GET VPN 相互運用性

GETVPN キーサーバーでの D3P サポートの機能、アクティブ化時間遅延の機能、および Cisco GETVPN キーサーバーの GDOI 相互運用 ACK の機能により、キーサーバーとグループメンバーの間の相互運用性が強化されます。

GET VPN 相互運用性の前提条件

- グループの機能を有効にするには、グループ内のすべてのデバイスで互換性のあるバージョンの Cisco IOS ソフトウェアおよび Group Domain of Interpretation（GDOI）が実行されている必要があります。
- Cisco GETVPN キーサーバーのインターネットドラフト ACK とアクティブ化時間遅延の機能を設定する前に、GDOI グループでユニキャストキー再生成機能を有効にします。

GET VPN 相互運用性に関する制約事項

- GETVPN キーサーバー機能での IP-D3P サポートは、GETVPN の復元力（GM のエラー検出および Cisco TrustSec 用の IPsec インラインタギングの GET VPN サポートの機能）と共存できません。後者の機能は、GET VPN キーサーバーで IP-D3P サポートを有効にする前に無効にする必要があります。また、GETVPN キーサーバーで GETVPN の復元力のサポートを有効にする前に IP-D3P を無効にする必要があります。
- アクティブ化時間遅延機能は、IPsec セキュリティ アソシエーションでのみサポートされます。複数の IPsec SA を設定しないでください。

- Cisco-Metdata と IP-D3P は共存できません。CMD 機能と IP-D3P を切り替える場合、キーサーバーは、すべての GM に対して **crypto gdoi ks rekey replace** を実行して、これら 2 つの機能が同時に有効になっていないことを確認する必要があります。
- ASR1K は、GETVPN IPv4 トンネルモードでのみ IP-D3P をサポートします。

GET VPN 相互運用性に関する情報

IP 配信遅延検出プロトコル（IP-D3P）の概要

IPデータグラムは、ホストまたはゲートウェイが最新ではないデータグラムを受信する配信遅延攻撃の対象となる可能性があります。最新のデータグラムは、「プロトコルの以前のインタラクションから再生されたのではなく、最近生成されたデータグラム」として定義されます。IP-D3P データグラムは、ヘッダーと IP ペイロードで構成されます。IP-D3P ヘッダーには、パケットが最近生成されたかどうかを判断するためにパケットの受信者が使用するタイムスタンプが含まれています。受信者は、IPパケットで配信されたタイムスタンプをローカル時間と比較し、パケットを受け入れるかどうかを決定します。

IP-D3P は、グループメンバーのシステムクロックを使用して、IP-D3P データグラムのタイムスタンプを作成および確認します。ほとんどの場合、システムクロックは、送信者と受信者のシステムクロックを同期するために、Network Time Protocol（NTP）などの外部プロトコルから設定されます。

GETVPN キーサーバーでの D3P サポートの機能により、GET VPN での IP-D3P のサポートが有効になります。

キーサーバーの IP-D3P サポート

GDOI ローカル サーバー コンフィギュレーション モードで新しい コンフィギュレーション コマンドの **d3p** を使用すると、キーサーバーで IP-D3P を有効にできます。D3P コマンドを有効にすると、プライマリキーサーバーは、D3P 属性を持つグループ関連ポリシー（GAP）ペイロードがあるすべてのグループメンバーにキー再生成を発行します。GAPペイロードのキー再生成メッセージには次の属性が含まれます。

- D3P-TYPE：Portable Operating System Interface（POSIX）時間（ミリ秒単位）。
- D3P-WINDOWSIZE：IP-D3P ウィンドウサイズ（ミリ秒単位）。

show crypto gkm ks コマンドは、キーサーバーで有効になっている IP-D3P パラメータを表示します。

連携キーサーバーの IP-D3P サポート

GET VPN グループに複数のキーサーバーがある場合は、すべてのキーサーバーで IP-D3P を有効にする必要があります。プライマリキーサーバーは、アナウンスメッセージを介して、IP-D3P

