Cisco Group Encrypted Transport VPN

Cisco Group Encrypted Transport VPN（GET VPN）は、Cisco IOS デバイス上で発生する、または Cisco IOS デバイス を経由するプライベート WAN 上の IP マルチキャスト トラフィック グループまたはユニキャスト トラフィックの安全を守るために必要な一連の機能です。GET VPN では、キーイング プロトコルであるグループ ドメイン オブ インタープリテーション（GDOI）と、IP セキュリティ（IPsec）暗号化が組み合されており、ユーザは、IP マルチキャスト トラフィックやユニキャスト トラフィックをセキュリティ保護するための効果的な方式を利用できます。GET VPN では、ルータによって、トンネル化されていない（つまり「ネイティブな」）IP マルチキャストおよびユニキャスト パケットに対して暗号化を適用できるので、マルチキャストおよびユニキャスト トラフィックを保護するためにトンネルを設定する必要がありません。

（注） セキュリティに対する脅威は、脅威からの保護に役立つ暗号化技術と同様に絶え間なく変化しています。シスコの暗号化に関する最新の推奨事項の詳細は、『Next Generation Encryption』（NGE）ホワイトペーパーを参照してください。

ここでは、Cisco GET VPN の設定、確認、およびトラブルシューティングの方法を説明します。

Cisco Group Encrypted Transport VPN には、次のような利点があります。

- データ セキュリティおよびトランスポート認証が利用可能で、すべての WAN トラフィックを暗号化することによって、セキュリティ適合性および内部規則を満たすことが可能。
- 大規模なネットワーク メッシュが可能であり、グループ暗号キーを使用した、複雑なピア ツーピアのキー管理が不要。
- マルチプロトコル ラベル スイッチング（MPLS）ネットワークの場合でも、ネットワーク インテリジェンス（フルメッシュ接続、ナチュラル ルーティング パス、Quality of Service（QoS）など）を維持。
- 一元化されたキー サーバを使用してメンバーシップを簡単に管理可能。
- 中央集中型ハブを介した転送が不要な、サイト間におけるフルタイムの直接通信を実現することによって遅延とジッタの低減が可能。

- マルチキャスト トラフィックの複製にコア ネットワークを使用し、個々のピア サイトごとにおけるパケットの複製を不要にすることによって、宅内装置（CPE）およびプロバイダー エッジ（PE）暗号化デバイスの負荷を削減。

Cisco Group Encrypted Transport VPN の前提条件

- Cisco IOS XE リリース 2.3 以降を使用している必要があります。
- IPsec およびインターネット キー交換（IKE）に関する知識が必要です。
- Cisco IOS XE グローバル ルータにおけるマルチキャストおよびユニキャスト ルーティングの設定方法を知っている必要があります。
- IKE ポリシーを設定する際、IKE ライフタイムを最小値の 5 分に設定する必要があります。その結果、不要なリソースが、IKE セキュリティ アソシエーション（SA）のメンテナンスで無駄に使用されなくなります。登録 IKE SA が確立したら、キー再生成 SA が作成済みとなり、将来のキー再生成を受け入れるために使用されるので、登録 SA を維持する必要はなくなります。
- グループのキー再生成のライフタイムが 300 秒に設定され、ポリシーの変更による強制的なキー再生成が実行されると、ネットワークの問題が発生する可能性があります。この問題を解決するには、グループのキー再生成（KEK）に関して次のいずれかが推奨されます。
  - ライフタイムを、transform-set で設定された TEK ライフタイムの 3 倍に設定します。
  - グループのキー再生成のライフタイムをデフォルト値の 24 時間（86,400 秒）に設定します。
  - キー再生成のライフタイムを 7,200 秒（2 時間）に設定します。

Cisco Group Encrypted Transport VPN の制約事項

- カウンタ ベースのアンチ リプレイ用に高パケット レートを暗号化する場合、ライフタイムを長く設定し過ぎないようにしてください。長く設定し過ぎると、シーケンス番号のラップに数時間かかってしまう可能性があります。たとえば、パケット レートが毎秒 100

キロパケットである場合、ライフタイムは、SA がシーケンス番号のラップ前に使用されるように 11.93 時間より短く設定する必要があります。

- 仮想 PPP インターフェイスを備えた Cisco ASR 1000 シリーズ アグリゲーション ルータは、GETVPN グループメンバーとして設定できません。
- Cisco IOS XE ソフトウェアでは、ネットワークにアクセスするユーザの包含ポート範囲を **permit** コマンドを使用して拡張 ACL と照合することはできません。
- ユニキャスト トラフィックおよびカウンタベースのアンチ リプレイでは、グループ メンバーの 1 つが停止してから復帰した場合、シーケンス番号がグループ メンバー間で同期されていない状態になる可能性があります。たとえば、グループ メンバー 1 からグループ メンバー 2 へのトラフィックが存在し、最後のシーケンス番号が *n* になる場合です。Group Member 1 が停止してから復帰します。グループ メンバー 1 における SA のシーケンス番号は現在 1 で始まっていますが、グループ メンバー 2 では、前のシーケンス番号から連続する番号（*n*+1）と予測しています。このような状況の結果、Group Member 1 のシーケンス番号が *n* になるか、次のキー再生成まで、Group Member 1 からの後続のトラフィックは停止します。
- 転送モード トラフィック セレクタを設定する際、転送モードを SA にすることが可能です。パケット サイズが MTU を超え、パケットが転送できなくなると、SA が発生します。
- 転送モードは、Group Encrypted Transport VPN Mode（GM）から GM へのトラフィックだけに使用してください。
- カプセル化されたパケットの IP ヘッダー内の don't fragment bit（df-bit）設定を上書きする場合、グローバル コンフィギュレーション モードで上書きコマンドを設定する必要があります。GET VPN では、インターフェイス コンフィギュレーションは受け入れられません。この制限事項は、GET VPN にだけ当てはまります。IPsec では、グローバル コンフィギュレーション専用上書きコマンドおよびインターフェイス専用上書きコマンドの両方が受け入れられます。
- カウンタベースのアンチ リプレイは推奨できません。カウンタベースのアンチ リプレイは、1 つのグループ内に 2 つのグループ メンバーが存在している時にだけ動作します。
- GET VPN 時間ベースのアンチリプレイ機能では、Cisco ASR 1000 シリーズアグリゲーション サービス ルータと Cisco 4330 サービス統合型ルータの Encapsulating Security Payload（ESP）転送モードがサポートされていません。
- Path MTU Discovery（PMTUD）は、GET VPN に対しては動作しないので、df-bit が設定されており、中間リンクの MTU がカプセル化されたパケットのサイズより小さい場合に、カプセル化されたパケットが廃棄される可能性があります。このようなイベントが発生した場合、パケットを廃棄するルータによってパケット上の発信元 IP アドレスに対して通知が送信され、df-bit の設定のためにルータによるパケットのフラグメント化ができなかったために、パケットが廃棄されたことが通知されます。GET VPN ではヘッダー保存機能があるため、このメッセージはカプセル化を行うエンドポイントを経由しないで、直接データの発信元に送信されます。そのため、カプセル化を行うルータは、カプセル化の後で df-bit を設定する前により小さいサイズにパケットをフラグメント化しなければならないと判断できません。パケット上の df-bit 設定は継続され、中間ルータにおいて、それら

のパケットは引き続き廃棄されます（これはトラフィックの Null ルーティングと呼ばれます）。

- Cisco IOS XE リリース 3.5S 以前のリリースでは、Cisco IOS XE イメージを使用してキーサーバを設定することはできません。これらは Cisco IOS T ベースまたはメインラインベース イメージを使用して設定する必要があります。これは、Cisco IOS XE リリース 3.6S 以降のリリースの制約ではありません。
- 暗号化エンジンの最適化のために、時間ベースのアンチリプレイ（TBAR）のオーバーヘッドは 12 バイトではなく 16 バイトです。
- GET VPN は、TBAR Cisco Metadata Protocol を使用して TBAR 情報を伝送します。Cisco IOS ソフトウェアは 12 バイトのヘッダーを使用し、Cisco IOS XE は 16 バイトのヘッダーを使用します。GETVPN グループメンバーで設定され、アンチリプレイに TBAR を使用する Cisco IOS XE ソフトウェアでは、IPsec トラフィックの有効な MTU（「クリアテキスト MTU」）が、Cisco IOS ソフトウェアによって設定されるグループメンバーよりも 4 バイト小さくなります。GET VPN グループメンバーを Cisco IOS ソフトウェアから Cisco IOS XE ソフトウェアに移行する場合、4 バイトの減少により、予期しないパフォーマンスの問題が発生する可能性があります。
- Cisco ASR 1000 シリーズ アグリゲーション サービス ルータの GET VPN 設定で正常なトラフィック フローを保証するため、Cisco IOS XE リリース 3.12S 以前のリリース、Cisco IOS XE リリース 3.14S および Cisco IOS XE リリース 3.15S では 20 秒を超える TBAR ウィンドウ サイズが推奨されます。Cisco IOS XE リリース 3.13S、Cisco IOS XE リリース 3.16S 以降のリリースでは、20 秒以内の TBAR ウィンドウ サイズが許可されます。
- 暗号マップは、トンネルインターフェイスとポートチャネルインターフェイス上でサポートされません。ただし、ルールの例外として、GDOI の暗号マップはトンネルインターフェイスでサポートされます。
- 暗号マップは VLAN インターフェイスではサポートされません。
- Mediatrace で使用される RSVP は、「ルータアラート」 IP オプションフラグを設定します。Cavium N2 暗号アクセラレータは、IP オプションの使用をサポートしていません。そのため、Mediatrace は、Cavium N2 を搭載した ASR1000 での IPsec 暗号化に失敗します。Mediatrace は、Cavium N2 を搭載した ASR1000 での GETVPN 暗号化（ヘッダーが維持される IPsec）に失敗します。
- 拒否（deny）ステートメントは、ローカルでのみ GM に追加できます。許可（permit）ステートメントは、ローカルに設定されたポリシーではサポートされません。競合が発生した場合、ローカルポリシーは、KS からダウンロードされたポリシーを上書きします。
- Cisco ASR 1000 シリーズアグリゲーション サービス ルータでは、再登録に失敗した場合、実際の ACE の代わりにダミーの ACE がプッシュされるため、QFP からのアウトバウンドフローは削除されません。その結果、SA が期限切れになると、GM は、トラフィックをローカルにドロップするのではなく、期限切れの SPI を使用してアウトバウンドトラフィックを暗号化しつづけます。無効な SPI メカニズムが原因で、トラフィックは、最終的に受信側 GM でドロップされます。

- キーサーバーで IPv6 アクセスリストを設定しているときは、**permit** コマンドまたは **deny** コマンドで **ahp** オプションを使用しないでください。
- GETVPN グループメンバーとして動作している Cisco IOS XE プラットフォームは、1 つの GETVPN-ipv4 グループ メンバー インスタンスと 1 つの GETVPN-ipv6 グループ メンバー インスタンスのみをサポートできます。
- **SSO の制約事項**
- Cisco ASR 1000 シリーズ ルータは、Embedded Services Processor（ESP）スイッチオーバーでステートフル IPsec セッションをサポートします。ESP スイッチオーバー中は、すべての IPsec セッションがアップ状態のままになるので、IPsec セッションを維持するためにユーザーの操作は必要ありません。
- ESP をリロードした場合（スタンバイ ESP なし）、SA シーケンス番号は 0 から再開されます。ピア ルータは、予期されたシーケンス番号を持たないパケットをドロップします。単一の ESP を使用するシステムで ESP のリロード後にこの問題を回避するには、IPSec セッションを明示的に再確立することが必要になる場合があります。このような場合、リロード中に IPSec セッションでトラフィックの中断が発生することがあります。
- Cisco ASR 1000 シリーズ ルータは、現在、ルートプロセッサ（RP）でのステートフル スイッチオーバー（SSO）の IPsec セッションをサポートしていません。IPsec セッションはスイッチオーバーの開始時にダウンしますが、新しい RP がアクティブになるとアップ状態に戻ります。ユーザーの操作は必要ありません。セッションがアップ状態に戻るまでの間、スイッチオーバー中に IPSec セッションでトラフィックの中断が発生することがあります。
- Cisco ASR 1000 シリーズ ルータは、IPsec セッションのステートフル ISSU をサポートしていません。ISSU を実行する前に、既存のすべての IPSec セッションまたはトンネルを明示的に終了し、ISSU の実行後に再確立する必要があります。具体的には、ISSU を実行する前に、ハーフオープンまたは確立途中の IPsec トンネルが存在しないことを確認します。これを行うには、トンネルセットアップを開始する可能性のあるインターフェイス（トンネルセットアップを開始するルーティングプロトコルなど）、キープアライブが有効になっているインターフェイス、または IPsec セッションの自動トリガーが存在するインターフェイスの場合は、インターフェイスをシャットダウンすることをお勧めします。この場合、ISSU の実行中に IPsec セッションでトラフィックの中断が発生します。

Cisco Group Encrypted Transport VPN に関する情報

Cisco Group Encrypted Transport VPN の概要

音声やビデオなどのネットワークを利用するアプリケーションによって、即時に通信可能で各ブランチが相互接続された、QoS 対応 WAN の必要性が増しています。これらのアプリケーションは分散して配置されるため、スケーラビリティに対する要求も高まります。同時に、企業の WAN テクノロジーにおいては、QoS 対応ブランチ間相互接続と転送のセキュリティとの

間でトレードオフが発生します。ネットワーク セキュリティのリスクが増大し、適合認定が重要になりつつある中、次世代のWAN暗号化テクノロジーであるGET VPNを利用すれば、ネットワークのインテリジェント化とデータ プライバシとの間で折り合いをつける必要性を低下させることができます。

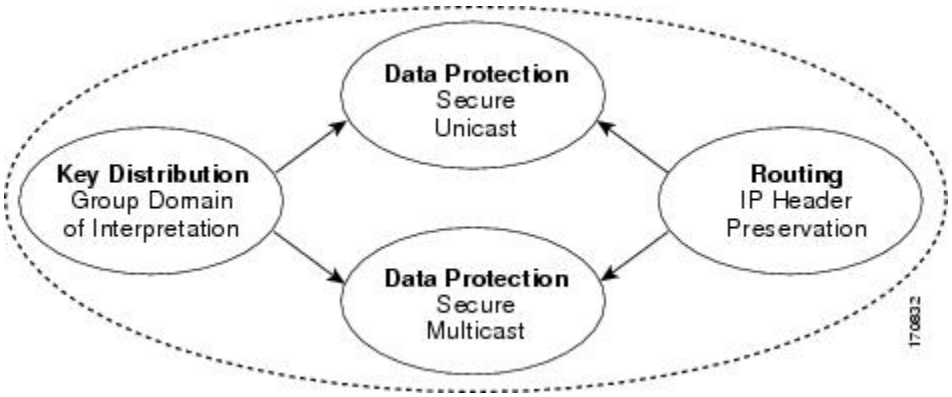
シスコでは、GET の導入に伴い、トンネルレス VPN を提供しており、これによりトンネルが不要になります。ポイントツーポイント トンネルの必要性をなくすことで、メッシュ ネットワークを大規模化すると同時に、音声やビデオの品質にとって重要なネットワークインテリジェンス機能を維持することが可能となっています。GET では、「信頼できる」グループ メンバーというコンセプトを基にした、各種の標準規格に準拠準拠したセキュリティ モデルが用意されています。信頼できるメンバーのルータでは、ポイントツーポイント IPsec トンネル関係とは独立した共通のセキュリティ方式が使用されます。ポイントツーポイント トンネルではなく信頼できるグループを使用することによって、「any-any」ネットワークを大規模化すると同時に、音声やビデオの品質にとって重要なネットワークインテリジェンス機能（QoS、ルーティング、マルチキャストなど）を維持することが可能となっています。

GET ベースのネットワークは、IP や MPLS などを含む、さまざまな WAN 環境で使用できます。この暗号化テクノロジーを使用する MPLS VPN はスケーラビリティ、管理性、コストに優れており、政府によって義務付けられている暗号化要件が満たされます。GETは柔軟であるため、セキュリティを必要とする企業では、サービス プロバイダー WAN サービスにおいて独自のネットワーク セキュリティを管理することも、暗号化サービスをプロバイダーに委託することもできます。GETによって、部分メッシュ接続または完全メッシュ接続を必要とする大規模なレイヤ 2 または MPLS ネットワークの保護が簡易化されます。

Cisco Group Encrypted Transport VPN のアーキテクチャ

GET VPN は、マルチキャスト キー再生、「ネイティブの」マルチキャスト パケットの暗号化を可能にする手段、およびプライベート WAN を介したユニキャスト キー再生成を網羅するソリューションです。マルチキャスト キー再生と GET VPN は、インターネット技術特別調査委員会（IETF）の RFC 3547 で定義されている GDOI を基盤としています。また、ヘッダー保存および SA 検索の領域においては、IPsec と各種の共通点が存在します。IPsec SA の動的配信が追加され、IPsec のトンネルが重複する特性が削除されています。次の図に、GET VPN の各概念と、概念間の関係を示します。

図 *1 : GET VPN* の概念と関係



キー配布グループ ドメイン オブ インタープリテーション（GDOI）

GDOI

GDOI は、グループ キー管理のための、Internet Security Association Key Management Protocol（ISAKMP）ドメイン オブ インタープリテーション（DOI）として定義されています。グループ管理モデルでは、GDOI プロトコルが、グループ メンバーと、グループ コントローラまたはキー サーバ（GCKS）との間で動作し、その結果、認証されているグループ メンバー間での SA が確立されます。ISAKMP では、ネゴシエーションの 2 つのフェーズが定義されています。GDOI は、フェーズ 1 の ISAKMP セキュリティ アソシエーションによって保護されます。フェーズ 2 の交換は、RFC 6407 によって定義されています。次の図に示したトポロジとそれに続く説明は、このプロトコルのしくみを説明したものです。

グループ メンバー

グループ メンバーは、グループと通信するために必要な IPsec SA または SA を取得するためのキー サーバに登録します。グループ メンバーによって、そのグループの個別のポリシーおよびキーを取得するためのキー サーバにグループ ID が提供されます。これらのキーは、現在の IPsec SA が期限切れになる前に、定期的に更新されます。その結果、トラフィックのロスがなくなります。

show crypto isakmp sa detail コマンドの出力では、GET VPN のキー暗号化キー（KEK）キー再生成認証に RSA 署名が使用されるため、セキュリティ アソシエーション（SA）認証を「rsig」として表示します。

キー サーバ

キー サーバの役割には、ポリシーの維持や、グループのキーの作成および維持などがあります。グループ メンバーが登録されると、キー サーバによってこのポリシーおよびキーが、グループ メンバーに対してダウンロードされます。また、キー サーバは、既存のキーの期限が切れる前にグループに対してキーの再生成を実行します。

（注） Cisco IOS XE リリース 3.5S 以前のリリースでは、キー サーバは Cisco ASR 1000 シリーズ ルータではサポートされていません。これらは Cisco IOS T ベースまたはメインラインベース イメージを使用して設定する必要があります。これは、Cisco IOS XE リリース 3.6S 以降のリリースの制限ではありません。

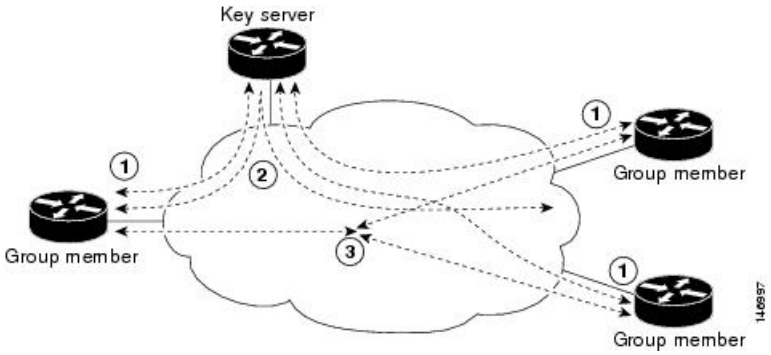
キー サーバには、登録要求の処理およびキーの再生成の送信という 2 つの機能があります。グループ メンバーはいつでも登録可能で、最新のポリシーおよびキーを受信できます。グループ メンバーがキー サーバに登録する場合、キー サーバによって、グループ メンバーが参加を試みているグループ ID が確認されます。この ID が有効なグループ ID だった場合、キー サーバによって、SA ポリシーがグループ メンバーに対して送信されます。ダウンロードされたポリシーを処理できることがグループ メンバーによって確認されると、キー サーバから各キーがダウンロードされます。

キーサーバからダウンロードされるキーには、キー暗号キー（KEK）とトラフィック暗号キー（TEK）の 2 種類があります。TEK は、同じグループ内のグループ メンバーどうしの通信で使用される IPsec SA になります。KEK は、キー再生成メッセージを暗号化します。

IPsec SA の期限切れが近づいた場合、またはキーサーバ上のポリシーが変更（コマンドライン インターフェイス [CLI] を使用）された場合、GDOI サーバによってキー再生成メッセージが送信されます。CSCti89255 では、KEK タイマーが期限切れになる前に KEK のキー再生成が行われます。グループ メンバーもタイマーを開始し、タイマーの期限が切れる前に更新されたキーを受け取ることを期待します。これらを受け取らない場合、グループ メンバーは KEK の期限切れの前にジッタが生じた再登録を開始します。KEK ライフタイムが期限切れになると、KEK は削除されます。

パケット損失に備えて、キー再生成メッセージが定期的に送信される場合もあります。パケット損失が発生する原因としては、信頼できる転送を使用することなくキー再生成メッセージが送信されることなどが考えられます。キーの再生成メカニズムがマルチキャストである場合は、受信者がキーの再生成メッセージを受信できなかったことを示す有効なフィードバック メカニズムがないため、定期的に再送信することによってすべての受信者が最新の情報を受信できるようにします。キー再生成メカニズムがユニキャストである場合、受信元によって確認応答メッセージが送信されます。

図 *2:* グループ メンバーがグループに参加するうえで必要なプロトコル フロー



上記のトポロジは、次のようにグループ メンバーがグループに参加するうえで必要なプロトコル フローを示しています。

1. グループ メンバーがキー サーバに登録されます。キー サーバによってグループ メンバーが認証および許可され、グループ メンバーが IP マルチキャスト パケットを暗号化および復号化するうえで必要な IPsec ポリシーおよびキーがダウンロードされます。
2. 必要に応じて、キー サーバからグループ メンバーに対してキーの再生成メッセージが「プッシュ」されます。キー再生成メッセージには、古い IPsec SA の期限が切れた際に使用される新しい IPsec ポリシーおよびキーが格納されています。常に有効なグループ キーが使用できるように、キーの再生成メッセージは SA の期限が切れる前に送信されます。
3. 各グループ メンバーは、キー サーバによって認証を受けてから、キー サーバから受信した IPsec SA を使用して、同じグループ内の他の認証済みグループ メンバーと通信します。

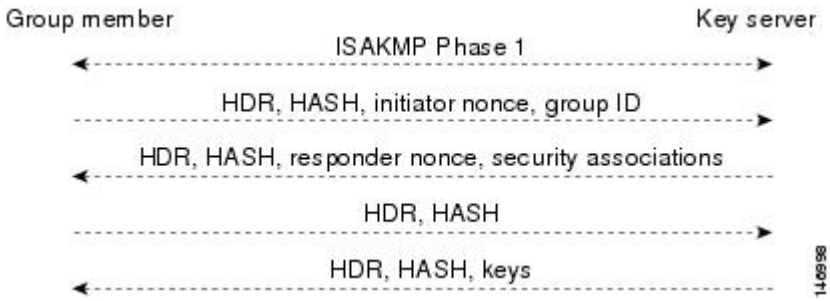
Cisco ソフトウェアでのプロトコル メッセージの動作

マルチキャスト キー再生では、グループのポリシーおよびキーを配信するためにGDOIプロトコル（RFC 6407）が使用されます。GDOI プロトコルは、キー サーバとグループ メンバーの間で使用されます。キー サーバによってポリシーとキーが作成および維持され、さらに、認証された各グループ メンバーにダウンロードされます。

GDOI プロトコルは、ISAKMP フェーズ 1 交換によって保護されます。GDOI キー サーバと GDOI グループ メンバーの ISAKMP ポリシーは同じである必要があります。このフェーズ 1 ISAKMP ポリシーは、そのポリシーに従うGDOIプロトコルを保護できる程度に強力なものである必要があります。GDOI プロトコルは、フェーズ 1 ISAKMP ポリシーに従う 4 メッセージ交換です。フェーズ 1 ISAKMP 交換は、メイン モードまたはアグレッシブ モードで発生する可能性があります。

