



Group Encrypted Transport (GET) VPN

Cisco Group Encrypted Transport Virtual Private Network (GET VPN; Group Encrypted Transport バーチャルプライベートネットワーク) は、IP やマルチプロトコルラベルスイッチング (MPLS) を含むさまざまな WAN 環境で使用できる、完全メッシュ VPN テクノロジーです。GET VPN は、プライベート WAN 上で、Cisco IOS デバイスから発信される、または Cisco IOS デバイスを通過する IP マルチキャストグループトラフィックまたはユニキャストトラフィックを保護するために必要な機能のセットで構成されています。GET VPN では、キー管理プロトコルである Group Domain of Interpretation (GDOI) と IP Security (IPsec; IP セキュリティ) 暗号化が組み合わせて使用され、IP マルチキャストまたはユニキャストトラフィックを保護するための効率的な方法がユーザに対して提供されます。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。

- [Group Encrypted Transport \(GET\) VPN について \(1 ページ\)](#)
- [GET VPN 登録プロセスについて \(5 ページ\)](#)
- [GET VPN セキュリティ ポリシーおよびセキュリティアソシエーションについて \(13 ページ\)](#)
- [GET VPN の設定 \(16 ページ\)](#)
- [RSA キーの生成と同期 \(18 ページ\)](#)
- [GET VPN の IKE プロポーザルの設定 \(20 ページ\)](#)
- [GET VPN のグローバル設定 \(22 ページ\)](#)
- [GET VPN キー サーバの設定 \(24 ページ\)](#)
- [GET VPN グループメンバーの設定 \(26 ページ\)](#)
- [パッシブモードを使用した GET VPN への移行 \(30 ページ\)](#)
- [GET VPN 設定のトラブルシューティング \(33 ページ\)](#)

Group Encrypted Transport (GET) VPN について

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。現在ネットワークセキュリティのリスクが増加し、規制への準拠が重要となりつつありますが、WAN 暗号化テクノロジーである Group Encrypted Transport VPN (GET VPN) を使用すると、ネットワーク インテリジェンスとデータ プライバシーのいずれかを犠牲にする必要がなくなります。

GET では、トンネルなしの VPN が提供されるため、IPsec トンネルは必要ありません。ポイントツーポイントトンネルが不要になったことにより、メッシュ構造のネットワークのスケラビリティが高まり、音声および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が維持されます。GET は、信頼グループの概念に基づき、ポイントツーポイント IPsec トンネルおよびそれに関連するオーバーレイルーティングが不要な、標準規格に準拠したセキュリティモデルです。信頼グループメンバーは、グループ SA と呼ばれる共通の Security Association (SA; セキュリティ アソシエーション) を共有します。これにより、グループメンバーは、他の任意のグループメンバーが暗号化したトラフィックを復号化できます。ポイントツーポイントトンネルではなく信頼グループを使用することによって、完全メッシュネットワークのスケラビリティが高まり、音声および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) が維持されます。

GET ベースのネットワークは、IP やマルチプロトコル ラベル スイッチング (MPLS) 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。

既存の IKE、IPsec、およびマルチキャストテクノロジーを利用できることに加えて、GET VPN トポロジには、次のような主要な要素および機能が備えられています。

- **グループメンバー**：VPN 内で実際のトラフィックを交換するルータは、グループメンバーと呼ばれます。グループメンバーによって、トラフィックに対して暗号化サービスが提供されます。暗号化ポリシーは、キー サーバに集中的に定義されて、登録時にグループメンバーにダウンロードされます。グループメンバーは、このようにダウンロードされたポリシーに基づいて、トラフィックで暗号化または復号化が必要であるかどうか、および使用するキーを決定します。

グループメンバーは、主にキーサーバから暗号化ポリシーを取得しますが、グループメンバーにローカル サービス ポリシー ACL を設定して、ローカル要件に基づいて特定のトラフィックを暗号化から除外することができます。詳細については、[GET VPN セキュリティ ポリシーおよびセキュリティ アソシエーションについて \(13 ページ\)](#) を参照してください。



(注) デバイスは、複数のグループのグループメンバーとなることができます。

- **キーサーバ**：キーサーバとして動作するルータは、トポロジへのゲートキーパーとなります。グループメンバーが VPN のアクティブなメンバーとなるには、まずキーサーバに

正常に登録される必要があります。キー サーバは共有サービス ポリシーを管理し、キーを生成して、グループ メンバーに対してキーを送信します。キー サーバ自体はグループ メンバーとなることができませんが、1つのキーサーバが複数のトポロジのキーサーバとすることができます。詳細については、[GET VPN 登録プロセスについて \(5 ページ\)](#)を参照してください。

- **Group Domain of Interpretation (GDOI)** グループ キー管理プロトコルを使用して、デバイスのグループに対して暗号キーおよびポリシーのセットが提供されます。GET VPN ネットワークでは、GDOIを使用して、安全に通信する必要がある企業 VPN ゲートウェイ (グループ メンバー) のグループに対して共通の IPsec キーが配布されます。キーサーバとして指定されたデバイスは、「キーの再生成」と呼ばれるプロセスを使用して、定期的にキーをリフレッシュし、グループメンバーに最新のキーを送信します。

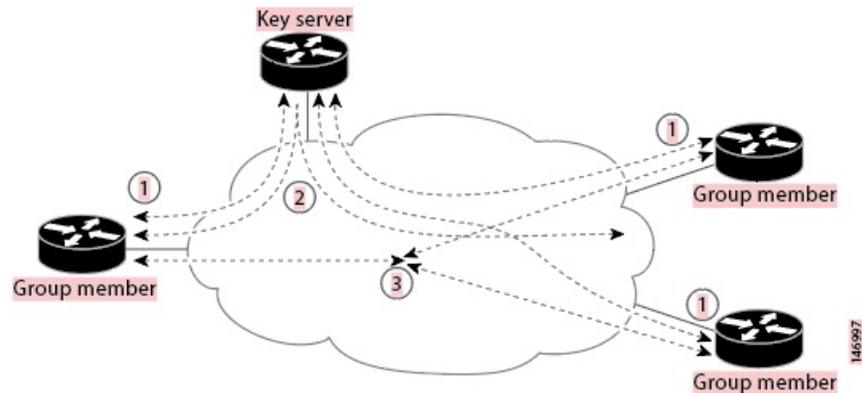
GDOI プロトコルでは、フェーズ 1 Internet Key Exchange (IKE; インターネット キー交換) SA が使用されます。参加するすべての VPN ゲートウェイは、キーを提供するデバイスに対して IKE を使用して自身を認証します。初期認証では、Pre-Shared Key (PSK; 事前共有キー) や Public Key Infrastructure (PKI; 公開キー インフラストラクチャ) などのすべての IKE 認証方式がサポートされています。IKE SA を使用して VPN ゲートウェイが認証され、適切なセキュリティ キーが提供されたあと、IKE SA は期限切れとなります。これ以降は、GDOI を使用して、よりスケーラブルで効率的な方法でグループメンバーが更新されます。GDOI の詳細については、RFC 3547 を参照してください。

- **アドレスの維持**：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。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実体化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「ブラックホール」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)。

次の図に、GET VPN トポロジの一般的な動作を示します。

図 1:一般的な GET VPN の動作



1. グループメンバーは、Group Domain of Interpretation (GDOI) プロトコルを使用して、キーサーバに登録します。キーサーバは、グループメンバーを認証および認可して、IP マルチキャストおよびユニキャストパケットの暗号化と復号化に必要な IPsec ポリシーとキーをメンバーにダウンロードします。登録プロセスでは、ユニキャストまたはマルチキャスト通信を使用できます。
2. グループメンバーは、IPsec を使用して暗号化された IP パケットを交換します。グループメンバーだけが VPN のアクティブな要素となります。
3. 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。キーの再生成メッセージには、古い IPsec Security Association (SA; セキュリティアソシエーション) が期限切れとなった場合に使用する新しい IPsec ポリシーとキーが含まれています。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。

Security Manager を使用して GET VPN をプロビジョニングする場合には、次の点に注意します。

- GET VPN 対応 VRF はサポートされていません。
- Security Manager においてトンネル保護なしで DMVPN を定義する方法がないため、DMVPN と GET を併用することはできません。
- グループ メンバーを手動で設定してマルチキャスト グループに参加させること (ip igmp join-group) はできません。Security Manager では、静的な Source-Specific Multicast (SSM) マッピングだけがプロビジョニングされます。

関連項目

- [GET VPN 登録プロセスについて \(5 ページ\)](#)
- [GET VPN セキュリティ ポリシーおよびセキュリティ アソシエーションについて \(13 ページ\)](#)
- [GET VPN の設定 \(16 ページ\)](#)

GET VPN 登録プロセスについて

GETVPN では、VPN トポロジはグループメンバーによって構成されます。VPN 内のトラフィックは、グループメンバー間のトラフィックです。デバイスがグループメンバーとなるには、デバイスはキーサーバに正常に登録される必要があります。キーサーバでは、Security Association (SA; セキュリティ アソシエーション) ポリシーが保持され、グループ用のキーが作成および保持されます。グループメンバーが登録されると、キーサーバはグループメンバーにポリシーとキーをダウンロードします。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。

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。グループ ID が有効な場合、キーサーバはグループメンバーに対してセキュリティ アソシエーション ポリシーを送信します。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。

