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 （1 ページ）
- メッセージ 211001 ～ 219002 （10 ページ）

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。

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。