次の図は、ISAKMP フェーズ 1 交換を示しています。

図 *3 : ISAKMP* フェーズ *1* 交換と *GDOI* 登録



上記メッセージ（ISAKMP フェーズ 1 メッセージと 4 つの GDOI プロトコル メッセージ）をGDOI登録と呼びます。上に示した交換全体は、グループ メンバーとキー サーバ間のユニキャスト交換です。

キー再生成メカニズムがマルチキャストである場合、登録中、グループ メンバーによってマルチキャスト グループのアドレスが受信され、そのグループ メンバーが、マルチキャスト キー再生成を受信するうえで必要なマルチキャスト グループに登録されます。

GDOI プロトコルでは、ユーザ データグラム プロトコル（UDP）ポート 848 が使用されます（Network Address Translation-Traversal（NAT-T）が使用されている場合、ポートは 4500 まで変化します）。

IPsec

IPsec は、IP レイヤのトラフィックのための各種セキュリティ サービスを提供するためのアーキテクチャが定義された、よく知られた RFC です。IETF RFC 2401 には、各種コンポーネントおよびそれらがどのように互いに組み合されてIP環境を形成しているかが記述されています。

IPsec SA を更新するためのキー サーバとグループ メンバー間の通信フロー

キー サーバとグループ メンバーは、GET VPN アーキテクチャを構成する 2 つのコンポーネントです。キー サーバには、グループ認証キーと IPsec SA が保存され、グループ メンバーに対して提供されます。

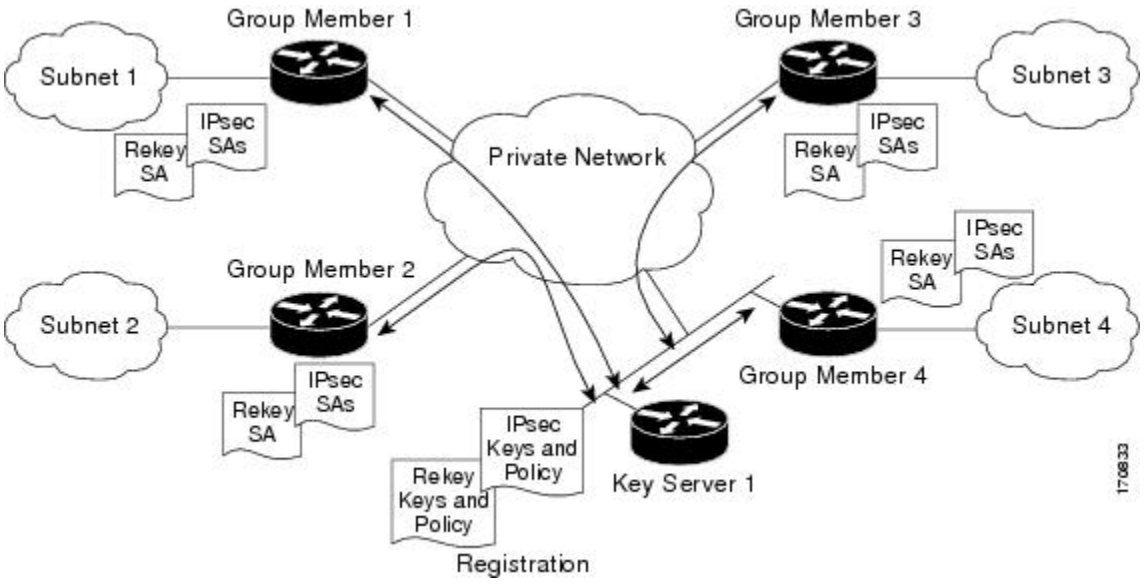
グループ メンバーでは、対象となるトラフィック（暗号化するに値し、IPsec によってセキュリティ保護されるトラフィック）に対して暗号化サービスが提供されます。

キー サーバとグループ メンバー間における通信は暗号化およびセキュリティ保護されます。GDOI には、TEK と KEK という 2 つのキーがサポートされています。TEK は、キー サーバからすべてのグループ メンバーにダウンロードされます。ダウンロードされた TEK は、グループ メンバー間で安全に通信するためにすべてのグループ メンバーで使用されます。このキーは、実質的には、すべてのグループ メンバーによって共有されるグループ キーとなります。グループ ポリシーおよび IPsec SA は、グループ メンバーへの定期的なキーの再生成メッセージを使用して、キー サーバによってリフレッシュされます。KEK もキー サーバによってダウンロードされ、グループ メンバーによって、キー サーバから受信するキーの再生成メッセージの復号化に使用されます。

キー サーバによって、GDOI グループのグループ ポリシーと IPsec SA が生成されます。キー サーバによって生成される情報には、複数の TEK 属性、トラフィック暗号化ポリシー、ライフタイム、送信元と宛先、各 TEK に関連付けられるセキュリティ パラメータ インデックス（SPI）ID、キーの再生成ポリシー（1 つの KEK）などがあります。

次の図に、グループ メンバーおよびキー サーバ間の通信フローを示します。キー サーバは、グループ メンバーからの登録メッセージを受信したあと、グループ ポリシーと新しい IPsec SA を含む情報を生成します。次に、新しい IPsec SA がグループ メンバーにダウンロードされます。キー サーバでは、グループごとに、各グループ メンバーの IP アドレスを含むテーブルが保持されます。グループ メンバーが登録されると、キー サーバはメンバーの IP アドレスを関連するグループのテーブルに追加します。これにより、キー サーバは、アクティブなグループ メンバーをモニタできるようになります。1 つのキー サーバで複数のグループをサポートできます。また、1 つのグループ メンバーは、複数のグループに属することができます。

図 *4:* グループ メンバーおよびキー サーバ間の通信フロー



IPsec と ISAKMP タイマー

IPsec と ISAKMP SA は、次のタイマーによって維持されます。

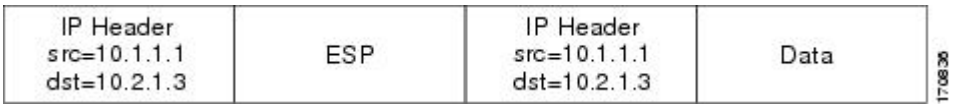
- TEK ライフタイム：IPsec SA のライフタイムを決定します。TEK ライフタイムが終了する前に、キー サーバによってキー再生成メッセージが送信されます。このメッセージには、新しい TEK 暗号キーと変換、および既存の KEK 暗号キーと変換が格納されています。TEK ライフタイムはキーサーバ上でだけ設定します。ライフタイムは、GDOI プロトコルによって各グループ メンバーに対して「プッシュ ダウン」されます。TEK ライフタイムの値はネットワークのセキュリティ ポリシーによって異なります。**set security-association lifetime** コマンドが設定されていない場合、デフォルト値である 86,400 秒が有効になります。TEK ライフタイムを設定するには、「IPsec ライフタイム タイマーの設定」セクションを参照してください。
- KEK ライフタイム：GET VPN キー再生成 SA のライフタイムを決定します。ライフタイムが終了する前に、キーサーバによってキー再生成メッセージが送信されます。このメッセージには、新しい KEK 暗号キーと変換、および新しい TEK 暗号キーと変換が格納されています。TEK ライフタイムはキー サーバ上でだけ設定します。ライフタイムは、GDOI プロトコルによって各グループ メンバーに対して動的にプッシュ ダウンされます。KEK ライフタイム値は、TEK ライフタイム値よりも大きい必要があります（KEK ライフタイム値は、TEK ライフタイム値の少なくとも 3 倍以上にすることが推奨されます）。 **rekey lifetime** コマンドが設定されていない場合、デフォルト値である 86,400 秒が有効になります。KEK ライフタイムを設定するには、「マルチキャスト キー再生成の設定」セクションを参照してください。
- ISAKMP SA ライフタイム：ISAKMP SA が期限切れになる前にどれだけの期間存在するべきかを定義します。ISAKMP SA ライフタイムは、グループ メンバーおよびキー サーバ上で設定します。グループ メンバーとキー サーバに連携可能なキー サーバがない場合、グループ メンバーの登録が終了しても ISAKMP SA は使用されません。このような（連携可能なキー サーバがない）場合、ISAKMP SA のライフタイムを短く設定できます（最小 60 秒）。連携可能なキーサーバが存在する場合は、連携可能なキーサーバの通信中に ISAKMP SA を「アップ」の状態に保つため、すべてのキー サーバのライフタイムを長く設定する必要があります。 **lifetime** コマンドが設定されていない場合、デフォルト値である 86,400 秒が有効になります。ISAKMP SA ライフタイムを設定するには、「ISAKMP ライフタイム タイマーの設定」セクションを参照してください。

アドレス保存

ここでは、GET VPN でのアドレス保存について説明します。

以下の図に示すように、IPsec で保護されたデータ パケットでは、外側の IP ヘッダーで元の送信元と宛先が伝送されます。トンネルエンドポイントのアドレスには置換されません。この技術は、IPsec Tunnel Mode with Address Preservation と呼ばれています。

図 *5:* ヘッダー保存



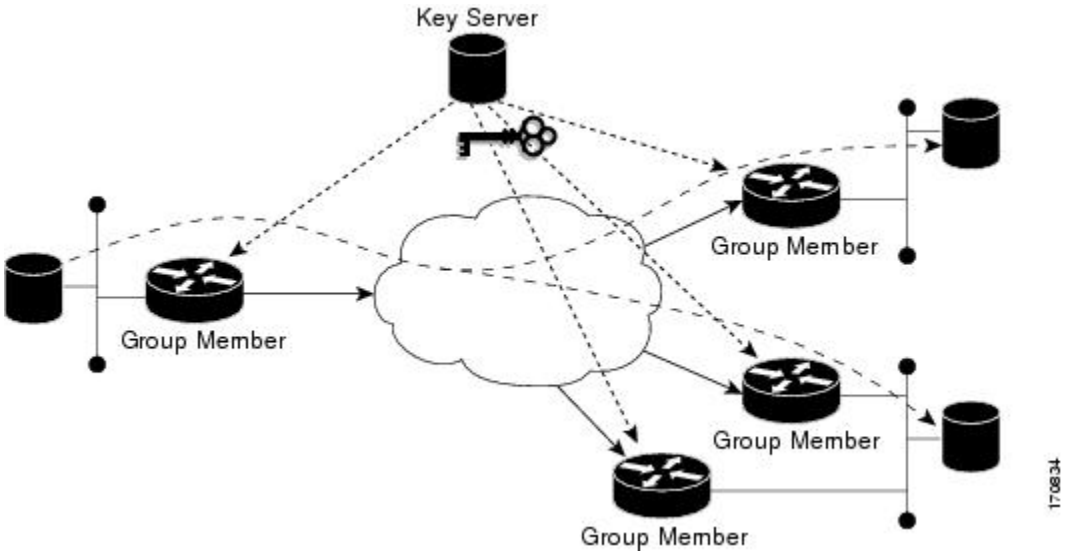
GET VPN では、アドレスが維持されるため、コア ネットワーク内のルーティング機能を使用できます。アドレスの維持によって、ネットワーク内の、宛先アドレスへのルートをアドバタイズする任意のカスタマー エッジ（CE）デバイスにパケットを配送するルーティングが可能となります。グループのポリシーに一致するすべての送信元および宛先は、同様に処理されます。アドレスの維持は、IPsec ピア間のリンクが利用できない状況では、トラフィックの「ルート不在」状況に対処するのに役立ちます。

また、ヘッダーが維持されることによって、企業のアドレス空間全体および WAN においてルーティングの継続性が維持されます。その結果、キャンパスのエンド ホスト アドレスは WAN に公開されます（MPLS では、これは WAN のエッジに適用されます）。このため、GET VPN は、WAN ネットワークが「プライベート」ネットワークとして動作する場合にだけ適用できます（MPLS ネットワークなど）。

セキュア データ プレーン マルチキャスト

マルチキャストの送信元では、キー サーバから取得される TEK が使用され、ヘッダーが保存されたマルチキャスト データ パケットが、スイッチングされる前に暗号化されます。マルチキャストパケットのレプリケーションが、マルチキャストパケット内に保持されている（S,G）ステートに基づいてコア内で実行されます。次の図に、このプロセスを示します。

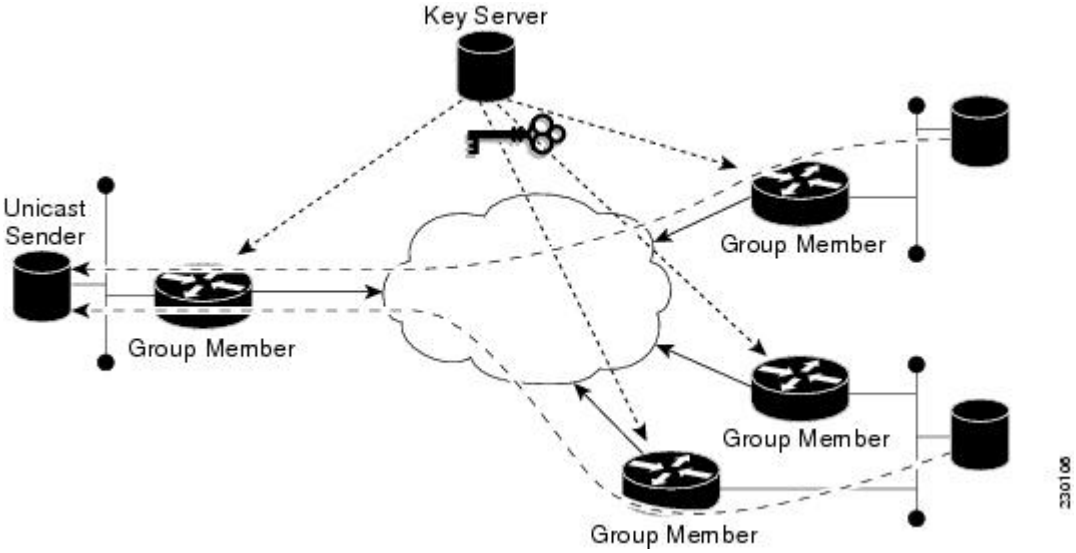
図 *6:* セキュア データ プレーン マルチキャスト プロセス



セキュア データ プレーン ユニキャスト

ユニキャストの送信元では、キー サーバから取得される TEK が使用され、ヘッダーが保存されたユニキャスト データ パケットが、宛先にスイッチングされる前に暗号化されます。次の図に、このプロセスを示します。

図 *7:* セキュア データ プレーン ユニキャスト プロセス



Cisco Group Encrypted Transport VPN の機能

キー再生成

キー再生成は IPsec SA を更新するために使用されます。IPsec SA またはキー再生成 SA の期限切れが近づくと、特定のグループの単一のキー再生成メッセージがキー サーバ上で生成されます。キー再生成の配信のために新しいIKEセッションが生成されることはありません。キー再生成メッセージは、キー サーバによって、既存の IKE SA を介して配信されます。

キー再生成では、マルチキャスト メッセージまたはユニキャスト メッセージを使用できます。GET VPN では、ユニキャスト キー再生成とマルチキャスト キー再生成の両方がサポートされています。

CSCti89255 では、KEK タイマーが期限切れになる前に KEK のキー再生成が行われます。グループ メンバーもタイマーを開始し、タイマーの期限が切れる前に更新されたキーを受け取ることを期待します。これらを受け取らない場合、グループ メンバーは KEK の期限切れの前にジッタが生じた再登録を開始します。KEK ライフタイムが期限切れになると、KEK は削除されます。これにより以下が確保されます。

- より安全な KEK の有効期限確認メカニズム
- より安全な KEK の再登録メカニズム
- 設定されたライフタイムを超える KEK の使用の回避

次のサブセクションではキー再生成の詳細情報を提供します。

キー再生成のシーケンス番号

TEK/KEK ライフタイムが終了する前に、KS は、シーケンス番号を 1 つ増やしたキー再生成メッセージを送信します。ただし、最後のキー再生成メッセージの送信以降にセカンダリ KS がプライマリ KS になった場合、新しいプライマリ KS は、キー再生成メッセージのシーケンス番号を 10 ずつ増やします。

プライマリ KS とセカンダリ KS は、20 秒ごとにシーケンス番号を同期します。

次の例は、プライマリ KS（KS1）とセカンダリ KS（KS2）で構成される展開においてキー再生成メッセージのシーケンス番号がどのように変化するのかを示しています。この例では、シーケンス番号の初期値が 1 であると想定されています。

また、展開に多数の GM があることと、KS がキー再生成メッセージの配信を再試行する必要がある場合があることも想定されています。シーケンス番号は、再試行ごとに 1 ずつ増加します。

1. キー再生成メッセージを送信する時間になると、KS1 はシーケンス番号を 2 に増やします。
2. すべての GM がメッセージを受信するように、KS1 がキー再生成メッセージを 3 回再送信するとします。再試行ごとに、シーケンス番号が 1 ずつ増加します。そのため、このキー再生成が終わったときのシーケンス番号の値は 5 です。
3. 次のキー再生成メッセージを送信する時間になると、KS1 がキー再生成メッセージを 1 回だけ送信するとします。そのため、この 2 回目のキー再生成が終わったときのシーケンス番号は 6 です。
4. 次のキー再生成メッセージが送信される前に、KS2 がプライマリ KS になるとします。
5. キー再生成メッセージを送信する時間になると、KS2 はシーケンス番号を 10 ずつ増やします。そのため、キー再生成メッセージはシーケンス番号 16 で送信されます。
6. すべての GM がメッセージを受信するように、KS2 がキー再生成メッセージを 2 回再送信するとします。再試行ごとに、シーケンス番号が 1 ずつ増加します。そのため、このキー再生成が終わったときのシーケンス番号の値は 18 です。
7. 次のキー再生成メッセージが送信される前に、KS1 がプライマリ KS になるとします。
8. キー再生成メッセージを送信する時間になると、KS1 はシーケンス番号を 10 ずつ増やします。そのため、キー再生成メッセージはシーケンス番号 28 で送信されます。KS1 がキー再生成メッセージを 1 回だけ送信するとします。キー再生成が終わったときのシーケンス番号は 28 です。
9. 次のキー再生成メッセージを送信する時間になると、KS1 はシーケンス番号を 1 ずつ増やします。KS1 がキー再生成メッセージを 1 回だけ送信するとします。キー再生成が終わったときのシーケンス番号は 29 です。

次の表に、各キー再生成動作でのシーケンス番号の変化の概要を示します。

キー再生成番号	1（3 回の再試行）	2（0 回の再試行）	3（2 回の再試行）	4（0 回の再試行）	5（0 回の再試行）

シーケンス番号	2、3、4、5	6	16、17、18	28	29

キー再生成シーケンス番号のチェック

キー サーバとグループ メンバー間のキー再生成シーケンス番号のチェックは次のように行われます。

1. GROUPKEY-PUSH メッセージのアンチリプレーは RFC 6407 で規定されているように復元されます。
   - グループ メンバーは、最後に受信したキー再生成メッセージのシーケンス番号以下の番号のキー再生成メッセージをすべてドロップします。
   - グループ メンバーは、最後に受信したキー再生成メッセージのシーケンス番号より大きい番号のキー再生成メッセージをすべて（差がどれだけ大きくても）承認します。
2. シーケンス番号は、KEK 再生成メッセージ時ではなく、KEK 再生成キーの後の最初のキー再生成メッセージ時に 1 にリセットされます。

マルチキャスト キー再生成

マルチキャスト キー再生成は、有効なマルチキャスト キー再生成が使用されて送信されます。登録が成功すると、グループ メンバーが特定のマルチキャスト グループに登録されます。グループに登録されているすべてのグループ メンバーによって、このマルチキャスト キー再生成が受信されます。マルチキャスト キー再生成は、キー サーバに設定されているライフタイムに基づいて定期的に送信されます。IPsec またはキー再生成ポリシーがキー サーバ上で変更された場合もマルチキャスト キー再生成が送信されます。設定の変更によってトリガーされると、キー再生成によって、新しく更新されたポリシーが有効なマルチキャスト キー再生成を持つすべてのグループ メンバーに送信されます。

キー サーバによって、キー再生成の時間が次のようにプッシュ バックされます。

1. TEK のタイムアウトが 300 秒の場合：

tek_rekey_offset = 90（300 < 900 のため）

再送信が設定されている場合、キー再生成タイマーがさらに戻されます。

3 つの再送信がすべて 10 秒の場合：3 * 10

その結果、キー再生成が実際に発生するのは (300 - 90 - 30) = 180 秒

2. TEK のタイムアウトが 3600 秒の場合：

tek_rekey_offset = 3600 * 10% = 360 秒

再送信が設定されている場合、キー再生成タイマーがさらに戻されます。

3 つの再送信がすべて 10 秒の場合：3 * 10

その結果、キー再生成が実際に発生するのは (3600 - 360 - 30) = 3210 秒

KEK の期限が切れ、転送モードがマルチキャストである場合、マルチキャスト KEK キー再生成が送信されます。マルチキャスト KEK が送信されると、グループ メンバーによって古い

KEK が新しい KEK に置き換えられます。これはマルチキャスト キー再生成であり、再送信が送信されるので、古い KEK は引き続き暗号化に使用されます。このような状況が発生するのは、グループ メンバーによって新しい KEK キー再生成が受信されていないためです。そのため、マルチキャスト キー再生成を受信したグループ メンバーには古い KEK は存在せず、それらの再送信は廃棄されます。

最初に KEK キーを受信せず、現在は KEK 再送信を受信して古い KEK を新しい KEK に置き換えているグループ メンバーの場合、後の再送信は廃棄されます。たとえば、5 つの再送信が設定されており、シーケンス番号が 1 のマルチキャスト KEK キー再生成がグループ メンバー 1 で受信される場合、グループ メンバーに古い KEK がないため、シーケンス番号が 2、3、4、5、6 である他のすべての再送信は廃棄されます。

グループ メンバー 2 によってシーケンス番号が 1 の KEK キー再生成が取得されず、シーケンス番号が 2 である再送信が受信された場合、他の再送信 3、4、5、6 は廃棄されます。

マルチキャスト キー再生成の設定要件

グループ メンバーがキー サーバに登録するときは、データベースに KEK SA をインストールします。キー再生成の転送がマルチキャストのとき、グループ メンバーは IGMP を使用して、キー サーバによって定義されたマルチキャスト ストリームに参加します。IGMP 参加は、暗号マップを含むインターフェイスから送信されます。

（注） IGMP トラフィックは、キー サーバで定義された ACL またはグループ メンバーのローカル拒否 ACL による暗号化から除外する必要があります。

暗号マップを使用して設定されたものと同じインターフェイス経由でキー サーバに到達できないときは、ストリームに手動で参加する必要があります。

ユニキャスト キー再生成と SA

大型のユニキャスト グループでは、遅延問題を軽減するため、キー サーバによって一度にごく少数のグループ メンバーのキー再生成メッセージだけが生成されます。すべてのグループ メンバーによって、古い SA の期限が切れる前に新しい SA の同じキー再生成メッセージが受信されることが、キー サーバには保証されています。さらに、ユニキャスト グループでは、キー サーバからのキー再生成メッセージが受信された後、グループ メンバーによって、暗号化された確認応答（ACK）メッセージが、キー再生成メッセージの一部として受信されたキーが使用されて、キー サーバに送信されます。キー サーバによって ACK メッセージが受信されると、その受信が関連するグループのテーブルに書き込まれ、次のことが実行されます。

- キー サーバにアクティブなグループ メンバーの最新リストが保管されます。
- キー サーバによって、アクティブなメンバーにだけキー再生成メッセージが送信されます。

さらに、ユニキャストグループでは、3 回連続したキー再生成が行われて ACK メッセージが 1 つもキー サーバによって受信されなかった場合、キー サーバによってアクティブ リストからグループ メンバーが削除され、その特定のグループ メンバーに対するキー再生成メッセー

ジの送信が停止されます。3 回連続したキー再生成が行われて ACK メッセージが 1 つも受信されなくても、グループ メンバーがキー再生成メッセージを受信する必要がある場合には、現在の SA が期限切れになった後には、グループ メンバーはキー サーバに完全に再登録される必要があります。非応答グループ メンバーのイジェクトは、キー サーバがユニキャスト キー再生成モードで動作している場合にだけ行われます。マルチキャスト キー再生成モードでは、キー サーバによるグループ メンバーの排出は行われません。そのモードでは、グループ メンバーが ACK メッセージを送信できないからです。

