GETVPN GDOI バイパス

GETVPN GDOI バイパス機能では、デフォルトのグループ ドメイン オブ インタープリテーション（GDOI）バイパス暗号化ポリシーの有効化と無効化をサポートします。また、有効にすると、デフォルト GDOI バイパス暗号化ポリシーの強化もサポートされます。

GETVPN GDOI バイパスの制約事項

キー サーバ（KS）がグループ メンバー（GM）の後ろに配置されるときは、ローカルの拒否アクセス コントロール リスト（ACL）を明示的に設定し、トランスポート プロトコルとして UDP を、送信元または宛先のいずれかとしてポート 848 を使用するトラフィック（UDP 848 トラフィック）が通過できるようにする必要があります。

GETVPN GDOI バイパスに関する情報

GDOI バイパス暗号化ポリシー

Cisco IOS の Group Encrypted Transport VPN（GETVPN）は、グループはキー管理プロトコルとしてグループ ドメイン オブ インタープリテーション（GDOI）を使用します。

グループ メンバー（GM）は暗号化と復号を担当するデバイスです。つまり、GET VPN データ プレーンを処理するデバイスです。

キー サーバ（KS）は、GET VPN コントロール プレーンを作成し、維持するデバイスです。トラフィック、暗号化プロトコル、セキュリティ アソシエーション、キー再生成タイマーなどの

すべての暗号化ポリシーは KS で一元的に定義され、登録時にすべての GM にプッシュされます。

デフォルト GDOI バイパス暗号化ポリシーの有効化と無効化

新しいグループ メンバー（GM）設定では、GM ローカル アクセス コントロール リスト（ACL）を明示的に設定することによって、ユーザはグループ ドメイン オブ インタープリテーション（GDOI）バイパス暗号化ポリシーを無効にし、トラフィックの例外を制御することができます。

デフォルト GDOI バイパス暗号化ポリシーの強化

セキュリティを強化するため、デフォルトのグループ ドメイン オブ インタープリテーション（GDOI）バイパス暗号化ポリシーを適用する一方、次の変更が実施されています。

- デフォルト GDOI バイパス暗号化ポリシーは、Group Encrypted Transport VPN（GETVPN）保護インターフェイス（GDOI 暗号マップが適用されるインターフェイス）にのみインストールされます。登録またはキー再生成に使用するグループ メンバー（GM）のアドレス宛ての UDP848 トラフィックのみが許可されます。
- GM VRF 認識型機能を使用して GDOI データ プレーンとコントロール プレーンが異なる VRF にあることを指定する場合、デフォルト GDOI バイパス暗号化ポリシーの自動挿入は GDOI 保護インターフェイスに適用されません。
- UDP をトランスポート プロトコルとして、ポート 848 を送信元または宛先（UDP 848 トラフィック）として使用するトラフィックが他の非 GDOI 保護インターフェイスに着信すると予想される場合は、非 GDOI 暗号マップの例外を明示的に設定する必要があります。
- 複数グループの暗号マップ セットを設定する場合、インストールされる全体の GDOI バイパス暗号化ポリシーは、セキュリティ アソシエーション データベース（SADB）内の各グループの GDOI バイパス暗号化ポリシーすべての統合です。

以下に説明する条件のいずれかにより、GETVPN 保護インターフェイスに適用されるデフォルト GDOI バイパス暗号化ポリシーの再計算がトリガーされます。

- **no client bypass-policy** コマンドを使用して **client bypass-policy** 設定を削除。
- インターフェイスの GDOI バイパス暗号マップの適用または削除。
- 暗号マップ セットの GDOI バイパス暗号マップの適用または削除。
- GDOI 保護インターフェイスの IP アドレスの変更（**no client registration interface** が使用される場合）。
  - **client registration interface** が使用される場合、次の場合に GETVPN 保護インターフェイスに適用されるデフォルト GDOI バイパス暗号化ポリシーの再計算がトリガーされます。
    - **no client registration interface** から **client registration interface** に変更

- クライアント登録インターフェイスに対する変更（たとえば、ループバック 0 からループバック 1）
- クライアント登録インターフェイス アドレスの変更

GETVPN GDOI バイパスの設定方法

デフォルト GDOI バイパス暗号化ポリシーの有効化

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto gdoi group** *group-name*
4. **client bypass-policy**
5. **end**

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	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**crypto gdoi group** *group-name* 例： `Device(config)# crypto gdoi group GETVPN`	GDOI グループを指定し、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 4	**client bypass-policy** 例： `Device(config-gdoi-group)# client bypass-policy`	デフォルト GDOI バイパス暗号化ポリシーを有効化します。
ステップ 5	**end** 例： `Device(config-gdoi-group)# end`	GDOI グループ コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

デフォルト GDOI バイパス暗号化ポリシーの無効化

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto gdoi group** *group-name*
4. **no client bypass-policy**
5. **end**

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	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**crypto gdoi group** *group-name* 例： `Device(config)# crypto gdoi group GETVPN`	GDOI グループを指定し、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 4	**no client bypass-policy** 例： `Device(config-gdoi-group)# no client bypass-policy`	デフォルト GDOI バイパス暗号化ポリシーを無効にします。
ステップ 5	**end** 例： `Device(config-gdoi-group)# end`	GDOI グループ コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

デフォルト GDOI バイパス暗号化ポリシーの有効性と無効性の確認

手順の概要

1. **enable**
2. **show crypto gdoi gm acl**
3. **show crypto gdoi gm acl**

手順の詳細

ステップ 1 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）。

例：

```
Device> enable
```

ステップ 2 show crypto gdoi gm acl

デフォルト GDOI バイパス暗号化ポリシーの有効性を確認します。

（注） VRF は、非グローバルである場合にのみ表示されます。

例：

```
Device# show crypto gdoi gm acl

Group Name: GETVPN
 ACL Downloaded From KS 10.0.0.2:
   access-list   deny eigrp any any
   access-list   permit ip any any
 ACL Configured Locally:
 ACL of default GDOI bypass policy:
   Ethernet1/0: deny udp host 10.0.0.9 eq 848 any eq 848 vrf RED*
```

ステップ 3 show crypto gdoi gm acl

デフォルト GDOI バイパス暗号化ポリシーの無効性を確認します。

例：

```
Device# show crypto gdoi gm acl

Group Name: GETVPN
 ACL Downloaded From KS 10.0.0.2:
   access-list   deny eigrp any any
   access-list   permit ip any any
 ACL Configured Locally:
 ACL of default GDOI bypass policy: Disabled
```

GETVPN GDOI バイパスの設定例

例：デフォルト GDOI バイパス暗号化ポリシーの有効化

```
Device> enable
Device# configure terminal
Device(config)# crypto gdoi group getvpn
```

```
Device(config-gdoi-group)# client bypass-policy
Device(config-gdoi-group)# end
```

例：デフォルト GDOI バイパス暗号化ポリシーの無効化

```
Device> enable
Device# configure terminal
Device(config)# crypto gdoi group getvpn
Device(config-gdoi-group)# no client bypass-policy
Device(config-gdoi-group)# end
```

GETVPN GDOI バイパス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*』
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
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

GETVPN GDOI バイパスの機能情報

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 GDOI* バイパスの機能情報

機能名	リリース	機能情報
GETVPN GDOI バイパス		次のコマンドが導入されました。**client bypass-policy** および **show crypto gdoi gm acl**。

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。