属性を含む GAP ペイロードをセカンダリキーサーバーに送信します。これにより、すべての連携キーサーバーに、IP-D3P がグループ内で適用されるようになったことが通知されます。

GAP ペイロードを受信すると、連携キーサーバーは、IP-D3P 属性をグループ設定と照合します。不一致がある場合、連携キーサーバーは、次に示すように、ネットワーク管理者に誤った設定または不適切な設定を警告する Syslog メッセージを生成します。

```
%GDOI-3-COOP_CONFIG_MISMATCH: WARNING: IP-D3P configuration between Primary KS and
Secondary KS are mismatched
```

グループメンバーの IP-D3P サポート

グループメンバーは、キー再生成メッセージに含まれる IP-D3P パラメータを受信します。グループメンバーは、新しい GAP ペイロード属性（D3P-TYPE および D3P-WINDOWSIZE）を処理します。グループメンバーの IP-D3P で使用する必要があるウィンドウサイズは、GDOI グループ設定で **client d3p** コマンドを使用して上書きできます。たとえば、キーサーバーの設定が **d3p window msec 1000** であり、グループメンバーの設定が **client d3p window sec 50** である場合、グループメンバーは、次のパラメータを使用して、キーサーバーから受信したパラメータを上書きし、IP-D3P を有効にすることができます。

```
D3P-TYPE = POSIX-TIME-MSEC
D3P-WINDOWSIZE = 50000
```

グループメンバーの IP-D3P 設定と、発生した IP-D3P エラー（ある場合）を表示するには、**show crypto gdoi gm** コマンドを使用します。

（注） IP-D3P は、キーサーバーから送信されたパラメータを使用する Cisco ASR 9000 シリーズ アグリゲーション サービス ルータでは有効にできません。Cisco ASR 9000 シリーズ アグリゲーション サービス ルータ上のキーサーバーから送信されたパラメータを表示するには、**show crypto gdoi group** コマンドを使用します。

アクティブ化時間遅延

GET VPN は、アクティブ化時間遅延（ATD）機能をサポートします。この機能では、キーサーバーがグループメンバーに対して、トラフィック暗号化のための新しいセキュリティ アソシエーション（SA）の使用を遅らせるように指示します。キーサーバーは、ユニキャストキー再生成メッセージをグループメンバーに送信するときに、グループ関連ポリシー（GAP）ペイロードに ATD 値を含めます。遅延時間の値は、ユーザーが設定できません。SA の有効期限が切れる 30 秒前に固定されています。ATD 値を計算する式は、次のとおりです。

ATD = Max((Max(old-SA-remaining-lifetime_sec, 30sec) – 30sec), 1sec)

（注） ATD のサポートは、Cisco ASR 9000 シリーズ アグリゲーション サービス ルータおよび非 Cisco デバイスで設定されているグループメンバーに限定されます。そのため、キーサーバーは、Cisco ASR 9000 シリーズ アグリゲーション サービス ルータおよび非 Cisco デバイス以外のデバイスに ATD 情報を送信しません。

.

キー再生成確認応答

キーサーバーが、グループのキーとポリシーを更新するために、グループメンバーにキー再生成メッセージを送信する場合、すべてのグループメンバーがキー再生成メッセージを受信して、新しいキーおよびポリシーが正常に処理され、インストールされ、応答されたかどうかが分かると便利です。

シスコのユニキャストキー再生成確認応答メッセージ

ユニキャストキー再生成が設定されている場合、キーサーバーはキー再生成メッセージを送信し、グループメンバーはそれに対して確認応答キー再生成メッセージを送信することで応答します。

（注） マルチキャストキー再生成が設定されている場合、確認応答メッセージは存在しません。

キーサーバーが、応答確認されていないユニキャストキー再生成をグループメンバーに3回連続して送信し、そのユニキャストキー再生成がそのグループメンバーによって確認応答されなかった場合、そのグループメンバーはキーサーバーのグループ メンバー データベースから削除され、以降のユニキャストキー再生成はそのグループメンバーに送信されません。

