GET VPN GM の削除とポリシー トリガー

GET VPN GM の削除とポリシー トリガー機能では、グループ暗号化トランスポート（GET）VPN ネットワークから不要なグループ メンバー（GM）を簡単に削除できます。新しいセキュリティ アソシエーション（SA）をインストールし、古い SA を削除するキー再生成トリガーの方法を提供します。また、デバイスがこれらの機能をサポートする GET VPN ソフトウェアのバージョンを実行しているかどうかを確認することができます。

GM の削除とポリシー トリガーに関する情報

GET VPN のソフトウェア バージョン

GET VPN のソフトウェア バージョンは次の形式です。

major-version.minor-version.mini-version

値は次のとおりです。

- *major-version* は、すべての GET VPN デバイスの互換性を定義します。
- *minor-version* は、キー サーバ（KS）/KS 間（連携キー サーバ）の関係と GM/GM 間の相互運用性に関する互換性を定義します。
- *mini-version* は、互換性に影響しない機能変更を追跡します。

たとえば、基本バージョン（以前のすべての GET VPN 機能）は 1.0.1 です。また、たとえば GM の削除機能とポリシー交換機能が含まれるバージョンは 1.0.2 である場合、これらの機能は（トリガーされるキー再生成でのこれらの機能の動作導入に関係なく）基本バージョンと完全な後方互換性があることを意味します。

GM はインターネット キー エクスチェンジ（IKE）フェーズ 1 ネゴシエーション（RFC 2408、『*Internet Security Association and Key Management Protocol [ISAKMP]*』で定義されています）の間にベンダー ID ペイロードで KS に GET VPN ソフトウェア バージョンを送信します。KS は、連携 KS 通知（ANN）メッセージのバージョン フィールドで他の連携 KS にソフトウェア バージョンを送信します。連携 KS も、各 GM が使用しているバージョンのリストを同期します。

GM 削除機能とポリシー交換機能はそれぞれ、その機能をサポートしていないグループのデバイスを検出するために KS（またはプライマリ KS）で実行するコマンドを提供しています。

GM の削除

GM の削除とポリシー交換機能がないとき、グループから不要な GM を削除するには、次の手順を実行する必要があります。

1. フェーズ 1 のクレデンシャル（たとえば、事前共有キーまたは 1 つ以上の PKI 証明書）を失効にします。
2. KS のトラフィック暗号キー（TEK）および Key Encryption Key（KEK）データベースをクリアします。
3. 各 GM で TEK および KEK データベースを個別にクリアし、強制的に各 GM を再登録します。

GET VPN グループが数千の GM にサービスを提供しているとき、機能させるとき、3 番目のステップには時間がかかります。また、実稼動ネットワークのグループ全体をクリアすると、ネットワーク中断を引き起こす可能性があります。GET VPN GM 削除機能とポリシー トリガー機能では、KS（またはプライマリ KS）で入力したコマンドを使用して新たな一連の TEK および KEK キーを作成し、それらを GM に伝播することによって、このプロセスを自動化します。

他の GET VPN ソフトウェア バージョンとの GM 削除の互換性

GET VPN の GM 削除およびポリシー トリガー機能は、GET VPN ネットワークのすべてのデバイスがこの機能をサポートする GET VPN ソフトウェア バージョンにアップグレードされた後にのみ使用する必要があります。そうしないと、古いソフトウェアを実行しているセカンダリ KS または GM が GM の削除メッセージを無視し、古い SA を使用してトラフィックの暗号化と復号化を続行します。この動作により、ネットワーク トラフィックの中断が発生します。

この機能には、ネットワークのすべてのデバイスが GM の削除をサポートするバージョンを実行しているかどうかを確認するために KS（またはプライマリ KS）で使用するコマンドが用意されています。プライマリ KS が GM の削除をサポートしていないデバイスを含むネットワークの GM を削除しようとすると、警告メッセージが表示されます。詳細については、「GM の削除をサポートするソフトウェア バージョンを GM が実行していることを確認する」セクションを参照してください。

