
- Citrix サーバーのコンフィギュレーション
- Citrix ICA クライアントの情報
- 問題を再現する手順
- 関連するすべてのメッセージの完全なテキスト

723003

エラーメッセージ `%Threat Defense-7-723003: No memory for WebVPN Citrix ICA connection connection .`

説明 Secure Firewall Threat Defense デバイス のメモリが不足しています。Citrix 接続が拒否されました。

- **connection**：Citrix 接続識別子

推奨アクション Secure Firewall Threat Defense デバイス が正常に動作していることを確認します。メモリおよびバッファの使用量に特に注意します。Secure Firewall Threat Defense デバイスに重い負荷がかかっている場合は、増設メモリを購入するか、Secure Firewall Threat Defense デバイスをアップグレードするか、Secure Firewall Threat Defense デバイスの負荷を減らします。問題が解決しない場合、Cisco TAC にお問い合わせください。

723004

エラーメッセージ `%Threat Defense-7-723004: WebVPN Citrix encountered bad flow control` *`flow`* `.`

説明 Secure Firewall Threat Defense デバイス で内部フロー制御のミスマッチが発生しました。この問題は、大量のデータ フロー（ストレス テスト中などに発生）や大量の ICA 接続が原因となっている可能性があります。

推奨アクション Secure Firewall Threat Defense デバイス への ICA 接続を減らします。問題が解決しない場合、Cisco TAC にお問い合わせください。

723005

エラーメッセージ `%Threat Defense-7-723005: No channel to set up WebVPN Citrix ICA connection.`

説明 Secure Firewall Threat Defense デバイス が Citrix 用の新しいチャネルを作成できませんでした。

推奨アクション Citrix ICA クライアントと Citrix サーバーが稼働していることを確認します。稼働していない場合は、起動して、再度テストします。メモリおよびバッファの使用量に特に注意しながら、Secure Firewall Threat Defense デバイスの負荷を確認します。Secure Firewall Threat Defense デバイスに重い負荷がかかっている場合は、Secure Firewall Threat Defense デバイスをアップグレードするか、メモリを追加するか、負荷を減らします。問題が解決しない場合、Cisco TAC にお問い合わせください。

723006

エラーメッセージ `%Threat Defense-7-723006: WebVPN Citrix SOCKS errors.`

説明 Secure Firewall Threat Defense デバイス で内部 Citrix SOCKS エラーが発生しました。

推奨アクション Citrix ICA クライアントが正常に動作していることを確認します。さらに、パケット損失に注意しながら、Citrix ICA クライアントとSecure Firewall Threat Defense デバイスの間のネットワーク接続ステータスを確認します。異常なネットワーク状態がある場合は、それを解決します。問題が解決しない場合、Cisco TAC にお問い合わせください。

723007

エラーメッセージ `%Threat Defense-7-723007: WebVPN Citrix ICA connection` *`connection`* `list is broken.`

説明 Secure Firewall Threat Defense デバイス の内部 Citrix 接続リストが破損しています。

- **connection**：Citrix 接続識別子

推奨アクション メモリおよびバッファの使用量に特に注意しながら、Secure Firewall Threat Defense デバイス が正常に動作していることを確認します。Secure Firewall Threat Defense デバイスに重い負荷がかかっている場合は、Secure Firewall Threat Defense デバイスをアップグレードするか、メモリを追加するか、負荷を減らします。問題が解決しない場合、Cisco TAC にお問い合わせください。

723008

エラーメッセージ `%Threat Defense-7-723008: WebVPN Citrix ICA SOCKS Server server is invalid.`

説明存在しない Citrix Socks サーバーにアクセスしようとしました。

- **server**：Citrix サーバー識別子

推奨アクション Secure Firewall Threat Defense デバイス が正常に動作していることを確認します。メモリまたはバッファのリークがないかどうかに注意してください。この問題が頻繁に発生する場合は、メモリ使用量、ネットワーク トポロジ、およびこのメッセージを受信したときの状態に関する情報を取り込みます。調査のために、これらの情報を Cisco TAC に送信します。このメッセージを受信している間も WebVPN セッションがアップしていることを確認します。アップしていない場合は、WebVPN セッションがダウンしている原因を確認します。Secure Firewall Threat Defense デバイスに重い負荷がかかっている場合は、Secure Firewall Threat Defense デバイスをアップグレードするか、メモリを追加するか、負荷を減らします。問題が解決しない場合、Cisco TAC にお問い合わせください。

723009

エラーメッセージ `%Threat Defense-7-723009: Group group-name , User user-name , IP IP_address : WebVPN Citrix received data on invalid connection connection .`

説明存在しない Citrix 接続に関するデータを受信しました。

- **group-name**：Citrix グループの名前
- **user-name**：Citrix ユーザーの名前
- **IP_address**：Citrix ユーザーの IP アドレス
- **connection**：Citrix 接続識別子

推奨アクション元の公開済み Citrix アプリケーションの接続が終了した可能性があり、残りのアクティブな公開済みアプリケーションが接続を失いました。すべての公開済みアプリケーションを再起動して、新しい Citrix ICA トンネルを生成します。Secure Firewall Threat Defense デバイスに重い負荷がかかっている場合は、Secure Firewall Threat Defense デバイスをアップグレードするか、メモリを追加するか、負荷を減らします。問題が解決しない場合、Cisco TAC にお問い合わせください。

723010

エラーメッセージ `%Threat Defense-7-723010: Group group-name , User user-name , IP IP_address : WebVPN Citrix received closing channel channel for invalid connection connection .`

説明存在しない Citrix 接続に関する中断を受信しました。この問題は、特にネットワーク遅延やパケット損失が発生している間の、大量のデータ フロー（ストレス テストなど）や大量の ICA 接続が原因となっている可能性があります。

- **group-name**：Citrix グループの名前
- **user-name**：Citrix ユーザーの名前
- **IP_address**：Citrix ユーザーの IP アドレス
- channel：Citrix チャネル識別子
- **connection**：Citrix 接続識別子

推奨アクション Secure Firewall Threat Defense デバイス への ICA 接続の数を減らすか、Secure Firewall Threat Defense デバイス 用の増設メモリを入手するか、ネットワークの問題を解決します。

723011

エラーメッセージ `%Threat Defense-7-723011: Group group-name , User user-name , IP IP_address : WebVPN Citrix receives bad SOCKS socks message length msg-length. Expected length is exp-msg-length .`

説明 Citrix SOCKS メッセージの長さが誤っています。

- **group-name**：Citrix グループの名前
- **user-name**：Citrix ユーザーの名前
- **IP_address**：Citrix ユーザーの IP アドレス

推奨アクション Citrix ICA クライアントが正常に動作していることを確認します。さらに、パケット損失に注意しながら、ICA クライアントとSecure Firewall Threat Defense デバイスの間のネットワーク接続ステータスを確認します。異常なネットワーク状態を解決した後も問題が存在する場合は、Cisco TAC にお問い合わせください。

723012

エラーメッセージ `%Threat Defense-7-723012: Group group-name , User user-name , IP IP_address : WebVPN Citrix received bad SOCKS socks message format.`

説明 Citrix SOCKS メッセージの形式が誤っています。

- **group-name**：Citrix グループの名前
- **user-name**：Citrix ユーザーの名前
- **IP_address**：Citrix ユーザーの IP アドレス

推奨アクション Citrix ICA クライアントが正常に動作していることを確認します。さらに、パケット損失に注意しながら、ICA クライアントとSecure Firewall Threat Defense デバイスの間のネットワーク接続ステータスを確認します。異常なネットワーク状態を解決した後も問題が存在する場合は、Cisco TAC にお問い合わせください。

723013

エラーメッセージ `%Threat Defense-7-723013: WebVPN Citrix encountered invalid connection connection during periodic timeout.`

説明 Secure Firewall Threat Defense の内部 Citrix タイマーが期限切れで、Citrix 接続が無効です。

- **connection**：Citrix 接続識別子

推奨アクション Citrix ICA クライアントと Secure Firewall Threat Defense デバイス の間、および Secure Firewall Threat Defense デバイス と Citrix サーバーの間のネットワーク接続を確認します。異常なネットワーク状態、特に遅延とパケット損失を解決します。メモリまたはバッファの問題に特に注意しながら、Secure Firewall Threat Defense デバイスが正常に動作することを確認します。Secure Firewall Threat Defense デバイスに重い負荷がかかっている場合は、増設メモリを入手するか、Secure Firewall Threat Defense デバイスをアップグレードするか、負荷を減らします。問題が解決しない場合、Cisco TAC にお問い合わせください。

723014

エラーメッセージ `%Threat Defense-7-723014: Group group-name , User user-name , IP IP_address : WebVPN Citrix TCP connection connection to server server on channel channel initiated.`

説明 Secure Firewall Threat Defense の内部 Citrix Secure Gateway が Citrix サーバーに接続されています。

- **group-name**：Citrix グループの名前
- **user-name**：Citrix ユーザーの名前
- **IP_address**：Citrix ユーザーの IP アドレス
- **connection**：接続名
- server：Citrix サーバー識別子
- channel：Citrix チャネル識別子（16 進数）

推奨アクション 不要。

724001

エラーメッセージ `%Threat Defense-4-724001: Group group-name User user-name IP IP_address WebVPN session not allowed. Unable to determine if Cisco Secure Desktop was running on the client's workstation.`

説明 Secure Firewall Threat Defense デバイス で CSD Host Integrity Check の結果を処理しているときにエラーが発生したため、セッションが許可されませんでした。

- **group-name**：グループの名前
- **user-name**：ユーザーの名前
- **IP_address**：IP アドレス

推奨アクション クライアント ファイアウォールが長い URL を切り捨てていないかどうかを確認します。クライアントから CSD をアンインストールして、Secure Firewall Threat Defense デバイスに再接続します。

724002

エラーメッセージ `%Threat Defense-4-724002: Group group-name User user-name IP IP_address WebVPN session not terminated. Cisco Secure Desktop was not running on the client's workstation.`

説明 クライアント マシン上で CSD が動作していません。

- **group-name**：グループの名前
- **user-name**：ユーザーの名前
- **IP_address**：IP アドレス

推奨アクション エンドユーザーがクライアント マシンに CSD をインストールして実行できることを確認します。

725001

エラーメッセージ `%Threat Defense-6-725001: Starting SSL handshake with peer-type interface :src-ip /src-port to dst-ip /dst-port for protocol session.`

説明 SSL ハンドシェイクがリモート デバイス（クライアントまたはサーバーのいずれか）から開始されました。

- **peer-type**：接続を開始したデバイスに応じた、サーバーまたはクライアント
- **interface**：SSL セッションが使用しているインターフェイス名
- **source-ip**：送信元の IPv4 アドレスまたは IPv6 アドレス
- **src-port**：送信元ポート番号
- **dst-ip**：宛先 IP アドレス
- **dst-port**：宛先ポート番号
- **protocol**：SSL ハンドシェイクに使用された SSL のバージョン

推奨アクション 不要。

725002

エラーメッセージ `%Threat Defense-6-725002: Device completed SSL handshake with peer-type interface :src-ip /src-port to dst-ip /dst-port for protocol-version session`

説明 リモート デバイスとの SSL ハンドシェイクが正常に完了しました。

- **peer-type**：接続を開始したデバイスに応じた、サーバーまたはクライアント

- **interface**：SSL セッションが使用しているインターフェイス名
- **source-ip**：送信元の IPv4 アドレスまたは IPv6 アドレス
- **src-port**：送信元ポート番号
- *dst-ip*：宛先 IP アドレス
- *dst-port*：宛先ポート番号
- *protocol-version*：使用されている SSL プロトコルのバージョン：SSLv3、TLSv1、DTLSv1、TLSv1.1 または TLSv1.2

推奨アクション 不要。

725003

エラーメッセージ `%Threat Defense-6-725003: SSL peer-type interface :src-ip /src-port to dst-ip /dst-port request to resume previous session.`

説明リモート デバイスが以前の SSL セッションを再開しようとしています。

- **peer-type**：接続を開始したデバイスに応じた、サーバーまたはクライアント
- **interface**：SSL セッションが使用しているインターフェイス名
- **source-ip**：送信元の IPv4 アドレスまたは IPv6 アドレス
- **src-port**：送信元ポート番号
- *dst-ip*：宛先 IP アドレス
- *dst-port*：宛先ポート番号

推奨アクション 不要。

725004

エラーメッセージ `%Threat Defense-6-725004: Device requesting certificate from SSL peer-type interface :src-ip /src-port to dst-ip /dst-port for authentication.`

説明 Secure Firewall Threat Defense デバイス が認証のためにクライアント証明書を要求しました。

- **peer-type**：接続を開始したデバイスに応じた、サーバーまたはクライアント
- **interface**：SSL セッションが使用しているインターフェイス名
- **source-ip**：送信元の IPv4 アドレスまたは IPv6 アドレス
- **src-port**：送信元ポート番号
- *dst-ip*：宛先 IP アドレス
- *dst-port*：宛先ポート番号

推奨アクション 不要。

725005

エラーメッセージ `%Threat Defense-6-725005: SSL peer-type interface :src-ip /src-port to dst-ip /dst-port requesting our device certificate for authentication.`

説明サーバーが認証のために Secure Firewall Threat Defense デバイス の証明書を要求しました。

- **peer-type**：接続を開始したデバイスに応じた、サーバーまたはクライアント
- **interface**：SSL セッションが使用しているインターフェイス名
- **source-ip**：送信元の IPv4 アドレスまたは IPv6 アドレス
- **src-port**：送信元ポート番号
- *dst-ip*：宛先 IP アドレス
- *dst-port*：宛先ポート番号

推奨アクション 不要。

725006

エラーメッセージ `%Threat Defense-6-725006: Device failed SSL handshake with peer-type interface :src-ip /src-port to dst-ip /dst-port`

説明リモート デバイスとの SSL ハンドシェイクが失敗しました。

- **peer-type**：接続を開始したデバイスに応じた、サーバーまたはクライアント
- **interface**：SSL セッションが使用しているインターフェイス名
- **source-ip**：送信元の IPv4 アドレスまたは IPv6 アドレス
- **src-port**：送信元ポート番号
- *dst-ip*：宛先 IP アドレス
- *dst-port*：宛先ポート番号

推奨アクション syslog メッセージ 725014 を検索します。このメッセージに失敗の原因が示されています。

725007

エラーメッセージ `%Threat Defense-6-725007: SSL session with peer-type interface :src-ip /src-port to dst-ip /dst-port terminated.`

説明 SSL セッションが終了しました。

- **peer-type**：接続を開始したデバイスに応じた、サーバーまたはクライアント
- **interface**：SSL セッションが使用しているインターフェイス名
- **source-ip**：送信元の IPv4 アドレスまたは IPv6 アドレス
- **src-port**：送信元ポート番号
- *dst-ip*：宛先 IP アドレス
- *dst-port*：宛先ポート番号

推奨アクション 不要。

725008

エラーメッセージ `%Threat Defense-7-725008: SSL peer-type interface :src-ip /src-port to dst-ip /dst-port proposes the following n cipher(s).`

説明リモート SSL デバイスによって提案された暗号の数が表示されます。

- **peer-type**：接続を開始したデバイスに応じた、サーバーまたはクライアント
- **interface**：SSL セッションが使用しているインターフェイス名
- **source-ip**：送信元の IPv4 アドレスまたは IPv6 アドレス
- **src-port**：送信元ポート番号
- *dst-ip*：宛先 IP アドレス
- *dst-port*：宛先ポート番号
- *n*：サポートされている暗号方式の数

推奨アクション 不要。

725009

エラーメッセージ `%Threat Defense-7-725009 Device proposes the following n cipher(s) peer-type interface :src-ip /src-port to dst-ip /dst-port .`

説明 SSL サーバーに対して提案された暗号の数が表示されます。

- **peer-type**：接続を開始したデバイスに応じた、サーバーまたはクライアント
- **interface**：SSL セッションが使用しているインターフェイス名
- **source-ip**：送信元の IPv4 アドレスまたは IPv6 アドレス
- **src-port**：送信元ポート番号
- *dst-ip*：宛先 IP アドレス
- *dst-port*：宛先ポート番号
- *n*：サポートされている暗号方式の数

推奨アクション 不要。

725010

エラーメッセージ `%Threat Defense-7-725010: Device supports the following n cipher(s).`

説明 SSL セッションのために Secure Firewall Threat Defense デバイス がサポートしている暗号の数が表示されます。

- **n**：サポートされている暗号方式の数

推奨アクション 不要。

725011

エラーメッセージ `%Threat Defense-7-725011 Cipher[order ]: cipher_name`

説明このメッセージは常にメッセージ 725008、725009、および 725010 の後に表示され、暗号名とその優先順位を示しています。

- **order**：暗号リスト内の暗号の順位
- **cipher_name**：暗号リストからの OpenSSL 暗号の名前

推奨アクション 不要。

725012

エラーメッセージ `%Threat Defense-7-725012: Device chooses cipher cipher for the SSL session with peer-type interface :src-ip /src-port to dst-ip /dst-port.`

説明シスコ デバイスが SSL セッション用に選択した暗号が表示されます。

- **cipher**：暗号リストからの OpenSSL 暗号の名前
- **peer-type**：接続を開始したデバイスに応じた、サーバーまたはクライアント
- **interface**：SSL セッションが使用しているインターフェイス名
- **source-ip**：送信元の IPv4 アドレスまたは IPv6 アドレス
- **src-port**：送信元ポート番号
- *dst-ip*：宛先 IP アドレス
- *dst-port*：宛先ポート番号

推奨アクション 不要。

725013

エラーメッセージ `%Threat Defense-7-725013 SSL peer-type interface :src-ip /src-port to dst-ip /dst-port chooses cipher cipher`

説明サーバーが SSL セッション用に選択した暗号を示しています。

- **peer-type**：接続を開始したデバイスに応じた、サーバーまたはクライアント
- **interface**：SSL セッションが使用しているインターフェイス名
- **source-ip**：送信元の IPv4 アドレスまたは IPv6 アドレス
- **src-port**：送信元ポート番号
- *dst-ip*：宛先 IP アドレス
- *dst-port*：宛先ポート番号
- **cipher**：暗号リストからの OpenSSL 暗号の名前

推奨アクション 不要。

725014

エラーメッセージ `%Threat Defense-7-725014 SSL lib error. Function: function Reason: reason`

説明 SSL ハンドシェイクが失敗した原因を示しています。

- **function**：失敗が報告された機能名
- **reason**：失敗状態の説明

推奨アクション SSL 関連の問題を Cisco TAC に報告する場合は、このメッセージを添付します。

725015

エラーメッセージ `%Threat Defense-3-725015 Error verifying client certificate. Public key size in client certificate exceeds the maximum supported key size.`

説明 サポートされていない（大きな）キー サイズが原因で、SSL クライアント証明書の検証が失敗したことを示しています。

推奨アクション 4096 ビット以下のキー サイズのクライアント証明書を使用します。

725016

エラーメッセージ `%Threat Defense-6-725016: Device selects trust-point trustpoint for peer-type interface :src-ip /src-port to dst-ip /dst-port`

説明サーバー名指定（SNI）では、特定の接続に使用された証明書が、インターフェイス上で設定された証明書ではない場合があります。また、どの証明書トラストポイントが選択されたかも示されていません。この syslog は、接続（*interface* :*src-ip* /*src-port* で指定）によって使用されるトラストポイントを示すものです。

- *trustpoint*：指定された接続に使用されている設定済みのトラストポイントの名前
- *interface*：Secure Firewall Threat Defense デバイス 上のインターフェイスの名前
- *src-ip*：ピアの IP アドレス
- *src-port*：ピアのポート番号
- *dst-ip*：宛先の IP アドレス
- *dst-port*：宛先のポート番号

推奨アクション 不要。

725017

エラーメッセージ `%Threat Defense-7-725017: No certificates received during the handshake with %s %s :%B /%d to %B /%d for %s session`

説明リモート クライアントが有効な証明書を送信していません。

- *remote_device*：ハンドシェイクを実行したのがクライアントかサーバーかを示します
- *ctm->interface*：ハンドシェイクが送信されるインターフェイス名
- *ctm->src_ip*：クライアントと通信する SSL サーバーの IP アドレス
- *ctm->src_port*：クライアントと通信する SSL サーバーのポート
- *ctm->dst_ip*：クライアントの IP アドレス
- *ctm->dst_port*：応答が通過するクライアントのポート
- *s->method->version*：トランザクションに関係したプロトコルのバージョン（SSLv3、TLSv1、または DTLSv1）

推奨アクション 不要。

725021

エラーメッセージ `%Threat Defense-7-725021: Device preferring cipher-suite cipher(s). Connection info: interface :src-ip /src-port to dst-ip /dst-port`

説明 このメッセージには、ハンドシェイクのネゴシエーション時に優先される暗号スイートが一覧表示されています。

- **cipher-suite**：優先される暗号スイート文字列
- **interface**：SSL セッションが使用しているインターフェイス名
- **src-ip**：送信元 IPv4 アドレスまたは IPv6 アドレス
- **src-port**：送信元ポート番号
- **dst-ip**：宛先 IPv4 アドレスまたは IPv6 アドレス
- **dst-port**：宛先ポート番号

以下は、ハンドシェイクをネゴシエートするときに使用される、優先される暗号スイート文字列のリストです。

- サーバー
- SUITE-B
- ChaCha20
- クライアント
- SHA-256 ハッシュ

推奨アクション 不要。

725022

エラーメッセージ `%Threat Defense-7-725022: Device skipping cipher : cipher - reason. Connection info: interface :src-ip /src-port to dst-ip /dst-port`

説明 この syslog は、ハンドシェイクのネゴシエーション時に暗号スイートのリストに含まれる特定の暗号をスキップした理由を表示します。

- **cipher-suite**：優先される暗号スイート文字列
- **reason**：暗号をスキップする理由。
- **interface**：SSL セッションが使用しているインターフェイス名
- **src-ip**：送信元 IPv4 アドレスまたは IPv6 アドレス
- **src-port**：送信元ポート番号
- **dst-ip**：宛先 IPv4 アドレスまたは IPv6 アドレス

- **dst-port**：宛先ポート番号

次のリストに、特定の暗号をスキップする理由の例をいくつか示します。

- 一時 EC キーにトラストポイント <trust point> との互換性がない
- プロトコルバージョンによってサポートされていない
- PSK サーバーのコールバックが設定されていない
- セキュリティコールバックによって許可されていない
- Safari の ECDHE-ECDSA が壊れている
- 暗号スイートが SHA256 を使用していない
- 暗号が不明である
- 暗号が間違っている
- メッセージダイジェストが変更されている
- 前のセッションの暗号スイートが選択されていない

推奨アクション 不要。

726001

エラーメッセージ `%Threat Defense-6-726001: Inspected im_protocol im_service Session between Client im_client_1 and im_client_2 Packet flow from src_ifc :/sip /sport to dest_ifc :/dip /dport Action: action Matched Class class_map_id class_map_name`

説明 IM メッセージに対して検査が実施され、指定の基準が満たされました。設定済みのアクションが実行されます。

- *im_protocol*：MSN IM または Yahoo IM
- *im_service*：IM サービス（チャット、会議、ファイル転送、音声、ビデオ、ゲーム、不明など）
- *im_client_1*、*im_client_2*：セッションで IM サービスを使用しているクライアント ピア（*client_login_name* または「?」）
- *src_ifc*：送信元インターフェイス名
- *sip*：送信元 IP アドレス
- *sport*：送信元ポート
- *dest_ifc*：宛先インターフェイス名
- *dip*：宛先 IP アドレス
- *dport*：宛先ポート
- *action*：実行されるアクション（接続のリセット、接続の廃棄、または受信）
- *class_map_id*：一致したクラス マップ ID
- *class_map_name*：一致したクラス マップ名

推奨アクション 不要。

733100

エラーメッセージ `%Threat Defense-4-733100: Object drop rate rate_ID exceeded. Current burst rate is rate_val per second, max configured rate is rate_val ; Current average rate is rate_val per second, max configured rate is rate_val ; Cumulative total count is total_cnt`

説明このメッセージで指摘されたオブジェクトが、指摘されたバーストしきい値レートまたは平均しきい値レートを超えました。このオブジェクトには、ホスト、TCP/UDP ポート、IP プロトコルの廃棄アクティビティなど、攻撃の可能性に起因するさまざまな廃棄が考えられます。Secure Firewall Threat Defense デバイス が攻撃を受けている可能性があります。

- *Object*：ドロップ レート カウントの一般的な送信元または特定の送信元。次が含まれる場合があります

- Firewall

- Bad pkts

- Rate limit

- DoS attck

- ACL drop

- Conn limit

- ICMP attk

- Scanning

- SYN attck

- Inspect

- Interface

（特定のインターフェイス オブジェクトを示すために、さまざまな形式が使用されることがあります。たとえば、周知のプロトコル HTTP のポート 80 を意味する **80/HTTP** が表示されることがあります）

- *rate_ID*：超過している設定レート。ほとんどのオブジェクトでは、異なる間隔で最大3つの異なるレートを設定できます。
- *rate_val*：特定のレート値。
- *total_cnt*：オブジェクトが作成されたか、またはクリアされてからの合計カウント。

次の 3 つの例は、これらの変数がどのように表示されるかを示しています。

- CPU またはバスの制限に起因するインターフェイス廃棄の場合

```
%Threat Defense-4-733100: [Interface] drop rate 1 exceeded. Current burst rate is 1 per
 second, max configured rate is 8000; Current average rate is 2030 per second, max
configured rate is 2000; Cumulative total count is 3930654.”
```

- 攻撃の可能性に起因するスキャニング廃棄の場合

```
%Threat Defense-4-733100: [Scanning] drop rate-1 exceeded. Current burst rate is 10 per
 second_max configured rate is 10; Current average rate is 245 per second_max configured
 rate is 5; Cumulative total count is 147409 (35 instances received)
```

- 攻撃の可能性に起因する不良パケットの場合

```
%Threat Defense-4-733100: [Bad pkts] drop rate 1 exceeded. Current burst rate is 0 per
second, max configured rate is 400; Current average rate is 760 per second, max configured
 rate is 100; Cumulative total count is 1938933
```

- 設定されたスキャン レートおよび **threat-detection rate scanning-rate 3600 average-rate 15** コマンドによる場合

```
%Threat Defense-4-733100: [144.60.88.2] drop rate-2 exceeded. Current burst rate is 0
per second, max configured rate is 8; Current average rate is 5 per second, max configured
 rate is 4; Cumulative total count is 38086
```

メッセージに示されている指定オブジェクト タイプに応じて、次の手順を実行します。

1. メッセージ内のオブジェクトが次のいずれかの場合
   - Firewall
   - Bad pkts
   - Rate limit
   - DoS attck
   - ACL drop
   - Conn limit
   - ICMP attck
   - Scanning
   - SYN attck
   - Inspect
   - Interface

推奨アクション ドロップ レートが実行時環境で許容可能かどうかを確認します。

1. threat-detection rate xxx コマンドを使用して、特定のドロップのしきい値レートを適切な値に調整します。ここで、*xxx* は次のいずれかです。
   - acl-drop
   - bad-packet-drop
   - conn-limit-drop
   - dos-drop
   - fw-drop
   - icmp-drop
   - inspect-drop
   - interface-drop
   - scanning-threat
   - syn-attack
2. メッセージ内のオブジェクトが TCP/UDP ポート、IP アドレス、またはホストの廃棄である場合は、実行環境でその廃棄レートを許容できるかどうかを確認します。

3. threat-detection rate bad-packet-drop コマンドを使用して特定のドロップのしきい値レートを適切な値に調整します。

（注） ドロップ レート超過の警告を表示させたくない場合は、no threat-detection basic-threat コマンドを使用してディセーブルにすることができます。

733101

エラーメッセージ `%Threat Defense-4-733101: Object objectIP (is targeted|is attacking). Current burst rate is rate_val per second, max configured rate is rate_val ; Current average rate is rate_val per second, max configured rate is rate_val ; Cumulative total count is total_cnt.`

説明 Secure Firewall Threat Defense デバイス が特定のホスト（または同じ 1024 ノード サブネット内の複数のホスト）がネットワークをスキャンしている（攻撃している）か、またはスキャンされている（ターゲットとなっている）ことが検出されました。

- *object*：攻撃者またはターゲット（特定のホストまたは同じ 1024 ノードサブネット内の複数のホスト）
- *objectIP*：スキャンしている攻撃者またはスキャンされているターゲットの IP アドレス
- *rate_val*：特定のレート値
- *total_cnt*：合計カウント

次の 2 つの例は、これらの変数がどのように表示されるかを示しています。

```
%Threat Defense-4-733101: Subnet 100.0.0.0 is targeted. Current burst rate is 200 per
second, max configured rate is 0; Current average rate is 0 per second, max configured
rate is 0; Cumulative total count is 2028.
%Threat Defense-4-733101: Host 175.0.0.1 is attacking. Current burst rate is 200 per
second, max configured rate is 0; Current average rate is 0 per second, max configured
rate is 0; Cumulative total count is 2024
```

推奨アクション特定のホストまたはサブネットに対して、**show threat-detection statistics host ip-address ip-mask** コマンドを使用し、全体的な状況を確認してから、脅威スキャンのしきい値レートを適切な値に調整します。適切な値を確定したら、**threat-detection scanning-threat shun-host** コマンドを設定して、ホスト攻撃者（サブネット攻撃者ではない）を排除するためのオプションの処置を行うことができます。shun-host except リストで、特定のホストまたはオブジェクト グループを指定できます。詳細については、CLI 設定ガイドを参照してください。スキャンの検出が必要ない場合は、**no threat-detection scanning** コマンドを使用してこの機能をディセーブルにできます。

733102

エラーメッセージ `%Threat Defense-4-733102:Threat-detection adds host %I to shun list`

説明脅威検出エンジンによってホストが排除されました。**threat-detection scanning-threat shun** コマンドが設定されている場合、攻撃しているホストは脅威検出エンジンによって排除されます。

- *%I*：特定のホスト名

次のメッセージは、このコマンドがどのように実装されるかを示しています。

```
%Threat Defense-4-733102: Threat-detection add host 11.1.1.40 to shun list
```

推奨アクション排除されたホストが実際の攻撃者であるかどうかを調査するには、**threat-detection statistics host ip-address** コマンドを使用します。排除されたホストが攻撃者でない場合は、**clear threat-detection shun ip address** コマンドを使用して、排除されたホストを脅威検出エンジンから削除できます。排除されたすべてのホストを脅威検出エンジンから削除するには、**clear shun** コマンドを使用します。

不適切なしきい値レート設定によって脅威検出エンジンがトリガーされたために、このメッセージを受信した場合は、**threat-detection rate scanning-threat rate-interval x average-rate y burst-rate z** コマンドを使用して、しきい値レートを調整します。

733103

エラーメッセージ `%Threat Defense-4-733103: Threat-detection removes host %I from shun list`

説明脅威検出エンジンによってホストが排除されました。**clear-threat-detection shun** コマンドを使用すると、指摘されたホストが排除リストから削除されます。

- *%I*：特定のホスト名

次のメッセージは、このコマンドがどのように実装されるかを示しています。

```
%Threat Defense-4-733103: Threat-detection removes host 11.1.1.40 from shun list
```

推奨アクション 不要。

733104

エラーメッセージ `%Threat Defense-4-733104: TD_SYSLOG_TCP_INTERCEPT_AVERAGE_RATE_EXCEED`

説明 Secure Firewall Threat Defense デバイスが SYN フラッドアタックを受けているが、TCP 代行受信メカニズムによって保護されています（代行受信される攻撃の平均レートがしきい値の設定値を超えた場合）。メッセージに、攻撃を受けているサーバーと攻撃元が示されます。

推奨アクション攻撃を除外するための ACL を作成します。

733105

エラーメッセージ `%Threat Defense-4-733105: TD_SYSLOG_TCP_INTERCEPT_BURST_RATE_EXCEED`

説明 Secure Firewall Threat Defense デバイスが SYN フラッドアタックを受けているが、TCP 代行受信メカニズムによって保護されています（代行受信される攻撃のバーストレートがしきい値の設定値を超えた場合）。メッセージに、攻撃を受けているサーバーと攻撃元が示されます。

推奨アクション攻撃を除外するための ACL を作成します。

734001

エラーメッセージ `%Threat Defense-6-734001: DAP: User user, Addr ipaddr , Connection connection : The following DAP records were selected for this connection: DAP record names`

説明接続用に選択された DAP レコードが表示されます。

- *user*：認証されたユーザー名
- *ipaddr*：リモート クライアントの IP アドレス
- *connection*：クライアント接続のタイプ。次のいずれかです。

- IPsec

- AnyConnect

- Clientless（Web ブラウザ）

- Cut-Through-Proxy

- L2TP

- *DAP record names*：DAP レコード名のカンマ区切りリスト

推奨アクション 不要。

734002

エラーメッセージ `%Threat Defense-5-734002: DAP: User user, Addr ipaddr : Connection terrminated by the following DAP records: DAP record names`

説明接続を終了した DAP レコードが表示されます。

- *user*：認証されたユーザー名
- *ipaddr*：リモート クライアントの IP アドレス
- *DAP record names*：DAP レコード名のカンマ区切りリスト

推奨アクション 不要。

734003

エラーメッセージ `%FTD-7-734003: DAP: User name , Addr ipaddr : Session Attribute: attr name/value`

説明接続に関連付けられている、AAA とエンドポイントのセッション属性が表示されます。

- *user*：認証されたユーザー名
- *ipaddr*：リモート クライアントの IP アドレス
- *attr/value*：AAA またはエンドポイントの属性名と値

推奨アクション 不要。

734004

エラーメッセージ `%FTD-3-734004: DAP: Processing error: internal error code`

説明 DAP 処理エラーが発生しました。

- *internal error code*：内部エラー文字列

推奨アクション **debug dap errors** コマンドをイネーブルにし、DAP 処理をもう一度実行して、さらにデバック情報を取得します。これで問題が解決しない場合は、Cisco TAC に連絡し、内部エラー コードと、エラーを発生させた状態に関する情報を提供します。

735001

エラーメッセージ `%FTD-1-735001 IPMI: Cooling Fan var1 : OK`

説明冷却ファンが正常な動作に復元されました。

- *var1*：デバイス番号マーキング

推奨アクション 不要。

735002

エラーメッセージ `%FTD-1-735002 IPMI: Cooling Fan var1 : Failure Detected`

説明冷却ファンで障害が発生しています。

- *var1*：デバイス番号マーキング

推奨アクション：次のステップを実行します。

1. ファンの回転を妨げる障害物がないかどうかを確認します。
2. 冷却ファンを交換します。
3. 問題が解決しない場合、メッセージをそのまま記録し、Cisco TAC にお問い合わせください。

735003

エラーメッセージ `%FTD-1-735003 IPMI: Power Supply var1 : OK`

説明電源モジュールが正常な動作に復元されました。

- *var1*：デバイス番号マーキング

推奨アクション 不要。

735004

エラーメッセージ `%FTD-1-735004 IPMI: Power Supply var1 : Failure Detected`

説明 AC 電源が失われたか、または電源モジュールで障害が発生しています。

- *var1*：デバイス番号マーキング

推奨アクション：次のステップを実行します。

1. AC 電源障害の有無を確認します。
2. 電源装置を交換してください。
3. 問題が解決しない場合、メッセージをそのまま記録し、Cisco TAC にお問い合わせください。

735005

エラーメッセージ `%FTD-1-735005 IPMI: Power Supply Unit Redundancy OK`

説明電源装置の冗長性が復元されました。

推奨アクション 不要。

735006

エラーメッセージ `%FTD-1-735006 IPMI: Power Supply Unit Redundancy Lost`

説明電源障害が発生しました。電源装置の冗長性は失われましたが、Secure Firewall Threat Defense デバイス は最小限のリソースで正常に機能しています。これ以上の障害が発生した場合は、Secure Firewall Threat Defense デバイス はシャットダウンされます。

推奨アクション 完全な冗長性を取り戻すには、次の手順を実行します。

1. AC 電源障害の有無を確認します。
2. 電源装置を交換してください。
3. 問題が解決しない場合、メッセージをそのまま記録し、Cisco TAC にお問い合わせください。

735007

エラーメッセージ `%FTD-1-735007 IPMI: CPU var1 : Temp: var2 var3 , Critical`

説明 CPU が臨界温度に達しました。

- *var1*：デバイス番号マーキング
- *var2*：温度値
- *var3*：温度値の単位（C、F）

推奨アクション メッセージをそのまま記録し、Cisco TAC にお問い合わせください。

735008

エラーメッセージ `%FTD-1-735008 IPMI: Chassis Ambient var1 : Temp: var2 var3 , Critical`

説明シャーシの周囲温度センサーが臨界レベルに達しました。

- *var1*：デバイス番号マーキング
- *var2*：温度値
- *var3*：温度値の単位（C、F）

推奨アクション メッセージをそのまま記録し、Cisco TAC にお問い合わせください。

735009

エラーメッセージ `%FTD-2-735009: IPMI: Environment Monitoring has failed initialization and configuration. Environment Monitoring is not running.`

説明 初期化中に環境モニタリングに致命的なエラーが発生したため、続行できませんでした。

推奨アクション **show environment** コマンドと **debug ipmi** コマンドの出力を収集します。メッセージをそのまま記録し、Cisco TAC にお問い合わせください。

735010

エラーメッセージ `%FTD-3-735010: IPMI: Environment Monitoring has failed to update one or more of its records.`

説明環境モニタリングで、1 つまたは複数のレコードのアップデートを一時的に妨げるエラーが発生しました。

推奨アクション このメッセージが繰り返し表示される場合は、**show environment driver** コマンドと **debug ipmi** コマンドの出力を収集します。メッセージをそのまま記録し、Cisco TAC にお問い合わせください。

735011

エラーメッセージ `%FTD-1-735011: Power Supply var1 : Fan OK`

説明電源ファンが動作状態に戻りました。

- *var1*：ファンの番号

推奨アクション 不要。

735012

エラーメッセージ `%Threat Defense-1-735012: Power Supply var1 : Fan Failure Detected`

説明電源ファンに障害が発生しました。

- *var1*：ファンの番号

推奨アクション Cisco TAC に連絡して、障害のトラブルシューティングを行ってください。この障害が解決するまで装置の電源をオフにします。

735013

エラーメッセージ `%FTD-1-735013: Voltage Channel var1 : Voltage OK`

説明電圧チャネルが正常な動作レベルに戻りました。

- *var1*：電圧チャネルの番号

推奨アクション 不要。

735014

エラーメッセージ `%FTD-1-735014: Voltage Channel var1: Voltage Critical`

説明電圧チャネルが重大レベルに変化しました。

- *var1*：電圧チャネルの番号

推奨アクション Cisco TAC に連絡して、障害のトラブルシューティングを行ってください。この障害が解決するまで装置の電源をオフにします。

735015

エラーメッセージ `%FTD-4-735015: CPU var1 : Temp: var2 var3 , Warm`

説明 CPU の温度が正常な動作範囲よりも高くなっています。

- *var1*：CPU の番号
- *var2*：温度値
- *var3*：単位

推奨アクションこのコンポーネントの監視を続行し、危険な温度に到達しないようにします。

735016

エラーメッセージ `%FTD-4-735016: Chassis Ambient var1 : Temp: var2 var3 , Warm`

説明シャーシの温度が正常な動作範囲よりも高くなっています。

- *var1*：シャーシ センサーの番号
- *var2*：温度値
- *var3*：単位

推奨アクションこのコンポーネントの監視を続行し、危険な温度に到達しないようにします。

735017

エラーメッセージ `%Threat Defense-1-735017: Power Supply var1 : Temp: var2 var3 , OK`

説明電源装置の温度が正常な動作温度に戻りました。

- *var1*：電源装置の番号
- *var2*：温度値
- *var3*：単位

推奨アクション 不要。

735018

エラーメッセージ `%FTD-4-735018: Power Supply var1 : Temp: var2 var3 , Critical`

説明電源装置が危険な動作温度に達しました。

- *var1*：電源装置の番号
- *var2*：温度値
- *var3*：単位

推奨アクションCisco TAC に連絡して、障害のトラブルシューティングを行ってください。この障害が解決するまで装置の電源をオフにします。

735019

エラーメッセージ `%FTD-4-735019: Power Supply var1 : Temp: var2 var3 , Warm`

説明電源装置の温度が正常な動作範囲よりも高くなっています。

- *var1*：電源装置の番号
- *var2*：温度値
- *var3*：単位

推奨アクションこのコンポーネントの監視を続行し、危険な温度に到達しないようにします。

735020

エラーメッセージ `%FTD-1-735020: CPU var1: Temp: var2 var3 OK`

説明 CPU の温度が正常な動作温度に戻りました。

- *var1*：CPU の番号
- *var2*：温度値
- *var3*：単位

推奨アクション 不要。

735021

エラーメッセージ `%FTD-1-735021: Chassis var1: Temp: var2 var3 OK`

説明シャーシの温度が正常な動作温度に戻りました。

- *var1*：シャーシ センサーの番号
- *var2*：温度値
- *var3*：単位

推奨アクション 不要。

735022

エラーメッセージ `%FTD-1-735022: CPU# is running beyond the max thermal operating temperature and the device will be shutting down immediately to prevent permanent damage to the CPU.`

説明 Secure Firewall Threat Defense デバイス は、CPU が最大動作温度を超えたことを検出しました。検出直後にシャット ダウンします。

推奨アクション シャーシおよび CPU に通気の問題がないか、ただちに検査する必要があります。

735023

エラーメッセージ `%FTD-2-735023: ASA was previously shutdown due to the CPU complex running beyond the maximum thermal operating temperature. The chassis needs to be inspected immediately for ventilation issues.`

説明 Secure Firewall Threat Defense デバイス は、CPU が最大安全動作温度を超えて稼働していたために発生したシャットダウンを検出しました。**show environment** コマンドを使用すると、このイベントが発生したことが示されます。

推奨アクション シャーシをただちに調査し、換気に問題がないことを確認する必要があります。

735024

エラーメッセージ `%Threat Defense-1-735024: IO Hub var1 : Temp: var2 var3 , OK`

説明 IO ハブの温度が正常な動作温度に戻りました。

- *ar1*：IO ハブの番号
- *var2*：温度値
- *var3*：単位

推奨アクション 不要。

735025

エラーメッセージ `%FTD-1-735025: IO Hub var1 : Temp: var2 var3 , Critical`

説明 IO ハブの温度が危険な温度に達しました。

- *ar1*：IO ハブの番号
- *var2*：温度値
- *var3*：単位

推奨アクション メッセージを表示されているとおりに記録し、Cisco TAC にお問い合わせください。

735026

エラーメッセージ `%FTD-4-735026: IO Hub var1 : Temp: var2 var3 , Warm`

説明 IO ハブの温度が正常な動作範囲よりも高くなっています。

- *ar1*：IO ハブの番号
- *var2*：温度値
- *var3*：単位

推奨アクション このコンポーネントの監視を続行し、クリティカル温度に達しないようにします。

735027

エラーメッセージ `%FTD-1-735027: CPU cpu_num Voltage Regulator is running beyond the max thermal operating temperature and the device will be shutting down immediately. The chassis and CPU need to be inspected immediately for ventilation issues.`

説明 Secure Firewall Threat Defense デバイス は CPU の電圧レギュレータが最大熱動作温度を超えて稼働していることを検出しました。検出後にただちにシャットダウンします。

- *cpu_num*：熱イベントを発生させた CPU 電圧レギュレータを識別する番号

推奨アクション シャーシおよび CPU に通気の問題がないか、ただちに検査する必要があります。

735028

エラーメッセージ `%FTD-2-735028: ASA was previously shutdown due to a CPU Voltage Regulator running beyond the max thermal operating temperature. The chassis and CPU need to be inspected immediately for ventilation issues.`

説明 Secure Firewall Threat Defense デバイス は、CPU 電圧レギュレータが最大安全動作温度を超えて稼働していたために発生したシャットダウンを検出しました。**show environment** コマンドを入力すると、このイベントが発生したことが示されます。

推奨アクション シャーシおよび CPU に通気の問題がないか、ただちに検査する必要があります。

735029

エラーメッセージ `%FTD-1-735029: IO Hub is running beyond the max thermal operating temperature and the device will be shutting down immediately to prevent permanent damage to the circuit.`

説明 Secure Firewall Threat Defense デバイス は、IO ハブが最大動作温度を超えたことを検出しました。検出直後にシャット ダウンします。

推奨アクション シャーシと IO ハブをただちに調査し、換気に問題がないことを確認する必要があります。

736001

エラーメッセージ `%FTD-2-736001: Unable to allocate enough memory at boot for jumbo-frame reservation. Jumbo-frame support has been disabled.`

説明 ジャンボ フレーム サポートを設定していたときに、メモリの不足が検出されました。その結果、ジャンボフレーム サポートがディセーブルになりました。

推奨アクション **jumbo-frame reservation** コマンドを使用して、ジャンボ フレーム サポートをもう一度イネーブルにしてみてください。実行コンフィギュレーションを保存し、Secure Firewall Threat Defense デバイス をリブートします。問題が解決しない場合、Cisco TAC にお問い合わせください。

メッセージ 737001 ～ 776254

この項では、737001 ～ 776254 のメッセージについて説明します。

737001

エラーメッセージ `%FTD-7-737001: IPAA: Received message` *`message-type`*

説明 IP アドレス割り当てプロセスはメッセージを受信しました。

- *message-type*：IP アドレス割り当てプロセスで受信したメッセージ

推奨アクション 不要。

737002

エラーメッセージ `%FTD-3-737002: IPAA: Session=` *`session`*`,Received unknown message` *`num`* `variables`

説明 IP アドレス割り当てプロセスはメッセージを受信しました。

- *session*：16 進数の VPN セッション ID
- *num*：IP アドレス割り当てプロセスで受信したメッセージの識別子

推奨アクション 不要。

737003

エラーメッセージ `%FTD-5-737003: IPAA: Session= session, DHCP configured, no viable servers found for tunnel-group tunnel-group`

説明指摘されたトンネル グループの DHCP サーバー コンフィギュレーションが無効です。

- *session*：16 進数の VPN セッション ID
- *tunnel-group*：IP アドレス割り当てでコンフィギュレーションに使用されているトンネル グループ

推奨アクション トンネル グループの DHCP 設定を検証します。DHCP サーバーがオンラインであることを確認します。

737004

エラーメッセージ `%Threat Defense-5-737004: IPAA: Session= session, DHCP configured, request failed for tunnel-group 'tunnel-group'`

説明指摘されたトンネル グループの DHCP サーバー コンフィギュレーションが無効です。

- *session*：16 進数の VPN セッション ID
- *tunnel-group*：IP アドレス割り当てでコンフィギュレーションに使用されているトンネル グループ

推奨アクション トンネル グループの DHCP 設定を検証します。DHCP サーバーがオンラインであることを確認します。

737005

エラーメッセージ `%FTD-6-737005: IPAA: Session= session, DHCP configured, request succeeded for tunnel-group tunnel-group`

説明 DHCP サーバー要求が成功しました。

- *session*：16 進数の VPN セッション ID
- *tunnel-group*：IP アドレス割り当てでコンフィギュレーションに使用されているトンネル グループ

推奨アクション 不要。

737006

エラーメッセージ `%FTD-6-737006: IPAA: Session= session, Local pool request succeeded for tunnel-group tunnel-group`

説明ローカル プール要求が成功しました。

- *session*：16 進数の VPN セッション ID
- *tunnel-group*：IP アドレス割り当てでコンフィギュレーションに使用されているトンネル グループ

推奨アクション 不要。

737007

エラーメッセージ `%FTD-5-737007: IPAA: Session= session, Local pool request failed for tunnel-group tunnel-group`

説明ローカル プール要求が失敗しました。トンネル グループに割り当てられているプールが枯渇している可能性があります。

- *session*：16 進数の VPN セッション ID
- *tunnel-group*：IP アドレス割り当てでコンフィギュレーションに使用されているトンネル グループ

推奨アクション **show ip local pool** コマンドを使用して、IP ローカル プールの設定を検証します。

737008

エラーメッセージ `%FTD-5-737008: IPAA: Session= session, 'tunnel-group' not found`

説明コンフィギュレーション用の IP アドレスを取得しようとしたときに、トンネル グループが見つかりませんでした。このメッセージは、ソフトウェア障害が原因で生成される場合があります。

- *session*：16 進数の VPN セッション ID
- *tunnel-group*：IP アドレス割り当てでコンフィギュレーションに使用されているトンネル グループ

推奨アクション トンネル グループ設定を確認しますCisco TAC に問い合わせて、問題を報告してください。

737009

エラーメッセージ `%FTD-6-737009: IPAA: Session= session, AAA assigned address ip-address , request failed`