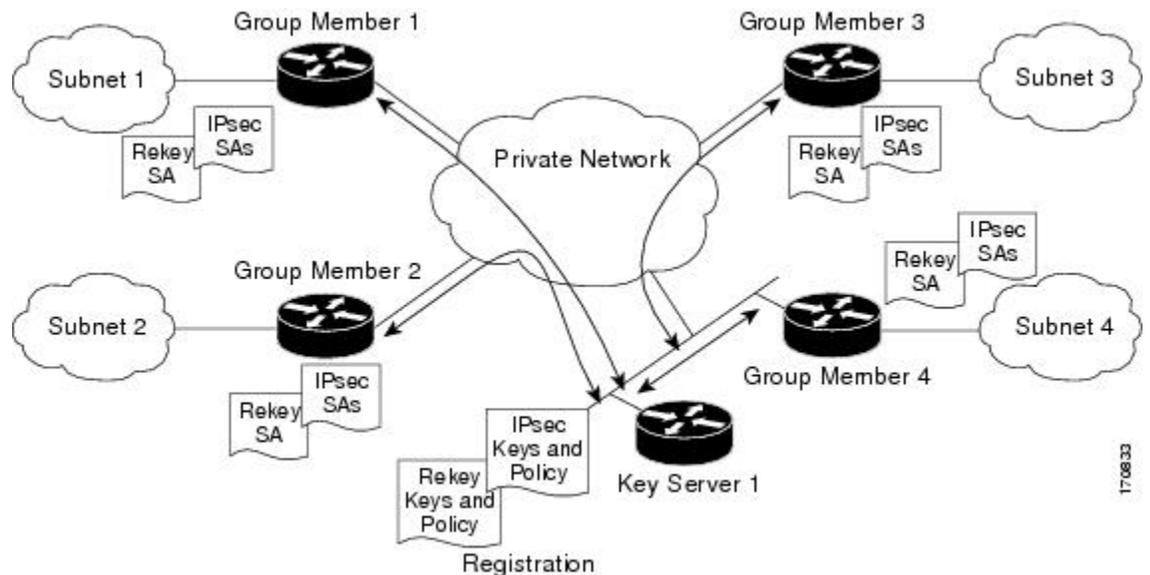
キーサーバおよびグループメンバー間の通信は暗号化され、Traffic Encryption Key (TEK; トラフィック暗号キー) および Key Encryption Key (KEK; キー暗号キー) という2種類のキーを使用して保護されます。TEK は、キーサーバからすべてのグループメンバーにダウンロードされます。ダウンロードされた TEK は、グループメンバー間で安全に通信するためにすべてのグループメンバーで使用されます。このキーは、実質的には、すべてのグループメンバーによって共有されるグループキーとなります。グループポリシーおよび IPsec SA は、グループメンバーへの定期的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

シユされます。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。

キーサーバは、近々 IPsec SA の期限が切れる場合や、キーサーバでセキュリティポリシーが変更された場合に、キーの再生成メッセージを送信します。KEK タイマーの期限が切れた場合もキーの再生成が実行されます（キーサーバはKEK キーの再生成を送信します）。キーの再生成メッセージは、パケット損失が発生した場合に備えて定期的に再送信される場合もあります。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。キーの再生成メカニズムがユニキャストである場合、受信者は確認応答メッセージを送信します。

キーサーバは、GDOI グループ用のグループポリシーおよび IPsec Security Association (SA; セキュリティアソシエーション) を生成します。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。グループメンバーにローカルセキュリティポリシーが設定され、ダウンロードされたポリシーとマージして使用されることがあります。詳細については、[GET VPN セキュリティポリシーおよびセキュリティアソシエーションについて \(13 ページ\)](#) を参照してください。

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 アドレスに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。



GET VPN トポロジを設定する場合、次の登録関連機能を設定できます。

- グループ登録およびキーの再生成にユニキャストまたはマルチキャストのいずれを使用するかを決定します。詳細については、[キーの再生成転送メカニズムの選択 \(7 ページ\)](#) を参照してください。



(注) マルチキャストを使用する場合は、キー サーバおよびグループ メンバーで手動でマルチキャストをイネーブルにする必要があります。マルチキャスト コマンドは、Security Manager によってプロビジョニングされません。

- 複数のキー サーバを設定して、冗長性を確保し、ロード バランシングを行うかどうかを決定します。詳細については、[協調キー サーバを使用した冗長性の設定 \(9 ページ\)](#) を参照してください。
- キー サーバに正常に登録される前にグループ メンバーのトラフィックを保護するためにグループ メンバーにフェールクローズ モードを設定するかどうかを決定します。詳細については、[登録の失敗時にも保護するためのフェールクローズの設定 \(10 ページ\)](#) を参照してください。
- グループ メンバーがグループに参加するときに認可が必要かどうかを決定します。証明書認可 (Public Key Infrastructure ポリシーも設定する必要があります) または事前共有キーを使用できます。キーサーバが複数のグループに対応する場合は、認可を設定する必要があります。設定オプションの詳細については、[GET VPN グループ暗号化の定義の \[Authorization Type\] 設定](#) を参照してください。

関連項目

- [RSA キーの生成と同期 \(18 ページ\)](#)
- [GET VPN の設定 \(16 ページ\)](#)

キーの再生成転送メカニズムの選択

Group Encryption ポリシーでキーの再生成設定を設定する場合 ([GET VPN グループ暗号化の定義](#)を参照)、キーの再生成転送メカニズムとしてマルチキャストまたはユニキャストのいずれを使用するかを選択する必要があります。キー サーバは、グループ メンバーまたは他のキー サーバに対して新しいキーおよび IPsec Security Association (SA; セキュリティ アソシエーション) を送信する場合には常にこの方法を使用します。それぞれの方法には利点と欠点があります。

マルチキャストが標準的な選択肢です。マルチキャストを使用した場合、キー サーバは、各キーの再生成メッセージの 1 つのコピーを、マルチキャスト グループ アドレスを使用してすべてのグループ メンバーに一度に送信します。そのため、キーの再生成で遅延は発生せず、グループ メンバーは更新されたセキュリティ ポリシーをほぼ同時にインストールできます (通常のネットワーク遅延を除く)。ただし、一部のネットワークでは、マルチキャスト機能を使用すると余分のコストが発生したり、マルチキャスト機能が許可されていない場合があります。

す。マルチキャストを設定する場合は、GET VPN トポロジで使用されるマルチキャストアドレスを指定する必要があります。

マルチキャストが使用できない場合や、マルチキャストの使用が望ましくない場合は、**ユニキャスト**を使用できます。ユニキャストを使用した場合、キー サーバは、個別のグループメンバーに対してキーの再生成および IPsec SA を送信します。各グループメンバーはメッセージを受信したことを示す確認応答を送信します。ユニキャストでは、メッセージを直接送信したり、確認応答を受信したりする必要があるため、キー サーバはサブネットごとに順番にグループメンバーに対してユニキャストメッセージを送信します（ただし、グループメンバー数が30未満などの比較的小規模なVPNでは、すべてのグループメンバーに同時にメッセージが送信されることがあります）。

したがって、マルチキャストとユニキャストを比較した場合の利点は次のようになります。

- マルチキャストでは、キー サーバはグループメンバーがメッセージを受信したかどうかを把握できません。一方、ユニキャストでは、確認応答が送信されます。ユニキャストでは、キー サーバが確認応答を受信できない場合、メッセージが再送信されます。
- マルチキャストはユニキャストよりも高速です。特に、数百のグループメンバーがあるような大規模なトポロジでは高速になります。マルチキャストのキーの再生成では、グループ内のグループメンバー数が1つの場合でも数千の場合でも、CPUのオーバーヘッドは変わらず、いずれの場合も低くなります。
- ユニキャストでは、グループメンバーが連続して確認応答を送信しないと、キー サーバはグループメンバーが存在しないと判断して、キーの再生成メッセージの送信を停止します。そのため、キー サーバには常にアクティブなグループメンバーのリストが保持されています。応答しなくなったグループメンバーがGET VPN トポロジに再度参加するためには、もう一度登録が必要です。マルチキャストでは確認応答が使用されないため、グループメンバーが応答しなくなってもキー サーバでは把握できず、アクティブなグループメンバーのリストも保持されません。



ヒント マルチキャストを使用するには、キー サーバおよびグループメンバーでマルチキャストをイネーブルにする必要があります。これらのコマンドは、**Security Manager**によってプロビジョニングされません。**Security Manager**では、マルチキャストによるキーの再生成だけがイネーブルにされ、ルータでのマルチキャストトラフィックの送受信はイネーブルにされません。そのため、デバイスで手動でマルチキャストをイネーブルにするか、または**FlexConfig**ポリシーを使用してコマンドをプロビジョニングする必要があります（[FlexConfig ポリシー オブジェクトの作成](#)を参照）。

すべてのキー サーバでマルチキャストがサポートされている場合は、単一のGET VPN トポロジ内でマルチキャストとユニキャストの混在させることができます。どちらの転送メカニズムを使用するかを決定する場合には、次の推奨事項を考慮してください。

- すべてのキー サーバ、すべてのグループメンバー、およびネットワークでマルチキャストがサポートされている場合は、マルチキャストを使用します。

- すべてのキー サーバとほとんどのグループ メンバーでマルチキャストがサポートされており、少数のグループメンバーでマルチキャストがサポートされていない場合は、マルチキャストを使用します。マルチキャストをサポートしないグループメンバーは、キーの再生成およびIPsec SA 更新を受信しません。ただし、これらの項目のライフタイム設定の期限が切れる前に、ユニキャスト グループ メンバーはキー サーバに再登録し、新しいキー と IPsec SA を取得します。
- どのグループメンバーでもマルチキャストがサポートされていない場合や、少数のグループメンバーだけがマルチキャストをサポートしている場合は、ユニキャストを使用します。この場合、グループ メンバーは、キー サーバからキーの再生成と IPsec SA 更新を受信するため、キー サーバに再登録する必要はありません。

関連項目

- [GET VPN 登録プロセスについて \(5 ページ\)](#)
- [RSA キーの生成と同期 \(18 ページ\)](#)
- [GET VPN の設定 \(16 ページ\)](#)

