GETVPN 復元力 GM - エラー検出

GETVPN 復元力 - GM エラー検出機能では、無効なステートフル パケット インスペクション（SPI）または時間ベースのアンチリプレイ（TBAR）エラーなど、各グループ ドメイン オブ インタープリテーション（GDOI）のデータ プレーンで異常なパケットを検出します。これらのエラーは追跡され、パケットの外部送信元 IP アドレスが記録されます。

GETVPN の復元力：GM のエラー検出に関する情報

エラー処理

エラー処理を機能させるには、GM と KS の両方で GETVPN の復元力（GM のエラー検出の機能）を有効にする必要があります。KS は、SPI（セキュリティ パラメータ インデックス）のグループ情報をエンコードし、TEK ポリシーを介してそれを GM にダウンロードします。

GETVPN 復元力 - GM エラー検出機能によって障害が検出されると、異常なパケットの送信元 IP アドレスを示す syslog メッセージが生成されます。

```
 *Feb 10 21:01:56.043:
%GDOI-4-TIMEBASED_REPLAY_FAILED: An anti replay check has failed in
group GETVPN from sourceip-address
100.0.0.9.
 my_pseudotime is 600006.78 secs,
peer_pseudotime is 500033.34 secs, replay_window is 100
(second)
 *Feb 10 21:01:56.043:
%CRYPTO-4-PKT_REPLAY_ERR: decrypt: replay check failed
 connection id=29, sequence
number=11
```

show crypto gdoi gm コマンドは、直近の 50 個の時間ベースのアンチリプレイ（TBAR）エラーの履歴を表示します。これらの送信元 IP アドレス レコードを使用すると、送信者グループ メ

ンバー（GM）を突き止め、既存のハードウェアまたはソフトウェアの問題を調査することができます。次の統計情報もコマンドで利用できます。

- GM リカバリ機能のオン/オフ
- リカバリの間隔
- 適用される GM リカバリの再登録の数

エラーが発生すると、GM は次に使用可能なキー サーバ（KS）に再登録し、最新のポリシーとキーを取得し、登録が完了するまで以前にダウンロードされたすべてのグループ ポリシーとキーを維持します。

たとえば、連携キーサーバ（COOP KS）の分割が発生すると、レベルを上げられた各 KS が独自の Key Encryption Key（KEK）とトラフィック暗号化キー（TEK）を生成します。GM は、無効な SPI パケットを受信すると、それをデコードします（KS は SPI のグループ情報をエンコードし、TEK ポリシーを介してそれを GM にダウンロードします）。それが現在の GETVPN グループに属していることが判明した場合は、リカバリ登録を開始します。

無効な SPI は、次の 2 つのカテゴリのいずれかに属している可能性があります。

- 正の無効な SPI：現在のグループに属しており、GM リカバリ登録が必要な、無効な SPI。
- 負の無効な SPI：リカバリ登録を必要としない無効な SPI。

正の無効な SPI の場合、リスト内の次のキーサーバー（KS）へのリカバリ登録が実行されます。このリカバリ登録は、リスト内の次の KS への各クライアント リカバリ間隔で、無効なステートフル パケット インスペクション（SPI）パケットまたは TBAR エラーごとに繰り返されます。リスト内のすべての KS が回復され、無効な SPI が含まれなくなると、その SPI は誤検出としてマークされ、それ以上のリカバリ登録は実行されません。KS は TBAR エラーに対して常にリカバリ登録を実行します。ただし、無効な SPI のために GM がリストのすべての KS を回復し、SPI がある KS がなくなると、その SPI は誤検出としてマークされ、その SPI のためにさらにリカバリ登録が実行されることはなくなります。

この GM リカバリの再登録機能がトリガーされたことを通知するため、syslog メッセージが生成されます。たとえば、GM が 300 秒ごとにコントロール プレーンのエラーをモニタするように設定している場合、リカバリ登録が発生すると、次の syslog が生成されます。

```
*Feb 23 19:06:28.600: %GDOI-5-GM_RECOVERY_REGISTER: received invalid GDOI packets;
register to KS to refresh policy, keys, and PST.
```

GETVPN の復元力：GM のエラー検出の設定方法

GETVPN の復元力：GM のエラー検出の設定

手順の概要

1. **crypto gdoi group** *group-name*
2. **identity number** *number*

3. **server address ipv4** *address*
4. **client recovery-check interval** *interval*
5. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**crypto gdoi group** *group-name* 例： `Device(config)# crypto gdoi group GETVPN`	グループ ドメイン オブ インタープリテーション（GDOI）グループを作成し、GDOI グループ コンフィギュレーション モードを開始します。
ステップ 2	**identity number** *number* 例： `Device(config-gdoi-group)# identity number 1111`	GDOI グループ番号を指定します。
ステップ 3	**server address ipv4** *address* 例： `Device(config-gdoi-group)# server address ipv4 1.0.0.2`	GDOI グループが到達しようとするサーバの IP アドレスを指定します。
ステップ 4	**client recovery-check interval** *interval* 例： `Device(config-gdoi-group)# client recovery-check interval 300`	コントロール プレーンを監視するクライアント グループ メンバー（GM）の時間間隔を設定します。
ステップ 5	**exit** 例： `Device(config-gdoi-group)# exit`	GDOI グループ コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。

GETVPN の復元力：GM のエラー検出の設定例

例：GETVPN の復元力：GM のエラー検出の設定

次の例は、グループ メンバー（GM）が 300 秒ごとにコントロール プレーンのエラーを監視できるようにする方法を示します。

```
crypto gdoi group GETVPN
 identity number 1111
 server address ipv4 1.0.0.2
 client recovery-check interval 300
```

GETVPN の復元力：GM のエラー検出その他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS セキュリティ コマンド	『*Cisco IOS Security Command References*』
エンタープライズ ネットワークの GET VPN の有効化のための基本的な導入ガイドライン	『*Cisco IOS GET VPN Solutions Deployment Guide*』
GET VPN ネットワークの設計と実装	『*Group Encrypted Transport VPN (GETVPN) Design and Implementation Guide*』

標準および RFC

標準/RFC	タイトル
RFC 6407	『*The Group Domain of Interpretation*』

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

GETVPN の復元力：GM のエラー検出の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *1 : GETVPN* の復元力：*GM* のエラー検出の機能情報

機能名	リリース	機能情報
GETVPN の復元力：GM のエラー検出		各 GDOI グループのデータ プレーンのエラー パケットを検出します。 次のコマンドが導入されました。 **client recovery-check interval.**

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。