マルチキャスト キー再生成におけるのと同様、再送信が設定されている場合、各キー再生成は、設定された回数再送信されます。

キー再生成転送モードおよび認証は、GDOI グループ下で設定できます。

ユニキャスト キー再生成転送モードが定義されていない場合、デフォルトでマルチキャストが適用されます。

TEK キー再生成が受信されなかった場合、現在の IPsec SA が期限切れになる 60 秒前にグループ メンバーがキー サーバに再登録されます。グループ メンバーの再登録が発生する前に、キー サーバによってキー再生成が送信される必要があります。再送信が設定されていない場合、SA が期限切れになる前に、キー サーバによってキー再生成 tek_rekey_offse が送信されます。tek_rekey_offset は、設定されているキー再生成ライフタイムに基づいて算出されます。TEK キー再生成のライフタイムが 900 秒より短い場合、tek_rekey_offset は 90 秒に設定されます。TEK キー再生成のライフタイムが 900 秒を超えるように設定されている場合、rekey_offset = (設定されている TEK キー再生成のライフタイム)/10 となります。再送信が設定されている場合、SA が期限切れになる 90 秒前に最新の再送信が送信されるように、tek_rekey_offset よりも前にキー再生成が発生します。

キー サーバでは、すべてのユニキャスト グループ メンバーに対するキー再生成の送信をいつ開始するか計算するために、次の例に示す数式が使用されます。キー サーバにおけるユニキャスト キー再生成処理によって、1 回のループで 50 のグループにおけるユニキャスト グループ メンバーに対してキー再生成が送信されます。このループ内でかかる時間は推定 5 秒です。

キー サーバによって、50 のグループのグループ メンバーのキー再生成が行われます。これは 2 回のループに相当します。たとえば、グループ メンバーの数が 100 の場合：

キー再生成ループの数 = (100 グループ メンバー)/50 = 2 ループ：

- 1 回のループでのキー再生成にかかる時間（推定）= 5 秒
- 50 の 2 回ループにおける 100 グループ メンバーに対するキー再生成にかかる時間：2 * 5 秒 = 10 秒

そのため、キー サーバによって、キー再生成の時間が次のようにプッシュ バックされます。

- TEK のタイムアウトが 300 の場合：300 - 10 = 290

ただし、開始は TEK が期限切れになるよりも前である必要があります（マルチキャストの場合と同じです）。

- 300 < 900 であるため、tek_rekey_offset = 90
- そのため、実際の TEK 時間から 90 秒を引いて、290 - tek_rekey_offset = 200 秒

再送信が設定されている場合、キー再生成タイマーがさらに戻されます。

- 3 つの再送信がすべて 10 秒の場合：200 - (3 * 10) = 170
- TEK のタイムアウトが 3600 秒である場合：3600 - 10 = 3590

ただし、開始は TEK が期限切れになるよりも前である必要があります（マルチキャストの場合と同じです）。

- 3600 > 900 であるため、tek_rekey_offset = 3600 * 10% = 360
- そのため、実際の TEK 時間から 360 秒を引いて、3590 - tek_rekey_offset = 3230 秒

再送信が設定されている場合、キー再生成タイマーがさらに戻されます。

- 3 つの再送信がすべて 10 秒の場合：3230 - (3 * 10) = 3200 秒

数式 tek_rekey_offset は、ユニキャストおよびマルチキャスト キー再生成に適用されます。

ポリシー変更後のキー再生成の動作

次の表に、セキュリティ ポリシーの変更に対応したキー再生成の動作の一覧を示します。

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。
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は、即座に新しいアクセス コントロール リスト（ACL）が使用されます。古い SA は SA データベース内に保存されたままになります。
TEK：リプレイ カウンタのイネーブル化	Yes	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。

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：リプレイ カウンタの変更	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	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：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	変更は次のキー再生成時に適用されます。
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。

ポリシーの変更を即時に有効にするには、次の手順に従います。

- キーサーバーで **clear crypto gdoi** [**group**] コマンドを使用します。
- すべてのグループメンバーで **clear crypto gdoi** [**group**] コマンドを使用します。

（注） キー サーバは管理者がコンフィギュレーション モードを終了するとポリシーの更新のためのキー再生成を送信し、適切な場合にキー再生成が送信されるようにします。

（注） グループ メンバーで双方向モードに変更する前のパッシブ モードの動作は次のとおりです。

キー サーバの SA モードを「no sa receive-only」に変更し、コンフィギュレーション モードを終了する場合、キー再生成はグループ メンバーに送信され、「受信専用」から「発信オプション」にグループ メンバーの状態が変化するのを確認できます。組み込みタイマーによって設定されたインターバル（約 5 分）の後は「両方」に状態が変化します。

キー サーバはこの状態をすぐに「両方」として示します。すべてのグループ メンバーが更新される過程である可能性があるため、これは意図的に行われます。

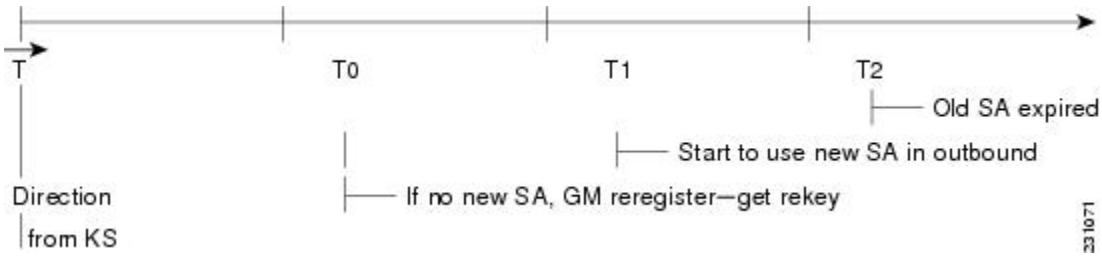
グループ メンバーにおけるIPsec SA の使用

グループ メンバー上でキー再生成が受信され、処理されると、新しい IPsec SA（SPI）がインストールされます。古い IPsec SA と新しい IPsec SA が共に使用される期間が存在します。指定された一定期間の経過後に、古い IPsec SA は削除されます。この重複によって、すべてのグループ メンバーが現在のキー再生成を受信し、新しい IPsec SA を追加できます。この動作は、キー サーバからのキー再生成のための転送モード（マルチキャストまたはユニキャスト キー再生成転送）とは無関係です。

グループ メンバー上では、古い SA が期限切れになる約 30 秒前に、グループ メンバーによって、パケットを暗号化するために発信方向で新しい SA が使用されます。古い SA が期限切れになる約 60 秒前にキー サーバからのキー再生成を介して新しい SA がグループ メンバー側で受信されていない場合、グループ メンバーが登録されます。

次の図では、時間 T2 が古い SA が期限切れになる時間です。T1 が T2 の 30 秒前で、これは、グループ メンバー（GM）によって発信方向で新しい SA の使用が開始される時間です。T0 は、T2 の 30 秒前です。T0 の時点で新しい SA が受信されない場合、グループ メンバーが登録される必要があります。T は、T0 の 30 秒前です。T の時点でキー サーバによってキー再生成が送信される必要があります。

図 *8 : グループ メンバーにおける IPsec SA* の使用



設定変更によってキー サーバごとのキー再生成のトリガーが可能

（注） セキュリティに対する脅威は、脅威からの保護に役立つ暗号化技術と同様に絶え間なく変化しています。最新のシスコの暗号化に関する推奨事項については、『Next Generation Encryption』（NGE）ホワイト ペーパーを参照してください。

キー サーバ上の設定変更によって、キー サーバごとの再生成のトリガーが可能です。次のサンプル設定を参照し、サンプルに記述されたもののうち、キー再生成が発生する変更と発生しない変更を確認してください。

```
crypto ipsec transform-set gdoi-p esp-aes esp-sha-hmac
!
crypto ipsec profile gdoi-p
 set security-association lifetime seconds 900
set transform-set gdoi-p
!
crypto gdoi group diffint
 identity number 3333
 server local
```

```
rekey algorithm aes 128
rekey address ipv4 121
rekey lifetime seconds 3600
no rekey retransmit
rekey authentication mypubkey rsa mykeys
sa ipsec 1
 profile gdoi-p
 match address ipv4 120
 replay counter window-size 3
```

次に示すキーサーバ上での設定変更では、キーサーバからのキー再生成がトリガーされます。

- TEK 設定におけるすべての変更（例の「sa ipsec 1」）。
  - ACL（上記例の「match address ipv4 120」）が変更された場合。ACL におけるすべての追加、削除、または変更がキー再生成の原因となります。
  - TEK リプレイがキー サーバ上でイネーブルまたはディセーブルになっている場合、キー再生成が送信されます。
  - TEK 内の IPsec プロファイルの削除または追加（例の「profile gdoi-p」）。
  - マルチキャストからユニキャスト転送への変更。
  - ユニキャストからマルチキャスト転送への変更。

次に示すキー サーバ上での設定変更は、キー サーバからのキー再生成のトリガーとはなりません。

- TEK 下におけるリプレイ カウンタ ウィンドウ サイズの変更（例の「sa ipsec 1」）。
- キー再生成再送信の設定または削除。
- キー再生成 ACL の削除または設定。
- TEK ライフタイムの変更（上記例の「set security-association lifetime seconds 300」）または KEK ライフタイムの変更（例の「rekey lifetime seconds 500」）。
- キー再生成アルゴリズムの追加、削除、または変更（例の「rekey algorithm aes 128」）。

キー再生成をトリガーするコマンド

次の表は、GET VPN コマンドによる変更の包括的な一覧です。どのコマンドがキー再生成のトリガーとなり、どのコマンドがならないのかを示しています。各コマンドは、それらのコマンドが入力されるコンフィギュレーションモードに基づいて分類しています。表には、キー再生成のトリガーになるか否かを問わず、コマンドが有効になるタイミングも示しています。

（注） GDOI グループで KEK ライフタイムが変更されると、現在の KEK が期限切れになり、新しい KEK が生成された場合にのみ変更が適用されます。キーサーバーでキー再生成コマンドの **crypto gdoi ks rekey** を発行することにより、強制的に変更を適用できます。

表 *2:* キー再生成をトリガーするコマンド

説明	コマンド	キー再生成のトリガーとなるか	トリガーするタイミング	変更が有効になるタイミング
Mode = (config)	**configure terminal**	—	—	—
GDOI グループ内で使用される ACL の変更または削除（例：**rekey address ipv4** *access-list-number*[*options*]）	[**no**] **access-list** *access-list-number*[*options*]	非対応	—	即時
IPsec プロファイルで使用される ACL の変更または削除（例：**match address ipv4** *access-list-id* | *name*[*options*]）	[**no**] **access-list** *access-list-number*[*options*]	Yes	コンフィギュレーションモードの終了時	キーサーバー上での **show running-config** コマンドの出力は、ポリシーが不完全である、パケットがまだ既存の SA によって暗号化または復号されている、ダウンロードされた ACL は消去されたが mtree エントリがまだ存在している（**show crypto ruleset** コマンドの出力を表示することによる）、および、新しい SA がダウンロードされず、古い SA が暗号化または復号でまだアクティブであることを示します。
ISAKMP 事前共有キー（任意のキー）の追加または削除	**crypto isakmp key address** *peer-address*	非対応	—	即時

説明	コマンド	キー再生成のトリガーとなるか	トリガーするタイミング	変更が有効になるタイミング
ISAKMP 事前共有キー（グループ メンバーのキー）の追加または削除	**crypto isakmp key address** *peer-address*	非対応	—	Key Encryption Key（KEK）SA が期限切れになった後（再登録）
IPsec プロファイルの追加	**crypto ipsec profile**	非対応	—	即時
ISAKMP ポリシーの追加または削除	**crypto isakmp policy** *priority*	非対応	—	即時
Mode = (ipsec-profile)	**crypto ipsec profile** *name*	—	—	—
（IPsec プロファイル内の）SA ライフタイムの変更	**set security-association lifetime** *seconds*	非対応	—	次のキー再生成
トランスフォームセットの変更	**set transform-set** *transform-set-name*	Yes	コンフィギュレーション モードの終了時	古いトランスフォーム セットの 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。
Mode = (config-gdoi-group)	**crypto gdoi group** *group-name*	—	—	—
ID 番号の変更	**identity number** *number*	非対応	—	グループ メンバー上でただちに設定する必要があります。他のグループ メンバーでは、古いグループ ID の TEK および KEK が引き続き使用されます。
Mode = (gdoi-local-server)	**server local**	—	—	—
ユニキャストからマルチキャスト転送への変更	**rekey transport unicast**	Yes	即時	キー再生成がトリガーされた後

説明	コマンド	キー再生成のトリガーとなるか	トリガーするタイミング	変更が有効になるタイミング
マルチキャストからユニキャスト転送への変更	[**no**] **rekey transport unicast**	Yes	コンフィギュレーションモードの終了時	キー再生成がトリガーされた後
キー再生成アドレスの変更	**rekey address ipv4** {*access-list-number* | *access-list-name*}	Yes	コンフィギュレーションモードの終了時	キー再生成がトリガーされた後（ただし、ACL自体を変更してもマルチキャストキー再生成はトリガーされません)
キー再生成ライフタイムの変更	**rekey lifetime seconds** *number-of-seconds*	非対応	—	次のキー再生成。ただし、コマンドが発行される（現在のライフタイムがキー再生成と共に送信される）と、ライフタイムは減少を開始します。
キー再生成再送信のイネーブル化またはディセーブル化	**rekey retransmit** *number-of-seconds* [**number** *number-of-retransmissions*]	非対応	—	次のキー再生成
キー再生成認証のイネーブル化	**rekey authentication mypubkey rsa** *key-name*	Yes	コンフィギュレーションモードの終了時	キー再生成がトリガーされた後
キー再生成認証のディセーブル化	[**no**] **rekey authentication**	非対応	—	即時

説明	コマンド	キー再生成のトリガーとなるか	トリガーするタイミング	変更が有効になるタイミング
キー再生成認証キーの変更	**rekey authentication mypubkey rsa** *key-name*	Yes	コンフィギュレーションモードの終了時	キー再生成がトリガーされた後
キー再生成暗号化の変更	**rekey algorithm** *type-of-encryption-algorithm*	Yes	コンフィギュレーションモードの終了時	新しいアルゴリズムは即座に有効になります。
Mode = (gdoi-sa-ipsec)	**sa ipsec** *sequence-number*	—	—	—
プロファイルの変更	**profile** *ipsec-profile-name*	Yes	コンフィギュレーションモードの終了時	ライフタイムが期限切れになるまで古いプロファイルの SA は有効のままです。
ACL の一致の変更	**match address** [options]	Yes	コンフィギュレーションモードの終了時	キー再生成がトリガーされた後
カウンタ リプレイのイネーブル化	**replay counter window-size** *seconds*	Yes	コンフィギュレーションモードの終了時	ライフタイムが期限切れになるまでカウンタリプレイなしの古い SA は非アクティブになります。
リプレイ カウンタ値の変更	**replay counter window-size** *seconds*	非対応	—	次のキー再生成

説明	コマンド	キー再生成のトリガーとなるか	トリガーするタイミング	変更が有効になるタイミング
時間ベースのアンチ リプレイのイネーブル化	**replay time window-size** *seconds*	Yes	コンフィギュレーション モードの終了時	時間ベースのアンチリプレイがイネーブルになった新しい SA が送信されますが、時間ベースのアンチリプレイがディセーブルになった古い 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。
時間ベースのアンチ リプレイ ウィンドウの変更	**replay time window-size** *seconds*	非対応	—	新しい時間ベースのアンチリプレイウィンドウが有効になるのは、キーサーバーとグループメンバーの両方で **clear crypto gdoi** コマンドが入力された後だけです。
Mode = (gdoi-coop-ks-config)	**redundancy**	—	—	—
冗長性のイネーブル化	**redundancy**	非対応	—	他の各キーサーバ上でただちに設定する必要があります。
ローカル プライオリティの変更	**local priority** *number*	非対応	—	即時にですが、キーサーバに選択は強要しません。
ピア アドレスの追加または削除	[**no**] **peer address ipv4** *ip-address*	非対応	—	次の連携可能な（COOP）メッセージ

説明	コマンド	キー再生成のトリガーとなるか	トリガーするタイミング	変更が有効になるタイミング
冗長性のディセーブル化	[**no**] **redundancy**	非対応	—	他の各キーサーバ上でただちに設定する必要があります。

疑似時間同期によってタイムアウトが発生した場合、KEK タイマーまたは TEK タイマーのどちらかが次の 60 秒間に期限切れになるようにスケジュールされているかどうかがキー サーバによって確認されます。そのようにスケジュールされている場合、そのタイムアウトと疑似時間同期タイムアウトが結合されます。つまり、そのキー再生成は TEK キー再生成または KEK キー再生成と、疑似時間同期タイムアウトキー再生成の両方として動作します。疑似時間同期の詳細については、「時間ベースのアンチ リプレイ」セクションを参照してください。

キー再生成の再送信

マルチキャストキー再生成は、デフォルトで再送信されます。ユニキャストキー再生成では、キー サーバが ACK を受信しない場合にキー再生成が再送信されます。どちらの場合も、キー再生成の再送信前に、次の 120 秒間にスケジュールされている TEK キー再生成または KEK キー再生成があるかどうかがキーサーバによって確認されます。ある場合、現在の再送信は停止され、スケジュールされたキー再生成が発生するまで待機します。

グループ メンバー アクセス コントロール リスト

GET VPN の場合、保護する必要があるトラフィックは、 ACL によってキー サーバ上にスタティックに定義されます。グループ メンバーによって、キー サーバから保護対象に関する情報が取得されます。この構造によって、キーサーバによる必要に応じたポリシーの動的な選択および変更が可能となっています。Secure Multicast では、キー サーバの ACL が包括的に定義されます。ACLには、暗号化する必要があるトラフィックだけが厳密に定義されているだけでなく、暗黙の拒否によって、他のすべてのトラフィックは暗号化されない状態で許可されるようになっています（つまり、許可がない場合、他のすべてのトラフィックは許可されます）。

GET VPN では、異なる考え方が採用されています。つまり、暗号化する必要のあるパケットの定義が独立して配信されます。GET VPN でサポートしているのはスタティックに定義されたトラフィック セレクタだけです。キー サーバ上で、拒否 ACL と許可 ACL の両方を使用してポリシーを定義できます。グループ メンバー上で、手動で設定できるのは拒否 ACL だけです。キー サーバからダウンロードされるポリシーと、グループ メンバー上で設定されるポリシーは結合されます。グループ メンバー上で設定された ACL はすべて、キー サーバからダウンロードされたものよりも優先されます。

グループ メンバーによってキー サーバから ACL が取得されると、グループ メンバーによって、一時的な ACL が作成され、それがデータベースに挿入されます。何らかの理由によりグループ メンバーが GDOI グループから削除されると、この ACL は削除されます。パケットが

ACL に一致しているが、そのパケット用に IPsec SA が存在していない場合、インターフェイスから出ていくパケットは、グループ メンバーによって廃棄されます。

キー サーバによって一連のトラフィック セレクタが送信され、それらがグループ メンバー上のグループ メンバー ACL と正確には一致していない場合があります。このような違いが発生した場合、その違いを結合して解決する必要があります。グループ メンバーは、キー サーバよりもトポロジを認識するので、ダウンロードされた ACL は、グループ メンバー ACL の末尾に追加されます。グループ メンバー ACL（暗黙の拒否を除く）が最初にデータベースに挿入され、次に、ダウンロードされたキー サーバ ACL が挿入されます。このデータベースは優先化され、一致したエントリが検出された時はいつでも、データベース検索は終了します。

グループ メンバー ACL の設定方法については、「グループ メンバー ACL の設定」セクションを参照してください。

セキュリティ ポリシー変更時におけるグループ メンバーの動作

キー サーバで ACL または他のポリシーが変更されると、グループ メンバーの動作が変わります。次の 3 種類のシナリオで、グループ メンバーの動作に対するポリシーの各種変更の影響を説明します。

シナリオ 1

次の例では、ホスト A とホスト B を許可するように ACL が最初に設定されています。

```
ip access-list extended get-acl
permit ip host A host B
permit ip host B host A
```

次に、キー サーバで、ホスト C とホスト D を許可するように ACL が変更されます。

```
ip access-list extended get-acl
permit ip host C host D
permit ip host D host C
```

ACL の変更は、次の方法でグループ メンバーの動作に影響を与えます。

- キー サーバによって、ただちに、すべてのグループ メンバーに対してキー再生成が送信されます。
- キー再生成後ただちに、グループメンバーによって、ホストAとホストB間のトラフィックが暗号化されていないテキストで送信されます。
- キー再生成後ただちに、グループメンバーによって、ホストCとホストD間のトラフィックが暗号化されたテキストで送信されます。

（注） Cisco ASR 1000 シリーズ アグリゲーション サービス ルータと Cisco ISR G2 ルータの GETVPN グループメンバーは、キーサーバーでの ACL の変更またはその他のポリシー変更に続くキー再生成（トリガーまたは定期的）の後に、異なる動作をします。Cisco ISR G2 ルータのグループメンバーは、完全な再登録なしで新しいポリシーをインストールしますが、Cisco ASR 1000 シリーズ アグリゲーション サービス ルータのグループメンバーは、更新されたポリシーを取得するために再登録します。

シナリオ 2

ポリシーによってトランスフォームセットが更新され、時間ベースのアンチリプレイ（TBAR）の変更がキー サーバに対して行われると、グループ メンバーの動作が変わります。

このシナリオでは、次のことが想定されています。

- トランスフォーム セットが、ESP-3DES から ESP-AES へ変更されている。
- ポリシーの変更は、現在の TEK ライフタイムが期限切れになる 1000 秒前に発生する。

これらのポリシーの変更は、次のようにグループ メンバーの動作に影響を与えます。

- キー サーバによって、古い SA（3DES）と新しい SA（AES）の両方のキー再生成が送信されます。
- グループ メンバーでは、期限切れになるまでの 1000 秒間、古い SA（3DES）の使用が継続されます。
- 古い SA が期限切れになると、グループ メンバーによって、新しい SA（AES）に自動的に切り替えられます。

シナリオ 3

キー サーバで、ACL の変更と、トランスフォーム セットや TBAR など他の変更の両方を含むその他のポリシーの更新が行われると、グループ メンバーの動作が変わります。

このシナリオでは、次のことが想定されています。

- ACL がシナリオ 1 で指定されたとおりに更新されている。
- トランスフォーム セットが、ESP-3DES から ESP-AES へ変更されている。
- ポリシーの変更は、現在の TEK ライフタイムが期限切れになる 1000 秒前に発生する。

ACL の変更とその他のポリシーの更新は、次のようにグループ メンバーの動作に影響を与えます。

- キーサーバによって、古いSA（3DES）と新しいSA（AES）の両方で構成されているキー再生成が送信されます。
- キー再生成後ただちに、グループ メンバーによって、ホストAとホストB間のトラフィックが暗号化されていないテキストで送信されます。
- グループ メンバーによって、TEK のライフタイムが期限切れにならない限り 1000 秒間、古い SA（3DES）を使用した、ホスト C とホスト D 間の暗号化されたトラフィックが送信されます。
- 古い SA（3DES）が期限切れになると、グループ メンバーによる新しい SA への切り替えが自動的に行われ、AES におけるホスト C とホスト D 間のトラフィックが暗号化されます。

時間ベースのアンチリプレイ

アンチ リプレイは、IPSec（RFC 2401）のようなデータ暗号化プロトコルにおいて重要な機能の 1 つです。アンチ リプレイによって、第三者が IPsec カンバセーションを盗聴したり、パケットを盗んだり、さらにはそれらのパケットを後でセッションに挿入したりすることを防ぐことが可能です。時間ベースのアンチ リプレイ メカニズムを利用すれば、過去にすでに到着しているはずのリプレイ パケットを検出することによって、無効なパケットを廃棄できます。

GET VPN では、マルチセンダ トラフィック用のアンチ リプレイ保護を提供するために、同期アンチ リプレイ（SAR）が使用されています。SAR は、実社会のネットワーク タイム プロトコル（NTP）クロックや、シーケンシャル カウンタ メカニズム（パケットが送信順に受信されて処理されることを保証するメカニズム）とは独立しています。SAR クロックは、ルール正しく進みます。このクロックによって追跡される時間は、疑似時間と呼ばれます。疑似時間はキー サーバ上で維持され、キー再生成メッセージ内で指定されているグループ メンバーに対して、pseudoTimeStamp というタイムスタンプ フィールドとして定期的に送信されます。GET VPN では、Metadata というシスコ独自のプロトコルによって、psuedoTimeStamp をカプセル化しています。グループ メンバーは、定期的にキー サーバの疑似時間に再同期される必要があります。キー サーバの疑似時間は、最初のグループ メンバーが登録されたときから進み始めます。最初は、登録プロセス中に、キー サーバからグループ メンバーに対して、キー サーバの現在の疑似時間の値およびウィンドウ サイズが送信されます。時間ベースのリプレイ対応情報、ウィンドウ サイズ、キー サーバの疑似時間などの新しい属性は、SA ペイロード（TEK）で送信されます。