協調キー サーバを使用した冗長性の設定

GET VPN ネットワークでは、キーサーバがコントロールプレーンとなるため、キーサーバがこのネットワークにおける最も重要なエンティティとなります。したがって、キーサーバが1台しかない場合は、このキーサーバがGET VPN ネットワーク全体のシングルポイント障害となります。キーサーバにおいて冗長性を考慮することは重要であるため、GET VPN では、Cooperative (COOP; 協調) キーサーバと呼ばれる複数のキーサーバを用意して、キーサーバのうちの1つで障害が発生したり、到達不能になったりした場合に、シームレスな障害回復を行うことができます。

すべてのCOOPキーサーバのリストから使用可能な任意のキーサーバに登録するようにグループメンバーを設定できます。グループメンバーの設定によって、登録の順序が決まります ([GET VPN グループメンバーの設定 \(26 ページ\)](#) および [\[Edit Group Member\] ダイアログボックス \(27 ページ\)](#) を参照)。最初に定義されたキーサーバに対して接続が試みられ、その後、定義された順番でキーサーバへの接続が試みられます。すべての使用可能なCOOPキーサーバにグループメンバーの登録を分散して、1つのキーサーバにおけるIKE処理の負荷を低減することを推奨します。キーの再生成メッセージを送信するのは、プライマリキーサーバだけです。

COOPキーサーバが起動すると、すべてのキーサーバはセカンダリとしての役割を担い、選定プロセスが開始されます。通常は、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して選定されます。他のキーサーバは、セカンダリのままとなります。プライマリキーサーバは、グループポリシーを作成してすべてのグループメンバーに配布する処理、およびCOOPキーサーバを定期的に同期する処理を担当します。

協調キーサーバは、(プライマリからセカンダリへの) 一方向の通知メッセージを交換します。セカンダリキーサーバが、一定期間プライマリキーサーバから通知を受信しない場合、

セカンダリ キー サーバはプライマリ キー サーバへの接続を試みて、更新情報を要求します。プライマリ キー サーバが応答しない場合（セカンダリ キー サーバがプライマリ キー サーバから情報を受信しない場合）は、COOP キー サーバの再選定がトリガーされて、新しいプライマリ キー サーバが選定されます。

最大 8 台のキー サーバを COOP キー サーバとして定義できますが、5 台以上の COOP キー サーバが必要となることはほとんどありません。キーの再生成情報は単一のプライマリ キー サーバによって生成および配布されるため、3 台以上のキーサーバを展開することの利点は、ネットワークの障害が発生した場合の登録の負荷に対応でき、同時に再登録も実行できることにあります。Public Key Infrastructure (PKI; 公開キー インフラストラクチャ) を使用する IKE ネゴシエーションは、Pre-Shared Key (PSK; 事前共有キー) を使用する IKE ネゴシエーションと比較してはるかに多くの CPU パワーを必要とするため、このことは PKI によるグループメンバー認可を使用する場合に特に重要となります。

ヒント

- RSA キーはすべての協調キー サーバで同じである必要があります。RSA キーの同期の詳細については、[RSA キーの生成と同期 \(18 ページ\)](#) を参照してください。
- キー サーバ間での定期的な ISAKMP キープアライブをイネーブルにして、プライマリ キー サーバで他のセカンダリ キー サーバの状態を追跡および表示できるようにすることを推奨します。グループメンバーとキーサーバとの間の IKE キープアライブは必要ではなく、またサポートもされていません。キープアライブの設定の詳細については、[GET VPN のグローバル設定 \(22 ページ\)](#) を参照してください。
- COOP プロトコルは、GDOI グループごとに設定されます。複数の GDOI グループが設定されたキーサーバでは、異なるキーサーバとの固有の COOP 関係を複数維持できます。

登録の失敗時にも保護するためのフェールクローズの設定

グループメンバーは、GET VPN のメンバーとなるためにはキーサーバに登録する必要があります。グループメンバーがキーサーバに正常に登録されるまでは、グループメンバーの GET VPN インターフェイス経由で送受信されるトラフィックは暗号化されません。クリアテキストでの伝送が行われる期間は、登録に成功すると短い期間で済みますが、何らかの理由でグループメンバーが登録に失敗すると、長くなる可能性があります。

このデフォルトの動作はフェールオープンと呼ばれています。いかなる場合でもトラフィックがクリアテキストで送信されることをセキュリティ標準違反であると見なす場合は、フェールクローズモードを設定して、登録前（または登録中）のトラフィックを保護できます。フェールクローズモードを使用すると、インターフェイスを経由するトラフィックのうち、フェールクローズ ACL で明示的に特定したトラフィック以外のすべてのトラフィックがドロップされます。フェールクローズモードでは、グループメンバーがキーサーバに正常に登録されて、必要なキー、セキュリティポリシー、およびセキュリティアソシエーションがダウンロードされるまでは、インターフェイスが実質的にシャットダウンされます。フェールクローズモードを使用するには、Cisco IOS ソフトウェア Release 12.4(22)T または 15.0 以上が必要です。また、フェールクローズモードは、サポートされているすべての ASR に設定できます（[各 IPsec テクノロジーでサポートされるデバイスについて](#)を参照）。

フェールクローズモードは、最初の登録時にだけ使用されます。グループメンバーがすでに正常に登録されている場合、そのグループメンバーは、その後登録に失敗しても、キーサーバからダウンロードされたポリシーを保持し続けます。ただし、グループメンバーに対して **clear crypto gdoi** コマンドを使用した場合は、そのあとに行われる登録の試行が1回目の登録であると見なされて、フェールクローズモードが適用されます。

GET VPN グループメンバーの設定 (26 ページ) で説明するように、フェールクローズモードは、個別のグループメンバーに対して設定します。したがって、すべてのグループメンバーでモードをイネーブルにせずに、選択したグループメンバーに対してモードをイネーブルにできます。ユーザ（および Security Manager）がデバイスからロックアウトされ、登録が成功するまで設定の更新やメンテナンスができなくなる事態を回避するためには、フェールクローズ ACL を指定する必要があります。

フェールクローズ ACL は拡張 ACL ポリシー オブジェクトであり、デバイスにクリプトマップの一部として設定されます。ルールは、グループメンバーの観点から設定します。次のヒントを参照して、適切なフェールクローズ ACL の作成に役立ててください。

- **permit** ステートメントと **deny** ステートメントの両方を設定できます。フェールクローズ ACL では、「**permit**」は「このトラフィックを送信しない」を意味し、「**deny**」は「このトラフィックをクリアテキストで送信する」ことを意味します。この動作は、ステートメントが次の意味を持つ通常のクリプトマップ ACL の動作とは異なります。
 - **Permit** : このトラフィックを暗号化する」ことを意味します。グループメンバーは、登録前にはトラフィックを暗号化するために必要な IPsec セキュリティ アソシエーションを持っていないため、結果としてトラフィックはドロップされます。
 - **deny** : 「このトラフィックを暗号化しない」ことを意味します。一般的なクリプトマップ ACL では、**deny** ステートメントを使用すると、条件に一致したパケットは、デバイスに設定されている次のクリプトマップ ACL と比較されます（設定されている場合）。ただし、トラフィックがフェールクローズ ACL 内の **deny** ステートメントに一致した場合、すべてのクリプトマップ ACL 処理が終了し、クリアテキストでのトラフィックの送信が許可されます。

フェールクローズモードで **deny** がこのように動作するのは、フェールクローズでは、クリプトマップ ACL のリストの最後に暗黙的に ACL ステートメントが追加されているためです。そのステートメントは **permit ip any any** であり、すべてのトラフィックに一致します。登録がまだ完了していないため IPsec セキュリティ アソシエーションがなく、どの条件にも一致しなかったトラフィックは、暗号化する方法が存在せずに、ドロップされます。

この最後の **permit ip any any** ステートメントによって、フェールクローズ ACL では **deny** ステートメントだけを設定することが可能となります。

- フェールクローズ ACL は、オプションのグループメンバーセキュリティポリシー ACL のあとに続いて処理されます。ただし、グループメンバーセキュリティポリシー ACL 内のすべてのステートメントは **deny** ステートメントである必要があります。これにより、一致するトラフィックがクリアテキストで送信される必要があることが指定されます。セキュリティポリシーは、通常のクリプトマップルールに従って処理されるため、**deny** ステートメントに一致するトラフィックは、そのあとでフェールクローズ ACL と比較されます。フェールクローズ ACL 内に一致する **deny** ステートメントがない場合、トラフィッ

クは、フェールクロースの暗黙的な最後の `permit ip any any` ステートメントによってドロップされます。

したがって、グループメンバーセキュリティポリシー ACL を使用し、グループメンバーの登録ステータスにかかわらず特定のトラフィックをクリアテキストで送信する場合、フェールクロース ACL には、少なくともセキュリティポリシー ACL に含まれているものと同じステートメントがすべて含まれている必要があります。両方の ACL に同じ ACL オブジェクトを使用することもできます。

グループメンバーセキュリティポリシーの詳細については、[GET VPN セキュリティポリシーおよびセキュリティアソシエーションについて \(13 ページ\)](#) を参照してください。