GDOI I-D キー再生成確認応答メッセージ

Cisco キーサーバーの GDOI 相互運用 ACK の機能は、シスコ製ではないグループメンバーとキーサーバーの間で、RFC-8263（GROUPKEY-PUSH 確認応答メッセージ）で定義されているキー再生成確認応答メッセージの標準規格を実装します。

GDOI GROUPKEY-PUSH 確認応答メッセージ（「GDOI I-D キー再生成 ACK」と呼ばれる）では、シスコのユニキャストキー再生成確認応答メッセージとは異なり、グループメンバーがグループ内の任意のキーサーバーにキー再生成確認応答を送信するための相互運用可能な方式が定義されています。

キーサーバーの GDOI I-D キー再生成 ACK サポート

rekey acknowledgement コマンドを使用すると、キーサーバーは、 コマンドで選択されているキーワードに応じて、グループメンバーにキー再生成の確認応答を要求できます。

- **cisco**：シスコ独自のキー再生成 ACK（暗号化）メッセージを受け入れます。

- **interoperable**：対応するインターネットドラフトに従って、キー再生成ACK（暗号化されていない）メッセージを要求して受け入れます。
- **any**：グループキーメンバーのバージョンに基づいて、サポートされているすべてのACKメッセージを受け入れます。

rekey acknowledgement コマンドを有効にすると、キーサーバーは、新しいポリシー属性 **KEK_ACK_REQUESTED** を送信します。これは、登録およびキー再生成のためにキー暗号化キー（KEK）SA ペイロードに含まれる新しいポリシー属性です。

連携キーサーバーの GDOI I-D キー再生成 ACK サポート

GET VPN グループに複数のキーサーバーがある場合は、すべてのキーサーバーで **rekey acknowledgement** コマンドを設定する必要があります。プライマリキーサーバーがセカンダリキーサーバーにアナウンスメッセージを送信する場合、プライマリキーサーバーには、**KEK_ACK_REQUESTED** 属性を伝送する **KEK SA** ペイロードも含まれます。これにより、すべての連携キーサーバーに、それらの下に登録されているグループメンバーに **KEK_ACK_REQUESTED** 属性を送信するように通知されます。

KEK_ACK_REQUESTED 属性を持つ **KEK SA** ペイロードを受信すると、連携キーサーバーは、グループ設定を確認します。不一致がある場合、連携キーサーバーは、次に示すように、ネットワーク管理者に誤った設定または不適切な設定を警告するメッセージを生成します。

```
%GDOI-3-COOP_CONFIG_MISMATCH: WARNING: Interoperable Rekey ACK configuration between
Primary KS and Secondary KS are mismatched
```

（注） キー再生成メッセージを送信するのはプライマリキーサーバーであるため、キー再生成確認応答はプライマリキーサーバーにのみ送信されます。キー再生成確認応答は、連携キーサーバーがプライマリキーサーバーとして昇格され、古いプライマリキーサーバーがキー暗号化キー（KEK）またはトラフィック暗号化キー（TEK）ポリシーを作成しなかった場合にのみ、連携サーバーに送信されます。

グループメンバーの GDOI I-D キー再生成サポート

グループメンバーが、KEK SA ペイロードに KEK_ACK_REQUESTED 属性を含むキー再生成メッセージを受信し、確認応答メッセージを介してキーサーバーに GDOI ID キー再生成 ACK を送信する場合、そのグループメンバーは、Cisco GETVPN キーサーバーのインターネットドラフト ACK の機能をサポートしていると見なされます。

キーサーバーとグループメンバーの通信

キーサーバーが KEK SA ペイロードで KEK_ACK_REQUESTED 属性を送信すると、対応するキーサーバーから別の通知がないかぎり、グループメンバーは、後続のキー再生成メッセージに GDOI ID キー再生成 ACK で応答する必要があります。キーサーバーとグループメンバーの間の通信は、次のとおりです。