一時的な IPsec SA による GM の削除

GET VPN GM の削除とポリシー トリガー機能には、一時的な IPsec SA により GM の削除をトリガーするためにKS（またはプライマリKS）で使用するコマンドが用意されています。この動作により、すべてのGMのキーのライフタイムが短縮され、キーの有効期限が切れる前に再登録します。GM の削除の間、ライフタイムが期限切れになるまで一時的なIPsec SA を使用してトラフィックの暗号化と復号化が継続されるため、ネットワーク中断は発生しません。詳細については、「一時的な IPsec SA による GM の削除」セクションを参照してください。

即時の IPsec SA 削除による GM の削除

GET VPN GM の削除とポリシー トリガー機能では、GM が強制的に古い TEK と KEK を（一時的な SA を使用せず）即座に削除し、再登録するために KS（またはプライマリ KS）で使用できるオプションのキーワードを提供します。ただし、この動作により、データプレーンに中断が引き起こされる可能性があります。そのため、重大なセキュリティ上の理由がある場合のみこの方式を使用する必要があります。詳細については、「GMの削除とIPSecSAの即座の削除」セクションを参照してください。

ポリシーの交換とキー再生成のトリガー

GET VPN GM 削除およびポリシー トリガー機能では、古い SA を削除し、新しい SA をインストールするための新しいキー再生成トリガー方法を提供します。

キー再生成をトリガーする TEK および KEK ポリシー変更に関する不整合

この機能なしでは、キー再生成をトリガーする TEK および KEK ポリシー変更に関して不整合があります。

- セキュリティ ポリシーの更新中に複数のキー再生成が送信される可能性があります。
- 一部のポリシー変更は（たとえば、トランスフォームセット、プロファイル、ライフタイム、およびアンチリプレイ）新しい SA を GM にインストールしますが、既存のポリシーからの SA はライフタイムが期限切れになるまでアクティブのままになります。
- 一部のポリシー変更（たとえば、TEK のアクセス コントロール エントリ/アクセス コントロール リスト（ACE/ACL）の変更）は新しい SA を GM にインストールし、即座に有効になります。ただし、古い SA は各 GM のデータベースで維持されます（ライフタイムが期限切れになるまで **show crypto ipsec sa** コマンドを使用して表示できます）。

たとえば、KS が Data Encryption Standard（DES）から Advanced Encryption Standard（AES）にポリシーを変更する場合、GM がこのトリガーされたキー再生成を受け取ると、新しい SA（例：AES）がインストールされ、古いSA（例：DES）のライフタイムは短縮されます。GM は短縮されたライフタイムが期限切れになるまで古い SA を使用してトラフィックの暗号化と復号化を継続します。

次に、短縮されたライフタイムを計算する式を示します。

TEK_SLT = MIN(TEK_RLT, MAX(90s, MIN(5%(TEK_CLT), 3600s)))

値は次のとおりです。

- TEK_SLT は TEK の短縮されたライフタイムです。
- TEK_RLT は TEK の残りのライフタイムです。
- TEK_CLT は TEK の設定されたライフタイムです。