- フェールクロース ACL は、最後のクリプトマップ ACL として挿入されます。したがって、クリプトマップを使用する他の機能を GET VPN インターフェイスに設定する場合は、それらの他の ACL 内の `deny` ステートメントで特定されるすべてのトラフィックも、フェールクロース ACL および暗黙的な最後の `permit ip any any` ステートメントによってトラップ（およびドロップ）されます。そのため、GET VPN にフェールクロースモードを設定すると、そのインターフェイスに設定する GET VPN 以外のサービスにも影響を与えることがあります。
- 登録に成功すると、フェールクロース ACL および暗黙的な最後の `permit ip any any` ステートメントはクリプトマップから削除されます。これらのポリシーは、永続的ではありません。
- フェールクロース ACL ポリシー オブジェクトでは、次のルールを含めることを検討する必要があります。これらのルールは、グループメンバーの観点からのものであることに注意してください。
 - SSH および SSL (HTTPS) トラフィック：ユーザおよび Security Manager は、デバイスにアクセスして、デバイスを設定できる必要があります。デバイスをロックすることがないように、SSH および SSL 用の `deny` ステートメントを含めます。SSH 用には、`deny tcp any eq 22 <host or network address>` ステートメントを含めます。SSL 用には、`deny tcp any eq 443 <host or network address>` ステートメントを含めます。ホストのアドレスを指定する場合は、Security Manager サーバもホストの 1 つとして含めます。
 - ルーティングトラフィック：ルーティングをイネーブルにするには、ルーティングプロセスのトラフィックを許可します。たとえば、OSPF を使用している場合は、`deny ospf any any` を含めます。
 - GDOI トラフィック：デバイスでは、フェールクロース ACL の内容にかかわらず GDOI 登録メッセージが検索されるため、正常に登録するためには明示的にこれらのメッセージを許可する必要はありません。ただし、グループメンバー (1) がキーサーバと他のグループメンバー (2) との間のパス上に位置している場合、グループメンバー (1) が登録に失敗すると、グループメンバー (2) がブロックされて、正常に登録できなくなります。グループメンバー (2) が正常に登録されるためには、グループメンバー (1) に、GDOI トラフィックの通過を許可するフェールクロース ACL を設定する必要があります。したがって、フェールクロース ACL に `deny udp any eq 848 any eq 848` を含めて、GDOI トラフィックを許可することを推奨します。

関連項目

- [GET VPN の設定 \(16 ページ\)](#)
- [アクセス コントロール リスト オブジェクトの作成](#)
- [拡張アクセス コントロール リスト オブジェクトの作成](#)

GET VPN セキュリティ ポリシーおよびセキュリティ アソシエーションについて

GET VPN では、クリプト マップ アクセス コントロール リスト (ACL) を使用して、VPN で暗号化される必要があるトラフィックが特定されます。これらの ACL では、暗号化する代わりにクリア テキストとして送信する必要があるトラフィック (実質的に VPN 外部となるトラフィック) も指定されます。これらの ACL の集合によって、VPN のセキュリティ ポリシーが定義されます。

GET VPN では、多階層のセキュリティ ポリシーが提供されます。VPN 全体の一般的なポリシーはキー サーバに定義しますが、グループ メンバーに個別のセキュリティ ポリシーを定義して、ローカルのバリエーションを用意することもできます。グループメンバーセキュリティ ポリシーは、キーサーバから受信したポリシーよりも常に優先されます。グループメンバーがキーサーバに登録されると、グループメンバーはキーサーバのセキュリティポリシーとセキュリティアソシエーションをダウンロードします。次に、グループメンバーは、1 番めにグループメンバーの ACL、2 番めにキーサーバの 1 つめの ACL、3 番め以降も同様にキーサーバのすべての ACL をキーサーバに定義されている順序で連結することによって、新しい単一のセキュリティポリシークリプトマップ ACL を作成します。これらのマージされた ACL は単一の ACL として処理されることを理解することが重要です。これらは別個の ACL として検索されるわけではありません。したがって、トラフィックがグループメンバーの ACL の deny ステートメントに一致した場合、そのトラフィックは、キーサーバからダウンロードされたものの ACL ルールに対してもテストされることはありません。



ヒント グループメンバーが GET VPN から離脱すると、キーサーバからダウンロードされた ACL は削除されますが、グループメンバーセキュリティポリシー ACL は維持されて、デバイスに設定されたままとなります。

GET VPN セキュリティ ポリシー ACL (およびクリプト マップ ACL 全般) では、permit キーワードと deny キーワードには特別な意味があります。

- **Permit** : このトラフィックを暗号化する」ことを意味します。permit エントリは、キーサーバの [グループ暗号化ポリシー (Group Encryption Policy)] で定義されるセキュリティポリシー ACL にだけ設定できます。これは、暗号化されるトラフィックには、トラフィックの暗号化に使用されるトランスフォームセット、アンチリプレイ設定、IPsec ライフタイム設定を含む、完全な IPsec セキュリティアソシエーションが存在する必要がある

るためです。パケットが **permit** エントリに一致するが、そのパケットに IPsec SA がない場合、そのパケットはドロップされます。

通常、**permit** ルールは対称的である必要があります。つまり、送信元アドレスと宛先アドレスは同じである必要があります。異なる送信元アドレスと宛先アドレスを指定する必要がある場合は、2つのルールを作成する必要があります。2つめのルールは、1つめのルールの送信元アドレスと宛先アドレスを入れ替えた、対称的なルールとする必要があります。

- **deny** : 「このトラフィックを暗号化しない」ことを意味します。実際には、通常、**deny** ステートメントに一致するトラフィックがクリアテキストで送信されることを意味します。ただし、クリプトマップを使用する他の機能を設定した場合、「拒否された」トラフィックは後続の（プライオリティの低い）クリプトマップ ACL と比較されて、一致するエントリがあるかどうかを確認されます。**deny** ルールに対しては、IPsec Security Association (SA; セキュリティ アソシエーション) は生成されません。

次に、設定できるセキュリティ ポリシーをプライオリティ順にまとめます。

- **グループ メンバー セキュリティ ポリシー** : グループメンバーの設定時に ([GET VPN グループ メンバーの設定 \(26 ページ\)](#)) を参照)、ローカル グループ メンバー セキュリティ ポリシーを定義する ACL ポリシーオブジェクトをオプションで選択できます。

このグループメンバー ACL ポリシーオブジェクトには、**deny** ステートメントだけを設定できます。この ACL を使用して、暗号化から除外し、クリアテキストで送信するトラフィックを特定できます。たとえば、グループ内の一部のグループメンバーが通常とは異なるルーティングプロトコルを実行している場合、キーサーバーレベルでグローバルにポリシーを定義する代わりに、これらのグループメンバーのセキュリティポリシー ACL にローカルエントリを設定して、ルーティングプロトコルトラフィックの暗号化を回避できます。

- **キーサーバー セキュリティ ポリシーおよびセキュリティ アソシエーション** : GET VPN に Group Encryption ポリシーを設定する場合 ([GET VPN グループ暗号化の定義](#)を参照)、VPN で暗号化および保護する必要があるトラフィックを特定する ACL を設定します。

キーサーバーのセキュリティポリシーと、トランスフォームセットやその他の設定が組み合わせられて、セキュリティアソシエーションが定義されます。実際には、ACL 内の各ルールに対して2つの IPsec Security Association (SA; セキュリティアソシエーション) が設定され、これらの SA によって、選択されたトラフィックの暗号化方法が定義されます。したがって、すべてのグループメンバーで同じグループ SA が使用されるため、グループメンバー間で SA をネゴシエートする必要がありません。

キーサーバーのポリシーはグループメンバーのポリシーに付加されるため、ポリシーは **permit ip any any** のようなシンプルなものになるかもしれません。つまりグループメンバーポリシーによって除外されていないすべてのトラフィックを暗号化します。

ただし、異なるトランスフォームセットに関連付けられて異なるタイプの暗号化を定義する、いくつかの別個の ACL ポリシーオブジェクトを設定して、より複雑なセキュリティポリシーとセキュリティアソシエーションのセットを作成することもできます。

複数のセキュリティアソシエーションを作成する場合は、順序を指定する必要があります。セキュリティアソシエーションは、指定された順序でグループポリシーに追加されます。追加

された結果単一の ACL が作成されるため、最初の ACL に deny ステートメントを含めると、後続のセキュリティアソシエーションにおける同じトラフィックに対するすべての permit ルールは無視されて、トラフィックは暗号化されずにクリア テキストで送信されます。



- (注) Group Encryption ポリシーに定義されるセキュリティアソシエーションを全体としては、最大 100 の ACL permit エントリを定義できます。各 permit エントリによって、IPsec SA のペアが作成されます。グループ内の IPsec SA の最大数は 200 を超えることができません。対象のトラフィックを可能なかぎり少ない permit エントリにまとめ、送信元アドレスと宛先アドレスが同じである対称的なポリシーを構築することを推奨します。一意の送信元アドレス範囲と宛先アドレス範囲を定義する必要がある通常の IPsec ポリシーとは異なり、送信元アドレス範囲と宛先アドレス範囲が同じである場合に GET VPN は最適化されます。送信元アドレスと宛先アドレスが異なるルールを設定する場合は、(送信元アドレスと宛先アドレスを入れ替えた) 対称的なルールも設定する必要があります。この場合、4 つの SA が使用されます。

これらのセキュリティ ポリシー以外に、グループ メンバーにフェールクローズ モードを設定した場合にトラフィック パターンに影響を与える追加のフェールクローズ ACL もあります。詳細については、[登録の失敗時にも保護するためのフェールクローズの設定 \(10 ページ\)](#) を参照してください。

関連項目

- [GET VPN の設定 \(16 ページ\)](#)
- [アクセス コントロール リスト オブジェクトの作成](#)
- [拡張アクセス コントロール リスト オブジェクトの作成](#)

時間ベースのアンチリプレイについて

アンチリプレイは、IPsec (RFC 2401) などのデータ暗号化プロトコルにおける重要な機能です。アンチリプレイを使用すると、第三者が IPsec 通信やパケットを盗聴して、あとでこれらのパケットをセッションに挿入することを防止できます。時間ベースのアンチリプレイメカニズムは、すでに過去の時点で到着しているパケットの再送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、Synchronous Anti-Replay (SAR; 同期アンチリプレイ) メカニズムを使用して、複数の送信者からのトラフィックに対するアンチリプレイ保護が提供されます。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 サーバによって管理され、キーの再生成メッセージ内の pseudoTimeStamp と呼ばれるタイムスタンプフィールドとしてグループ メンバーに定期的送信されます。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