説明リモート アクセス クライアント ソフトウェアが特定のアドレスの使用を要求しました。AAA サーバーに対する対象のアドレスの使用要求が失敗しました。アドレスが使用中の可能性があります。

- *session*：16 進数の VPN セッション ID
- *ip-address*：クライアントが要求した IPv4 アドレスまたは IPv6 アドレス

推奨アクションAAA サーバーのステータスと IP ローカル プールのステータスを確認します。

737010

エラーメッセージ `%FTD-6-737010: IPAA: Session= session, AAA assigned address ip-address , request succeeded`

説明リモート アクセス クライアント ソフトウェアが特定のアドレスの使用を要求し、対象のアドレスを正常に受け取りました。

- *session*：16 進数の VPN セッション ID
- *ip-address*：クライアントが要求した IPv4 アドレスまたは IPv6 アドレス

推奨アクション 不要。

737011

エラーメッセージ `%FTD-5-737011: IPAA: Session= session, AAA assigned ip-address , not permitted, retrying`

説明リモート アクセス クライアント ソフトウェアが特定のアドレスの使用を要求しました。**vpn-addr-assign aaa** コマンドが設定されていません。その代わりとして設定されているアドレス割り当て方法が使用されます。

- *session*：16 進数の VPN セッション ID
- *ip-address*：クライアントが要求した IPv4 アドレスまたは IPv6 アドレス

推奨アクション クライアントがそれら自体のアドレスを指定することを許可する場合は、**vpn-addr-assign aaa** コマンドをイネーブルにします。

737012

エラーメッセージ `%FTD-4-737012: IPAA: Session= session, Address assignment failed`

説明リモート アクセス クライアント ソフトウェアによる特定のアドレスの要求が失敗しました。

- *session*：16 進数の VPN セッション ID
- *ip-address*：クライアントが要求した IP アドレス

推奨アクション IP ローカル プールを使用している場合は、ローカル プールの設定を検証します。AAA を使用している場合は、AAA サーバーのコンフィギュレーションとステータスを検

証します。DHCP を使用している場合は、DHCP サーバーのコンフィギュレーションとステータスを検証します。ログ レベルを上げて（通知または情報を使用）、失敗の原因を示す追加のメッセージを取得します。

737013

エラーメッセージ `%FTD-4-737013: IPAA: Session= session, Error freeing address ip-address , not found`

説明 Secure Firewall Threat Defense デバイス がアドレスを解放しようとしましたが、最近のコンフィギュレーション変更により、そのアドレスが割り当て済みリストにありませんでした。

- *session*：16 進数の VPN セッション ID
- *ip-address*：解放対象の IPv4 アドレスまたは IPv6 アドレス

推奨アクションアドレスの割り当て設定を検証します。このメッセージが引き続き発生する場合は、ソフトウェア障害が原因となっている可能性があります。Cisco TAC に問い合わせて、問題を報告してください。

737014

エラーメッセージ `%FTD-6-737014: IPAA: Session= session, Freeing AAA address ip-address`

説明 Secure Firewall Threat Defense デバイス が、AAA を使用して割り当てられた IP アドレスを正常に解放しました。

- *session*：16 進数の VPN セッション ID
- *ip-address*：解放対象の IPv4 アドレスまたは IPv6 アドレス

推奨アクション 不要。

737015

エラーメッセージ `%Threat Defense-6-737015: IPAA: Session= session, Freeing DHCP address ip-address`

説明 Secure Firewall Threat Defense デバイス が、DHCP を使用して割り当てられた IP アドレスを正常に解放しました。

- *session*：16 進数の VPN セッション ID
- *ip-address*：解放対象の IP アドレス

推奨アクション 不要。

737016

エラーメッセージ `%FTD-6-737016: IPAA: Session= session, Freeing local pool pool-name address ip-address`

説明 Secure Firewall Threat Defense デバイス が、ローカル プールを使用して割り当てられた IP アドレスを正常に解放しました。

- *session*：16 進数の VPN セッション ID
- *ip-address*：解放対象の IPv4 アドレスまたは IPv6 アドレス
- *pool-name*：アドレスが返されているプール

推奨アクション 不要。

737017

エラーメッセージ `%FTD-6-737017: IPAA: Session= session, DHCP request attempt num succeeded`

説明 Secure Firewall Threat Defense デバイス が DHCP サーバーに要求を正常に送信しました。

- *session*：16 進数の VPN セッション ID
- *num*：試行回数

推奨アクション 不要。

737018

エラーメッセージ `%FTD-5-737018: IPAA: Session= session, DHCP request attempt num failed`

説明 Secure Firewall Threat Defense デバイス が DHCP サーバーに要求を送信できませんでした。

- *session*：16 進数の VPN セッション ID
- *num*：試行回数

推奨アクション DHCP の設定と DHCP サーバーへの接続を検証します。

737019

エラーメッセージ `%FTD-4-737019: IPAA: Session= session, Unable to get address from group-policy or tunnel-group local pools`

説明 Secure Firewall Threat Defense デバイス が、グループ ポリシーまたはトンネル グループに設定されているローカル プールからアドレスを取得できませんでした。ローカル プールが枯渇している可能性があります。

- *session*：16 進数の VPN セッション ID

推奨アクション ローカル プールのコンフィギュレーションとステータスを検証します。ローカルプールのグループポリシーとトンネルグループのコンフィギュレーションを検証します。

737023

エラーメッセージ `%FTD-5-737023: IPAA: Session= session, Unable to allocate memory to store local pool address ip-address`

説明 Secure Firewall Threat Defense デバイス のメモリが不足しています。

- *session*：16 進数の VPN セッション ID
- *ip-address*：取得された IP アドレス

推奨アクション Secure Firewall Threat Defense デバイス の負荷が高くなっているためにより多くのメモリが必要になっているか、またはソフトウェアの不具合によってメモリ リークが生じている可能性があります。Cisco TAC に問い合わせて、問題を報告してください。

737024

エラーメッセージ `%FTD-5-737024: IPAA: Session= session, Client requested address ip-address , already in use, retrying`

説明クライアントが要求した IP アドレスはすでに使用されています。要求は、新しい IP アドレスを使用して試行されます。

- *session*：16 進数の VPN セッション ID
- *ip-address*：クライアントが要求した IP アドレス

推奨アクション 不要。

737025

エラーメッセージ `%FTD-5-737025: IPAA:Session= session, Duplicate local pool address found, ip-address in quarantine`

説明クライアントに渡されることになっていた IP アドレスはすでに使用されています。IP アドレスはプールから削除され、再び使用されることはありません。

- *session*：16 進数の VPN セッション ID
- *ip-address*：取得された IP アドレス

推奨アクション ローカル プールの設定を検証します。ソフトウェアの不具合によって重複が発生している可能性があります。Cisco TAC に問い合わせて、問題を報告してください。

737026

エラーメッセージ `%FTD-6-737026: IPAA:Session= session, Client assigned ip-address from local pool pool-name`

説明指摘されたアドレスがローカル プールから割り当てられました。

- *session*：16 進数の VPN セッション ID

- *ip-address*：クライアントに割り当てられた IP アドレス
- *pool-name*：アドレスの割り当て元のプール

推奨アクション 不要。

737027

エラーメッセージ `%FTD-3-737027: IPAA:Session= session, No data for address request`

説明ソフトウェア障害が検出されました。

- *session*：16 進数の VPN セッション ID

推奨アクション Cisco TAC に問い合わせて、問題を報告してください。

737028

エラーメッセージ `%FTD-4-737028: IPAA:Session= session, Unable to send ip-address to standby: communication failure`

説明アクティブ Secure Firewall Threat Defense デバイス が、スタンバイ Secure Firewall Threat Defense デバイス と通信できませんでした。フェールオーバー ペアが同期していない可能性があります。

- *session*：16 進数の VPN セッション ID
- *ip-address*：クライアントに割り当てられた IP アドレス

推奨アクション フェールオーバー設定ステータスを検証します。

737029

エラーメッセージ `%FTD-6-737029: IPAA:Session= session, Added ip-address to standby`

説明スタンバイ Secure Firewall Threat Defense デバイス が IP アドレス割り当てを受け入れました。

- *session*：16 進数の VPN セッション ID
- *ip-address*：クライアントに割り当てられた IP アドレス

推奨アクション 不要。

737030

エラーメッセージ `%FTD-4-737030: IPAA:Session= session, Unable to send ip-address to standby: address in use`

説明アクティブ Secure Firewall Threat Defense デバイス が指摘されたアドレスを取得しようとしましたが、そのアドレスはスタンバイ Secure Firewall Threat Defense デバイス ですでに使用されていました。フェールオーバー ペアが同期していない可能性があります。

- *session*：16 進数の VPN セッション ID
- *ip-address*：クライアントに割り当てられた IP アドレス

推奨アクション フェールオーバー設定ステータスを検証します。

737031

エラーメッセージ `%FTD-6-737031: IPAA:Session= session, Removed ip-address from standby`

説明スタンバイ Secure Firewall Threat Defense デバイス が IP アドレス割り当てを消去しました。

- *session*：16 進数の VPN セッション ID
- *ip-address*：クライアントに割り当てられた IP アドレス

推奨アクション 不要。

737032

エラーメッセージ `%FTD-4-737032: IPAA:Session= session, Unable to remove ip-address from standby: address not found`

説明スタンバイ Secure Firewall Threat Defense デバイス で使用されていない IP アドレスをアクティブ Secure Firewall Threat Defense デバイス が解放しようとしました。フェールオーバー ペアが同期していない可能性があります。

- *session*：16 進数の VPN セッション ID
- *ip-address*：クライアントに割り当てられた IP アドレス

推奨アクション フェールオーバー設定ステータスを検証します。

737033

エラーメッセージ `%FTD-4-737033: IPAA:Session= session, Unable to assign addr_allocator provided IP address ip_addr to client. This IP address has already been assigned by previous_addr_allocator`

説明 AAA/DHCP/ローカル プールによって割り当てられたアドレスがすでに使用されています。

- *session*：16 進数の VPN セッション ID
- *addr_allocator*：DHCP/AAA/ローカル プール
- *ip_addr*：DHCP/AAA/ローカル プールによって割り当てられた IP アドレス
- *previous_ addr_allocator*：すでに IP アドレスを割り当てたアドレス アロケータ（ローカル プール、AAA、または DHCP）

推奨アクション AAA/DHCP/ローカル プールのアドレス設定を検証します。重複が発生している可能性があります。

737034

エラーメッセージ `%Threat Defense-5-737034: IPAA: Session= session, <IP version> address: <explanation>`

説明 IP アドレス割り当てプロセスがアドレスを提供できません。<explanation> テキストにその理由が説明されます。

- *session*：16 進数の VPN セッション ID

推奨アクション処置は説明に基づきます。

737035

エラーメッセージ `%FTD-7-737035: IPAA: Session= session, '<message type>' message queued`

説明メッセージは IP アドレス割り当てにキューイングされます。これは syslog 737001 に対応しています。このメッセージはレート制限されていません。

- *session*：16 進数の VPN セッション ID

推奨アクション処置は必要ありません。

737036

エラーメッセージ `%FTD-6-737035:IPAA: Session= session, Client assigned <address> from DHCP`

説明 IP アドレス割り当てプロセスで、VPN クライアントに DHCP プロビジョニングされたアドレスが返されました。このメッセージはレート制限されていません。

- *session*：16 進数の VPN セッション ID

推奨アクション処置は必要ありません。

737038

エラーメッセージ `%FTD7-737038: IPAA: Session=session, specified address ip-address was in-use, trying to get another.`

説明 このログは、ユーザーに割り当てるアドレスが AAA サーバー（内部または外部）によって指定されている場合に生成されます。ただし、このアドレスはすでに使用されています。要求は再キューイングされており、指定されたアドレスが DHCP またはローカルプールにフォールバックされることはありません。

- *session*：要求しているセッションの VPN セッション ID
- *ip-address*：AAA によって指定されている IPv4 または IPv6 アドレス

推奨アクション必要なし

737200

エラーメッセージ `%FTD-7-737200: VPNFIP: Pool=pool, Allocated ip-address from pool`

説明 このログは、アドレスがローカルプールから割り当てられると生成されます。

- *pool*：ローカルプール名
- *ip-address*：AAA によって指定されている IPv4 または IPv6 アドレス

推奨アクション必要なし

737201

エラーメッセージ `%FTD-7-737201: VPNFIP: Pool=pool, Returned ip-address to pool (recycle=recycle)`

説明 このログは、アドレスがローカルプールに返されると生成されます。リサイクルフラグは、このアドレスを次の要求に再利用する必要があるかどうかを示します。まれに、リサイクルフラグが FALSE になります。たとえば、アドレスの衝突がある（そのアドレスが AAA や DHCP などの他の手段によってすでに VPN セッションに割り当てられている）場合などです。この場合、次の要求でそのアドレスを再利用することは、すぐには試みられません。

- *pool*：ローカルプール名
- *ip-address*：AAA によって指定されている IPv4 または IPv6 アドレス

推奨アクション必要なし

737202

エラーメッセージ `%FTD-3-737202: VPNFIP: Pool=pool, ERROR: message`

説明このログは、VPN FIP データベースに関連するエラーイベントが検出されると生成されます。

- *pool*：ローカルプール名
- *message*：イベントの詳細

推奨アクション エラーが解消されない場合は、Cisco TAC にお問い合わせください。

737203

エラーメッセージ `%FTD-4-737203: VPNFIP: Pool=pool, WARN: message`

説明このログは、VPN FIP データベースに関連するイベントを警告するために生成されます。

- *pool*：ローカルプール名
- *message*：イベントの詳細

推奨アクション 警告が続く場合は、Cisco TAC にお問い合わせください。

737204

エラーメッセージ `%FTD-5-737204: VPNFIP: Pool=pool, NOTIFY: message`

説明 このログは、VPNFIPデータベースに関連するイベントを通知するために生成されます。

- *pool*：ローカルプール名
- *message*：イベントの詳細

推奨アクション必要なし

737205

エラーメッセージ `%FTD-6-737205: VPNFIP: Pool=pool, INFO: message`

説明 このログは、VPNFIPデータベースに関連するイベントを報知するために生成されます。

- *pool*：ローカルプール名
- *message*：イベントの詳細

推奨アクション必要なし

737206

エラーメッセージ `%FTD-7-737206: VPNFIP: Pool=pool, DEBUG: message`

説明 このログは、VPNFIPデータベースに関連するイベントをデバッグするために生成されます。

- *pool*：ローカルプール名
- *message*：イベントの詳細

推奨アクション必要なし

737400

エラーメッセージ `%FTD-7-737400: POOLIP: Pool=pool, Allocated ip-address from pool`

説明 このログは、アドレスがローカルプールから割り当てられると生成されます。

- *pool*：ローカルプール名
- *ip-address*：AAA によって指定されている IPv4 または IPv6 アドレス

推奨アクション必要なし

737401

エラーメッセージ `%FTD-7-737401: POOLIP: Pool=pool, Returned ip-address to pool (recycle=recycle).`

説明 このログは、アドレスがローカルプールに返されると生成されます。リサイクルフラグは、このアドレスを次の要求に再利用する必要があるかどうかを示します。まれに、リサイクルフラグが FALSE になります。たとえば、アドレスの衝突がある（そのアドレスが AAA や DHCP などの他の手段によってすでに VPN セッションに割り当てられている）場合などです。この場合、次の要求でそのアドレスを再利用することは、すぐには試みられません。

- *pool*：ローカルプール名
- *ip-address*：AAA によって指定されている IPv4 または IPv6 アドレス

推奨アクション必要なし

737402

エラーメッセージ `%FTD-4-737402: POOLIP: Pool=pool, Failed to return ip-address to pool (recycle=recycle). Reason: message`

説明 このログは、アドレスをアドレスプールに返すことができない場合に生成されます。

- *pool*：ローカルプール名
- *ip-address*：AAA によって指定されている IPv4 または IPv6 アドレス
- *message*：失敗の詳細（たとえば、アドレスがプールの範囲外である）

推奨アクション必要なし

737403

エラーメッセージ `%FTD-3-737403: POOLIP: Pool=pool, ERROR: message`

説明 このログは、IP ローカルプールデータベースに関連するエラーイベントが検出されると生成されます。

- *pool*：ローカルプール名
- *message*：イベントの詳細

推奨アクション エラーが解消されない場合は、Cisco TAC にお問い合わせください。

737404

エラーメッセージ `%FTD-4-737404: POOLIP: Pool=pool, WARN: message`

説明 このログは、IP ローカルプールデータベースに関連するイベントを警告するために生成されます。

- *pool*：ローカルプール名
- *message*：イベントの詳細

推奨アクション 警告が続く場合は、Cisco TAC にお問い合わせください。

737405

エラーメッセージ `%FTD-5-737405: POOLIP: Pool=pool, NOTIFY: message`

説明 このログは、IP ローカルプールデータベースに関連するイベントを通知するために生成されます。

- *pool*：ローカルプール名
- *message*：イベントの詳細

推奨アクション必要なし

737406

エラーメッセージ `%FTD-6-737406: POOLIP: Pool=pool, INFO: message`

説明 このログは、IP ローカルプールデータベースに関連するイベントを報知するために生成されます。

- *pool*：ローカルプール名
- *message*：イベントの詳細

推奨アクション必要なし

737407

エラーメッセージ `%FTD-7-737407: POOLIP: Pool=pool, DEBUG: message`

説明 このログは、IP ローカルプールデータベースに関連するイベントをデバッグするために生成されます。

- *pool*：ローカルプール名
- *message*：イベントの詳細

推奨アクション必要なし

741000

エラーメッセージ `%FTD-6-741000: Coredump filesystem image created on variable 1 -size variable 2 MB`

説明コア ダンプ ファイル システムが正常に作成されました。ファイル システムは、コア ダンプで使用できるディスク スペースの量を制限することでコア ダンプを管理するためのものです。

- *variable 1*：コア ダンプが配置されるファイル システム（disk0:、disk1:、flash: など）
- *variable 2*：作成されたコア ダンプ ファイル システムのサイズ（MB 単位）

推奨アクション コア ダンプ ファイル システムの作成後に設定を必ず保存してください。

741001

エラーメッセージ `%FTD-6-741001: Coredump filesystem image on variable 1 - resized from variable 2 MB to variable 3 MB`

説明コア ダンプ ファイル システムのサイズが正常に変更されました。

- *variable 1*：コア ダンプが配置されるファイル システム
- *variable 2*：以前のコア ダンプ ファイル システムのサイズ（MB 単位）
- *variable 3*：新たにサイズが変更された現在のコア ダンプ ファイル システムのサイズ（MB 単位）

推奨アクション コア ダンプ ファイル システムのサイズの変更後に設定を必ず保存してください。コア ダンプ ファイル システムのサイズを変更すると、既存のコア ダンプ ファイル システムの内容が削除されます。そのため、コア ダンプ ファイル システムのサイズを変更する前に、すべての情報をアーカイブしてください。

741002

エラーメッセージ `%FTD-6-741002: Coredump log and filesystem contents cleared on variable 1`

説明コア ダンプ ファイル システムからすべてのコア ダンプが削除され、コア ダンプ ログが消去されました。コア ダンプ ファイル システムとコア ダンプ ログは常に相互に同期されます。

- *variable 1*：コア ダンプが配置されているファイル システム（disk0:、disk1:、flash: など）

推奨アクション 不要。**clear coredump** コマンドを使用すると、コ アダンプ ファイル システムを消去して既知の状態にリセットできます。

741003

エラーメッセージ `%FTD-6-741003: Coredump filesystem and its contents removed on variable 1`

説明コア ダンプ ファイル システムとその内容が削除され、コア ダンプ機能がディセーブルになりました。

- *variable 1*：コア ダンプが配置されているファイル システム（disk0:、disk1:、flash: など）

推奨アクション コア ダンプ機能がディセーブルになった後、コンフィギュレーションを必ず保存します。

741004

エラーメッセージ `%Threat Defense-6-741004: Coredump configuration reset to default values`

説明コア ダンプのコンフィギュレーションがデフォルト値にリセットされました。つまり、コア ダンプがディセーブルになりました。

推奨アクション コア ダンプ機能が無効になった後、設定を必ず保存します。

741005

エラーメッセージ `%FTD-4-741005: Coredump operation variable 1 failed with error variable 2 variable 3`

説明コア ダンプ関連の操作の実行中にエラーが発生しました。

- *variable 1*：この変数の有効な値は次のとおりです。

- CREATE_FSYS：コア ダンプ ファイル システムの作成中にエラーが発生しました。

- CLEAR_LOG：コア ダンプ ログの消去中にエラーが発生しました。

- DELETE_FSYS：コア ダンプ ファイル システムの削除中にエラーが発生しました。

- CLEAR_FSYS：コア ダンプ ファイル システムの内容の削除中にエラーが発生しました。

- MOUNT_FSYS：コア ダンプ ファイル システムのマウント中にエラーが発生しました。

- *variable 2*：*variable 1* に指定されたエラーの原因に関する追加情報を提供する 10 進数。
- *variable 3*：*variable 2* に関連付けられている説明のための ASCII 文字列。ASCII 文字列には、次の値が使用されます。

- coredump files already exist

- unable to create coredump filesystem

- unable to create loopback device

- filesystem type not supported

- unable to delete the coredump filesystem

- unable to delete loopback device

- unable to unmount coredump filesystem

- unable to mount coredump filesystem

- unable to mount loopback device

- unable to clear coredump filesystem

- coredump filesystem not found

- requested coredump filesystem too big

- coredump operation aborted by administrator

- coredump command execution failed

- coredump IFS error encountered

- coredump, unidentified error encountered

推奨アクション 設定でコア ダンプ機能がディセーブルになっていることを確認し、詳細に分析するために Cisco TAC にメッセージを送信します。

741006

エラーメッセージ `%FTD-4-741006: Unable to write Coredump Helper configuration, reason variable 1`

説明コアダンプ ヘルパーのコンフィギュレーション ファイルへの書き込み中にエラーが発生しました。このエラーは、disk0:がいっぱいになっている場合にだけ発生します。コンフィギュレーション ファイルは disk0: にあります（.coredumpinfo/coredump.cfg）。

- *variable 1*：この変数には、core dump helper 設定ファイルへの書き込みが失敗した理由を示す基本的なファイル システム関連の文字列が含まれています。

推奨アクション コア ダンプ機能をディセーブルにし、不要なアイテムを disk0: から削除してから、必要に応じてコア ダンプをもう一度イネーブルにします。

742001

エラーメッセージ `%FTD-3-742001: failed to read master key for password encryption from persistent store`

説明起動後に不揮発性メモリからのプライマリパスワード暗号キーを読み取ろうとしましたが失敗しました。コンフィギュレーションの中の暗号化されたパスワードは、**key config-key password encryption** コマンドを使用してプライマリキーを正しい値に設定しない限り、復号されません。

推奨アクションコンフィギュレーションの中に、使用する必要がある暗号化されたパスワードがある場合は、**key config-key password encryption** コマンドを使用して、プライマリキーをパスワードを暗号化するために使用した以前の値に設定します。暗号化されたパスワードがない場合、または暗号化されたパスワードを破棄できる場合は、新しいプライマリキーを設定します。パスワード暗号化を使用していない場合、処置は不要です。

742002

エラーメッセージ `%Threat Defense-3-742002: failed to set master key for password encryption`

説明 key config-key password encryption コマンドの読み込みに失敗しました。このエラーは、次の理由で発生することがあります。

- セキュアでない端末（たとえば、Telnet 接続経由）から設定された。

- フェールオーバーがイネーブルであるが、暗号化されたリンクを使用していない。
- 他のユーザーが同時にキーを設定している。
- キーを変更しようとしたときに、古いキーが正しくない。
- キーがセキュアであるには小さすぎる。

他にもエラーの理由が考えられます。このような場合、実際のエラーがコマンドに対して表示されます。

推奨アクション コマンドの応答に示されている問題を修正します。

742003

エラーメッセージ `%Threat Defense-3-742003: failed to save master key for password encryption, reason reason_text`

説明 不揮発性メモリにプライマリキーを保存しようとしましたが失敗しました。実際の原因は *reason_text* パラメータで指定されます。原因としては、メモリ不足状態や、不揮発性ストレージに不整合があることが考えられます。

推奨アクション 問題が解決しない場合は、キーを保存するために使用した不揮発性ストアを **write erase** コマンドを使用して再フォーマットします。この手順を実行する前に、アウトオブザボックス コンフィギュレーションをバックアップしてください。その後 **write erase** コマンドを再入力します。

742004

エラーメッセージ `%FTD-3-742004: failed to sync master key for password encryption, reason reason_text`

説明 ピアにプライマリキーを同期しようとしましたが失敗しました。実際の原因は *reason_text* パラメータで指定されます。

推奨アクション *reason_text* パラメータに指定された問題の修正を試みます。

742005

エラーメッセージ `%FTD-3-742005: cipher text enc_pass is not compatible with the configured master key or the cipher text has been tampered with`

説明 パスワードを復号化しようとしましたが失敗しました。パスワードは現在のプライマリキーとは異なるプライマリキーを使用して暗号化されているか、暗号化されたパスワードが元の形式から変更された可能性があります。

推奨アクション 正しいプライマリキーが使用されていない場合、問題を解決します。暗号化されたパスワードが変更された場合、新しいパスワードを使用して問題のコンフィギュレーションを再適用します。

742006

エラーメッセージ `%FTD-3-742006: password decryption failed due to unavailable memory`

説明メモリがないために、パスワードの復号化に失敗しました。このパスワードを使用した機能は要求どおりに動作しません。

推奨アクション メモリの問題を修正します。

742007

エラーメッセージ `%Threat Defense-3-742007: password encryption failed due to unavailable memory`

説明メモリがないために、パスワードの暗号化に失敗しました。コンフィギュレーションの中のパスワードは、クリア テキスト形式のままになる可能性があります。

推奨アクションメモリの問題を修正し、パスワードの暗号化に失敗したコンフィギュレーションを再適用します。

742008

エラーメッセージ `%FTD-3-742008: password enc_pass decryption failed due to decoding error`

説明デコードエラーが原因でパスワードの復号化に失敗しました。これは、暗号化されたパスワードが暗号化後に変更されたことが原因である可能性があります。

推奨アクション クリア テキスト パスワードを使用して問題の設定を再適用します。

742009

エラーメッセージ `%FTD-3-742009: password encryption failed due to decoding error`

説明パスワードの暗号化はデコード エラーが原因で失敗しました。内部ソフトウェア エラーが発生している可能性があります。

推奨アクション クリア テキスト パスワードを使用して問題の設定を再適用します。問題が解決しない場合、Cisco TAC にお問い合わせください。

742010

エラーメッセージ `%FTD-3-742010: encrypted password enc_pass is not well formed`

説明コマンドで指定された暗号化パスワードの形式が正しくありません。パスワードは、有効な暗号化パスワードではないか、暗号化後に変更された可能性があります。

- *reason_text*：障害の実際の原因を表す文字列
- *enc_pass*：問題に関連する暗号化されたパスワード

推奨アクション クリア テキスト パスワードを使用して問題の設定を再適用します。

743000

エラーメッセージ `%FTD-1-743000: The PCI device with vendor ID: vendor_id device ID: device_id located at bus:device.function bus_num:dev_num, func_num has a link link_attr_name of actual_link_attr_val when it should have a link link_attr_name of expected_link_attr_val .`

説明システムのPCIデバイスが適切に設定されていません。システムが最適レベルで動作しなくなる可能性があります。

推奨アクション show controller pci detail コマンドの出力を収集し、Cisco TAC にお問い合わせください。

743001

エラーメッセージ `%FTD-1-743001: Backplane health monitoring detected link failure`

説明 Secure Firewall Threat Defense サービス モジュールとスイッチ シャーシ間のリンクの 1 つでハードウェア障害が発生し検出された可能性があります。

推奨アクション Cisco TAC にお問い合わせください。

743002

エラーメッセージ `%FTD-1-743002: Backplane health monitoring detected link OK`

説明 Secure Firewall Threat Defense サービス モジュールとスイッチ シャーシ間のリンクが復元されました。ただし、障害およびその後の復旧は、ハードウェア障害を示している可能性があります。

推奨アクション Cisco TAC にお問い合わせください。

743004

エラーメッセージ `%Threat Defense-1-743004: System is not fully operational - PCI device with vendor ID vendor_id (vendor_name ), device ID device_id (device_name ) not found`

説明システムが完全に機能するために必要な PCI デバイスがシステムに見つかりませんでした。

- *vendor_id*：デバイス ベンダーを識別する 16 進値
- *vendor_name*：ベンダー名を識別するテキスト文字列
- *device_id*：ベンダー デバイスを識別する 16 進値
- *device_name*：デバイス名を識別するテキスト文字列

推奨アクション show controller pci detail コマンドの出力を収集し、Cisco TAC にお問い合わせください。

743010

エラーメッセージ `%Threat Defense-3-743010: EOBC RPC server failed to start for client module client name .`

説明サーバー上の EOBC RPC サービスの特定のクライアントに対しサービスを開始できませんでした。

推奨アクション Cisco TAC に電話でお問い合わせください。

743011

エラーメッセージ `%Threat Defense-3-743011: EOBC RPC call failed, return code code string.`

説明 EOBC RPC クライアントが目的のサーバーへの RPC を作成できませんでした。

推奨アクション Cisco TAC に電話でお問い合わせください。

746014

エラーメッセージ `%Threat Defense-5-746014: user-identity: [FQDN] fqdn address IP Address obsolete.`

説明 完全修飾ドメイン名が古くなっています。

推奨アクション 不要。

746015

エラーメッセージ `%Threat Defense-5-746015: user-identity: FQDN] fqdn resolved IP address .`

説明 完全修飾ドメイン名のルックアップが成功しました。

推奨アクション 不要。

746016

エラーメッセージ `%Threat Defense-3-746016: user-identity: DNS lookup failed, reason: reason`

説明DNS のルックアップが失敗しました。失敗の理由は、次のいずれかです。タイムアウト、解決不能、メモリ不足。

推奨アクション FQDN が有効であり、DNS サーバーが ASA から到達可能であることを確認します。問題が解決しない場合、Cisco TAC にお問い合わせください。

747001

エラーメッセージ %Threat Defense-3-747001: Clustering: Recovered from state machine event queue depleted. Event (*event-id* , *ptr-in-hex* , *ptr-in-hex*) dropped. Current state *state-name* , stack *ptr-in-hex* , *ptr-in-hex* , *ptr-in-hex* , *ptr-in-hex* , *ptr-in-hex* , *ptr-in-hex*

説明クラスタ FSM イベント キューがいっぱいです。新しいイベントがドロップされました。

推奨アクション なし。

747002

エラーメッセージ %Threat Defense-5-747002: Clustering: Recovered from state machine dropped event (*event-id* , *ptr-in-hex* , *ptr-in-hex*). Intended state: *state-name* . Current state: *state-name* .

説明クラスタ FSM が現在の状態と一致しないイベントを受信しました。

推奨アクション なし。

747003

エラーメッセージ %Threat Defense-5-747003: Clustering: Recovered from state machine failure to process event (*event-id* , *ptr-in-hex* , *ptr-in-hex*) at state *state-name* .

説明クラスタ FSM が指定されたすべての理由に対するイベントの処理に失敗しました。

推奨アクション なし。

747004

エラーメッセージ %Threat Defense-6-747004: Clustering: state machine changed from state *state-name* to *state-name* .

説明クラスタ FSM は新しい状態に進みました。

推奨アクション なし。

747005

エラーメッセージ %Threat Defense-7-747005: Clustering: State machine notify event *event-name* (*event-id* , *ptr-in-hex* , *ptr-in-hex*)

説明クラスタ FSM がクライアントにイベントを通知しました。

推奨アクション なし。

747006

エラーメッセージ %Threat Defense-7-747006: Clustering: State machine is at state *state-name*

説明クラスタFSMが安定状態（ディセーブル、スレーブ、またはマスター）に移行しました。

推奨アクション なし。

747007

エラーメッセージ `%Threat Defense-5-747007: Clustering: Recovered from finding stray config sync thread, stack ptr-in-hex , ptr-in-hex , ptr-in-hex , ptr-in-hex , ptr-in-hex , ptr-in-hex .`

説明誤った場所に入った設定同期スレッドが検出されました。

推奨アクション なし。

747008

エラーメッセージ `%Threat Defense-4-747008: Clustering: New cluster member name with serial number serial-number-A rejected due to name conflict with existing unit with serial number serial-number-B .`

説明同じユニット名が複数のユニットに設定されています。

推奨アクション なし。

747009

エラーメッセージ `%Threat Defense-2-747009: Clustering: Fatal error due to failure to create RPC server for module module name .`

説明 Secure Firewall Threat Defense デバイス が RPC サーバーの作成に失敗しました。

推奨アクションこの装置でのクラスタリングをディセーブルにし、もう一度イネーブルにしてみます。問題が続く場合には、Cisco TAC に連絡してください。

747010

エラーメッセージ `%Threat Defense-3-747010: Clustering: RPC call failed, message message-name , return code code-value .`

説明 RPC コール失敗が発生しました。システムは障害からの回復を試みます。

推奨アクション なし。

747011

エラーメッセージ `%Threat Defense-2-747011: Clustering: Memory allocation error.`

説明クラスタリングでメモリ割り当ての失敗が発生しました。

推奨アクションこの装置でのクラスタリングをディセーブルにし、もう一度イネーブルにしてみます。問題が解決しない場合は、Secure Firewall Threat Defense デバイス のメモリ使用量を確認してください。

747012

エラーメッセージ `%Threat Defense-3-747012: Clustering: Failed to replicate global object id hex-id-value in domain domain-name to peer unit-name , continuing operation.`

説明グローバル オブジェクト ID の複製に失敗しました。

推奨アクション なし。

747013

エラーメッセージ `%Threat Defense-3-747013: Clustering: Failed to remove global object id hex-id-value in domain domain-name from peer unit-name , continuing operation.`

説明グローバル オブジェクト ID の削除に失敗しました。

推奨アクション なし。

747014

エラーメッセージ `%Threat Defense-3-747014: Clustering: Failed to install global object id hex-id-value in domain domain-name , continuing operation.`

説明グローバル オブジェクト ID のインストールに失敗しました。

推奨アクション なし。

747015

エラーメッセージ `%Threat Defense-4-747015: Clustering: Forcing stray member unit-name to leave the cluster.`

説明不適切なクラスタ メンバーが見つかりました。

推奨アクション なし。

747016

エラーメッセージ `%Threat Defense-4-747016: Clustering: Found a split cluster with both unit-name-A and unit-name-B as master units. Master role retained by unit-name-A , unit-name-B will leave, then join as a slave.`

説明スプリット クラスタが見つかりました。

推奨アクション なし。

747017

エラーメッセージ `%Threat Defense-4-747017: Clustering: Failed to enroll unit unit-name due to maximum member limit limit-value reached.`

説明最大メンバー数の制限に到達したため、Secure Firewall Threat Defense デバイス は新しいユニットの登録に失敗しました。

推奨アクション なし。

747018

エラーメッセージ `%Threat Defense-3-747018: Clustering: State progression failed due to timeout in module module-name .`

説明クラスタ FSM の進行がタイム アウトしました。

推奨アクション なし。

747019

エラーメッセージ `%Threat Defense-4-747019: Clustering: New cluster member name rejected due to Cluster Control Link IP subnet mismatch (ip-address /ip-mask on new unit, ip-address /ip-mask on local unit).`

説明 制御ユニットは、新規参加ユニットに互換性のないクラスタインターフェイスの IP アドレスがあることを検出しました。

推奨アクションなし。

747020

エラーメッセージ `%Threat Defense-4-747020: Clustering: New cluster member unit-name rejected due to encryption license mismatch.`

説明 制御ユニットは、新規参加ユニットに互換性のない暗号化ライセンスがあることを検出しました。

推奨アクションなし。

747021

エラーメッセージ `%Threat Defense-3-747021: Clustering: Master unit unit-name is quitting due to interface health check failure on interface-name .`

説明インターフェイスのヘルスチェックに失敗したため、制御ユニットはクラスタリングを無効にしました。

推奨アクションなし。

747022

エラーメッセージ %Threat Defense-3-747022: Clustering: Asking slave unit *unit-name* to quit because it failed interface health check *x* times, rejoin will be attempted after *y* min. Failed interface: *interface-name* .

説明このsyslogメッセージは、再参加の最大試行回数を超えていない場合に出力されます。指定された時間にわたってインターフェイスのヘルスチェックに失敗したため、データユニットはクラスタリングを無効にしました。このユニットは、指定された時間（ミリ秒）後に自動的に再度イネーブルになります。

推奨アクション なし。

747025

エラーメッセージ %Threat Defense-4-747025: Clustering: New cluster member *unit-name* rejected due to firewall mode mismatch.

説明制御ユニットは、互換性のないファイアウォールモードを持つ参加ユニットを検出しました。

推奨アクションなし。

747026

エラーメッセージ %Threat Defense-4-747026: Clustering: New cluster member *unit-name* rejected due to cluster interface name mismatch (*ifc-name* on new unit, *ifc-name* on local unit).

説明 制御ユニットは、互換性のないクラスタ制御リンクのインターフェイス名を持つ参加ユニットを検出しました。

推奨アクションなし。

747027

エラーメッセージ %Threat Defense-4-747027: Clustering: Failed to enroll unit *unit-name* due to insufficient size of cluster pool *pool-name* in *context-name* .

説明最小クラスタプールのサイズ制限が設定されているため、制御ユニットは参加ユニットを登録できませんでした。

推奨アクションなし。

747028

エラーメッセージ %Threat Defense-4-747028: Clustering: New cluster member *unit-name* rejected due to interface mode mismatch (*mode-name* on new unit, *mode-name* on local unit).

説明 制御ユニットは、互換性のないインターフェイスモード（spanned または individual）を持つ参加ユニットを検出しました。

推奨アクション なし。

747029

エラーメッセージ `%Threat Defense-4-747029: Clustering: Unit unit-name is quitting due to Cluster Control Link down.`

説明 クラスタインターフェイスの障害のため、ユニットはクラスタリングをディセーブルにしました。

推奨アクション なし。

747030

エラーメッセージ `%Threat Defense-3-747030: Clustering: Asking slave unit unit-name to quit because it failed interface health check x times (last failure on interface-name ), Clustering must be manually enabled on the unit to re-join.`

説明 インターフェイスのヘルスチェックが失敗し、再参加の最大試行回数を超えました。インターフェイスのヘルスチェックに失敗したため、データユニットはクラスタリングを無効にしました。

推奨アクション なし。

747031

エラーメッセージ `%Threat Defense-3-747031: Clustering: Platform mismatch between cluster master (platform-type ) and joining unit unit-name (platform-type ). unit-name aborting cluster join.`

説明 参加ユニットのプラットフォームタイプが、クラスタ制御ユニットのプラットフォームタイプと一致しません。

- *unit-name*：クラスタ ブートストラップ内のユニット名
- *platform-type*：Secure Firewall Threat Defense プラットフォームのタイプ

推奨アクション 参加ユニットのプラットフォームタイプは、必ずクラスタ制御ユニットのプラットフォームタイプと同じにしてください。

747032

エラーメッセージ `%Threat Defense-3-747032: Clustering: Service module mismatch between cluster master (module-name ) and joining unit unit-name (module-name )in slot slot-number . unit-name aborting cluster join.`

説明 参加ユニットの外部モジュール（モジュールタイプおよびそれらのインストール順）がクラスタ制御ユニットの外部モジュールと整合していません。

- *module-name*：外部モジュールの名前
- *unit-name*：クラスタ ブートストラップ内のユニット名
- *slot-number*：不一致が発生したスロットの番号

推奨アクション参加ユニットにインストールされているモジュールが、クラスタ制御ユニット内にあるものと同じタイプで、同じ順序であることを確認します。

747033

エラーメッセージ `%Threat Defense-3-747033: Clustering: Interface mismatch between cluster master and joining unit unit-name . unit-name aborting cluster join.`

説明参加ユニットのインターフェイスがクラスタ制御ユニットのインターフェイスと同じではありません。

- *unit-name*：クラスタ ブートストラップ内のユニット名

推奨アクション 参加ユニットで使用可能なインターフェイスがクラスタ制御ユニットのインターフェイスと同じであることを確認します。

747034

エラーメッセージ `%Threat Defense-4-747034: Unit %s is quitting due to Cluster Control Link down (%d times after last rejoin). Rejoin will be attempted after %d minutes.`

説明 Cluster Control Link がダウンしており、装置が再参加でキックアウトされました。

推奨アクション 装置が再参加するまで待機します。

747035

エラーメッセージ `%Threat Defense-4-747035: Unit %s is quitting due to Cluster Control Link down. Clustering must be manually enabled on the unit to rejoin.`

説明 Cluster Control Link がダウンしており、装置は再参加なしでキックアウトされました。

推奨アクション 装置を手動で再参加させます。

747036

エラーメッセージ `%Threat Defense-3-747036: Application software mismatch between cluster master %s[Master unit name] (%s[Master application software name]) and joining unit (%s[Joining unit application software name]). %s[Joining member name] aborting cluster join.`

説明制御ユニットのアプリケーションと参加データユニットが同一ではありません。データユニットは削除されます。

推奨アクション データユニットが同じアプリケーション/サービスを実行していることを確認し、手動でユニットを再参加させます。

747042

エラーメッセージ `%Threat Defense-3-747042: Clustering: Master received the config hash string request message from an unknown member with id cluster-member-id`

説明 制御ユニットが設定ハッシュ文字列要求イベントを受信しました。

推奨アクション 要求元メンバーがまだ OnCall 状態にあることを確認します。

747043

エラーメッセージ `%Threat Defense-3-747043: Clustering: Get config hash string from master error: ret_code ret_code, string_len string_len`

説明 制御ユニットからの設定ハッシュ文字の取得に失敗しました。

- ret_code：エラーの戻りコード（0 は OK を示し、1 は失敗を示す）
- string_len：hash_str の長さ

推奨アクションテクニカルサポートに連絡して、制御ユニットの問題のトラブルシューティングを実行します。根本原因を特定するために「 debug cluster ccp 」がオンになっていることを確認してください。

747044

エラーメッセージ `%Threat Defense-6-747044: Configuration Hash string verification result`

説明 設定ハッシュ文字列の比較の結果です。

- result：この結果は PASSED または FAILED になります。

推奨アクション 不要。

748001

エラーメッセージ `%Threat Defense-5-748001: Module slot_number in chassis chassis_number is leaving the cluster due to a chassis configuration change`

説明クラスタ制御リンクが MIO で変更された、クラスタ グループが MIO で削除された、またはブレード モジュールが MIO 構成で削除されました。

- *slot_number*：シャーシ内のブレード スロット ID
- *chassis_number*：各シャーシで一意なシャーシ ID

推奨アクション 不要。

748002

エラーメッセージ `%Threat Defense-4-748002: Clustering configuration on the chassis is missing or incomplete; clustering is disabled`

説明 MIO の構成が欠落しているか不完全です（たとえば、クラスタ グループが構成されていない、クラスタ制御リンクが構成されていないなど）。

- *slot_number*：シャーシ内のブレード スロット ID
- *chassis_number*：各シャーシで一意なシャーシ ID

推奨アクション MIO コンソールに移動してクラスタのサービス タイプを設定し、サービス タイプにモジュールを追加し、それに応じて Cluster Control Link を定義します。

748003

エラーメッセージ `%Threat Defense-4-748003: Module slot_number in chassis chassis_number is leaving the cluster due to a chassis health check failure`

説明ブレードは MIO と通信できないため、MIO に依存してこの通信の問題を検出し、データ ポートのバンドルを解除します。データ ポートのバンドルが解除されると、インターフェイスのヘルス チェックによって Secure Firewall Threat Defense デバイス がキックアウトされます。

- *slot_number*：シャーシ内のブレード スロット ID
- *chassis_number*：各シャーシで一意なシャーシ ID

推奨アクション MIO カードがアップしているか、または MIO とブレード間の通信がまだアップしているのかを確認します。

748004

エラーメッセージ `%Threat Defense-5-748004: Module slot_number in chassis chassis_number is re-joining the cluster due to a chassis health check recovery`

説明 MIO ブレードのヘルス チェックが回復し、Secure Firewall Threat Defense デバイス はクラスタの再参加を試行します。

- *slot_number*：シャーシ内のブレード スロット ID
- *chassis_number*：各シャーシで一意なシャーシ ID

推奨アクション MIO カードがアップしているか、または MIO とブレード間の通信がまだアップしているのかを確認します。

748005

エラーメッセージ `%Threat Defense-3-748005: Failed to bundle the ports for module slot_number in chassis chassis_number ; clustering is disabled`

説明 MIO は自身のためのポートのバンドルに失敗しました。

- *slot_number*：シャーシ内のブレード スロット ID

- *chassis_number*：各シャーシで一意なシャーシ ID

推奨アクション MIO が正しく動作しているかどうかを確認します。

748006

エラーメッセージ `%Threat Defense-3-748006: Asking module slot_number in chassis chassis_number to leave the cluster due to a port bundling failure`

説明 MIO がブレード用にポートをバンドルできなかったため、ブレードがキックアウトされました。

- *slot_number*：シャーシ内のブレード スロット ID
- *chassis_number*：各シャーシで一意なシャーシ ID

推奨アクション MIO が正しく動作しているかどうかを確認します。

748007

エラーメッセージ `%Threat Defense-2-748007: Failed to de-bundle the ports for module slot_number in chassis chassis_number ; traffic may be black holed`

説明 MIO はポートのバンドル解除に失敗しました。

- *slot_number*：シャーシ内のブレード スロット ID
- *chassis_number*：各シャーシで一意なシャーシ ID

推奨アクション MIO が正しく動作しているかどうかを確認します。

748008

エラーメッセージ `%Threat Defense-6-748008: [CPU load percentage | memory load percentage ] of module slot_number in chassis chassis_number (member-name ) exceeds overflow protection threshold [CPU percentage | memory percentage ]. System may be oversubscribed on member failure.`

説明 CPU の負荷が (N-1)/N を超えています（N はアクティブなクラスタ メンバーの合計数）。または、メモリの負荷が (100 – x) * (N – 1) / N + x を超えています（N はクラスタ メンバーの数、x は最後の参加メンバーの基準メモリ使用量）。

- *percentage*：CPU 負荷またはメモリ負荷のパーセンタイル データ
- *slot_number*：シャーシ内のブレード スロット ID
- *chassis_number*：各シャーシで一意なシャーシ ID

推奨アクション ネットワークとクラスタリングの導入を再計画します。トラフィックの量を減らすか、またはブレード/シャーシを追加します。

748009

エラーメッセージ `%Threat Defense-6-748009: [CPU load percentage | memory load percentage ] of chassis chassis_number exceeds overflow protection threshold [CPU percentage | memory percentage ]. System may be oversubscribed on chassis failure.`

説明 シャーシのトラフィック負荷が特定のしきい値を超えました。

- *percentage*：CPU 負荷またはメモリ負荷のパーセンタイル データ
- *chassis_number*：各シャーシで一意なシャーシ ID

推奨アクションネットワークとクラスタリングの導入を再計画します。トラフィックの量を減らすか、またはブレード/シャーシを追加します。

748011

エラーメッセージ `%Threat Defense-4-748011: Mismatched resource profile size with Master. Master: cores number CPU cores / RAM size MB RAM, Mine: cores number CPU cores / RAM size MB RAM`

説明クラスタに参加しているユニットを制御ユニットと比較したときにリソースプロファイルサイズが異なっている場合、この syslog が参加ユニットに表示されます。

例

```
%Threat Defense-4-748011: Mismatched resource profile size with Master. Master: 6 CPU cores / 14426 MB RAM,  Mine: 8 CPU cores 19261 MB RAM.
```

推奨アクション 不要。

748012

エラーメッセージ `%Threat Defense-4-748012: Mismatched module type with Master. Master: PID, MINE: PID`

説明クラスタに参加しているユニットを制御ユニットと比較したときにモジュールタイプが異なっている場合、この syslog が参加ユニットに表示されます。

例

```
%Threat Defense-4-748012: Mismatched module type with Master. Master: FPR4K-SM-24, Mine:  FPR4K-SM-24s
```

推奨アクション 不要。

748100

エラーメッセージ `%Threat Defense-3-748100: <application_name> application status is changed from <status> to <status>.`

説明ある状態から別の状態へのアプリケーション状態の変化を検出します。アプリケーションステータスの変化によって、アプリケーションのヘルス チェック メカニズムがトリガーされます。

- application name：snort または disk_full
- status：init、up、down

推奨アクション アプリケーションのステータスを確認します。

748101

エラーメッセージ `%Threat Defense-3-748101: Peer unit <unit_id> reported its <application_name> application status is <status>.`

