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 *1 : 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。

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。