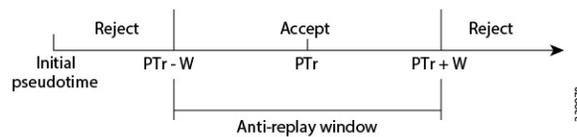
まず、最初は、登録プロセス中に、キー サーバからグループ メンバーに対して、キー サーバの現在の疑似時間の値およびウィンドウサイズが送信されます。時間ベースのリプレイ対応情報、ウィンドウサイズ、キー サーバの疑似時間などの新しい属性は、SA ペイロード (TEK) で送信されます。

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。受信者は、時間ベースのアンチリプレイ ウィンドウを使用して、そのウィンドウ内のタイムスタンプ値を含むパケットを受け入れます。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。

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。

アンチリプレイは、Group Encryption ポリシーのセキュリティ アソシエーション定義に設定します。詳細については、[GET VPN グループ暗号化の定義](#)および[\[Add New Security Association\]/\[Edit Security Association\] ダイアログボックス](#)を参照してください。

図 2: アンチリプレイ ウィンドウ



GET VPN の設定

Group Encrypted Transport (GET) を使用して完全メッシュ VPN を設定するには、[VPN トポロジの作成または編集](#)の説明に従って Create VPN ウィザードを使用します。ウィザードが終了したら、RSA キーを同期するかどうかを尋ねられます。RSA キーの同期は、VPN が正常に動作するために必要です。詳細については、[RSA キーの生成と同期 \(18 ページ\)](#)を参照してください。

キーの再生成転送メカニズムとしてマルチキャストを選択した場合は、すべてのキーサーバおよび必要なグループメンバーにおいてマルチキャストをイネーブルにする必要があります。詳細については、[キーの再生成転送メカニズムの選択 \(7 ページ\)](#) を参照してください。

EditVPN ウィザードを使用すると、GET VPN の名前と説明だけを変更できます。他のポリシーや設定を変更する必要がある場合は、[Site-to-Site Manager] ページで次のようにポリシーを開きます。

- ISAKMP および IPsec 設定の場合は、[GET VPN のグローバル設定 (Global Settings for GET VPN)] を選択します。[GET VPN のグローバル設定 \(22 ページ\)](#) を参照してください。
- IKE プロポーザルポリシーの場合は、[GET VPN のIKEA プロポーザルポリシー (IKE Proposal Policy for GET VPN)] を選択します。[GET VPN の IKE プロポーザルの設定 \(20 ページ\)](#) を参照してください。
- セキュリティ アソシエーション (ACL ルール) および IPsec ポリシーの場合は、[グループ暗号化ポリシー (Group Encryption Policy)] > [セキュリティアソシエーション (Security Associations)] を選択します。[GET VPN グループ暗号化の定義](#) を参照してください。
- 事前共有キーポリシーの場合は、[IKEv1 事前共有キー (IKEv1 Preshared Key)] を選択します。[IKEv1 事前共有キー ポリシーの設定](#) を参照してください。
- 公開キー (PKI) ポリシーの場合は、[公開キーインフラストラクチャ (Public Key Infrastructure)] を選択します。[サイト間 VPN での IKEv1 公開キー インフラストラクチャ ポリシーの設定](#) を参照してください。
- キーの再生成設定の場合は、[グループ暗号化ポリシー (Group Encryption Policy)] > [グループ設定 (Group Settings)] を選択します。[GET VPN グループ暗号化の定義](#) および [RSA キーの生成と同期 \(18 ページ\)](#) を参照してください。
- RSA キーの同期を含むキーサーバの設定の場合は、[キーサーバ (Key Servers)] を選択します。[GET VPN キーサーバの設定 \(24 ページ\)](#) および [RSA キーの生成と同期 \(18 ページ\)](#) を参照してください。
- グループメンバーシップおよびエンドポイント設定の場合は、[グループメンバー (Group Members)] を選択します。[GET VPN グループメンバーの設定 \(26 ページ\)](#) を参照してください。

関連項目

- [Group Encrypted Transport \(GET\) VPN について \(1 ページ\)](#)
- [GET VPN 登録プロセスについて \(5 ページ\)](#)
- [GET VPN セキュリティ ポリシーおよびセキュリティアソシエーションについて \(13 ページ\)](#)
- [GET VPN 設定のトラブルシューティング \(33 ページ\)](#)
- [サイト間 VPN での IKEv1 事前共有キー ポリシーについて](#)

RSA キーの生成と同期

Group Encryption ポリシーで RSA キーラベルを指定する場合 ([GET VPN グループ暗号化の定義](#)を参照)、対応する RSA キー (公開キーと秘密キー) が GET VPN トポロジ内のすべてのキーサーバーに設定されている必要があります。キーは、デバイスに定義した既存のキー、または新しいキー ラベルを指定できます。Security Manager によってキーが生成されて、すべてのキー サーバが同じキーを使用するように同期されます。

Security Manager で RSA キーを生成して同期するには、次の方法を使用できます。

- Create VPN ウィザードを使用して新しい GET VPN を作成する場合は、ウィザードの最後に、キーを同期するかどうかを尋ねられます。[はい (Yes)] をクリックすると、Security Manager によってすぐにキーの同期が実行され、キーがまだ存在していない場合には新しいキーが生成されます。Create VPN ウィザードの使用の詳細については、[VPN トポロジの作成または編集](#)を参照してください。
- 既存の GET VPN では、キーサーバーポリシーで [キーの同期 (Synchronize Keys)] ボタンをクリックできます。キーサーバーを追加する場合や、プライマリ キーサーバーで新しいキーを生成する場合には、必ずこのプロセスを使用します。既存のトポロジにおけるキーサーバーの設定の詳細については、[GET VPN キー サーバの設定 \(24 ページ\)](#) を参照してください。



ヒント 既存の GET VPN トポロジで新しい RSA キーを生成する場合は、Group Encryption ポリシーを更新して新しい未使用の RSA キー ラベルを指定し、Key Servers ポリシーで [Synchronize Keys] ボタンをクリックするのが最も簡単な方法です。キーはどのキーサーバーにも存在しないため、Security Manager によって新しいキーが生成されて、すべてのキーサーバーにインポートされます。その後、各キーサーバーから古いキーを手動で削除できます。

RSA キーは、次のように使用されます。

- キーサーバーは、RSA 秘密キーを使用して、グループメンバーからのキーの再生成メッセージを認証します。
- キーサーバーは、登録時にグループメンバーに対して RSA 公開キーを提供します。
- キーサーバーは、秘密キーを使用して、Key Encryption Key (KEK; キー暗号キー) および Traffic Encryption Key (TEK; トラフィック暗号キー) に署名します。RSA キーがないと、キーサーバーは KEK および TEK を作成できません。
- RSA キーは、協調キーサーバー間のメッセージの署名にも使用されます。

RSA キー同期プロセスを開始すると、[Synchronize Keys] ダイアログボックスが開き、全体的な経過および各キーサーバーにおける結果が表示されます ([停止 (Abort)] ボタンをクリックすると、プロセスをいつでも停止できます)。Security Manager によって次の手順が実行されます。

1. すべてのキーサーバにログインして、VPNに設定されたRSA キー ラベルに対応するRSA キー情報が各サーバから取得されます。
2. いずれかのキーサーバに、必要なラベルを持つキーが存在しているかどうか判断されます。
 - どのキーサーバにも必要なラベルを持つRSA キーがない場合は、Security Manager によってプライマリ キーサーバ（最も高いプライオリティを持つサーバ）にキーが生成されます。
 - 1つ以上のキーサーバにキーがなく、キーがあるすべてのキーサーバのキーが同じものである場合は、Security Manager によって、キーがある任意のサーバの既存のキーが使用されます。
 - 複数のキーサーバにキーがあるが、キーの内容がサーバ間で異なる場合は、Security Manager がキーを上書きしてもよいかどうかを尋ねられます。[はい (Yes)] をクリックすると、Security Manager では、プライマリキーサーバーの既存のキーが使用されます。

[いいえ (No)] をクリックした場合は、Security Manager 外部でキーサーバーにログインして、必要に応じて手動でキーを調整できます。ただし、すべてのキーサーバのRSA キーの内容は同じである必要があります。このプロセスについては、後述の説明を参照してください。

1. キーのエクスポート可能なバージョンが作成されます。
2. キーが、残りの各キーサーバにインポートされます。



ヒント 同期プロセスが成功するためには、デバイスがオンラインかつ到達可能であり、ユーザに展開権限がある必要があります。デバイスへの接続が失敗したり、タイムアウトしたりした場合は、Security Manager サーバからキーサーバに対する ping が成功することを確認します。ライブ デバイスではなくファイルに展開する場合は、後述の説明に従って手動でキーを生成および同期する必要がある場合があります。十分な権限がない場合は、プロセスを開始できないため、他のユーザにプロセスの実行を依頼する必要があります。

RSA キーの手動での生成と同期

Security Manager でキーを生成および同期しない場合、または何らかの理由で Security Manager においてプロセスを完了できない場合には、特権 EXEC（イネーブル）コンフィギュレーション モードで次の手順を使用して手動でキーを生成および同期できます。

1. 次のコマンドを使用して、キーサーバーにキーを生成します。**rekeyrsa** はキーの名前です（任意の名前を指定できます）。キーは、エクスポート可能にする必要があります。

crypto key generate rsa general-keys label rekeyrsa modulus 1024 exportable

1. 次のコマンドを使用して、キーのエクスポート可能なコピーを作成します。**passphrase** は、インポート用にキーを暗号化するために使用される文字列です（任意のパスフレーズを指定できます）。

crypto key export rsa rekeyrsa pem terminal 3des passphrase

このコマンドによって、公開キーと秘密キーが端末に出力されます。これらをクリップボードにコピーして、他のキーサーバへのインポートに使用できます。キーは **----BEGIN/END PUBLIC KEY----** と **----BEGIN/END RSA PRIVATE KEY----** によって区切られています。また、URL にエクスポートすることもできます。コマンドの使用方法の詳細については、Cisco.com の『*Cisco IOS Security Command Reference*』を参照してください。