次の表は、キー再生成に関する不整合をまとめたものです。

表 *1:* セキュリティ ポリシー変更後のキー再生成の動作

ポリシーの変更	キー再生成を送信するか	ポリシー変更後のキー再生成の動作
TEK：SA ライフタイム	No	古い SA は、そのライフタイムが期限切れになるまでアクティブのままになります。新しいライフタイムは、次にスケジュールされたキー再生成の後に有効になります。**clear crypto sa** コマンドを入力しても、古いライフタイムを使用して再登録され、古い SA が再度ダウンロードされます。
TEK：IPSEC トランスフォーム セット	Yes	古いトランスフォーム セットの SA は、そのライフタイムが期限切れになるまでアクティブのままになります。
TEK：IPSEC プロファイル	Yes	古いプロファイルの SA は、そのライフタイムが期限切れになるまでアクティブのままになります。
TEK：一致する ACL	Yes	発信パケット分類ですぐに ACL が使用されます。ただし、古い SA は SA データベースに残ります（**show crypto ipsec sa** コマンドを使用して表示できます）。
TEK：リプレイ カウンタのイネーブル化	Yes	ただし、カウンタ リプレイがない古い SA は、そのライフタイムが期限切れになるまでアクティブのままになります。
TEK：リプレイ カウンタ値の変更	No	新しいリプレイ カウンタがある SA は、次にスケジュールされたキー再生成時に送信されます。
TEK：リプレイ カウンタのディセーブル化	Yes	ただし、カウンタ リプレイがイネーブルになっている古い SA は、そのライフタイムが期限切れになるまでアクティブのままになります。
TEK：TBAR の有効化	Yes	ただし、時間ベースのアンチリプレイ（TBAR）が無効になった古い SA は、そのライフタイムが期限切れになるまでアクティブのままになります。

ポリシーの変更	キー再生成を送信するか	ポリシー変更後のキー再生成の動作
TEK：TBAR ウィンドウの変更	No	新しい TBAR ウィンドウがある SA は、次にスケジュールされたキー再生成時に送信されます。
TEK：TBAR の無効化	Yes	ただし、TBAR がイネーブルになっている古い SA は、そのライフタイムが期限切れになるまでアクティブのままになります。
TEK：受信専用のイネーブル	Yes	受信専用モードは、キー再生成後ただちにアクティブになります。
TEK：受信専用のディセーブル	Yes	受信専用モードは、キー再生成後ただちに非アクティブになります。
KEK：SA ライフタイムの動作	No	変更は次のキー再生成時に適用されます。
KEK：認証キーの変更	Yes	変更は即時に適用されます。
KEK：暗号アルゴリズムの変更	Yes	変更は即時に適用されます。

この機能では、一貫性を確保することで、これらの問題を解決します。この機能によって、GET VPN ポリシーの変更単独ではキー再生成がトリガーされなくなります。ポリシー（およびグローバル コンフィギュレーション モードの終了）を変更すると、ポリシーが変更され、キー再生成が必要であることを示す syslog メッセージがプライマリ KS に表示されます。この機能には、（実行コンフィギュレーションの最新のセキュリティポリシーに基づく）キー再生成を送信するために KS（またはプライマリ KS）で入力する新しいコマンドが用意されています。

この機能ではまた、古い TEK および KEK を即座に削除し、新しい TEK および KEK をインストールするようにキー再生成を受信する GM に強制する追加のキーワードを新しいコマンドに用意しています。そのため、新しいポリシーは古い SA ポリシーが期限切れになるのを待たずにただちに反映されます。（ただし、すべての GM が同時にキー再生成メッセージを受信しない場合があるため、このキーワードを使用すると、一時的なトラフィックの切断が発生する可能性があります）。

ポリシーの交換およびキー再生成のトリガーの他の GET VPN ソフトウェア バージョンとの互換性

キー再生成のトリガーは、GET VPN ネットワーク内のすべてのデバイスをこの機能をサポートする GET VPN ソフトウェア バージョンにアップグレードしてから使用する必要があります。**crypto gdoi ks** コマンドをまだサポートしていない古いバージョンを実行している GM では、プライマリ KS はソフトウェアバージョン管理機能を使用してこれらのバージョンを検出し、ポリシー交換のための命令を送信せずにキー再生成のトリガーのみ実行します。したがっ

て、GM がキー再生成を受信すると、新しい SA をインストールしますが、古い SA の有効期間は短縮しません。（この動作は以前のキー再生成メソッドと同様であり、ポリシーの交換をサポートしないデバイスの後方互換性が確保されます。）

この機能は、ネットワークのすべてのデバイスがポリシーの交換をサポートするバージョンを実行しているかどうかを確認するためにKS（またはプライマリ KS）で使用するコマンドを提供します。詳細については「GM がポリシーの交換をサポートするソフトウェア バージョンを実行していることを確認する」セクションを参照してください。