説明 ピアのユニットがアプリケーション状態の変化を報告したので、アプリケーションのヘルス チェック メカニズムが起動します。

- unit id：ユニット ID
- application name：snort または disk_full
- status：init、up、down

推奨アクション アプリケーションのステータスを確認します。

748102

エラーメッセージ `%Threat Defense-3-748102: Master unit <unit_id> is quitting due to <application_name> Application health check failure, and master's application state is <status>.`

説明 アプリケーションのヘルスチェックは、制御ユニットが正常でないことを検出します。制御ユニットはクラスタグループを離れます。

- unit id：ユニット ID
- application name：snort または disk_full
- status：init、up、down

推奨アクション アプリケーションのステータスを確認します。アプリケーション（snort）が再度起動すると、ユニットが自動的に再参加します。

748103

エラーメッセージ `%Threat Defense-3-748103: Asking slave unit <unit_id> to quit due to <application_name> Application health check failure, and slave's application state is <status>.`

説明 アプリケーションのヘルスチェックは、データユニットが正常でないことを検出します。制御ユニットはデータノードを削除します。

- unit id：ユニット ID

- application name：snort または disk_full
- status：init、up、down

推奨アクションアプリケーションのステータスを確認します。アプリケーション（snort）が再度起動すると、ユニットが自動的に再参加します。

748201

エラーメッセージ `%Threat Defense-4-748201: <Application name> application on module <module id> in chassis <chassis id> is <status>.`

説明サービス チェーン内のアプリケーションのステータスが変更されます。

- status：up、down

推奨アクション サービス チェーン内のアプリケーションのステータスを確認します。

748202

エラーメッセージ `%Threat Defense-3-748202: Module <module_id> in chassis <chassis id> is leaving the cluster due to <application name> application failure\n.`

説明 vDP などのアプリケーションに障害が発生した場合、ユニットはクラスタからキックアウトされます。

推奨アクション サービス チェーン内のアプリケーションのステータスを確認します。

748203

エラーメッセージ `%Threat Defense-5-748203: Module <module_id> in chassis <chassis id> is re-joining the cluster due to a service chain application recovery\n.`

説明 vDP などのサービス チェーン アプリケーションが回復すると、ユニットは自動的にクラスタに再参加します。

推奨アクション サービス チェーン内のアプリケーションのステータスを確認します。

750001

エラーメッセージ `%Threat Defense-5-750001: Local:`*`local IP`*` :`*`local port`* `Remote:`*`remote IP`*` : `*`remote port`* `Username: `*`username`* `Received request to `*`request`* `an IPsec tunnel; local traffic selector = `*`local selectors: range, protocol, port range`* ` ; remote traffic selector = `*`remote selectors: range, protocol, port range`*

説明キー再生成、接続確立の要求などの、IPSec トンネルに対する操作が要求されています。

- *local IP:local port*：この要求のローカル IP アドレス。この接続に使用される Secure Firewall Threat Defense の IP アドレスとポート番号

- *remote IP:remote port*：この要求のリモート IP アドレス。接続の送信元のピア IP アドレスとポート番号
- *username*：リモートアクセスの要求者のユーザー名（既知の場合）またはトンネルグループ
- *local selectors*：ローカルに設定されたトラフィック セレクタ、またはこの IPsec トンネルに使用されているプロキシ
- *remote selectors*：リモート ピアが要求したトラフィック セレクタ、またはこの IPsec トンネルのプロキシ

推奨アクション 不要。

750002

エラーメッセージ `%Threat Defense-5-750002: Local:local IP :local port Remote: remote IP : remote port Username: username Received a IKE_INIT_SA request`

説明着信トンネルまたは SA の開始要求（IKE_INIT_SA 要求）を受信しました。

- *local IP:local port*：この要求のローカル IP アドレス。この接続に使用される Secure Firewall Threat Defense の IP アドレスとポート番号
- *remote IP:remote port*：この要求のリモート IP アドレス。接続の送信元のピア IP アドレスとポート番号
- *username*：リモートアクセスの要求者のユーザー名（既知の場合）またはトンネルグループ

推奨アクション 不要。

750003

エラーメッセージ `%Threat Defense-4-750003: Local: local IP:local port Remote: remote IP:remote port Username: username Negotiation aborted due to ERROR: error`

説明指摘されたエラー理由により、SA のネゴシエーションが打ち切られました。

- *local IP:local port*：この要求のローカル IP アドレス。この接続に使用される Secure Firewall Threat Defense の IP アドレスとポート番号
- *remote IP:remote port*：この要求のリモート IP アドレス。接続の送信元のピア IP アドレスとポート番号
- *username*：リモート アクセスの要求者のユーザー名（既知の場合）
- *error*：ネゴシエーション中止のエラーの理由。その場合のエラーは次のとおりです。

- Failed to send data on the network

- Asynchronous request queued

- Failed to enqueue packet

- A supplied parameter is incorrect

- Failed to allocate memory

- Failed the cookie negotiation
- Failed to find a matching policy
- Failed to locate an item in the database
- Failed to initialize the policy database
- Failed to insert a policy into the database
- The peer's proposal is invalid
- Failed to compute the DH value
- Failed to construct a NONCE
- An expected payload is missing from the packet
- Failed to compute the SKEYSEED
- Failed to create child SA keys
- The peer's KE payload contained the wrong DH group
- Received invalid KE notify, yet we've tried all configured DH groups
- Failed to compute a hash value
- Failed to authenticate the IKE SA
- Failed to compute or verify a signature
- Failed to validate the certificate
- The certificate has been revoked and is consequently invalid
- Failed to build or process a certificate request
- We requested a certificate, but the peer supplied none
- While sending the certificate chain, peer did not send its certificate as the first in the chain
- Detected an unsupported ID type
- Failed to construct an encrypted payload
- Failed to decrypt an encrypted payload
- Detected an invalid value in the packet
- The initiator bit is asserted in packet from original responder
- The initiator bit isn't asserted in packet from original initiator
- The message response bit is asserted in a packet from the exchange initiator
- The message response bit isn't asserted in a packet from the exchange responder
- Detected an invalid IKE SPI
- Packet is a retransmission
- Detected an invalid protocol ID
- Detected unsupported critical payload
- Detected an invalid traffic selector type

- Failed to create new SA
- Failed to delete SA
- Failed to add new SA into session DB
- Failed to add session to PSH
- Failed to delete session from osal
- Failed to delete a session from the database
- Failed to add request to SA
- Throttling request queue exceeds reasonable limit, increase the window size on peer
- Received an IKE msg id outside supported window
- Detected unsupported version number
- Received no proposal chosen notify
- Detected an error notify payload
- Detected NAT-d hash doesn't match
- Initialize sadb failed
- Initialize session db failed
- Failed to get PSH
- Negotiation context locked currently in use
- Negotiation context was not freed!
- Invalid data state found
- Failed to open PKI session
- Failed to insert public keys
- No certificate found
- Unsupported cert encoding found or Peer requested HTTP URL but never sent HTTP_LOOKUP_SUPPORTED Notification
- Sending BUNDLE URL is not supported at least for now. However, processing a BUNDLE URL is supported
- Local certificate has expired
- Failed to construct State Machine
- Error encountered while navigating State Machine
- SM Validation failed
- Could not find neg context
- Failed to add work request to SM Q
- Nonce payload is missing
- Traffic selector payload is missing
- Unsupported DH group

- Expected keypair is unavailable
- Packet isn't encrypted
- Packet is missing KE payload
- Packet is missing SA payload
- Invalid SA
- Invalid negotiation context
- Remote or local ID isn't defined
- Invalid connection id
- Unsupported auth method
- Ipsec policy not found
- Failed to initialize the event priority queue
- Failed to enqueue an item to a list
- Failed to remove an item from list
- Data in the event priority queue is NULL or corrupt
- No local IKE policy found
- Can't delete IKE SA due to in-progress task
- Expected Cookie Notify not received
- Failed to generate auth data: My auth info missing
- Failed to generate auth data: Failed to sign data
- Failed to generate auth data: Signature operation successful but unable to locate generated auth material
- Failed to receive the AUTH msg before the timer expired
- Maximum number of retransmissions reached
- Initial exchange failed
- Auth exchange failed
- Create child exchange failed
- Platform errors
- Failed to log a message
- Unwanted debug level turned on
- There are additional TS possible
- A single pairs of addresses is required
- Invalid session
- There was no IPSEC policy found for received TS
- Cannot remove request from window
- There was no proposal found in configured policy

- Nat-t test failure
- No pskey found
- Invalid compression algorithm
- Failed to get profile name from platform service handle
- Failed to find profile
- Initiator failed to match profile sent by IPSEC with profile found by peer id or certificate
- Failed to get peer id from platform service handle
- The transform attribute is invalid
- Extensible Authentication Protocol failed
- Authenticator sent NULL EAP message
- The config attribute is invalid
- Failed to calculate packet hash
- The AAA context is deleted
- Cannot alloc AAA ID
- Cannot alloc AAA request
- Cannot init AAA request
- The Authen list is not configured
- Fail to send AAA request
- Fail to alloc IP addr
- Invalid message context
- Key Auth memory failure
- EAP method does not generate MSK
- Failed to register new SA with platform
- Failed to async process session register, error: %d
- Failed to insert SA due to ipsec rekey collision
- Failed while handling a ipsec rekey collision
- Failed to accept rekey on SA that caused a rekey collision
- Failed to start timer to ensure IPsec collision SA SPI %s/%s will be deleted by the peer
- Error/Debug codes and strings are not matched
- Failed to initialize SA lifetime
- Failed to find rekey SA
- Failed to generate DH shared secret
- Failed to retrieve issuer public key hash list
- Failed to build certificate payload

- Unable to initialize the timer

- Failed to generate DH shared secret

- Failed to initialized authorization request

- Incorrect author record received from AAA

- Failed to fetch the keys from AAA

- Failed to add attribute to AAA request

- Failed to send tunnel password request to AAA

- Failed to allocate AAA context

- Insertion to policy AVL tree failed

- Deletion from policy AVL tree failed

- No Matching node found in policy AVL tree

- No Matching policy found

- No Matching proposal found

- Proposal is incomplete to be attached to the policy

- Proposal is in use

- Peer authentication method configured is mismatching with the method proposed by peer

- Failed to find the session in osal

- Failed to allocate event

- Failed to create accounting record

- Accounting not required

- Accounting not started for this session

- NAT-T disabled via cli

- Negotiating limit reached, deny SA request

- SA is already in negotiation, hence not negotiating again

- AAA グループ認証に失敗した

- AAA ユーザー認証に失敗した

- %% Dropping received fragment, as fragmentation is not negotiated for this SA!

- Maximum number of received fragments reached for the SA

- Number of fragments exceeds maximum allowed

- 構築されたパケット長 %d が最大 ikev2 パケット サイズ %d より大きい

- Received fragment numbers were NOT continuous or IKEV2_FRAG_FLAG_LAST_FRAGMENT flag was set on the wrong packet

- Received fragment is not valid, hence being dropped

- AAA グループ認証に失敗した

- AAA ユーザー認証に失敗した
- AAA author not configured in IKEv2 profile
- Failed to extract the skeyid
- Failed to send a failover msg to the standby unit
- Detected unsupported failover version
- Request was received but failover is not enabled
- Received an active unit request but the negotiated role is %s
- Received a standby unit request but the negotiated role is %s
- Invalid IP Version
- GDOI is not yet supported in IKEv2
- Failed to allocate PSH from platform
- Redirect the session to another gateway
- Redirect check failed
- Accept the session on this gateway after Redirect check
- Detected unsupported Redirect gateway ID type
- Redirect accepted, initiate new request
- Redirect accepted, clean-up IKEv2 SA, platform will initiate new request
- SA got redirected, it should not do any CREATE_CHILD_SA exchange
- DH public key computation failed
- DH secret computation failed
- IN-NEG IKEv2 Rekey SA got deleted
- Number of cert req exceeds the reasonable limit (%d)
- The negotiation context has been freed
- 構築されたパケット長 %d が最大 ikev2 パケット サイズ %d より大きい
- Received fragment numbers were NOT continuous or IKEV2_FRAG_FLAG_LAST_FRAGMENT flag was set on the wrong packet
- AAA 作成者が IKEv2 プロファイルに設定されていない
- Assembled packet is not valid, hence being dropped
- Invalid VCID context

推奨アクション syslog を確認し、ログのフローを追跡してこの syslog が交換の最後のものであるか、および再ネゴシエートされた潜在的な障害または一時的なエラーの原因かを判断します。たとえば、ピアは、設定されていない KE ペイロードによって DH グループを提案できます。これにより最初の要求が失敗しますが、ピアが新しい要求の中で正しいグループに戻ることができるように、正しい DH グループが伝えられます。

750004

エラーメッセージ `%Threat Defense-5-750004: Local: local IP: local port Remote: remote IP: remote port Username: username Sending COOKIE challenge to throttle possible DoS`

説明着信接続要求で、DoS 攻撃を防ぐために設定されたクッキー チャレンジしきい値に基づいてクッキーが要求されました。

- *local IP:local port*：この要求のローカル IP アドレス。この接続に使用される Secure Firewall Threat Defense の IP アドレスとポート番号
- *remote IP:remote port*：この要求のリモート IP アドレス。接続の送信元のピア IP アドレスとポート番号
- *username*：リモート アクセスの要求者のユーザー名（既知の場合）

推奨アクション 不要。

750005

エラーメッセージ `%Threat Defense-5-750005: Local: local IP: local port Remote: remote IP: remote port Username: username IPsec rekey collision detected. I am lowest nonce initiator, deleting SA with inbound SPI SPI`

説明キー再生成コリジョンが検出され（両方のピアで同時にキー再生成を開始しようとしている）、最も小さいナンスを持っていたため、この Secure Firewall Threat Defense デバイス が開始したほうを保持することでコリジョンが解決されました。この操作によって、SPI により参照されている指摘された SA が削除されました。

- *local IP:local port*：この要求のローカル IP アドレス。この接続に使用される Secure Firewall Threat Defense の IP アドレスとポート番号
- *remote IP:remote port*：この要求のリモート IP アドレス。接続の送信元のピア IP アドレスとポート番号
- *username*：リモート アクセスの要求者のユーザー名（既知の場合）
- *SPI*：検出されたキー再生成コリジョンを解決することによって検出される SA の SPI ハンドル

推奨アクション 不要。

750006

エラーメッセージ `%Threat Defense-5-750006: Local: local IP: local port Remote: remote IP: remote port Username: username SA UP. Reason: reason`

説明新たに確立された接続またはキー再生成などの理由で、SA がアップ状態になりました。

- *local IP:local port*：この要求のローカル IP アドレス。この接続に使用される Secure Firewall Threat Defense の IP アドレスとポート番号
- *remote IP:remote port*：この要求のリモート IP アドレス。接続の送信元のピア IP アドレスとポート番号
- *username*：リモート アクセスの要求者のユーザー名（既知の場合）

- *reason*：SA がアップ状態になった理由

推奨アクション 不要。

750007

エラーメッセージ `%Threat Defense-5-750007: Local: local IP: local port Remote: remote IP: remote port Username: username SA DOWN. Reason: reason`

説明ピアからの要求、オペレータ要求（管理者アクションを通して）、キー再生成などの指摘された理由により、SA が切断または削除されました。

- *local IP:local port*：この要求のローカル IP アドレス。この接続に使用される Secure Firewall Threat Defense の IP アドレスとポート番号
- *remote IP:remote port*：この要求のリモート IP アドレス。接続の送信元のピア IP アドレスとポート番号
- *username*：リモート アクセスの要求者のユーザー名（既知の場合）
- *reason*：SA がダウン状態になった理由

推奨アクション 不要。

750008

エラーメッセージ `%Threat Defense-5-750008: Local: local IP: local port Remote: remote IP: remote port Username: username SA rejected due to system resource low`

説明 SA 要求は、システム リソースの低下状態を軽減するために拒否されました。

- *local IP:local port*：この要求のローカル IP アドレス。この接続に使用される Secure Firewall Threat Defense の IP アドレスとポート番号
- *remote IP:remote port*：この要求のリモート IP アドレス。接続の送信元のピア IP アドレスとポート番号
- *username*：リモート アクセスの要求者のユーザー名（既知の場合）

推奨アクション IKEv2 の CAC 設定を確認し、これが設定されたしきい値に基づく予期された動作であるかどうかを判断します。そうではなく、問題が続く場合は、問題を軽減するために、さらに調査します。

750009

エラーメッセージ `%Threat Defense-5-750009: Local: local IP: local port Remote: remote IP: remote port Username: username SA request rejected due to CAC limit reached: Rejection reason: reason`

説明コネクション アドミッション制御（CAC）制限しきい値に達し、SA 要求が拒否されました。

- *local IP:local port*：この要求のローカル IP アドレス。この接続に使用される Secure Firewall Threat Defense の IP アドレスとポート番号

- *remote IP:remote port*：この要求のリモート IP アドレス。接続の送信元のピア IP アドレスとポート番号
- *username*：リモート アクセスの要求者のユーザー名（既知の場合）
- *reason*：SA が拒否された理由

推奨アクション IKEv2 の CAC 設定を確認し、これが設定されたしきい値に基づく予期された動作であるかどうかを判断します。そうではなく、問題が続く場合は、問題を軽減するために、さらに調査します。

750010

エラーメッセージ `%Threat Defense-5-750010: Local: local-ip Remote: remote-ip Username:username IKEv2 local throttle-request queue depth threshold of threshold reached; increase the window size on peer peer for better performance`

- *local-ip*：ローカル ピアの IP アドレス
- *remote-ip*：リモート ピアの IP アドレス
- *username*：リモート アクセスの要求者のユーザー名、または、その時点でも既知の場合は、L2L のトンネル グループ名
- *threshold*：到達したローカル スロットル要求のキューの深さのしきい値
- *peer*：リモート ピアの IP アドレス

説明 指定されたピアに Secure Firewall Threat Defense デバイス がスロットル要求キューをオーバーフローしました。これは、ピアが低速になりことを示しています。スロットル要求キューは、ピアへの要求を保持します。IKEv2 のウィンドウ サイズに基づいて対応できる最大数の要求がすでに対応中だったため、すぐには送信できません。送信中の要求が完了すると、要求はスロットル要求キューから引き出されてピアに送信されます。ピアがこれらの要求を迅速に処理していない場合は、スロットル キューが保持します。

推奨アクション 可能な場合は、リモート ピアの IKEv2 のウィンドウ サイズを引き上げ、より多くの同時要求を送信できるようにします。これでパフォーマンスが向上する場合があります。

（注） Secure Firewall Threat Defense デバイス では現在、IKEv2 のウィンドウ サイズ設定の引き上げをサポートしていません。

750011

エラーメッセージ `%Threat Defense-3-750011: Tunnel Rejected: Selected IKEv2 encryption algorithm (IKEV2 encry algo ) is not strong enough to secure proposed IPSEC encryption algorithm (IPSEC encry algo ).`

説明選択された IKEv2 暗号化アルゴリズムが、提示された IPSec 暗号化アルゴリズムの安全を保護するのに十分な強度ではないため、トンネルが拒否されました。

推奨アクション IPSec 子 SA 暗号化アルゴリズムの強度に匹敵するかそれを上回る、より強力な IKEv2 暗号化アルゴリズムを設定します。

750012

エラーメッセージ `%Threat Defense-4-750012: Selected IKEv2 encryption algorithm (IKEV2 encry algo ) is not strong enough to secure proposed IPSEC encryption algorithm (IPSEC encry algo ).`

説明選択された IKEv2 暗号化アルゴリズムは、提示された IPSec 暗号化アルゴリズムの安全を保護するのに十分な強度ではありません。

推奨アクション IPSec 子 SA 暗号化アルゴリズムの強度に匹敵するかそれを上回る、より強力な IKEv2 暗号化アルゴリズムを設定します。

750013

エラーメッセージ `%Threat Defense-5-750013 - IKEv2 SA (iSPI <ISPI> rRSP <rSPI>) Peer Moved: Previous <prev_remote_ip>:<prev_remote_port>/<prev_local_ip>:<prev_local_port>. Updated <new_remote_ip>:<new_remote_port>/<new_local_ip>:<new_local_port>`

説明 新しいモバイル機能を使用すると、トンネルを切断しなくてもピア IP を変更できます。たとえば、モバイル デバイス（スマートフォン）は別のネットワークに接続した後に新しい IP を取得します。次のリストでメッセージ値について説明します。

- *ip*：以前の IP アドレスと、新しいローカルおよびリモートのIP アドレスを指定します
- *port*：以前のポート情報と、新しいローカルおよびリモートのポート情報
- *SPI*：イニシエータおよびレスポンダ SPI を示します
- *iSPI*：イニシエータ SPI を指定します
- *rSPI*：レスポンダ SPI を指定します

推奨アクション 開発エンジニアにお問い合わせください。

751001

エラーメッセージ `%Threat Defense-3-751001: Local: localIP:port Remote:remoteIP:port Username: username/group Failed to complete Diffie-Hellman operation. Error: error`

説明 error で示されているように、Diffie-Hellman オペレーションを完了できませんでした。

- *localIP:port*：ローカル IP アドレスとポート番号
- *remoteIP:port*：リモート IP アドレスとポート番号
- *username/group*：この接続試行に関連するユーザー名またはグループ
- *error*：特定のエラーを示すエラー文字列

推奨アクション ロー メモリの問題か、または解決する必要があるその他の内部エラーが発生しました。このステートが続く場合、問題の識別のためにメモリ追跡ツールを使用します。

751002

エラーメッセージ `%Threat Defense-3-751002: Local: localIP:port Remote:remoteIP:port Username: username/group No preshared key or trustpoint configured for self in tunnel group group`

説明 Secure Firewall Threat Defense デバイス は、ピアに対する自身の認証に使用可能な、何らかの種類の認証情報をトンネル グループ中に見つけることができませんでした。

- *localIP:port*：ローカル IP アドレスとポート番号
- *remoteIP:port*：リモート IP アドレスとポート番号
- *username/group*：この接続試行に関連するユーザー名またはグループ
- *group*：トンネル グループの名前

推奨アクション トンネル グループの設定を確認し、示されているトンネル グループでの自己認証用の事前共有キーまたは証明書を設定します。

751003

エラーメッセージ `%Threat Defense-7-751003: Local: localIP:port Remote:remoteIP:port Username: username/group Need to send a DPD message to peer`

説明指定したピアが起動しているかどうかを確認するため、デッドピア検出を実行する必要があります。Secure Firewall Threat Defense デバイス は、ピアへの接続を終了した可能性があります。

- *localIP:port*：ローカル IP アドレスとポート番号
- *remoteIP:port*：リモート IP アドレスとポート番号
- *username/group*：この接続試行に関連するユーザー名またはグループ

推奨アクション 不要。

751004

エラーメッセージ `%Threat Defense-3-751004: Local: localIP:port Remote:remoteIP:port Username: username/group No remote authentication method configured for peer in tunnel group group`

説明接続を許可するためにリモート ピアを認証するための方法が、コンフィギュレーション中に見つかりませんでした。

- *localIP:port*：ローカル IP アドレスとポート番号
- *remoteIP:port*：リモート IP アドレスとポート番号
- *username/group*：この接続試行に関連するユーザー名またはグループ
- *group*：トンネル グループの名前

推奨アクション 設定を調べ、有効なリモート ピア認証設定があることを確認します。

751005

エラーメッセージ `%Threat Defense-3-751005: Local: localIP:port Remote:remoteIP:port Username: username/group AnyConnect client reconnect authentication failed. Session ID: sessionID , Error: error`

説明 セッション トークンを使用した AnyConnect クライアントの再接続の試行中に障害が発生しました。

- *localIP:port*：ローカル IP アドレスとポート番号
- *remoteIP:port*：リモート IP アドレスとポート番号
- *username/group*：この接続試行に関連するユーザー名またはグループ
- *sessionID*：再接続の試行に使用されたセッション ID
- *error*：再接続試行中に発生した特定のエラーを示すエラー文字列

推奨アクション 必要に応じて、指摘されたエラーに従って処置を実行します。このエラーは、クライアントの切断が検出されるか、Secure Firewall Threat Defense デバイス 上でセッションがクリアされたことにより、再開状態を維持する代わりにセッションが削除されたことを示している場合があります。必要に応じて、このメッセージを、Anyconnect クライアント上のイベント ログと比較します。

751006

エラーメッセージ `%Threat Defense-3-751006: Local: localIP:port Remote:remoteIP:port Username: username/group Certificate authentication failed. Error: error`

説明 証明書認証に関連した障害が発生しました。

- *localIP:port*：ローカル IP アドレスとポート番号
- *remoteIP:port*：リモート IP アドレスとポート番号
- *username/group*：この接続試行に関連するユーザー名またはグループ
- *error*：特定の証明書認証障害を示すエラー文字列

推奨アクション 必要に応じて、指摘されたエラーに従って処置を実行します。証明書トラストポイントの設定を確認し、クライアント証明書チェーンが適切に確認できるように、必要な CA 証明書が存在することを確認します。障害を切り分けるには **debug crypto ca** コマンドを使用します。

751007

エラーメッセージ `%Threat Defense-5-751007: Local: localIP:port Remote:remoteIP:port Username: username/group Configured attribute not supported for IKEv2. Attribute: attribute`

説明設定された属性は、IKE バージョン 2 接続でサポートされないため、IKE バージョン 2 接続に適用できませんでした。

- *localIP:port*：ローカル IP アドレスとポート番号
- *remoteIP:port*：リモート IP アドレスとポート番号

- *username/group*：この接続試行に関連するユーザー名またはグループ
- *attribute*：適用するように設定した属性

推奨アクション 不要。このメッセージが生成されないようにするには、IKE バージョン 2 構成設定を削除します。

751008

エラーメッセージ `%Threat Defense-3-751008: Local: localIP:port Remote:remoteIP:port Username: username/group  Group=group , Tunnel rejected: IKEv2 not enabled in group policy`

説明 接続試行がマッピングされた、指摘されたグループで有効なプロトコルに基づき、IKE バージョン 2 は許可されず、接続が拒否されました。

- *localIP:port*：ローカル IP アドレスとポート番号
- *remoteIP:port*：リモート IP アドレスとポート番号
- *username/group*：この接続試行に関連するユーザー名またはグループ
- *group*：接続に使用したトンネル グループ

推奨アクション グループ ポリシーの VPN トンネル プロトコルの設定を確認し、必要に応じて IKE バージョン 2 をイネーブルにします。

751009

エラーメッセージ `%Threat Defense-3-751009: Local: localIP:port Remote:remoteIP:port Username: username/group Unable to find tunnel group for peer.`

説明 ピアのトンネル グループを検出できませんでした。

- *localIP:port*：ローカル IP アドレスとポート番号
- *remoteIP:port*：リモート IP アドレスとポート番号
- *username/group*：この接続試行に関連するユーザー名またはグループ

推奨アクション 設定およびトンネル グループ マッピングのルールを確認してから、設定したグループにピアが到達できるようにそれらを設定します。

751010

エラーメッセージ `%Threat Defense-3-751010: Local: localIP:port Remote:remoteIP:port Username: username/group  Unable to determine self-authentication method. No crypto map setting or tunnel group found.`

説明 Secure Firewall Threat Defense デバイス がピアを認証する方式がトンネル グループでも、暗号マップでも見つかりませんでした。

- *localIP:port*：ローカル IP アドレスとポート番号
- *remoteIP:port*：リモート IP アドレスとポート番号
- *username/group*：この接続試行に関連するユーザー名またはグループ

推奨アクション設定を確認し、イニシエータL2L用の暗号マップ内か、または該当するトンネル グループ内に自己認証方式を設定します。

751011

エラーメッセージ `%Threat Defense-3-751011: Local: localIP:port Remote:remoteIP:port Username: username/group Failed user authentication. Error: error`

説明 ユーザー認証中に、IKE バージョン 2 のリモート アクセス接続用の EAP 内で障害が発生しました。

- *localIP:port*：ローカル IP アドレスとポート番号
- *remoteIP:port*：リモート IP アドレスとポート番号
- *username/group*：この接続試行に関連するユーザー名またはグループ
- *error*：特定のエラーを示すエラー文字列

推奨アクション正しい認証クレデンシャルが提供されていることを確認し、必要に応じて、さらにデバッグを実行して障害の正確な原因を突き止めます。

751012

エラーメッセージ `%Threat Defense-3-751012: Local: localIP:port Remote:remoteIP:port Username: username/group Failure occurred during Configuration Mode processing. Error: error`

説明コンフィギュレーションモードの処理中に、設定を接続に適用しているときにエラーが発生しました。

- *localIP:port*：ローカル IP アドレスとポート番号
- *remoteIP:port*：リモート IP アドレスとポート番号
- *username/group*：この接続試行に関連するユーザー名またはグループ
- *error*：特定のエラーを示すエラー文字列

推奨アクション 示されているエラーに基づいてアクションを実行します。**debug crypto ikev2** コマンドを使用して失敗の原因を特定するか、エラーによって指摘されたサブシステムを必要に応じてデバッグします。

751013

エラーメッセージ `%Threat Defense-3-751013: Local: localIP:port Remote:remoteIP:port Username: username/group Failed to process Configuration Payload request for attribute attribute ID . Error: error`

説明ピアによって要求された Configuration Payload 要求の処理に失敗し、属性に対する Configuration Payload 応答を生成できませんでした。

- *localIP:port*：ローカル IP アドレスとポート番号
- *remoteIP:port*：リモート IP アドレスとポート番号
- *username/group*：この接続試行に関連するユーザー名またはグループ

- *attribute ID*：障害が発生した属性 ID
- *error*：特定のエラーを示すエラー文字列

推奨アクション メモリ エラー、設定エラー、または別のタイプのエラーが発生しました。障害の原因を切り分けるには、**debug crypto ikev2** コマンドを使用します。

751014

エラーメッセージ `%Threat Defense-4-751014: Local: localIP:port Remote remoteIP:port Username: username/group Warning Configuration Payload request for attribute attribute ID could not be processed. Error: error`

説明 要求された属性に CP 応答を生成する CP 要求の処理の最中に警告が発生しました。

- *localIP:port*：ローカル IP アドレスとポート番号
- *remoteIP:port*：リモート IP アドレスとポート番号
- *username/group*：この接続試行に関連するユーザー名またはグループ
- *attribute ID*：障害が発生した属性 ID
- *error*：特定のエラーを示すエラー文字列

推奨アクション 警告に示されている属性と、示されている警告メッセージに基づいて、アクションを実行します。たとえば、新しいクライアントが、クライアントに追加された新しい属性を認識しない古い Secure Firewall Threat Defense イメージで使用されています。属性を処理できるように、Secure Firewall Threat Defense イメージのアップグレードが必要な場合があります。

751015

エラーメッセージ `%Threat Defense-4-751015: Local: localIP:port Remote remoteIP:port Username: username/group SA request rejected by CAC. Reason: reason`

説明 リストされている理由で示されている設定済みのしきい値または条件に基づいて Secure Firewall Threat Defense デバイス を保護するため、コール アドミッション制御によって接続が拒否されました。

- *localIP:port*：ローカル IP アドレスとポート番号
- *remoteIP:port*：リモート IP アドレスとポート番号
- *username/group*：この接続試行に関連するユーザー名またはグループ
- *reason*：SA 要求が拒否された理由

推奨アクション 理由を確認し、新しい接続が許可される必要があった場合は条件を解決するか、または設定されているしきい値を変更します。

751016

エラーメッセージ `%Threat Defense-4-751016: Local: localIP:port Remote remoteIP:port Username: username/group  L2L peer initiated a tunnel with the same outer and inner addresses. Peer could be Originate only - Possible misconfiguration!`

説明 ピアは、トンネルの受信した外部 IP アドレスと内部 IP アドレスに基づいて発信専用接続用に設定されている可能性があります。

- *localIP:port*：ローカル IP アドレスとポート番号
- *remoteIP:port*：リモート IP アドレスとポート番号
- *username/group*：この接続試行に関連するユーザー名またはグループ

推奨アクション L2L ピアの設定を確認します。

751017

エラーメッセージ `%Threat Defense-3-751017: Local: localIP:port Remote remoteIP:port Username: username/group  Configuration Error error description`

説明接続を妨げるコンフィギュレーション エラーが検出されました。

- *localIP:port*：ローカル IP アドレスとポート番号
- *remoteIP:port*：リモート IP アドレスとポート番号
- *username/group*：この接続試行に関連するユーザー名またはグループ
- *error description*：接続エラーの簡単な説明

推奨アクション 示されているエラーに基づいて設定を修正します。

751018

エラーメッセージ `%Threat Defense-3-751018: Terminating the VPN connection attempt from attempted group . Reason: This connection is group locked to locked group .`

説明接続が試行されるトンネル グループは、グループ ロックに設定されているトンネル グループと同じではありません。

- *attempted group*：接続が着信するトンネル グループ
- *locked group*：接続がロックまたは限定されるトンネル グループ

推奨アクション グループ ポリシーまたはユーザー属性でグループ ロック値を確認します。

751019

エラーメッセージ `%Threat Defense-4-751019: Local:LocalAddr Remote:RemoteAddr Username:username Failed to obtain an licenseType license. Maximum license limit limit exceeded.`

説明最大ライセンス制限を超えたため、セッション作成に失敗しました。そのため、トンネル要求の開始または応答に失敗しました。

- *LocalAddr*：この接続試行のローカル アドレス
- *RemoteAddr*：この接続試行のリモート ピア アドレス
- *username*：接続を試行しているピアのユーザー名
- *licenseType*：超過したライセンス タイプ（他の VPN または AnyConnect Premium/Essentials）

• *limit*：許可され、超過したライセンスの数

推奨アクション 許可されているすべてのユーザーに利用するために十分な数のライセンスがあることを確認するか、または拒否された接続を許可するためにより多くのライセンスを取得します。あるいは、その両方を実行します。マルチ コンテキスト モードの場合、障害を報告したコンテキストに対し、必要に応じてより多くのライセンスを割り当てます。

751020

エラーメッセージ `%Threat Defense-3-751020: Local:%A:%u Remote:%A:%u Username:%s An %s remote access connection failed. Attempting to use an NSA Suite B crypto algorithm (%s) without an AnyConnect Premium license.`

説明 AnyConnect Premium ライセンスは適用されましたが、webvpn コンフィギュレーション モードで **anyconnect-essentials** を使用して明示的にディセーブルにされているため、IKEv2 リモート アクセス トンネルを作成できませんでした。

推奨アクション Secure Firewall Threat Defense デバイス に AnyConnect Premium ライセンスがインストールされ、リモート アクセス IKEv2 ポリシーまたは IPsec プロポーザルに設定されていることを確認します。

751021

エラーメッセージ `%Threat Defense-4-751021: Local:variable 1 :variable 2 Remote:variable 3 :variable 4 Username:variable 5 variable 6 with variable 7 encryption is not supported with this version of the AnyConnect Client. Please upgrade to the latest Anyconnect Client.`

説明 古い AnyConnect クライアントが、AES-GCM 暗号化ポリシーを使用して IKEv2 が設定されている Secure Firewall Threat Defense デバイス に接続しようとしました。

- *variable 1*：ローカル IP アドレス
- *variable 2*：ローカル ポート
- *variable 3*：リモート クライアント IP アドレス
- *variable 4*：リモート クライアント ポート
- *variable 5*：AnyConnect クライアントのユーザー名（ユーザーがユーザー名を入力する前にこのエラーが発生したため、不明である可能性もあります）
- *variable 6*：接続プロトコル タイプ（IKEv1、IKEv2）
- *variable 7*：連結モード暗号化タイプ（AES-GCM、AES-GCM 256）

推奨アクション AES-GCM 暗号化で IKEv2 を使用するため、AnyConnect クライアントを最新バージョンにアップグレードします。

751022

エラーメッセージ `%Threat Defense-3-751022: Local: local-ip Remote: remote-ip Username:username Tunnel rejected: Crypto Map Policy not found for remote traffic selector rem-ts-start /rem-ts-end /rem-ts.startport /rem-ts.endport /rem-ts.protocol local traffic`

`selector local-ts-start /local-ts-end /local-ts.startport /local-ts.endport /local-ts.protocol !`

説明 Secure Firewall Threat Defense デバイス が、メッセージに示されているプライベート ネットワークまたはホストのセキュリティ ポリシー情報を検出できませんでした。これらのネットワークまたはホストは、発信側によって送信され、Secure Firewall Threat Defense デバイス のどの暗号 ACL とも一致しません。多くの場合、これはコンフィギュレーションの誤りです。

- *local-ip*：ローカル ピアの IP アドレス
- *remote-ip*：リモート ピアの IP アドレス
- *username*：リモート アクセスの要求者のユーザー名（既知の場合）
- *rem-ts-start*：リモート トラフィック セレクタの開始アドレス
- *rem-ts-end*：リモート トラフィック セレクタの終了アドレス
- *rem-ts.startport*：リモート トラフィック セレクタの開始ポート
- *rem-ts.endport*：リモート トラフィック セレクタの終了ポート
- *rem-ts.protocol*：リモート トラフィック セレクタのプロトコル
- *local-ts-start*：ローカル トラフィック セレクタの開始アドレス
- *local-ts-end*：ローカル トラフィック セレクタの終了アドレス
- *local-ts.startport*：ローカル トラフィック セレクタの開始ポート
- *local-ts.endport*：ローカル トラフィック セレクタの終了ポート
- local-*ts.protocol*：ローカル トラフィック セレクタのプロトコル

推奨アクション 両側の暗号化 ACL の保護されているネットワーク設定を確認し、イニシエータのローカル ネットワークがレスポンダのリモート ネットワークであること、およびイニシエータのリモート ネットワークがレスポンダのローカル ネットワークであることを確認します。ワイルドカード マスクと、ネットワーク アドレスと比較したホスト アドレスに特に注意します。シスコ以外の実装では、プロキシ アドレスまたは「red」ネットワークというラベルが付いたプライベート アドレスがある場合があります。

751023

エラーメッセージ `%Threat Defense-6-751023: Local a :p Remote: a :p Username:n Unknown client connection`

説明未知またはシスコ以外の IKEv2 クライアントが Secure Firewall Threat Defense デバイス に接続しました。

- *n*：グループまたはユーザー名（コンテキストによる）
- *a*：IP アドレス
- *p*：ポート番号
- *ua*：クライアントが Secure Firewall Threat Defense デバイス に提示したユーザーエージェント

推奨アクション シスコがサポートしている IKEv2 クライアントにアップグレードします。

751024

エラーメッセージ `%Threat Defense-3-751024: Local:ip-addr Remote:ip-addr Username:username IKEv2 IPv6 User Filter tempipv6 configured. This setting has been deprecated, terminating connection`

説明 IPv6 VPN フィルタは廃止されており、IPv6 トラフィックのアクセス制御に統合フィルタの代わりに設定されている場合は、接続が終了します。

推奨アクション IPv6 エントリで統合フィルタを設定し、ユーザー用の IPv6 トラフィックを制御します。

751025

エラーメッセージ `%Threat Defense-5-751025: Local: local IP :local port Remote: remote IP :remote port Username:username Group:group-policy IPv4 Address=assigned_IPv4_addr IPv6 address=assigned_IPv6_addr assigned to session.`

説明このメッセージには、指定されたユーザーの AnyConnect IKEv2 接続に割り当てられた IP アドレス情報が表示されます。

- *local IP* :*local port*：この要求のローカル IP アドレスこの接続に使用される Secure Firewall Threat Defense の IP アドレスとポート番号
- *remote IP* :*remote port*：この要求のリモート IP アドレス接続の送信元のピア IP アドレスとポート番号
- *username*：リモート アクセスの要求者のユーザー名（既知の場合）
- *group-policy*：ユーザーに対してアクセスを許可したグループ ポリシー
- *assigned_IPv4_addr*：クライアントに割り当てられている IPv4 アドレス
- *assigned_IPv6_addr*：クライアントに割り当てられている IPv6 アドレス

推奨アクション 不要。

751026

エラーメッセージ `%Threat Defense-6-751026: Local: localIP:port Remote: remoteIP:port Username: username/group IKEv2 Client OS: client-os Client: client-name client-version`

説明指摘されたユーザーが、表示されているオペレーティング システムとクライアントのバージョンに接続しようとしています。

- *localIP:port*：ローカル IP アドレスとポート番号
- *remoteIP:port*：リモート IP アドレスとポート番号
- *username/group*：この接続試行に関連するユーザー名またはグループ
- *client-os*：クライアントが報告したオペレーティング システム
- *client-name*：クライアントが報告したクライアント名（通常は AnyConnect）
- *client-version*：クライアントが報告したクライアント バージョン

推奨アクション 不要。

751027

エラーメッセージ `%Threat Defense-4-751027: Local:local IP :local port Remote:peer IP :peer port Username:username IKEv2 Received INVALID_SELECTORS Notification from peer. Peer received a packet (SPI=spi). The decapsulated inner packet didn't match the negotiated policy in the SA. Packet destination pkt_daddr , port pkt_dest_port , source pkt_saddr , port pkt_src_port , protocol pkt_prot .`

説明 ピアが IPsec セキュリティ アソシエーション（SA）上で受信したパケットが、その SA のネゴシエートされたトラフィック記述子に一致しませんでした。ピアは、不正パケットの SPI とパケット データを含む INVALID_SELECTORS 通知を送信しました。

- *local IP*：Secure Firewall Threat Defense ローカル IP アドレス
- *local port*：Secure Firewall Threat Defense ローカル ポート
- *peer IP*：ピアとなる IP アドレス
- *peer port*：ピア ポート
- *username*：ユーザー名
- *spi*：パケットの IPsec SA の SPI
- *pkt_daddr*：パケット宛先 IP アドレス
- *pkt_dest_port*：パケット宛先ポート
- *pkt_saddr*：パケット送信元 IP アドレス
- *pkt_src_port*：パケット送信元ポート
- *pkt_prot*：パケット プロトコル

推奨アクション エラー メッセージ、設定、およびこのエラーにつながったイベントの詳細をコピーし、それらを Cisco TAC に送信してください。

752001

エラーメッセージ `%Threat Defense-2-752001: Tunnel Manager received invalid parameter to remove record`

説明 トンネルマネージャからレコードを削除できませんでした。これにより、同じピアに今後トンネルを開始できない可能性があります。

推奨アクション デバイスをリロードするとレコードは削除されますが、エラーが解決しないか、または再発する場合は、特定のトンネル試行のデバッグをさらに実行します。

752002

エラーメッセージ `%Threat Defense-7-752002: Tunnel Manager Removed entry. Map Tag = mapTag . Map Sequence Number = mapSeq .`

説明 トンネルを開始するエントリが正常に削除されました。

- *mapTag*：開始エントリが削除されたクリプト マップ名
- *mapSeq*：開始エントリが削除されたクリプト マップのシーケンス番号

推奨アクション 不要。

752003

エラーメッセージ `%Threat Defense-5-752003: Tunnel Manager dispatching a KEY_ACQUIRE message to IKEv2. Map Tag = mapTag . Map Sequence Number = mapSeq`

説明 示されている暗号マップに基づいたIKEv2トンネルを開始するための試行を実行中です。

- *mapTag*：開始エントリが削除されたクリプトマップ名
- *mapSeq*：開始エントリが削除されたクリプトマップのシーケンス番号

推奨アクション 不要。

752004

エラーメッセージ `%Threat Defense-5-752004: Tunnel Manager dispatching a KEY_ACQUIRE message to IKEv1. Map Tag = mapTag . Map Sequence Number = mapSeq`

説明 示されている暗号マップに基づいたIKEv1トンネルを開始するための試行を実行中です。

- *mapTag*：開始エントリが削除されたクリプトマップ名
- *mapSeq*：開始エントリが削除されたクリプトマップのシーケンス番号

推奨アクション 不要。

752005

エラーメッセージ `%Threat Defense-2-752005: Tunnel Manager failed to dispatch a KEY_ACQUIRE message. Memory may be low. Map Tag = mapTag . Map Sequence Number = mapSeq.`

説明 トンネル開始試行をディスパッチしようとしましたが、メモリ割り当ての障害などの内部エラーによって失敗しました。

- *mapTag*：開始エントリが削除されたクリプトマップ名
- *mapSeq*：開始エントリが削除されたクリプトマップのシーケンス番号

推奨アクション メモリ トラッキング ツールを使用し、さらにデバッグを実行することで問題を切り分けます。

752006

エラーメッセージ `%Threat Defense-3-752006: Tunnel Manager failed to dispatch a KEY_ACQUIRE message. Probable mis-configuration of the crypto map or tunnel-group. Map Tag = Tag . Map Sequence Number = num, SRC Addr: address port: port Dst Addr: address port: port .`

説明 トンネルの開始の試行をディスパッチしようとして、指摘されたクリプトマップまたは関連付けられているトンネル グループのコンフィギュレーション エラーが原因で、失敗しました。

- *Tag*：開始エントリが削除された暗号マップの名前
- *num*：開始エントリが削除された暗号マップのシーケンス番号

- *address*：送信元 IP アドレスまたは宛先 IP アドレス
- *port*：送信元ポート番号または宛先ポート番号

推奨アクション 示されているトンネル グループと暗号マップの設定を調べ、完全であることを確認します。

752007

エラーメッセージ `%Threat Defense-3-752007: Tunnel Manager failed to dispatch a KEY_ACQUIRE message. Entry already in Tunnel Manager. Map Tag = mapTag . Map Sequence Number = mapSeq`

説明 既存のエントリをトンネル マネージャに再追加しようとしました。

- *mapTag*：開始エントリが削除されたクリプト マップ名
- *mapSeq*：開始エントリが削除されたクリプト マップのシーケンス番号

推奨アクション 問題が解決しない場合は、ピアの設定でトンネルが許可されることを確認し、さらにデバッグを実行して、トンネル開始時にトンネルマネージャのエントリが追加されてから正しく削除されること、および開始試行の成否を確認します。引き続きトンネルの作成中である可能性があるため、IKE バージョン 2 または IKE バージョン 1 の接続をさらにデバッグします。

752008

エラーメッセージ `%Threat Defense-7-752008: Duplicate entry already in Tunnel Manager`

説明 トンネルを開始するための重複した要求が行われ、トンネルマネージャは、すでにトンネルを開始しようとしています。

推奨アクション 不要。問題が解消されない場合、IKE バージョン 1 または IKE バージョン 2 がトンネルの開始を試行し、まだタイムアウトしていない可能性があります。該当するコマンドを使用してさらにデバッグし、開始の試行が成功または失敗した後に、トンネルマネージャ エントリが削除されることを確認します。

752009

`%Threat Defense-4-752009: IKEv2 Doesn't support Multiple Peers`

説明 複数のピアを使用してクリプトマップが設定されているため、IKE バージョン 2 のトンネルを開始する試みが失敗しました。この設定は、IKE バージョン 2 でサポートされていません。IKE バージョン 1 のみが複数のピアをサポートします。

推奨アクション 設定を確認し、複数のピアでの IKE バージョン 2 のサイト間での開始が予期されていないことを確認します。

752010

エラーメッセージ `%Threat Defense-4-752010: IKEv2 Doesn't have a proposal specified`

説明 IKE バージョン 2 トンネルを開始するための IPSec プロポーザルが見つかりませんでした。

推奨アクション 設定を確認し、必要に応じて、トンネルの開始に使用できる IKE バージョン 2 プロポーザルを設定します。

752011

エラーメッセージ `%Threat Defense-4-752011: IKEv1 Doesn't have a transform set specified`

説明 IKE バージョン 2 トンネルを開始するための、IKE バージョン 1 トランスフォーム セットが見つかりませんでした。

推奨アクション 設定を確認し、必要に応じて、トンネルの開始に使用できる IKE バージョン 2 トランスフォーム セットを設定します。

752012

エラーメッセージ `%Threat Defense-4-752012: IKEv protocol was unsuccessful at setting up a tunnel. Map Tag = mapTag . Map Sequence Number = mapSeq .`

説明指摘されたプロトコルが、設定されたクリプトマップを使用してトンネルを開始できませんでした。

- *protocol*：IKEv1 または IKEv2 を示す IKE バージョン番号 1 または 2
- *mapTag*：開始エントリが削除されたクリプト マップ名
- *mapSeq*：開始エントリが削除されたクリプト マップのシーケンス番号

推奨アクション設定を確認し、示されているプロトコル内をさらにデバッグしてトンネル試行が失敗した原因を特定します。

752013

エラーメッセージ `%Threat Defense-4-752013: Tunnel Manager dispatching a KEY_ACQUIRE message to IKEv2 after a failed attempt. Map Tag = mapTag . Map Sequence Number = mapSeq .`