1. 次のコマンドを使用して、他の各キーサーバにキーをインポートします。

crypto key import rsa rekeyrsa pem exportable terminal passphrase

キーをコピー アンド ペーストする場合は、BEGIN と END の行を含めます。

GET VPN の IKE プロポーザルの設定

[IKE Proposal for GET VPN] ページを使用して、GET VPN トポロジで使用される IKE プロポーザルを定義します。IKE プロポーザルは、キーサーバおよびグループメンバーに設定されます。

これらの設定は、ISAKMP Security Association (SA; セキュリティ アソシエーション) 用の設定です。単一のキーサーバを使用している場合、最初のグループメンバー登録後には ISAKMP SA は使用されません。複数のキーサーバ（協調キーサーバ）を使用している場合は、キーサーバ間の通信で ISAKMP SA が必要です。

[IKE Proposal for GET VPN] ページを開くには、次の手順を実行します。

- ([Site-to-Site VPN Manager] ウィンドウ) 既存の GET VPN トポロジを選択して、ポリシーセレクトアで [GET VPN の IKE プロポーザル (IKE Proposal for GET VPN)] を選択します。
- (ポリシービュー) [サイト間 VPN (Site-to-Site VPN)] > [GET VPN の IKE プロポーザル (IKE Proposal for GET VPN)] を選択して、既存のポリシーを選択するか、または新しいポリシーを作成します。

次の表で、このポリシーで定義できる設定について説明します。

表 1: IKE Proposal for GET VPN ポリシー

要素	説明
IKE Proposal	<p>使用する設定を定義した IKE プロポーザル ポリシー オブジェクト。そのまま使用できる定義済みのオブジェクトもいくつか用意されています。</p> <p>[選択 (Select)] をクリックして、既存の IKE プロポーザルオブジェクトのリストを開きます。選択するオブジェクトでは、グループに設定する認可方式と同じ方式が使用されている必要があります (たとえば、事前共有キーを使用する場合はプレフィックス presared を持つオブジェクト名を、Public Key Infrastructure (PKI) 証明書を使用する場合はプレフィックス cert を持つオブジェクト名を選択します)。</p> <p>オブジェクトを選択して [OK] をクリックすると、オブジェクトに定義されている設定が [IKE プロポーザルの設定 (IKE Proposal Settings)] 表示フィールドに表示されます。また、選択リストで編集することによっても設定を確認できます。適切な既存のオブジェクトが見つからない場合は、選択リストの [追加 (Add)] (+) ボタンをクリックして、新しいオブジェクトを作成します (詳細およびオプションの詳細な説明については、[IKEv1 Proposal] ポリシー オブジェクトの設定を参照してください)。</p>
IKE Proposal Overrides	<p>キー サーバおよびグループ メンバーの ISAKMP SA の有効秒数。ライフタイムを超えると、SA の期限が切れ、ピア間で再ネゴシエートする必要があります。1 ~ 86400 の値を指定できます。</p> <ul style="list-style-type: none"> • 協調キー サーバ (複数のキー サーバ) を使用している場合は、キー サーバのライフタイムを高く設定します。デフォルトの 86400 が適切です。 • 単一のキー サーバを使用している場合は、必要以上に長く ISAKMP SA が保持されないようにライフタイムを低く設定します (ただし、60 秒未満には設定しないでください)。グループ メンバー登録後は使用されません。 • 特に協調キー サーバが設定されている場合には、キー サーバのライフタイムと比較してグループ メンバーのライフタイムを低く設定することを推奨します。

関連項目

- [IKE について](#)
- [サイト間 VPN での IKEv1 事前共有キー ポリシーについて](#)
- [GET VPN グループ暗号化の定義](#)
- [Group Encrypted Transport \(GET\) VPN について \(1 ページ\)](#)
- [GET VPN の設定 \(16 ページ\)](#)

GET VPN のグローバル設定

[Global Settings for GET VPN] ページを使用して、GET VPN トポロジ内のデバイスに適用する ISAKMP および IPsec のグローバル設定を定義します。



- (注) このポリシー内のライフタイム設定は、キーサーバおよびグループメンバーの ISAKMP セキュリティアソシエーションのライフタイムには適用されません。これらのライフタイム値は、IKE Proposal for GET VPN ポリシーで設定されます。詳細については、[GET VPN の IKE プロポーザルの設定 \(20 ページ\)](#) を参照してください。

[Global Settings for GET VPN] ページを開くには、次の手順を実行します。

- ([Site-to-Site VPN Manager] ウィンドウ) 既存の GET VPN トポロジを選択して、ポリシーセレクトで [GET VPN のグローバル設定 (Global Settings for GET VPN)] を選択します。
- (ポリシービュー) [サイト間 VPN (Site-to-Site VPN)] > [GET VPN のグローバル設定 (Global Settings for GET VPN)] を選択して、既存のポリシーを選択するか、または新しいポリシーを作成します。

次の表で、このポリシーで定義できる設定について説明します。

表 2: Global Settings for GET VPN

要素	説明
Enable Keepalive (キーサーバだけ)	<p>キーサーバ間で Dead Peer Detection (DPD) キープアライブメッセージをイネーブルにするかどうかを指定します。複数のキーサーバ（協調キーサーバ）がある場合は、定期的なキープアライブをイネーブルにして、サーバ間で相互のステータスを把握し、必要に応じて新しいプライマリサーバを選定できるようにする必要があります。次を設定します。</p> <ul style="list-style-type: none"> • [間隔 (Interval)]: [定期 (Periodic)] も選択した場合は、DPD メッセージ間の秒数です。[Periodic] を選択しない場合は、トラフィックがピアから受信されない場合に DPD リトライメッセージが送信されるまでの秒数です。範囲は 10 ~ 3600 秒です。 • [リトライ (Retry)]: DPD リトライメッセージに対するピアからの応答がない場合の DPD リトライメッセージ間の秒数です。値の範囲は 2 ~ 60 秒です。デフォルトで、DPD リトライメッセージは 2 秒ごとに送信されます。5 回 DPD リトライメッセージを送信しても応答がない場合、そのキーサーバはダウンとマークされます。 • [定期 (Periodic)]: (他のキーサーバからトラフィックを受信しているかどうかにかかわらず) DPD メッセージを定期的に送信するかどうかを指定します。GET VPN では、[Periodic] を選択する必要があります。

要素	説明
アイデンティティ (Identity)	<p>フェーズIのIKEネゴシエーション中に、ピアは相互に識別する必要があります。使用するISAKMPアイデンティティを選択します。</p> <ul style="list-style-type: none"> • [Address] (デフォルト) : IKEネゴシエーションに参加するインターフェイスのIPアドレス。アドレスは、1つのインターフェイスだけがネゴシエーションに参加し、そのIPアドレスが既知である(スタティックである)場合に使用します。 • [Hostname] : 完全修飾ホスト名 (router1.example.com など)。 • [識別名 (Distinguished Name)]
SA Requests System Limit	<p>IKEがSA要求の拒否を開始する前に許可されるSA要求の最大数。ピアの数以上の値を指定する必要があります。ピアの数未満の値を指定した場合は、VPNトンネルが切断される可能性があります。</p> <p>0 ~ 99999の値を入力できます。</p>
SA Requests System Threshold	<p>IKEが新規SA要求の拒否を開始する前に使用できるシステムリソースのパーセンテージ。デフォルトは75%です。</p>
IPsec 設定	<p>IPsec SAのデフォルトのライフタイム設定を変更する場合は、[ライフタイムを有効化 (Enable Lifetime)]を選択します。グループメンバー間のトラフィック量 (KB単位)、秒数、またはその両方に基づいてライフタイムを設定できます。いずれかの値に達するとキーが失効します。デフォルトは次のとおりです (これらのデフォルトは、このオプションを選択しない場合でも設定されています)。</p> <ul style="list-style-type: none"> • [ライフタイム (秒) (Lifetime (secs))] : 3600 秒 (1 時間)。 • [ライフタイム (KB) (Lifetime (kbytes))] : 4,608,000 KB。 <p>ヒント セキュリティアソシエーションの設定時に、トラフィック暗号キー用のこれらの値を上書きできます。GET VPN グループ暗号化の定義および[Add New Security Association]/[Edit Security Association] ダイアログボックスを参照してください。</p>

関連項目

- [IKE について](#)
- [サイト間 VPN の IPsec プロポーザルについて](#)
- [Group Encrypted Transport \(GET\) VPN について \(1 ページ\)](#)
- [GET VPN の設定 \(16 ページ\)](#)

GET VPN キー サーバの設定

Key Servers ポリシーを使用して、GET VPN トポロジで使用するキー サーバを定義します。

Key Servers ポリシーを開くには、[\[Site-to-Site VPN Manager\] ウィンドウ](#)で既存の GET VPN トポロジを選択して、[ポリシー (Policies)] リストから[キーサーバー (Key Servers)] を選択します。

テーブルに、VPNで使用されているキーサーバが表示され、デバイス名、アイデンティティ、プライオリティ、および登録インターフェイスが表示されます。これらの属性の詳細については、[\[Edit Key Server\] ダイアログボックス \(25 ページ\)](#) を参照してください。

- テーブルにキーサーバーを追加するには、[行の追加 (Add Row)] ボタンをクリックして、表示されるリストからデバイスを選択します。キーサーバとして含めることができるデバイスだけが表示されます。
- キーサーバーの特性を編集するには、キーサーバーを選択して、[行の編集 (Edit Row)] ボタンをクリックします。[\[Edit Key Server\] ダイアログボックス](#)に入力します ([\[Edit Key Server\] ダイアログボックス \(25 ページ\)](#) を参照)。
- キーサーバーを削除するには、キーサーバーを選択して、[行の削除 (Delete Row)] ボタンをクリックします。
- キーサーバー間で RSA キーを同期して、すべてのサーバーで同じキーが使用されるようにするには、[キーの同期 (Synchronize Keys)] ボタンをクリックします。キーの同期が必要なタイミングや理由を含むキー同期プロセスの詳細については、[RSA キーの生成と同期 \(18 ページ\)](#) を参照してください。