GET VPN GM 削除およびポリシー トリガーの設定方法

GM の削除をサポートするソフトウェア バージョンを GM が実行していることを確認する

GET VPN の GM 削除およびポリシー トリガー機能は、GET VPN ネットワークのすべてのデバイスがこの機能をサポートする GET VPN ソフトウェア バージョンにアップグレードされた後にのみ使用する必要があります。そうしないと、古いソフトウェアを実行しているセカンダリ KS または GM が GM 削除メッセージを無視して、古い SA を使用するトラフィックの暗号化および復号化を継続します。この動作により、ネットワーク トラフィックの中断が発生します。

ネットワーク内のすべてのデバイスが GM 削除をサポートすることを確認するには、KS（またはプライマリ KS）でこの作業を実行します。

手順の概要

1. **enable**
2. **show crypto gdoi feature gm-removal**
3. **show crypto gdoi feature gm-removal | include No**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**show crypto gdoi feature gm-removal** 例： `Device# show crypto gdoi feature gm-removal`	GET VPN ネットワーク内の各 KS および GM で実行されている GET VPN ソフトウェアのバージョンを表示し、そのデバイスが GM 削除をサポートしているかどうかを表示します。

	コマンドまたはアクション	目的
ステップ 3	**show crypto gdoi feature gm-removal | include No** 例： `Device# show crypto gdoi feature gm-removal | include No`	（オプション）GM 削除をサポートしないデバイスのみ表示します。

一時的な IPsec SA による GM の削除

一時的な IPsec SA の GM の削除をトリガーするには、KS（またはプライマリ KS）でこの作業を実行します。

手順の概要

1. **enable**
2. **clear crypto gdoi** [**group** *group-name*] **ks members**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**clear crypto gdoi** [**group** *group-name*] **ks members** 例： `Device# clear crypto gdoi ks members`	新しい TEK および KEK キーのセットを作成します。またこのコマンドは、すべての GM に古い TEK および KEK データベースをクリーンアップするための GM 削除メッセージも送信します。

例

KS に次のようにメッセージが表示されます。

```
Device# clear crypto gdoi ks members

% This GM-Removal message will shorten all GMs' key lifetimes and cause them to
re-register before keys expiry.
Are you sure you want to proceed? ? [yes/no]: yes
Sending GM-Removal message to group GET...
```

各 GM が GM 削除メッセージを受信すると、次の syslog メッセージが各 GM に表示されます。

```
*Jan 28 08:37:03.103: %GDOI-4-GM_RECV_DELETE: GM received delete-msg from KS in group
GET.
TEKs lifetime are reduced and re-registration will start before SA expiry
```

各 GM は KEK を即時削除し、次のように古い TEK のライフタイムを短縮します。

```
TEK_SLT = MIN(TEK_RLT, MAX(90s, MIN(5%(TEK_CLT), 3600s)))
TEK_SLT: TEK shortened lifetime
TEK_RLT: TEK Remaining LIfeTime
TEK_CLT: TEK Configured LIfeTime
```

また GM は、従来の再登録タイマーに従いジッター（ランダムな遅延）が適用された新しい TEK と KEK を取得するために KS への再登録を開始します。ジッターは、すべての GM が同時に再登録してキー サーバの CPU に過負荷を与えることを防ぎます。KS にインストールされた新しいクレデンシャルに基づいて認証を通す GM だけが新しい TEK と KEK を受信します。

トラフィックはライフタイムが期限切れになるまで一時的な IPsec SA を使用して暗号化と復号化を続けるため、GM 削除によってネットワークの中断が発生することはありません。

セカンダリ KS でこのコマンドを使用しようとすると、次のように拒否されます。

```
Device# clear crypto gdoi ks members

ERROR for group GET: can only execute this command on Primary KS
```