説明トンネル マネージャは、失敗した後に、トンネルを再開しようとしています。

- *mapTag*：開始エントリが削除されたクリプト マップ名
- *mapSeq*：開始エントリが削除されたクリプト マップのシーケンス番号

推奨アクション設定を調べ、暗号マップが正しく設定されていることを確認します。その後、トンネルが、2 回目の試行で正常に作成されたことを確認します。

752014

エラーメッセージ `%Threat Defense-4-752014: Tunnel Manager dispatching a KEY_ACQUIRE message to IKEv1 after a failed attempt. Map Tag = mapTag . Map Sequence Number = mapSeq .`

説明トンネル失敗後、トンネル マネージャはフォール バックし、IKE バージョン 1 を使用してトンネルを開始しようとしています。

- *mapTag*：開始エントリが削除されたクリプト マップ名
- *mapSeq*：開始エントリが削除されたクリプト マップのシーケンス番号

推奨アクション 設定を確認し、クリプト マップが正しく設定されていることを確認します。その後、トンネルが、2 回目の試行で正常に作成されたことを確認します。

752015

エラーメッセージ `%Threat Defense-3-752015: Tunnel Manager has failed to establish an L2L SA. All configured IKE versions failed to establish the tunnel. Map Tag = mapTag . Map Sequence Number = mapSeq .`

説明ピアへの L2L トンネルを確立する試行が、設定されたすべてのプロトコルを使用して試行した後に失敗しました。

- *mapTag*：開始エントリが削除されたクリプト マップ名
- *mapSeq*：開始エントリが削除されたクリプト マップのシーケンス番号

推奨アクション 設定を確認し、クリプト マップが正しく設定されていることを確認します。障害の原因を特定するには、個々のプロトコルをデバッグします。

752016

エラーメッセージ `%Threat Defense-5-752016: IKEv protocol was successful at setting up a tunnel. Map Tag = mapTag . Map Sequence Number = mapSeq.`

説明 示されているプロトコル（IKE バージョン 1 または IKE バージョン 2）で L2L トンネルが正常に作成されました。

- *protocol*：IKEv1 または IKEv2 を示す IKE バージョン番号 1 または 2
- *mapTag*：開始エントリが削除されたクリプト マップ名
- *mapSeq*：開始エントリが削除されたクリプト マップのシーケンス番号

推奨アクション 不要。

752017

エラーメッセージ `%Threat Defense-4-752017: IKEv2 Backup L2L tunnel initiation denied on interface interface matching crypto map name , sequence number number . Unsupported configuration.`

説明 IKEv2 はバックアップ L2L をサポートしていないため、Secure Firewall Threat Defense デバイス は IKEv1 を使用して接続を開始します。

推奨アクション IKEv1 がイネーブルの場合、処置は不要です。バックアップ L2L 機能を使用するには、IKEv1 をイネーブルにする必要があります。

753001

エラーメッセージ `%Threat Defense-4-753001: Unexpected IKEv2 packet received from <IP>:<port>. Error: <reason>`

説明 クラスタが分散型 VPN クラスタリング モードで動作しており、データパスで実行した初期の整合性チェックまたはエラーチェック、あるいはその両方が失敗したときに IKEv2 パケットを受信してこの syslog が生成されます。

- <IP>：パケットを送信した送信元 IP アドレス
- <port>：パケットを送信した送信元ポート
- <reason>：パケットが無効とみなされている理由この値は *Corrupted SPI detected* または *Expired SPI received* である可能性があります。

推奨アクション IKEv1 がイネーブルの場合、処置は不要です。バックアップ L2L 機能を使用するには、IKEv1 をイネーブルにする必要があります。

767001

エラーメッセージ `%Threat Defense-6-767001: Inspect-name : Dropping an unsupported IPv6/IP46/IP64 packet from interface :IP Addr to interface :IP Addr (fail-close)`

説明 fail-close オプションがサービス ポリシーに設定され、特定の検査によって IPv6、IP64、または IP46 のパケットが受信されています。fail-close オプション設定に基づいて、この syslog メッセージが生成され、パケットはドロップされます。

推奨アクション 不要。

768001

エラーメッセージ `%Threat Defense-3-768001: QUOTA: resource utilization is high: requested req , current curr , warning level level`

説明 システム リソースの割り当てレベルが警告しきい値に達しました。管理セッションの場合、リソースは同時管理セッションです。

- *resource*：システム リソース名。この場合は管理セッションです。
- *req*：要求された数。管理セッションでは常に 1 です。
- *curr*：現在の割り当て数。管理セッションでは *level* と等しくなります。
- *level*：警告レベル。設定されている制限の 90 %。

推奨アクション 不要。

768002

エラーメッセージ `%Threat Defense-3-768002: QUOTA: resource quota exceeded: requested req , current curr , limit limit`

説明システム リソースに対する要求は、設定された制限を超過したため拒否されました。管理セッションの場合、システムの同時管理セッションの最大数に到達しました。

- *resource*：システム リソース名。この場合は管理セッションです。
- *req*：要求された数。管理セッションでは常に 1 です。
- *curr*：現在の割り当て数。管理セッションでは *level* と等しくなります。
- *limit*：設定されているリソース制限

推奨アクション 不要。

768003

エラーメッセージ `%Threat Defense-3-768003: QUOTA: management session quota exceeded for user user name: current 3, user limit 3`

説明 現在の管理セッションが、ユーザーに設定されている制限を超えました。

- *current*：ユーザーの管理セッションに割り当てられている現在の番号
- *limit*：設定されている管理セッションの制限（デフォルト値は 15）

推奨アクション必要なし。

768004

エラーメッセージ `%Threat Defense-3-768004: QUOTA: management session quota exceeded for ssh/telnet/http protocol: current 2, protocol limit 2`

説明 プロトコル（SSH、Telnet、または HTTP）の管理セッションの最大数が、設定されている制限を超えました。

- *current*：管理セッションに割り当てられている現在の番号
- *limit*：設定されているプロトコルあたりのリソース制限（デフォルト値は 5）

推奨アクション必要なし。

769001

エラーメッセージ `%Threat Defense-5-769001: UPDATE: ASA image src was added to system boot list`

説明システムイメージが更新されました。以前にシステムにダウンロードされたファイルの名前が、システム ブートのリストに追加されました。

- *src*：送信元イメージファイルの名前または URL

推奨アクション 不要。

769002

エラーメッセージ `%Threat Defense-5-769002: UPDATE: ASA image src was copied to dest`

説明システムイメージが更新されました。イメージファイルがシステムにコピーされました。

- *src*：ソース イメージ ファイルの名前または URL
- *dest*：コピー先のイメージ ファイルの名前

推奨アクション 不要。

769003

エラーメッセージ `%Threat Defense-5-769003: UPDATE: ASA image src was renamed to dest`

説明システム イメージが更新されました。既存のイメージ ファイル名は、システム ブート リスト内のイメージ ファイル名に変更されました。

- *src*：ソース イメージ ファイルの名前または URL
- *dest*：コピー先のイメージ ファイルの名前

推奨アクション 不要。

769004

エラーメッセージ `%Threat Defense-2-769004: UPDATE: ASA image src_file failed verification, reason: failure_reason`

説明イメージは、copy コマンドまたは verify コマンドのいずれかで検証に失敗しました。

- *src_file*：送信元イメージ ファイルのファイル名または URL
- *failure_reason*：宛先イメージ ファイルのファイル名

推奨アクション 障害の考えられる理由として、システム メモリが不足している、ファイルでイメージが見つからなかった、チェックサムに失敗した、ファイルで署名が見つからなかった、署名が無効だった、署名のアルゴリズムがサポートされていない、署名処理の問題があります。

769005

エラーメッセージ `%Threat Defense-5-769005: UPDATE: ASA image image_name passed image verification.`

説明これは、イメージが検証に合格したことを示す通知メッセージです。

- *image_name*：Secure Firewall Threat Defense イメージファイルの名前

推奨アクション 不要。

769006

エラーメッセージ `%Threat Defense-3-769006: UPDATE: ASA boot system image image_name was not found on disk.`

説明これは、ブート システム リストで設定されたファイルをディスク上に置くことができなかったことを示すエラー メッセージです。

- *image_name*：Secure Firewall Threat Defense イメージファイルの名前

推奨アクションデバイスがブートできない場合は、デバイスをリブートする前に有効なファイルをポイントするように boot system コマンドを変更するか、または欠落しているファイルをディスクにインストールします。

769007

エラーメッセージ `%Threat Defense-6-769007: UPDATE: Image version is version_number`

説明 このメッセージは、デバイスがアップグレードされると表示されます。

- *version_number*：Secure Firewall Threat Defense イメージファイルのバージョン番号

推奨アクション必要なし。

769009

エラーメッセージ `%Threat Defense-4-769009: UPDATE: Image booted image_name is different from boot images.`

説明これは、設定されたファイルがブートイメージの既存のリストと異なることを示す、デバイスのアップグレード後に表示されるエラーメッセージです。

- *image_name*：Secure Firewall Threat Defense イメージ ファイルのファイル名

推奨アクション 不要。

770001

エラーメッセージ `%Threat Defense-4-770001: Resource resource allocation is more than the permitted list of limit for this platform. If this condition persists, the ASA will be rebooted.`

説明 Secure Firewall Threat Defense 仮想マシンの CPU またはメモリ リソース割り当てが、このプラットフォームに許可されている制限を超えました。この条件は、Secure Firewall Threat Defense仮想マシンの設定が、Cisco.comからダウンロードしたソフトウェアでの指定から変更されていない場合には発生しません。

推奨アクション Secure Firewall Threat Defense のオペレーションを続行するには、CPU または仮想マシンのメモリ リソース割り当てをCisco.comからダウンロードしたソフトウェアで指定したものに変更するか、変更します。

770002

エラーメッセージ `%Threat Defense-1-770002: Resource resource allocation is more than the permitted limit for this platform. ASA will be rebooted.`

説明 Secure Firewall Threat Defense 仮想マシンの CPU またはメモリ リソース割り当てが、このプラットフォームに許可されている制限を超えました。この条件は、Secure Firewall Threat Defense仮想マシンの設定が、Cisco.comからダウンロードしたソフトウェアでの指定から変更されていない場合には発生しません。リソース割り当てを変更しない限り、Secure Firewall Threat Defense デバイス は再起動し続けます。

推奨アクションCPUまたは仮想マシンのメモリリソース割り当てをCisco.comからダウンロードしたソフトウェアで指定したものに変更するか、変更します。

770003

エラーメッセージ `%Threat Defense-4-770003: Resource resource allocation is less than the minimum requirement of value for this platform. If this condition persists, performance will be lower than normal.`

説明 Secure Firewall Threat Defense 仮想マシンへの CPU またはメモリ リソース割り当てがこのプラットフォームの最小要件を下回っています。この状態が解消されない場合は、パフォーマンスが通常より低くなります。

推奨アクション Secure Firewall Threat Defense の操作を続行するには、仮想マシンの CPU またはメモリリソース割り当てを、シスコからダウンロードしたソフトウェアで指定されたものに変更します。

772002

エラーメッセージ `%Threat Defense-3-772002: PASSWORD: console login warning, user username , cause: password expired`

説明ユーザーが有効期限の切れたパスワードを使用してシステム コンソールにログインしました。これはシステムのロックアウトを避けるために許可されています。

- *username*：ユーザーの名前

推奨アクション ユーザーはログイン パスワードを変更する必要があります。

772003

エラーメッセージ `%Threat Defense-2-772003: PASSWORD: session login failed, user username , IP ip , cause: password expired`

説明ユーザーが有効期限の切れたパスワードを使用してシステムにログインしようとしましたが、アクセスを拒否されました。

- *session*：セッション タイプ。SSH または Telnet
- *username*：ユーザーの名前
- *ip*：ユーザーの IP アドレス

推奨アクションユーザーにアクセス権限がある場合は、管理者がユーザーのパスワードを変更する必要があります。不正なアクセスが試みられると適切な応答がトリガーされます。たとえば、その IP アドレスからのトラフィックをブロックできます。

772004

エラーメッセージ `%Threat Defense-3-772004: PASSWORD: session login failed, user username , IP ip , cause: password expired`

説明ユーザーが有効期限の切れたパスワードを使用してシステムにログインしようとしましたが、アクセスを拒否されました。

- *session*：セッション タイプ。これは ASDM です。
- *username*：ユーザーの名前
- *ip*：ユーザーの IP アドレス

推奨アクションユーザーにアクセス権限がある場合は、管理者がユーザーのパスワードを変更する必要があります。不正なアクセスが試みられると適切な応答がトリガーされます。たとえば、その IP アドレスからのトラフィックをブロックできます。

772005

エラーメッセージ `%Threat Defense-6-772005: REAUTH: user username passed authentication`

説明ユーザーはパスワードの変更後に正常に認証されました。

- *username*：ユーザーの名前

推奨アクション 不要。

772006

エラーメッセージ `%Threat Defense-2-772006: REAUTH: user username failed authentication`

説明ユーザーがパスワードを変更しようとして誤ったパスワードを入力しました。その結果、パスワードは変更されていません。

- *username*：ユーザーの名前

推奨アクションユーザーは**change-password** コマンドを使用してパスワードの変更を再試行する必要があります。

774001

エラーメッセージ `%Threat Defense-2-774001: POST: unspecified error`

説明暗号化サービス プロバイダーが電源投入時自己診断テストに失敗しました。

推奨アクション Cisco TAC にお問い合わせください。

774002

エラーメッセージ `%Threat Defense-2-774002: POST: error err, func func , engine eng , algorithm alg , mode mode , dir dir , key len len`

説明暗号化サービス プロバイダーが電源投入時自己診断テストに失敗しました。

- *err*：失敗の原因
- *func*：関数
- *eng*：エンジン。NPX、Nlite、またはソフトウェア
- *alg*：アルゴリズム。RSA、DSA、DES、3DES、AES、RC4、MD5、SHA1、SHA256、SHA386、SHA512、HMAC-MD5、HMAC-SHA1、HMAC-SHA2、または AES-XCBC のいずれか
- *mode* ：モード。none、CBC、CTR、CFB、ECB、stateful-RC4、stateless-RC4 のいずれか
- *dir*：encryption または decryption のいずれか
- *len*：ビット単位のキーの長さ

推奨アクション Cisco TAC にお問い合わせください。

776251

エラーメッセージ `%Threat Defense-6-776251: CTS SGT-MAP: Binding binding IP - SGname (SGT ) from source name added to binding manager.`

説明指定された送信元からのバインディングがバインディングマネージャに追加されました。

- *binding IP*：IPv4 または IPv6 のバインディングアドレス。
- *SGname* (*SGT*)：バインディング SGT の情報SGname が使用可能な場合は *SGname* (*SGT*) の形式になり、SGname が使用できない場合は *SGT* という形式になります。
- *source name*：関係する送信元の名前。

推奨アクション 不要。

776252

エラーメッセージ `%Threat Defense-5-776252: CTS SGT-MAP: CTS SGT-MAP: Binding binding IP - SGname (SGT ) from source name deleted from binding manager.`

説明 指定された送信元からのバインディングがバインディング マネージャから削除されました。

指定した送信元からのバインドが、バインディング マネージャに追加されました。

- *binding IP*：IPv4 または IPv6 のバインディングアドレス。
- *SGname* (*SGT*)：バインディング SGT の情報SGname が使用可能な場合は *SGname* (*SGT*) の形式になり、SGname が使用できない場合は *SGT* という形式になります。
- *source name*：関係する送信元の名前。

推奨アクション 不要。

776253

エラーメッセージ `%Threat Defense-6-776253: CTS SGT-MAP: Binding binding IP - new SGname (SGT ) from new source name changed from old sgt: old SGname (SGT ) from old source old source name .`

説明 特定の IP から SGT へのバインディングがバインディング マネージャ内で変更されました。

- *binding IP*：IPv4 または IPv6 のバインディングアドレス。
- *new SGname* (*SGT*)：新しいバインディング SGT 情報。SGname が使用可能な場合は *SGname* (*SGT*) の形式になり、SGname が使用できない場合は *SGT* という形式になります。
- *new source name*：新たに関係する送信元の名前
- *old SGname* (*SGT*)：古いバインディング SGT 情報。SGname が使用可能な場合は *SGname* (*SGT*) の形式になり、SGname が使用できない場合は *SGT* という形式になります。
- *old source name*：以前に関係していた送信元の名前

推奨アクション必要なし。

776254

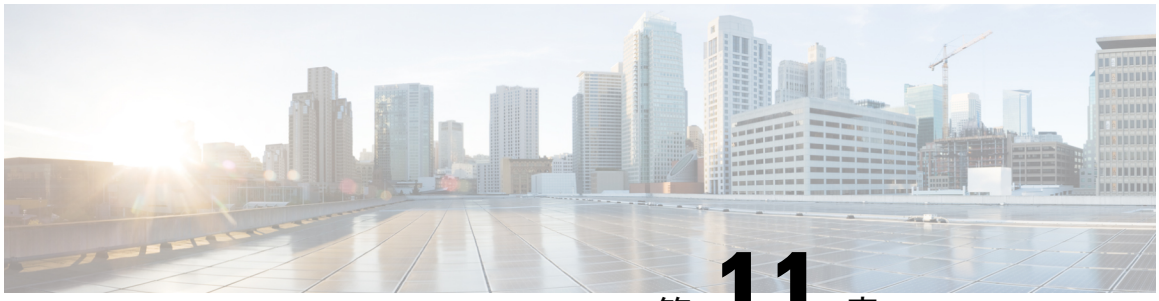
エラーメッセージ `%Threat Defense-3-776254: CTS SGT-MAP: Binding manager unable to action binding binding IP - SGname (SGT ) from source name.`

説明 バインディング マネージャがバインディングを挿入、削除、または更新できません。

- *action*：バインディング マネージャの動作insert、delete、または update です。
- *binding IP*：IPv4 または IPv6 のバインディングアドレス。
- *SGname* (*SGT*)：バインディング SGT の情報SGname が使用可能な場合は *SGname* (*SGT*) の形式になり、SGname が使用できない場合は *SGT* という形式になります。
- *source name*：関係する送信元の名前。

推奨アクション Cisco TAC に連絡して、サポートを受けてください。

776254



第 11 章

Syslog メッセージ 778001 ～ 8300006

この章は、次の項で構成されています。

メッセージ 778001 ～ 785001

この項では、778001 ～ 785001 のメッセージについて説明します。

778001

エラーメッセージ `%Threat Defense-6-778001: VXLAN: Invalid VXLAN segment-id segment-id for protocol from ifc-name :(IP-address/port) to ifc-name :(IP-address/port).`

説明 Secure Firewall Threat Defense デバイス は VXLAN パケットの内部接続を作成しようとしていますが、VXLAN パケットに無効なセグメント ID があります。

推奨アクション 不要。

778002

エラーメッセージ `%Threat Defense-6-778002: VXLAN: There is no VNI interface for segment-id segment-id .`

説明 VXLAN ヘッダーのセグメント ID が Secure Firewall Threat Defense デバイス で設定された VNI インターフェイスのセグメント ID と一致しないため、カプセル除去された入力 VXLAN パケットは廃棄されます。

推奨アクション 不要。

778003

エラーメッセージ `%Threat Defense-6-778003: VXLAN: Invalid VXLAN segment-id segment-id for protocol from ifc-name :(IP-address/port) to ifc-name :(IP-address/port) in FP.`

説明 Secure Firewall Threat Defense Fast Path は、無効なセグメント ID を持つ VXLAN パケットを確認しています。

推奨アクション VNI インターフェイス セグメント ID の設定をチェックし、VNI セグメント ID の設定と一致していない VXLAN セグメントがドロップした パケットにあることを確認します。

778004

エラーメッセージ `%Threat Defense-6-778004: VXLAN: Invalid VXLAN header for protocol from ifc-name :(IP-address/port) to ifc-name :(IP-address/port) in FP.`

説明 Secure Firewall Threat Defense VTEP は、無効な VXLAN ヘッダーを持つ VXLAN パケットを確認しています。

推奨アクション 不要。

778005

エラーメッセージ `%Threat Defense-6-778005: VXLAN: Packet with VXLAN segment-id segment-id from ifc-name is denied by FP L2 check.`

説明 Fast Path L2 チェックによって VXLAN パケットが拒否されます。

推奨アクション VNI インターフェイス セグメント ID の設定をチェックし、VNI セグメント ID の設定と一致していない VXLAN セグメントがドロップした パケットにあることを確認します。ドロップされたパケットのセグメント ID と一致するエントリが STS テーブルにあるかどうかを確認します。

778006

エラーメッセージ `%Threat Defense-6-778006: VXLAN: Invalid VXLAN UDP checksum from ifc-name :(IP-address/port) to ifc-name :(IP-address/port) in FP.`

説明 Secure Firewall Threat Defense VTEP は、無効な UDP チェックサム値を持つ VXLAN パケットを受信しました。

推奨アクション 不要。

778007

エラーメッセージ `%Threat Defense-6-778007: VXLAN: Packet from ifc-name :IP-address/port to IP-address/port was discarded due to invalid NVE peer.`

説明 Secure Firewall Threat Defense VTEP は、設定された NVE ピアとは異なる IP アドレスから VXLAN パケットを受信しました。

推奨アクション 不要。

779001

エラーメッセージ `%Threat Defense-6-779001: STS: Out-tag lookup failed for in-tag segment-id of protocol from ifc-name :IP-address /port to IP-address /port .`

説明 Secure Firewall Threat Defense デバイス は VXLAN パケットの接続を作成しようとしましたが、STS ルックアップ テーブルを使用して VXLAN パケット内のインタグ（セグメント ID）に対するアウトタグを見つけられませんでした。

推奨アクション 不要。

779002

エラーメッセージ `%Threat Defense-6-779002: STS: STS and NAT locate different egress interface for segment-id segment-id , protocol from ifc-name :IP-address /port to IP-address /port`

説明 Secure Firewall Threat Defense デバイス は VXLAN パケットの接続を作成しようとしていますが、STS ルックアップ テーブルと NAT ポリシーが別の出力インターフェイスを検索しています。

推奨アクション 不要。

779003

エラーメッセージ `%Threat Defense-3-779003: STS: Failed to read tag-switching table - reason`

説明 Secure Firewall Threat Defense デバイス はタグスイッチング テーブルを読み取ろうとしましたが、失敗しました。

推奨アクション 不要。

779004

エラーメッセージ `%Threat Defense-3-779004: STS: Failed to write tag-switching table - reason`

説明 Secure Firewall Threat Defense デバイス はタグスイッチング テーブルに書き込もうとしましたが、失敗しました。

推奨アクション 不要。

779005

エラーメッセージ `%Threat Defense-3-779005: STS: Failed to parse tag-switching request from http - reason`

説明 Secure Firewall Threat Defense デバイス は HTTP 要求を解析して、タグスイッチング テーブルで何をすべきかを確認しようとしましたが、失敗しました。

推奨アクション 不要。

779006

エラーメッセージ `%Threat Defense-3-779006: STS: Failed to save tag-switching table to flash - reason`

説明 Secure Firewall Threat Defense デバイス はタグスイッチング テーブルをフラッシュ メモリに保存しようとしましたが、失敗しました。

推奨アクション 不要。

779007

エラーメッセージ `%Threat Defense-3-779007: STS: Failed to replicate tag-switching table to peer - reason`

説明 Secure Firewall Threat Defense デバイス はタグスイッチングテーブルをフェールオーバー スタンバイ ユニットまたはクラスタリング データ ユニットに複製しようとしましたが、失敗しました。

推奨アクション 不要。

780001

エラーメッセージ `%Threat Defense-6-780001: RULE ENGINE: Started compilation for access-group transaction - description of the transaction .`

説明 ルール エンジンがアクセス グループ トランザクションに必要なコンパイルを開始しました。description of the transaction は、アクセス グループ自体のコマンド ライン入力です。

推奨アクション 不要。

780002

エラーメッセージ `%Threat Defense-6-780002: RULE ENGINE: Finished compilation for access-group transaction - description of the transaction .`

説明 ルールエンジンがトランザクションに必要なコンパイルを終了しました。アクセス グループを例に取ると、description of the transaction は、アクセス グループ自体のコマンド ライン入力です。

推奨アクション 不要。

780003

エラーメッセージ `%Threat Defense-6-780003: RULE ENGINE: Started compilation for nat transaction - description of the transaction .`

説明 ルールエンジンがNATトランザクションに必要なコンパイルを開始しました。description of the transaction は、**nat** コマンド自体のコマンド ライン入力です。

推奨アクション 不要。

780004

エラーメッセージ `%Threat Defense-6-780004: RULE ENGINE: Finished compilation for nat transaction - description of the transaction .`

説明 ルールエンジンがNATトランザクションに必要なコンパイルを終了しました。description of the transaction は、**nat** コマンド自体のコマンド ライン入力です。

推奨アクション 不要。

780005

エラーメッセージ `%FTD-6-780005: RULE ENGINE: Started compilation for session transaction - description of the transaction .`

説明 ルールエンジンによりセッショントランザクションに必要なコンパイルが終了しました。このメッセージは、トランザクションコミットが有効な場合にのみ生成されます。

推奨アクション 不要。

780006

エラーメッセージ `%Threat Defense-6-780006: RULE ENGINE: Finished compilation for session transaction - description of the transaction .`

説明 ルールエンジンによりトランザクションに必要なコンパイルが終了しました。このメッセージは、トランザクションコミットが有効な場合にのみ生成されます。

推奨アクション 不要。

785001

エラーメッセージ `%Threat Defense-7-785001: Clustering: Ownership for existing flow from <in_interface>:<src_ip_addr>/<src_port> to <out_interface>:<dest_ip_addr>/<dest_port> moved from unit <old-owner-unit-id> at site <old-site-id> to <new-owner-unit-id> at site <old-site-id> due to <reason>.`

説明 このsyslogは、クラスタリングによって、DC間環境におけるあるサイトのある装置から別のサイトの別の装置にフローが移動した場合に生成されます。reasonはLISP通知など、移動をトリガーしたものである必要があります。

推奨アクション 新しいサイトの新しい装置のフロー ステータスを確認します。

メッセージ 803001 ～ 8300006

この項では、803001 ～ 852002 および 8300001 ～ 8300006 のメッセージについて説明します。

803001

エラーメッセージ `%Threat Defense-6-803001: bypass is continuing after power up, no protection will be provided by the system for traffic over GigabitEthernet 1/1-1/2`

説明ブートアップ後にハードウェア バイパスが継続されることを示すユーザーへの情報メッセージ。

推奨アクション必要なし。

エラーメッセージ `%Threat Defense-6-803001: bypass is continuing after power up, no protection will be provided by the system for traffic over GigabitEthernet 1/3-1/4`

説明ブートアップ後にハードウェア バイパスが継続されることを示すユーザーへの情報メッセージ。

推奨アクション 不要。

803002

エラーメッセージ `%Threat Defense-6-803002: no protection will be provided by the system for traffic over GigabitEthernet 1/1-1/2`

説明ハードウェア バイパスが手動で有効になっているというユーザーに対する情報メッセージ。

推奨アクション必要なし。

エラーメッセージ `%Threat Defense-6-803002: no protection will be provided by the system for traffic over GigabitEthernet 1/3-1/4`

説明ハードウェア バイパスが手動で有効になっているというユーザーに対する情報メッセージ。

推奨アクション 不要。

803003

エラーメッセージ `%Threat Defense-6-803003: User disabled bypass manually on GigabitEthernet 1/1-1/2.`

説明ハードウェア バイパスが手動で無効になっているというユーザーに対する情報メッセージ。

推奨アクション 不要。

エラーメッセージ `%Threat Defense-6-803003: User disabled bypass manually on GigabitEthernet 1/3-1/4.`

説明ハードウェア バイパスが手動で無効になっているというユーザーに対する情報メッセージ。

推奨アクション 不要。

804001

エラーメッセージ `%Threat Defense-6-804001: Interface GigabitEthernet1/3 1000BaseSX SFP has been inserted`

説明サポートされているSFPモジュールのオンライン挿入に関するユーザーへの情報メッセージ。

推奨アクション 不要。

804002

エラーメッセージ `%Threat Defense-6-804002: Interface GigabitEthernet1/3 SFP has been removed`

説明サポートされている SFP モジュールの削除に関するユーザーへの情報メッセージ。

推奨アクション 不要。

805001

エラーメッセージ `%Threat Defense-6-805001: Flow offloaded: connection conn_id outside_ifc:outside_addr/outside_port (mapped_addr/mapped_port) inside_ifc:inside_addr/inside_port (mapped_addr/mapped_port) Protocol`

説明フローが超高速パスにオフロードされることを示します。

推奨アクション 不要。

805002

エラーメッセージ `%Threat Defense-6-805002: Flow is no longer offloaded: connection conn_id outside_ifc:outside_addr/outside_port (mapped_addr/mapped_port) inside_ifc:inside_addr/inside_port (mapped_addr/mapped_port) Protocol`

説明超高速パスにオフロードされたフローでフローのオフロードが無効になっていることを示します。

推奨アクション 不要。

805003

エラーメッセージ `%Threat Defense-6-805003: TCP Flow could not be offloaded for connection conn_id from outside_ifc:outside_addr/outside_port (mapped_addr/mapped_port) to inside_ifc:inside_addr/inside_port (mapped_addr/mapped_port)`*reason*

説明 フローをオフロードできなかったことを示します。たとえば、オフロード フロー テーブルでのフロー エントリ コリジョンが原因です。

推奨アクション 不要。

806001

エラーメッセージ `%Threat Defense-6-806001: Primary alarm CPU temperature is High temperature`

説明 CPUが高温のプライマリ アラーム温度設定を上回りました。また、このアラームがイネーブルになっています。

- temperature：CPU の現在の温度（セ氏）。

推奨アクション 次のアクションでこのアラームを設定した管理者に問い合わせてください。

806002

エラーメッセージ `%Threat Defense-6-806002: Primary alarm for CPU high temperature is cleared`

説明 CPU の温度が高温のプライマリ アラーム温度設定を下回りました。

推奨アクション 不要。

806003

エラーメッセージ `%Threat Defense-6-806003: Primary alarm CPU temperature is Low temperature`

説明 CPU が低温に関するプライマリ アラーム温度設定を下回りました。また、このアラームがイネーブルになっています。

- temperature：CPU の現在の温度（セ氏）。

  推奨アクション 次のアクションでこのアラームを設定した管理者に問い合わせてください。

806004

エラーメッセージ `%Threat Defense-6-806004: Primary alarm for CPU Low temperature is cleared`

説明 CPU の温度が低温のプライマリ アラーム温度設定を上回りました。

推奨アクション 不要。

806005

エラーメッセージ `%Threat Defense-6-806005: Secondary alarm CPU temperature is High temperature`

説明 CPUが高温のセカンダリ アラーム温度設定を上回りました。また、このアラームがイネーブルになっています。

- temperature：CPU の現在の温度（セ氏）。

推奨アクション 次のアクションでこのアラームを設定した管理者に問い合わせてください。

806006

エラーメッセージ `%Threat Defense-6-806006: Secondary alarm for CPU high temperature is cleared`

説明 CPU の温度が高温のセカンダリ アラーム温度設定を下回りました。

推奨アクション 不要。

806007

エラーメッセージ `%Threat Defense-6-806007: Secondary alarm CPU temperature is Low temperature`

説明 CPU が低温に関するセカンダリ アラーム温度設定を下回りました。また、このアラームがイネーブルになっています。

- temperature：CPU の現在の温度（セ氏）。

推奨アクション 次のアクションでこのアラームを設定した管理者に問い合わせてください。

806008

エラーメッセージ `%Threat Defense-6-806008: Secondary alarm for CPU Low temperature is cleared`

説明 CPU の温度が低温のセカンダリ アラーム温度設定を上回りました。

推奨アクション 不要。

806009

エラーメッセージ `%Threat Defense-6-806009: Alarm asserted for ALARM_IN_1 description`

説明 アラーム入力ポート 1 がトリガーされます。

• description：このアラーム入力ポートのユーザーが設定したアラームの説明。

推奨アクション 次のアクションでこのアラームを設定した管理者に問い合わせてください。

806010

エラーメッセージ `%Threat Defense-6-806010: Alarm cleared for ALARM_IN_1 alarm_1_description`

説明 アラーム入力ポート 1 はクリアされます。

• description：このアラーム入力ポートのユーザーが設定したアラームの説明。

推奨アクション 不要。

806011

エラーメッセージ `%Threat Defense-6-806011: Alarm asserted for ALARM_IN_2 description`

説明 アラーム入力ポート 2 がトリガーされます。

• description：このアラーム入力ポートのユーザーが設定したアラームの説明。

推奨アクション 次のアクションでこのアラームを設定した管理者に問い合わせてください。

806012

エラーメッセージ `%Threat Defense-6-806012: Alarm cleared for ALARM_IN_2 alarm_2_description`

説明 アラーム入力ポート 2 はクリアされます。

• description：このアラーム入力ポートのユーザーが設定したアラームの説明。

推奨アクション 不要。

840001

エラーメッセージ `%Threat Defense-3-840001: Failed to create the backup for an IKEv2 session <Local IP>, <Remote IP>`

説明分散型サイト間 VPN の高可用性設定では、IKEv2 セッションが確立されたとき、またはクラスタ メンバーシップが変更されたときにバックアップセッションの作成が試行されます。ただし、容量制限などの理由で試行が失敗する場合があります。したがって、このメッセージは、バックアップの作成に失敗したことが通知されるたびに、セッション所有者の装置で生成されます。

推奨アクションなし。

850001

エラーメッセージ `%Threat Defense-3-850001: SNORT ID (<snort-instance-id>/<snort-process-id>) Automatic-Application-Bypass due to delay of <delay>ms (threshold <AAB-threshold>ms) with <connection-info>`

説明 パケット遅延が自動アプリケーションバイパス（AAB）しきい値を超えたために AAB イベントがトリガーされました。

推奨アクション トラブルシューティングアーカイブ（Snort コアファイル）を収集し、Cisco TAC に連絡します。

850002

エラーメッセージ `%Threat Defense-3-850002: SNORT ID (<snort-instance-id>/<snort-process-id>) Automatic-Application-Bypass due to SNORT not responding to traffics for <timeout-delay>ms(threshold <AAB-threshold>ms)`

説明 自動アプリケーションバイパス（AAB）しきい値を超える期間にわたって Snort がトラフィックに応答しなかったために AAB イベントがトリガーされました。

推奨アクション トラブルシューティングアーカイブ（Snort コアファイル）を収集し、Cisco TAC に連絡します。

852001

エラーメッセージ `%FTD-6-852001: Received Lightweight to Full Proxy event from application Snort for TCP flow ip-address/port to ip-address/port`

説明 このメッセージは、Snort が接続の照合ポリシー（SSL ポリシーなど）に基づいて TCP のペイロードを検査することを決定すると表示されます。

- ip-address：フローの IPv4 または IPv6 アドレス
- port：TCP ポート番号

推奨アクション 不要。

852002

エラーメッセージ `%FTD-6-852002: Received Full Proxy to Lightweight event from application Snort for TCP flow ip-address/port to ip-address/port`

説明 このメッセージは、Snort が接続の照合ポリシー（SSL ポリシー DND など）に基づいて TCP のペイロードを検査する必要がなくなると表示されます。

- ip-address：フローの IPv4 または IPv6 アドレス
- port：TCP ポート番号

推奨アクション 不要。

8300001

エラーメッセージ `%Threat Defense-6-8300001: VPN session redistribution <variable 1>`

説明これらのイベントは、「cluster redistribute vpn-sessiondb」に関連する操作が開始または完了したことを管理者に通知します。それぞれの説明は次のとおりです。

- <variable 1>：アクション。started または completed

推奨アクション なし。

8300002

エラーメッセージ `%Threat Defense-6-8300002: Moved <variable 1> sessions to <variable 2>`

説明クラスタの別のメンバーに移動されたアクティブ セッション数の詳細を示します。

- <variable 1>：移動されたアクティブなセッションの数（要求された数よりも少ない可能性があります）
- <variable 2>：移動先のセッションのクラスタ メンバーの名前

推奨アクション なし。

8300003

エラーメッセージ `%Threat Defense-3-8300003: Failed to send session redistribution message to <variable 1>`

説明要求を別のクラスタ メンバーに送信するエラーが発生しました。内部エラーのためか、またはメッセージの宛先のクラスタ メンバーが利用できないためである可能性があります。

- <variable 1>：メッセージの宛先のクラスタ メンバーの名前

推奨アクション このメッセージが表示され続ける場合は、カスタマー サポートにお問い合わせください。

8300004

エラーメッセージ `%Threat Defense-6-8300004: <variable 1> request to move <variable 2> sessions from <variable 3> to <variable 4>`

説明 このイベントは、メンバーが特定の数のアクティブセッションをグループ内の別のメンバーに移動する要求をディレクタから受け取った場合に表示されます。

- <variable 1>：アクション。Received、Sent
- <variable 2>：移動するアクティブなセッション数
- <variable 3>：移動セッション要求を受信しているメンバーの名前

- <variable 4>：アクティブセッションを受信するメンバーの名前

推奨アクションなし。

8300005

エラーメッセージ `%Threat Defense-3-8300005: Failed to receive session move response from <variable 1>`

説明ディレクタが、アクティブなセッションを別のメンバーに移動するようにメンバーに要求しました。ディレクタが定義された期間内にこの要求に対する応答を受信しなかった場合、このイベントを表示し、再配布プロセスを終了します。

- <variable 1>：タイムアウト期間内に移動応答を送信できなかったメンバーの名前

推奨アクション「cluster redistribute vpn-sessiondb」を再発行しても問題が解決しない場合は、サポートにお問い合わせください。

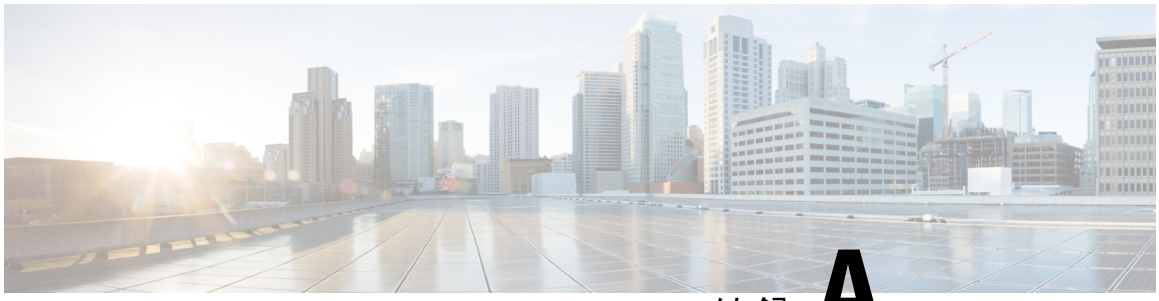
8300006

エラーメッセージ `%Threat Defense-5-8300006: Cluster topology change detected. VPN session redistribution aborted.`

説明 VPN セッションの再配布移動計算は、プロセスの開始時にアクティブなメンバーに基づいて行われます。このプロセス中にメンバーが参加したり離脱したりすると、ディレクタはセッションの再配布を終了します。

推奨アクションメンバーのすべてがグループに参加したり離脱したりした場合は、操作を再試行します。

8300006



付録 A

重大度別システムヘルスおよびネットワーク診断メッセージリスト

この付録の内容は、次のとおりです。

アラート メッセージ、重大度 1

次のメッセージが重大度 1（アラート）で表示されます。

- %FTD-1-101001: (Primary) Failover cable OK.
- %FTD-1-101002: (Primary) Bad failover cable.
- %FTD-1-101003: (Primary) Failover cable not connected (this unit).
- %FTD-1-101004: (Primary) Failover cable not connected (other unit).
- %FTD-1-101005: (Primary) Error reading failover cable status.
- %FTD-1-103001: (Primary) No response from other firewall (reason code = code).
- %FTD-1-103002: (Primary) Other firewall network interface interface_number OK.
- %FTD-1-103003: (Primary) Other firewall network interface interface_number failed.
- %FTD-1-103004: (Primary) Other firewall reports this firewall failed. Reason: reason-string
- %FTD-1-103005: (Primary) Other firewall reporting failure. Reason: SSM card failure
- %FTD-1-103006: (Primary|Secondary) Mate version ver_num is not compatible with ours ver_num

重大度別システムヘルスおよびネットワーク診断メッセージリスト

- %FTD-1-103007: (Primary|Secondary) Mate version ver_num is not identical with ours ver_num
- %FTD-1-103008: Mate hwdib index is not compatible.
- %Threat Defense-1-104001: (Primary) Switching to ACTIVE (cause: string).
- %FTD-1-104002: (Primary) Switching to STANDBY (cause: string).
- %FTD-1-104003: (Primary) Switching to FAILED.
- %FTD-1-104004: (Primary) Switching to OK.
- %FTD-1-105001: (Primary) Disabling failover.
- %FTD-1-105002: (Primary) Enabling failover.
- %FTD-1-105003: (Primary) Monitoring on interface interface_name waiting
- %FTD-1-105004: (Primary) Monitoring on interface interface_name normal
- %FTD-1-105005: (Primary) Lost Failover communications with mate on interface interface_name.
- %FTD-1-105006: (Primary) Link status Up on interface interface_name.
- %FTD-1-105007: (Primary) Link status Down on interface interface_name.
- %FTD-1-105008: (Primary) Testing interface interface_name.
- %FTD-1-105009: (Primary) Testing on interface interface_name {Passed|Failed}.
- %FTD-1-105011: (Primary) Failover cable communication failure
- %FTD-1-105020: (Primary) Incomplete/slow config replication
- %FTD-1-105021: (failover_unit) Standby unit failed to sync due to a locked context_name config. Lock held by lock_owner_name
- %FTD-1-105022: (host) Config replication failed with reason = (reason)
- %FTD-1-105031: Failover LAN interface is up
- %FTD-1-105032: LAN Failover interface is down
- %FTD-1-105034: Receive a LAN_FAILOVER_UP message from peer.
- %FTD-1-105035: Receive a LAN failover interface down msg from peer.
- %FTD-1-105036: dropped a LAN Failover command message.
- %FTD-1-105037: The primary and standby units are switching back and forth as the active unit.
- %FTD-1-105038: (Primary) Interface count mismatch
- %FTD-1-105039: (Primary) Unable to verify the Interface count with mate. Failover may be disabled in mate.
- %FTD-1-105040: (Primary) Mate failover version is not compatible.
- %FTD-1-105041: cmd failed during sync.
- %FTD-1-105042: (Primary) Failover interface OK
- %FTD-1-105043: (Primary) Failover interface failed

重大度別システムヘルスおよびネットワーク診断メッセージリスト

- %FTD-1-105044: (Primary) Mate operational mode mode is not compatible with my mode mode.
- %FTD-1-105045: (Primary) Mate license (number contexts) is not compatible with my license (number contexts).
- %FTD-1-105046: (Primary|Secondary) Mate has a different chassis
- %FTD-1-105047: Mate has a io_card_name1 card in slot slot_number which is different from my io_card_name2
- %FTD-1-105048: (unit) Mate's service module (application) is different from mine (application)
- %FTD-1-106021: Deny protocol reverse path check from source_address to dest_address on interface interface_name
- %FTD-1-106022: Deny protocol connection spoof from source_address to dest_address on interface interface_name
- %FTD-1-106101 The number of ACL log deny-flows has reached limit (number).
- %FTD-1-107001: RIP auth failed from IP_address: version=number, type=string, mode=string, sequence=number on interface interface_name
- %FTD-1-107002: RIP pkt failed from IP_address: version=number on interface interface_name
- %FTD-1-111111 error_message
- %FTD-1-114001: Failed to initialize 4GE SSM I/O card (error error_string).
- %FTD-1-114002: Failed to initialize SFP in 4GE SSM I/O card (error error_string).
- %FTD-1-114003: Failed to run cached commands in 4GE SSM I/O card (error error_string).
- %FTD-1-1199012: Stack smash during new_stack_call in process/fiber process/fiber, call target f, stack size s, process/fiber name of the process/fiber that caused the stack smash
- %FTD-1-199010: Signal 11 caught in process/fiber(rtcli async executor process)/(rtcli async executor) at address 0xf132e03b, corrective action at 0xca1961a0
- %Threat Defense-1-199013: syslog
- %FTD-1-199021: System memory utilization has reached the configured watchdog trigger level of Y%. System will now reload
- %FTD-1-211004: WARNING: Minimum Memory Requirement for ASA version ver not met for ASA image. min MB required, actual MB found.
- %FTD-n-216001: internal error in: function: message
- %FTD-1-323006: Module ips experienced a data channel communication failure, data channel is DOWN.
- %FTD-1-332004: Web Cache IP_address/service_ID lost
- %FTD-1-505011: Module ips data channel communication is UP.
- %FTD-1-505014: Module module_id, application down name, version version reason
- %FTD-1-505015: Module module_id, application up application, version version
- %FTD-1-709003: (Primary) Beginning configuration replication: Sending to mate.

重大度別システムヘルスおよびネットワーク診断メッセージリスト

- %FTD-1-709004: (Primary) End Configuration Replication (ACT)
- %FTD-1-709005: (Primary) Beginning configuration replication: Receiving from mate.
- %FTD-1-709006: (Primary) End Configuration Replication (STB)
- %FTD-1-713900: Descriptive_event_string.
- %FTD-1-716507: Fiber scheduler has reached unreachable code. Cannot continue, terminating.
- %FTD-1-716508: internal error in: function: Fiber scheduler is scheduling rotten fiber. Cannot continuing terminating
- %FTD-1-716509: internal error in: function: Fiber scheduler is scheduling alien fiber. Cannot continue terminating
- %FTD-1-716510: internal error in: function: Fiber scheduler is scheduling finished fiber. Cannot continue terminating
- %FTD-1-716516: internal error in: function: OCCAM has corrupted ROL array. Cannot continue terminating
- %FTD-1-716519: internal error in: function: OCCAM has corrupted pool list. Cannot continue terminating
- %FTD-1-716528: Unexpected fiber scheduler error; possible out-of-memory condition
- %FTD-1-717049: Local CA Server certificate is due to expire in number days and a replacement certificate is available for export.
- %FTD-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
- %FTD-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
- %FTD-1-735001 Cooling Fan var1: OK
- %FTD-1-735002 Cooling Fan var1: Failure Detected
- %FTD-1-735003 Power Supply var1: OK
- %FTD-1-735004 Power Supply var1: Failure Detected
- %FTD-1-735005 Power Supply Unit Redundancy OK
- %FTD-1-735006 Power Supply Unit Redundancy Lost
- %FTD-1-735007 CPU var1: Temp: var2 var3, Critical
- %FTD-1-735008 IPMI: Chassis Ambient var1: Temp: var2 var3, Critical
- %FTD-1-735011: Power Supply var1: Fan OK
- %FTD-1-735012: Power Supply var1: Fan Failure Detected
- %FTD-1-735013: Voltage Channel var1: Voltage OK
- %FTD-1-735014: Voltage Channel var1: Voltage Critical

- %FTD-1-735017: Power Supply var1: Temp: var2 var3, OK
- %FTD-1-735020: CPU var1: Temp: var2 var3 OK
- %FTD-1-735021: Chassis var1: Temp: var2 var3 OK
- %FTD-1-735022: CPU# is running beyond the max thermal operating temperature and the device will be shutting down immediately to prevent permanent damage to the CPU.
- %FTD-1-735024: IO Hub var1: Temp: var2 var3, OK
- %FTD-1-735025: IO Hub var1: Temp: var2 var3, Critical
- %FTD-1-735027: CPU cpu_num Voltage Regulator is running beyond the max thermal operating temperature and the device will be shutting down immediately. シャーシおよび CPU に通気の問題がないか、ただちに検査する必要があります。
- %FTD-1-735029: IO Hub is running beyond the max thermal operating temperature and the device will be shutting down immediately to prevent permanent damage to the circuit.
- %FTD-1-743000: The PCI device with vendor ID: vendor_id device ID: device_id located at bus:device.function bus_num:dev_num, func_num has a link link_attr_name of actual_link_attr_val when it should have a link link_attr_name of expected_link_attr_val.
- %FTD-1-743001: Backplane health monitoring detected link failure
- %FTD-1-743002: Backplane health monitoring detected link OK
- %FTD-1-743004: System is not fully operational - PCI device with vendor ID vendor_id (vendor_name), device ID device_id (device_name) not found
- %Threat Defense-1-770002: Resource resource allocation is more than the permitted limit for this platform. ASA will be rebooted.