協調キー サーバを使用する場合のキー サーバの順序を変更するには、キー サーバを選択して、上向きまたは下向きの矢印ボタンをクリックします。この順序では、どのサーバがプライマリ キー サーバであるかは定義されません (プライマリ キー サーバは、[Priority] の値によって決定されます。値が大きいほど、そのサーバがプライマリ キー サーバとして選定される確率が高くなります)。

代わりに、グループ メンバーがキー サーバへの登録を試みるデフォルトの順序が決定されません。グループ メンバーは、リストの最初のキー サーバに登録されます。最初のキー サーバに到達できない場合、グループ メンバーは、2 番め以降のキー サーバに順番に登録を試みます。キー サーバの冗長性の詳細については、[協調キー サーバを使用した冗長性の設定 \(9 ページ\)](#) を参照してください。個別のグループ メンバーでこの順序を上書きできます。[GET VPN グループ メンバーの設定 \(26 ページ\)](#) および [\[Edit Group Member\] ダイアログボックス \(27 ページ\)](#) を参照してください。



ヒント テーブルの下にある[表示 (Show)] フィールドを使用して、[アイデンティティ (Identity)] カラムおよび[インターフェイス (interfaces)] カラムに、インターフェイスロールを表示するか、またはこれらのロールによって定義されている実際のインターフェイスを表示するかを切り替えることができます。

関連項目

- [GET VPN 登録プロセスについて \(5 ページ\)](#)
- [Group Encrypted Transport \(GET\) VPN について \(1 ページ\)](#)
- [GET VPN の設定 \(16 ページ\)](#)
- [デバイス ビューにおける VPN トポロジの設定](#)
- [テーブルのフィルタリング](#)

[Add Key Server]、[Add Group Member] ダイアログボックス

[Add Key Server] ダイアログボックスおよび [Add Group Member] ダイアログボックスを使用して、GET VPN トポロジで使用されるキー サーバまたはグループ メンバーを選択します。目的のデバイスの横にあるチェックボックスを選択して、[OK] をクリックします。

ナビゲーションパス

GET VPN トポロジにキーサーバーまたはグループメンバーを追加するには、[VPNの作成 (Create VPN)] ウィザードの [VPNピアの取得 (GET VPN Peers)] ページにある [キーサーバーまたはグループメンバー (Key Server or Group Member)] テーブルの下の [行の追加 (Add Row)] (+) をクリックします。既存のトポロジの場合は、[キーサーバー (Key Servers)] ポリシーまたは [グループメンバー (Group Members)] ポリシーを使用します。詳細については、次の項を参照してください。

- [GET VPN ピアの定義](#)
- [GET VPN キー サーバの設定 \(24 ページ\)](#)
- [GET VPN グループ メンバーの設定 \(26 ページ\)](#)

[Edit Key Server] ダイアログボックス

[Edit Key Servers] ダイアログボックスを使用して、GET VPN トポロジのキー サーバに定義されている属性を変更します。

ナビゲーションパス

- (Create VPN ウィザード) [GET VPNピア (GET VPN Peers)] ページに移動し、キーサーバーを選択して、[行の編集 (Edit Row)] ボタンをクリックします。 [GET VPN ピアの定義](#) を参照してください。
- ([Site-to-Site VPN Manager] ウィンドウ) [キーサーバー (Key Servers)] ポリシーを選択し、キーサーバーを選択して、[行の編集 (Edit Row)] ボタンをクリックします。 [GET VPN キー サーバの設定 \(24 ページ\)](#) を参照してください。

関連項目

- [Group Encrypted Transport \(GET\) VPN について \(1 ページ\)](#)
- [GET VPN の設定 \(16 ページ\)](#)

フィールドリファレンス

表 3: [Edit Key Server] ダイアログボックス

要素	説明
Identity Interface	グループメンバーがキーサーバを識別し、キーサーバに登録するために使用するインターフェイス。デフォルトは、すべてのループバックインターフェイスを識別するループバック インターフェイス ロールです。
プライオリティ	キーサーバのロール（プライマリまたはセカンダリ）を指定する、1～100 の数値。最も高い数値を持つキーサーバがプライマリ キーサーバとなります。2つ以上のキーサーバに同じプライオリティが割り当てられている場合は、最も大きい IP アドレスを持つデバイスが使用されます。デフォルトのプライオリティは、最初のキーサーバに対しては 100、2 番めのキーサーバに対しては 95 などになります。 (注) ネットワークがパーティション化されている場合は、複数のプライマリ キーサーバが存在することがあります。
登録インターフェイス (Registration Interface)	Group Domain of Interpretation (GDOI) 登録を受け入れることができるインターフェイス。登録インターフェイスを指定しない場合、GDOI 登録は任意のインターフェイスで実行できます。

GET VPN グループメンバーの設定

Group Members ポリシーを使用して、GET VPN トポロジ内のグループメンバーを定義します。

Group Members ポリシーを開くには、[Site-to-Site VPN Manager] ウィンドウで既存の GET VPN トポロジを選択して、[ポリシー (Policies)] リストから [グループメンバー (Group Members)] を選択します。

グループメンバーのテーブルには、GET VPN のメンバーが表示され、デバイス名、GET 対応インターフェイス、ローカルインターフェイス、およびセキュリティポリシーが表示されます。これらの属性の詳細については、[Edit Group Member] ダイアログボックス (27 ページ) を参照してください。

- テーブルにグループメンバーを追加するには、[行の追加 (Add Row)] ボタンをクリックして、表示されるリストからデバイスを選択します。グループメンバーとして含めることができるデバイスだけが表示されます。

- グループメンバーのエンドポイント特性を編集するには、グループメンバーを選択して、[行の編集 (Edit Row)] ボタンをクリックします。[Edit Group Member] ダイアログボックスに入力します（[Edit Group Member] ダイアログボックス (27 ページ) を参照）。

テーブル内の複数のグループメンバーを選択した場合は、右クリックして次のコマンドを選択することによって、それぞれに示す属性だけを編集することもできます。

- [キーサーバー順序の編集 (Edit Key Server Order)] : 選択したグループメンバーのキーサーバーリストおよび優先順位を変更します。
- [パッシブSAモードの編集 (Edit Passive SA Mode)] : 選択したグループメンバーでパッシブ SA モードを使用するかどうかを変更します。
- グループメンバーを削除するには、グループメンバーを選択して、[行の削除 (Delete Row)] ボタンをクリックします。



ヒント テーブルの下にある [表示 (Show)] フィールドを使用して、[インターフェイス (Interfaces)] 列に、インターフェイスロールを表示するか、またはそれらのロールによって定義されている実際のインターフェイスを表示するかを切り替えることができます。

関連項目

- [登録の失敗時にも保護するためのフェールクローズの設定 \(10 ページ\)](#)
- [パッシブモードを使用した GET VPN への移行 \(30 ページ\)](#)
- [Group Encrypted Transport \(GET\) VPN について \(1 ページ\)](#)
- [GET VPN の設定 \(16 ページ\)](#)
- [デバイスビューにおける VPN トポロジの設定](#)
- [テーブルのフィルタリング](#)

[Edit Group Member] ダイアログボックス

[Edit Group Members] ダイアログボックスを使用して、GET VPN トポロジのグループメンバーに定義されている属性を変更します。



ヒント 複数のデバイスを選択して、右クリックメニューから編集コマンドを選択すると、このダイアログボックスには選択した編集コマンドに関連するオプションだけが表示されます。

ナビゲーションパス

- (Create VPN ウィザード) [GET VPN ピア (GET VPN Peers)] ページに移動し、グループメンバーを選択して、[行の編集 (Edit Row)] ボタンをクリックします。 [GET VPN ピアの定義](#) を参照してください。
- ([Site-to-Site VPN Manager] ウィンドウ) GET VPN トポロジを選択して、[グループメンバー (Group Members)] ポリシーを選択します。グループメンバーを選択して、[行の編集 (Edit Row)] ボタンをクリックします。 [GET VPN グループメンバーの設定 \(26 ページ\)](#) を参照してください。

関連項目

- [Group Encrypted Transport \(GET\) VPN について \(1 ページ\)](#)
- [GET VPN の設定 \(16 ページ\)](#)

フィールドリファレンス

表 4: [Edit Group Member] ダイアログボックス

要素	説明
GET-Enabled Interface	<p>プロバイダー エッジ (PE) への VPN 対応外部インターフェイス。このインターフェイスで発信または終了するトラフィックは、暗号化または復号化が適宜評価されます。複数のインターフェイスを設定できます。</p> <p>インターフェイスまたはインターフェイスロールの名前を入力するか、あるいは [選択 (Select)] をクリックして、リストから名前を選択するか、新しいインターフェイスロールを作成します。</p>
Interface to be used as local address	<p>キーの再生成情報などのデータを送信するために、キーサーバでグループメンバーを識別する場合に IP アドレスが使用されるインターフェイス。GET が 1 つのインターフェイスでだけイネーブルになっている場合は、ローカルアドレスとして使用するインターフェイスを指定する必要はありません。GET が複数のインターフェイスでイネーブルになっている場合は、ローカルアドレスとして使用するインターフェイスを指定する必要があります。</p> <p>インターフェイスまたはインターフェイスロールの名前を入力するか、あるいは [選択 (Select)] をクリックして、リストから名前を選択するか、新しいインターフェイスロールを作成します。</p>