GM の削除と IPSec SA の即時削除

古い TEK と KEK を即時削除して再登録するように GM に強制するには KS（またはプライマリ KS）でこの作業を実行します。

手順の概要

1. **enable**
2. **clear crypto gdoi** [**group** *group-name*] **ks members now**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**clear crypto gdoi** [**group** *group-name*] **ks members now** 例： `Device# clear crypto gdoi ks members now`	新しい TEK および KEK キーのセットを作成します。またこのコマンドは、すべての GM に古い TEK および KEK データベースをクリーンアップするための GM 削除メッセージも送信します。 （注） **now** キーワードの使用により、データプレーンにネットワーク中断が発生することがあります。セキュリティに関する問題が中断よりも重要である場合にのみ、GM 削除を進めます。

例

KS に次のようにメッセージが表示されます。

```
Device# clear crypto gdoi ks members now

% This GM-Removal immediate message will cleanup all GMs downloaded policies
% This will cause all GMs to re-register.
Are you sure you want to proceed? ? [yes/no]: yes
Sending GM-Removal message to group GET...
```

上記のコマンドの入力後、KS は、各 GM の次のアクションをトリガーするために「remove now」メッセージを各 GM に送信します。

1. ダウンロードされたTEKおよびKEKならびにそのポリシーがすぐにクリーンアップされ、（明示的にフェールクローズ モードが設定されていない限り）フェールオープン モードに戻ります。
2. 設定されている TEK ライフタイムの 2 パーセント以内のランダムに選択された期間でタイマーを設定します。
3. ステップ 2 のタイマーの期限が切れると、GM は新しい TEK および KEK をダウンロードするために KS への再登録を開始します。

各 GM では、GM がランダムな期間内に再登録されることを示すために次の syslog メッセージが表示されます。

```
*Jan 28 08:27:05.627: %GDOI-4-GM_RECV_DELETE_IMMEDIATE: GM receive REMOVAL-NOW in group

GET to cleanup downloaded policy now. Re-registration will start in a randomly chosen
period of 34 sec
```

GM 削除をサポートしていないデバイスを含むネットワークの GM を削除しようとすると、警告メッセージが表示されます。

```
Device# clear crypto gdoi ks members now

% This GM-Removal immediate message will cleanup all GMs downloaded policies
% This will cause all GMs to re-register.
Are you sure you want to proceed? ? [yes/no]: yes
WARNING for group GET: some devices cannot support GM-REMOVAL and can cause network
disruption. Please check 'show crypto gdoi feature'.
Are you sure you want to proceed ? [yes/no]: no
```

GM がポリシーの交換をサポートするソフトウェア バージョンを実行していることを確認する

ネットワーク内のすべてのデバイスがポリシーの交換をサポートするかどうかを確認するには、KS（またはプライマリ KS）でこの作業を実行します。

手順の概要

1. **enable**

2. **show crypto gdoi feature policy-replace**
3. **show crypto gdoi feature policy-replace | include No**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**show crypto gdoi feature policy-replace** 例： `Device# show crypto gdoi feature policy-replace`	GET VPN ネットワーク内の各 KS および GM で実行されている GET VPN ソフトウェアのバージョンを表示し、そのデバイスがポリシーの交換をサポートしているかどうかを表示します。
ステップ 3	**show crypto gdoi feature policy-replace | include No** 例： `Device# show crypto gdoi feature policy-replace | include No`	（オプション）ポリシーの交換をサポートしないデバイスのみ検索します。これらのデバイスでは、プライマリ KS はポリシー交換に関する手順なしでトリガーされるキー再生成のみを送信します。したがって、GM がキー再生成を受信すると、新しい SA をインストールしますが、古い SA の有効期間は短縮しません。この動作は既存のキー再生成メソッドと同じであり後方互換性があります。

キー再生成のトリガー

KS（またはプライマリ KS）でセキュリティ ポリシーを変更し（たとえば、DES から AES）、グローバル コンフィギュレーション モードを終了すると、ポリシーが変更され、キー再生成が必要であることを示す syslog メッセージが KS に表示されます。実行コンフィギュレーションの最新のポリシーに基づくキー再生成を送信するために、次のようにキー再生成をトリガーするコマンドを入力します。