1. キーサーバーによって送信されるすべてのGROUPKEY-PUSHメッセージに対して、グループメンバーはGROUP-PUSH-KEY ACKメッセージで応答する必要があります。
2. キーサーバーは、メッセージの形式とペイロードを検証して妥当性を確認します。検証に失敗すると、メッセージはドロップされます。
3. 検証に成功すると、キーサーバーは、SEQペイロードとIDペイロードを処理して、IDに関連付けられたグループメンバーの最新の確認応答済みシーケンス番号を記録します。シーケンス番号は、最後に送信されたシーケンス番号と同じである必要があります。それ以外の場合、SEQペイロードとIDペイロードは記録されません。

（注） Ciscoキーサーバーの場合、グループメンバーがキー再生成メッセージに対して3回連続して確認応答を送信しない場合、そのグループメンバーはデータベースから削除されます。グループメンバーにユニキャストキー再生成機能が設定されており、特定のKEKセキュリティパラメータインデックス（SPI）に対してKEK_ACK_REQUESTED属性が送信されない場合、グループメンバーは、Ciscoユニキャストキー再生成ACKメッセージをキーサーバーに送信する必要があります。

次の表で、KEK SAペイロードで送信される属性と、キーサーバーで設定された各確認応答オプションに対して送信される値について説明します。

表 *1:* 各確認応答オプションの *KEK SA* ペイロード

確認応答オプション	新しいシスコグループメンバー	Cisco ASR 9000 グループメンバー	シスコ製以外のグループメンバー
Cisco	属性なし	属性なし	属性なし
相互運用可能	KEK_ACK_REQ REKEY_ACK_KEK_SHA256	KEK_ACK_REQ REKEY_ACK_KEK_SHA256	KEK_ACK_REQ REKEY_ACK_KEK_SHA256
いずれか	属性なし	KEK_ACK_REQ REKEY_ACK_KEK_SHA256	KEK_ACK_REQ REKEY_ACK_KEK_SHA256

（注） **no rekey acknowledgement** コマンドを使用してキー再生成確認応答をデフォルト値の「Cisco」に設定すると、キーサーバーは、KEK SAペイロードにKEK_ACK_REQUESTED属性を含めません。

次の表で、キーサーバーにおいて **rekey acknowledgement** コマンドでキーワードを使用して設定された各確認応答タイプの確認手法について説明します。

表 *2*：確認応答の方法論

確認応答オプション	キーサーバーが I-D ACK を受け入れる	キーサーバーが Cisco ACK を受け入れる
Cisco	いいえ（エラーになります）	対応
相互運用可能	対応	いいえ（エラーになります）
いずれか	対応	対応

GET VPN 相互運用性の設定方法

キーサーバー上の正しい GDOI バージョンの確認

手順の概要

1. **enable**
2. **show crypto gkm feature** *feature name*
3. **show crypto gkm feature** *feature-name* | **include no**

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）。

```
Device> enable
```

ステップ 2 **show crypto gkm feature** *feature name*

ネットワーク内の各キーサーバーおよびグループメンバーで実行されている GDOI バージョンと、デバイスが GET VPN 相互運用性機能（つまり、GETVPN キーサーバーでの D3P サポートと Cisco GETVPN キーサーバーのインターネットドラフト ACK）をサポートしているかどうかに関する情報を表示します。

例：

```
Device# show crypto gkm feature ip-d3p
Group Name: GET VPN1
    Key Server ID       Version   Feature Supported
        10.0.8.1         1.0.11         Yes
        10.0.9.1         1.0.10         No
    Group Member ID     Version   Feature Supported
        10.0.3.1         1.0.11         Yes
        10.65.9.2        1.0.10         No
```

例：

```
Device# show crypto gkm feature gdoi-interop-ack
Group Name: GET VPN2
    Key Server ID       Version   Feature Supported
        10.0.8.1         1.0.11         Yes
        10.0.9.1         1.0.10         No
    Group Member ID     Version   Feature Supported
        10.0.3.1         1.0.11         Yes
        10.65.9.2        1.0.10         No
```