グループ メンバーは、疑似時間を使用して次のようにリプレイを防止します。pseudoTimeStamp には、送信者がパケットを作成したときの疑似時間の値が含まれています。受信者は、送信者の疑似時間の値と自身の疑似時間の値を比較して、パケットが再送されたパケットであるかどうかを判断します。受信元では、時間ベースのアンチリプレイ「ウィンドウ」を利用して、そのウィンドウ内のタイプスタンプ値が格納されたパケットを受信します。ウィンドウ サイズは、キー サーバで設定されて、すべてのグループ メンバーに送信されます。

（注） グループ メンバーとして Cisco VSA を使用している場合、時間ベースのアンチ リプレイは使用しないでください。

次の図は、アンチリプレイ ウィンドウを示しています。値PTrは受信者のローカルの疑似時間を、W はウィンドウ サイズを示しています。

図 *9:* アンチリプレイ ウィンドウ

クロック同期

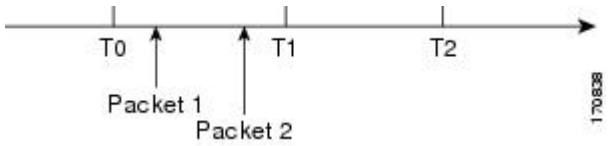
グループ メンバーのクロックとキー サーバとの同期は、ずれたり失われたりする可能性があります。クロックの同期を維持するため、キー サーバの最新の疑似時間値が格納されたキー再生成メッセージ（マルチキャストがユニキャストかは状況に応じます）が（キー再生成メッセージで、あるいは、グループ メンバーに対して最小で30分ごとに）定期的に送信されます。このアンチ リプレイ チェックでパケットにエラーが発生した場合、送信元および受信元の両方の疑似時間がプリントされ、エラー メッセージが生成され、カウントの値が増分されます。

アンチリプレイの統計情報を表示するには、送信元および受信元デバイスの両方で **show crypto gdoi group** *group-name* **gm replay** コマンドを使用します。管理者がサイズ設定のリプレイ方法に影響を与えるような設定変更を行った場合、キー サーバによってキー再生成メッセージが発信されます。

インターバル期間

ティックは、SAR クロックのインターバル期間です。この期間に送信された各パケットの pseudoTimeStamp は同じものになります。またティックは、キー サーバからの疑似時間と共にグループ メンバーにダウンロードされます。たとえば、次の図に示すように、T0 と T1 の間で送信されたパケットの pseudoTimeStamp は同じ T0 になります。SAR には、ルーズなアンチ リプレイ保護が用意されています。リプレイされたパケットは、それらがウィンドウ内にリプレイされている場合は、受信されます。デフォルトのウィンドウ サイズは 100 秒です。パケットのリプレイを最小限に抑えるため、ウィンドウ サイズを小さく保つことを推奨します。

図 *10 : SAR* クロックのインターバル期間



アンチ リプレイ設定

アンチ リプレイ機能をキー サーバ上の IPsec SA 下でイネーブルにするには、次のコマンドを使用します。

- **replay time window-size**：非シーケンシャルまたは時間ベースモードがサポートされるリプレイ時間オプションをイネーブルにします。ウィンドウ サイズは秒単位です。このモードは、1 つのグループ内に 3 つ以上のグループ メンバーが存在している場合にだけ使用します。
- **replay counter window-size**：シーケンシャルモードをイネーブルにします。このモードは、1 つのグループ内に 2 つのグループ メンバーだけが存在している場合に便利です。
- **no replay counter window-size**：アンチリプレイをディセーブルにします。

コントロール プレーンの時間ベースのアンチリプレイ

キー再生成疑似時間のチェック

キーサーバとグループメンバー間のキー再生成疑似時間のチェックは次のように行われます。

- グループメンバーがキーサーバと自身との疑似時間の許容差を計算します。データプレーンで設定された TBAR ウィンドウ サイズ、または 30 秒の小さい方となります。
- グループメンバーは自身より疑似時間が大きいすべてのキー再生成を受け入れ、自身の疑似時間をより大きい値に更新します。計算された疑似時間の許容差よりも差が大きい場合は、次の syslog メッセージも生成されます。

```
*Jul 28 22:56:37.503: %GDOI-3-PSEUDO_TIME_LARGE: Pseudotime difference between key server
 (20008 sec) and GM (10057 sec) is larger than expected in group GET. Adjust to new
pseudotime
```

- グループメンバーが自身よりも疑似時間が小さいが許容差以内のキー再生成を受信した場合、グループメンバーはキー再生成を受け入れ、疑似時間値をそのキー再生成疑似時間値に更新します。
- グループメンバーが自身よりも疑似時間が小さいが許容差を超えているキー再生成を受信した場合、グループメンバーはキー再生成メッセージをドロップし、次の syslog メッセージを生成します。

```
*Jul 28 23:37:59.699: %GDOI-3-PSEUDO_TIME_TOO_OLD: Rekey received in group GET is too
old and fail PST check: my_pst is 22490 sec, peer_pst is 10026 sec, allowable_skew is
30 sec
```

セカンダリ キー サーバでの ANN メッセージ疑似時間の処理

連携キー サーバ間のポリシーおよびグループメンバー情報の同期には、連携キー サーバ通知（ANN）メッセージが使用されます。

セカンダリ サーバ キーは次のように ANN メッセージを処理します。

- セカンダリ キー サーバが ANN メッセージの許容疑似時間を計算します。データ プレーンで設定された TBAR ウィンドウ サイズの値、または 30 秒の小さい方となります。
- セカンダリ キーサーバが疑似時間がより大きいプライマリ キーサーバから ANN メッセージを受信した場合、次が行われます。
- 疑似時間をプライマリ キー サーバの値に更新します。
- 疑似時間の差が許容差よりも大きい場合は、次の syslog メッセージが生成されます。

```
*Jul 28 23:48:56.871: %GDOI-4-GDOI_ANN_TIMESTAMP_LARGE: COOP_KS ANN received from KS
10.0.8.1 in group GET has pseudotime bigger than myself. Adjust to new pseudotime:
my_old_pst is 23147 sec, peer_pst is 30005 sec
```

- セカンダリ キーサーバが疑似時間がより小さいプライマリ キーサーバから ANN メッセージを受信した場合、次のようになります。

- 差が許容範囲内の場合、セカンダリ キー サーバはそれを受け入れ、疑似時間をプライマリ キー サーバの値に更新します。
- 差が許容範囲を超える場合は、次の syslog メッセージが生成されます。

```
*Jul 28 23:42:12.603: %GDOI-4-GDOI_ANN_TIMESTAMP_TOO_OLD: COOP_KS ANN from KS 10.0.8.1
in group GET is too old and fail PST check:
my_pst is 22743 sec, peer_pst is 103 sec, allowable_skew is 10 sec
```

3 つの再送信要求の後、セカンダリ キー サーバが有効な疑似時間の ANN メッセージを受信していない場合は、次のように、新しいグループメンバー登録のブロックが開始されます。

```
*Jul 28 23:38:57.859: %GDOI-5-COOP_KS_VALID_ANN_TIMER_EXPIRED: This sec-KS has NOT
received an ANN with valid pseudotime for an extended period in group GET. It will block
 new group members registration temporarily until a valid ANN is received
*Jul 29 00:08:47.775: %GDOI-5-COOP_KS_BLOCK_NEW_GM_REGISTER: This key server temporarily
 blocks group member with ip-addr 10.0.0.2 from registering in group GET as it has not
received an ANN with valid pseudotime for prolonged period
```

セカンダリ キー サーバは、次のいずれかが発生するとグループ メンバー登録機能を再開します。

- プライマリ キー サーバから有効な疑似時間の ANN を受け取る。
- プライマリ キー サーバになる。
- **clear crypto gdoi group** コマンドはセカンダリキーサーバーで実行されます。

プライマリ キー サーバでの ANN メッセージ疑似時間の処理

プライマリ サーバ キーは次のように ANN メッセージを処理します。

- ANN メッセージの許容疑似時間を計算します。データ プレーンで設定された TBAR ウィンドウ サイズの値、または 30 秒の小さい方となります。
- 疑似時間が小さいが許容差以内のセカンダリ キー サーバ ANN メッセージは受け入れられます。
- 疑似時間が小さいが許容差を超えている ANN メッセージは拒否されます。

ネットワークのマージ中は、次の条件が適用されます。

- 新しいプライマリ キー サーバは 2 つのキー サーバ間で大きい方の疑似時間を常に選択します。
- 差が計算された疑似時間の許容差よりも大きい場合、新しいプライマリ キー サーバはキー再生成をすべてのグループ メンバーに対して送信し、疑似時間を更新します。また、次の syslog メッセージも生成されます。

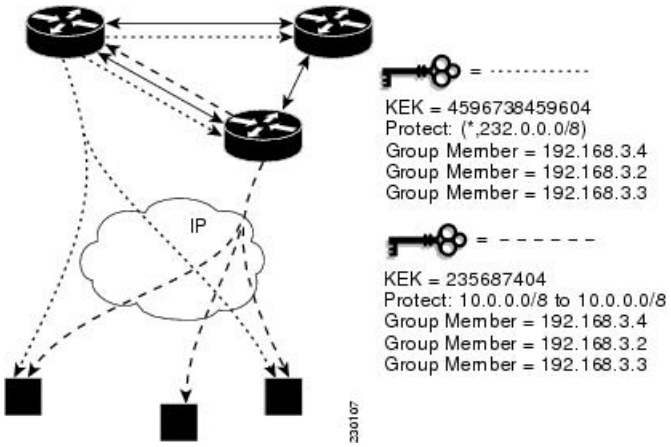
```
*Jul 28 23:42:41.311: %GDOI-5-COOP_KS_ELECTION: KS entering election mode in group GET
(Previous Primary = NONE)
*Jul 28 23:42:41.311: %GDOI-4-GDOI_ANN_TIMESTAMP_LARGE: COOP_KS ANN received from KS
10.0.9.1 in group GET has PST bigger than myself. Adjust to new pseudotime:
my_old_pst is 0 sec, peer_pst is 22772 sec
```

```
*Jul 28 23:43:16.335: %GDOI-5-COOP_KS_TRANS_TO_PRI: KS 10.0.8.1 in group GET transitioned
 to Primary (Previous Primary = NONE)
*Jul 28 23:43:16.347: %GDOI-5-KS_SEND_UNICAST_REKEY: Sending Unicast Rekey for group GET
 from address 10.0.8.1 with seq # 1
```

連携キー サーバ

次の図は、連携キー サーバのキー配布を示したものです。図の下のテキストで、連携キー サーバ機能について説明します。

図 *11* : 連携キー サーバのキー配布



連携キー サーバを利用すると、GET VPN に冗長性が与えられます。冗長性、高可用性、およびプライマリ キー サーバに障害が発生した場合の素早いリカバリを確保するために、複数のキー サーバが GET VPN によってサポートされます。複数の連携 GDOI キー サーバによって、共同でグループの GDOI 登録が管理されます。各キー サーバはアクティブなキー サーバであり、各グループ メンバーからの GDOI 登録要求を処理します。キー サーバどうしで連携しているので、各キー サーバから、そのキー サーバに登録するグループ メンバーに対して同じ状態が配信されます。それぞれの GDOI キー サーバによって、GDOI 登録の一部を処理できるので、ロードバランスが実現します。

プライマリ キーの役割は、グループ ポリシーの作成と配信です。連携キー サーバのキー配布が発生すると、1 つのキー サーバが自身をプライマリとして宣言し、ポリシーを作成し、そのほかのセカンダリ キー サーバにポリシーを送信します。セカンダリ キー サーバは、ポリシーを取得して選択モードを終了すると、プライマリ キー サーバをプライマリ キー サーバとして宣言します。また、セカンダリ キー サーバは、連携キー サーバのキー配布が進行している間、GM 登録をブロックします。この変更により時間が短縮されるため、連携キー サーバの配布はより効率的になります。たとえば、配布時には次のような syslog の警告メッセージが表示されます。

```
00:00:16: %GDOI-5-COOP_KS_BLOCK_NEW_GM_REGISTER_ELECTION: This KS temporarily blocks GM
 with ip-addr 10.0.4.1 from registering in group diffint as the KS election is underway
```

プライマリ キー サーバによってグループ情報のアップデートが他のすべてのキー サーバに定期的に送信（またはブロードキャスト）され、その結果、これらのサーバどうしの同期が維持されます。何らかの理由によりセカンダリ キー サーバがアップデートの受信に失敗した場合、

そのセカンダリ キー サーバは、プライマリ キー サーバにアクセスして、直接情報のアップデートを要求します。延長期間にアップデートが受信されない場合、セカンダリ キー サーバによって、プライマリ サーバが到達不能（つまり「dead」）としてマーキングされます。

新しいポリシーがプライマリ キー サーバで作成されると、グループ メンバーが登録されるキー サーバがどのサーバかにかかわらず、プライマリ キー サーバの役割は、GDOI グループ メンバーに対するキー再生成メッセージの配信となります。

連携キー サーバ設定では、キー再生成のシーケンス番号がプライマリおよびセカンダリ キー サーバ間で同期されます。

ネットワーク マージでは、キー サーバは両者の大きい方のキー再生成シーケンス番号が選択されます。

連携キーサーバーの設定で 300 を超えるグループメンバーをサポートしている場合、**buffers huge size** コマンドを使用してバッファサイズを増やす必要があります。

キーサーバーの GETVPN グループ設定で使用される登録インターフェイスがシャットダウンされると、ネットワークスピットが発生します。推奨設定であるループバック インターフェイスの場合のように、インターフェイスが転送インターフェイスでない場合、キー再生成はグループ内のすべての KS から GM に送信されます。インターフェイスをシャットダウンすることによってキーサーバーをオフにすることはできません。キーサーバーを安全にオフにするには、**no crypto gdoi group** *group name* コマンドを使用します。

次の例は、キーサーバーの GETVPN グループ設定で参照される登録インターフェイスを示しています。

```
crypto gdoi group groupA
identity number 111
server local
  sa ipsec 10
   profile groupA
   match address ipv4 groupA-crypto-policy
   no replay
  no tag
  address ipv4 a.b.c.d
  redundancy
   local priority 250
   peer address ipv4 a.b.c.d
   peer address ipv4 a.b.c.d
```

通知メッセージ

通知メッセージは IKE フェーズ 1 によってセキュリティ保護され、IKE 通知メッセージとして送信されます。IKE によって提供される認証および機密保持は、キー サーバ間のメッセージをセキュリティ保護するために使用されます。通知メッセージ内のシーケンス番号によって、アンチ リプレイ保護が提供されます。通知メッセージは定期的にプライマリ キー サーバからセカンダリ キー サーバに送信されます。

通知メッセージには、現在の状態を維持するための次のコンポーネントが含まれます。

キー サーバの送信元プライオリティ

この値は送信元のプライオリティを示します。CLIによって設定可能です。最も高いプライオリティを持つキー サーバがプライマリ キー サーバとなります。プライオリティの値が同じ場合、最も高いIPアドレスを持つキー サーバがプライマリ キー サーバになります。

送信元のロールの維持

同期期間中、各キー サーバが地理的に分散した場所にある場合、それらのキー サーバにネットワーク分割イベントが発生する可能性があります。ネットワーク分割イベントが発生した場合、一定の期間中、複数のキーサーバがプライマリ キーサーバになる可能性があります。ネットワークが再び正常に動作し、すべてのキー サーバが互いに検知したら、各キー サーバがそれぞれの正しいロールを維持できるように、それらのサーバに対して、送信元の現在のロールを通知する必要があります。

リターン パケット フラグの要求

すべてのメッセージは一方向のメッセージとして定義されています。必要に応じて、キーサーバによってピアから現在の状態を要求し、そのロールを検出するか、グループの現在の状態を要求するかを行うことができます。

グループ ポリシー

グループ ポリシーは、任意のグループのために維持されるポリシーです。グループ メンバーの情報、IPsec SA、およびキーなどがあります。

アンチリプレイ機能および組み込まれた連携通知メッセージがサポートされています。プライマリ キー サーバによって疑似時間値が更新され、その値がグループ内のすべてのセカンダリ キーサーバに送信されます。セカンダリ キーサーバによって、それらのサーバのSARクロックとこの更新された値とが同期されます。

連携キー サーバ間の ANN メッセージ シーケンス番号のチェック

次に、連携キー サーバ間のシーケンス番号のチェックについて説明します。

- 連携キーサーバは、最後に受信したANNメッセージのシーケンス番号以下の番号のANNメッセージをすべてドロップします。
- ANNメッセージは、その差が大きくても、最後に受信したキー再生成メッセージよりシーケンス番号が大きい場合に承認されます。
- キー サーバがリロードされると、新しいIKEセッションがピア間に作成され、リロードされたキー サーバのANNシーケンス番号はゼロから開始します。この場合、もう一方ではどのシーケンス番号のANNメッセージも受け入れます。

キー サーバのロールの変更

連携キー サーバのネットワークでは、プライマリ サーバが、選択時における最も高いプライオリティに基づいて選択されます。他のキーサーバのステータスはセカンダリになります。プ

ライマリキーサーバーが停止状態として検知されたり、そのロールが変更されたりした場合、**clear crypto gdoi ks coop role** コマンドを使用すれば、プライマリキーサーバーの連携ロールをリセットできます。

clear crypto gdoi ks coop role コマンドがセカンダリキーサーバー上で実行されると、選択がそのセカンダリキーサーバー上でトリガーされますが、すでに選択されているプライマリキーサーバーが存在しているため、たいていの場合そのサーバーはセカンダリキーサーバーのままとなります。しかし、**clear crypto gdoi ks coop role** コマンドがプライマリキーサーバー上で実行された場合、そのプライマリキーサーバーはセカンダリロールに再割り当てされ、その結果、すべてのキーサーバーが関わる新しい選択がトリガーされます。前のプライマリ サーバのプライオリティが（すべてのキーサーバの中で）最も高い場合、そのサーバが再びプライマリサーバになります。前のプライマリ サーバがプライオリティの最も高いサーバではない場合、プライオリティが最も高いサーバが新しいプライマリ サーバとして選択されます。

受信専用 SA

マルチキャスト トラフィックで GDOI プロトコルが使用されている場合、双方向 SA がインストールされます。受信専用機能を利用すれば、段階的な導入が可能となり、ネットワーク全体を稼働させる前にごく少数のサイトを確認できます。サイトをテストするには、グループ メンバーの 1 つが他のすべてのグループ メンバーに暗号化されたトラフィックを送信し、トラフィックを復号化してトラフィックを「暗号化せずに」転送させる必要があります。受信専用 SA モードでは、期間の受信方向のみで暗号化できます。（受信専用 SA プロセスの手順を参照してください）。キーサーバーで **sa receive-only** コマンドを設定する場合、ステップ 2 および 3 は自動的に発生します。

1. GDOI キー サーバ上で IPsec SA を「受信専用」としてマーキングします。

これにより、グループ メンバーによる着信方向だけの SA のインストールが可能となります。受信専用 SA は、暗号グループの下で設定できます（「グループ ID、サーバ タイプ、および SA タイプの設定」セクションを参照してください）。

1. GDOI TEK ペイロードを「受信専用」としてマーキングします。

sa receive-only コマンドが設定されている場合、このグループ下のすべての TEK は、グループ メンバーへの送信時に、キーサーバーによって「受信専用」としてマーキングされます。

1. 一方向の IPsec フローのインストール

GDOI グループ メンバーによって、「受信専用」としてマーキングされているキー サーバからの IPsec SA が受信される度に、グループ メンバーによって、着信方向と発信方向の両方ではなく、着信方向だけでこの IPsec SA がインストールされます。

1. 次のローカル変換コマンドを使用して個々のグループ メンバーをテストします。
2. **crypto gdoi gm ipsec direction inbound optional**
3. **crypto gdoi gm ipsec direction both**

最初に、個々のグループ メンバーを個別に passive モード（この変換により、発信チェックに対して有効な SA が存在することが通知されます）に変換してから、次に、双方向モードに変換します。

1. 「受信専用」から「受信および送信」にグローバルに変換します。

テスト フェーズが終了し「受信専用」SA を双方向 SA に変換しなければならない時には、次の方式を使用できます。

グローバル変換

グループ下の **sa receive-only** コマンドを削除します。**sa receive-only** コマンドを削除すると、このグループの新しい IPsec SA が作成され、キー再生成が開始されます。受信と同時に、グループ メンバーによって、双方向で SA が再インストールされ、その SA の passive モードでの使用が開始されます。SA が永続的に passive モードでいることはできないので、5 分間キー再生成がなかった場合、グループ メンバーによって、これらの SA が受信モードまたは送信モードに変更されます。passive モードから双方向暗号化モードへの変換は自動で行われるので、管理者は何もする必要はありません。

パッシブ SA

パッシブ SA 機能によって、グループ メンバーを、永続的に passive モードにするように設定できます。パッシブ SA 機能を使用すれば、**crypto gdoi gm ipsec direction inbound optional** 特権 EXEC コマンドを使用する必要はなくなります。ただし、ルータのリロード後にこれが永続するわけではなく、キー再生成からのキーサーバー設定によって無効にできます。passive モードのグループ メンバーがあると、GET VPN への移行中におけるネットワーク テストやデバッグに利点があります。移行中に完全な暗号化保護を利用できるからです。グループ メンバーの passive モード設定は、キー サーバ設定よりも高いプライオリティを持ちます。**crypto gdoi gm ipsec direction inbound optional** 特権 EXEC コマンドは、グループメンバーとキーサーバーの設定を元に戻す次のキー再生成まで設定を無効にすることができます。

パッシブ SA 機能を設定するには、「パッシブ SA の設定」セクションを参照してください。

拡張ソリューションの管理性

機能の確認を支援するために、複数の **show** コマンドおよび **debug** コマンドがサポートされています。詳細については、「Fail-Close モードのアクティブ化」セクションを参照してください。

VRF-Lite インターフェイスによるサポート

VRF-Lite アプリケーションでは、ルーティング テーブルをユーザ グループ（または VPN）ごとに分離することによって、コントロール プレーンおよびフォワーディング プレーンでのトラフィックのセグメンテーションがサポートされています。また、各ユーザ グループの関連インターフェイスまたは専用インターフェイス上のトラフィックが転送されます。

MPLS VPN ネットワークに接続されているリモート サイトによって、セグメンテーションをキャンパスから WAN へ拡張する導入シナリオがあります。このような拡張されたセグメンテーションの場合、CE（グループ メンバーまたはキー サーバ）デバイス上の CE-PE インター

フェイスが、関連する Virtual Routing and Forwarding（VRF）に「バインド」されます。この VRF インターフェイスは、MPLS PE デバイスに接続されます。MPLS PE デバイスでは、VRF インターフェイスが関連するボーダー ゲートウェイ プロトコル（BGP）VRF プロセスにマッピングされています。このような場合、クリプト マップが VRF インターフェイスに適用されます。他の設定変更は必要ありません。

GM 登録の認証ポリシー

GM は、事前共有キーまたは公開キー インフラストラクチャ（PKI）を使用して登録時にキー サーバに認証できます。事前共有キーは、展開が容易ですが、プロアクティブに管理する必要があります。シスコはネットワーク内のすべてのデバイスに対してデフォルト キー（0.0.0.0 のアドレスで定義されるキー）を定義するのではなく、ピアベースの事前共有キーを展開することをお勧めします。事前共有キーは定期的に更新する必要があります（数ヵ月ごと）。

（注） キー再生成は KEK を使用してセキュリティが確保されるため、事前共有キーは暗号化データ プレーンまたはコントロール プレーンに影響を与えずにキー サーバ グループ メンバー（KS-GM）ピアごとに更新できます。新しく割り当てられた事前共有キーを使用して、発注済みの一連のキー サーバごとに GM を再登録できるようにすることが重要です。

PKI では、事前共有キーを使用するときに直面するキー管理の困難を克服するためにインフラストラクチャを使用します。PKI インフラストラクチャは認証局（CA）として機能し、ここでルータ証明書が発行され、維持されます。ただし、IKE 認証中に PKI を使用することは計算負荷が集中します。PKI の展開では、キー サーバのキャパシティ、設計、および配置が重要になります。