キー再生成をトリガーするには KS（プライマリ KS）でこの作業を実行します。

手順の概要

1. **enable**
2. **crypto gdoi ks** [**group** *group-name*] **rekey** [**replace-now**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例：	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
	`Device> enable`	
ステップ 2	**crypto gdoi ks** [**group** *group-name*] **rekey** [**replace-now**] 例： `Device# crypto gdoi ks group mygroup rekey`	すべての GM のキー再生成をトリガーします。 オプションの **replace-now** キーワードは、各 GM の古い TEK および KEK を即時に置き換え、SA が期限切れになる前に新しいポリシーを有効にします。 （注） **replace-now** キーワードを使用すると、一時的なトラフィックの不連続を引き起こすことがあります。

例

KS に次のようにメッセージが表示されます。

```
Device# crypto gdoi ks rekey
Device#
*Jan 28 09:17:44.363: %GDOI-5-KS_SEND_UNICAST_REKEY: Sending Unicast Rekey with
policy-replace for group GET from address 10.0.8.1 with seq # 2
```

ポリシーの変更後、各 GM がこのトリガーされたキー再生成を受信すると、新しい SA（たとえば、AES 用）をインストールして、古い SA（たとえば、DES 用）のライフタイムを短縮します。各 GM はこの短縮されたライフタイムが期限切れになるまで古い SA を使用してトラフィックの暗号化および復号化を続けます。

セカンダリ KS のキー再生成をトリガーしようとすると、次のようにコマンドが拒否されます。

```
Device# crypto gdoi ks rekey
ERROR for group GET: This command must be executed on Pri-KS
```

GET VPN GM の削除とポリシーのトリガーの設定例

例：GET VPN ネットワークからの GM の削除

GM の削除をサポートするソフトウェア バージョンを GM が実行していることを確認する

次の例は、ネットワーク内のすべてのデバイスが GM 削除機能をサポートしているかどうかを確認するために KS（またはプライマリ KS）で GET VPN ソフトウェア バージョン管理コマンドを使用する方法を示します。

```
Device# show crypto gdoi feature gm-removal
```

```
Group Name: GET
 Key Server ID       Version   Feature Supported
    10.0.8.1         1.0.2          Yes
    10.0.9.1         1.0.2          Yes
    10.0.10.1        1.0.2          Yes
    10.0.11.1        1.0.2          Yes
 Group Member ID     Version   Feature Supported
    10.0.0.2         1.0.2          Yes
    10.0.0.3         1.0.1          No
```

次の例は、GMの削除をサポートしていないデバイスのみを検索する方法を示します。

```
Device# show crypto gdoi feature gm-removal | include No

       10.0.0.3          1.0.1          No
```

上記の例では、IP アドレス 10.0.0.3 の GM は（GM の削除をサポートしない）古いソフトウェア バージョン 1.0.1 を実行中であり、アップグレードする必要があることを示しています。

一時的な IPsec SA による GM の削除

次の例では、一時的な IPsec SA を使用する GM の削除をトリガーする方法を示します。KS（またはプライマリ KS）でこのコマンドを使用します。

```
Device# clear crypto gdoi ks members

% This GM-Removal message will shorten all GMs' key lifetimes and cause them to
re-register before keys expiry.
Are you sure you want to proceed? ? [yes/no]: yes
Sending GM-Removal message to group GET...
```

GM の削除と IPSec SA の即時削除

次の例は、古い TEK と KEK を即座に削除して再登録するために GM を強制適用する方法を示しています。KS（またはプライマリ KS）でこのコマンドを使用します。

```
Device# clear crypto gdoi ks members now

% This GM-Removal immediate message will cleanup all GMs downloaded policies
% This will cause all GMs to re-register.
Are you sure you want to proceed? ? [yes/no]: yes
Sending GM-Removal message to group GET...
```