ステップ 3 **show crypto gkm feature** *feature-name* | **include no**

（任意）機能をサポートしていないデバイスを検索します。

例：

```
Device# show crypto gkm feature gdoi-interop-ack | include no
```

グループメンバー上の正しい GDOI バージョンの確認

手順の概要

1. **enable**
2. **show crypto gkm feature** *feature name*

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）。

ステップ 2 **show crypto gkm feature** *feature name*

ネットワーク内のグループメンバーで実行されている GDOI バージョンと、デバイスが GET VPN 相互運用性機能（つまり、GETVPN キーサーバーでの D3P サポートと Cisco GETVPN キーサーバーのインターネットドラフト ACK）をサポートしているかどうかに関する情報を表示します。

例：

```
Device# show crypto gkm feature ip-d3p
       Version    Feature Supported
        1.0.11           Yes
```

例：

```
Device# show crypto gkm feature gdoi-interop-ack
       Version    Feature Supported
        1.0.10           No
```

キーサーバーでの IP-D3P の有効化

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto gkm group GETVPN**
4. **server local**
5. **sa d3p window**{**sec** *seconds* | **msec** *milliseconds*}
6. **exit**
7. **show crypto gkm ks replay**

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 gkm group GETVPN** 例： `Device(config)# crypto gkm group GETVPN`	グループキー管理（GKM）グループを設定し、GKM 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	**server local** 例： `Device(config-gkm-group)# server local`	デバイスをキーサーバーとして指定し、GDOI ローカル サーバー コンフィギュレーション モードを開始します。
ステップ 5	**sa d3p window**{**sec** *seconds* | **msec** *milliseconds*} 例： `Device(gdoi-local-server)# sa d3p window msec 5000`	グループ内のすべてのセキュリティ アソシエーションで IP 配信遅延検出プロトコル（IP-D3P）を有効にします。 • **sec** *seconds*：ウィンドウサイズ（秒単位）。範囲は 1 ～ 100 です。 • **msec** *milliseconds*：ウィンドウサイズ（ミリ秒単位）。範囲は 100 ～ 10000 です。
ステップ 6	**exit** 例： `Device(gdoi-local-server)# exit`	GDOI ローカル サーバ 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。

	コマンドまたはアクション	目的
ステップ 7	**show crypto gkm ks replay** 例： `Device# show crypto gkm ks replay`	時間ベースのアンチリプレイのキーサーバーグループ情報を表示します。

例

次に、**show crypto gkm ks replay** コマンドの出力例を示します。

```
Device# show crypto gkm ks replay
Anti-replay Information For Group GETVPN:
    IP-D3P: Type = POSIX-TIME-MSEC, Window-size = 5000 msec
```

グループメンバーでの IP-D3P の有効化

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto gkm group GET**
4. **client d3p window** {**sec** *seconds* | **msec** *milliseconds*}
5. **exit**
6. **show crypto gkm gm replay**

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 gkm group GET** 例： `Device(config)# crypto gkm group GETVPN`	グループキー管理（GKM）グループを設定し、GKM 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 d3p window** {**sec** *seconds* | **msec** *milliseconds*} 例： `Device(config-gkm-group)# client d3p window sec 50`	クライアントが許容できるIP配信遅延検出プロトコル（IP-D3P）を有効にします。 • **sec** *seconds*：ウィンドウサイズ（秒単位）。範囲は 1 ～ 100 です。

	コマンドまたはアクション	目的
		• **msec** *milliseconds*：ウィンドウサイズ（ミリ秒単位）。範囲は 100 ～ 10000 です。
ステップ 5	**exit** 例： `Device(gdoi-local-server)# exit`	GDOI ローカルサーバ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。
ステップ 6	**show crypto gkm gm replay** 例： `Device# show crypto gkm gm replay`	時間ベースのアンチリプレイのグループメンバー情報を表示します。