セキュリティを強化するため、GET VPN では事前共有キーまたは PKI を使用する GM 認証もサポートします。詳細については、「GET VPN 認証」セクションを参照してください。

GET VPN GM 認証

GET VPN GM 認証は、事前共有キーまたは PKI を使用して実行できます。GET VPN 認証をオンにすることはベスト プラクティスです。キー サーバが複数の GDOI グループに使用される際、あるグループの GM が別のグループからキーとポリシーを要求するのを防ぐには、キー サーバ認証が必要です。ISAKMP 認証では GM がキー サーバから GDOI 属性を要求できることが確認され、GDOI 認証では GM がキー サーバに設定された特定のグループから GDOI 属性を要求できることが確認されます。

GDOI 認証は、GM から送信された ISAKMP ID に基づきます。GM が ID として IP アドレスを送信すると、認証アドレスのみが認証に使用されます。GM が識別名（DN）またはホスト名を送信すると、認証 ID が使用されます。ID として IP アドレスを使用すると、DN またはホスト名と照合する認証がバイパスされます。逆も同様です。特定の DN の GM だけが接続できる（別の ID を使用する GM が接続できない）ようにするには、認証アドレスで **deny any** を指定する必要があります。

事前共有キーを使用する GM 認証

事前共有キーを使用するとき、GET VPN では IP アドレスを使用する GM 認証がサポートされます。GM の WAN アドレス（またはサブネット）を照合する ACL は、GET VPN グループ設定に定義し、適用することができます。ACL と一致する IP アドレスを持つ GM は認証が成功し、キー サーバに登録できます。GM IP アドレスが ACL と一致しない場合、キー サーバは GM の登録要求を拒否します。

認証失敗の場合、次の syslog メッセージが生成されます。

```
%GDOI-1-UNAUTHORIZED_IPADDR: Group getvpn received registration from
unauthorized ip address: 10.1.1.9
```

PKI を使用する GM 認証

PKI を使用する場合、GET VPN では一般的に使用される DN または完全修飾ドメイン名（FQDN）を使用する GM 認証がサポートされます。GM 認証をアクティブにするには、**authorization identity** コマンドを使用します。GM 証明書の特定のフィールド（通常、組織ユニット（OU））と一致する暗号 ID は、GET VPN グループ設定に定義し、適用することができます。暗号 ID を定義するには、**crypto identity** コマンドを使用します。

証明書クレデンシャルが ISAKMP ID と一致する GM は認証され、キー サーバに登録できます。たとえば、すべての GM 証明書に OU=GETVPN が発行される場合、すべての GM が OU=GETVPN を持つ証明書を提示することをチェック（認証）するようにキー サーバを設定できます。GM が提示する証明書の OU がそれ以外に設定されている場合、GM のキー サーバへの登録は認証されません。

認証が失敗した場合、次の syslog メッセージが生成されます。

```
%GDOI-1-UNAUTHORIZED_IDENTITY: Group getvpn received registration from
unauthorized identity: Dist.name: hostname=GroupMember-1, ou=TEST
```

Protocol Independent Multicast-Sparse Mode でのキー再生成機能

マルチキャスト キー再生成は、マルチキャストのすべてのモードで使用できます。継続するトラフィックが受信されないと PIM-SM Shortest Path Tree（SPT）が廃棄される可能性があるため、Protocol Independent Multicast-Sparse Mode（PIM-SM）を設定するときは必ず、**rekey retransmit** コマンドを使用する必要があります。トラフィックが再開すると、PIM-SM によって SPT が必ず確立されます。キー再生成パケットを再送信すると、PIM-SM による SPT の設定時にグループ メンバーによってキー再生成が受信される可能性が高くなります。

Fail-Close モード

グループ メンバーがキー サーバに登録されないと、そのグループ メンバーを通過するトラフィックが暗号化されません。この状態は「フェール オープン」と呼ばれます。グループ メンバーが登録される前に暗号化されていないトラフィックがそのグループ メンバーを通過することを防ぐには、Fail-Close 機能を設定します。この機能を設定すると、暗黙的な「permit ip any any」ポリシーがインストールされ、そのグループ メンバーを通過する暗号化されていないトラフィックはすべて廃棄されます（この状態を Fail-Close モードと呼びます）。

Fail-Close 機能は、インターフェイス ACL を設定することによっても実現可能です。ただし、Fail-Close 機能は、ACL リストよりも管理しやすく、実装も簡単です。

Fail-Close 機能を設定している場合でも、 **match address** コマンド（**match address** {*access-list-number* | *access-list-name*}）を設定することによって、特定の暗号化されていないトラフィックがグループメンバーを通過することを許可することが可能です。この明示的な「deny」ACL は、暗黙的な「permit ip any any」によって、拒否された（暗号化されていない）トラフィックがグループ メンバーの通過を許可される前に追加されます。

グループ メンバーの登録が正常終了したら、Fail-Close ポリシーが明示的であるか暗黙的であるかを問わず削除され、グループ メンバーの動作が、Fail-Close 機能が設定される以前のものと同じになります。

Fail-Close 機能の使用上の注意事項

Fail-Close モードで作業するためにクリプト マップを設定する場合、注意しなければならないことがあります。Fail-Close ACL を正しく定義しないと、自分自身をロックアウトしてしまう可能性があります。たとえば、セキュアシェル（SSH）を使用して暗号マップが適用されたインターフェイス経由でルータにログインする場合、**deny tcp any eq** *port* **host** *address* コマンドラインを Fail-Close ACL 下に含める必要があります。キーサーバーへのパスを検索する場合は、ルータが使用しているルーティングプロトコル（**deny ospf any any** など）も含める必要がある場合もあります。最初に Fail-Close とその ACL を設定し、次に **show crypto map gdoi fail-close** *map-name* コマンドを使用して Fail-Close ACL を確認します。Fail-Close ACL を確認し、それが正しいと確信したら、**activate** コマンドを設定して、Fail-Close モードで暗号マップを動作させることができます。**activate** コマンドを設定しない限り、Fail-Close はアクティブになりません。

Fail-Close ACL はグループ メンバーの視点で設定します。Fail-Close ACL は、グループ メンバー上で次のように設定されます。

access-list 125 deny ip host *host1-ip-addr host2-ip-addr*

Fail-Close モードでは、host1 から host2 へのすべての IP トラフィックが、Group Member 1 によって、暗号化されていないテキストで送信されます。さらに、着信ミラートラフィック（つまり、host2 から host1 への IP トラフィック）も、GM1 によって暗号化されていないテキストで受信されます。

（注） deny エントリに一致するすべての IP トラフィックは、グループ メンバーによって、暗号化されていないテキストで送信されます。

着信トラフィックは、ミラー アクセス リストに対応付けられます。

Fail-Close アクセス リストは、グループ メンバー アクセス リストと同じルールに従います。詳細は、「グループ メンバー アクセス コントロール リスト」のセクションを参照してください。

GDOI 登録を行うために **deny udp any eq 848 any eq 848** コマンドを設定する必要はありません。コード自体によって、そのコードの設定対象となっているキー サーバからの、特定のグ

ループ メンバーの GDOI パケットであるかどうかが判断されます。そのグループ メンバーの GDOI パケットだった場合、そのパケットは処理されます。ただし、キーサーバーがグループ メンバー 1 の後になるシナリオでは、グループメンバー 1 がキーサーバーに正常に登録できない場合、グループメンバー 1 に対して明示的に **deny udp any eq 848 any eq 848** コマンドラインが設定されていない限り、他のグループメンバーも登録できなくなります。しかし、Fail-Close 機能が正しく設定されている場合は、グループ メンバーがキーサーバへの登録に失敗しても、望まないトラフィックが「暗号化されずに」出ていくことがないようにすることができます。ただし、他のグループ メンバーからの登録パケットが、登録に失敗した場合でもグループ メンバー 1 経由でキー サーバに到達できる場合、指定されたトラフィックが暗号化されずに出ていくことを許可することができます。

Fail-Close モードの設定の詳細については、「Fail-Close モードのアクティブ化」セクションを参照してください。

Fail-Close モードがアクティブになっているか確認するには、**show crypto map gdoi fail-close** コマンドを使用します。

フェールクローズ復帰

フェールクローズモードでは、フェールクローズモードで登録する前は、グループメンバーはそのローカル フェールクローズポリシーを適用し、それに応じてトラフィックを管理します。登録後は、グループメンバーはキーサーバーからダウンロードされたポリシーを適用し、それに応じてトラフィックを処理します。

キー再生成がない場合またはグループメンバーがキーサーバーに再登録できない場合、グループメンバーは、キーサーバーからダウンロードされた同じポリシーを使用します。暗号化または復号のためのキーがないため、パケットのドロップが発生します。フェールクローズ復帰により、グループメンバーは、フェールクローズモードに戻り、ダウンロードしたキーサーバーポリシーを削除することができます。これは、グループメンバーでフェールクローズ復帰が有効になっている場合にのみ発生します。

このフェールクローズ復帰は、すべてのアクティブな SA が期限切れになり、再登録のために到達できるキーサーバーがない場合にトリガーされます。clear crypto sa コマンドを使用して IPsec SA を手動でクリアすると、機能の意図した動作が得られません。ただし、キーサーバーに到達できない場合、clear crypto gdoi コマンドを使用するとフェールクローズモードに戻ります。

この機能の設定手順については、「フェールクローズ復帰の設定」のセクションを参照してください。

GDOI 登録成功を追跡する MIB オブジェクトの作成

Null ルートを回避するため、GET VPN のルーティングプレーンと暗号プレーンは同期される必要があります。GET VPN Null ルートは、次の状況で発生します。

- アクティブな TEK がない KS に GM が登録できず、トラフィックを暗号化または復号化できない。
- GM TEK SA の期限が切れたがキー再生成または再登録によって KS から新しいキーを受け取っていない。

- GM は KS からキー再生成を受け取ったが、SA を暗号エンジンにインストールするときにエラーが発生する。

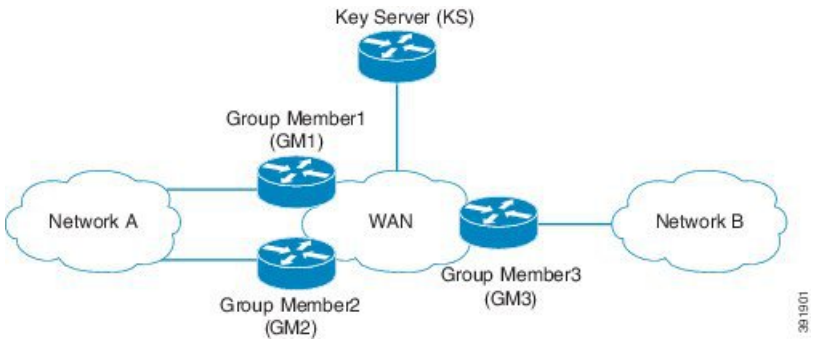
GDOI 登録成功を追跡する MIB オブジェクトの作成機能では、グループ内のアクティブな TEK 数を示すため、GDOI MIB に新しい MIB オブジェクトが導入されています。

BGP の GET VPN ルーティング認識

Null ルートを回避するため、GET VPN のルーティングプレーンと暗号プレーンは同期する必要があります。グループ メンバー（GM）がキー サーバ（KS）に正常に登録される場合、セキュリティ ポリシーまたはキーは GM にインストールされません。ただし、GM は他の GM に対して保護されたネットワークのルートをアドバタイズできます。

次の図は、Null ルートの生成について説明しています。

図 *12 : Null* ルートの生成



1. グループ メンバー 1、グループ メンバー 2、グループ メンバー 3 が起動し、WAN とルーティング アジャセンシー関係を確立します。
2. グループ メンバー 1 およびグループ メンバー 2 は、ネットワーク A のプレフィックスを WAN にアドバタイズします。ネットワーク B からネットワーク A へのトラフィックの優先パスは、グループ メンバー 1 経由です。
3. グループ メンバー 3 はネットワーク B を WAN にアドバタイズします。トラフィック ネットワーク A からネットワーク B への優先パスは、グループ メンバー 1 経由です。
4. KS は、ネットワーク A とネットワーク B の間のすべてのトラフィックを保護するためのセキュリティを定義します。
5. グループ メンバー 1 とグループ メンバー 3（およびグループ メンバー 2）は正常に KS からセキュリティ キーを取得し、ネットワーク A とネットワーク B 間のすべてのトラフィックを保護します。
6. グループ メンバー 2 およびグループ メンバー 3 が正常にキーを取得する一方、グループ メンバー 1 は更新されたキーまたはポリシーの受信に失敗し、KS への再登録に失敗します。
7. ルーティング プロトコルは、ネットワーク A とネットワーク B 間のすべてのトラフィックに対してグループ メンバー 1 経由のパスを優先し続けます。

8. グループ メンバー 1 は、ポリシーまたはキーが無効なため、ネットワーク A とネットワーク B の間に流れるトラフィックすべてをドロップします。

ネットワーク B のホストがネットワーク A のホストにトラフィックを送信する際、トラフィックはグループ メンバー 3 によって暗号化され、グループ メンバー 1 経由（優先パス）でネットワーク A に送信されます。ただし、グループ メンバー 1 はトラフィックを復号するためのポリシーまたは現在のキーを持たないため、パケットをドロップします。その結果、トラフィックはドロップされ、Null ルートが生成されます。同様に、ネットワーク A のホストがネットワーク B のホストにトラフィックを送信する際、トラフィックはグループ メンバー 1（優先パス）に転送され、グループ メンバー 1 にポリシーまたは現在のキーがないためにドロップされます。グループ メンバー 1 にポリシーまたはキーがない場合、適切な動作としてトラフィックはグループ メンバー 2 経由で転送および再ルーティングされます。

BGP の GET VPN ルーティング認識機能では、GETVPN GM の暗号化状態を追跡し、追跡情報を適用して GM で双方向条件付きルートフィルタリングを実行することにより、ルーティングが存在しない状態を回避します。

双方向条件付きルート フィルタリング

双方向条件付きルート フィルタリングでは、BGP、OSPF、EIGRP、RIPv2 などのさまざまなルーティング プロトコルをサポートしています。EOT は GET VPN GM 暗号化状態を追跡し、EOT 値に基づいて条件により特定のルートマップ エントリを有効または無効にします。次に、GET VPN GM 暗号化状態をモニタする設定例を示します。

```
route-map bgp-policy-out permit 10
 match ip address register-int-Only
route-map bgp-policy-out permit 20
 match track 99
 match ip address orig_route_map_acl_out
route-map bgp-policy-out deny 30

route-map bgp-policy-in permit 10
 match ip address noc
route-map bgp-policy-in permit 20
 match track 99
 match ip address orig_route_map_acl_in
route-map bgp-policy-in deny 30

ip access-list standard noc
 permit 1.1.1.0                                  <---- NOC subnet with Keyserver (KS)
ip access-list standard register-int-Only
 permit 2.2.2.2                                 <---- registration interface ip of the
 GM itself
ip access-list standard orig_route_map_acl_in      <---- original inbound route-map ACL

 permit a.b.c.d
 permit .......
ip access-list standard orig_route_map_acl_out     <---- original outbound route-map
ACL
 permit e.f.g.h
 permit .......

router bgp 64600
 no synchronization
 bgp router-id xxxxxxxx
 bgp log-neighbor-changes
 network xxxxxxxxxx mask 255.255.255.255
```

```
network xxxxxxxxxx mask 255.255.255.252
neighbor xxxxxxxxxx remote-as 65000
neighbor xxxxxxxxxx description PE
neighbor xxxxxxxxxx route-map bgp-policy-in in
neighbor xxxxxxxxxx route-map bgp-policy-out out
```

上記の例では、GET VPN GM 暗号化状態をモニタするために **match track 99** コマンドが指定されています。GM が適切に機能する場合、**match track 99** コマンドは値 *true* を返し、GM は次のルートをアドバタイズまたは受信します。

- 発信：GM 登録インターフェイスに到達するルート、および着信ルートマップのアクセスコントロール リスト（ACL）「orig_route_map_acl_out」によって許可されたルート。
- 着信：NOC に到達するルート、およびルーティングは、ピアから受信した発信ルートマップ ACL「orig_route_map_acl_in」によって許可されたルート。

一方、GM が正しく機能しない場合、**match track 99** コマンドは値 *false* を返し、GM は次のルートのみをアドバタイズまたは受信します。

- 発信：GM 登録インターフェイスに到達するルート。
- 着信：NOC サブネットに到達するルート。

Cisco Group Encrypted Transport VPN システム ロギング メッセージ

次の表に、GET VPN システム ロギング（syslog とも呼ばれます）メッセージと説明を示します。

表 *3 : GET VPN* システム ロギング メッセージ

メッセージ	説明
COOP_CONFIG_MISMATCH	プライマリ KS とセカンダリ KS 間の設定が一致しません。
COOP_KS_ADD	グループ内の連携 KS のリストに KS が追加されました。
COOP_KS_ELECTION	ローカル KS によってグループ内の選択プロセスが開始されました。
COOP_KS_REACH	設定済み連携 KS 間の到達可能性は回復しています。
COOP_KS_REMOVE	グループ内の連携 KS のリストから KS が削除されました。
COOP_KS_TRANS_TO_PRI	ローカル KS が、グループ内のセカンダリ サーバからプライマリ ロールに移行しました。

メッセージ	説明
COOP_KS_UNAUTH	認証されていないリモートサーバーによって、グループ内のローカル KS へのアクセスが試行されました。敵対的なイベントの可能性があります。
COOP_KS_UNREACH	設定済み連携 KS 間の到達可能性が失われています。敵対的なイベントの可能性があります。
COOP_KS_VER_MISMATCH	各 KS が、異なるバージョンの Cisco IOS コードを実行しています。
COOP_PACKET_DROPPED	ドライババッファ サイズに設定されたハード制限によって、このサイズ以上のパケットの送信はできません。
GDOI-3-GDOI_REKEY_SEQ_FAILURE	シーケンス番号のアンチ リプレイ チェックが失敗したため、キー再生成メッセージが拒否されています。
GDOI-3-GM_NO_CRYPTO_ENGINE	リソースが不足しているかサポートされていない機能が要求されたために暗号化エンジンが検出できません。
GDOI-3-PSEUDO_TIME_LARGE	キー再生成に、計算された許容される疑似時間の差を超える大きな疑似時間があります。
GDOI-3-PSEUDO_TIME_TOO_OLD	キー再生成に、計算された許容される疑似時間の差を超える小さな疑似時間があります。
GDOI-4-GDOI_ANN_TIMESTAMP_ LARGE	セカンダリ KS が、プライマリ KS から計算された許容される疑似時間の差を超える大きな疑似時間がある ANN を受信しています。
GDOI-4-GDOI_ANN_TIMESTAMP_ TOO_OLD	セカンダリ KS が、プライマリ KS から計算された許容される疑似時間の差を超える小さな疑似時間がある ANN を受信しています。
GDOI-5-COOP_KS_BLOCK_NEW_GM_REGISTER	セカンダリ KS がプライマリ KS から有効な疑似時間を受信していないため、GM のグループへの登録を一時的にブロックしています。

メッセージ	説明
GDOI-5-COOP_KS_VALID_ANN_ TIMER_EXPIRED	セカンダリ KS が 3 つの再送信後に無効な疑似時間のある ANN を受信し続けています。セカンダリ KS は有効な ANN が受信されるまで一時的に新しいグループ メンバー登録をブロックします。
GDOI_ACL_NUM	ACL のエントリが多すぎます。GDOI は、指定された最初の 100 個の ACL エントリだけを受け入れます。
GDOI_REKEY_FAILURE	GDOI キー再生成中に、KS からのペイロード構文解析が、この GM 上で失敗しました。
GM_ACL_MERGE	GM と KS 間における ACL の違いは解決され、結合が実行されました。
GM_ACL_PERMIT	GM は「拒否」の ACL のみをサポートできます。「許可」エントリと一致するすべてのトラフィックがドロップされます。
GM_CLEAR_REGISTER	ローカル GM によって、**clear crypto gdoi** コマンドが実行されました。
GM_CM_ATTACH	このローカル GM 用の暗号マップが追加されました。
GM_CM_DETACH	このローカル GM 用の暗号マップが削除されました。
GM_CONV_SA_DUPLEX	IPsec SA が、GM 上のグループ内で双方向モードに変換されました。
GM_CONV_SA_DUPLEX_LOCAL	CLI コマンドによって、GM 上のグループ内で、IPsec SA が双方向モードに変換されました。
GM_DELETE	グループ内の GM が KS から削除されました。
GM_ENABLE_GDOI_CM	GM に、KS を持つグループ内の GDOI 暗号マップ上のイネーブルにされた ACL があります。
GM_HASH_FAIL	GDOI 登録プロトコル中に KS によって送信されたメッセージに不具合があるか、ハッシュがありません。

メッセージ	説明
GM_INCOMPLETE_CFG	GDOI グループ設定で、グループ ID、サーバID、またはその両方が見つからないために、登録が完了できません。
GM_NO_IPSEC_FLOWS	IPsec フロー 制限に関するハードウェアの制限に達しました。IPsec SA をこれ以上作成できません。
GM_RE_REGISTER	あるグループのために作成された IPsec SA が期限切れか、消去された可能性があります。KS に再登録する必要があります。
GM_RECV_DELETE	GM を削除するために KS によって送信されたメッセージを受信しました。
GM_RECV_REKEY	キー再生成を受信しました。
GM_REGS_COMPL	Registration complete.
GM_REJECTING_SA_PAYLOAD	GDOI 登録プロトコル中に、KS によって送信された提案が、ローカル GM によって拒否されました。
GM_REKEY_NOT_RECD	GMによって、グループ内のKSからのキー再生成メッセージが受信されませんでした。現在実装されていません。
GM_REKEY_TRANS_2_MULTI	GM が、ユニキャスト キー再生成メカニズムの使用から、マルチキャストメカニズムの使用へと移行しました。
GM_REKEY_TRANS_2_UNI	GM が、マルチキャスト キー再生成メカニズムの使用から、ユニキャストメカニズムの使用へと移行しました。
GM_SA_INGRESS	グループ内の KS からの受信専用 ACL が、GM によって受信されました。
GM_UNREGISTER	GM がグループから去りました。
KS_BAD_ID	GDOI 登録プロトコル中に、ローカル KS と GM との間で設定の不一致が発生しました。
KS_BLACKHOLE_ACK	KS が、GM からの Null ルートメッセージの状態になりました。敵対的なイベントの可能性があります。

メッセージ	説明
KS_CLEAR_REGISTER	ローカル KS によって、**clear crypto gdoi** コマンドが実行されました。
KS_CONV_SAS_DUPLEX	IPsec SA が、グループ内で双方向モードに変換されました。
KS_CONV_SAS_INGRESS	IPsec SA が、グループ内で受信専用モードに変換されました。
KS_FIRST_GM, GDOI, LOG_INFO	ローカル KS がグループに参加している最初の GM を受信しました。
KS_GM_REJECTS_SA_PAYLOAD	GDOI 登録プロトコル中に、KS によって送信された提案が、GM によって拒否されました。
KS_GM_REVOKED	キー再生成プロトコル中に、認証されていないメンバーによるグループへの加入が試行されました。敵対的なイベントの可能性があります。
KS_GROUP_ADD	コンフィギュレーション コマンドが実行され、グループ内に KS が追加されました。
KS_GROUP_DELETE	コンフィギュレーション コマンドが実行され、グループから KS が削除されました。
KS_HASH_FAIL	GDOI 登録プロトコル中に GM によって送信されたメッセージに不具合があるか、ハッシュがありません。
KS_LAST_GM	最後の GM がローカル KS でグループを去りました。
KS_NACK_GM_EJECT	KS が、GM からの ACK メッセージを受信しない状態になり、イジェクトされました。
KS_NO_RSA_KEYS	RSA キーが作成されなかったか、失われています。
KS_REGS_COMPL	KS による、グループ内における登録が正常終了しました。
KS_REKEY_TRANS_2_MULTI	グループが、ユニキャスト キー再生成メカニズムの使用から、マルチキャスト メカニズムへと移行しました。