例：グループ メンバーのキー再生成のトリガー

GM がキー再生成のトリガーをサポートするソフトウェア バージョンを実行していることを確認する

次の例は、GET VPN ネットワークのデバイスのソフトウェアのバージョンを表示し、またポリシー変更後のキー再生成のトリガーをサポートするかどうかを表示するために、KS（またはプライマリ KS）で GET VPN ソフトウェア バージョン管理コマンドを使用する方法を示します。

```
Device# show crypto gdoi feature policy-replace

Key Server ID       Version  Feature Supported
  10.0.8.1         1.0.2          Yes
  10.0.9.1         1.0.2          Yes
  10.0.10.1        1.0.2          Yes
  10.0.11.1        1.0.2          Yes
 Group Member ID     Version  Feature Supported
  5.0.0.2          1.0.2          Yes
  9.0.0.2          1.0.1          No
```

次の例は、ポリシー交換後のキー再生成のトリガーをサポートしていないデバイスのみを検索する方法を示します。

```
Device# show crypto gdoi feature policy-replace  | include No

       9.0.0.2          1.0.1          No
```

これらのデバイスでは、プライマリ KS はポリシー交換に関する手順なしでトリガーされるキー再生成のみを送信します。したがって、GM がキー再生成を受信すると、新しい SA をインストールしますが、古い SA の有効期間は短縮しません。

キー再生成のトリガー

次の例では、ポリシー変更の実行後にキー再生成をトリガーする方法を示します。この例では、**profile gdoi-p2** コマンドで IPSec ポリシーの変更（たとえば、DES から AES）が発生します。

```
Device# configure terminal
Device(config)# crypto gdoi group GET
Device(config-gdoi-group)# server local
Device(gdoi-local-server)# sa ipsec 1
Device(gdoi-sa-ipsec)# no profile gdoi-p
Device(gdoi-sa-ipsec)# profile gdoi-p2
Device(gdoi-sa-ipsec)# end
Device#

*Jan 28 09:15:15.527: %SYS-5-CONFIG_I: Configured from console by console
*Jan 28 09:15:15.527: %GDOI-5-POLICY_CHANGE: GDOI group GET policy has changed. Use
'crypto gdoi ks rekey' to send a rekey, or the changes will be send in the next scheduled
```

```
rekey
Device# crypto gdoi ks rekey
Device#
*Jan 28 09:17:44.363: %GDOI-5-KS_SEND_UNICAST_REKEY: Sending Unicast Rekey with
policy-replace for group GET from address 10.0.8.1 with seq # 2
```

次の例では、セカンダリ KS のキー再生成をトリガーしようとすると表示されるエラーメッセージを示します。

```
Device# crypto gdoi ks rekey

ERROR for group GET: This command must be executed on Pri-KS
```

（注） 時間ベースのアンチリプレイ（TBAR）が設定されると、キー サーバは 2 時間（7200 秒）ごとに定期的にキー再生成をグループ メンバーに送信します。次の例では、有効期間が 8 時間（28800 秒）に設定されていますが、キー再生成タイマーは 2 時間に設定されています。

```
Device(config)# crypto ipsec profile atm-profile
Device(ipsec-profile)# set security-association lifetime seconds 28800
!
Device(ipsec-profile)# exit
Device(config)# crypto gdoi group ATM-DSL
Device(config-gdoi-group)# server local
Device(gdoi-sa-ipsec)# sa ipsec 1
!
Device(gdoi-sa-ipsec)# replay time window-size 100
```

show crypto gdoi gm replay コマンドおよび **show crypto gdoi ks replay** コマンドにより TBAR 情報が表示されます。

GET VPN GM の削除とポリシーのトリガーのその他の参考資料

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*』

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

GET VPN GM の削除とポリシーのトリガーの機能情報

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 *2 : GET VPN GM* の削除とポリシーのトリガーの機能情報

機能名	リリース	機能情報
GET VPN GM の削除とポリシー トリガー		この機能は、GET VPN ネットワークから不要な GM を効率的に削除するコマンド、新しい SA をインストールして古い SA を削除するためにキー再生成をトリガーするコマンド、およびネットワーク デバイスがこれらの機能をサポートする GET VPN ソフトウェアのバージョンを実行しているかどうかを表示するコマンドを提供します。 次のコマンドが導入または変更されました。**clear crypto gdoi, crypto gdoi ks, show crypto gdoi.**

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。