例

次に、**show crypto gkm gm replay** コマンドの出力例を示します。

```
Device# show crypto gkm gm replay
Anti-replay Information For Group GET:
   IP-D3P:
     Posix-time-msec           : 502764.17
     Input Packets            : 5        Output Packets           : 5
     Input Error Packets      : 5        Output Error Packets     : 0

IP-D3P Error History (sampled at 10pak/min):
     xx:xx:xx.xxx PST Tue Feb 25 2014: src=5.0.0.2; my_time=502729.95; peer_time=33.46;
 win=10
     yy:yy:yy.yyy PST Tue Feb 25 2014: src=5.0.0.2; my_time=502723.95; peer_time=27.45;
 win=10
```

キー再生成確認応答の有効化

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto gkm group GET**
4. **server local**
5. **rekey acknowledgement**{**cisco** | **interoperable** | **any**}
6. **exit**
7. **show crypto gkm ks replay**

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	**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 gkm group GET** 例： `Device(config)# crypto gkm group GET`	グループキー管理（GKM）グループを設定し、GKM 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	**server local** 例： `Device(config-gkm-group)# server local`	デバイスをキーサーバーとして指定し、GDOI ローカル サーバー コンフィギュレーション モードを開始します。
ステップ 5	**rekey acknowledgement**{**cisco** | **interoperable** | **any**} 例： `Device(gdoi-local-server)# rekey acknowledgment interoperable`	グループメンバーがキー再生成を確認応答できるようにします。 • **cisco**：Cisco Rekey ACK（暗号化）メッセージを受け入れます。 • **interoperable**：相互運用可能なキー再生成 ACK（非暗号化）メッセージを要求して受け入れます。 • **any**：グループキーメンバーのバージョンに基づいて、サポートされている ACK メッセージを受け入れます。
ステップ 6	**exit** 例： `Device(gdoi-local-server)# exit`	GDOI ローカルサーバ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。
ステップ 7	**show crypto gkm ks replay** 例： `Device# show crypto gkm ks replay`	キーサーバーでのキー再生成確認応答の設定を表示します。

例

次に、キー再生成確認応答の設定を表示する **show** コマンドの出力例を示します。

```
Device# show crypto gkm

GROUP INFORMATION
    Group Name               : GETVPN (Unicast)
 .
 .
 .
```

```
    Group Rekey Lifetime     : 86400 secs
    Group Rekey
        Remaining Lifetime   : 44710 secs
        Time to Rekey        : 44485 secs
        Acknowledgement Cfg  : {Cisco|Interoperable|Any}
 .
 .
 .

Device# show crypto gkm ks

Total group members registered to this box: 0
Key Server Information For Group GETVPN:
    Group Name               : GETVPN
Group Name               : GETVPN (Unicast)
 .
 .
 .
    Group Members            : 0
      GDOI Group Members     : 0
      G-IKEv2 Group Members  : 0
    Rekey Acknowledgement Cfg: {Cisco|Interoperable|Any}
    IPSec SA Direction       : Both
 .
 .
 .
Device# show crypto gkm ks rekey

Group GETVPN (Unicast)
    Acknowledgement Type In-Use         : {Cisco|Interoperable|Any}
    Number of Rekeys sent               : 20
 .
 .
 .
Device# show crypto gkm ks rekey

Group GETVPN (Multicast)
    Acknowledgement Type In-Use         : None
    Number of Rekeys sent               : 20
 .
 .
 .
Device# show crypto gkm ks policy

Key Server Policy:
For group diffint (handle: 2147483650) server 10.0.8.1 (handle: 2147483650):
  # of teks : 2  Seq num : 7
  KEK POLICY (transport type : Unicast)
    spi : 0x7D32D2052B87CEFE14060B58B0176129
    management alg     : disabled    encrypt alg       : AES
    crypto iv length   : 16          key size          : 16
    orig life(sec): 86400       remaining life(sec): 44699
    time to rekey (sec): 44474
    sig hash algorithm : enabled     sig key length    : 162
    sig size           : 128
    sig key name       : mykeys
    acknowledgement    : {cisco|interoperable|any}

Device# show crypto gkm ks policy

Key Server Policy:
For group diffint (handle: 2147483650) server 10.0.8.1 (handle: 2147483650):
  # of teks : 2  Seq num : 7
  KEK POLICY (transport type : Multicast)
```

```
spi : 0x7D32D2052B87CEFE14060B58B0176129
management alg     : disabled    encrypt alg       : AES
crypto iv length   : 16          key size          : 16
orig life(sec): 86400       remaining life(sec): 44699
time to rekey (sec): 44474
sig hash algorithm : enabled     sig key length    : 162
sig size           : 128
sig key name       : mykeys
acknowledgement    : none
```