メッセージ	説明
KS_REKEY_TRANS_2_UNI	グループが、マルチキャスト キー再生成メカニズムの使用から、ユニキャスト メカニズムの使用へと移行しました。
KS_SEND_MCAST_REKEY	マルチキャスト キー再生成を送信中です。
KS_SEND_UNICAST_REKEY	ユニキャスト キー再生成を送信中です。
KS_UNAUTHORIZED	GDOI 登録プロトコル中に、認証されていないメンバーによるグループへの加入が試行されました。敵対的なイベントの可能性があります。
KS_UNSOL_ACK	KS によって、過去の GM からの非送信請求 ACK メッセージが受信されたか、DoS 攻撃を受けています。敵対的なイベントの可能性があります。
PSEUDO_TIME_LARGE	GM によって、その GM の疑似時間とは大きく異なる値を持つ疑似時間が受信されました。
REPLAY_FAILED	GM または KS のアンチ リプレイ チェックが失敗しました。
UNAUTHORIZED_IDENTITY	登録要求が、要求を行っているデバイスがグループの参加を許可されなかったために廃棄されました。
UNAUTHORIZED_IPADDR	登録要求が、要求を行っているデバイスがグループの参加を許可されなかったために廃棄されました。
UNEXPECTED_SIGKEY	予期しないシグニチャ キーが検出されました。このシグニチャ キーを解除します。
UNREGISTERED_INTERFACE	未登録のインターフェイスからの登録を受信中です。処理を停止してください。
UNSUPPORTED_TEK_PROTO	予期しない TEK プロトコルです。

Cisco Group Encrypted Transport VPN の設定方法

キー サーバの設定

前提条件

GDOI グループを作成する前に、最初に IKE および IPsec トランスフォーム セットを設定してから、IPsec プロファイルを作成する必要があります。IKE と IPsec トランスフォーム セットの設定方法、および IPsec プロファイルの作成方法については、「その他の関連資料」セクションの「関連資料」の項を参照してください。

キー再生成メッセージに署名するための RSA キーの設定

（注） セキュリティに対する脅威は、脅威からの保護に役立つ暗号化技術と同様に絶え間なく変化しています。最新のシスコの暗号化に関する推奨事項については、『Next Generation Encryption（NGE）ホワイト ペーパー』を参照してください。

キー再生成メッセージに署名するために使用される RSA キーを設定するには、次の手順を実行します。キー再生成が使用中でない場合、このサブ作業はスキップしてください。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto key generate rsa general-keys label** *name-of-key*

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： `Router> 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： `Router# 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 key generate rsa general-keys label** *name-of-key* 例：	キー再生成メッセージに署名するために使用される RSA キーを生成します。生成されるキーの長さ（ビット単位）を確認するプロンプトが表示されま

	コマンドまたはアクション	目的
	`Router(config)# crypto key generate rsa general-keys label mykeys`	す。2048 未満の長さを指定することは推奨されません。

次の作業

グループ ID、サーバ タイプ、および SA タイプを設定します（「グループ ID、サーバ タイプ、および SA タイプの設定」セクションを参照してください）。

グループ ID、サーバ タイプ、および SA タイプの設定

サイトが大量にある場合、特にあるサイトが Dual Multipoint VPN（DMVPN）のような他の暗号化ソリューションから移行する場合は、予防措置を取り、段階的に機能を追加する必要があります。たとえば、すべての CPE デバイスを、トラフィックが双方向で暗号化されるように設定するのではなく、1 つまたは少数のグループだけが暗号化されたトラフィックの送信を許可されるように、一方向の暗号化を設定することが可能です。その他のデバイスは暗号化されたトラフィックだけを受信することが許可されます。1 つまたは少数のメンバーに関する一方向の暗号化の検証が終わったら、すべてのメンバーに対して双方向の暗号化をオンにできます。この「着信専用」トラフィックは、暗号グループ下で **sa receive only** コマンドを使用して制御可能です。

グループ ID、サーバ タイプ、および SA タイプを設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto gdoi group** *group-name*
4. 次のいずれかのコマンドを入力します。
   - **identity number** *number*
   - **identity address ipv4** *address*
5. **server local**
6. **sa receive-only**

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： `Router> 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：	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。

	コマンドまたはアクション	目的
	`Router# configure terminal`	
ステップ 3	**crypto gdoi group** *group-name* 例： `Router(config)# crypto gdoi group gdoigroupname`	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	次のいずれかのコマンドを入力します。
	• **identity number** *number*
	• **identity address ipv4** *address*
	例：
	`Router(config-gdoi-group)# identity number 3333`
	例：
	`Router(config-gdoi-group)# identity address ipv4 209.165.200.225`
		GDOI グループ番号またはアドレスを指定します。

ステップ 5	**server local** 例： `Router(config-gdoi-group)# server local`	デバイスを GDOI キー サーバとして指定し、GDOI ローカル サーバ コンフィギュレーション モードを開始します。
ステップ 6	**sa receive-only** 例： `Router(config-local-server)# sa receive-only`	IPsec SA がグループ メンバーによって「着信専用」としてインストールされるように指定します。

次の作業

グループ メンバーが双方向の受信および送信モードで動作するように、キー サーバ上の受信専用設定を削除します。

キー再生成の設定

ここでは、次のオプションの作業について説明します。

キー再生成は、グループのポリシーと IPsec SA を定期的に更新するために、キー サーバによってコントロール プレーンで使用されます。グループ メンバー側では、他の何らかの理由によりタイマーが満了するときに完全に登録するのではないので、キー再生成への登録の更新がより効率的になります。最初の登録は常にユニキャスト登録です。

キー サーバは、ユニキャストまたはマルチキャスト モードでキー再生成を送信するように設定できます。キー再生成の転送モードは、キー サーバによって IP マルチキャストが使用されてキー再生成が配信できるかどうかによって決まります。マルチキャスト機能がカスタマーの

ネットワーク内に存在しない場合、キー サーバを、ユニキャスト メッセージを使用してキー再生成を送信するように設定する必要があります。

キー再生成の追加オプションでは、**rekey authentication**、**rekey retransmit**、および **rekey address ipv4** コマンドを使用します。ユニキャスト転送モードが設定されている場合、このユニキャストキー再生成メッセージの送信元アドレスが指定されるように **source address** コマンドを指定する必要があります。

マルチキャストは、キー再生成メッセージのデフォルトの転送タイプです。次の箇条書きでは、キー再生成転送タイプにどのような場合にマルチキャストにするか、あるいはユニキャストにするかを説明します。

- グループ内のすべてのメンバーがマルチキャストに対応している場合は、**rekey transport unicast** コマンドを設定しません。マルチキャストキー再生成はデフォルトでオンになっているので、このグループ下でキー再生成転送タイプ「ユニキャスト」が過去に設定されていない場合、**no rekey transport unicast** コマンドは必要ありません。
- グループ内のすべてのメンバーがユニキャストである場合、**rekey transport unicast** コマンドを使用します。
- グループ内に混合されたメンバーがある場合（つまり、大多数がマルチキャストで、少数がユニキャスト）、**rekey transport unicast** コマンドは設定しません。キー再生成は、グループ メンバーの大多数に対して、マルチキャストで配信されます。マルチキャスト メッセージを受信しない残りのグループ メンバー（ユニキャスト グループ メンバー）は、そのポリシーが期限切れになった時にキー サーバに再登録する必要があります。混合モード（つまり、ユニキャストとマルチキャスト キー再生成モード）は現在サポートされていません。

no rekey transport unicast コマンドが使用されている場合、マルチキャストキー再生成メッセージを受信できないGDOIグループ内のメンバーを、最新のグループポリシーを取得するようにキーサーバーに再登録する必要があります。再登録すると、デフォルトの転送タイプが強制的にマルチキャストになります。過去に転送タイプが設定されていない場合、マルチキャスト転送タイプがデフォルトで適用されます。

前提条件

rekey authentication コマンドを設定する前に、**crypto key generate rsa** コマンドおよび **general-keys** キーワードと **label** キーワードを使用して RSA キーが生成されるようにルータを設定しておく必要があります（例：「crypto key generate rsa general-key label my keys」）。

ユニキャスト キー再生成の設定

次の設定作業表では、アドレス「ipv4 10.0.5.2」は、ユニキャストまたはマルチキャスト キー再生成メッセージを送信するキー サーバ上のインターフェイスを示しています。このアドレスは、ユニキャスト キー再生成では必須ですが、マルチキャスト キー再生成では任意です。マルチキャスト キー再生成の場合、キー サーバの送信元アドレスを、キー再生成 ACL から取得できます。

ユニキャスト キー再生成を設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto gdoi group** *group-name*
4. 次のいずれかのコマンドを入力します。
   - **identity number** *number*
   - **identity address ipv4** *address*
5. **server local**
6. **rekey transport unicast**
7. **rekey lifetime seconds** *number-of-seconds*
8. **rekey retransmit** *number-of-seconds* **number** *number-of-retransmissions*
9. **rekey authentication mypubkey rsa** *key-name*
10. **address ipv4** *ipv4-address*

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： `Router> 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： `Router# 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： `Router(config)# crypto gdoi group gdoigroupname`	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	次のいずれかのコマンドを入力します。
	• **identity number** *number*
	• **identity address ipv4** *address*
	例：
	`Router(config-gdoi-group)# identity number 3333`
	例：
	`Router(config-gdoi-group)# identity address ipv4 209.165.200.225`
		GDOI グループ番号またはアドレスを指定します。

	コマンドまたはアクション	目的
ステップ 5	**server local** 例： `Router(config-gdoi-group)# server local`	デバイスを GDOI キー サーバとして指定し、GDOI ローカル サーバ コンフィギュレーション モードを開始します。
ステップ 6	**rekey transport unicast** 例： `Router(config-local-server)# rekey transport unicast`	グループ メンバーに対するキー再生成メッセージのユニキャスト配信を設定します。
ステップ 7	**rekey lifetime seconds** *number-of-seconds* 例： `Router(gdoi-local-server)# rekey lifetime seconds 300`	（任意）任意の暗号キーが使用される秒数を制限します。 • このコマンドが設定されていない場合、デフォルト値の 86,400 秒が有効になります。
ステップ 8	**rekey retransmit** *number-of-seconds* **number** *number-of-retransmissions* 例： `Router(gdoi-local-server)# rekey retransmit 10 number 3`	（任意）キー再生成メッセージが再送信される回数を指定します。 • このコマンドが設定されていない場合、再送信は行われません。
ステップ 9	**rekey authentication mypubkey rsa** *key-name* 例： `Router(gdoi-local-server)# rekey authentication mypubkey rsa mykeys`	（任意）GDOI グループ メンバーに対するキー再生成に使用されるキーを指定します。 • キー再生成が不要な場合、このコマンドは任意です。キー再生成が必須の場合、このコマンドは必須です。
ステップ 10	**address ipv4** *ipv4-address* 例： `Router(gdoi-local-server)# address ipv4 209.165.200.225`	（任意）ユニキャスト キー再生成メッセージの送信元情報を指定します。 • キー再生成が不要な場合、このコマンドは任意です。キー再生成が必須の場合、このコマンドは必須です。

マルチキャスト キー再生成の設定

マルチキャスト キー再生成を設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto gdoi group** *group-name*

4. 次のいずれかのコマンドを入力します。
   - **identity number** *number*
   - **identity address ipv4** *address*
5. **server local**
6. **rekey address ipv4** {*access-list-name* | *access-list-number*}
7. **rekey lifetime seconds** *number-of-seconds*
8. **rekey retransmit** *number-of-seconds* **number** *number-of-retransmissions*
9. **rekey authentication** {**mypubkey** | **pubkey**} **rsa** *key-name*
10. **exit**
11. **exit**
12. **access-list** *access-list-number* {**deny** | **permit**} **udp host** *source* [*operator*[*port*]] **host** *source* [*operator*[*port*]]
13. **interface** *type slot/ port*
14. **ip igmp join-group** *group-address* [**source** *source-address*]

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： `Router> 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： `Router# 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： `Router(config)# crypto gdoi group gdoigroupname`	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	次のいずれかのコマンドを入力します。
	• **identity number** *number*
	• **identity address ipv4** *address*
	例：
	`Router(config-gdoi-group)# identity number 3333`
	例：
	`Router(config-gdoi-group)# identity address ipv4 209.165.200.225`
		GDOI グループ番号またはアドレスを指定します。

	コマンドまたはアクション	目的
ステップ 5	**server local** 例： `Router(config-gdoi-group)# server local`	デバイスを GDOI キー サーバとして指定し、GDOI ローカル サーバ コンフィギュレーション モードを開始します。
ステップ 6	**rekey address ipv4** {*access-list-name* | *access-list-number*} 例： `Router(gdoi-local-server)# rekey address ipv4 121`	登録するマルチキャスト サブアドレス範囲グループ メンバーを定義します。
ステップ 7	**rekey lifetime seconds** *number-of-seconds* 例： `Router(gdoi-local-server)# rekey lifetime seconds 300`	（任意）任意の暗号キーが使用される秒数を制限します。 • このコマンドが設定されていない場合、デフォルト値の 86,400 秒が有効になります。
ステップ 8	**rekey retransmit** *number-of-seconds* **number** *number-of-retransmissions* 例： `Router(gdoi-local-server)# rekey retransmit 10 number 3`	（任意）キー再生成メッセージが再送信される回数を指定します。 • このコマンドが設定されていない場合、再送信は行われません。
ステップ 9	**rekey authentication** {**mypubkey** | **pubkey**} **rsa** *key-name* 例： `Router(gdoi-local-server)# rekey authentication mypubkey rsa mykeys`	（任意）GDOI グループ メンバーに対するキー再生成に使用されるキーを指定します。 • キー再生成が不要な場合、このコマンドは任意です。キー再生成が必須の場合、このコマンドは必須です。
ステップ 10	**exit** 例： `Router(gdoi-local-server)# exit`	GDOI サーバ ローカル コンフィギュレーション モードを終了します。
ステップ 11	**exit** 例： `Router(config-gdoi-group)# exit`	GDOI グループ コンフィギュレーション モードを終了します。
ステップ 12	**access-list** *access-list-number* {**deny** | **permit**} **udp** **host** *source* [*operator*[*port*]] **host** *source* [*operator*[*port*]] 例：	拡張 IP アクセス リストを定義します。

	コマンドまたはアクション	目的
	`Router(config)# access-list 121 permit udp host 10.0.5.2 eq 848 host 239.0.1.2 eq 848`	
ステップ 13	**interface** *type slot/ port* 例： `Router(config)# interface gigabitethernet 0/0`	インターフェイス タイプを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 14	**ip igmp join-group** *group-address* [**source** *source-address*] 例： `Router(config-if)# ip igmp join-group 232.2.2.2 source 10.1.1.1`	指定したグループまたはチャネルに参加するようにルータのインターフェイスを設定します。 （注） 暗号マップが設定されているものと同じインターフェイスでキー サーバに到達できない場合に手動でストリームに参加するには、このコマンドを使用します。

グループ メンバー ACL の設定

deny エントリに一致するすべての IP トラフィックは、グループ メンバーによって、暗号化されていないテキストで送信されます。着信トラフィックは、ミラー アクセス リストに対応付けられます。

（注） グループ メンバー ACL にエントリを追加または削除するために推奨の方法として、最初に既存のグループ メンバー ACL のコピーを異なる名前で作成してから、この新しい ACL のエントリに追加または削除します。その後 GDOI 暗号マップ下の既存のグループ メンバー ACL を新しく作成したグループ メンバー ACL で置き換える必要があります。この推奨の方法に従わない場合、予期しない動作が発生する可能性があります。

グループ メンバー ACL を設定するには、このタスクを実行します（グループ メンバーのアクセス リストに拒否ステートメントが含まれている場合があることに注意してください）。

手順の概要

1. **enable**
2. **configure terminal**
3. **access-list** *access-list-number* **deny ip host** *source* **host** *source*
4. **access-list** *access-list-number* **permit ip** *source*

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： `Router> 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： `Router# 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	**access-list** *access-list-number* **deny ip host** *source* **host** *source* 例： `Router(config)# access-list 101 deny ip host 10.0.0.1 host 10.0.0.2`	拒否される IP アクセス リストを定義します。
ステップ 4	**access-list** *access-list-number* **permit ip** *source* 例： `Router(config)# access-list 103 permit ip 209.165.200.225 0.255.255.255 10.20.0.0 0.255.255.255`	許可される IP アクセス リストを定義します。

次の作業

手順4で定義したアクセス リストは、SAの設定に使用する必要があるものと同じです。「IPsec SA の設定」のセクションを参照してください。

IPsec ライフタイム タイマーの設定

プロファイルのIPsec ライフタイム タイマーを設定するには、次の手順を実行します。この設定作業を実行しない場合、デフォルトは最大IPsec SA ライフタイムの3600秒になります。TEK ライフタイム値は 900 秒を超える値にする必要があります。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto ipsec profile** *name*
4. **set security-association lifetime seconds** *seconds*

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： `Router> 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： `Router# 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 ipsec profile** *name* 例： `Router(config)# crypto ipsec profile profile1`	2 つの IPsec ルータ間における IPsec 暗号化で使用される IPsec パラメータを定義し、暗号化 IPsec プロファイル コンフィギュレーション モードを開始します。
ステップ 4	**set security-association lifetime seconds** *seconds* 例： `Router(ipsec-profile)# set security-association lifetime seconds 2700`	IPsec SA をネゴシエーションするときに使用されるグローバル ライフタイム値を上書きします（特定のクリプト マップ エントリの場合）。

次の作業

IPsec SA を設定します。「IPsec SA の設定」のセクションを参照してください。

ISAKMP ライフタイム タイマーの設定

ISAKMP ライフタイム タイマーを設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto isakmp policy** *priority*
4. **lifetime** *seconds*

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： `Router> 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）。

	コマンドまたはアクション	目的
ステップ 2	**configure terminal** 例： `Router# 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 isakmp policy** *priority* 例： `Router(config)# crypto isakmp policy 1`	IKE ポリシーを定義し、ISAKMP ポリシー コンフィギュレーション モードを開始します。
ステップ 4	**lifetime** *seconds* 例： `Router(config-isakmp-policy)# lifetime 86400`	IKE SA のライフタイムを指定します。

IPsec SA の設定

時間ベースのアンチ リプレイがキー サーバ上で設定されているが、それに対応する機能がグループ メンバーにない場合、GDOI-3-GM_NO_CRYPTO_ENGINE syslog メッセージがグループ メンバーに記録されます。システム エラー メッセージの一覧については、「Cisco Group Encrypted Transport VPN システム ロギング メッセージ」セクションを参照してください。

（注） セキュリティに対する脅威は、脅威からの保護に役立つ暗号化技術と同様に絶え間なく変化しています。最新のシスコの暗号化に関する推奨事項については、『Next Generation Encryption（NGE）ホワイト ペーパー』を参照してください。

IPsec SA を設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto ipsec transform-set** *transform-set-name transform* [*transform2...transform4*]
4. **crypto ipsec profile** *ipsec-profile-name*
5. **set transform-set** *transform-set-name*
6. **exit**
7. **crypto gdoi group** *group-name*
8. 次のいずれかのコマンドを入力します。
   - **identity number** *number*
   - **identity address ipv4** *address*
9. **server local**
10. **sa ipsec** *sequence-number*

11. **profile** *ipsec-profile-name*
12. **match address ipv4** {*access-list-number* | *access-list-name*}
13. **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： `Router> 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： `Router# 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 ipsec transform-set** *transform-set-name transform* [*transform2...transform4*] 例： `Router(config)# crypto ipsec transform-set gdoi-trans esp-aes esp-sha-hmac`	トランスフォーム セット（セキュリティ プロトコルとセキュリティ アルゴリズムの受け入れ可能な組み合わせ）を定義します。
ステップ 4	**crypto ipsec profile** *ipsec-profile-name* 例： `Router(config)# crypto ipsec profile profile1`	IPsec プロファイルを定義し、暗号 ipsec プロファイル コンフィギュレーション モードを開始します。
ステップ 5	**set transform-set** *transform-set-name* 例： `Router(ipsec-profile)# set transform-set transformset1`	クリプト マップ エントリで使用可能なトランスフォーム セットを指定します。
ステップ 6	**exit** 例： `Router(ipsec-profile)# exit`	IPSec プロファイル コンフィギュレーション モードを終了します。
ステップ 7	**crypto gdoi group** *group-name* 例： `Router(config)# crypto gdoi group gdoigroupname`	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 8	次のいずれかのコマンドを入力します。 • **identity number** *number*	GDOI グループ番号またはアドレスを指定します。

	コマンドまたはアクション	目的

	• **identity address ipv4** *address*
	例：
	`Router(config-gdoi-group)# identity number 3333`
	例：
	`Router(config-gdoi-group)# identity address ipv4 209.165.200.225`	

ステップ 9	**server local** 例： `Router(config-gdoi-group)# server local`	デバイスを GDOI キー サーバとして指定し、GDOI ローカル サーバ コンフィギュレーション モードを開始します。
ステップ 10	**sa ipsec** *sequence-number* 例： `Router(gdoi-local-server)# sa ipsec 1`	GDOI グループに使用される IPsec SA ポリシー情報を指定し、GDOI SA IPsec コンフィギュレーション モードを開始する。
ステップ 11	**profile** *ipsec-profile-name* 例： `Router(gdoi-sa-ipsec)# profile gdoi-p`	GDOI グループ用の IPsec SA ポリシーを定義します。
ステップ 12	**match address ipv4** {*access-list-number* | *access-list-name*} 例： `Router(gdoi-sa-ipsec)# match address ipv4 102`	GDOI 登録の IP 拡張アクセス リストを指定します。
ステップ 13	**end** 例： `Router(gdoi-sa-ipsec)# end`	GDOI SA IPsec 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。

次の作業

リプレイを設定する必要があります。リプレイを設定しない場合、デフォルトはカウンタ モードになります。

GDOI グループ用の時間ベースのアンチリプレイの設定

GDOI グループ用の時間ベースのアンチ リプレイを設定するには、次の手順を実行します。

手順の概要

1. **enable**

2. **configure terminal**
3. **crypto gdoi group** *group-name*
4. **identity number** *policy-name*
5. **server local**
6. **address** *ip-address*
7. **sa ipsec** *sequence-number*
8. **profile** *ipsec-profile-name*
9. **match address** {**ipv4** *access-list-number* | *access-list-name*}
10. **replay counter window-size** *seconds*
11. **replay time window-size** *seconds*

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： `Router> 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： `Router# 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： `Router(config)# crypto gdoi group gdoigroup1`	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	**identity number** *policy-name* 例： `Router(config-gdoi-group)# identity number 1234`	GDOI グループ番号を指定します。
ステップ 5	**server local** 例： `Router(config-gdoi-group)# server local`	デバイスを GDOI キー サーバとして指定し、GDOI ローカル サーバ コンフィギュレーション モードを開始します。
ステップ 6	**address** *ip-address* 例： `Router(config-server-local)# address 209.165.200.225`	送信元アドレスを設定します。このアドレスは、ローカル キー サーバによって送信されるパケットの送信元として使用されます。
ステップ 7	**sa ipsec** *sequence-number* 例：	IPsec SA を指定し、GDOI SA IPsec コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
	`Router(config-server-local)# sa ipsec 1`	
ステップ 8	**profile** *ipsec-profile-name* 例： `Router(gdoi-sa-ipsec)# profile test1`	GDOI グループ用の IPsec SA ポリシーを定義します。
ステップ 9	**match address** {**ipv4** *access-list-number* | *access-list-name*} 例： `Router(gdoi-sa-ipsec)# match address ipv4 101`	GDOI 登録の IP 拡張アクセス リストを指定します。
ステップ 10	**replay counter window-size** *seconds* 例： `Router(gdoi-sa-ipsec)# replay counter window-size 512`	1 つのグループ内に 2 つのグループ メンバーだけが存在している場合、GDOI を使用して、アクセス リスト内に定義されたトラフィックのカウンタ ベースのアンチ リプレイ保護をオンにします。 （注） このコマンドによる動作と **replay time window-size** コマンドによる動作は、相互に排他的な関係にあります。設定できるのはどちらか一方だけです。
ステップ 11	**replay time window-size** *seconds* 例： `Router(gdoi-sa-ipsec)# replay time window-size 1`	1 つのグループ内に 3 つ以上のグループ メンバーが存在している場合、GDOI を使用して、アンチ リプレイ保護のウィンドウ サイズを設定します。 （注） このコマンドによる動作と **replay counter window-size** コマンドによる動作は、相互に排他的な関係にあります。設定できるのはどちらか一方だけです。

パッシブ SA の設定

（グループ メンバーを passive モードにするために）パッシブ SA を設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto gdoi group** *group-name*
4. **identity** *name*
5. **passive**
6. **server address ipv4** {*address* | *hostname*}