クリティカル メッセージ、重大度 2

次のメッセージが重大度 2（クリティカル）で表示されます。

- %Threat Defense-2-106001: Inbound TCP connection denied from IP_address/port to IP_address/port flags tcp_flags on interface interface_name
- %Threat Defense-2-106002: protocol Connection denied by outbound list acl_ID src inside_address dest outside_address
- %Threat Defense-2-106006: Deny inbound UDP from outside_address/outside_port to inside_address/inside_port on interface interface_name.
- %Threat Defense-2-106007: Deny inbound UDP from outside_address/outside_port to inside_address/inside_port due to DNS {Response|Query}.
- %Threat Defense-2-106013: Dropping echo request from IP_address to PAT address IP_address
- %Threat Defense-2-106016: Deny IP spoof from (IP_address) to IP_address on interface interface_name.
- %Threat Defense-2-106017: Deny IP due to Land Attack from IP_address to IP_address

重大度別システムヘルスおよびネットワーク診断メッセージリスト

- %Threat Defense-2-106018: ICMP packet type ICMP_type denied by outbound list acl_ID src inside_address dest outside_address
- %Threat Defense-2-106020: Deny IP teardrop fragment (size = number, offset = number) from IP_address to IP_address
- %Threat Defense-2-106024: Access rules memory exhausted
- %Threat Defense-2-108003: Terminating ESMTP/SMTP connection; malicious pattern detected in the mail address from source_interface:source_address/source_port to dest_interface:dest_address/dset_port. Data:string
- %Threat Defense-2-109011: Authen Session Start: user 'user', sid number
- %Threat Defense-2-112001: (string:dec) Clear complete.
- %Threat Defense-2-113022: AAA Marking RADIUS server servername in aaa-server group AAA-Using-DNS as FAILED
- %Threat Defense-2-113023: AAA Marking protocol server ip-addr in server group tag as ACTIVE
- %Threat Defense-2-113027: Username could not be found in certificate
- %Threat Defense-2-115000: Critical assertion in process: process name fiber: fiber name, component: component name, subcomponent: subcomponent name, file: filename, line: line number, cond: condition
- %Threat Defense-2-199011: Close on bad channel in process/fiber process/fiber, channel ID p, channel state s process/fiber name of the process/fiber that caused the bad channel close operation.
- %Threat Defense-2-199014: syslog
- %Threat Defense-2-199020: System memory utilization has reached X%. System will reload if memory usage reaches the configured trigger level of Y%.
- %Threat Defense-2-201003: Embryonic limit exceeded nconns/elimit for outside_address/outside_port (global_address) inside_address/inside_port on interface interface_name
- %Threat Defense-2-214001: Terminating manager session from IP_address on interface interface_name. Reason: incoming encrypted data (number bytes) longer than number bytes
- %Threat Defense-2-215001:Bad route_compress() call, sdb= number
- %Threat Defense-2-217001: No memory for string in string
- %Threat Defense-2-218001: Failed Identification Test in slot# [fail#/res].
- %Threat Defense-2-218002: Module (slot#) is a registered proto-type for Cisco Lab use only, and not certified for live network operation.
- %Threat Defense-2-218003: Module Version in slot# is obsolete. The module in slot = slot# is obsolete and must be returned via RMA to Cisco Manufacturing. If it is a lab unit, it must be returned to Proto Services for upgrade.
- %Threat Defense-2-218004: Failed Identification Test in slot# [fail#/res]
- %Threat Defense-2-218005: Inconsistency detected in the system information programmed in non-volatile memory
- %Threat Defense-2-321005: System CPU utilization reached utilization %

重大度別システムヘルスおよびネットワーク診断メッセージリスト

- %Threat Defense-2-321006: System memory usage reached utilization %
- %Threat Defense-2-410002: Dropped num DNS responses with mis-matched id in the past sec second(s): from src_ifc:sip/sport to dest_ifc:dip/dport
- %Threat Defense-2-709007: Configuration replication failed for command command
- %Threat Defense-2-713078: Temp buffer for building mode config attributes exceeded: bufsize available_size, used value
- %Threat Defense-2-713176: Device_type memory resources are critical, IKE key acquire message on interface interface_number, for Peer IP_address ignored
- %Threat Defense-2-713901: Descriptive_text_string.
- %Threat Defense-2-716500: internal error in: function: Fiber library cannot locate AK47 instance
- %Threat Defense-2-716501: internal error in: function: Fiber library cannot attach AK47 instance
- %Threat Defense-2-716502: internal error in: function: Fiber library cannot allocate default arena
- %Threat Defense-2-716503: internal error in: function: Fiber library cannot allocate fiber descriptors pool
- %Threat Defense-2-716504: internal error in: function: Fiber library cannot allocate fiber stacks pool
- %Threat Defense-2-716505: internal error in: function: Fiber has joined fiber in unfinished state
- %Threat Defense-2-716506: UNICORN_SYSLOGID_JOINED_UNEXPECTED_FIBER
- %Threat Defense-2-716512: internal error in: function: Fiber has joined fiber waited upon by someone else
- %Threat Defense-2-716513: internal error in: function: Fiber in callback blocked on other channel
- %Threat Defense-2-716515: internal error in: function: OCCAM failed to allocate memory for AK47 instance
- %Threat Defense-2-716517: internal error in: function: OCCAM cached block has no associated arena
- %ASWA-2-716518: internal error in: function: OCCAM pool has no associated arena
- %Threat Defense-2-716520: internal error in: function: OCCAM pool has no block list
- %Threat Defense-2-716521: internal error in: function: OCCAM no realloc allowed in named pool
- %Threat Defense-2-716522: internal error in: function: OCCAM corrupted standalone block
- %Threat Defense-2-716525: UNICORN_SYSLOGID_SAL_CLOSE_PRIVDATA_CHANGED
- %Threat Defense-2-716526: UNICORN_SYSLOGID_PERM_STORAGE_SERVER_LOAD_FAIL
- %Threat Defense-2-716527: UNICORN_SYSLOGID_PERM_STORAGE_SERVER_STORE_FAI
- %Threat Defense-2-717008: Insufficient memory to process_requiring_memory.
- %Threat Defense-2-717011: Unexpected event event event_ID
- %Threat Defense-2-735009: IPMI: Environment Monitoring has failed initialization and configuration. Environment Monitoring is not running.

- %Threat Defense-2-735023: ASA was previously shutdown due to the CPU complex running beyond the maximum thermal operating temperature. The chassis needs to be inspected immediately for ventilation issues.
- %Threat Defense-2-735028: ASA was previously shutdown due to a CPU Voltage Regulator running beyond the max thermal operating temperature. The chassis and CPU need to be inspected immediately for ventilation issues.
- %Threat Defense-2-736001: Unable to allocate enough memory at boot for jumbo-frame reservation. Jumbo-frame support has been disabled.
- %Threat Defense-2-747009: Clustering: Fatal error due to failure to create RPC server for module module name.
- %Threat Defense-2-747011: Clustering: Memory allocation error.
- %Threat Defense-2-752001: Tunnel Manager received invalid parameter to remove record.
- %Threat Defense-2-748007: Failed to de-bundle the ports for module slot_number in chassis chassis_number; traffic may be black holed
- %Threat Defense-2-752001: Tunnel Manager received invalid parameter to remove record.
- %Threat Defense-2-752005: Tunnel Manager failed to dispatch a KEY_ACQUIRE message. Memory may be low. Map Tag = mapTag. Map Sequence Number = mapSeq.
- %Threat Defense-2-772003: PASSWORD: session login failed, user username, IP ip, cause: password expired
- %Threat Defense-2-772006: REAUTH: user username failed authentication
- %Threat Defense-2-774001: POST: unspecified error
- %Threat Defense-2-774002: POST: error err, func func, engine eng, algorithm alg, mode mode, dir dir, key len len

エラー メッセージ、重大度 3

次のメッセージが重大度 3（エラー）で表示されます。

- %FTD-3-105010: (Primary) Failover message block alloc failed
- %FTD-3-106010: Deny inbound protocol src [interface_name: source_address/source_port] [([idfw_user | FQDN_string], sg_info)] dst [interface_name: dest_address/dest_port}[([idfw_user | FQDN_string], sg_info)]
- %FTD-3-106011: Deny inbound (No xlate) string
- %FTD-3-106014: Deny inbound icmp src interface_name: IP_address [([idfw_user | FQDN_string], sg_info)] dst interface_name: IP_address [([idfw_user | FQDN_string], sg_info)] (type dec, code dec)
- %FTD-3-109013: User must authenticate before using this service
- %FTD-3-109016: Can't find authorization ACL acl_ID for user 'user'
- %FTD-3-109018: Downloaded ACL acl_ID is empty

重大度別システムヘルスおよびネットワーク診断メッセージリスト

- %FTD-3-109019: Downloaded ACL acl_ID has parsing error; ACE string
- %FTD-3-109020: Downloaded ACL has config error; ACE
- %FTD-3-109026: [aaa protocol] Invalid reply digest received; shared server key may be mismatched.
- %FTD-3-109032: Unable to install ACL access_list, downloaded for user username; Error in ACE: ace.
- %FTD-3-109037: Exceeded 5000 attribute values for the attribute name attribute for user username
- %FTD-3-109038: Attribute internal-attribute-name value string-from-server from AAA server could not be parsed as a type internal-attribute-name string representation of the attribute name
- %FTD-3-109103: CoA action-type from coa-source-ip failed for user username, with session ID: audit-session-id.
- %FTD-3-109104: CoA action-type from coa-source-ip failed for user username, session ID: audit-session-id. Action not supported.
- %FTD-3-109203: UAUTH Session *session*, User *username*, Assigned IP *IP Address*, Failed adding entry.
- %FTD-3-109205: UAUTH Session *session*, User *username*, Assigned IP *IP Address*, Failed applying filter.
- %FTD-3-109206: UAUTH Session *session*, User *username*, Assigned IP *IP Address*, Removing stale entry added *hours* ago.
- %FTD-3-109208: UAUTH Session *session*, User *username*, Assigned IP *IP Address*, Failed updating entry - no entry.
- %FTD-3-109209: UAUTH Session *session*, User *username*, Assigned IP *IP Address*, Failed updating filter for entry.
- %FTD-3-109212: UAUTH Session *session*, User *username*, Assigned IP *IP Address*, Failed removing entry.
- %FTD-3-109213: UAUTH Session *session*, User *username*, Assigned IP *IP Address* Failed removing entry.
- %FTD-3-113001: Unable to open AAA session. Session limit [limit] reached.
- %FTD-3-113018: User: user, Unsupported downloaded ACL Entry: ACL_entry, Action: action
- %FTD-3-113020: Kerberos error: Clock skew with server ip_address greater than 300 seconds
- %FTD-3-113021: Attempted console login failed. User username did NOT have appropriate Admin Rights.
- %FTD-3-114006: Failed to get port statistics in 4GE SSM I/O card (error error_string).
- %FTD-3-114007: Failed to get current msr in 4GE SSM I/O card (error error_string).
- %FTD-3-114008: Failed to enable port after link is up in 4GE SSM I/O card due to either I2C serial bus access error or switch access error.
- %FTD-3-114009: Failed to set multicast address in 4GE SSM I/O card (error error_string).
- %FTD-3-114010: Failed to set multicast hardware address in 4GE SSM I/O card (error error_string).

重大度別システムヘルスおよびネットワーク診断メッセージリスト

- %FTD-3-114011: Failed to delete multicast address in 4GE SSM I/O card (error error_string).
- %FTD-3-114012: Failed to delete multicast hardware address in 4GE SSM I/O card (error error_string).
- %FTD-3-114013: Failed to set mac address table in 4GE SSM I/O card (error error_string).
- %FTD-3-114014: Failed to set mac address in 4GE SSM I/O card (error error_string).
- %FTD-3-114015: Failed to set mode in 4GE SSM I/O card (error error_string).
- %FTD-3-114016: Failed to set multicast mode in 4GE SSM I/O card (error error_string).
- %FTD-3-114017: Failed to get link status in 4GE SSM I/O card (error error_string).
- %FTD-3-114018: Failed to set port speed in 4GE SSM I/O card (error error_string).
- %FTD-3-114019: Failed to set media type in 4GE SSM I/O card (error error_string).
- %FTD-3-114020: Port link speed is unknown in 4GE SSM I/O card.
- %FTD-3-114021: Failed to set multicast address table in 4GE SSM I/O card due to error.
- %FTD-3-114022: Failed to pass broadcast traffic in 4GE SSM I/O card due to error_string
- %FTD-3-114023: Failed to cache/flush mac table in 4GE SSM I/O card due to error_string.
- %FTD-3-115001: Error in process: process name fiber: fiber name, component: component name, subcomponent: subcomponent name, file: filename, line: line number, cond: condition.
- %FTD-3-199015: syslog
- %FTD-3-201002: Too many TCP connections on {static|xlate} global_address! econns nconns
- %FTD-3-201004: Too many UDP connections on {static|xlate} global_address! udp connections limit
- %FTD-3-201005: FTP data connection failed for IP_address IP_address
- %FTD-3-201006: RCMD backconnection failed for IP_address/port.
- %FTD-3-201008: Disallowing new connections.
- %FTD-3-201009: TCP connection limit of number for host IP_address on interface_name exceeded
- %FTD-3-201011: Connection limit exceeded cnt/limit for dir packet from sip/sport to dip/dport on interface if_name.
- %FTD-3-201013: Per-client connection limit exceeded curr num/limit for [input|output] packet from ip/port to ip/port on interface interface_name
- %FTD-3-202010: [NAT | PAT] pool exhausted for pool-name, port range [1-511 | 512-1023 | 1024-65535]. Unable to create protocol connection from in-interface:src-ip/src-port to out-interface:dst-ip/dst-port
- %FTD-3-208005: (function:line_num) clear command return code
- %FTD-3-210001: LU sw_module_name error = number
- %FTD-3-210002: LU allocate block (bytes) failed.
- %FTD-3-210003: Unknown LU Object number

重大度別システムヘルスおよびネットワーク診断メッセージリスト

- %FTD-3-210005: LU allocate secondary(optional) connection failed for protocol[TCP|UDP] connection from ingress interface name:Real IP Address/Real Port to egress interface name:Real IP Address/Real Port
- %FTD-3-210006: LU look NAT for IP_address failed
- %FTD-3-210007: LU allocate xlate failed for type[static | dynamic]-[NAT | PAT] secondary(optional) protocol translation from ingress interface name:Real IP Address/real port (Mapped IP Address/Mapped Port) to egress interface name:Real IP Address/Real Port (Mapped IP Address/Mapped Port)
- %FTD-3-210008: LU no xlate for inside_address/inside_port outside_address/outside_port
- %FTD-3-210010: LU make UDP connection for outside_address:outside_port inside_address:inside_port failed
- %FTD-3-210020: LU PAT port port reserve failed
- %FTD-3-210021: LU create static xlate global_address ifc interface_name failed
- %FTD-3-211001: Memory allocation Error
- %FTD-3-211003: Error in computed percentage CPU usage value
- %FTD-3-212001: Unable to open SNMP channel (UDP port port) on interface interface_number, error code = code
- %FTD-3-212002: Unable to open SNMP trap channel (UDP port port) on interface interface_number, error code = code
- %FTD-3-212003: Unable to receive an SNMP request on interface interface_number, error code = code, will try again.
- %FTD-3-212004: Unable to send an SNMP response to IP Address IP_address Port port interface interface_number, error code = code
- %FTD-3-212005: incoming SNMP request (number bytes) on interface interface_name exceeds data buffer size, discarding this SNMP request.
- %FTD-3-212006: Dropping SNMP request from src_addr/src_port to ifc:dst_addr/dst_port because: reason username.
- %FTD-3-212010: Configuration request for SNMP user %s failed. Host %s reason.
- %FTD-3-212011: SNMP engineBoots is set to maximum value. Reason: %s User intervention necessary.
- %FTD-3-212012: Unable to write SNMP engine data to persistent storage.
- %FTD-3-216002: Unexpected event (major: major_id, minor: minor_id) received by task_string in function at line: line_num
- %FTD-3-216003: Unrecognized timer timer_ptr, timer_id received by task_string in function at line: line_num
- %FTD-3-219002: I2C_API_name error, slot = slot_number, device = device_number, address = address, byte count = count. Reason: reason_string
- %FTD-3-302019: H.323 library_name ASN Library failed to initialize, error code number
- %FTD-3-302302: ACL = deny; no sa created

重大度別システムヘルスおよびネットワーク診断メッセージリスト

- %FTD-3-305006: {outbound static|identity|portmap|regular) translation creation failed for protocol src interface_name:source_address/source_port [(idfw_user)] dst interface_name:dest_address/dest_port [(idfw_user)]
- %FTD-3-305016: Unable to create protocol connection from real_interface:real_host_ip/real_source_port to real_dest_interface:real_dest_ip/real_dest_port due to reason.
- %FTD-3-305017: Pba-interim-logging: Active ICMP block of ports for translation from <source device IP> to <destination device IP>/<Active Port Block >
- %FTD-3-313001: Denied ICMP type=number, code=code from IP_address on interface interface_name
- %FTD-3-313008: Denied ICMPv6 type=number, code=code from IP_address on interface interface_name
- %FTD-3-316001: Denied new tunnel to IP_address. VPN peer limit (platform_vpn_peer_limit) exceeded
- %FTD-3-316002: VPN Handle error: protocol=protocol, src in_if_num:src_addr, dst out_if_num:dst_addr
- %FTD-3-317001: No memory available for limit_slow
- %FTD-3-317002: Bad path index of number for IP_address, number max
- %FTD-3-317003: IP routing table creation failure - reason
- %FTD-3-317004: IP routing table limit warning
- %FTD-3-317005: IP routing table limit exceeded - reason, IP_address netmask
- %FTD-3-317006: Pdb index error pdb, pdb_index, pdb_type
- %FTD-3-317012: Interface IP route counter negative - nameif-string-value
- %FTD-3-318001: Internal error: reason
- %FTD-3-318002: Flagged as being an ABR without a backbone area
- %FTD-3-318003: Reached unknown state in neighbor state machine
- %FTD-3-318004: area string lsid IP_address mask netmask adv IP_address type number
- %FTD-3-318005: lsid ip_address adv IP_address type number gateway gateway_address metric number network IP_address mask netmask protocol hex attr hex net-metric number
- %FTD-3-318006: if interface_name if_state number
- %FTD-3-318007: OSPF is enabled on interface_name during idb initialization
- %FTD-3-318008: OSPF process number is changing router-id. Reconfigure virtual link neighbors with our new router-id
- %FTD-3-318009: OSPF: Attempted reference of stale data encountered in function, line: line_num
- %FTD-3-318101: Internal error: %REASON
- %FTD-3-318102: Flagged as being an ABR without a backbone area T
- %FTD-3-318103: Reached unknown state in neighbor state machine

重大度別システムヘルスおよびネットワーク診断メッセージリスト

- %FTD-3-318104: DB already exist : area %AREA_ID_STR lsid %i adv %i type 0x%x
- %FTD-3-318105: lsid %i adv %i type 0x%x gateway %i metric %d network %i mask %i protocol %#x attr %#x net-metric %d
- %FTD-3-318106: if %IF_NAME if_state %d
- %FTD-3-318107: OSPF is enabled on %IF_NAME during idb initialization
- %FTD-3-318108: OSPF process %d is changing router-id. Reconfigure virtual link neighbors with our new router-id
- %FTD-3-318109: OSPFv3 has received an unexpected message: %0x/%0x
- %FTD-3-318110: Invalid encrypted key %s.
- %FTD-3-318111: SPI %u is already in use with ospf process %d
- %FTD-3-318112: SPI %u is already in use by a process other than ospf process %d.
- %FTD-3-318113: %s %s is already configured with SPI %u.
- %FTD-3-318114: The key length used with SPI %u is not valid
- %FTD-3-318115: %s error occured when attempting to create an IPsec policy for SPI %u
- %FTD-3-318116: SPI %u is not being used by ospf process %d.
- %FTD-3-318117: The policy for SPI %u could not be removed because it is in use.
- %FTD-3-318118: %s error occured when attemtping to remove the IPsec policy with SPI %u
- %FTD-3-318119: Unable to close secure socket with SPI %u on interface %s
- %FTD-3-318120: OSPFv3 was unable to register with IPsec
- %FTD-3-318121: IPsec reported a GENERAL ERROR: message %s, count %d
- %FTD-3-318122: IPsec sent a %s message %s to OSPFv3 for interface %s. Recovery attempt %d .
- %FTD-3-318123: IPsec sent a %s message %s to OSPFv3 for interface %IF_NAME. Recovery aborted
- %FTD-3-318125: Init failed for interface %IF_NAME
- %FTD-3-318126: Interface %IF_NAME is attached to more than one area
- %FTD-3-318127: Could not allocate or find the neighbor
- %FTD-3-320001: The subject name of the peer cert is not allowed for connection
- %FTD-3-321007: System is low on free memory blocks of size block_size (free_blocks CNT out of max_blocks MAX)
- %FTD-3-322001: Deny MAC address MAC_address, possible spoof attempt on interface interface
- %FTD-3-322002: ARP inspection check failed for arp {request|response} received from host MAC_address on interface interface. This host is advertising MAC Address MAC_address_1 for IP Address IP_address, which is {statically|dynamically} bound to MAC Address MAC_address_2.

重大度別システムヘルスおよびネットワーク診断メッセージリスト

- %FTD-3-322003:ARP inspection check failed for arp {request|response} received from host MAC_address on interface interface. This host is advertising MAC Address MAC_address_1 for IP Address IP_address, which is not bound to any MAC Address.
- %FTD-3-323001: Module module_id experienced a control channel communications failure.
- %FTD-3-323002: Module module_id is not able to shut down, shut down request not answered.
- %FTD-3-323003: Module module_id is not able to reload, reload request not answered.
- %FTD-3-323004: Module module_id failed to write software vnewver (currently vver), reason. Hw-module reset is required before further use.
- %FTD-3-323005: Module module_id can not be started completely
- %FTD-3-323007: Module in slot slot experienced a firware failure and the recovery is in progress.
- %FTD-3-325001: Router ipv6_address on interface has conflicting ND (Neighbor Discovery) settings
- %FTD-3-326001: Unexpected error in the timer library: error_message
- %FTD-3-326002: Error in error_message: error_message
- %FTD-3-326004: An internal error occurred while processing a packet queue
- %FTD-3-326005: Mrib notification failed for (IP_address, IP_address)
- %FTD-3-326006: Entry-creation failed for (IP_address, IP_address)
- %FTD-3-326007: Entry-update failed for (IP_address, IP_address)
- %FTD-3-326008: MRIB registration failed
- %FTD-3-326009: MRIB connection-open failed
- %FTD-3-326010: MRIB unbind failed
- %FTD-3-326011: MRIB table deletion failed
- %FTD-3-326012: Initialization of string functionality failed
- %FTD-3-326013: Internal error: string in string line %d (%s)
- %FTD-3-326014: Initialization failed: error_message error_message
- %FTD-3-326015: Communication error: error_message error_message
- %FTD-3-326016: Failed to set un-numbered interface for interface_name (string)
- %FTD-3-326017: Interface Manager error - string in string: string
- %FTD-3-326019: string in string: string
- %FTD-3-326020: List error in string: string
- %FTD-3-326021: Error in string: string
- %FTD-3-326022: Error in string: string
- %FTD-3-326023: string - IP_address: string
- %FTD-3-326024: An internal error occurred while processing a packet queue.

重大度別システムヘルスおよびネットワーク診断メッセージリスト

- %FTD-3-326025: string
- %FTD-3-326026: Server unexpected error: error_message
- %FTD-3-326027: Corrupted update: error_message
- %FTD-3-326028: Asynchronous error: error_message
- %FTD-3-327001: IP SLA Monitor: Cannot create a new process
- %FTD-3-327002: IP SLA Monitor: Failed to initialize, IP SLA Monitor functionality will not work
- %FTD-3-327003: IP SLA Monitor: Generic Timer wheel timer functionality failed to initialize
- %FTD-3-328001: Attempt made to overwrite a set stub function in string.
- %FTD-3-329001: The string0 subblock named string1 was not removed
- %FTD-3-331001: Dynamic DNS Update for 'fqdn_name' = ip_address failed
- %FTD-3-332001: Unable to open cache discovery socket, WCCP V2 closing down.
- %FTD-3-332002: Unable to allocate message buffer, WCCP V2 closing down.
- %FTD-3-336001 Route desination_network stuck-in-active state in EIGRP-ddb_name as_num. Cleaning up
- %FTD-3-336002: Handle handle_id is not allocated in pool.
- %FTD-3-336003: No buffers available for bytes byte packet
- %FTD-3-336004: Negative refcount in pakdesc pakdesc.
- %FTD-3-336005: Flow control error, error, on interface_name.
- %FTD-3-336006: num peers exist on IIDB interface_name.
- %FTD-3-336007: Anchor count negative
- %FTD-3-336008: Lingering DRDB deleting IIDB, dest network, nexthop address (interface), origin origin_str
- %FTD-3-336009 ddb_name as_id: Internal Error
- %FTD-3-336012: Interface interface_names going down and neighbor_links links exist
- %FTD-3-336013: Route iproute, iproute_successors successors, db_successors rdbs
- %FTD-3-336014: "EIGRP_PDM_Process_name, event_log"
- %FTD-3-336015: Unable to open socket for AS as_number"
- %FTD-3-336016: Unknown timer type timer_type expiration
- %FTD-3-336018: process_name as_number: prefix_source threshold prefix level (prefix_threshold) reached
- %FTD-3-336019: process_name as_number: prefix_source prefix limit reached (prefix_threshold).
- %FTD-3-339006: Umbrella resolver *current resolver ipv46* is reachable, resuming Umbrella redirect.

重大度別システムヘルスおよびネットワーク診断メッセージリスト

- %FTD-3-339007: Umbrella resolver *current resolver ipv46* is unreachable, moving to fail-open. Starting probe to resolver.
- %FTD-3-339008: Umbrella resolver *current resolver ipv46* is unreachable, moving to fail-close.
- %FTD-3-340001: Loopback-proxy info: error_string context id context_id, context type = version/request_type/address_type client socket (internal)= client_address_internal/client_port_internal server socket (internal)= server_address_internal/server_port_internal server socket (external)= server_address_external/server_port_external remote socket (external)= remote_address_external/remote_port_external
- %FTD-3-341003: Policy Agent failed to start for VNMC vnmc_ip_addr
- %FTD-3-341004: Storage device not available: Attempt to shutdown module %s failed.
- %FTD-3-341005: Storage device not available. Shutdown issued for module %s.
- %FTD-3-341006: Storage device not available. Failed to stop recovery of module *%s*.
- %FTD-3-341007: Storage device not available. Further recovery of module *%s* was stopped. 終了するまでに数分かかる場合があります。
- %FTD-3-341008: Storage device not found. Auto-boot of module %s cancelled. Install drive and reload to try again.
- %FTD-3-341011: Storage device with serial number ser_no in bay bay_no faulty.
- %FTD-3-402140: CRYPTO: RSA key generation error: modulus len len
- %FTD-3-402141: CRYPTO: Key zeroization error: key set type, reason reason
- %FTD-3-402142: CRYPTO: Bulk data op error: algorithm alg, mode mode
- %FTD-3-402143: CRYPTO: alg type key op
- %FTD-3-402144: CRYPTO: Digital signature error: signature algorithm sig, hash algorithm hash
- %FTD-3-402145: CRYPTO: Hash generation error: algorithm hash
- %FTD-3-402146: CRYPTO: Keyed hash generation error: algorithm hash, key len len
- %FTD-3-402147: CRYPTO: HMAC generation error: algorithm alg
- %FTD-3-402148: CRYPTO: Random Number Generator error
- %FTD-3-402149: CRYPTO: weak encryption type (length). Operation disallowed. Not FIPS 140-2 compliant
- %FTD-3-402150: CRYPTO: Deprecated hash algorithm used for RSA operation (hash alg). Operation disallowed. Not FIPS 140-2 compliant
- %FTD-3-403501: PPPoE - Bad host-unique in PADO - packet dropped. Intf:interface_name AC:ac_name
- %FTD-3-403502: PPPoE - Bad host-unique in PADS - dropping packet. Intf:interface_name AC:ac_name
- %FTD-3-403503: PPPoE:PPP link down:reason
- %FTD-3-403504: PPPoE:No vpdn group group_name for PPPoE is created

重大度別システムヘルスおよびネットワーク診断メッセージリスト

- %FTD-3-403507: PPPoE:PPPoE client on interface interface failed to locate PPPoE vpdn group group_name
- %FTD-3-414001: Failed to save logging buffer using file name filename to FTP server ftp_server_address on interface interface_name: [fail_reason]
- %FTD-3-414002: Failed to save logging buffer to flash:/syslog directory using file name: filename: [fail_reason]
- %FTD-3-414003: TCP Syslog Server intf: IP_Address/port not responding. New connections are [permitted|denied] based on logging permit-hostdown policy.
- %FTD-3-414005: TCP Syslog Server intf: IP_Address/port connected, New connections are permitted based on logging permit-hostdown policy
- %FTD-3-414006: TCP Syslog Server configured and logging queue is full. New connections denied based on logging permit-hostdown policy.
- %FTD-3-421001: TCP|UDP flow from interface_name:ip/port to interface_name:ip/port is dropped because application has failed.
- %FTD-3-421007: TCP|UDP flow from interface_name:IP_address/port to interface_name:IP_address/port is skipped because application has failed.
- %FTD-3-425006 Redundant interface redundant_interface_name switch active member to interface_name failed.
- %FTD-3-505016: Module module_id application changed from: name version version state state to: name version state state.
- %FTD-3-500005: connection terminated from in_ifc_name:src_adddress/src_port to out_ifc_name:dest_address/dest_port due to invalid combination of inspections on same flow. Inspect inspect_name is not compatible with inspect inspect_name_2
- %FTD-3-507003: The flow of type protocol from the originating interface: src_ip/src_port to dest_if:dest_ip/dest_port terminated by inspection engine, reason -
- %FTD-3-520001: error_string
- %FTD-3-520002: bad new ID table size
- %FTD-3-520003: bad id in error_string (id: 0xid_num)
- %FTD-3-520004: error_string
- %FTD-3-520005: error_string
- %FTD-3-520010: Bad queue elem – qelem_ptr: flink flink_ptr, blink blink_ptr, flink->blink flink_blink_ptr, blink->flink blink_flink_ptr
- %FTD-3-520011: Null queue elem
- %FTD-3-520013: Regular expression access check with bad list acl_ID
- %FTD-3-520020: No memory available
- %FTD-3-520021: Error deleting trie entry, error_message
- %FTD-3-520022: "Error adding mask entry, error_message

重大度別システムヘルスおよびネットワーク診断メッセージリスト

- %FTD-3-520023: Invalid pointer to head of tree, 0x<radix_node_ptr>
- %FTD-3-520024: Orphaned mask #radix_mask_ptr, refcount= radix_mask_ptr ‘s ref count at # radix_node_address, next=# radix_node_next
- %Threat Defense-3-520025: No memory for radix initialization: error_msg
- %Threat Defense-3-602305: IPSEC: SA creation error, source source address, destination destination address, reason error string
- %FTD-3-611313: VPN Client: Backup Server List Error: reason
- %FTD-3-613004: Internal error: memory allocation failure
- %FTD-3-613005: Flagged as being an ABR without a backbone area
- %FTD-3-613006: Reached unknown state in neighbor state machine
- %FTD-3-613007: area string lsid IP_address mask netmask type number
- %FTD-3-613008: if inside if_state number
- %FTD-3-613011: OSPF process number is changing router-id. Reconfigure virtual link neighbors with our new router-id
- %FTD-3-613013: OSPF LSID IP_address adv IP_address type number gateway IP_address metric number forwarding addr route IP_address /mask type number has no corresponding LSA
- %Threat Defense-3-613029: Router-ID IP_address is in use by ospf process number
- %Threat Defense-3-613016: Area string router-LSA of length number bytes plus update overhead bytes is too large to flood.
- %Threat Defense-3-613032: Init failed for interface inside, area is being deleted. 再度お試しください。
- %Threat Defense-3-613033: Interface inside is attached to more than one area
- %FTD-3-613034: Neighbor IP_address not configured
- %Threat Defense-3-613035: Could not allocate or find neighbor IP_address
- %Threat Defense-4-613015: Process 1 flushes LSA ID IP_address type-number adv-rtr IP_address in area mask.
- %FTD-3-710003: {TCP|UDP} access denied by ACL from source_IP/source_port to interface_name:dest_IP/service
- %FTD-3-713004: device scheduled for reboot or shutdown, IKE key acquire message on interface interface num, for Peer IP_address ignored
- %FTD-3-713008: Key ID in ID payload too big for pre-shared IKE tunnel
- %FTD-3-713009: OU in DN in ID payload too big for Certs IKE tunnel
- %FTD-3-713012: Unknown protocol (protocol). Not adding SA w/spi=SPI value
- %FTD-3-713014: Unknown Domain of Interpretation (DOI): DOI value
- %FTD-3-713016: Unknown identification type, Phase 1 or 2, Type ID_Type

重大度別システムヘルスおよびネットワーク診断メッセージリスト

- %FTD-3-713017: Identification type not supported, Phase 1 or 2, Type ID_Type
- %FTD-3-713018: Unknown ID type during find of group name for certs, Type ID_Type
- %FTD-3-713020: No Group found by matching OU(s) from ID payload: OU_value
- %FTD-3-713022: No Group found matching peer_ID or IP_address for Pre-shared key peer IP_address
- %FTD-3-713032: Received invalid local Proxy Range IP_address - IP_address
- %FTD-3-713033: Received invalid remote Proxy Range IP_address - IP_address
- %FTD-3-713042: IKE Initiator unable to find policy: Intf interface_number, Src: source_address, Dst: dest_address
- %FTD-3-713043: Cookie/peer address IP_address session already in progress
- %FTD-3-713048: Error processing payload: Payload ID: id
- %FTD-3-713056: Tunnel rejected: SA (SA_name) not found for group (group_name)!
- %FTD-3-713060: Tunnel Rejected: User (user) not member of group (group_name), group-lock check failed.
- %FTD-3-713061: Tunnel rejected: Crypto Map Policy not found for Src:source_address, Dst: dest_address!
- %FTD-3-713062: IKE Peer address same as our interface address IP_address
- %FTD-3-713063: IKE Peer address not configured for destination IP_address
- %FTD-3-713065: IKE Remote Peer did not negotiate the following: proposal attribute
- %FTD-3-713072: Password for user (user) too long, truncating to number characters
- %FTD-3-713081: Unsupported certificate encoding type encoding_type
- %FTD-3-713082: Failed to retrieve identity certificate
- %FTD-3-713083: Invalid certificate handle
- %FTD-3-713084: Received invalid phase 1 port value (port) in ID payload
- %FTD-3-713085: Received invalid phase 1 protocol (protocol) in ID payload
- %FTD-3-713086: Received unexpected Certificate payload Possible invalid Auth Method (Auth method (auth numerical value))
- %FTD-3-713088: Set Cert file handle failure: no IPSec SA in group group_name
- %FTD-3-713098: Aborting: No identity cert specified in IPSec SA (SA_name)!
- %FTD-3-713102: Phase 1 ID Data length number too long - reject tunnel!
- %FTD-3-713105: Zero length data in ID payload received during phase 1 or 2 processing
- %FTD-3-713107: IP_Address request attempt failed!
- %FTD-3-713109: Unable to process the received peer certificate
- %FTD-3-713112: Failed to process CONNECTED notify (SPI SPI_value)!

重大度別システムヘルスおよびネットワーク診断メッセージリスト

- %FTD-3-713014: Unknown Domain of Interpretation (DOI): DOI value
- %FTD-3-713016: Unknown identification type, Phase 1 or 2, Type ID_Type
- %FTD-3-713017: Identification type not supported, Phase 1 or 2, Type ID_Type
- %FTD-3-713118: Detected invalid Diffie-Helmann group_descriptor group_number, in IKE area
- %FTD-3-713122: Keep-alives configured keepalive_type but peer IP_address support keep-alives (type = keepalive_type)
- %FTD-3-713123: IKE lost contact with remote peer, deleting connection (keepalive type: keepalive_type)
- %FTD-3-713124: Received DPD sequence number rcv_sequence_# in DPD Action, description expected seq #
- %FTD-3-713127: Xauth required but selected Proposal does not support xauth, Check priorities of ike xauth proposals in ike proposal list
- %FTD-3-713129: Received unexpected Transaction Exchange payload type: payload_id
- %FTD-3-713132: Cannot obtain an IP_address for remote peer
- %FTD-3-713133: Mismatch: Overriding phase 2 DH Group(DH group DH group_id) with phase 1 group(DH group DH group_number
- %FTD-3-713134: Mismatch: P1 Authentication algorithm in the crypto map entry different from negotiated algorithm for the L2L connection
- %FTD-3-713138: Group group_name not found and BASE GROUP default preshared key not configured
- %FTD-3-713140: Split Tunneling Policy requires network list but none configured
- %FTD-3-713141: Client-reported firewall does not match configured firewall: action tunnel. Received -- Vendor: vendor(id), Product product(id), Caps: capability_value. Expected -- Vendor: vendor(id), Product: product(id), Caps: capability_value
- %FTD-3-713142: Client did not report firewall in use, but there is a configured firewall: action tunnel. Expected -- Vendor: vendor(id), Product product(id), Caps: capability_value
- %FTD-3-713146: Could not add route for Hardware Client in network extension mode, address: IP_address, mask: netmask
- %FTD-3-713149: Hardware client security attribute attribute_name was enabled but not requested.
- %FTD-3-713152: Unable to obtain any rules from filter ACL_tag to send to client for CPP, terminating connection.
- %FTD-3-713159: TCP Connection to Firewall Server has been lost, restricted tunnels are now allowed full network access
- %FTD-3-713161: Remote user (session Id - id) network access has been restricted by the Firewall Server
- %FTD-3-713162: Remote user (session Id - id) has been rejected by the Firewall Server
- %FTD-3-713163: Remote user (session Id - id) has been terminated by the Firewall Server

重大度別システムヘルスおよびネットワーク診断メッセージリスト

- %FTD-3-713165: Client IKE Auth mode differs from the group's configured Auth mode
- %FTD-3-713166: Headend security gateway has failed our user authentication attempt - check configured username and password
- %FTD-3-713167: Remote peer has failed user authentication - check configured username and password
- %FTD-3-713168: Re-auth enabled, but tunnel must be authenticated interactively!
- %FTD-3-713174: Hardware Client connection rejected! Network Extension Mode is not allowed for this group!
- %FTD-3-713182: IKE could not recognize the version of the client! IPSec Fragmentation Policy will be ignored for this connection!
- %FTD-3-713185: Error: Username too long - connection aborted
- %FTD-3-713186: Invalid secondary domain name list received from the authentication server. List Received: list_text Character index (value) is illegal
- %FTD-3-713189: Attempted to assign network or broadcast IP_address, removing (IP_address) from pool.
- %FTD-3-713191: Maximum concurrent IKE negotiations exceeded!
- %FTD-3-713193: Received packet with missing payload, Expected payload: payload_id
- %FTD-3-713194: Sending IKE|IPSec Delete With Reason message: termination_reason
- %FTD-3-713195: Tunnel rejected: Originate-Only: Cannot accept incoming tunnel yet!
- %FTD-3-713198: User Authorization failed: user User authorization failed.
- %FTD-3-713203: IKE Receiver: Error reading from socket.
- %FTD-3-713205: Could not add static route for client address: IP_address
- %FTD-3-713206: Tunnel Rejected: Conflicting protocols specified by tunnel-group and group-policy
- %FTD-3-713208: Cannot create dynamic rule for Backup L2L entry rule rule_id
- %FTD-3-713209: Cannot delete dynamic rule for Backup L2L entry rule id
- %FTD-3-713210: Cannot create dynamic map for Backup L2L entry rule_id
- %FTD-3-713212: Could not add route for L2L peer coming in on a dynamic map. address: IP_address, mask: netmask
- %FTD-3-713214: Could not delete route for L2L peer that came in on a dynamic map. address: IP_address, mask: netmask
- %FTD-3-713217: Skipping unrecognized rule: action: action client type: client_type client version: client_version
- %FTD-3-713218: Tunnel Rejected: Client Type or Version not allowed.
- %FTD-3-713226: Connection failed with peer IP_address, no trust-point defined in tunnel-group tunnel_group

重大度別システムヘルスおよびネットワーク診断メッセージリスト

- %FTD-3-713227: Rejecting new IPSec SA negotiation for peer Peer_address. A negotiation was already in progress for local Proxy Local_address/Local_netmask, remote Proxy Remote_address/Remote_netmask
- %FTD-3-713230: Internal Error, ike_lock trying to lock bit that is already locked for type type
- %FTD-3-713231: Internal Error, ike_lock trying to unlock bit that is not locked for type type
- %FTD-3-713232: SA lock refCnt = value, bitmask = hexvalue, p1_decrypt_cb = value, qm_decrypt_cb = value, qm_hash_cb = value, qm_spi_ok_cb = value, qm_dh_cb = value, qm_secret_key_cb = value, qm_encrypt_cb = value
- %FTD-3-713238: Invalid source proxy address: 0.0.0.0! Check private address on remote client
- %FTD-3-713258: IP = var1, Attempting to establish a phase2 tunnel on var2 interface but phase1 tunnel is on var3 interface. Tearing down old phase1 tunnel due to a potential routing change.
- %FTD-3-713254: Group = groupname, Username = username, IP = peerip, Invalid IPSec/UDP port = portnum, valid range is minport - maxport, except port 4500, which is reserved for IPSec/NAT-T
- %FTD-3-713260: Output interface %d to peer was not found
- %FTD-3-713261: IPV6 address on output interface %d was not found
- %FTD-3-713262: Rejecting new IPSec SA negotiation for peer Peer_address. A negotiation was already in progress for local Proxy Local_address/Local_prefix_len, remote Proxy Remote_address/Remote_prefix_len
- %FTD-3-713266: Could not add route for L2L peer coming in on a dynamic map. address: IP_address, mask: /prefix_len
- %FTD-3-713268: Could not delete route for L2L peer that came in on a dynamic map. address: IP_address, mask: /prefix_len
- %FTD-3-713270: Could not add route for Hardware Client in network extension mode, address: IP_addres>, mask: /prefix_len
- %FTD-3-713272: Terminating tunnel to Hardware Client in network extension mode, unable to delete static route for address: IP_address, mask: /prefix_len
- %FTD-3-713274: Could not delete static route for client address: IP_Address IP_Address address of client whose route is being removed
- %FTD-3-713902: Descriptive_event_string.
- %FTD-3-716056: Group group-name User user-name IP IP_address Authentication to SSO server name: name type type failed reason: reason
- %FTD-3-716057: Group group User user IP ip Session terminated, no type license available.
- %FTD-3-716061: Group DfltGrpPolicy User user IP ip addr IPv6 User Filter tempipv6 configured for AnyConnect. This setting has been deprecated, terminating connection
- %FTD-3-716158: Failed to create SAML logout request, initiated by SP. Reason: *reason*
- %FTD-3-716159: Failed to process SAML logout request, initiated by SP. Reason: *reason*
- %FTD-3-716160: Failed to create SAML authentication request. Reason: *reason*
- %FTD-3-716162: Failed to consume SAML assertion. Reason: *reason*

- %FTD-3-716600: Rejected size-recv KB Hostscan data from IP src-ip. Hostscan results exceed default | configured limit of size-conf KB.
- %FTD-3-716601: Rejected size-recv KB Hostscan data from IP src-ip. System-wide limit onthe amount of Hostscan data stored on ASA exceeds the limit of data-max KB.
- %FTD-3-716602: Memory allocation error. Rejected size-recv KB Hostscan data from IP src-ip.
- %FTD-3-717001: Querying keypair failed.
- %FTD-3-717002: Certificate enrollment failed for trustpoint trustpoint_name. Reason: reason_string.
- %FTD-3-717009: Certificate validation failed. Reason: reason_string.
- %FTD-3-717010: CRL polling failed for trustpoint trustpoint_name.
- %FTD-3-717012: Failed to refresh CRL cache entry from the server for trustpoint trustpoint_name at time_of_failure
- %FTD-3-717015: CRL received from issuer is too large to process (CRL size = crl_size, maximum CRL size = max_crl_size)
- %FTD-3-717017: Failed to query CA certificate for trustpoint trustpoint_name from enrollment_url
- %FTD-3-717018: CRL received from issuer has too many entries to process (number of entries = number_of_entries, maximum number allowed = max_allowed)
- %FTD-3-717019: Failed to insert CRL for trustpoint trustpoint_name. Reason: failure_reason.
- %FTD-3-717020: Failed to install device certificate for trustpoint label. Reason: reason string.
- %FTD-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.
- %FTD-3-717023: SSL failed to set device certificate for trustpoint trustpoint name. Reason: reason_string.
- %FTD-3-717027: Certificate chain failed validation. reason_string.
- %FTD-3-717032: OCSP status check failed. Reason: reason_string
- %FTD-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
- %FTD-3-717063: protocol Certificate enrollment failed for the trustpoint tpname with the CA ca
- %FTD-3-719002: Email Proxy session pointer from source_address has been terminated due to reason error.
- %FTD-3-719008: Email Proxy service is shutting down.
- %FTD-3-722007: Group group User user-name IP IP_address SVC Message: type-num/ERROR: message
- %FTD-3-722008: Group group User user-name IP IP_address SVC Message: type-num/ERROR: message
- %FTD-3-722009: Group group User user-name IP IP_address SVC Message: type-num/ERROR: message

重大度別システムヘルスおよびネットワーク診断メッセージリスト

- %FTD-3-722020: TunnelGroup tunnel_group GroupPolicy group_policy User user-name IP IP_address No address available for SVC connection
- %FTD-3-722035: Group group User user-name IP IP_address Received large packet length threshold num).
- %FTD-3-722036: Group group User user-name IP IP_address Transmitting large packet length (threshold num).
- %FTD-3-722045: Connection terminated: no SSL tunnel initialization data.
- %FTD-3-722046: Group group User user IP ip Session terminated: unable to establish tunnel.
- %FTD-3-725015 Error verifying client certificate. Public key size in client certificate exceeds the maximum supported key size.
- %FTD-3-734004: DAP: Processing error: internal error code
- %FTD-3-735010: IPMI: Environment Monitoring has failed to update one or more of its records.
- %FTD-3-737002: IPAA: Received unknown message 'num'
- %FTD-3-737027: IPAA: No data for address request
- %FTD-3-737202: VPNFIP: Pool=pool, ERROR: message
- %FTD-3-737403: POOLIP: Pool=pool, ERROR: message
- %FTD-3-742001: failed to read master key for password encryption from persistent store
- %FTD-3-742002: failed to set master key for password encryption
- %FTD-3-742003: failed to save master key for password encryption, reason reason_text
- %FTD-3-742004: failed to sync master key for password encryption, reason reason_text
- %FTD-3-742005: cipher text enc_pass is not compatible with the configured master key or the cipher text has been tampered with
- %FTD-3-742006: password decryption failed due to unavailable memory
- %FTD-3-742007: password encryption failed due to unavailable memory
- %FTD-3-742008: password enc_pass decryption failed due to decoding error
- %FTD-3-742009: password encryption failed due to decoding error
- %FTD-3-742010: encrypted password enc_pass is not well formed
- %FTD-3-743010: EOBC RPC server failed to start for client module client name.
- %FTD-3-743011: EOBC RPC call failed, return code code string.
- %FTD-3-746016: user-identity: DNS lookup failed, reason: reason.
- %FTD-3-747001: Clustering: Recovered from state machine event queue depleted. Event (event-id, ptr-in-hex, ptr-in-hex) dropped. Current state state-name, stack ptr-in-hex, ptr-in-hex, ptr-in-hex, ptr-in-hex, ptr-in-hex, ptr-in-hex
- %FTD-3-747010: Clustering: RPC call failed, message message-name, return code code-value.