GET VPN 相互運用性の設定例

例：キーサーバーでの IP-D3P の有効化

```
Device> enable
Device# configure terminal
Device(config)# crypto gkm group GETVPN
Device(config-gkm-group)# server local
Device(gdoi-local-server)# sa d3p window msec 5000
Device(gdoi-local-server)# exit
```

例：グループメンバーでの IP-D3P の有効化

```
Device> enable
Device# configure terminal
Device(config-gkm-group)# client d3p window sec 50
Device(gdoi-local-server)# exit
```

例：キー再生成確認応答の有効化

```
Device> enable
Device# configure terminal
Device(config)# crypto gkm group GET
Device(config-gkm-group)# server local
Device(gdoi-local-server)# rekey acknowledgment interoperable
Device(gdoi-local-server)# exit
```

GET VPN の相互運用性に関する追加情報

関連資料

関連項目	マニュアル タイトル

関連項目	マニュアル タイトル
セキュリティ コマンド	• 『Cisco IOS Security Command Reference: Commands A to C』 • 『Cisco IOS Security Command Reference Commands D to L』 • 『Cisco IOS Security Command Reference: Commands M to R』 • 『Cisco IOS Security Command Reference: Commands S to Z』
GET VPN の設定	*Cisco Group Encrypted Transport VPN*
ユニキャストキー再生成	*GET VPN* モジュールの「Unicast Rekeying」セクション

標準および RFC

標準/RFC	タイトル
draft-weis-delay-detection-00	『*IP Delivery Delay Detection Protocol*』
draft-weis-gdoi-rekey-ack-01	『*GDOI GROUPKEY-PUSH Acknowledgement Message*』
RFC 5374 - セクション 5.4：グループ関連ポリシー	『*Multicast Extensions to the Security Architecture for the Internet Protocol*』
RFC 6407 - セクション 4.2.1：アクティブ化時間遅延	『*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

GET VPN 相互運用性の機能情報

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 *3 : GET VPN* 相互運用性の機能情報

機能名	リリース	機能情報
GETVPN キーサーバーでの D3P サポート		GETVPN キーサーバーでの D3P サポートの機能は、GET VPN ネットワークでの IP-D3P のサポートを有効にします。 次のコマンドが導入または変更されました。**client d3p**、**sa d3p**、**show crypto gkm gm replay**、**show crypto gkm ks replay**
Cisco GETVPN キーサーバーのインターネットドラフト ACK		Cisco GETVPN キーサーバーのインターネットドラフト ACK は、シスコ製ではないグループメンバーとキーサーバーの間で、GDOI GROUPKEY-PUSH 確認応答メッセージドラフトで定義されているキー再生成確認応答メッセージの標準規格を実装します。 次のコマンドが導入または変更されました。 **rekey acknowledgement**、**show crypto gkm**。
RFC 8263 ID Ack の実装		Group Domain of Interpretation（GDOI）には、現在の一連のデバイスに追加のセキュリティアソシエーションを提供するキーサーバーの機能が含まれています。たとえば、期限切れのセキュリティ アソシエーションのキーを再生成できます。この機能により、グループデバイスがキー再生成メッセージの受信確認応答を返すように要求するキーサーバーの機能が追加され、確認応答の方式が指定されます。

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。