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： `Router> 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： `Router# 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： `Router(config)# crypto gdoi group group1`	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	**identity** *name* 例： `Router(config-gdoi-group)# identity 2345`	クリプト マップに対して ID を設定します。
ステップ 5	**passive** 例： `Router(config-gdoi-group)# passive`	グループ メンバーを passive モードにします。
ステップ 6	**server address ipv4** {*address* | *hostname*} 例： `Router(config-gdoi-group)# server address ipv4 209.165.200.225`	GDOI グループが到達しようとするサーバのアドレスを指定します。

キー サーバのロールのリセット

プライマリ サーバの連係可能なロールをリセットするには、次の手順を実行します。

手順の概要

1. **enable**
2. **clear crypto gdoi ks coop role**

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： `Router> 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 ks coop role** 例： `Router# clear crypto gdoi ks coop role`	キー サーバの連携ロールをリセットします。

グループ メンバーの設定

グループ メンバーを設定するには、次のサブ作業を実行します。

グループ名、ID、キー サーバ IP アドレス、およびグループ メンバー登録の設定

グループ名、ID、キー サーバ IP アドレス、およびグループ メンバー登録を設定するには、次の手順を実行します。キー サーバ アドレスは 8 個まで設定できます。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto gdoi group** *group-name*
4. 次のいずれかを実行します。
   - **identity number** *number*
   - **identity address ipv4** *address*
5. **server address ipv4** *address*

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： `Router> 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： `Router# 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。

	コマンドまたはアクション	目的
ステップ 3	**crypto gdoi group** *group-name* 例： `Router(config)# crypto gdoi group gdoigroupone`	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	次のいずれかを実行します。
	• **identity number** *number*
	• **identity address ipv4** *address*
	例：
	`Router(config-gdoi-group)# identity number 3333`
	例：
	`Router(config-gdoi-group)# identity address ipv4 209.165.200.225`
		GDOI グループ番号またはアドレスを指定します。

ステップ 5	**server address ipv4** *address* 例： `Router(config-gdoi-group)# server address ipv4 209.165.200.225`	GDOI グループが到達しようとするサーバのアドレスを指定します。 • アドレスを無効にするには、このコマンドの **no** 形式を使用します。

次の作業

クリプト マップを設定します。「暗号マップ エントリの作成」セクションを参照してください。

暗号マップ エントリの作成

クリプト マップ エントリを作成し、それに GDOI グループを関連付けるには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto map** *map-name seq-num* **gdoi**
4. **set group** *group-name*

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
	`Router> enable`	
ステップ 2	**configure terminal** 例： `Router# 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 map** *map-name seq-num* **gdoi** 例： `Router(config)# crypto map mymap 10 gdoi`	クリプト マップ コンフィギュレーション モードを開始して、クリプト マップ エントリを作成または変更します。
ステップ 4	**set group** *group-name* 例： `Router(config-crypto-map)# set group group1`	GDOI グループをクリプト マップに関連付けます。

次の作業

トラフィックを暗号化する必要があるインターフェイスにクリプトマップを適用します。「トラフィックを暗号化する必要があるインターフェイスへの暗号マップの適用」セクションを参照してください。

トラフィックを暗号化する必要があるインターフェイスへの暗号マップの適用

トラフィックを暗号化する必要があるインターフェイスに暗号マップを適用するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type slot* / *port*
4. **crypto map** *map-name* **redundancy** *standby-group-name* **stateful**

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： `Router> 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：	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。

	コマンドまたはアクション	目的
	`Router# configure terminal`	
ステップ 3	**interface** *type slot* / *port* 例： `Router(config)# interface gigabitethernet 0/0`	インターフェイスタイプを設定し、インターフェイス 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	**crypto map** *map-name* **redundancy** *standby-group-name* **stateful** 例： `Router(config-if)# crypto map map1`	クリプトマップをインターフェイスに適用します。

Fail-Close モードのアクティブ化

Fail-Close モードは、グループ メンバーがキー サーバに登録される前に暗号されていないトラフィックがそのグループ メンバーを通過しないようにします。

クリプト マップを Fail-Close モードで動作するように設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto map** *map-name* **gdoi fail-close**
4. **match address** {*access-list-number* | *access-list-name*}
5. **activate**

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： `Router> 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： `Router# 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 map** *map-name* **gdoi fail-close** 例： `Router(config)# crypto map map1 gdoi fail-close`	暗号マップが Fail-Close モードで動作するように指定して暗号マップ Fail-Close コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 4	**match address** {*access-list-number* | *access-list-name*} 例： `Router(crypto-map-fail-close)# match address 133`	（オプション）GDOI 登録用の ACL を指定します。
ステップ 5	**activate** 例： `Router(crypto-map-fail-close)# activate`	Fail-Close モードをアクティブ化します。

フェールクローズ復帰の設定

（注） フェールクローズ復帰機能では、フェールクローズモードをアクティブにする必要があります。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto gdoi group** *group-name*
4. 次のいずれかのコマンドを入力します。
   - **identity number** *number*
   - **identity address ipv4** *address*
5. **server address ipv4** *address*
6. **client fail-close revert**
7. **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： `Router> 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： `Router# 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。

	コマンドまたはアクション	目的
ステップ 3	**crypto gdoi group** *group-name* 例： `Router(config)# crypto gdoi group gdoigroupone`	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	次のいずれかのコマンドを入力します。
	• **identity number** *number*
	• **identity address ipv4** *address*
	例：
	`Router(config-gdoi-group)# identity number 3333`
	例：
	`Router(config-gdoi-group)# identity address ipv4 10.2.2.2`
		GDOI グループ番号またはアドレスを指定します。

ステップ 5	**server address ipv4** *address* 例： `Router(config-gdoi-group)# server address ipv4 10.0.5.2`	GDOI グループが到達しようとするサーバのアドレスを指定します。 • アドレスを無効にするには、このコマンドの **no** 形式を使用します。
ステップ 6	**client fail-close revert** 例： `Router(config-gdoi-group)# client fail-close revert`	クライアント フェール クローズ復帰機能を有効にします。
ステップ 7	**end** 例： `Router(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。

KEK の許容可能な暗号化アルゴリズムまたはハッシュ アルゴリズムの設定

（注） セキュリティに対する脅威は、脅威からの保護に役立つ暗号化技術と同様に絶え間なく変化しています。最新のシスコの暗号化に関する推奨事項については、『Next Generation Encryption』（NGE）ホワイト ペーパーを参照してください。

GM によって許可される KEK の暗号化およびハッシュ アルゴリズムを設定するには、次のステップを実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto gdoi group** *group-name*
4. 次のいずれかのコマンドを入力します。
   - **identity number** *number*
   - **identity address ipv4** *address*
5. **server address ipv4** *address*
6. **client rekey encryption** *cipher* [*... [cipher*]]
7. **client rekey hash** *hash*
8. **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： `Router> 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： `Router# 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： `Router(config)# crypto gdoi group gdoigroupone`	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	次のいずれかのコマンドを入力します。
	• **identity number** *number*
	• **identity address ipv4** *address*
	例：
	`Router(config-gdoi-group)# identity number 3333`
	例：
	`Router(config-gdoi-group)# identity address ipv4 10.2.2.2`
		GDOI グループ番号またはアドレスを指定します。

ステップ 5	**server address ipv4** *address* 例：	GDOI グループが到達しようとするサーバのアドレスを指定します。

	コマンドまたはアクション	目的
	`Router(config-gdoi-group)# server address ipv4 10.0.5.2`	• アドレスを無効にするには、このコマンドの **no** 形式を使用します。
ステップ 6	**client rekey encryption** *cipher* [*... [cipher]*] 例： `Router(config-gdoi-group)# client rekey encryption aes 128 aes 192 aes 256`	KEK のクライアント受け入れ可能キー再生成暗号化を設定します。
ステップ 7	**client rekey hash** *hash* 例： `Router(config-gdoi-group)# client rekey hash sha`	KEK のクライアント受け入れ可能ハッシュを設定します。
ステップ 8	**end** 例： `Router(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。

TEK の受け入れ可能トランスフォーム セットの設定

GM によって許可されるデータ暗号化または認証のために TEK が使用するトランスフォーム セットを設定するには、次のステップを実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto ipsec transform-set** *transform-set-name transform* [*transform2...transform4*]
4. **exit**
5. **crypto gdoi group** *group-name*
6. **client transform-sets** *transform-set-name1* [*... [transform-set-name6*]]
7. **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： `Router> 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：	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。

	コマンドまたはアクション	目的
	`Router# configure terminal`	
ステップ 3	**crypto ipsec transform-set** *transform-set-name transform* [*transform2...transform4*] 例： `Router(config)# crypto ipsec transform-set g1 esp-aes 192 esp-sha-hmac`	トランスフォーム セット（セキュリティ プロトコルおよびアルゴリズムの受け入れ可能な組み合わせ）を定義し、暗号化トランスフォーム 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	**exit** 例： `Router(cfg-crypto-trans)# exit`	暗号化トランスフォーム コンフィギュレーション モードを終了します。
ステップ 5	**crypto gdoi group** *group-name* 例： `Router(config)# crypto gdoi group gdoigroupone`	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 6	**client transform-sets** *transform-set-name1* [*... [transform-set-name6*]] 例： `Router(config-gdoi-group)# client transform-sets g1`	データの暗号化および認証のために TEK によって使用される受け入れ可能トランスフォーム タグを指定します。 • トランスフォーム セット タグは 6 個まで指定できます。
ステップ 7	**end** 例： `Router(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。

グループ メンバーの暗号状態の追跡

設定済みの拡張オブジェクト トラッカー（EOT）のスタブオブジェクト ID を使用してグループ メンバー（GM）の暗号化状態を追跡するには、この作業を実行します。

始める前に

スタブオブジェクトを作成し、このオブジェクトにトラッキング ID を割り当てて GDOI MIB をモニタすることにより、拡張オブジェクト トラッキング（EOT）を設定する必要があります。次に、トラッキング ID 99 をスタブオブジェクトに割り当てる設定例を示します。

```
event manager applet test1
 event snmp oid <new GDOI MIB object> .....
 action 2.0 track set 99 state up

track 99 stub-object
 delay up 60
```

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto gdoi group** *group-name*
4. **client status active-sa track** *tracking-number*
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	**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 gdoigroupone`	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 status active-sa track** *tracking-number* 例： `Device(config-gdoi-group)# client status active-sa track 99`	スタブオブジェクトの追跡を有効化します。この例では、GM がキー サーバ（KS）から有効なトラフィック暗号キー（TEK）を受信すると、スタブオブジェクト 99 の状態を「UP」に設定します。一方、登録失敗やキー再生成の前に TEK の期限が切れた場合などのエラーのために有効な TEK がない場合、GM はスタブオブジェクト 99 の状態を「DOWN」に設定します。
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、特権 EXEC モードに戻ります。

GET VPN GM 認証の設定

GET VPN GM 認証は、事前共有キーまたは PKI を使用して実行できます。GET VPN 認証をオンにすることはベスト プラクティスです。キー サーバが複数の GDOI グループに使用される際、あるグループの GM が別のグループからキーとポリシーを要求するのを防ぐには、キー サーバ認証が必要です。ISAKMP 認証では GM がキー サーバから GDOI 属性を要求できることが確認され、GDOI 認証では GM がキー サーバに設定された特定のグループから GDOI 属性を要求できることが確認されます。

GET VPN GM 認証を設定するには、次のいずれかのタスクを実行します。

事前共有キーを使用する GM 認証の設定

事前共有キーを使用する GM の認証を設定するには、次のステップを実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto gdoi group** *group-name*
4. **server local**
5. **authorization address ipv4 {** *access-list-name* | *access-list-number* **}**
6. **exit**
7. **exit**
8. **access-list** *access-list-number* [**dynamic** *dynamic-name* [**timeout** *minutes*]] {**deny** | **permit**} *protocol source source-wildcard destination destination-wildcard* [**precedence** *precedence*] [**tos** *tos*] [**time-range** *time-range-name*] [**fragments**] [**log** [*word*] | **log-input** [*word*]]
9. **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	**enable** 例： `Router> 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： `Router# 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： `Router(config)# crypto gdoi group getvpn`	GDOI 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	**server local** 例： `Router(config-gdoi-group)# server local`	デバイスを GDOI キー サーバとして指定し、GDOI ローカル サーバ 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	**authorization address ipv4 {** *access-list-name* | *access-list-number* **}** 例：	GDOI のアドレスのリストを指定します。

	コマンドまたはアクション	目的
	`Router(gdoi-local-server)# authorization address ipv4 50`	
ステップ 6	**exit** 例： `Router(gdoi-local-server)# exit`	GDOI ローカル コンフィギュレーション モードを終了して GDOI グループ コンフィギュレーション モードに戻ります。
ステップ 7	**exit** 例： `Router(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。
ステップ 8	**access-list** *access-list-number* [**dynamic** *dynamic-name* [**timeout** *minutes*]] {**deny** | **permit**} *protocol source source-wildcard destination destination-wildcard* [**precedence** *precedence*] [**tos** *tos*] [**time-range** *time-range-name*] [**fragments**] [**log** [*word*] | **log-input** [*word*]] 例： `Router(config)# access-list 50 permit ip 209.165.200.225 0.0.0.0 209.165.200.254 0.0.0.0`	許可される IP アクセス リストを定義します。 • この例では、アクセス リスト番号 50 のアクセス リストが定義され、送信元 IP アドレス 209.165.200.225 から宛先 IP アドレス 209.165.200.254 に送信されるパケットが許可されます。
ステップ 9	**exit** 例： `Router(config)# exit`	グローバル 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。

PKI を使用する GM 認証の設定

PKI を使用する GM の認証を設定するには、次のステップを実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto isakmp identity** {**address** | **dn** | **hostname**}
4. **crypto pki trustpoint** *name*
5. **subject-name** [*x.500-name*]
6. **exit**
7. **crypto gdoi group** *group-name*
8. **server local**
9. **authorization identity** *name*
10. **exit**
11. **exit**

12. **crypto identity** *name*
13. **dn** *name=string* [, *name=string*]
14. **exit**
15. **crypto isakmp identity** {**address** | **dn** | **hostname** }
16. **crypto pki trustpoint** *name*
17. **subject-name** [*x.500-name*]
18. **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： `Router> 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： `Router# 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 isakmp identity** {**address** | **dn** | **hostname**} 例： `Router(config)# crypto isakmp identity dn`	ルータがインターネットキー交換（IKE）プロトコルに参加する際にルータが使用するアイデンティティを定義します。
ステップ 4	**crypto pki trustpoint** *name* 例： `Router(config)# crypto pki trustpoint GETVPN`	ルータで使用するトラストポイントを宣言し、CA トラストポイント 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	**subject-name** [*x.500-name*] 例： `Router(ca-trustpoint)# subject-name OU=GETVPN`	証明書要求の所有者名を指定します。
ステップ 6	**exit** 例： `Router(ca-trustpoint)# exit`	CA トラストポイント 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。
ステップ 7	**crypto gdoi group** *group-name* 例： `Router(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。

	コマンドまたはアクション	目的
ステップ 8	**server local** 例： `Router(config-gdoi-group)# server local`	デバイスを GDOI キー サーバとして指定し、GDOI ローカル サーバ コンフィギュレーション モードを開始します。
ステップ 9	**authorization identity** *name* 例： `Router(gdoi-local-server)# authorization identity GETVPN_FILTER`	GDOI グループのアイデンティティを指定します。
ステップ 10	**exit** 例： `Router(gdoi-local-server)# exit`	GDOI ローカル サーバ コンフィギュレーション モードを終了して GDOI グループ コンフィギュレーション モードに戻ります。
ステップ 11	**exit** 例： `Router(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。
ステップ 12	**crypto identity** *name* 例： `Router(config)# crypto identity GETVPN_FILTER`	ルータの証明書内にある指定 DN リストを使用してルータのアイデンティティを設定し、暗号アイデンティティ コンフィギュレーション モードを開始します。
ステップ 13	**dn** *name=string* [, *name=string*] 例： `Router(config-crypto-identity)# dn ou=GETVPN`	ルータの証明書内にある DN に、ルータのアイデンティティを関連付けます。
ステップ 14	**exit** 例： `Router(config-crypto-identity)# 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。
ステップ 15	**crypto isakmp identity** {**address** | **dn** | **hostname** } 例： `Router(config)# crypto isakmp identity dn`	IKE プロトコルに参加する際にルータが使用するアイデンティティを定義します。
ステップ 16	**crypto pki trustpoint** *name* 例： `Router(config)# crypto pki trustpoint GETVPN`	ルータで使用するトラストポイントを宣言し、CA トラストポイント コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 17	**subject-name** [*x.500-name*] 例： `Router(ca-trustpoint)# subject-name ou=getvpn`	証明書要求の所有者名を指定します。
ステップ 18	**end** 例： `Router(ca-trustpoint)# exit`	GDOI グループ コンフィギュレーション モードを終了し、設定を保存して、特権 EXEC モードに戻ります。

Cisco Group Encrypted Transport VPN 設定の確認とトラブルシューティング

GET VPN の設定を確認およびトラブルシューティングするには、次の作業を行います。これらの作業は任意であり、トラブルシューティング中に情報を収集するために行います。

（注） CSCsi82594 では、時間ベースのアンチリプレイ（TBAR）を有効にした場合、キー再生成の期間は 2 時間（7200 秒）に設定されます。このシナリオでは、キー サーバは 2 時間（7200 秒）ごとにグループ メンバーに定期的にキー再生成を送信します。次の例では、トラフィック暗号キー（TEK）のライフタイムが 28800 秒（8 時間）に設定されていますが、キー再生成タイマーは依然として 2 時間です。TBAR 情報を表示する show 出力の場合は、**show crypto gdoi gm replay** コマンドおよび **show crypto gdoi ks replay** コマンドを使用します。

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

キー サーバ上のアクティブなグループ メンバーの確認

キー サーバ上のアクティブなグループ メンバーを確認するには、次の手順を実行します。

手順の概要

1. **enable**
2. **show crypto gdoi 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： `Router> 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 ks members** 例： `Router# show crypto gdoi ks members`	キー サーバ メンバーに関する情報を表示します。

キー再生成関連統計情報の確認

キー再生成関連統計情報を確認するには、次の手順を実行します。

手順の概要

1. **enable**
2. **show crypto gdoi ks rekey**
3. **show crypto gdoi [gm]**

手順の詳細

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 ks rekey**

例：

```
Device# show crypto gdoi ks rekey

For group diffint (handle: 2147483650) server 10.0.8.1 (handle: 2147483650):

# of teks : 1 Seq num : 0
KEK POLICY (transport type : Unicast)
spi : 0xA8110DE7CC8B0FB201F2A8BFAA0F2D90
management alg : disabled encrypt alg : 3DES
crypto iv length : 8 key size : 24
orig life(sec): 300 remaining life(sec): 296 <------- ticking down
sig hash algorithm : enabled sig key length : 94
```

```
sig size : 64
sig key name : mykeys
```

キーサーバ上でこのコマンドを実行すると、キーサーバから送信されるキー再生成に関する情報が表示されます。出力は、KEK の残りのライフタイムの経過を表示します。

ステップ 3 show crypto gdoi [gm]

例：

```
Device# show crypto gdoi
GROUP INFORMATION

Group Name : diffint
Group Identity : 3333
Rekeys received : 0
IPSec SA Direction : Both

Group Server list : 10.0.8.1

Group member : 10.0.3.1 vrf: None
Version : 1.0.2
Registration status : Registered
Registered with : 10.0.8.1
Re-registers in : 93 sec <-----------re-registration time for TEK or KEK
Succeeded registration: 1
Attempted registration: 1
Last rekey from : 0.0.0.0
Last rekey seq num : 0
Unicast rekey received: 0
Rekey ACKs sent : 0
Rekey Received : never
allowable rekey cipher: any
allowable rekey hash : any
allowable transformtag: any ESP

Rekeys cumulative
Total received : 0
After latest register : 0
Rekey Acks sents : 0

ACL Downloaded From KS 10.0.8.1:
access-list permit ip host 10.0.1.1 host 239.0.1.1
access-list permit ip host 10.0.100.2 host 238.0.1.1

KEK POLICY:
Rekey Transport Type : Unicast
Lifetime (secs) : 255 <-----------lifetime ticking
Encrypt Algorithm : 3DES
Key Size : 192
Sig Hash Algorithm : HMAC_AUTH_SHA
Sig Key Length (bits) : 512
```

グループメンバー上でこのコマンドを実行すると、キーサーバから送信されるキー再生成に関する情報が表示されます。出力の「re-registers in」フィールドは、その後にグループ メンバーが TEK または KEK に再登録する、より短い方の期間を表示します。

グループ メンバー上で GDOI によって作成された IPsec SA の確認

グループ メンバー上で GDOI によって作成された IPsec SA を確認するには、次の手順を実行します。

手順の概要

1. **enable**
2. **show crypto gdoi group** *group-name* **ipsec sa**

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： `Router> 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 group** *group-name* **ipsec sa** 例： `Router# show crypto gdoi group diffint ipsec sa`	グループ メンバー上で GDOI によって作成された IPsec SA に関する情報を表示します。 • この場合、表示されるのは、グループ「diffint」に関する情報だけです。 • すべてのグループの IPsec SA に関する情報を表示するには、**group** キーワードおよび *group-name* 引数を省略します。

キー サーバ上で GDOI によって作成された IPsec SA の確認

キー サーバ上で GDOI によって作成された IPsec SA を確認するには、次の手順を実行します。

手順の概要

1. **enable**
2. **show crypto ipsec sa**

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 ipsec sa** 例：	現在の SA によって使用されている設定を表示します。

	コマンドまたはアクション	目的
	`Device# show crypto ipsec sa`	

グループ メンバーが最後にキー サーバから受信した TEK の確認

GM が最後に KS から受信した TEK を確認するには、GM で次のステップを実行します。

手順の概要

1. **enable**
2. **show crypto gdoi**

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： `Router> 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** 例： `Router# show crypto gdoi`	現在の GDOI 構成、および KS からダウンロードされたポリシーを表示します。TEK は TEK POLICY セクションに表示されます。デバッグを有効にせずに、次のコマンドを使用することで、TEK が実際に最後に受信した GM を KS から IPsec コントロールプレーンにダウンロードした TEK（**show crypto ipsec sa** コマンドを使用して表示可能）と比較できます。

連携キー サーバの状態と統計情報の確認

連携キーサーバーの状態と統計情報を確認するには、**debug** および **show** コマンドのうち 1 つまたは両方を使用して、次の手順を実行します。

手順の概要

1. **enable**
2. **debug crypto gdoi ks coop**
3. **show crypto gdoi group** *group-name* **ks coop** [**version**]

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
	`Router> enable`	
ステップ 2	**debug crypto gdoi ks coop** 例： `Router# debug crypto gdoi ks coop`	連携キー サーバに関する情報を表示します。
ステップ 3	**show crypto gdoi group** *group-name* **ks coop** [**version**] 例： `Router# show crypto gdoi group diffint ks coop version`	グループ「diffint」に関する情報と、連携キー サーバに関するバージョン情報を表示します。

アンチリプレイ疑似時間関連の統計情報の確認

アンチリプレイ疑似時間関連の統計情報を確認するには、**clear**、**debug**、および **show** コマンドのうち 1 つまたはすべてを使用して、次の手順を実行します。

手順の概要

1. **enable**
2. **clear crypto gdoi group** *group-name* **replay**
3. **debug crypto gdoi replay**
4. **show crypto gdoi group** *group-name*
5. **show crypto gdoi group** *group-name* **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： `Router> 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* **replay** 例： `Router# clear crypto gdoi group diffint replay`	リプレイ カウンタを消去します。
ステップ 3	**debug crypto gdoi replay** 例： `Router# debug crypto gdoi replay`	パケット内に格納されている疑似時間スタンプに関する情報を表示します。

	コマンドまたはアクション	目的
ステップ 4	**show crypto gdoi group** *group-name* 例： `Router# show crypto gdoi group diffint`	グループ メンバーの現在の疑似時間に関する情報を表示します。 • このグループのアンチ リプレイに関連する各種カウントも表示します。
ステップ 5	**show crypto gdoi group** *group-name* **ks replay** 例： `Router# show crypto gdoi group diffint ks replay`	キー サーバの現在の疑似時間に関する情報を表示します。

暗号マップの Fail-Close モードの状態の確認

クリプト マップの Fail-Close モードの状態を確認するには、次の手順を実行します。

手順の概要

1. **enable**
2. **show crypto map gdoi fail-close**

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： `Router> 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 map gdoi fail-close** 例： `Router# show crypto map gdoi fail-close`	Fail-Close モードの状態に関する情報を表示します。