- %FTD-3-747012: Clustering: Failed to replicate global object id hex-id-value in domain domain-name to peer unit-name, continuing operation.
- %FTD-3-747013: Clustering: Failed to remove global object id hex-id-value in domain domain-name from peer unit-name, continuing operation.
- %FTD-3-747014: Clustering: Failed to install global object id hex-id-value in domain domain-name, continuing operation.
- %FTD-3-747018: Clustering: State progression failed due to timeout in module module-name.
- %FTD-3-747021: Clustering: Master unit unit-name is quitting due to interface health check failure on failed-interface.
- %FTD-3-747022: Clustering: Asking slave unit unit-name to quit because it failed interface health check x times, rejoin will be attempted after y min. Failed interface: interface-name.
- %FTD-3-747030: Clustering: Asking slave unit unit-name to quit because it failed interface health check x times (last failure on interface-name), Clustering must be manually enabled on the unit to re-join.
- %FTD-3-747031: Clustering: Platform mismatch between cluster master (platform-type) and joining unit unit-name (platform-type). unit-name aborting cluster join.
- %FTD-3-747032: Clustering: Service module mismatch between cluster master (module-name) and joining unit unit-name (module-name) in slot slot-number. unit-name aborting cluster join.
- %FTD-3-747033: Clustering: Interface mismatch between cluster master and joining unit unit-name. unit-name aborting cluster join.
- %FTD-3-747042: Master receives config hash string request message from unknown member id <cluster-member-id>
- %FTD-3-747043: Get config hash string from master error: ret_code <ret_code>, string_len: <string_len>
- %FTD-3-748005: Failed to bundle the ports for module slot_number in chassis chassis_number; clustering is disabled
- %FTD-3-748006: Asking module slot_number in chassis chassis_number to leave the cluster due to a port bundling failure
- %FTD-3-750011: Tunnel Rejected: Selected IKEv2 encryption algorithm (IKEV2 encry algo) is not strong enough to secure proposed IPSEC encryption algorithm (IPSEC encry algo).
- %FTD-3-751001: Local: localIP:port Remote:remoteIP:port Username: username/group Failed to complete Diffie-Hellman operation. Error: error
- %FTD-3-751002: Local: localIP:port Remote:remoteIP:port Username: username/group No preshared key or trustpoint configured for self in tunnel group group
- %FTD-3-751004: Local: localIP:port Remote:remoteIP:port Username: username/group No remote authentication method configured for peer in tunnel group group
- %FTD-3-751005: Local: localIP:port Remote:remoteIP:port Username: username/group AnyConnect client reconnect authentication failed. Session ID: sessionID, Error: error

重大度別システムヘルスおよびネットワーク診断メッセージリスト

- %FTD-3-751006: Local: localIP:port Remote:remoteIP:port Username: username/group Certificate authentication failed. Error: error
- %FTD-3-751008: Local: localIP:port Remote:remoteIP:port Username: username/group Group=group, Tunnel rejected: IKEv2 not enabled in group policy
- %FTD-3-751009: Local: localIP:port Remote:remoteIP:port Username: username/group Unable to find tunnel group for peer.
- %FTD-3-751010: Local: localIP:port Remote:remoteIP:port Username: username/group Unable to determine self-authentication method. No crypto map setting or tunnel group found.
- %FTD-3-751011: Local: localIP:port Remote:remoteIP:port Username: username/group Failed user authentication. Error: error
- %FTD-3-751012: Local: localIP:port Remote:remoteIP:port Username: username/group Failure occurred during Configuration Mode processing. Error: error
- %FTD-3-751013: Local: localIP:port Remote:remoteIP:port Username: username/group Failed to process Configuration Payload request for attribute attribute ID. Error: error
- %FTD-3-751017: Local: localIP:port Remote remoteIP:port Username: username/group Configuration Error error description
- %FTD-3-751018: Terminating the VPN connection attempt from landing group. Reason: This connection is group locked to locked group.
- %FTD-3-751020: Local:%A:%u Remote:%A:%u Username:%s An %s remote access connection failed. Attempting to use an NSA Suite B crypto algorithm (%s) without an AnyConnect Premium license.
- %FTD-3-751022: Local: local-ip Remote: remote-ip Username:username Tunnel rejected: Crypto Map Policy not found for remote traffic selector rem-ts-start/rem-ts-end/rem-ts.startport/rem-ts.endport/rem-ts.protocol local traffic selector local-ts-start/local-ts-end/local-ts.startport/local-ts.endport/local-ts.protocol!
- %FTD-3-751024: Local:ip addr Remote:ip addr Username:username IKEv2 IPv6 User Filter tempipv6 configured. This setting has been deprecated, terminating connection
- %FTD-3-752006: Tunnel Manager failed to dispatch a KEY_ACQUIRE message. Probable mis-configuration of the crypto map or tunnel-group. Map Tag = Tag. Map Sequence Number = num, SRC Addr: address port: port Dst Addr: address port: port.
- %FTD-3-752007: Tunnel Manager failed to dispatch a KEY_ACQUIRE message. Entry already in Tunnel Manager. Map Tag = mapTag. Map Sequence Number = mapSeq.
- %FTD-3-752015: Tunnel Manager has failed to establish an L2L SA. All configured IKE versions failed to establish the tunnel. Map Tag = mapTag. Map Sequence Number = mapSeq.
- %FTD-3-768001: QUOTA: resource utilization is high: requested req, current curr, warning level level
- %FTD-3-768002: QUOTA: resource quota exceeded: requested req, current curr, limit limit
- %FTD-3-768003: QUOTA: management session quota exceeded for user *user name*: current 3, user limit 3

- %FTD-3-768004: QUOTA: management session quota exceeded for *ssh/telnet/http* protocol: current 2, protocol limit 2
- %FTD-3-769006: UPDATE: ASA boot system image image_name was not found on disk
- %FTD-3-772002: PASSWORD: console login warning, user username, cause: password expired
- %FTD-3-772004: PASSWORD: session login failed, user username, IP ip, cause: password expired
- %FTD-3-776202: CTS PAC for Server IP_address, A-ID PAC issuer name has expired
- %FTD-3-776254: CTS SGT-MAP: Binding manager unable to action binding binding IP - SGname (SGT) from source name .
- %FTD-3-779003: STS: Failed to read tag-switching table - reason
- %FTD-3-779004: STS: Failed to write tag-switching table - reason
- %FTD-3-779005: STS: Failed to parse tag-switching request from http - reason
- %FTD-3-779006: STS: Failed to save tag-switching table to flash - reason
- %FTD-3-779007: STS: Failed to replicate tag-switching table to peer - reason
- %FTD-3-840001: Failed to create the backup for an IKEv2 session <Local IP>, <Remote IP>
- %FTD-3-850001: SNORT ID (<snort-instance-id>/<snort-process-id>) Automatic-Application-Bypass due to delay of <delay>ms (threshold <AAB-threshold>ms) with <connection-info>
- %FTD-3-850002: SNORT ID (<snort-instance-id>/<snort-process-id>) Automatic-Application-Bypass due to SNORT not responding to traffics for <timeout-delay>ms(threshold <AAB-threshold>ms)
- %FTD-3-8300003: Failed to send session redistribution message to <variable 1>
- %FTD-3-8300005: Failed to receive session move response from <variable 1>

警告メッセージ、重大度 4

次のメッセージが重大度 4（警告）で表示されます。

- %Threat Defense-4-106023: Deny protocol src [interface_name:source_address/source_port] [([idfw_user|FQDN_string], sg_info)] dst interface_name:dest_address/dest_port [([idfw_user|FQDN_string], sg_info)] [type {string}, code {code}] by access_group acl_ID [0x8ed66b60, 0xf8852875]
- %Threat Defense-4-106027: Deny src [source address] dst [destination address] by access-group “access-list name”.
- %Threat Defense-4-106103: access-list acl_ID denied protocol for user username interface_name/source_address source_port interface_name/dest_address dest_port hit-cnt number first hit hash codes
- %Threat Defense-4-109027: [aaa protocol] Unable to decipher response message Server = server_IP_address, User = user
- %Threat Defense-4-109030: Autodetect ACL convert wildcard did not convert ACL access_list source | dest netmask netmask.

重大度別システムヘルスおよびネットワーク診断メッセージリスト

- %Threat Defense-4-109033: Authentication failed for admin user user from src_IP. Interactive challenge processing is not supported for protocol connections
- %Threat Defense-4-109034: Authentication failed for network user user from src_IP/port to dst_IP/port. Interactive challenge processing is not supported for protocol connections
- %Threat Defense-4-109102: Received CoA action-type from coa-source-ip, but cannot find named session audit-session-id
- %Threat Defense-4-113019: Group = group, Username = user, IP = peer_address, Session disconnected. Session Type: type, Duration: duration, Bytes xmt: count, Bytes rcv: count, Reason: reason
- %Threat Defense-4-113026: Error error while executing Lua script for group tunnel group
- %Threat Defense-4-113029: Group group User user IP ipaddr Session could not be established: session limit of num reached
- %Threat Defense-4-113030: Group group User user IP ipaddr User ACL acl from AAA doesn't exist on the device, terminating connection.
- %Threat Defense-4-113031: Group group User user IP ipaddr AnyConnect vpn-filter filter is an IPv6 ACL; ACL not applied.
- %Threat Defense-4-113032: Group group User user IP ipaddr AnyConnect ipv6-vpn-filter filter is an IPv4 ACL; ACL not applied.
- %Threat Defense-4-113034: Group group User user IP ipaddr User ACL acl from AAA ignored, AV-PAIR ACL used instead.
- %Threat Defense-4-113035: Group group User user IP ipaddr Session terminated: AnyConnect not enabled or invalid AnyConnect image on the ASA.
- %Threat Defense-4-113036: Group group User user IP ipaddr AAA parameter name value invalid.
- %Threat Defense-4-113038: Group group User user IP ipaddr Unable to create AnyConnect p0arent session.
- %Threat Defense-4-113040: Terminating the VPN connection attempt from attempted group. Reason: This connection is group locked to locked group.
- %Threat Defense-4-113041: Redirect ACL configured for assigned IP does not exist on the device.
- %Threat Defense-4-113042: CoA: Non-HTTP connection from src_if:src_ip/src_port to dest_if:dest_ip/dest_port for user username at client_IP denied by redirect filter; only HTTP connections are supported for redirection.
- %Threat Defense-4-115002: Warning in process: process name fiber: fiber name, component: component name, subcomponent: subcomponent name, file: filename, line: line number, cond: condition
- %Threat Defense-4-199016: syslog
- %Threat Defense-4-209003: Fragment database limit of number exceeded: src = source_address, dest = dest_address, proto = protocol, id = number
- %Threat Defense-4-209004: Invalid IP fragment, size = bytes exceeds maximum size = bytes: src = source_address, dest = dest_address, proto = protocol, id = number

重大度別システムヘルスおよびネットワーク診断メッセージリスト

- %Threat Defense-4-209005: Discard IP fragment set with more than number elements: src = Too many elements are in a fragment set.
- %Threat Defense-4-209006: Fragment queue threshold exceeded, dropped TCP fragment from IP address/port to IP address/port on outside interface.
- %Threat Defense-4-216004: prevented: error in function at file(line) - stack trace
- %Threat Defense-4-302034: Unable to pre-allocate H323 GUP Connection for faddr interface: foreign address/foreign-port to laddr interface:local-address/local-port
- %Threat Defense-4-302311: Failed to create a new [protocol] connection from [ingress interface]:[source IP]/[source port] to [egress interface]:[destination IP]/[destination port] due to application cache memory allocation failure. The app-cache memory threshold level is [threshold%] and threshold check is [enabled/disabled].
- %Threat Defense-4-308002: static global_address inside_address netmask netmask overlapped with global_address inside_address
- %Threat Defense-4-313004: Denied ICMP type=icmp_type, from source_address on interface interface_name to dest_address:no matching session
- %Threat Defense-4-313005: No matching connection for ICMP error message: icmp_msg_info on interface_name interface. Original IP payload: embedded_frame_info icmp_msg_info = icmp src src_interface_name:src_address [([idfw_user | FQDN_string], sg_info)] dst dest_interface_name:dest_address [([idfw_user | FQDN_string], sg_info)] (type icmp_type, code icmp_code) embedded_frame_info = prot src source_address/source_port [([idfw_user | FQDN_string], sg_info)] dst dest_address/dest_port [(idfw_user|FQDN_string), sg_info]
- %Threat Defense-4-313009: Denied invalid ICMP code icmp-code, for src-ifc:src-address/src-port (mapped-src-address/mapped-src-port) to dest-ifc:dest-address/dest-port (mapped-dest-address/mapped-dest-port) [user], ICMP id icmp-id, ICMP type icmp-type
- %Threat Defense-4-325002: Duplicate address ipv6_address/MAC_address on interface
- %Threat Defense-4-337005: Phone Proxy SRTP: Media session not found for media_term_ip/media_term_port for packet from in_ifc:src_ip/src_port to out_ifc:dest_ip/dest_port
- %Threat Defense-4-338101: Dynamic filter action whitelisted protocol traffic from in_interface:src_ip_addr/src_port (mapped-ip/mapped-port) to out_interface:dest_ip_addr/dest_port, (mapped-ip/mapped-port), source malicious address resolved from local or dynamic list: domain name
- %Threat Defense-4-338102: Dynamic filter action whitelisted protocol traffic from in_interface:src_ip_addr/src_port (mapped-ip/mapped-port) to out_interface:dest_ip_addr/dest_port (mapped-ip/mapped-port), destination malicious address resolved from local or dynamic list: domain name
- %Threat Defense-4-338103: Dynamic filter action whitelisted protocol traffic from in_interface:src_ip_addr/src_port (mapped-ip/mapped-port) to out_interface:dest_ip_addr/dest_port, (mapped-ip/mapped-port), source malicious address resolved
- %Threat Defense-4-338104: Dynamic filter action whitelisted protocol traffic from in_interface:src_ip_addr/src_port (mapped-ip/mapped-port) to out_interface:dest_ip_addr/dest_port (mapped-ip/mapped-port), destination malicious address resolved from local or dynamic list: ip address/netmask from local or dynamic list: ip address/netmask

重大度別システムヘルスおよびネットワーク診断メッセージリスト

- %Threat Defense-4-338301: Intercepted DNS reply for domain name from in_interface:src_ip_addr/src_port to out_interface:dest_ip_addr/dest_port, matched list
- %Threat Defense-4-401001: Shuns cleared
- %Threat Defense-4-401002: Shun added: IP_address IP_address port port
- %Threat Defense-4-401003: Shun deleted: IP_address
- %Threat Defense-4-401004: Shunned packet: IP_address = IP_address on interface interface_name
- %Threat Defense-4-401005: Shun add failed: unable to allocate resources for IP_address IP_address port port
- %Threat Defense-4-402114: IPSEC: Received an protocol packet (SPI=spi, sequence number= seq_num) from remote_IP to local_IP with an invalid SPI.
- %Threat Defense-4-402115: IPSEC: Received a packet from remote_IP to local_IP containing act_prot data instead of exp_prot data.
- %Threat Defense-4-402116: IPSEC: Received an protocol packet (SPI=spi, sequence number= seq_num) from remote_IP (username) to local_IP. The decapsulated inner packet doesn't match the negotiated policy in the SA. The packet specifies its destination as pkt_daddr, its source as pkt_saddr, and its protocol as pkt_prot. The SA specifies its local proxy as id_daddr /id_dmask /id_dprot /id_dport and its remote proxy as id_saddr /id_smask /id_sprot /id_sport.
- %Threat Defense-4-402117: IPSEC: Received a non-IPSec (protocol) packet from remote_IP to local_IP.
- %Threat Defense-4-402118: IPSEC: Received an protocol packet (SPI=spi, sequence number seq_num) from remote_IP (username) to local_IP containing an illegal IP fragment of length frag_len with offset frag_offset.
- %Threat Defense-4-402119: IPSEC: Received an protocol packet (SPI=spi, sequence number= seq_num) from remote_IP (username) to local_IP that failed anti-replay checking.
- %Threat Defense-4-402120: IPSEC: Received an protocol packet (SPI=spi, sequence number= seq_num) from remote_IP (username) to local_IP that failed authentication.
- %Threat Defense-4-402121: IPSEC: Received an protocol packet (SPI=spi, sequence number= seq_num) from peer_addr (username) to lcl_addr that was dropped by IPSec (drop_reason).
- %Threat Defense-4-402122: Received a cleartext packet from src_addr to dest_addr that was to be encapsulated in IPSec that was dropped by IPSec (drop_reason).
- %Threat Defense-4-402123: CRYPTO: The accel_type hardware accelerator encountered an error (code= error_string) while executing crypto command command.
- %Threat Defense-4-402124: CRYPTO: The ASA hardware accelerator encountered an error (Hardware error address, Core, Hardware error code, IstatReg, PciErrReg, CoreErrStat, CoreErrAddr, Doorbell Size,DoorBell Outstanding, SWReset).
- %Threat Defense-4-402125: The ASA hardware accelerator ring timed out (parameters).
- %Threat Defense-4-402126: CRYPTO: The ASA created Crypto Archive File Archive Filename as a Soft Reset was necessary. Please forward this archived information to Cisco.

重大度別システムヘルスおよびネットワーク診断メッセージリスト

- %Threat Defense-4-402127: CRYPTO: The ASA is skipping the writing of latest Crypto Archive File as the maximum # of files, max_number, allowed have been written to archive_directory. Please archive & remove files from Archive Directory if you want more Crypto Archive Files saved.
- %Threat Defense-4-402131: CRYPTO: status changing the accel_instance hardware accelerator's configuration bias from old_config_bias to new_config_bias.
- %Threat Defense-4-403505: PPPoE:PPP - Unable to set default route to IP_address at interface_name
- %Threat Defense-4-403506: PPPoE:failed to assign PPP IP_address netmask netmask at interface_name
- %Threat Defense-4-405001: Received ARP {request | response} collision from IP_address/MAC_address on interface interface_name to IP_address/MAC_address on interface interface_name
- %Threat Defense-4-405002: Received mac mismatch collision from IP_address/MAC_address for authenticated host
- %Threat Defense-4-405003: IP address collision detected between host IP_address at MAC_address and interface interface_name, MAC_address.
- %Threat Defense-4-405101: Unable to Pre-allocate H225 Call Signalling Connection for foreign_address outside_address[/outside_port] to local_address inside_address[/inside_port]
- %Threat Defense-4-405102: Unable to Pre-allocate H245 Connection for foreign_address outside_address[/outside_port] to local_address inside_address[/inside_port]
- %Threat Defense-4-405103: H225 message from source_address/source_port to dest_address/dest_port contains bad protocol discriminator hex
- %Threat Defense-4-405104: H225 message received from outside_address/outside_port to inside_address/inside_port before SETUP
- %Threat Defense-4-405105: H323 RAS message AdmissionConfirm received from source_address/source_port to dest_address/dest_port without an AdmissionRequest
- %Threat Defense-4-406001: FTP port command low port: IP_address/port to IP_address on interface interface_name
- %Threat Defense-4-406002: FTP port command different address: IP_address(IP_address) to IP_address on interface interface_name
- %Threat Defense-4-407001: Deny traffic for local-host interface_name:inside_address, license limit of number exceeded
- %Threat Defense-4-407002: Embryonic limit nconns/elimit for through connections exceeded.outside_address/outside_port to global_address (inside_address)/inside_port on interface interface_name
- %Threat Defense-4-407003: Established limit for RPC services exceeded number
- %Threat Defense-4-408001: IP route counter negative - reason, IP_address Attempt: number
- %Threat Defense-4-408002: ospf process id route type update address1 netmask1 [distance1/metric1] via source IP:interface1 address2 netmask2 [distance2/metric2] interface2
- %Threat Defense-4-408003: can't track this type of object hex

重大度別システムヘルスおよびネットワーク診断メッセージリスト

- %Threat Defense-4-408101: KEYMAN : Type <encrption_type> encryption unknown. Interpreting keystring as literal.
- %Threat Defense-4-408102: KEYMAN : Bad encrypted keystring for key id <key id>
- %Threat Defense-4-409001: Database scanner: external LSA IP_address netmask is lost, reinstalls
- %Threat Defense-4-409002: db_free: external LSA IP_address netmask
- %Threat Defense-4-409003: Received invalid packet: reason from IP_address, interface_name
- %Threat Defense-4-409004: Received reason from unknown neighbor IP_address
- %Threat Defense-4-409005: Invalid length number in OSPF packet from IP_address (ID IP_address), interface_name
- %Threat Defense-4-409006: Invalid lsa: reason Type number, LSID IP_address from IP_address, IP_address, interface_name
- %Threat Defense-4-409007: Found LSA with the same host bit set but using different mask LSA ID IP_address netmask New: Destination IP_address netmask
- %Threat Defense-4-409008: Found generating default LSA with non-zero mask LSA type : number Mask: netmask metric: number area: string
- %Threat Defense-4-409009: OSPF process number cannot start. There must be at least one up IP interface, for OSPF to use as router ID
- %Threat Defense-4-409010: Virtual link information found in non-backbone area: string
- %Threat Defense-4-409011: OSPF detected duplicate router-id IP_address from IP_address on interface interface_name
- %Threat Defense-4-409012: Detected router with duplicate router ID IP_address in area string
- %Threat Defense-4-409013: Detected router with duplicate router ID IP_address in Type-4 LSA advertised by IP_address
- %Threat Defense-4-409014: No valid authentication *send* key is available on interface *nameif*.
- %Threat Defense-4-409015: Key ID *key-id received* on interface *nameif*.
- %Threat Defense-4-409016: Key chain name *key-chain-name* on *nameif* is invalid.
- %Threat Defense-4-409017: Key ID *key-id* in key chain *key-chain-name* is invalid.
- %Threat Defense-4-409023: Attempting AAA Fallback method method_name for request_type request for user user:Auth-server group server_tag unreachable
- %Threat Defense-4-409101: Received invalid packet: %s from %P, %s
- %Threat Defense-4-409102: Received packet with incorrect area from %P, %s, area %AREA_ID_STR, packet area %AREA_ID_STR
- %Threat Defense-4-409103: Received %s from unknown neighbor %i
- %Threat Defense-4-409104: Invalid length %d in OSPF packet type %d from %P (ID %i), %s
- %Threat Defense-4-409105: Invalid lsa: %s: Type 0x%x, Length 0x%x, LSID %u from %i

重大度別システムヘルスおよびネットワーク診断メッセージリスト

- %Threat Defense-4-409106: Found generating default LSA with non-zero mask LSA type: 0x%x Mask: %i metric: %lu area: %AREA_ID_STR
- %Threat Defense-4-409107: OSPFv3 process %d could not pick a router-id, please configure manually
- %Threat Defense-4-409108: Virtual link information found in non-backbone area: %AREA_ID_STR
- %Threat Defense-4-409109: OSPF detected duplicate router-id %i from %P on interface %IF_NAME
- %Threat Defense-4-409110: Detected router with duplicate router ID %i in area %AREA_ID_STR
- %Threat Defense-4-409111: Multiple interfaces (%IF_NAME /%IF_NAME) on a single link detected.
- %Threat Defense-4-409112: Packet not written to the output queue
- %Threat Defense-4-409113: Doubly linked list linkage is NULL
- %Threat Defense-4-409114: Doubly linked list prev linkage is NULL %x
- %Threat Defense-4-409115: Unrecognized timer %d in OSPF %s
- %Threat Defense-4-409116: Error for timer %d in OSPF process %s
- %Threat Defense-4-409117: Can't find LSA database type %x, area %AREA_ID_STR, interface %x
- %Threat Defense-4-409118: Could not allocate DBD packet
- %Threat Defense-4-409119: Invalid build flag %x for LSA %i, type 0x%x
- %Threat Defense-4-409120: Router-ID %i is in use by ospf process %d
- %Threat Defense-4-409121: Router is currently an ASBR while having only one area which is a stub area
- %Threat Defense-4-409122: Could not select a global IPv6 address. Virtual links require at least one global IPv6 address.
- %Threat Defense-4-409123: Neighbor command allowed only on NBMA networks
- %Threat Defense-4-409125: Can not use configured neighbor: poll and priority options are allowed only for a NBMA network
- %Threat Defense-4-409128: OSPFv3-%d Area %AREA_ID_STR: Router %i originating invalid type 0x%x LSA, ID %u, Metric %d on Link ID %d Link Type %d
- %Threat Defense-4-410001: UDP DNS request from source_interface:source_address/source_port to dest_interface:dest_address/dest_port; (label length | domain-name length) 52 bytes exceeds remaining packet length of 44 bytes.
- %Threat Defense-4-411001: Line protocol on interface interface_name changed state to up
- %Threat Defense-4-411002: Line protocol on interface interface_name changed state to down
- %Threat Defense-4-411003: Configuration status on interface interface_name changed state to downup
- %Threat Defense-4-411004: Configuration status on interface interface_name changed state to up
- %Threat Defense-4-411005: Interface variable 1 experienced a hardware transmit hang. The interface has been reset.
- %Threat Defense-4-412001: MAC MAC_address moved from interface_1 to interface_2

重大度別システムヘルスおよびネットワーク診断メッセージリスト

- %Threat Defense-4-412002: Detected bridge table full while inserting MAC MAC_address on interface interface. Number of entries = num
- %Threat Defense-4-413001: Module module_id is not able to shut down. Module Error: errnum message
- %Threat Defense-4-413002: Module module_id is not able to reload. Module Error: errnum message
- %Threat Defense-4-413003: Module module_id is not a recognized type
- %Threat Defense-4-413004: Module module_id failed to write software vnewver (currently vver), reason. Trying again.
- %Threat Defense-4-413005: Module module_id, application is not supported app_name version app_vers type app_type
- %Threat Defense-4-413006: prod-id Module software version mismatch; slot slot is prod-id version running-vers. Slot slot prod-id requires required-vers.
- %Threat Defense-4-415016: policy-map map_name:Maximum number of unanswered HTTP requests exceeded connection_action from int_type:IP_address/port_num to int_type:IP_address/port_num
- %Threat Defense-4-417001: Unexpected event received: number
- %Threat Defense-4-417004: Filter violation error: conn number (string:string) in string
- %Threat Defense-4-417006: No memory for string) in string. Handling: string
- %Threat Defense-4-418001: Through-the-device packet to/from management-only network is denied: protocol_string from interface_name IP_address (port) [([idfw_user|FQDN_string], sg_info)] to interface_name IP_address (port) [(idfw_user|FQDN_string), sg_info]
- %Threat Defense-4-419001: Dropping TCP packet from src_ifc:src_IP/src_port to dest_ifc:dest_IP/dest_port, reason: MSS exceeded, MSS size, data size
- %Threat Defense-4-419002: Received duplicate TCP SYN from in_interface:src_address/src_port to out_interface:dest_address/dest_port with different initial sequence number.
- %Threat Defense-4-419003: Cleared TCP urgent flag from out_ifc:src_ip/src_port to in_ifc:dest_ip/dest_port.
- %Threat Defense-4-422004: IP SLA Monitor number0: Duplicate event received. Event number number1
- %Threat Defense-4-422005: IP SLA Monitor Probe(s) could not be scheduled because clock is not set.
- %Threat Defense-4-422006: IP SLA Monitor Probe number: string
- %Threat Defense-4-424001: Packet denied protocol_string intf_in:src_ip/src_port [([idfw_user | FQDN_string], sg_info)] intf_out:dst_ip/dst_port[([idfw_user | FQDN_string], sg_info)]. [Ingress|Egress] interface is in a backup state.
- %Threat Defense-4-424002: Connection to the backup interface is denied: protocol_string intf:src_ip/src_port intf:dst_ip/dst_port
- %Threat Defense-4-426004: PORT-CHANNEL: Interface ifc_name1 is not compatible with ifc_name and will be suspended (speed of ifc_name1 is X Mbps, Y is 1000 Mbps).

重大度別システムヘルスおよびネットワーク診断メッセージリスト

- %Threat Defense-4-429008: Unable to respond to VPN query from CX for session 0x%x. Reason %s
- %Threat Defense-4-434001: SFR card not up and fail-close mode used, dropping protocol packet from ingress interface:source IP address/source port to egress interface:destination IP address/destination port
- %Threat Defense-4-434007: SFR redirect will override Scansafe redirect for flow from ingress interface:source IP address/source port to egress interface:destination IP address/destination port (user)
- %Threat Defense-4-446003: Denied TLS Proxy session from src_int:src_ip/src_port to dst_int:dst_ip/dst_port, UC-IME license is disabled.
- %Threat Defense-4-447001: ASP DP to CP queue_name was full. Queue length length, limit limit
- %Threat Defense-4-448001: Denied SRTP crypto session setup on flow from src_int:src_ip/src_port to dst_int:dst_ip/dst_port, licensed K8 SRTP crypto session of limit exceeded
- %Threat Defense-4-500004: Invalid transport field for protocol=protocol, from source_address/source_port to dest_address/dest_port
- %Threat Defense-4-507002: Data copy in proxy-mode exceeded the buffer limit
- %Threat Defense-4-603110: Failed to establish L2TP session, tunnel_id = tunnel_id, remote_peer_ip = peer_ip, user = username. Multiple sessions per tunnel are not supported
- %Threat Defense-4-604105: DHCPD: Unable to send DHCP reply to client hardware_address on interface interface_name. Reply exceeds options field size (options_field_size) by number_of_octets octets.
- %Threat Defense-4-608002: Dropping Skinny message for in_ifc:src_ip/src_port to out_ifc:dest_ip/dest_port, SCCPPrefix length value too small
- %Threat Defense-4-608003: Dropping Skinny message for in_ifc:src_ip/src_port to out_ifc:dest_ip/dest_port, SCCPPrefix length value too large
- %Threat Defense-4-612002: Auto Update failed:filename, version:number, reason:reason
- %Threat Defense-4-612003: Auto Update failed to contact:url, reason:reason
- %Threat Defense-4-613017: Bad LSA mask: Type number, LSID IP_address Mask mask from IP_address
- %Threat Defense-4-613018: Maximum number of non self-generated LSA has been exceeded “OSPF number” - number LSAs
- %Threat Defense-4-613019: Threshold for maximum number of non self-generated LSA has been reached "OSPF number" - number LSAs
- %Threat Defense-4-613021: Packet not written to the output queue
- %Threat Defense-4-613022: Doubly linked list linkage is NULL
- %Threat Defense-4-613023: Doubly linked list prev linkage is NULL number
- %Threat Defense-4-613024: Unrecognized timer number in OSPF string
- %Threat Defense-4-613025: Invalid build flag number for LSA IP_address, type number

重大度別システムヘルスおよびネットワーク診断メッセージリスト

- %Threat Defense-4-613026: Can not allocate memory for area structure
- %Threat Defense-4-613030: Router is currently an ASBR while having only one area which is a stub area
- %Threat Defense-4-613031: No IP address for interface inside
- %Threat Defense-4-613036: Can not use configured neighbor: cost and database-filter options are allowed only for a point-to-multipoint network
- %Threat Defense-4-613037: Can not use configured neighbor: poll and priority options are allowed only for a NBMA network
- %Threat Defense-4-613038: Can not use configured neighbor: cost or database-filter option is required for point-to-multipoint broadcast network
- %Threat Defense-4-613039: Can not use configured neighbor: neighbor command is allowed only on NBMA and point-to-multipoint networks
- %Threat Defense-4-613040: OSPF-1 Area string: Router IP_address originating invalid type number LSA, ID IP_address, Metric number on Link ID IP_address Link Type number
- %Threat Defense-4-613042: OSPF process number lacks forwarding address for type 7 LSA IP_address in NSSA string - P-bit cleared
- %Threat Defense-4-620002: Unsupported CTIQBE version: hex: from interface_name:IP_address/port to interface_name:IP_address/port
- %FTD-4-769009: UPDATE: Image booted image_name is different from boot images.
- %Threat Defense-4-709008: (Primary | Secondary) Configuration sync in progress. Command: ‘command’ executed from (terminal/http) will not be replicated to or executed by the standby unit.
- %Threat Defense-4-709013: Failover configuration replication hash comparison timeout expired.
- %Threat Defense-4-711002: Task ran for elapsed_time msecs, process = process_name, PC = PC Tracebeback = traceback
- %Threat Defense-4-711004: Task ran for msec msec, Process = process_name, PC = pc, Call stack = call stack
- %Threat Defense-4-713154: DNS lookup for peer_description Server [server_name] failed!
- %Threat Defense-4-713157: Timed out on initial contact to server [server_name or IP_address] Tunnel could not be established.
- %Threat Defense-4-713239: IP_Address: Tunnel Rejected: The maximum tunnel count allowed has been reached
- %Threat Defense-4-713240: Received DH key with bad length: received length=rlength expected length=elength
- %Threat Defense-4-713241: IE Browser Proxy Method setting_number is Invalid
- %Threat Defense-4-713242: Remote user is authenticated using Hybrid Authentication. Not starting IKE rekey.
- %Threat Defense-4-713243: META-DATA Unable to find the requested certificate

重大度別システムヘルスおよびネットワーク診断メッセージリスト

- %Threat Defense-4-713244: META-DATA Received Legacy Authentication Method(LAM) type type is different from the last type received type.
- %Threat Defense-4-713245: META-DATA Unknown Legacy Authentication Method(LAM) type type received.
- %Threat Defense-4-713246: META-DATA Unknown Legacy Authentication Method(LAM) attribute type type received.
- %Threat Defense-4-713247: META-DATA Unexpected error: in Next Card Code mode while not doing SDI.
- %Threat Defense-5-713248: META-DATA Rekey initiation is being disabled during CRACK authentication.
- %Threat Defense-4-713249: META-DATA Received unsupported authentication results: result
- %Threat Defense-4-713251: META-DATA Received authentication failure message
- %Threat Defense-4-713255: IP = peer-IP, Received ISAKMP Aggressive Mode message 1 with unknown tunnel group name group-name
- %Threat Defense-4-713903: Group = group policy, Username = user name, IP = remote IP, ERROR: Failed to install Redirect URL: redirect URL Redirect ACL: non_exist for assigned IP.
- %Threat Defense-4-716007: Group group User user WebVPN Unable to create session.
- %Threat Defense-4-716022: Unable to connect to proxy server reason.
- %Threat Defense-4-716023: Group name User user Session could not be established: session limit of maximum_sessions reached.
- %Threat Defense-4-716044: Group group-name User user-name IP IP_address AAA parameter param-name value param-value out of range.
- %Threat Defense-4-716045: Group group-name User user-name IP IP_address AAA parameter param-name value invalid.
- %Threat Defense-4-716046: Group group-name-name User user-name IP IP_address User ACL access-list-name from AAA doesn't exist on the device, terminating connection.
- %Threat Defense-4-716047: Group group-name User user-name IP IP_address User ACL access-list from AAA ignored, AV-PAIR ACL used instead.
- %Threat Defense-4-716048: Group group-name User user-name IP IP_address No memory to parse ACL.
- %Threat Defense-4-716052: Group group-name User user-name IP IP_address Pending session terminated.
- %Threat Defense-4-717026: Name lookup failed for hostname hostname during PKI operation.
- %Threat Defense-4-717031: Failed to find a suitable trustpoint for the issuer: issuer Reason: reason_string
- %Threat Defense-4-717035: OCSP status is being checked for certificate. certificate_identifier.
- %Threat Defense-4-717037: Tunnel group search using certificate maps failed for peer certificate: certificate_identifier.

重大度別システムヘルスおよびネットワーク診断メッセージリスト

- %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
- %Threat Defense-4-720001: (VPN-unit) Failed to initialize with Chunk Manager.
- %Threat Defense-4-720007: (VPN-unit) Failed to allocate chunk from Chunk Manager.
- %Threat Defense-4-720008: (VPN-unit) Failed to register to High Availability Framework.
- %Threat Defense-4-720009: (VPN-unit) Failed to create version control block.
- %Threat Defense-4-720011: (VPN-unit) Failed to allocate memory
- %Threat Defense-4-720013: (VPN-unit) Failed to insert certificate in trust point trustpoint_name
- %Threat Defense-4-720022: (VPN-unit) Cannot find trust point trustpoint
- %Threat Defense-4-720033: (VPN-unit) Failed to queue add to message queue.
- %Threat Defense-4-720038: (VPN-unit) Corrupted message from active unit.
- %Threat Defense-4-720043: (VPN-unit) Failed to send type message id to standby unit
- %Threat Defense-4-720044: (VPN-unit) Failed to receive message from active unit
- %Threat Defense-4-720047: (VPN-unit) Failed to sync SDI node secret file for server IP_address on the standby unit.
- %Threat Defense-4-720051: (VPN-unit) Failed to add new SDI node secret file for server id on the standby unit.
- %Threat Defense-4-720052: (VPN-unit) Failed to delete SDI node secret file for server id on the standby unit.
- %Threat Defense-4-720053: (VPN-unit) Failed to add cTCP IKE rule during bulk sync, peer=IP_address, port=port
- %Threat Defense-4-720054: (VPN-unit) Failed to add new cTCP record, peer=IP_address, port=port.
- %Threat Defense-4-720055: (VPN-unit) VPN Stateful failover can only be run in single/non-transparent mode.
- %Threat Defense-4-720064: (VPN-unit) Failed to update cTCP database record for peer=IP_address, port=port during bulk sync.
- %Threat Defense-4-720065: (VPN-unit) Failed to add new cTCP IKE rule, peer=peer, port=port.
- %Threat Defense-4-720066: (VPN-unit) Failed to activate IKE database.
- %Threat Defense-4-720067: (VPN-unit) Failed to deactivate IKE database.
- %Threat Defense-4-720068: (VPN-unit) Failed to parse peer message.
- %Threat Defense-4-720069: (VPN-unit) Failed to activate cTCP database.
- %Threat Defense-4-720070: (VPN-unit) Failed to deactivate cTCP database.
- %Threat Defense-4-720073: VPN Session failed to replicate - ACL acl_name not found
- %Threat Defense-4-721007: (device) Fail to update access list list_name on standby unit.

重大度別システムヘルスおよびネットワーク診断メッセージリスト

- %Threat Defense-4-721011: (device) Fail to add access list rule list_name, line line_no on standby unit.
- %Threat Defense-4-721013: (device) Fail to enable APCF XML file file_name on the standby unit.
- %Threat Defense-4-721015: (device) Fail to disable APCF XML file file_name on the standby unit.
- %Threat Defense-4-721017: (device) Fail to create WebVPN session for user user_name, IP ip_address.
- %Threat Defense-4-721019: (device) Fail to delete WebVPN session for client user user_name, IP ip_address.
- %Threat Defense-4-722001: IP IP_address Error parsing SVC connect request.
- %Threat Defense-4-722002: IP IP_address Error consolidating SVC connect request.
- %Threat Defense-4-722003: IP IP_address Error authenticating SVC connect request.
- %Threat Defense-4-722004: Group group User user-name IP IP_address Error responding to SVC connect request.
- %Threat Defense-4-722015: Group group User user-name IP IP_address Unknown SVC frame type: type-num
- %Threat Defense-4-722016: Group group User user-name IP IP_address Bad SVC frame length: length expected: expected-length
- %Threat Defense-4-722017: Group group User user-name IP IP_address Bad SVC framing: 525446, reserved: 0
- %Threat Defense-4-722018: Group group User user-name IP IP_address Bad SVC protocol version: version, expected: expected-version
- %Threat Defense-4-722019: Group group User user-name IP IP_address Not enough data for an SVC header: length
- %Threat Defense-4-722041: TunnelGroup tunnel_group GroupPolicy group_policy User username IP peer_address No IPv6 address available for SVC connection
- %Threat Defense-4-722042: Group group User user IP ip Invalid Cisco SSL Tunneling Protocol version.
- %Threat Defense-4-722047: Group group User user IP ip Tunnel terminated: SVC not enabled or invalid SVC image on the ASA.
- %Threat Defense-4-722048: Group group User user IP ip Tunnel terminated: SVC not enabled for the user.
- %Threat Defense-4-722049: Group group User user IP ip Session terminated: SVC not enabled or invalid image on the ASA.
- %Threat Defense-4-722050: Group group User user IP ip Session terminated: SVC not enabled for the user.
- %Threat Defense-4-722054: Group group policy User user name IP remote IP SVC terminating connection: Failed to install Redirect URL: redirect URL Redirect ACL: non_exist for assigned IP
- %Threat Defense-4-724001: Group group-name User user-name IP IP_address WebVPN session not allowed. Unable to determine if Cisco Secure Desktop was running on the client's workstation.

重大度別システムヘルスおよびネットワーク診断メッセージリスト

- %Threat Defense-4-724002: Group group-name User user-name IP IP_address WebVPN session not terminated. Cisco Secure Desktop was not running on the client's workstation.
- %Threat Defense-4-733100: Object drop rate rate_ID exceeded. Current burst rate is rate_val per second, max configured rate is rate_val; Current average rate is rate_val per second, max configured rate is rate_val; Cumulative total count is total_cnt
- %Threat Defense-4-733101: Object objectIP (is targeted|is attacking). Current burst rate is rate_val per second, max configured rate is rate_val; Current average rate is rate_val per second, max configured rate is rate_val; Cumulative total count is total_cnt.
- %Threat Defense-4-733102: Threat-detection adds host %I to shun list
- %Threat Defense-4-733103: Threat-detection removes host %I from shun list
- %Threat Defense-4-733104: TD_SYSLOG_TCP_INTERCEPT_AVERAGE_RATE_EXCEED
- %Threat Defense-4-733105: TD_SYSLOG_TCP_INTERCEPT_BURST_RATE_EXCEED
- %Threat Defense-4-735015: CPU var1: Temp: var2 var3, Warm
- %Threat Defense-4-735016: Chassis Ambient var1: Temp: var2 var3, Warm
- %Threat Defense-4-735018: Power Supply var1: Temp: var2 var3, Critical
- %Threat Defense-4-735019: Power Supply var1: Temp: var2 var3, Warm
- %Threat Defense-4-735026: CPU cpu_num Voltage Regulator is running beyond the max thermal operating temperature and the device will be shutting down immediately. The chassis and CPU need to be inspected immediately for ventilation issues.
- %Threat Defense-4-737012: IPAA: Address assignment failed
- %Threat Defense-4-737013: IPAA: Error freeing address ip-address, not found
- %Threat Defense-4-737019: IPAA: Unable to get address from group-policy or tunnel-group local pools
- %Threat Defense-4-737028: IPAA: Adding ip-address to standby: failed
- %Threat Defense-4-737030: IPAA: Adding %m to standby: address already in use
- %Threat Defense-4-737032: IPAA: Removing ip-address from standby: not found
- %Threat Defense-4-737033: IPAA: Unable to assign addr_allocator provided IP address ip_addr to client. This IP address has already been assigned by previous_addr_allocator
- %FTD-4-737038: IPAA: Session=session, specified address ip-address was in-use, trying to get another.
- %FTD-4-737203: VPNFIP: Pool=pool, WARN: message
- %FTD-4-737402: POOLIP: Pool=pool, Failed to return ip-address to pool (recycle=recycle). Reason: message
- %FTD-4-737404: POOLIP: Pool=pool, WARN: message
- %Threat Defense-4-741005: Coredump operation variable 1 failed with error variable 2 variable 3
- %Threat Defense-4-741006: Unable to write Coredump Helper configuration, reason variable 1

重大度別システムヘルスおよびネットワーク診断メッセージリスト

- %Threat Defense-4-747008: Clustering: New cluster member name with serial number serial-number-A rejected due to name conflict with existing unit with serial number serial-number-B.
- %Threat Defense-4-747015: Clustering: Forcing stray member unit-name to leave the cluster.
- %Threat Defense-4-747016: Clustering: Found a split cluster with both unit-name-A and unit-name-B as master units. Master role retained by unit-name-A, unit-name-B will leave, then join as a slave.
- %Threat Defense-4-747017: Clustering: Failed to enroll unit unit-name due to maximum member limit limit-value reached.
- %Threat Defense-4-747019: Clustering: New cluster member name rejected due to Cluster Control Link IP subnet mismatch (ip-address/ip-mask on new unit, ip-address/ip-mask on local unit).
- %Threat Defense-4-747020: Clustering: New cluster member unit-name rejected due to encryption license mismatch.
- %Threat Defense-4-747025: Clustering: New cluster member unit-name rejected due to firewall mode mismatch.
- %Threat Defense-4-747026: Clustering: New cluster member unit-name rejected due to cluster interface name mismatch (ifc-name on new unit, ifc-name on local unit).
- %Threat Defense-4-747027: Clustering: Failed to enroll unit unit-name due to insufficient size of cluster pool pool-name in context-name.
- %Threat Defense-4-747028: Clustering: New cluster member unit-name rejected due to interface mode mismatch (mode-name on new unit, mode-name on local unit).
- %Threat Defense-4-747029: Clustering: Unit unit-name is quitting due to Cluster Control Link down.
- %Threat Defense-4-748002: Clustering configuration on the chassis is missing or incomplete; clustering is disabled
- %Threat Defense-4-748003: Module slot_number in chassis chassis_number is leaving the cluster due to a chassis health check failure
- %Threat Defense-4-748011: Mismatched resource profile size with Master. Master: <cores number> CPU cores / <RAM size> MB RAM, Mine: <cores number> CPU cores / <RAM size> MB RAM
- %Threat Defense-4-748012: Mismatched module type with Master. Master: <PID>, MINE: <PID>
- %Threat Defense-4-750003: Local: local IP:local port Remote: remote IP:remote port Username: username Negotiation aborted due to ERROR: error
- %Threat Defense-4-750012: Selected IKEv2 encryption algorithm (IKEV2 encry algo) is not strong enough to secure proposed IPSEC encryption algorithm (IPSEC encry algo).
- %Threat Defense-4-750014: Local:<self ip>:<self port> Remote:<peer ip>:<peer port> Username:<TG or Username> IKEv2 Session aborted. Reason: Initial Contact received for Local ID: <self ID>, Remote ID: <peer ID> from remote peer:<peer ip>:<peer port> to <self ip>:<self port>
- %Threat Defense-4-751014: Local: localIP:port Remote remoteIP:port Username: username/group Warning Configuration Payload request for attribute attribute ID could not be processed. Error: error
- %Threat Defense-4-751015: Local: localIP:port Remote remoteIP:port Username: username/group SA request rejected by CAC. Reason: reason

- %Threat Defense-4-751016: Local: localIP:port Remote remoteIP:port Username: username/group L2L peer initiated a tunnel with the same outer and inner addresses. Peer could be Originate only - Possible misconfiguration!
- %Threat Defense-4-751019: Local:LocalAddr Remote:RemoteAddr Username:username Failed to obtain an licenseType license. Maximum license limit limit exceeded.
- %Threat Defense-4-751021: Local:variable 1:variable 2 Remote:variable 3:variable 4 Username:variable 5 variable 6 with variable 7 encryption is not supported with this version of the AnyConnect Client. Please upgrade to the latest Anyconnect Client.
- %Threat Defense-4-751027: Local:local IP:local port Remote:peer IP:peer port Username:username IKEv2 Received INVALID_SELECTORS Notification from peer. Peer received a packet (SPI=spi). The decapsulated inner packet didn’t match the negotiated policy in the SA. Packet destination pkt_daddr, port pkt_dest_port, source pkt_saddr, port pkt_src_port, protocol pkt_prot.
- %Threat Defense-4-752009: IKEv2 Doesn't support Multiple Peers
- %Threat Defense-4-752010: IKEv2 Doesn't have a proposal specified
- %Threat Defense-4-752011: IKEv1 Doesn't have a transform set specified
- %Threat Defense-4-752012: IKEv protocol was unsuccessful at setting up a tunnel. Map Tag = mapTag. Map Sequence Number = mapSeq.
- %Threat Defense-4-752013: Tunnel Manager dispatching a KEY_ACQUIRE message to IKEv2 after a failed attempt. Map Tag = mapTag. Map Sequence Number = mapSeq.
- %Threat Defense-4-752014: Tunnel Manager dispatching a KEY_ACQUIRE message to IKEv1 after a failed attempt. Map Tag = mapTag. Map Sequence Number = mapSeq.
- %Threat Defense-4-752017: IKEv2 Backup L2L tunnel initiation denied on interface interface matching crypto map name, sequence number number. Unsupported configuration.
- %Threat Defense-4-753001: Unexpected IKEv2 packet received from <IP>:<port>. Error: <reason>
- %Threat Defense-4-768003: SSH: connection timed out: username username, IP ip
- %Threat Defense-4-769009: UPDATE: Image booted image_name is different from boot images.
- %Threat Defense-4-770001: Resource resource allocation is more than the permitted list of limit for this platform. If this condition persists, the ASA will be rebooted.
- %Threat Defense-4-770003: Resource resource allocation is less than the minimum requirement of value for this platform. If this condition persists, performance will be lower than normal.
- %Threat Defense-4-775002: Reason - protocol connection conn_id from interface_name:real_address/real_port [(idfw_user)] to interface_name:real_address/real_port is action locally
- %Threat Defense-4-802006: IP ip_address MDM request details has been rejected: details.