Cisco Group Encrypted Transport VPN の設定例

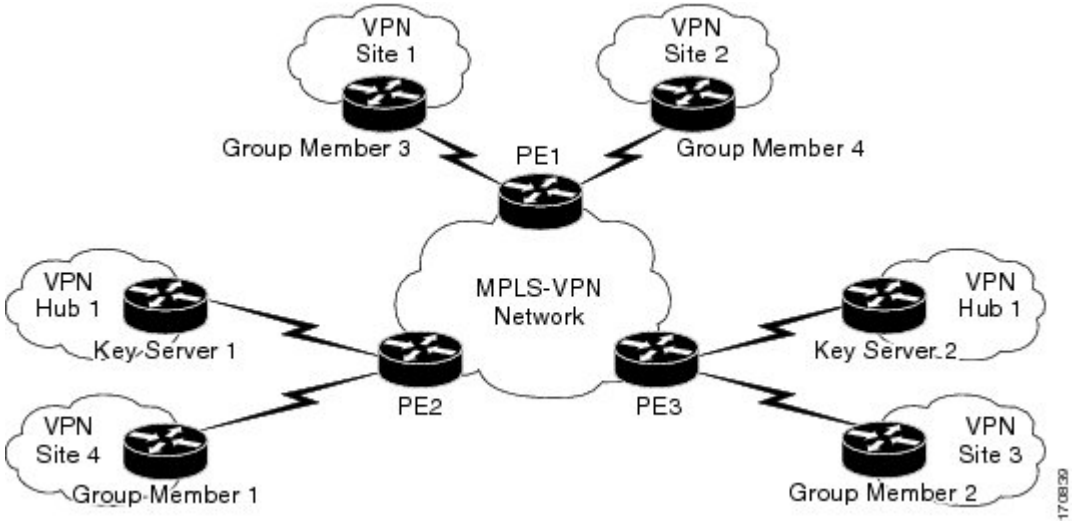
例：キー サーバとグループ メンバーのケース スタディ

次のケース スタディでは、MPLS VPN 環境における CE 間のトラフィックを暗号化します。

MPLS VPN コアによって、下図に示すとおりに各 VPN サイトを相互接続します。Group Member 1 から Group Member 4 までの VPN サイト CPE を、これらのサイトがその一部となっている VPN と関連付けられた単一の GDOI グループにグループ化します。このシナリオは、インター

ネット VPN のシナリオです。すべてのキー サーバおよびグループ メンバーは同じ VPN の一部です。Key Server 1 と Key Server 2 は連携キー サーバであり、VPN メンバーである Group Member 1 から Group Member 4 までがサポートされています。Key Server 1 はプライマリ キー サーバであり、Key Server 2 はセカンダリ キー サーバです。

図 *13*：キー サーバとグループ メンバーのシナリオ



次の設定例は上図のケース スタディに基づいています。

キー サーバ 1 の例

Key server 1 はプライマリ キー サーバです。

```
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service internal
!
hostname KS1
!
logging buffered 100000 debugging
no logging console
!
no aaa new-model
!
resource policy
!
clock timezone EST 0
ip subnet-zero
no ip domain lookup
ip domain name cisco.com
!
crypto isakmp policy 1
 encr 3des
 authentication pre-share
 group 2
 lifetime 400
crypto isakmp key cisco address 10.1.1.13
```

```
crypto isakmp key cisco address 10.1.1.9
crypto isakmp key cisco address 10.1.1.1
crypto isakmp key cisco address 10.1.1.5
crypto isakmp key cisco address 10.1.1.21
!
crypto ipsec transform-set gdoi-trans-group1 esp-3des esp-sha-hmac
!
crypto ipsec profile gdoi-profile-group1
 set security-association lifetime seconds 1800
 set transform-set gdoi-trans-group1
!
crypto gdoi group group1
 identity number 1
 server local
  rekey lifetime seconds 86400
  rekey retransmit 10 number 2
  rekey authentication mypubkey rsa group1-export-general
  rekey transport unicast
  sa ipsec 1
   profile gdoi-profile-group1
   match address ipv4 101
   replay counter window-size 64
  address ipv4 209.165.200.225
  redundancy
   local priority 10
   peer address ipv4 209.165.200.225
   !
interface Ethernet0/0
 ip address 209.165.200.225 255.255.255.252
!
ip classless
ip route 0.0.0.0 0.0.0.0 10.1.1.18
!
access-list 101 permit ip 10.1.0.0 0.0.255.255 10.1.0.0 0.0.255.255
!
end
```

キー サーバ 2 の例

Key Server 2はセカンダリ キー サーバです。

```
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service internal
!
hostname KS2
!
logging buffered 100000 debugging
no logging console
!
no aaa new-model
!
resource policy
!
clock timezone EST 0
ip subnet-zero
no ip domain lookup
ip domain name cisco
!
crypto isakmp policy 1
```

```
 encr 3des
 authentication pre-share
 group 2
 lifetime 400
crypto isakmp key cisco address 10.1.1.9
crypto isakmp key cisco address 10.1.1.1
crypto isakmp key cisco address 10.1.1.5
crypto isakmp key cisco address 10.1.1.17
crypto isakmp key cisco address 10.1.1.13
!
crypto ipsec transform-set gdoi-trans-group1 esp-3des esp-sha-hmac
!
crypto ipsec profile gdoi-profile-group1
 set security-association lifetime seconds 1800
 set transform-set gdoi-trans-group1
!
crypto gdoi group group1
 identity number 1
 server local

  rekey lifetime seconds 86400
  rekey retransmit 10 number 2
  rekey authentication mypubkey rsa group1-export-general
  rekey transport unicast
  sa ipsec 1
   profile gdoi-profile-group1
   match address ipv4 101
   replay counter window-size 64
  address ipv4 10.1.1.21
  redundancy
   local priority 1
   peer address ipv4 10.1.1.17
   !
interface Ethernet0/0
 ip address 209.165.200.225 255.255.255.252
!
ip classless
ip route 0.0.0.0 0.0.0.0 10.1.1.22
!
access-list 101 permit ip 10.1.0.0 0.0.255.255 10.1.0.0 0.0.255.255
!
end
```

例：グループ メンバー 1 の設定

Group Member 1 は、これらのサイトがその一部となっている VPN と関連付けられた GDOI グループの一部です。

```
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname GM1
!
resource policy
!
clock timezone EST 0
ip subnet-zero
!
crypto isakmp policy 1
 encr aes
```

```
 authentication pre-share
 group 14
 lifetime 3600
crypto isakmp key cisco address 209.165.200.225
crypto isakmp key cisco address 209.165.201.1
!
crypto gdoi group group1
 identity number 1
 server address ipv4 209.165.200.225
 server address ipv4 209.165.201.1
!
crypto map map-group1 10 gdoi
 set group group1
!
interface Ethernet0/0
 ip address 209.165.200.225 255.255.255.252
 crypto map map-group1
!
router bgp 1000
 no synchronization
 bgp log-neighbor-changes
 network 10.1.1.0 mask 255.255.255.0
 neighbor 10.1.1.2 remote-as 5000
 no auto-summary
!
ip classless
!
End
The same GDOI group cannot be applied to multiple interfaces. The following examples
show unsupported cases:
```

例 1

```
crypto map map-group1
  group g1
 interface ethernet 1/0
  crypto map map-group1
 interface ethernet 2/0
  crypto map map-group1
```

例 2

```
crypto map map-group1 10 gdoi
  set group group1
crypto map map-group2 10 gdoi
  set group group1
 interface ethernet 1/0
  crypto map map-group1
 interface ethernet 2/0
```

例：グループ メンバー 2 の設定

Group Member 2 は、これらのサイトがその一部となっている VPN と関連付けられた GDOI グループの一部です。

```
service timestamps debug datetime msec
service timestamps log datetime msec
!
```

```
hostname GM2
!
resource policy
!
clock timezone EST 0
ip subnet-zero
!
crypto isakmp policy 1
 encr aes
 authentication pre-share
 group 14
 lifetime 3600
crypto isakmp key cisco address 209.165.200.225
crypto isakmp key cisco address 209.165.201.1
!
crypto gdoi group group1
 identity number 1
 server address ipv4 209.165.201.1
 server address ipv4 209.165.200.225
!
crypto map map-group1 10 gdoi
 set group group1
!
interface Ethernet0/0
 ip address 209.165.200.225 255.255.255.252
 crypto map map-group1
!
router bgp 2000
 no synchronization
 bgp log-neighbor-changes
 network 10.1.2.0 mask 255.255.255.0
 neighbor 10.1.1.6 remote-as 5000
 no auto-summary
!
ip classless
!
end
```

例：グループ メンバー 3 の設定

Group Member 3 は、これらのサイトがその一部となっている VPN と関連付けられた GDOI グループの一部です。

```
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname GM3
!
resource policy
!
clock timezone EST 0
ip subnet-zero
!
crypto isakmp policy 1
 encr aes
 authentication pre-share
 group 14
 lifetime 3600
crypto isakmp key cisco address 209.165.200.225
crypto isakmp key cisco address 209.165.201.1
```

```
!
crypto ipsec transform-set gdoi-trans-group1 esp-aes esp-sha-hmac
crypto gdoi group group1
 identity number 1
 server address ipv4 209.165.200.225
 server address ipv4 209.165.201.1
!
crypto map map-group1 10 gdoi
 set group group1
!
interface Ethernet0/0
 ip address 209.165.201.1 255.255.255.252
 crypto map map-group1
!
router bgp 3000
 no synchronization
 bgp log-neighbor-changes
 network 10.1.3.0 mask 255.255.255.0
 neighbor 10.1.1.10 remote-as 5000
 no auto-summary
!
ip classless
!
end
```

例：グループ メンバー 4 の設定

Group Member 4 は、これらのサイトがその一部となっている VPN と関連付けられた GDOI グループの一部です。

```
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname GM4
!
clock timezone EST 0
ip subnet-zero
!
crypto isakmp policy 1
 encr aes
 authentication pre-share
 group 14
 lifetime 3600
crypto isakmp key cisco address 209.165.200.225
crypto isakmp key cisco address 209.165.201.1
!
crypto gdoi group group1
 identity number 1
 server address ipv4 209.165.200.225
 server address ipv4 209.165.201.1
!
crypto map map-group1 10 gdoi
 set group group1
!
interface Ethernet0/0
 ip address 209.165.201.1 255.255.255.252
 crypto map map-group1
!
router bgp 4000
 no synchronization
```

```
 bgp log-neighbor-changes
 network 10.1.4.0 mask 255.255.255.0
 neighbor 10.1.1.14 remote-as 5000
 no auto-summary
!
ip classless
!
end
```

例：グループ メンバー5 の設定

グループ メンバーの複数のインターフェイスが同じGDOIグループの一部である場合、ループバック インターフェイスを使用して暗号化を行う必要があります。ループバック インターフェイスを使用しない場合、暗号化されたトラフィックが処理される各インターフェイスを個別にキー サーバに登録する必要があります。

キー サーバではこれらが別個の要求と判断されるので、同一のグループ メンバーの複数のレコードが保管されます。これは、複数のキー再生成が送信されることも意味します。暗号化がループバック インターフェイスから行われる場合は、グループ メンバーを一度だけキー サーバに登録します。

次の設定は、どのようにグループ メンバーを一度だけキー サーバに登録するのかを示しています。

```
!


interface GigabitEthernet0/1
 description *** To AGG-1 ***
 crypto map dgvpn
!
interface GigabitEthernet0/2
 description *** To AGG-2 ***
 crypto map dgvpn
!
interface Loopback0
 ip address 209.165.201.1 255.255.255.255
!
 crypto map dgvpn local-address Loopback0
!
```

例：グループ メンバーが最後にキー サーバから受信した TEK の確認

次の例は、現在の GDOI 構成、および KS からダウンロードされたポリシーを表示する方法を示します。

```
Device# show crypto gdoi

GROUP INFORMATION

    Group Name               : GETV6
.
.
.
KEK POLICY:
.
```

```
.
.
TEK POLICY for the current KS-Policy ACEs Downloaded:
  Ethernet2/0:
    IPsec SA:
        spi: 0x627E4B84(1652444036)
        transform: esp-aes
        sa timing:remaining key lifetime (sec): (3214)
        Anti-Replay(Time Based) : 10 sec interval
        tag method : cts sgt
        alg key size: 24 (bytes)
        sig key size: 20 (bytes)
        encaps: ENCAPS_TUNNEL


GROUP INFORMATION

    Group Name               : GETV4
.
.
.
KEK POLICY:
.
.
.
TEK POLICY for the current KS-Policy ACEs Downloaded:
  Ethernet2/0:
    IPsec SA:
        spi: 0xF6E6B597(4142314903)
        transform: esp-aes
        sa timing:remaining key lifetime (sec): (3214)
        Anti-Replay : Disabled
        tag method : cts sgt
        alg key size: 24 (bytes)
        sig key size: 20 (bytes)
        encaps: ENCAPS_TUNNEL
```

TEK は TEK POLICY セクションに表示されます。デバッグを有効にせずに、次のコマンドを使用することで、TEK が実際に最後に受信した GM を KS から IPsec コントロールプレーンにダウンロードした TEK（**show crypto ipsec sa** コマンドを使用して表示可能）と比較できます。

タグ メソッド フィールドは、GET VPN インライン タギングに使用するメソッドを示します。可能な値は cts sgt（Cisco TrustSec セキュリティ グループ タグ用）または無効です。alg キー サイズ フィールドは、TEK ポリシーで設定されている暗号化アルゴリズムのキーの長さを示します。sig キー サイズ フィールドは、TEK ポリシーで設定されている署名のキーの長さを示します。encaps フィールドは、TEK ポリシーで設定されている IPsec カプセル化のタイプ（トンネルまたはトランスポート）を示します。

このコマンドの出力は、TEK が KS から受け取った時刻から期限切れになったことを示す場合があります。

パッシブ SA の例

次の例は、発信パケットに関する暗号化ルールに関する情報を示しています。

```
Router# show crypto ruleset
```

```
Ethernet0/0:
  59 ANY ANY DENY
  11 ANY/848 ANY/848 DENY
 IP ANY ANY IPSec SA Passive
 IP ANY ANY IPSec Cryptomap
```

次の例は、IPsec SA の方向モードを示しています。

```
Router# show crypto ruleset detail
Ethernet0/0:
 20000001000019  59 ANY ANY DENY -> 20000001999999
20000001000029  11 ANY/848 ANY/848 DENY -> 20000001999999
 20000001000035 IP ANY ANY IPSec SA Passive
 20000001000039 IP ANY ANY IPSec Cryptomap
```

Fail-Close モードの例

次の例は、Fail-Close モードがすでにアクティブになっていて、グループ メンバーが登録される前のアクセス リスト 102 からの暗号化されていないトラフィックが許可されていることを示しています。

```
crypto map map1 gdoi fail-close
 match address 102
 activate
crypto map map1 10 gdoi
 set group ks1_group
 match address 101
!
access-list 101 deny ip 10.0.1.0 0.0.0.255 10.0.1.0 0.0.0.255
access-list 102 deny tcp any eq telnet any
```

次の **show crypto map gdoi fail-close** コマンドの出力は、Fail-Close モードがすでにアクティブになっていることを示しています。

```
Router# show crypto map gdoi fail-close

Crypto Map: "svn"
        Activate: yes
        Fail-Close Access-List: (Deny = Forward In Clear, Permit = Drop)
            access-list 105 deny tcp any port = 23 any
            access-list 105 deny ospf any any
```

例：フェールクローズ復帰の確認

```
Device#show cry gdoi group GDOI_GROUP_1 | i Fail|Policy
       Fail-Close Revert : Enabled
       KS Policy Removal in : 697 sec
```

Cisco Group Encrypted Transport VPN の追加の制約事項

標準

標準	タイトル
新しい標準または変更された標準はサポートされていません。また、既存の標準に対するサポートに変更はありません。	—

MIB

MIB	MIB のリンク
CISCO-GDOI-MIB	選択したプラットフォーム、Cisco ソフトウェア リリース、およびフィーチャ セットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
RFC 2401	『*Security Architecture for the Internet Protocol*』
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

Cisco Group Encrypted Transport VPN 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 *4 : Cisco Group Encrypted Transport VPN* の機能情報

機能名	リリース	機能情報
Cisco Group Encrypted Transport VPN	Cisco IOS XE Release 2.3	Cisco Group Encrypted Transport VPN は、any-to-any の接続を必要とする大規模な IP または MPLS サイトに対する最適な暗号化ソリューションであり、コンバージェンスに要する時間が最短に抑えられ、処理、プロビジョニング、管理、トラブルシューティングの低いオーバヘッドを実現しています。 次のコマンドが導入または変更されました。**address ipv4 (GDOI)**、**clear crypto gdoi**、**crypto gdoi gm**、 **debug crypto gdoi**、 **local priority**、 **peer address ipv4**、 **redundancy**、 **rekey address ipv4**、 **rekey transport unicast**、 **replay counter window-size**、 **replay time window-size**、 **sa receive-only**、**show crypto gdoi**。
GDOI 登録成功を追跡する MIB オブジェクトの作成	Cisco IOS XE リリース 3.12S	GDOI 登録成功を追跡する MIB オブジェクトの作成機能では、グループ内のアクティブな TEK 数を示すため、GDOI MIB に新しい MIB オブジェクトが導入されています。
GET VPN の強化	Cisco IOS XE Release 3.9S	この機能は GET VPN の復元力を改善します。復元力を強化することで、次のいずれかの方法を使用してデータ トラフィックの中断を防止または最小化します。 • トラフィックの中断の原因となる状態が検出された場合に修正を行います。 • 障害が検出された場合に迅速に回復機能を実行します。 次のコマンドが変更されました。**show crypto gdoi**、**show crypto ipsec sa**、**show tech-support**。

機能名	リリース	機能情報
GET VPN IKEv1 の分離	Cisco IOS XE Release 3.11S	この機能は、メンテナンスやトラブルシューティングに役立ちます。 次のコマンドが変更されました。**show tech-support**、**show crypto gdoi**、および **show crypto ipsec sa**。
GET VPN フェーズ 1.2	Cisco IOS XE Release 2.3	これらの機能拡張には、次の機能があります。 • キー サーバのロールの変更 この機能を使用すれば、キー サーバのロールをプライマリからセカンダリに変更できます。 この機能により、次のコマンドが導入または変更されました。**clear crypto gdoi ks coop role** • Fail-Close モード この機能によって、グループ メンバーが登録される前に、暗号化されていないトラフィックがそのグループ メンバーを通過することを防止できます。 この機能により、次のコマンドが導入または変更されました。**activate**、**crypto map**、**match address**、および **show crypto map**。 • パッシブ SA この機能を使用すれば、グループ メンバーを passive モードに永続的に設定できます。 次のコマンドが導入されました：**passive**
BGP 向けの GETVPN ルーティング対応	Cisco IOS XE リリース 3.13S	次のコマンドが導入または変更されました。**client status active-sa track**。

機能名	リリース	機能情報
GET VPN の復元力	Cisco IOS XE Release 3.9S	この機能は、エラーが発生したときのデータ トラフィックの中断が防止または最小化されるように GET VPN の復元力を向上します。 この機能は、長い SA ライフタイムの機能を導入しています。これにより、キー暗号キーとトラフィック暗号キーのライフタイムを最大 24 時間から 30 日に延長して設定できます。また、この機能により、最後にスケジュールされたキー再生成の確認応答で応答しなかったグループ メンバーに、定期的にリマインダ キー再生成を送信し続けるようにキー サーバを設定することができます。 長いSAライフタイムを定期的なリマインダ キー再生成と組み合わせて使用することで、キーがロールオーバーする前にグループ メンバーがスケジュールされたキー再生成を行わない場合、キー サーバがグループ メンバーを効果的に同期できます。 次のコマンドが変更されました。**rekey lifetime**、**rekey retransmit**、**set security-association lifetime**、**show crypto gdoi**。
Cisco TrustSec の IPsec インライン タギングの GET VPN サポート	Cisco IOS XE Release 3.9S	Cisco TrustSec（CTS）は、認証時に取得したユーザとデバイスの ID 情報を使用して、ネットワークに進入するパケットを分類します。CTS では、CTS ネットワークへの進入時にセキュリティ グループ タグ（SGT）でパケットにタグを付けることで各パケットの分類が維持されます。これにより、パケットはデータパス全体を通じて識別され、セキュリティおよびその他のポリシー基準が適用されます。タグにより、スイッチやファイアウォールなどの中継ネットワークは分類に基づいてアクセス コントロール ポリシーを適用することができます。Cisco TrustSec の IPsec インライン タギングの GET VPN サポート機能では、GET VPN インライン タギングを使用してプライベート WAN 経由で SGT 情報を伝送します。 次のコマンドが導入または変更されました。**show crypto gdoi**、**show crypto ipsec sa**、**tag cts sgt**
GET VPN 時間ベースのアンチリプレイ	Cisco IOS XE Release 2.3	時間ベースのアンチリプレイのサポートが Cisco VSA に追加されました。

機能名	リリース	機能情報
GET VPN のトラブルシューティング	Cisco IOS XE Release 3.8S	この機能では、エラー状態のログとそのトレースバック、および条件付きデバッグを保存（これはキー サーバから個々のグループ メンバーをデバッグする機能を提供します）するために、デバッグ レベル（これによりデバッグ メッセージを機能ごとに有効にできます）、イベント ロギング、トレース終了の機能の向上を提供します。条件付きデバッグ機能は、GM またはそのほかの連携キー サーバに基づいてフィルタリングできるように、キー サーバの条件付きデバッグを実行する能力を提供します。イベント ロギング機能は、イベントの最後のセットを記録する機能を提供します。 次のコマンドが導入または変更されました。**clear crypto gdoi**、**debug crypto condition unmatched**、**debug crypto gdoi**、**debug crypto gdoi condition**、**monitor event-trace gdoi**、**show crypto gdoi**、および **show monitor event-trace gdoi**。
Group Encrypted Transport VPN キー サーバ	Cisco IOS XE Release 3.6S	キー サーバとして Cisco IOS XE を実行するデバイスを設定するためのサポートが追加されました。 この機能は、Cisco IOS XE リリース 3.6S で Cisco ASR 1000 シリーズ アグリゲーション サービス ルータに導入されました。 Cisco IOS XE リリース 3.13S では、シスコ クラウド サービス ルータ（CSR）1000V シリーズのサポートが追加されました。
GET VPN の VSA サポート	Cisco IOS XE Release 2.3	Cisco VSA（高性能暗号化エンジン）サポートが、GDOI および GET VPN に対して追加されました。

用語集

DOI：Domain of Interpretation（ドメイン オブ インタープリテーション）。Internet Security Association Key Management Protocol（ISAKMP）の場合、キー管理メッセージが送信されるコンテキスト内に記述されるセキュリティ アソシエーション（SA）のペイロード内の値です（IPsec または グループ ドメイン オブ インタープリテーション）。

GDOI：Group Domain of Interpretation（グループ ドメイン オブ インタープリテーション）。ISAKMP の場合、相互に信頼し合うシステムのグループのキーを配信および管理する手段です。

group member：グループに登録されるデバイス（Cisco IOS ルータ）。他のグループメンバーと通信するためにキーサーバーによって制御されます。

group security association：グループ内のすべてのグループメンバーによって共有される SA です。

IPsec：IP security（IP セキュリティ）。一連の RFC（IETF RFC 2401 を参照）で定義されている IP パケット用データ暗号化プロトコル。

ISAKMP：Internet Security Association and Key Management Protocol。暗号キー管理プロトコルのためのフレームワークを提供するプロトコルです。

KEK：Key Encryption Key（キー暗号化キー）。キー サーバとグループ メンバー間のキー再生成を保護するために使用されるキーです。

key server：グループメンバーに対してキーおよびポリシーを配信するデバイス（Cisco IOS ルータ）。

MTU：Maximum Transmission Unit（最大伝送単位）。通信プロトコルの特定のレイヤによって宛先に渡すことが可能な最大パケットまたはフレーム サイズ（バイト単位）です。

SA：Security Association（セキュリティ アソシエーション）。グループ内のすべてのグループメンバーによって共有される SA です。

Simple Network Management Protocol (SNMP)：SNMP エージェントからの管理対象デバイスの外部モニタリングを可能にする、相互運用可能な標準ベースのプロトコルです。

TEK：Traffic Encryption Key（トラフィック暗号化キー）。グループ メンバー間のキー再生成を保護するために使用されるキーです。

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。