通知メッセージ、重大度 5

次のメッセージが重大度 5（通知）で表示されます。

重大度別システムヘルスおよびネットワーク診断メッセージリスト

- %FTD-5-106029: New reverse carrier <protocol> <ingress_ifc>:<source_addr> to <egress_ifc>:<destination_addr> overshadows existing <ingress_ifc2>:<source_addr2> to <egress_ifc2>:<destination_addr2>
- %FTD-5-109012: Authen Session End: user 'user', sid number, elapsed number seconds
- %FTD-5-109029: Parsing downloaded ACL: string
- %FTD-5-109039: AAA Authentication:Dropping an unsupported IPv6/IP46/IP64 packet from lifc:laddr to fifc:faddr
- %FTD-5-109201: UAUTH Session *session*, User *username*, Assigned IP *IP Address*, Succeeded adding entry.
- %FTD-5-109204: UAUTH Session *session*, User *username*, Assigned IP *IP Address*, Succeeded applying filter.
- %FTD-5-109207: UAUTH Session *session*, User *username*, Assigned IP *IP Address*, Succeeded updating entry.
- %FTD-5-109210: UAUTH Session *session*, User *username*, Assigned IP *IP Address*, Successfully removed the rules for user during tunnel torn down.
- %FTD-5-111001: Begin configuration: IP_address writing to device
- %FTD-5-111002: Begin configuration: IP_address reading from device
- %FTD-5-111003: IP_address Erase configuration
- %FTD-5-111004: IP_address end configuration: {FAILED|OK}
- %FTD-5-111005: IP_address end configuration: OK
- %FTD-5-111007: Begin configuration: IP_address reading from device.
- %FTD-5-111008: User user executed the command string
- %FTD-5-111010: User username, running application-name from IP ip addr, executed cmd
- %FTD-5-113024: Group tg: Authenticating type connection from ip with username, user_name, from client certificate
- %FTD-5-113025: Group tg: FAILED to extract username from certificate while authenticating type connection from ip
- %FTD-5-199001: Reload command executed from Telnet (remote IP_address).
- %FTD-5-199017: syslog
- %FTD-5-212009: Configuration request for SNMP group groupname failed. User username, reason.
- %FTD-5-303004: FTP cmd_string command unsupported - failed strict inspection, terminating connection from source_interface:source_address/source_port to dest_interface:dest_address/dest_interface
- %FTD-5-303005: Strict FTP inspection matched match_string in policy-map policy-name, action_string from src_ifc:sip/sport to dest_ifc:dip/dport

重大度別システムヘルスおよびネットワーク診断メッセージリスト

- %FTD-5-305013: Asymmetric NAT rules matched for forward and reverse flows; Connection protocol src interface_name:source_address/source_port [(idfw_user)] dst interface_name:dest_address/dst_port [(idfw_user)] denied due to NAT reverse path failure.
- %FTD-5-321001: Resource var1 limit of var2 reached.
- %FTD-5-321002: Resource var1 rate limit of var2 reached.
- %FTD-5-331002: Dynamic DNS type RR for ('fqdn_name' - ip_address | ip_address - 'fqdn_name') successfully updated in DNS server dns_server_ip
- %FTD-5-332003: Web Cache IP_address/service_ID acquired
- %FTD-5-333002: Timeout waiting for EAP response - context:EAP-context
- %FTD-5-333010: EAP-SQ response Validation Flags TLV indicates PV request - context:EAP-context
- %FTD-5-334002: EAPoUDP association successfully established - host-address
- %FTD-5-334003: EAPoUDP association failed to establish - host-address
- %FTD-5-334005: Host put into NAC Hold state - host-address
- %FTD-5-334006: EAPoUDP failed to get a response from host - host-address
- %FTD-5-336010 EIGRP-ddb_name tableid as_id: Neighbor address (%interface) is event_msg: msg
- %FTD-5-402128: CRYPTO: An attempt to allocate a large memory block failed, size: size, limit: limit
- %FTD-5-425005 Interface interface_name become active in redundant interface redundant_interface_name
- %FTD-5-4302310: SCTP packet received from src_ifc:src_ip/src_port to dst_ifc:dst_ip/dst_port contains unsupported Hostname Parameter.
- %FTD-5-434004: SFR requested ASA to bypass further packet redirection and process flow from %s:%A/%d to %s:%A/%d locally
- %FTD-5-500001: ActiveX content in java script is modified: src src ip dest dest ip on interface interface name
- %FTD-5-500002: Java content in java script is modified: src src ip dest dest ip on interface interface name
- %FTD-5-500003: Bad TCP hdr length (hdrlen=bytes, pktlen=bytes) from source_address/source_port to dest_address/dest_port, flags: tcp_flags, on interface interface_name
- %FTD-5-501101: User transitioning priv level
- %FTD-5-502101: New user added to local dbase: Uname: user Priv: privilege_level Encpass: string
- %FTD-5-502102: User deleted from local dbase: Uname: user Priv: privilege_level Encpass: string
- %FTD-5-502103: User priv level changed: Uname: user From: privilege_level To: privilege_level
- %FTD-5-502111: New group policy added: name: policy_name Type: policy_type
- %FTD-5-502112: Group policy deleted: name: policy_name Type: policy_type
- %FTD-5-503001: Process number, Nbr IP_address on interface_name from string to string, reason

- %Threat Defense-5-503002: The last key has expired for interface *nameif*, packets sent using last valid key.
- %Threat Defense-5-503003: Packet *sent* | *received* on interface *nameif* with expired Key ID *key-id*.
- %Threat Defense-5-503004: Key ID *key-id* in key chain *key-chain-name* does not have a key.
- Threat Defense-5-503005: Key ID *key-id* in key chain *key-chain-name* does not have a cryptographic algorithm.
- %FTD-5-504001: Security context context_name was added to the system
- %FTD-5-504002: Security context context_name was removed from the system
- %FTD-5-505001: Module module_id is shutting down. Please wait...
- %FTD-5-505002: Module ips is reloading. Please wait...
- %FTD-5-505003: Module module_id is resetting. Please wait...
- %FTD-5-505004: Module module_id shutdown is complete.
- %FTD-5-505005: Module module_name is initializing control communication. Please wait...
- %FTD-5-505006: Module module_id is Up.
- %FTD-5-505007: Module module_id is recovering. Please wait...
- %FTD-5-505008: Module module_id software is being updated to vnewver (currently vver)
- %FTD-5-505009: Module module_id software was updated to vnewver (previously vver)
- %FTD-5-505010: Module in slot slot removed.
- %FTD-5-505012: Module module_id, application stopped application, version version
- %FTD-5-505013: Module module_id application changed from: application version version to: newapplication version newversion.
- %FTD-5-506001: event_source_string event_string
- %FTD-5-507001: Terminating TCP-Proxy connection from interface_inside:source_address/source_port to interface_outside:dest_address/dest_port - reassembly limit of limit bytes exceeded
- %FTD-5-509001: Connection attempt from src_intf:src_ip/src_port [([idfw_user | FQDN_string], sg_info)] to dst_intf:dst_ip/dst_port [([idfw_user | FQDN_string], sg_info)] was prevented by "no forward" command.
- %FTD-5-503101: Process %d, Nbr %i on %s from %s to %s, %s
- %FTD-5-611104: Serial console idle timeout exceeded
- %FTD-5-612001: Auto Update succeeded:filename, version:number
- %FTD-5-711005: Traceback: call_stack
- %FTD-5-713006: Failed to obtain state for message Id message_number, Peer Address: IP_address
- %FTD-5-713010: IKE area: failed to find centry for message Id message_number

重大度別システムヘルスおよびネットワーク診断メッセージリスト

- %FTD-5-713041: IKE Initiator: new or rekey Phase 1 or 2, Intf interface_number, IKE Peer IP_address local Proxy Address IP_address, remote Proxy Address IP_address, Crypto map (crypto map tag)
- %FTD-5-713049: Security negotiation complete for tunnel_type type (group_name) Initiator/Responder, Inbound SPI = SPI, Outbound SPI = SPI
- %FTD-5-713050: Connection terminated for peer IP_address. Reason: termination reason Remote Proxy IP_address, Local Proxy IP_address
- %FTD-5-713068: Received non-routine Notify message: notify_type (notify_value)
- %FTD-5-713073: Responder forcing change of Phase 1/Phase 2 rekeying duration from larger_value to smaller_value seconds
- %FTD-5-713074: Responder forcing change of IPSec rekeying duration from larger_value to smaller_value Kbs
- %FTD-5-713075: Overriding Initiator's IPSec rekeying duration from larger_value to smaller_value seconds
- %FTD-5-713076: Overriding Initiator's IPSec rekeying duration from larger_value to smaller_value Kbs
- %FTD-5-713092: Failure during phase 1 rekeying attempt due to collision
- %FTD-5-713115: Client rejected NAT enabled IPSec request, falling back to standard IPSec
- %FTD-5-713119: Group group IP ip PHASE 1 COMPLETED
- %FTD-5-713120: PHASE 2 COMPLETED (msgid=msg_id)
- %FTD-5-713130: Received unsupported transaction mode attribute: attribute id
- %FTD-5-713131: Received unknown transaction mode attribute: attribute_id
- %FTD-5-713135: message received, redirecting tunnel to IP_address.
- %FTD-5-713136: IKE session establishment timed out [IKE_state_name], aborting!
- %FTD-5-713137: Reaper overriding refCnt [ref_count] and tunnelCnt [tunnel_count] -- deleting SA!
- %FTD-5-713139: group_name not found, using BASE GROUP default preshared key
- %FTD-5-713144: Ignoring received malformed firewall record; reason - error_reason TLV type attribute_value correction
- %FTD-5-713148: Terminating tunnel to Hardware Client in network extension mode, unable to delete static route for address: IP_address, mask: netmask
- %FTD-5-713155: DNS lookup for Primary VPN Server [server_name] successfully resolved after a previous failure. Resetting any Backup Server init.
- %FTD-5-713156: Initializing Backup Server [server_name or IP_address]
- %FTD-5-713158: Client rejected NAT enabled IPSec Over UDP request, falling back to IPSec Over TCP
- %FTD-5-713178: IKE Initiator received a packet from its peer without a Responder cookie
- %FTD-5-713179: IKE AM Initiator received a packet from its peer without a payload_type payload

重大度別システムヘルスおよびネットワーク診断メッセージリスト

- %FTD-5-713196: Remote L2L Peer IP_address initiated a tunnel with same outer and inner addresses. Peer could be Originate Only - Possible misconfiguration!
- %FTD-5-713197: The configured Confidence Interval of number seconds is invalid for this tunnel_type connection. Enforcing the second default.
- %FTD-5-713199: Reaper corrected an SA that has not decremented the concurrent IKE negotiations counter (counter_value)!
- %FTD-5-713201: Duplicate Phase Phase packet detected. アクション
- %FTD-5-713216: Rule: action [Client type]: version Client: type version allowed/ not allowed
- %FTD-5-713229: Auto Update - Notification to client client_ip of update string: message_string.
- %FTD-5-713237: ACL update (access_list) received during re-key re-authentication will not be applied to the tunnel.
- %FTD-5-713248: META-DATA Rekey initiation is being disabled during CRACK authentication.
- %FTD-5-713250: META-DATA Received unknown Internal Address attribute: attribute
- %FTD-5-713252: Group = group, Username = user, IP = ip, Integrity Firewall Server is not available. VPN Tunnel creation rejected for client.
- %FTD-5-713253: Group = group, Username = user, IP = ip, Integrity Firewall Server is not available. Entering ALLOW mode. VPN Tunnel created for client.
- %FTD-5-713257: Phase *var1* failure: Mismatched attribute types for class *var2* : Rcv'd: *var3* Cfg'd: *var4*
- %FTD-5-713259: Group = groupname, Username = username, IP = peerIP, Session is being torn down. Reason: reason
- %FTD-5-713904: Descriptive_event_string.
- %FTD-5-716053: SAML Server added: name: name Type: SP
- %FTD-5-716054: SAML Server deleted: name: name Type: SP
- %FTD-5-717013: Removing a cached CRL to accommodate an incoming CRL. Issuer: issuer
- %FTD-5-717014: Unable to cache a CRL received from CDP due to size limitations (CRL size = size, available cache space = space)
- %FTD-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
- %FTD-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
- %FTD-5-717061: Starting protocol certificate enrollment for the trustpoint tpname with the CA ca_name. Request Type type Mode mode
- %FTD-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
- %FTD-5-717064: Keypair keyname in the trustpoint tpname is regenerated for mode protocol certificate renewal

重大度別システムヘルスおよびネットワーク診断メッセージリスト

- %FTD-5-718002: Create peer IP_address failure, already at maximum of number_of_peers
- %FTD-5-718005: Fail to send to IP_address, port port
- %FTD-5-718006: Invalid load balancing state transition [cur=state_number][event=event_number]
- %FTD-5-718007: Socket open failure failure_code
- %FTD-5-718008: Socket bind failure failure_code
- %FTD-5-718009: Send HELLO response failure to IP_address
- %FTD-5-718010: Sent HELLO response to IP_address
- %FTD-5-718011: Send HELLO request failure to IP_address
- %FTD-5-718012: Sent HELLO request to IP_address
- %FTD-5-718014: Master peer IP_address is not answering HELLO
- %FTD-5-718015: Received HELLO request from IP_address
- %FTD-5-718016: Received HELLO response from IP_address
- %FTD-5-718024: Send CFG UPDATE failure to IP_address
- %FTD-5-718028: Send OOS indicator failure to IP_address
- %FTD-5-718031: Received OOS obituary for IP_address
- %FTD-5-718032: Received OOS indicator from IP_address
- %FTD-5-718033: Send TOPOLOGY indicator failure to IP_address
- %FTD-5-718042: Unable to ARP for IP_address
- %FTD-5-718043: Updating/removing duplicate peer entry IP_address
- %FTD-5-718044: Deleted peer IP_address
- %FTD-5-718045: Created peer IP_address
- %FTD-5-718048: Create of secure tunnel failure for peer IP_address
- %FTD-5-718050: Delete of secure tunnel failure for peer IP_address
- %FTD-5-718052: Received GRAT-ARP from duplicate master MAC_address
- %FTD-5-718053: Detected duplicate master, mastership stolen MAC_address
- %FTD-5-718054: Detected duplicate master MAC_address and going to SLAVE
- %FTD-5-718055: Detected duplicate master MAC_address and staying MASTER
- %FTD-5-718057: Queue send failure from ISR, msg type failure_code
- %FTD-5-718060: Inbound socket select fail: context=context_ID.
- %FTD-5-718061: Inbound socket read fail: context=context_ID.
- %FTD-5-718062: Inbound thread is awake (context=context_ID).
- %FTD-5-718063: Interface interface_name is down.

重大度別システムヘルスおよびネットワーク診断メッセージリスト

- %FTD-5-718064: Admin. interface interface_name is down.
- %FTD-5-718065: Cannot continue to run (public=up/down, private=up/down, enable=LB_state, master=IP_address, session=Enable/Disable).
- %FTD-5-718066: Cannot add secondary address to interface interface_name, ip IP_address.
- %FTD-5-718067: Cannot delete secondary address to interface interface_name, ip IP_address.
- %FTD-5-718068: Start VPN Load Balancing in context context_ID.
- %FTD-5-718069: Stop VPN Load Balancing in context context_ID.
- %FTD-5-718070: Reset VPN Load Balancing in context context_ID.
- %FTD-5-718071: Terminate VPN Load Balancing in context context_ID.
- %FTD-5-718072: Becoming master of Load Balancing in context context_ID.
- %FTD-5-718073: Becoming slave of Load Balancing in context context_ID.
- %FTD-5-718074: Fail to create access list for peer context_ID.
- %FTD-5-718075: Peer IP_address access list not set.
- %FTD-5-718076: Fail to create tunnel group for peer IP_address.
- %FTD-5-718077: Fail to delete tunnel group for peer IP_address.
- %FTD-5-718078: Fail to create crypto map for peer IP_address.
- %FTD-5-718079: Fail to delete crypto map for peer IP_address.
- %FTD-5-718080: Fail to create crypto policy for peer IP_address.
- %FTD-5-718081: Fail to delete crypto policy for peer IP_address.
- %FTD-5-718082: Fail to create crypto ipsec for peer IP_address.
- %FTD-5-718083: Fail to delete crypto ipsec for peer IP_address.
- %FTD-5-718084: Public/cluster IP not on the same subnet: public IP_address, mask netmask, cluster IP_address
- %FTD-5-718085: Interface interface_name has no IP address defined.
- %FTD-5-718086: Fail to install LB NP rules: type rule_type, dst interface_name, port port.
- %FTD-5-718087: Fail to delete LB NP rules: type rule_type, rule rule_ID.
- %FTD-5-719014: Email Proxy is changing listen port from old_port to new_port for mail protocol protocol.
- %FTD-5-720016: (VPN-unit) Failed to initialize default timer #index.
- %FTD-5-720017: (VPN-unit) Failed to update LB runtime data
- %FTD-5-720018: (VPN-unit) Failed to get a buffer from the underlying core high availability subsystem. Error code code.
- %FTD-5-720019: (VPN-unit) Failed to update cTCP statistics.

重大度別システムヘルスおよびネットワーク診断メッセージリスト

- %FTD-5-720020: (VPN-unit) Failed to send type timer message.
- %FTD-5-720021: (VPN-unit) HA non-block send failed for peer msg message_number. HA error code.
- %FTD-5-720035: (VPN-unit) Fail to look up CTCP flow handle
- %FTD-5-720036: (VPN-unit) Failed to process state update message from the active peer.
- %FTD-5-720071: (VPN-unit) Failed to update cTCP dynamic data.
- %FTD-5-720072: Timeout waiting for Integrity Firewall Server [interface,ip] to become available.
- %FTD-5-722037: Group group User user-name IP IP_address SVC closing connection: reason.
- %FTD-5-722038: Group group-name User user-name IP IP_address SVC terminating session: reason.
- %FTD-5-722005: Group group User user-name IP IP_address Unable to update session information for SVC connection.
- %FTD-5-722006: Group group User user-name IP IP_address Invalid address IP_address assigned to SVC connection.
- %FTD-5-722010: Group group User user-name IP IP_address SVC Message: type-num/NOTICE: message
- %FTD-5-722011: Group group User user-name IP IP_address SVC Message: type-num/NOTICE: message
- %FTD-5-722012: Group group User user-name IP IP_address SVC Message: type-num/INFO: message
- %FTD-5-722028: Group group User user-name IP IP_address Stale SVC connection closed.
- %FTD-5-722032: Group group User user-name IP IP_address New SVC connection replacing old connection.
- %FTD-5-722033: Group group User user-name IP IP_address First SVC connection established for SVC session.
- %FTD-5-722034: Group group User user-name IP IP_address New SVC connection, no existing connection.
- %FTD-5-722037: Group group User user-name IP IP_address SVC closing connection: reason.
- %FTD-5-722038: Group group-name User user-name IP IP_address SVC terminating session: reason.
- %FTD-5-722043: Group group User user IP ip DTLS disabled: unable to negotiate cipher.
- %FTD-5-722044: Group group User user IP ip Unable to request ver address for SSL tunnel.
- %FTD-5-734002: DAP: User user, Addr ipaddr: Connection terminated by the following DAP records: DAP record names
- %FTD-5-737003: IPAA: DHCP configured, no viable servers found for tunnel-group 'tunnel-group'
- %FTD-5-737004: IPAA: DHCP configured, request failed for tunnel-group 'tunnel-group'
- %FTD-5-737007: IPAA: Local pool request failed for tunnel-group 'tunnel-group'
- %FTD-5-737008: IPAA: 'tunnel-group' not found

重大度別システムヘルスおよびネットワーク診断メッセージリスト

- %FTD-5-737011: IPAA: AAA assigned address ip-address, not permitted, retrying
- %FTD-5-737018: IPAA: DHCP request attempt num failed
- %FTD-5-737021: IPAA: Address from local pool (ip-address) duplicates address from DHCP
- %FTD-5-737022: IPAA: Address from local pool (ip-address) duplicates address from AAA
- %FTD-5-737023: IPAA: Unable to allocate memory to store local pool address ip-address
- %FTD-5-737024: IPAA: Local pool assignment failed for suggested IP ip-address, retrying
- %FTD-5-737025: IPAA: Not releasing local pool ip-address, due to local pool duplicate issue
- %FTD-5-737034: IPAA: Session=<session>, <IP version> address: <explanation>
- %FTD-5-737204: VPNFIP: Pool=pool, NOTIFY: message
- %FTD-5-737405: POOLIP: Pool=pool, NOTIFY: message
- %FTD-5-746014: user-identity: [FQDN] fqdn address IP Address obsolete.
- %FTD-5-746015: user-identity: [FQDN] fqdn resolved IP address.
- %FTD-5-747002: Clustering: Recovered from state machine dropped event (event-id, ptr-in-hex, ptr-in-hex). Intended state: state-name. Current state: state-name.
- %FTD-5-747003: Clustering: Recovered from state machine failure to process event (event-id, ptr-in-hex, ptr-in-hex) at state state-name.
- %FTD-5-747007: Clustering: Recovered from finding stray config sync thread, stack ptr-in-hex, ptr-in-hex, ptr-in-hex, ptr-in-hex, ptr-in-hex, ptr-in-hex.
- %FTD-5-748001: Module *slot_number* in chassis *chassis_number* is leaving the cluster due to a chassis configuration change
- %FTD-5-748004: Module *slot_number* in chassis *chassis_number* is re-joining the cluster due to a chassis health check recovery
- %FTD-5-750001: Local:local IP:local port Remote:remote IP: remote port Username: username Received request to request an IPsec tunnel; local traffic selector = local selectors: range, protocol, port range; remote traffic selector = remote selectors: range, protocol, port range
- %FTD-5-750002: Local:local IP:local port Remote: remote IP: remote port Username: username Received a IKE_INIT_SA request
- %FTD-5-750004: Local: local IP: local port Remote: remote IP: remote port Username: username Sending COOKIE challenge to throttle possible DoS
- %FTD-5-750005: Local: local IP: local port Remote: remote IP: remote port Username: username IPsec rekey collision detected. I am lowest nonce initiator, deleting SA with inbound SPI SPI
- %FTD-5-750006: Local: local IP: local port Remote: remote IP: remote port Username: username SA UP. Reason: reason
- %FTD-5-750007: Local: local IP: local port Remote: remote IP: remote port Username: username SA DOWN. Reason: reason
- %FTD-5-750008: Local: local IP: local port Remote: remote IP: remote port Username: username SA rejected due to system resource low

- %FTD-5-750009: Local: local IP: local port Remote: remote IP: remote port Username: username SA request rejected due to CAC limit reached: Rejection reason: reason
- %FTD-5-750010: Local: local-ip Remote: remote-ip Username:username IKEv2 local throttle-request queue depth threshold of threshold reached; increase the window size on peer peer for better performance
- %FTD-5-750013 - IKEv2 SA (iSPI <ISPI> rRSP <rSPI>) Peer Moved: Previous <prev_remote_ip>:<prev_remote_port>/<prev_local_ip>:<prev_local_port>. Updated <new_remote_ip>:<new_remote_port>/<new_local_ip>:<new_local_port>
- %FTD-5-751007: Local: localIP:port Remote:remoteIP:port Username: username/group Configured attribute not supported for IKEv2. Attribute: attribute
- %FTD-5-751025: Local: local IP:local port Remote: remote IP:remote port Username:username Group:group-policy IPv4 Address=assigned_IPv4_addr IPv6 address=assigned_IPv6_addr assigned to session.
- %FTD-5-752003: Tunnel Manager dispatching a KEY_ACQUIRE message to IKEv2. Map Tag = mapTag. Map Sequence Number = mapSeq.
- %FTD-5-752004: Tunnel Manager dispatching a KEY_ACQUIRE message to IKEv1. Map Tag = mapTag. Map Sequence Number = mapSeq.
- %FTD-5-752016: IKEv protocol was successful at setting up a tunnel. Map Tag = mapTag. Map Sequence Number = mapSeq.
- %FTD-5-769001: UPDATE: ASA image src was added to system boot list
- %FTD-5-769002: UPDATE: ASA image src was copied to dest
- %FTD-5-769003: UPDATE: ASA image src was renamed to dest
- %FTD-5-769004: UPDATE: ASA image src_file failed verification, reason: failure_reason
- %FTD-5-769005: UPDATE: ASA image image_name passed image verification
- %FTD-5-776252: CTS SGT-MAP: CTS SGT-MAP: Binding binding IP - SGname (SGT) from source name deleted from binding manager.
- %FTD-5-8300006: Cluster topology change detected. VPN session redistribution aborted.

情報メッセージ、重大度 6

次のメッセージが重大度 6（情報）で表示されます。

- %Threat Defense-6-106012: Deny IP from IP_address to IP_address, IP options hex.
- %Threat Defense-6-106015: Deny TCP (no connection) from IP_address/port to IP_address/port flags tcp_flags on interface interface_name.
- %Threat Defense-6-106100: access-list acl_ID {permitted | denied | est-allowed} protocol interface_name/source_address(source_port)(idfw_user, sg_info) interface_name/dest_address(dest_port) (idfw_user, sg_info) hit-cnt number ({first hit | number-second interval})

- %Threat Defense-6-106102: access-list acl_ID {permitted | denied} protocol for user username interface_name/source_address source_port interface_name/dest_address dest_port hit-cnt number {first hit | number-second interval} hash codes
- %Threat Defense-6-109036: Exceeded 1000 attribute values for the attribute name attribute for user username.
- %Threat Defense-6-109100: Received CoA update from *coa-source-ip* for user *username* , with session ID: *audit-session-id* , changing authorization attributes
- %Threat Defense-6-109101: Received CoA disconnect request from *coa-source-ip* for user *username* , with audit-session-id: *audit-session-id*
- %Threat Defense-6-109202: UAUTH Session *session*, User *username*, Assigned IP *IP Address*, Succeeded incrementing entry use.
- %Threat Defense-6-110002: Failed to locate egress interface for protocol from src interface:src IP/src port to dest IP/dest port
- %Threat Defense-6-110003: Routing failed to locate next-hop for protocol from src interface:src IP/src port to dest interface:dest IP/dest port
- %Threat Defense-6-110004: Egress interface changed from old_active_ifc to new_active_ifc on ip_protocol connection conn_id for outside_zone/parent_outside_ifc:outside_addr/outside_port (mapped_addr/mapped_port) to inside_zone/parent_inside_ifc:inside_addr/inside_port (mapped_addr/mapped_port)
- %Threat Defense-6-113003: AAA group policy for user user is being set to policy_name.
- %Threat Defense-6-113004: AAA user aaa_type Successful: server = server_IP_address, User = user
- %Threat Defense-6-113005: AAA user authentication Rejected: reason = string: server = server_IP_address, User = user: user IP = user_ip
- %Threat Defense-6-113006: User user locked out on exceeding number successive failed authentication attempts
- %Threat Defense-6-113007: User user unlocked by administrator
- %Threat Defense-6-113008: AAA transaction status ACCEPT: user = user
- %Threat Defense-6-113009: AAA retrieved default group policy policy for user user
- %Threat Defense-6-113010: AAA challenge received for user user from server server_IP_address
- %Threat Defense-6-113011: AAA retrieved user specific group policy policy for user user
- %Threat Defense-6-113012: AAA user authentication Successful: local database: user = user
- %Threat Defense-6-113013: AAA unable to complete the request Error: reason = reason: user = user
- %Threat Defense-6-113014: AAA authentication server not accessible: server = server_IP_address: user = user
- %Threat Defense-6-113015: AAA user authentication Rejected: reason = reason: local database: user = user: user IP =xxx.xxx.xxx.xxx
- %Threat Defense-6-113016: AAA credentials rejected: reason = reason: server = server_IP_address: user = user: user IP = xxx.xxx.xxx.xxx

重大度別システムヘルスおよびネットワーク診断メッセージリスト

- %Threat Defense-6-113017: AAA credentials rejected: reason = reason: local database: user = user: user IP = user_ip=xxx.xxx.xxx.xxx
- %Threat Defense-6-113033: Group group User user IP ipaddr AnyConnect session not allowed. ACL parse error.
- %Threat Defense-6-113037: Reboot pending, new sessions disabled. Denied user login.
- %Threat Defense-6-113039: Group group User user IP ipaddr AnyConnect parent session started.
- %Threat Defense-6-114004: 4GE SSM I/O Initialization start.
- %Threat Defense-6-114005: 4GE SSM I/O Initialization end.
- %Threat Defense-6-199002: startup completed. Beginning operation.
- %Threat Defense-6-199003: Reducing link MTU dec.
- %Threat Defense-6-199005: Startup begin
- %Threat Defense-6-199018: syslog
- %Threat Defense-6-201010: Embryonic connection limit exceeded econns/limit for dir packet from source_address/source_port to dest_address/dest_port on interface interface_name
- %Threat Defense-6-201012: Per-client embryonic connection limit exceeded curr num/limit for [input|output] packet from IP_address/ port to ip/port on interface interface_name
- %Threat Defense-6-210022: LU missed number updates
- %Threat Defense-6-302003: Built H245 connection for foreign_address outside_address/outside_port local_address inside_address/inside_port
- %Threat Defense-6-302004: Pre-allocate H323 UDP backconnection for foreign_address outside_address/outside_port to local_address inside_address/inside_port
- %Threat Defense-6-302010: connections in use, connections most used
- %Threat Defense-6-302012: Pre-allocate H225 Call Signalling Connection for faddr IP_address/port to laddr IP_address
- %Threat Defense-6-302013: Built {inbound|outbound} TCP connection_id for interface:real-address/real-port (mapped-address/mapped-port) [(idfw_user)] to interface:real-address/real-port (mapped-address/mapped-port) [(idfw_user)] [(user)]
- %Threat Defense-6-302014: Teardown TCP connection id for interface:real-address/real-port [(idfw_user)] to interface:real-address/real-port [(idfw_user)] duration hh:mm:ss bytes bytes [reason] [(user)]
- %Threat Defense-6-302015: Built {inbound|outbound} UDP connection number for interface_name:real_address/real_port (mapped_address/mapped_port) [(idfw_user)] to interface_name:real_address/real_port (mapped_address/mapped_port) [(idfw_user)] [(user)]
- %Threat Defense-6-302016: Teardown UDP connection number for interface:real-address/real-port [(idfw_user)] to interface:real-address/real-port [(idfw_user)] duration hh:mm:ss bytes bytes [(user)]
- %Threat Defense-6-302017: Built {inbound|outbound} GRE connection id from interface:real_address (translated_address) [(idfw_user)] to interface:real_address/real_cid (translated_address/translated_cid) [(idfw_user)] [(user)

- %Threat Defense-6-302018: Teardown GRE connection id from interface:real_address (translated_address) [(idfw_user)] to interface:real_address/real_cid (translated_address/translated_cid) [(idfw_user)] duration hh:mm:ss bytes bytes [(user)]
- %Threat Defense-6-302020: Built ICMP connection connection_id from interface:real-address/real-port (mapped-address/mapped-port) [(idfw_user)] to interface:real-address/real-port (mapped-address/mapped-port) [(idfw_user)] [(user)]
- %Threat Defense-6-302021: Teardown ICMP connection connection_id from interface:real-address/real-port (mapped-address/mapped-port) [(idfw_user)] to interface:real-address/real-port (mapped-address/mapped-port) [(idfw_user)] [(user)]
- %Threat Defense-6-302022: Built role stub TCP connection for interface:real-address/real-port (mapped-address/mapped-port) to interface:real-address/real-port (mapped-address/mapped-port)
- %Threat Defense-6-302023: Teardown stub TCP connection for interface:real-address/real-port to interface:real-address/real-port duration hh:mm:ss forwarded bytes bytes reason
- %Threat Defense-6-302024: Built role stub UDP connection for interface:real-address/real-port (mapped-address/mapped-port) to interface:real-address/real-port (mapped-address/mapped-port)
- %Threat Defense-6-302025: Teardown stub UDP connection for interface:real-address/real-port to interface:real-address/real-port duration hh:mm:ss forwarded bytes bytes reason
- %Threat Defense-6-302026: Built role stub ICMP connection for interface:real-address/real-port (mapped-address) to interface:real-address/real-port (mapped-address)
- %Threat Defense-6-302027: Teardown stub ICMP connection for interface:real-address/real-port to interface:real-address/real-port duration hh:mm:ss forwarded bytes bytes reason
- %Threat Defense-6-302033: Pre-allocated H323 GUP Connection for faddr interface:foreign address/foreign-port to laddr interface:local-address/local-port
- %Threat Defense-6-302303: Built TCP state-bypass connection conn_id from initiator_interface:real_ip/real_port(mapped_ip/mapped_port) to responder_interface:real_ip/real_port (mapped_ip/mapped_port)
- %Threat Defense-6-302304: Teardown TCP state-bypass connection conn_id from initiator_interface:ip/port to responder_interface:ip/port duration, bytes, teardown reason.
- %Threat Defense-6-303002: FTP connection from src_ifc:src_ip/src_port to dst_ifc:dst_ip/dst_port, user username action file filename
- %Threat Defense-6-305009: Built {dynamic|static} translation from interface_name [(acl-name)]:real_address [(idfw_user)] to interface_name:mapped_address
- %Threat Defense-6-305010: Teardown {dynamic|static} translation from interface_name:real_address [(idfw_user)] to interface_name:mapped_address duration time
- %Threat Defense-6-305011: Built {dynamic|static} {TCP|UDP|ICMP} translation from interface_name:real_address/real_port [(idfw_user)] to interface_name:mapped_address/mapped_port
- %Threat Defense-6-305012: Teardown {dynamic|static} {TCP|UDP|ICMP} translation from interface_name [(acl-name)]:real_address/{real_port|real_ICMP_ID} [(idfw_user)] to interface_name:mapped_address/{mapped_port|mapped_ICMP_ID} duration time
- %Threat Defense-6-305014: Allocated block of ports for translation from real_interface : real_host_ip /real_source_port to real_dest_interface :real_dest_ip /real_dest_port.

重大度別システムヘルスおよびネットワーク診断メッセージリスト

- %Threat Defense-6-305015: Released block of ports for translation from real_interface : real_host_ip /real_source_port to real_dest_interface :real_dest_ip /real_dest_port.
- %Threat Defense-6-308001: console enable password incorrect for number tries (from IP_address)
- %Threat Defense-6-311001: LU loading standby start
- %Threat Defense-6-311002: LU loading standby end
- %Threat Defense-6-311003: LU recv thread up
- %Threat Defense-6-311004: LU xmit thread up
- %Threat Defense-6-312001: RIP hdr failed from IP_address: cmd=string, version=number domain=string on interface interface_name
- %Threat Defense-6-314001: Pre-allocated RTSP UDP backconnection for src_intf:src_IP to dst_intf:dst_IP/dst_port.
- %Threat Defense-6-314002: RTSP failed to allocate UDP media connection from src_intf:src_IP to dst_intf:dst_IP/dst_port: reason_string.
- %Threat Defense-6-317007: Added route_type route dest_address netmask via gateway_address [distance/metric] on interface_name route_type
- %Threat Defense-6-317008: Deleted route_type route dest_address netmask via gateway_address [distance/metric] on interface_name route_type
- %Threat Defense-6-321003: Resource var1 log level of var2 reached.
- %Threat Defense-6-321004: Resource var1 rate log level of var2 reached
- %Threat Defense-6-322004: No management IP address configured for transparent firewall. Dropping protocol protocol packet from interface_in:source_address/source_port to interface_out:dest_address/dest_port
- %Threat Defense-6-333001: EAP association initiated - context:EAP-context
- %Threat Defense-6-333003: EAP association terminated - context:EAP-context
- %Threat Defense-6-333009: EAP-SQ response MAC TLV is invalid - context:EAP-context
- %Threat Defense-6-334001: EAPoUDP association initiated - host-address
- %Threat Defense-6-334004: Authentication request for NAC Clientless host - host-address
- %Threat Defense-6-334007: EAPoUDP association terminated - host-address
- %Threat Defense-6-334008: NAC EAP association initiated - host-address, EAP context:EAP-context
- %Threat Defense-6-334009: Audit request for NAC Clientless host - Assigned_IP.
- %Threat Defense-6-336011: event event
- %Threat Defense-6-337000: Created BFD session with local discriminator id on real_interface with neighbor real_host_ip.
- %Threat Defense-6-337001: Terminated BFD session with local discriminator id on real_interface with neighbor real_host_ip due to failure_reason.

- %Threat Defense-6-340002: Loopback-proxy info: error_string context id context_id, context type = version/request_type/address_type client socket (internal)= client_address_internal/client_port_internal server socket (internal)= server_address_internal/server_port_internal server socket (external)= server_address_external/server_port_external remote socket (external)= remote_address_external/remote_port_external
- %Threat Defense-6-341001: Policy Agent started successfully for VNMC vnmc_ip_addr
- %Threat Defense-6-341002: Policy Agent stopped successfully for VNMC vnmc_ip_add
- %Threat Defense-6-341010: Storage device with serial number ser_no [inserted into | removed from] bay bay_no
- %Threat Defense-6-402129: CRYPTO: An attempt to release a DMA memory block failed, location: address
- %Threat Defense-6-402130: CRYPTO: Received an ESP packet (SPI = xxxxxxxxxx, sequence number=xxxx) from 172.16.0.1 (user=user) to 192.168.0.2 with incorrect IPsec padding.
- %Threat Defense-6-403500: PPPoE - Service name 'any' not received in PADO. Intf:interface_name AC:ac_name.
- %FTD-6-419004: TCP connection <ID> from <src_ifc>:<src_ip>/<src_port> to <dst_ifc>:<dst_ip>/<dst_port> is probed by DCD
- %FTD-6-419005: TCP connection <ID> from <src_ifc>:<src_ip>/<src_port> to <dst_ifc>:<dst_ip>/<dst_port> duration <hh:mm:ss> data <bytes>, is kept open by DCD as valid connection
- %FTD-6-419006: Teardown TCP connection <ID> from <src_ifc>:<src_ip>/<src_port> to <dst_ifc>:<dst_ip>/<dst_port> duration<hh:mm:ss> data <bytes>, DCD probe was not responded from <client/server> interface <ifc_name>
- %Threat Defense-6-421006: There are number users of application accounted during the past 24 hours.
- %Threat Defense-6-425001 Redundant interface redundant_interface_name created.
- %Threat Defense-6-425002 Redundant interface redundant_interface_name removed.
- %Threat Defense-6-425003 Interface interface_name added into redundant interface redundant_interface_name.
- %Threat Defense-6-425004 Interface interface_name removed from redundant interface redundant_interface_name.
- %Threat Defense-6-426001: PORT-CHANNEL:Interface ifc_name bundled into EtherChannel interface Port-channel num
- %Threat Defense-6-426002: PORT-CHANNEL:Interface ifc_name unbundled from EtherChannel interface Port-channel num
- %Threat Defense-6-426003: PORT-CHANNEL:Interface ifc_name1 has become standby in EtherChannel interface Port-channel num
- %Threat Defense-6-426101: PORT-CHANNEL:Interface ifc_name is allowed to bundle into EtherChannel interface port-channel id by CLACP

重大度別システムヘルスおよびネットワーク診断メッセージリスト

- %Threat Defense-6-426102: PORT-CHANNEL:Interface ifc_name is moved to standby in EtherChannel interface port-channel id by CLACP
- %Threat Defense-6-426103: PORT-CHANNEL:Interface ifc_name is selected to move from standby to bundle in EtherChannel interface port-channel id by CLACP
- %Threat Defense-6-426104: PORT-CHANNEL:Interface ifc_name is unselected in EtherChannel interface port-channel id by CLACP
- %FTD-6-430001: *Intrusion event syslog*. 各フィールドの詳細については、セキュリティイベントの Syslog メッセージの ID （1 ページ）を参照してください。
- %FTD-6-430002: *Connection event logged at beginning of connection syslog*. 各フィールドの詳細については、セキュリティイベントの Syslog メッセージの ID （1 ページ）を参照してください。
- %FTD-6-430003: *Connection event logged at end of connection syslog*. 各フィールドの詳細については、セキュリティイベントの Syslog メッセージの ID （1 ページ）を参照してください。
- %FTD-6-430004: *File events syslog*. 各フィールドの詳細については、セキュリティイベントの Syslog メッセージの ID （1 ページ）を参照してください。
- %FTD-6-430005: *File malware events syslog*. 各フィールドの詳細については、セキュリティイベントの Syslog メッセージの ID （1 ページ）を参照してください。
- %FTD-6-430006: *File events from AMP for endpoints syslog*.
- %Threat Defense-6-602101: PMTU-D packet number bytes greater than effective mtu number dest_addr=dest_address, src_addr=source_address, prot=protocol
- %Threat Defense-6-602103: IPSEC: Received an ICMP Destination Unreachable from src_addr with suggested PMTU of rcvd_mtu; PMTU updated for SA with peer peer_addr, SPI spi, tunnel name username, old PMTU old_mtu, new PMTU new_mtu.
- %Threat Defense-6-602104: IPSEC: Received an ICMP Destination Unreachable from src_addr, PMTU is unchanged because suggested PMTU of rcvd_mtu is equal to or greater than the current PMTU of curr_mtu, for SA with peer peer_addr, SPI spi, tunnel name username.
- %Threat Defense-6-602303: IPSEC: An direction tunnel_type SA (SPI=spi) between local_IP and remote_IP (username) has been created.
- %Threat Defense-6-602304: IPSEC: An direction tunnel_type SA (SPI=spi) between local_IP and remote_IP (username) has been deleted.
- %Threat Defense-6-604101: DHCP client interface interface_name: Allocated ip = IP_address, mask = netmask, gw = gateway_address
- %Threat Defense-6-604102: DHCP client interface interface_name: address released
- %Threat Defense-6-604103: DHCP daemon interface interface_name: address granted MAC_address (IP_address)
- %Threat Defense-6-604104: DHCP daemon interface interface_name: address released build_name (IP_address)

重大度別システムヘルスおよびネットワーク診断メッセージリスト

- %Threat Defense-6-605004: Login denied from source-address/source-port to interface:destination/service for user “username”
- %Threat Defense-6-605005: Login permitted from source-address/source-port to interface:destination/service for user “username”
- %Threat Defense-6-607001: Pre-allocate SIP connection_type secondary channel for interface_name:IP_address/port to interface_name:IP_address from string message
- %Threat Defense-6-608001: Pre-allocate Skinny connection_type secondary channel for interface_name:IP_address to interface_name:IP_address from string message
- %Threat Defense-6-610101: Authorization failed: Cmd: command Cmdtype: command_modifier
- %Threat Defense-6-611301: VPN Client: NAT configured for Client Mode with no split tunneling: NAT address: mapped_address
- %Threat Defense-6-611302: VPN Client: NAT exemption configured for Network Extension Mode with no split tunneling
- %Threat Defense-6-611303: VPN Client: NAT configured for Client Mode with split tunneling: NAT address: mapped_address Split Tunnel Networks: IP_address/netmask IP_address/netmask
- %Threat Defense-6-611304: VPN Client: NAT exemption configured for Network Extension Mode with split tunneling: Split Tunnel Networks: IP_address/netmask IP_address/netmask
- %Threat Defense-6-611305: VPN Client: DHCP Policy installed: Primary DNS: IP_address Secondary DNS: IP_address Primary WINS: IP_address Secondary WINS: IP_address
- %Threat Defense-6-611306: VPN Client: Perfect Forward Secrecy Policy installed
- %Threat Defense-6-611307: VPN Client: Head end: IP_address
- %Threat Defense-6-611308: VPN Client: Split DNS Policy installed: List of domains: string string
- %Threat Defense-6-611309: VPN Client: Disconnecting from head end and uninstalling previously downloaded policy: Head End: IP_address
- %Threat Defense-6-611310: VNP Client: XAUTH Succeeded: Peer: IP_address
- %Threat Defense-6-611311: VNP Client: XAUTH Failed: Peer: IP_address
- %Threat Defense-6-611312: VPN Client: Backup Server List: reason
- %Threat Defense-6-611314: VPN Client: Load Balancing Cluster with Virtual IP: IP_address has redirected the to server IP_address
- %Threat Defense-6-611315: VPN Client: Disconnecting from Load Balancing Cluster member IP_address
- %Threat Defense-6-611316: VPN Client: Secure Unit Authentication Enabled
- %Threat Defense-6-611317: VPN Client: Secure Unit Authentication Disabled
- %Threat Defense-6-611318: VPN Client: User Authentication Enabled: Auth Server IP: IP_address Auth Server Port: port Idle Timeout: time
- %Threat Defense-6-611319: VPN Client: User Authentication Disabled
- %Threat Defense-6-611320: VPN Client: Device Pass Thru Enabled

重大度別システムヘルスおよびネットワーク診断メッセージリスト

- %Threat Defense-6-611321: VPN Client: Device Pass Thru Disabled
- %Threat Defense-6-611322: VPN Client: Extended XAUTH conversation initiated when SUA disabled
- %Threat Defense-6-611323: VPN Client: Duplicate split nw entry
- %Threat Defense-6-613001: Checksum Failure in database in area string Link State Id IP_address Old Checksum number New Checksum number
- %Threat Defense-6-613002: interface interface_name has zero bandwidth
- %Threat Defense-6-613003: IP_address netmask changed from area string to area string
- %Threat Defense-6-613014: Base topology enabled on interface string attached to MTR compatible mode area string
- %Threat Defense-6-613027: OSPF process number removed from interface interface_name
- %Threat Defense-6-613028: Unrecognized virtual interface intetface_name. Treat it as loopback stub route
- %Threat Defense-6-613041: OSPF-100 Areav string: LSA ID IP_address, Type number, Adv-rtr IP_address, LSA counter DoNotAge
- %Threat Defense-6-613043:
- %Threat Defense-6-613101: Checksum Failure in database in area %s\n Link State Id %i Old Checksum %#x New Checksum %#x\n
- %Threat Defense-6-613102: interface %s has zero bandwidth
- %Threat Defense-6-613103: %i%m changed from area %AREA_ID_STR to area %AREA_ID_STR
- %Threat Defense-6-613104: Unrecognized virtual interface %IF_NAME.
- %Threat Defense-6-614001: Split DNS: request patched from server: IP_address to server: IP_address
- %Threat Defense-6-614002: Split DNS: reply from server: IP_address reverse patched back to original server: IP_address
- %Threat Defense-6-615001: vlan number not available for firewall interface
- %Threat Defense-6-615002: vlan number available for firewall interface
- %Threat Defense-6-621001: Interface interface_name does not support multicast, not enabled
- %Threat Defense-6-621002: Interface interface_name does not support multicast, not enabled
- %Threat Defense-6-621003: The event queue size has exceeded number
- %Threat Defense-6-621006: Mrib disconnected, (IP_address, IP_address) event cancelled
- %Threat Defense-6-621007: Bad register from interface_name:IP_address to IP_address for (IP_address, IP_address)
- %Threat Defense-6-622001: string tracked route network mask address, distance number, table string, on interface interface-name
- %Threat Defense-6-622101: Starting regex table compilation for match_command; table entries = regex_num entries

重大度別システムヘルスおよびネットワーク診断メッセージリスト

- %Threat Defense-6-622102: Completed regex table compilation for match_command; table size = num bytes
- %Threat Defense-6-634001: DAP: User user, Addr ipaddr, Connection connection; The following DAP records were selected for this connection: DAP Record names
- %Threat Defense-6-709009: (unit-role) Configuration on Active and Standby is matching. No config sync. Time elapsed <time-elapsed> ms
- %Threat Defense-6-709010: Configuration between units doesn't match. Going for config sync (%d). Time elapsed <time-elapsed> ms.
- %Threat Defense-6-709011: Total time to sync the config *time* ms.
- %Threat Defense-6-709012: Skip configuration replication from mate as configuration on Active and Standby is matching.
- %Threat Defense-6-713128: Connection attempt to VCPIP redirected to VCA peer IP_address via load balancing
- %Threat Defense-6-713145: Detected Hardware Client in network extension mode, adding static route for address: IP_address, mask: netmask
- %Threat Defense-6-713147: Terminating tunnel to Hardware Client in network extension mode, deleting static route for address: IP_address, mask: netmask
- %Threat Defense-6-713172: Automatic NAT Detection Status: Remote end is|is not behind a NAT device This end is|is_not behind a NAT device
- %Threat Defense-6-713177: Received remote Proxy Host FQDN in ID Payload: Host Name: host_name Address IP_address, Protocol protocol, Port port
- %Threat Defense-6-713184: Client Type: Client_type Client Application Version: Application_version_string
- %Threat Defense-6-713202: Duplicate IP_addr packet detected.
- %Threat Defense-6-713213: Deleting static route for L2L peer that came in on a dynamic map. address: IP_address, mask: netmask
- %Threat Defense-6-713215: No match against Client Type and Version rules. Client: type version is/is not allowed by default
- %Threat Defense-6-713219: Queuing KEY-ACQUIRE messages to be processed when P1 SA is complete.
- %Threat Defense-6-713220: De-queuing KEY-ACQUIRE messages that were left pending.
- %Threat Defense-6-713228: Assigned private IP address assigned_private_IP
- %Threat Defense-6-713235: Attempt to send an IKE packet from standby unit. Dropping the packet!
- %Threat Defense-6-713256: IP = peer-IP, Sending spoofed ISAKMP Aggressive Mode message 2 due to receipt of unknown tunnel group. Aborting connection.
- %Threat Defense-6-713265: Adding static route for L2L peer coming in on a dynamic map. address: IP_address, mask: /prefix_len

重大度別システムヘルスおよびネットワーク診断メッセージリスト

- %Threat Defense-6-713267: Deleting static route for L2L peer that came in on a dynamic map. address: IP_address, mask: /prefix_len
- %Threat Defense-6-713269: Detected Hardware Client in network extension mode, adding static route for address: IP_address, mask: /prefix_len
- %Threat Defense-6-713271: Terminating tunnel to Hardware Client in network extension mode, deleting static route for address: IP_address, mask: /prefix_len
- %Threat Defense-6-713905: Descriptive_event_string.
- %Threat Defense-6-716001: Group group User user WebVPN session started.
- %Threat Defense-6-716002: Group group User user WebVPN session terminated: reason.
- %Threat Defense-6-716003: Group group User user WebVPN access GRANTED: url
- %Threat Defense-6-716004: Group group User user WebVPN access DENIED to specified location: url
- %Threat Defense-6-716005: Group group User user WebVPN ACL Parse Error: reason
- %Threat Defense-6-716006: Group name User user WebVPN session terminated. Idle timeout.
- %Threat Defense-6-716009: Group group User user WebVPN session not allowed. WebVPN ACL parse error.
- %Threat Defense-6-716038: Authentication: successful, group = name user = user, Session Type: WebVPN
- %Threat Defense-6-716039: Authentication: rejected, group = name user = user, Session Type: %s
- %Threat Defense-6-716040: Reboot pending, new sessions disabled. Denied user login.
- %Threat Defense-6-716041: access-list acl_ID action url url hit_cnt count
- %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
- %Threat Defense-6-716043 Group group-name, User user-name, IP IP_address: WebVPN Port Forwarding Java applet started. Created new hosts file mappings
- %Threat Defense-6-716049: Group group-name User user-name IP IP_address Empty SVC ACL.
- %Threat Defense-6-716050: Error adding to ACL: ace_command_line
- %Threat Defense-6-716051: Group group-name User user-name IP IP_address Error adding dynamic ACL for user.
- %Threat Defense-6-716055: Group group-name User user-name IP IP_address Authentication to SSO server name: name type type succeeded
- %Threat Defense-6-716058: Group group User user IP ip AnyConnect session lost connection. Waiting to resume.
- %Threat Defense-6-716059: Group group User user IP ip AnyConnect session resumed. Connection from ip2
- %Threat Defense-6-716060: Group group User user IP ip Terminated AnyConnect session in inactive state to accept a new connection. License limit reached.

- %Threat Defense-6-717003: Certificate received from Certificate Authority for trustpoint trustpoint_name.
- %Threat Defense-6-717004: PKCS #12 export failed for trustpoint trustpoint_name.
- %Threat Defense-6-717005: PKCS #12 export succeeded for trustpoint trustpoint_name.
- %Threat Defense-6-717006: PKCS #12 import failed for trustpoint trustpoint_name.
- %Threat Defense-6-717007: PKCS #12 import succeeded for trustpoint trustpoint_name.
- %Threat Defense-6-717016: Removing expired CRL from the CRL cache. Issuer: issuer
- %Threat Defense-6-717022: Certificate was successfully validated. certificate_identifiers
- %Threat Defense-6-717028: Certificate chain was successfully validated additional info.
- %Threat Defense-6-717033: OCSP response status - Successful.
- %Threat Defense-6-717056: Attempting type revocation check from Src Interface:Src IP/Src Port to Dst IP/Dst Port using protocol
- %Threat Defense-6-718003: Got unknown peer message message_number from IP_address, local version version_number, remote version version_number
- %Threat Defense-6-718004: Got unknown internal message message_number
- %Threat Defense-6-718013: Peer IP_address is not answering HELLO
- %Threat Defense-6-718027: Received unexpected KEEPALIVE request from IP_address
- %Threat Defense-6-718030: Received planned OOS from IP_address
- %Threat Defense-6-718037: Master processed number_of_timeouts timeouts
- %Threat Defense-6-718038: Slave processed number_of_timeouts timeouts
- %Threat Defense-6-718039: Process dead peer IP_address
- %Threat Defense-6-718040: Timed-out exchange ID exchange_ID not found
- %Threat Defense-6-718051: Deleted secure tunnel to peer IP_address
- %Threat Defense-6-719001: Email Proxy session could not be established: session limit of maximum_sessions has been reached.
- %Threat Defense-6-719003: Email Proxy session pointer resources have been freed for source_address.
- %Threat Defense-6-719004: Email Proxy session pointer has been successfully established for source_address.
- %Threat Defense-6-719010: protocol Email Proxy feature is disabled on interface interface_name.
- %Threat Defense-6-719011: Protocol Email Proxy feature is enabled on interface interface_name.
- %Threat Defense-6-719012: Email Proxy server listening on port port for mail protocol protocol.
- %Threat Defense-6-719013: Email Proxy server closing port port for mail protocol protocol.
- %Threat Defense-6-719017: WebVPN user: vpnuser invalid dynamic ACL.
- %Threat Defense-6-719018: WebVPN user: vpnuser ACL ID acl_ID not found

重大度別システムヘルスおよびネットワーク診断メッセージリスト

- %Threat Defense-6-719019: WebVPN user: vpnuser authorization failed.
- %Threat Defense-6-719020: WebVPN user vpnuser authorization completed successfully.
- %Threat Defense-6-719021: WebVPN user: vpnuser is not checked against ACL.
- %Threat Defense-6-719022: WebVPN user vpnuser has been authenticated.
- %Threat Defense-6-719023: WebVPN user vpnuser has not been successfully authenticated. Access denied.
- %Threat Defense-6-719024: Email Proxy piggyback auth fail: session = pointer user=vpnuser addr=source_address
- %Threat Defense-6-719025: Email Proxy DNS name resolution failed for hostname.
- %Threat Defense-6-719026: Email Proxy DNS name hostname resolved to IP_address.
- %Threat Defense-6-720002: (VPN-unit) Starting VPN Stateful Failover Subsystem...
- %Threat Defense-6-720003: (VPN-unit) Initialization of VPN Stateful Failover Component completed successfully
- %Threat Defense-6-720004: (VPN-unit) VPN failover main thread started.
- %Threat Defense-6-720005: (VPN-unit) VPN failover timer thread started.
- %Threat Defense-6-720006: (VPN-unit) VPN failover sync thread started.
- %Threat Defense-6-720010: (VPN-unit) VPN failover client is being disabled
- %Threat Defense-6-720012: (VPN-unit) Failed to update IPSec failover runtime data on the standby unit.
- %Threat Defense-6-720014: (VPN-unit) Phase 2 connection entry (msg_id=message_number, my cookie=mine, his cookie=his) contains no SA list.
- %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).
- %Threat Defense-6-720023: (VPN-unit) HA status callback: Peer is not present.
- %Threat Defense-6-720024: (VPN-unit) HA status callback: Control channel is status.
- %Threat Defense-6-720025: (VPN-unit) HA status callback: Data channel is status.
- %Threat Defense-6-720026: (VPN-unit) HA status callback: Current progression is being aborted.
- %Threat Defense-6-720027: (VPN-unit) HA status callback: My state state.
- %Threat Defense-6-720028: (VPN-unit) HA status callback: Peer state state.
- %Threat Defense-6-720029: (VPN-unit) HA status callback: Start VPN bulk sync state.
- %Threat Defense-6-720030: (VPN-unit) HA status callback: Stop bulk sync state.
- %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.
- %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.

重大度別システムヘルスおよびネットワーク診断メッセージリスト

- %Threat Defense-6-720039: (VPN-unit) VPN failover client is transitioning to active state
- %Threat Defense-6-720040: (VPN-unit) VPN failover client is transitioning to standby state.
- %Threat Defense-6-720045: (VPN-unit) Start bulk syncing of state information on standby unit.
- %Threat Defense-6-720046: (VPN-unit) End bulk syncing of state information on standby unit
- %Threat Defense-6-720056: (VPN-unit) VPN Stateful failover Message Thread is being disabled.
- %Threat Defense-6-720057: (VPN-unit) VPN Stateful failover Message Thread is enabled.
- %Threat Defense-6-720058: (VPN-unit) VPN Stateful failover Timer Thread is disabled.
- %Threat Defense-6-720059: (VPN-unit) VPN Stateful failover Timer Thread is enabled.
- %Threat Defense-6-720060: (VPN-unit) VPN Stateful failover Sync Thread is disabled.
- %Threat Defense-6-720061: (VPN-unit) VPN Stateful failover Sync Thread is enabled.
- %Threat Defense-6-720062: (VPN-unit) Active unit started bulk sync of state information to standby unit.
- %Threat Defense-6-720063: (VPN-unit) Active unit completed bulk sync of state information to standby.
- %Threat Defense-6-721001: (device) WebVPN Failover SubSystem started successfully.(device) either WebVPN-primary or WebVPN-secondary.
- %Threat Defense-6-721002: (device) HA status change: event event, my state my_state, peer state peer.
- %Threat Defense-6-721003: (device) HA progression change: event event, my state my_state, peer state peer.
- %Threat Defense-6-721004: (device) Create access list list_name on standby unit.
- %Threat Defense-6-721005: (device) Fail to create access list list_name on standby unit.
- %Threat Defense-6-721006: (device) Update access list list_name on standby unit.
- %Threat Defense-6-721008: (device) Delete access list list_name on standby unit.
- %Threat Defense-6-721009: (device) Fail to delete access list list_name on standby unit.
- %Threat Defense-6-721010: (device) Add access list rule list_name, line line_no on standby unit.
- %Threat Defense-6-721012: (device) Enable APCF XML file file_name on the standby unit.
- %Threat Defense-6-721014: (device) Disable APCF XML file file_name on the standby unit.
- %Threat Defense-6-721016: (device) WebVPN session for client user user_name, IP ip_address has been created.
- %Threat Defense-6-721018: (device) WebVPN session for client user user_name, IP ip_address has been deleted.
- %Threat Defense-6-722013: Group group User user-name IP IP_address SVC Message: type-num/INFO: message

重大度別システムヘルスおよびネットワーク診断メッセージリスト

- %Threat Defense-6-722014: Group group User user-name IP IP_address SVC Message: type-num/INFO: message
- %Threat Defense-6-722051: Group group-policy User username IP public-ip Address assigned-ip assigned to session
- %Threat Defense-6-722053: Group g User u IP ip Unknown client user-agent connection.
- %Threat Defense-6-722055: Group group-policy User username IP public-ip Client Type: user-agent
- %Threat Defense-6-723001: Group group-name, User user-name, IP IP_address: WebVPN Citrix ICA connection connection is up.
- %Threat Defense-6-723002: Group group-name, User user-name, IP IP_address: WebVPN Citrix ICA connection connection is down.
- %Threat Defense-6-725001: Starting SSL handshake with peer-type interface:src-ip/src-port to dst-ip/dst-port for protocol session.
- %Threat Defense-6-725002: Device completed SSL handshake with peer-type interface:src-ip/src-port to dst-ip/dst-port for protocol-version session
- %Threat Defense-6-725003: SSL peer-type interface:src-ip/src-port to dst-ip/dst-port request to resume previous session.
- %Threat Defense-6-725004: Device requesting certificate from SSL peer-type interface:src-ip/src-port to dst-ip/dst-port for authentication.
- %Threat Defense-6-725005: SSL peer-type interface:src-ip/src-port to dst-ip/dst-port requesting our device certificate for authentication.
- %Threat Defense-6-725006: Device failed SSL handshake with peer-type interface:src-ip/src-port to dst-ip/dst-port
- %Threat Defense-6-725007: SSL session with peer-type interface:src-ip/src-port to dst-ip/dst-port terminated.
- %Threat Defense-6-726001: Inspected im_protocol im_service Session between Client im_client_1 and im_client_2 Packet flow from src_ifc:/sip/sport to dest_ifc:/dip/dport Action: action Matched Class class_map_id class_map_name
- %Threat Defense-6-725016: Device selects trust-point <trustpoint> for peer-type interface:src-ip/src-port to dst-ip/dst-port
- %Threat Defense-6-734001: DAP: User user, Addr ipaddr, Connection connection: The following DAP records were selected for this connection: DAP record names
- %Threat Defense-6-737005: IPAA: DHCP configured, request succeeded for tunnel-group 'tunnel-group'
- %Threat Defense-6-737006: IPAA: Local pool request succeeded for tunnel-group 'tunnel-group'
- %Threat Defense-6-737009: IPAA: AAA assigned address ip-address, request failed
- %Threat Defense-6-737010: IPAA: AAA assigned address ip-address, request succeeded
- %Threat Defense-6-737014: IPAA: Freeing AAA address ip-address
- %Threat Defense-6-737015: IPAA: Freeing DHCP address ip-address

重大度別システムヘルスおよびネットワーク診断メッセージリスト

- %Threat Defense-6-737016: IPAA: Freeing local pool address ip-address
- %Threat Defense-6-737017: IPAA: DHCP request attempt num succeeded
- %Threat Defense-6-737026: IPAA: Client assigned ip-address from local pool
- %Threat Defense-6-737029: IPAA: Adding ip-address to standby: succeeded
- %Threat Defense-6-737031: IPAA: Removing %m from standby: succeeded
- %FTD-6-737036: IPAA: Session=<session>, Client assigned <address> from DHCP
- %FTD-6-737205: VPNFIP: Pool=pool, INFO: message
- %Threat Defense-6-737406: POOLIP: Pool=pool, INFO: message
- %Threat Defense-6-741000: Coredump filesystem image created on variable 1 -size variable 2 MB
- %Threat Defense-6-741001: Coredump filesystem image on variable 1 - resized from variable 2 MB to variable 3 MB
- %Threat Defense-6-741002: Coredump log and filesystem contents cleared on variable 1
- %Threat Defense-6-741003: Coredump filesystem and its contents removed on variable 1
- %Threat Defense-6-741004: Coredump configuration reset to default values
- %Threat Defense-6-747004: Clustering: state machine changed from state state-name to state-name.
- %FTD-6-747044: Clustering: Configuration Hash string verification <result>.
- %Threat Defense-6-748008: [CPU load *percentage* | memory load *percentage*] of module *slot_number* in chassis *chassis_number* (*member-name*) exceeds overflow protection threshold [CPU *percentage* | memory *percentage*]. System may be oversubscribed on member failure.
- %Threat Defense-6-748009: [CPU load percentage | memory load percentage] of chassis chassis_number exceeds overflow protection threshold [CPU percentage | memory percentage}. System may be oversubscribed on chassis failure.
- %Threat Defense-6-751023: Local a:p Remote: a:p Username:n Unknown client connection
- %Threat Defense-6-751026: Local: localIP:port Remote: remoteIP:port Username: username/group IKEv2 Client OS: client-os Client: client-name client-version
- %Threat Defense-6-767001: Inspect-name: Dropping an unsupported IPv6/IP46/IP64 packet from interface:IP Addr to interface:IP Addr (fail-close)
- %FTD-6-769007: UPDATE: Image version is version_number
- %Threat Defense-6-772005: REAUTH: user username passed authentication
- %FTD-6-776251: CTS SGT-MAP: Binding binding IP - SGname (SGT) from source name added to binding manager.
- %FTD-6-776253: CTS SGT-MAP: Binding binding IP - new SGname (SGT) from new source name changed from old sgt: old SGname (SGT) from old source old source name.
- %Threat Defense-6-778001: VXLAN: Invalid VXLAN segment-id segment-id for protocol from ifc-name:(IP-address/port) to ifc-name:(IP-address/port).
- %Threat Defense-6-778002: VXLAN: There is no VNI interface for segment-id segment-id.

重大度別システムヘルスおよびネットワーク診断メッセージリスト

- %Threat Defense-6-778003: VXLAN: Invalid VXLAN segment-id segment-id for protocol from ifc-name:(IP-address/port) to ifc-name:(IP-address/port) in FP.
- %Threat Defense-6-778004: VXLAN: Invalid VXLAN header for protocol from ifc-name:(IP-address/port) to ifc-name:(IP-address/port) in FP.
- %Threat Defense-6-778005: VXLAN: Packet with VXLAN segment-id segment-id from ifc-name is denied by FP L2 check.
- %Threat Defense-6-778006: VXLAN: Invalid VXLAN UDP checksum from ifc-name:(IP-address/port) to ifc-name:(IP-address/port) in FP.
- %Threat Defense-6-778007: VXLAN: Packet from ifc-name:IP-address/port to IP-address/port was discarded due to invalid NVE peer.
- %Threat Defense-6-779001: STS: Out-tag lookup failed for in-tag segment-id of protocol from ifc-name:IP-address/port to IP-address/port.
- %Threat Defense-6-779002: STS: STS and NAT locate different egress interface for segment-id segment-id, protocol from ifc-name:IP-address/port to IP-address/port
- %Threat Defense-6-780001: RULE ENGINE: Started compilation for access-group transaction - description of the transaction
- %Threat Defense-6-780002: RULE ENGINE: Finished compilation for access-group transaction - description of the transaction
- %Threat Defense-6-780003: RULE ENGINE: Started compilation for nat transaction -description of the transaction
- %Threat Defense-6-780004: RULE ENGINE: Finished compilation for nat transaction -description of the transaction
- %Threat Defense-6-802005: IP ip_address Received MDM request details.
- %Threat Defense-6-803001:Bypass is continuing after power up, no protection will be provided by the system for traffic over GigabitEthernet 1/1-1/2
- %Threat Defense-6-803002: No protection will be provided by the system for traffic over GigabitEthernet 1/1-1/2
- %Threat Defense-6-803003: User disabled bypass manually on GigabitEthernet 1/1-1/2
- %Threat Defense-6-804001: Interface GigabitEthernet1/3 1000BaseSX SFP has been inserted
- %Threat Defense-6-804002: Interface GigabitEthernet1/3 SFP has been removed
- %Threat Defense-6-805001: Flow offloaded: connection conn_id outside_ifc:outside_addr/outside_port (mapped_addr/mapped_port) inside_ifc:inside_addr/inside_port (mapped_addr/mapped_port) Protocol
- %Threat Defense-6-805002: Flow is no longer offloaded: connection conn_id outside_ifc:outside_addr/outside_port (mapped_addr/mapped_port) inside_ifc:inside_addr/inside_port (mapped_addr/mapped_port) Protocol
- %Threat Defense-6-805003: Flow could not be offloaded: connection <conn_id> <outside_ifc>:<outside_addr>/<outside_port> (<mapped_addr>/<mapped_port>) < inside_ifc>:<inside_addr>/<inside_port> (<mapped_addr>/<mapped_port>) <Protocol>
- %FTD-6-802005: IP ip_address Received MDM request details.

- %FTD-6-852001: Received Lightweight to Full Proxy event from application Snort for TCP flow ip-address/port to ip-address/port
- %FTD-6-852002: Received Full Proxy to Lightweight event from application Snort for TCP flow ip-address/port to ip-address/port
- %Threat Defense-6-8300001: VPN session redistribution <variable 1>
- %Threat Defense-6-8300002: Moved <variable 1> sessions to <variable 2>
- %Threat Defense-6-8300004: <variable 1> request to move <variable 2> sessions from <variable 3> to <variable 4>

デバッグ メッセージ、重大度 7

次のメッセージが重大度 7（デバッグ）で表示されます。

- %Threat Defense-7-111009: User user executed cmd:string
- %Threat Defense-7-113028: Extraction of username from VPN client certificate has string. [Request num]
- %Threat Defense-7-199019: syslog
- %Threat Defense-7-333004: EAP-SQ response invalid - context:EAP-context
- %Threat Defense-7-333005: EAP-SQ response contains invalid TLV(s) - context:EAP-context
- %Threat Defense-7-333006: EAP-SQ response with missing TLV(s) - context:EAP-context
- %Threat Defense-7-333007: EAP-SQ response TLV has invalid length - context:EAP-context
- %Threat Defense-7-333008: EAP-SQ response has invalid nonce TLV - context:EAP-context
- %Threat Defense-7-609001: Built local-host zone_name/*: ip_address
- %Threat Defense-7-609002: Teardown local-host zone_name/*: ip_address duration time
- %Threat Defense-7-701001: alloc_user() out of Tcp_user objects
- %Threat Defense-7-701002: alloc_user() out of Tcp_proxy objects
- %Threat Defense-7-702307: IPSEC: An direction tunnel_type SA (SPI=spi) between local_IP and remote_IP (username) is rekeying due to data rollover.
- %Threat Defense-7-703001: H.225 message received from interface_name:IP_address/port to interface_name:IP_address/port is using an unsupported version number
- %Threat Defense-7-703002: Received H.225 Release Complete with newConnectionNeeded for interface_name:IP_address to interface_name:IP_address/port
- %Threat Defense-7-703008: Allowing early-message: %s before SETUP from %s:%Q/%d to %s:%Q/%d\n
- %Threat Defense-7-709001: FO replication failed: cmd=command returned=code
- %Threat Defense-7-709002: FO unreplicable: cmd=command

重大度別システムヘルスおよびネットワーク診断メッセージリスト

- %Threat Defense-7-710001: TCP access requested from source_address/source_port to interface_name:dest_address/service
- %Threat Defense-7-710002: {TCP|UDP} access permitted from source_address/source_port to interface_name:dest_address/service
- %Threat Defense-7-710004: TCP connection limit exceeded from Src_ip/Src_port to In_name:Dest_ip/Dest_port (current connections/connection limit = Curr_conn/Conn_lmt)
- %Threat Defense-7-710005: {TCP|UDP} request discarded from source_address/source_port to interface_name:dest_address/service
- %Threat Defense-7-710006: protocol request discarded from source_address to interface_name:dest_address
- %Threat Defense-7-710007: NAT-T keepalive received from 86.1.161.1/1028 to outside:86:1.129.1/4500
- %Threat Defense-7-711001: debug_trace_msg
- %Threat Defense-7-711003: Unknown/Invalid interface identifier(vpifnum) detected.
- %Threat Defense-7-711006: CPU profiling has started for n-samples samples. Reason: reason-string.
- %Threat Defense-7-713024: Group group IP ip Received local Proxy Host data in ID Payload: Address IP_address, Protocol protocol, Port port
- %Threat Defense-7-713025: Received remote Proxy Host data in ID Payload: Address IP_address, Protocol protocol, Port port
- %Threat Defense-7-713028: Received local Proxy Range data in ID Payload: Addresses IP_address - IP_address, Protocol protocol, Port port
- %Threat Defense-7-713029: Received remote Proxy Range data in ID Payload: Addresses IP_address - IP_address, Protocol protocol, Port port
- %Threat Defense-7-713034: Received local IP Proxy Subnet data in ID Payload: Address IP_address, Mask netmask, Protocol protocol, Port port
- %Threat Defense-7-713035: Group group IP ip Received remote IP Proxy Subnet data in ID Payload: Address IP_address, Mask netmask, Protocol protocol, Port port
- %Threat Defense-7-713039: Send failure: Bytes (number), Peer: IP_address
- %Threat Defense-7-713040: Could not find connection entry and can not encrypt: msgid message_number
- %Threat Defense-7-713052: User (user) authenticated.
- %Threat Defense-7-713066: IKE Remote Peer configured for SA: SA_name
- %Threat Defense-7-713094: Cert validation failure: handle invalid for Main/Aggressive Mode Initiator/Responder!
- %Threat Defense-7-713099: Tunnel Rejected: Received NONCE length number is out of range!
- %Threat Defense-7-713103: Invalid (NULL) secret key detected while computing hash
- %Threat Defense-7-713104: Attempt to get Phase 1 ID data failed while hash computation

重大度別システムヘルスおよびネットワーク診断メッセージリスト

- %Threat Defense-7-713113: Deleting IKE SA with associated IPSec connection entries. IKE peer: IP_address, SA address: internal_SA_address, tunnel count: count
- %Threat Defense-7-713114: Connection entry (conn entry internal address) points to IKE SA (SA_internal_address) for peer IP_address, but cookies don't match
- %Threat Defense-7-713117: Received Invalid SPI notify (SPI SPI_Value)!
- %Threat Defense-7-713121: Keep-alive type for this connection: keepalive_type
- %Threat Defense-7-713143: Processing firewall record. Vendor: vendor(id), Product: product(id), Caps: capability_value, Version Number: version_number, Version String: version_text
- %Threat Defense-7-713160: Remote user (session Id - id) has been granted access by the Firewall Server
- %Threat Defense-7-713164: The Firewall Server has requested a list of active user sessions
- %Threat Defense-7-713169: IKE Received delete for rekeyed SA IKE peer: IP_address, SA address: internal_SA_address, tunnelCnt: tunnel_count
- %Threat Defense-7-713170: Group group IP ip IKE Received delete for rekeyed centry IKE peer: IP_address, centry address: internal_address, msgid: id
- %Threat Defense-7-713171: NAT-Traversal sending NAT-Original-Address payload
- %Threat Defense-7-713187: Tunnel Rejected: IKE peer does not match remote peer as defined in L2L policy IKE peer address: IP_address, Remote peer address: IP_address
- %Threat Defense-7-713190: Got bad refCnt (ref_count_value) assigning IP_address (IP_address)
- %Threat Defense-7-713204: Adding static route for client address: IP_address
- %Threat Defense-7-713221: Static Crypto Map check, checking map = crypto_map_tag, seq = seq_number...
- %Threat Defense-7-713222: Group group Username username IP ip Static Crypto Map check, map = crypto_map_tag, seq = seq_number, ACL does not match proxy IDs src:source_address dst:dest_address
- %Threat Defense-7-713223: Static Crypto Map check, map = crypto_map_tag, seq = seq_number, no ACL configured
- %Threat Defense-7-713224: Static Crypto Map Check by-passed: Crypto map entry incomplete!
- %Threat Defense-7-713225: [IKEv1], Static Crypto Map check, map map_name, seq = sequence_number is a successful match
- %Threat Defense-7-713233: (VPN-unit) Remote network (remote network) validated for network extension mode.
- %Threat Defense-7-713234: (VPN-unit) Remote network (remote network) from network extension mode client mismatches AAA configuration (aaa network).
- %Threat Defense-7-713236: IKE_DECODE tx/rx Message (msgid=msgid) with payloads:payload1 (payload1_len) + payload2 (payload2_len)...total length: tlen
- %Threat Defense-7-713263: Received local IP Proxy Subnet data in ID Payload: Address IP_address, Mask /prefix_len, Protocol protocol, Port port

重大度別システムヘルスおよびネットワーク診断メッセージリスト

- %Threat Defense-7-713264: Received local IP Proxy Subnet data in ID Payload: Address IP_address, Mask /prefix_len, Protocol protocol, Port port {“Received remote IP Proxy Subnet data in ID Payload: Address %a, Mask/%d, Protocol %u, Port %u”}
- %Threat Defense-7-713273: Deleting static route for client address: IP_Address IP_Address address of client whose route is being removed
- %Threat Defense-7-713906: Descriptive_event_string.
- %Threat Defense-7-714001: description_of_event_or_packet
- %Threat Defense-7-714002: IKE Initiator starting QM: msg id = message_number
- %Threat Defense-7-714003: IKE Responder starting QM: msg id = message_number
- %Threat Defense-7-714004: IKE Initiator sending 1st QM pkt: msg id = message_number
- %Threat Defense-7-714005: IKE Responder sending 2nd QM pkt: msg id = message_number
- %Threat Defense-7-714006: IKE Initiator sending 3rd QM pkt: msg id = message_number
- %Threat Defense-7-714007: IKE Initiator sending Initial Contact
- %Threat Defense-7-714011: Description of received ID values
- %Threat Defense-7-715001: Descriptive statement
- %Threat Defense-7-715004: subroutine name() Q Send failure: RetCode (return_code)
- %Threat Defense-7-715005: subroutine name() Bad message code: Code (message_code)
- %Threat Defense-7-715006: IKE got SPI from key engine: SPI = SPI_value
- %Threat Defense-7-715007: IKE got a KEY_ADD msg for SA: SPI = SPI_value
- %Threat Defense-7-715008: Could not delete SA SA_address, refCnt = number, caller = calling_subroutine_address
- %Threat Defense-7-715009: IKE Deleting SA: Remote Proxy IP_address, Local Proxy IP_address
- %Threat Defense-7-715013: Tunnel negotiation in progress for destination IP_address, discarding data
- %Threat Defense-7-715019: Group group Username username IP ip IKEGetUserAttributes: Attribute name = name
- %Threat Defense-7-715020: construct_cfg_set: Attribute name = name
- %Threat Defense-7-715021: Delay Quick Mode processing, Cert/Trans Exch/RM DSID in progress
- %Threat Defense-7-715022: Resume Quick Mode processing, Cert/Trans Exch/RM DSID completed
- %Threat Defense-7-715027: IPSec SA Proposal # chosen_proposal, Transform # chosen_transform acceptable Matches global IPSec SA entry # crypto_map_index
- %Threat Defense-7-715028: IKE SA Proposal # 1, Transform # chosen_transform acceptable Matches global IKE entry # crypto_map_index
- %Threat Defense-7-715033: Processing CONNECTED notify (MsgId message_number)
- %Threat Defense-7-715034: action IOS keep alive payload: proposal=time 1/time 2 sec.

重大度別システムヘルスおよびネットワーク診断メッセージリスト

- %Threat Defense-7-715035: Starting IOS keepalive monitor: seconds sec.
- %Threat Defense-7-715036: Sending keep-alive of type notify_type (seq number number)
- %Threat Defense-7-715037: Unknown IOS Vendor ID version: major.minor.variance
- %Threat Defense-7-715038: action Spoofing_information Vendor ID payload (version: major.minor.variance, capabilities: value)
- %Threat Defense-7-715039: Unexpected cleanup of tunnel table entry during SA delete.
- %Threat Defense-7-715040: Deleting active auth handle during SA deletion: handle = internal_authentication_handle
- %Threat Defense-7-715041: Received keep-alive of type keepalive_type, not the negotiated type
- %Threat Defense-7-715042: IKE received response of type failure_type to a request from the IP_address utility
- %Threat Defense-7-715044: Ignoring Keepalive payload from vendor not support KeepAlive capability
- %Threat Defense-7-715045: ERROR: malformed Keepalive payload
- %Threat Defense-7-715046: Group = groupname, Username = username, IP = IP_address, constructing payload_description payload
- %Threat Defense-7-715047: processing payload_description payload
- %Threat Defense-7-715048: Send VID_type VID
- %Threat Defense-7-715049: Received VID_type VID
- %Threat Defense-7-715050: Claims to be IOS but failed authentication
- %Threat Defense-7-715051: Received unexpected TLV type TLV_type while processing FWTYPE ModeCfg Reply
- %Threat Defense-7-715052: Old P1 SA is being deleted but new SA is DEAD, cannot transition centries
- %Threat Defense-7-715053: MODE_CFG: Received request for attribute_info!
- %Threat Defense-7-715054: MODE_CFG: Received attribute_name reply: value
- %Threat Defense-7-715055: Send attribute_name
- %Threat Defense-7-715056: Client is configured for TCP_transparency
- %Threat Defense-7-715057: Auto-detected a NAT device with NAT-Traversal. Ignoring IPSec-over-UDP configuration.
- %Threat Defense-7-715058: NAT-Discovery payloads missing. Aborting NAT-Traversal.
- %Threat Defense-7-715059: Proposing/Selecting only UDP-Encapsulated-Tunnel and UDP-Encapsulated-Transport modes defined by NAT-Traversal
- %Threat Defense-7-715060: Dropped received IKE fragment. Reason: reason
- %Threat Defense-7-715061: Rcv'd fragment from a new fragmentation set. Deleting any old fragments.
- %Threat Defense-7-715062: Error assembling fragments! Fragment numbers are non-continuous.

重大度別システムヘルスおよびネットワーク診断メッセージリスト

- %Threat Defense-7-715063: Successfully assembled an encrypted pkt from rcv'd fragments!
- %Threat Defense-7-715064 -- IKE Peer included IKE fragmentation capability flags: Main Mode: true/false Aggressive Mode: true/false
- %Threat Defense-7-715065: IKE state_machine subtype FSM error history (struct data_structure_address) state, event: state/event pairs
- %Threat Defense-7-715066: Can't load an IPSec SA! The corresponding IKE SA contains an invalid logical ID.
- %Threat Defense-7-715067: QM IsRekeyed: existing sa from different peer, rejecting new sa
- %Threat Defense-7-715067: QM IsRekeyed: existing sa from different peer, rejecting new sa
- %Threat Defense-7-715068: QM IsRekeyed: duplicate sa found by address, deleting old sa
- %Threat Defense-7-715069: Invalid ESP SPI size of SPI_size
- %Threat Defense-7-715070: Invalid IPComp SPI size of SPI_size
- %Threat Defense-7-715071: AH proposal not supported
- %Threat Defense-7-715072: Received proposal with unknown protocol ID protocol_ID
- %Threat Defense-7-715074: Could not retrieve authentication attributes for peer IP_address
- %Threat Defense-7-715075: Group = group_name, IP = IP_address Received keep-alive of type message_type (seq number number)
- %Threat Defense-7-715076: Computing hash for ISAKMP
- %Threat Defense-7-715077: Pitcher: msg string, spi spi
- %Threat Defense-7-715080: VPN: Starting P2 rekey timer: 28800 seconds.
- %Threat Defense-7-716008: WebVPN ACL: action
- %Threat Defense-7-716010: Group group User user Browse network.
- %Threat Defense-7-716011: Group group User user Browse domain domain.
- %Threat Defense-7-716012: Group group User user Browse directory directory.
- %Threat Defense-7-716013: Group group User user Close file filename.
- %Threat Defense-7-716014: Group group User user View file filename.
- %Threat Defense-7-716015: Group group User user Remove file filename.
- %Threat Defense-7-716016: Group group User user Rename file old_filename to new_filename.
- %Threat Defense-7-716017: Group group User user Modify file filename.
- %Threat Defense-7-716018: Group group User user Create file filename.
- %Threat Defense-7-716019: Group group User user Create directory directory.
- %Threat Defense-7-716020: Group group User user Remove directory directory.
- %Threat Defense-7-716021: File access DENIED, filename.

重大度別システムヘルスおよびネットワーク診断メッセージリスト

- %Threat Defense-7-716024: Group name User user Unable to browse the network.Error: description
- %Threat Defense-7-716025: Group name User user Unable to browse domain domain. Error: description
- %Threat Defense-7-716026: Group name User user Unable to browse directory directory. Error: description
- %Threat Defense-7-716027: Group name User user Unable to view file filename. Error: description
- %Threat Defense-7-716028: Group name User user Unable to remove file filename. Error: description
- %Threat Defense-7-716029: Group name User user Unable to rename file filename. Error: description
- %Threat Defense-7-716030: Group name User user Unable to modify file filename. Error: description
- %Threat Defense-7-716031: Group name User user Unable to create file filename. Error: description
- %Threat Defense-7-716032: Group name User user Unable to create folder folder. Error: description
- %Threat Defense-7-716033: Group name User user Unable to remove folder folder. Error: description
- %Threat Defense-7-716034: Group name User user Unable to write to file filename.
- %Threat Defense-7-716035: Group name User user Unable to read file filename.
- %Threat Defense-7-716036: Group name User user File Access: User user logged into the server server.
- %Threat Defense-7-716037: Group name User user File Access: User user failed to login into the server server.
- %Threat Defense-7-716603: Received size-recv KB Hostscan data from IP src-ip.
- %Threat Defense-7-717024: Checking CRL from trustpoint: trustpoint name for purpose
- %Threat Defense-7-717025: Validating certificate chain containing number of certs certificate(s).
- %Threat Defense-7-717029: Identified client certificate within certificate chain. serial number: serial_number, subject name: subject_name.
- %Threat Defense-7-717030: Found a suitable trustpoint trustpoint name to validate certificate.
- %Threat Defense-7-717034: No-check extension found in certificate. OCSP check bypassed.
- %Threat Defense-7-717036: Looking for a tunnel group match based on certificate maps for peer certificate with certificate_identifier.
- %Threat Defense-7-717038: Tunnel group match found. Tunnel Group: tunnel_group_name, Peer certificate: certificate_identifier.
- %Threat Defense-7-718001: Internal interprocess communication queue send failure: code error_code
- %Threat Defense-7-718017: Got timeout for unknown peer IP_address msg type message_type
- %Threat Defense-7-718018: Send KEEPALIVE request failure to IP_address
- %Threat Defense-7-718019: Sent KEEPALIVE request to IP_address
- %Threat Defense-7-718020: Send KEEPALIVE response failure to IP_address

重大度別システムヘルスおよびネットワーク診断メッセージリスト

- %Threat Defense-7-718021: Sent KEEPALIVE response to IP_address
- %Threat Defense-7-718022: Received KEEPALIVE request from IP_address
- %Threat Defense-7-718023: Received KEEPALIVE response from IP_address
- %Threat Defense-7-718025: Sent CFG UPDATE to IP_address
- %Threat Defense-7-718026: Received CFG UPDATE from IP_address
- %Threat Defense-7-718029: Sent OOS indicator to IP_address
- %Threat Defense-7-718034: Sent TOPOLOGY indicator to IP_address
- %Threat Defense-7-718035: Received TOPOLOGY indicator from IP_address
- %Threat Defense-7-718036: Process timeout for req-type type_value, exid exchange_ID, peer IP_address
- %Threat Defense-7-718041: Timeout [msgType=type] processed with no callback
- %Threat Defense-7-718046: Create group policy policy_name
- %Threat Defense-7-718047: Fail to create group policy policy_name
- %Threat Defense-7-718049: Created secure tunnel to peer IP_address
- %Threat Defense-7-718056: Deleted Master peer, IP IP_address
- %Threat Defense-7-718058: State machine return code: action_routine, return_code
- %Threat Defense-7-718059: State machine function trace: state=state_name, event=event_name, func=action_routine
- %Threat Defense-7-718088: Possible VPN LB misconfiguration. Offending device MAC MAC_address.
- %Threat Defense-7-719005: FSM NAME has been created using protocol for session pointer from source_address.
- %Threat Defense-7-719006: Email Proxy session pointer has timed out for source_address because of network congestion.
- %Threat Defense-7-719007: Email Proxy session pointer cannot be found for source_address.
- %Threat Defense-7-719009: Email Proxy service is starting.
- %Threat Defense-7-719015: Parsed emailproxy session pointer from source_address username: mailuser = mail_user, vpnuser = VPN_user, mailserver = server
- %Threat Defense-7-719016: Parsed emailproxy session pointer from source_address password: mailpass = ******, vpnpass= ******
- %Threat Defense-7-720031: (VPN-unit) HA status callback: Invalid event received. event=event_ID.
- %Threat Defense-7-720034: (VPN-unit) Invalid type (type) for message handler.
- %Threat Defense-7-720041: (VPN-unit) Sending type message id to standby unit
- %Threat Defense-7-720042: (VPN-unit) Receiving type message id from active unit

- %Threat Defense-7-720048: (VPN-unit) FSM action trace begin: state=state, last event=event, func=function.
- %Threat Defense-7-720049: (VPN-unit) FSM action trace end: state=state, last event=event, return=return, func=function.
- %Threat Defense-7-720050: (VPN-unit) Failed to remove timer. ID = id.
- %Threat Defense-7-722029: Group group User user-name IP IP_address SVC Session Termination: Conns: connections, DPD Conns: DPD_conns, Comp resets: compression_resets, Dcmp resets: decompression_resets
- %Threat Defense-7-722030: Group group User user-name IP IP_address SVC Session Termination: In: data_bytes (+ctrl_bytes) bytes, data_pkts (+ctrl_pkts) packets, drop_pkts drops
- %Threat Defense-7-722031: Group group User user-name IP IP_address SVC Session Termination: Out: data_bytes (+ctrl_bytes) bytes, data_pkts (+ctrl_pkts) packets, drop_pkts drops.
- %Threat Defense-7-723003: No memory for WebVPN Citrix ICA connection connection.
- %Threat Defense-7-723004: WebVPN Citrix encountered bad flow control flow.
- %Threat Defense-7-723005: No channel to set up WebVPN Citrix ICA connection.
- %Threat Defense-7-723006: WebVPN Citrix SOCKS errors.
- %Threat Defense-7-723007: WebVPN Citrix ICA connection connection list is broken.
- %Threat Defense-7-723008: WebVPN Citrix ICA SOCKS Server server is invalid.
- %Threat Defense-7-723009: Group group-name, User user-name, IP IP_address: WebVPN Citrix received data on invalid connection connection.
- %Threat Defense-7-723010: Group group-name, User user-name, IP IP_address: WebVPN Citrix received closing channel channel for invalid connection connection.
- %Threat Defense-7-723011: Group group-name, User user-name, IP IP_address: WebVPN Citrix receives bad SOCKS socks message length msg-length. Expected length is exp-msg-length.
- %Threat Defense-7-723012: Group group-name, User user-name, IP IP_address: WebVPN Citrix received bad SOCKS socks message format.
- %Threat Defense-7-723013: WebVPN Citrix encountered invalid connection connection during periodic timeout.
- %Threat Defense-7-723014: Group group-name, User user-name, IP IP_address: WebVPN Citrix TCP connection connection to server server on channel channel initiated.
- %Threat Defense-7-725008: SSL peer-type interface:src-ip/src-port to dst-ip/dst-port proposes the following n cipher(s).
- %Threat Defense-7-725009: Device proposes the following n cipher(s) peer-type interface:src-ip/src-port to dst-ip/dst-port.
- %Threat Defense-7-725010: Device supports the following n cipher(s).
- %Threat Defense-7-725011: Cipher[order]: cipher_name
- %Threat Defense-7-725012: Device chooses cipher cipher for the SSL session with peer-type interface:src-ip/src-port to dst-ip/dst-port.

重大度別システムヘルスおよびネットワーク診断メッセージリスト

- %Threat Defense-7-725013: SSL peer-type interface:src-ip/src-port to dst-ip/dst-port chooses cipher cipher
- %Threat Defense-7-725014: SSL lib error. Function: function Reason: reason
- %Threat Defense-7-725017: No certificates received during the handshake with %s %s:%B/%d to %B/%d for %s session
- %FTD-7-725021: Device preferring cipher-suite cipher(s). Connection info: interface :src-ip /src-port to dst-ip /dst-port
- %FTD-7-725022: Device skipping cipher : cipher - reason. Connection info: interface :src-ip /src-port to dst-ip /dst-port
- %Threat Defense-7-730002: Group groupname, User username, IP ipaddr: VLAN MAPPING to VLAN vlanid failed
- %Threat Defense-7-734003: DAP: User name, Addr ipaddr: Session Attribute: attr name/value
- %Threat Defense-7-737001: IPAA: Received message ‘message-type’
- %Threat Defense-7-737035: IPAA: Session=<session>, '<message type>' message queued
- %FTD-7-737200: VPNFIP: Pool=pool, Allocated ip-address from pool
- %FTD-7-737201: VPNFIP: Pool=pool, Returned ip-address to pool (recycle=recycle)
- %FTD-7-737206: VPNFIP: Pool=pool, DEBUG: message
- %FTD-7-737400: POOLIP: Pool=pool, Allocated ip-address from pool
- %FTD-7-737401: POOLIP: Pool=pool, Returned ip-address to pool (recycle=recycle)
- %FTD-7-737407: POOLIP: Pool=pool, DEBUG: message
- %Threat Defense-7-747005: Clustering: State machine notify event event-name (event-id, ptr-in-hex, ptr-in-hex)
- %Threat Defense-7-747006: Clustering: State machine is at state state-name
- %Threat Defense-7-751003: Local: localIP:port Remote:remoteIP:port Username: username/group Need to send a DPD message to peer
- %Threat Defense-7-752002: Tunnel Manager Removed entry. Map Tag = mapTag. Map Sequence Number = mapSeq.
- %Threat Defense-7-752008: Duplicate entry already in Tunnel Manager.
- %Threat Defense-7-785001: Clustering: Ownership for existing flow from <in_interface>:<src_ip_addr>/<src_port> to <out_interface>:<dest_ip_addr>/<dest_port> moved from unit <old-owner-unit-id> at site <old-site-id> to <new-owner-unit-id> at site <old-site-id> due to <reason>.

Syslog メッセージで使用される変数

多くの場合、syslog メッセージには変数が含まれています。次の表に、syslog メッセージを説明するためにこのガイドで使用されているほとんどの変数を示します。1 つの syslog メッセージにしか現れない変数の中には省略したものがあります。

syslog メッセージの変数フィールド

変数	説明
acl_ID	ACL 名。
bytes	バイト数。
code	syslog メッセージによって返される 10 進数。生成される syslog メッセージに応じて、エラーの原因または発生源を示します。
command	コマンド名。
command_modifier	**command_modifier** は、次の文字列のいずれかです。 • cmd（この文字列は、コマンドに修飾子がないことを意味します） • clear • no • show
connections	接続数。
connection_type	接続タイプは次のとおりです。 • SIGNALLING UDP • SIGNALLING TCP • SUBSCRIBE UDP • SUBSCRIBE TCP • Via UDP • Route • RTP • RTCP
dec	10 進数
dest_address	パケットの宛先アドレス。
dest_port	宛先ポート番号。

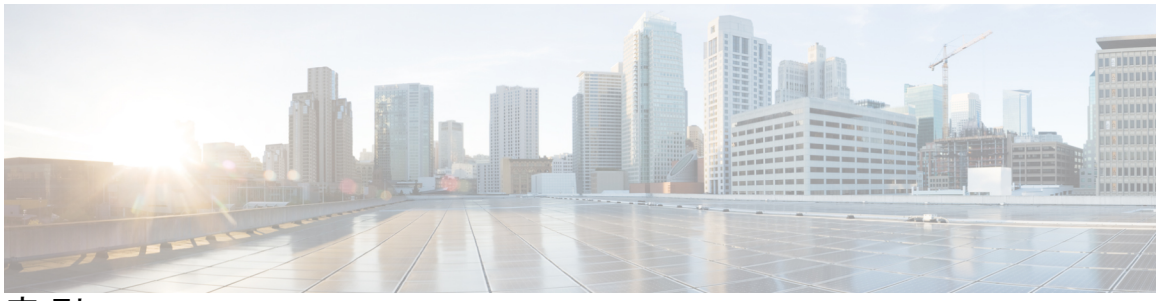
重大度別システムヘルスおよびネットワーク診断メッセージリスト

変数	説明
device	メモリ ストレージデバイス。たとえば、フロッピーディスク、内部フラッシュ メモリ、TFTP、フェールオーバー スタンバイ装置、またはコンソール端末です。
econns	初期接続数。
elimit	**static** コマンドまたは **nat** コマンドで指定された初期接続数。
filename	ASAimageタイプ、ASDMファイル、またはコンフィギュレーションのファイル名。
ftp-server	外部 FTP サーバー名または IP アドレス。
gateway_address	ネットワーク ゲートウェイ IP アドレス。
global_address	グローバル IP アドレス。セキュリティ レベルの低いインターフェイス上のアドレスです
global_port	グローバル ポート番号。
hex	16 進数
inside_address	内部（つまり、ローカル）IP アドレス。高セキュリティ レベル インターフェイス上のアドレス。
inside_port	内部ポート番号。
interface_name	インターフェイスの名前。
IP_address	IP アドレス。形式は *n n n n* で、*n* は 1 ～ 255 の整数です。
MAC_address	MAC アドレス。
mapped_address	変換済み IP アドレス。
mapped_port	変換済みポート番号。
message_class	ASA の機能エリアに関連付けられている syslog メッセージのカテゴリ。
message_list	syslog メッセージの ID 番号、クラス、または重大度のリストを含む作成ファイルの名前。
message_number	syslog メッセージ ID。
nconns	static テーブルまたは xlate テーブルに許可された接続数。
netmask	サブネット マスク。
number	数字。正確な形式は、syslog メッセージによって決まります。

重大度別システムヘルスおよびネットワーク診断メッセージリスト

変数	説明
octal	8 進数
outside_address	外側（つまり、外部）IPアドレス。通常は、外部ルータの先のネットワークにある低セキュリティ レベル インターフェイス上の syslog サーバーのアドレス。
outside_port	外部ポート番号。
port	TCP または UDP ポート番号。
privilege_level	ユーザー特権レベル。
protocol	パケットのプロトコル。たとえば、ICMP、TCP、または UDP。
real_address	NAT 前の実 IP アドレス。
real_port	NAT 前の実ポート番号。
reason	syslog メッセージの理由を記述するテキスト文字列。
service	パケットで指定されたサービス。たとえば、SNMP または Telnet。
severity_level	syslog メッセージの重大度。
source_address	パケットのソース アドレス。
source_port	ソース ポート番号。
string	テキスト文字列（ユーザー名など）
tcp_flags	TCP ヘッダー内のフラグ。たとえば、次に示すものです。 • ACK • FIN • PSH • RST • SYN • URG
time	継続時間（*hh mm ss* 形式）
url	URL。
user	ユーザー名。

重大度別システムヘルスおよびネットワーク診断メッセージリスト



索 引

数字

A

C

D

E

F

H

I

L

M

O

P

R

S

T

U

V

W

X

あ

い

く

さ

し

す

せ

そ

た

て

は

ひ

ふ

ほ

め

ゆ

り

る

ろ

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。