要素	説明
セキュリティポリシー	<p>キーサーバからダウンロードされたセキュリティACLよりも優先される、一部のグループメンバー固有のトラフィックを拒否するために使用されるローカルのグループメンバーセキュリティACL。拒否されたトラフィックは、暗号化されずにクリアテキストで送信されます。詳細については、GET VPN セキュリティポリシーおよびセキュリティアソシエーションについて (13 ページ) を参照してください。</p> <p>ACLオブジェクトの名前を入力します。あるいは、[選択 (Select)] をクリックして、リストから選択するか、または新しいオブジェクトを作成します。</p>
Enable Fail Close フェールクローズ ACL (Fail Close ACL)	<p>デバイスがキーサーバに正常に登録される前に、デバイスからクリアテキストのトラフィックが送信されることを防止するフェールクローズモードをデバイスでイネーブルにするかどうかを指定します。フェールクローズモードを使用するには、Cisco IOS ソフトウェア Release 12.4(22)T または 15.0 以上が必要です。また、フェールクローズモードは、サポートされているすべての ASR に設定できます。</p> <p>ヒント フェールクローズモードは複雑な機能であり、慎重にフェールクローズ ACL を作成しないとデバイスからロックアウトされる可能性があります。フェールクローズモードをイネーブルにする前に、登録の失敗時にも保護するためのフェールクローズの設定 (10 ページ) を参照してください。</p> <p>設定の更新が可能となるように、Security Manager サーバとの SSH 通信や SSL 通信などの許可するクリアテキストのトラフィックを指定した ACL ポリシーオブジェクトを選択する必要があります (deny ステートメントを使用)。オブジェクトの名前を入力します。あるいは、[選択 (Select)] をクリックして、オブジェクトを選択するか、または新しいオブジェクトを作成します。</p>
Override Key Servers	<p>この特定のグループメンバーにおいて、GET VPN トポロジ全体に設定されているキーサーバリストを上書きするかどうかを指定します。</p> <p>このオプションを選択した場合は、トポロジに設定されているキーサーバのうち、選択したグループメンバーで使用されるサブセットを選択できます。また、それらのサーバのプライオリティ順も変更できます。この設定は、複数の協調キーサーバ間で登録アクティビティを負荷分散するのに役立ちます。詳細については、協調キーサーバを使用した冗長性の設定 (9 ページ) を参照してください。</p> <p>[選択 (Select)] をクリックし、[キーサーバーの選択 (Key Servers Selection)] ダイアログボックスを使用して、キーサーバリストおよびキーサーバーのプライオリティ順を変更します。グループメンバーでのキーサーバの使用方法を変更する前に、GET VPN トポロジにそのキーサーバが定義されている必要があります。</p>

要素	説明
Enable Passive SA Mode	<p>グループメンバーをパッシブ Security Association (SA; セキュリティアソシエーション) モードに設定するかどうかを指定します。このモードでは、グループメンバーは SA をインバウンド方向でだけインストールします。つまり、グループメンバーは、暗号化されたデータを受信することができますが、クリアテキストのデータだけを送信します。このモードは、主に既存の VPN から GET VPN に移行する場合に、VPN のテスト目的でだけ役立ちます (このモードを使用するには、グループメンバーは、Cisco IOS ソフトウェアバージョン 12.4(22)T または 15.0 以上を実行しているか、あるいはサポートされている ASR である必要があります)。</p> <p>この設定は、Group Encryption ポリシーの [受信のみ (Receive Only)] 設定 (トポロジ全体に適用されます) と似ています。このグループメンバーオプションは、Group Encryption ポリシーの設定よりも優先されます。</p> <p>これらのパッシブモード機能を使用して GET VPN への移行または GET VPN のテストを行う方法の詳細については、パッシブモードを使用した GET VPN への移行 (30 ページ) を参照してください。</p>

パッシブモードを使用した GET VPN への移行

既存の VPN (特にクリアテキストを使用する VPN) から GET VPN テクノロジーに移行する場合は、2つの機能を使用して、ネットワークのダウンタイムを回避するために段階的な移行を行うことができます。これらの機能はほぼ同じものであり、暗号化されたトラフィックを受動的に受け入れるものですが、GET VPN 内の異なる種類のデバイスに設定できます。

通常、完全に展開された GET VPN では、トラフィックは双方向に暗号化されます (双方向 Security Association (SA; セキュリティアソシエーション))。ただし、テスト中にはパッシブモードを使用できます。パッシブモードでは、グループメンバーは SA をインバウンド方向でだけインストールします。これにより、グループメンバーは、暗号化されたトラフィックを受信できますが、トラフィックの送信はクリアテキストで行います。その後、VPN をテストし、期待どおりに動作していることを確認してから、完全な暗号化をオンにできます。

GET VPN にパッシブモードを設定するには、次の機能を使用します。

- SA 受信専用モード** : 受信専用モードは、Group Encryption ポリシーを使用して、トポロジ内のキーサーバーのセキュリティアソシエーションに設定します。したがって、この設定はトポロジ全体に適用されます。
- パッシブ SA モード** : パッシブセキュリティアソシエーションモードは、個別のグループメンバーに設定します。この設定は、SA 受信専用設定よりも優先されます。そのため、トポロジ全体に対して完全な暗号化をオンにして、一部のグループメンバーをパッシブモードのままにできます。これにより、グループメンバーを段階的にテストして、すべてのメンバーデバイスを確認してから完全な暗号化をイネーブルにできます。



ヒント グループメンバーにパッシブ SA モードを設定するには、Cisco IOS ソフトウェア Release 12.4(22)T+ または 15.0+、あるいは ASR では Release 2.3 (12.2(33)XNC) + が必要です。

ここでは、これらのパッシブモード機能を使用して GET VPN に移行する場合に使用できる、エンドツーエンドの移行プロセスの例を示します。

関連項目

- [Group Encrypted Transport \(GET\) VPN について \(1 ページ\)](#)
- [GET VPN の設定 \(16 ページ\)](#)

ステップ 1 Create VPN ウィザードを使用して、Security Manager に新しい GET VPN トポロジを作成します。ウィザードでは、次のように選択します。

- デバイスを選択するときには、トポロジのキーサーバを選択します。グループメンバーについては、移行するグループメンバーのうち最初のセットを選択します。詳細については、[VPN トポロジのデバイスの選択](#)を参照してください。
- グループ暗号化を設定するときには、[受信専用 (Receive Only)] を選択します。これにより、トポロジ全体で SA 受信専用機能がイネーブルになります。詳細については、[GET VPN グループ暗号化の定義](#)を参照してください。

VPN 作成の詳細については、[VPN トポロジの作成または編集](#)を参照してください。

ステップ 2 VPN のすべてのデバイスに設定を展開します。これで、グループメンバーは暗号化されたトラフィックの受信はできますが、送信はできなくなります。展開プロセスの詳細については、使用している Workflow モードに応じて次の項を参照してください。

- [Workflow 以外のモードでの設定の展開](#)
- [Workflow モードでの設定の展開](#)

ステップ 3 Security Manager の外部で、すべてのグループメンバーが正常に動作していることを確認します。

たとえば、グループメンバーデバイスでいくつかの CLI コマンドを使用して、グループメンバーで暗号化されたパケットを送受信できるかどうかをテストできます。

- グループメンバー 1 で、次のコマンドを設定します。「groupexample」は、VPN の GDOI グループの名前です。このコマンドによって、暗号化されたテキストまたはクリアテキストを受信できるが、クリアテキストだけを送信できるようにデバイスが設定されます。

crypto gdoi gm group groupexample ipsec direction inbound only

- グループメンバー 2 で、次のコマンドを設定します。このコマンドによって、暗号化されたテキストまたはクリアテキストを受信でき、暗号化されたテキストを送信できるようにデバイスが設定されます。

crypto gdoi gm group groupexample ipsec direction inbound optional

- グループメンバー2からグループメンバー1に ping を実行します。パケットは、グループメンバー2から送信される前に暗号化されます。グループメンバー1は、このパケットを受け入れて、復号化します。メンバー1からメンバー2に ping を実行した場合、ping はクリアテキストで送信されて、メンバー2によって受け入れられます。ACL で ping が許可されていることを確認してください。

ステップ4 Cisco Security Manager で、[管理 (Manage)]>[サイト間VPN (Site-to-Site VPNs)]を選択します ([Site-to-Site VPN Manager] ウィンドウを参照)。

GET VPN トポロジを選択して、[グループメンバー (Group Members)]を選択します。

トポロジに追加する残りのグループメンバーを追加します ([グループメンバーの追加 (Add Group Member)] (+) ボタンをクリックし、デバイスを選択して、[OK] をクリックします)。

完全な暗号化を有効にする前に、パッシブモードを使用して新しいグループメンバーをテストする場合は、グループメンバーの設定時に [パッシブSAモードの有効化 (Enable Passive SA Mode)]を選択します。

- 個別のグループメンバーを設定するには、メンバーを選択して、[グループメンバーの編集 (Edit Group Member)] (鉛筆) ボタンをクリックします。
- 一度に複数のデバイスでパッシブモードを有効にするには、Shift または Ctrl を押しながらクリックして複数のデバイスを選択し、右クリックして [パッシブSAモードの編集 (Edit Passive SA Mode)] を選択します。その後、オプションを選択して [OK] をクリックします。

グループメンバーの設定の詳細については、[GET VPN グループメンバーの設定 \(26 ページ\)](#) を参照してください。

ステップ5 設定変更を VPN のすべてのデバイスに展開します。この時点で、すべてのデバイスはパッシブモードで動作しています。

ステップ6 Site-to-Site VPN Manager で、GET VPN トポロジを選択して、[Group Encryptionポリシー (Group Encryption Policy)]を選択します。

[受信専用 (Receive Only)]の選択を解除します。これにより、トポロジレベルで SA 受信専用モードがオフになります。

ステップ7 設定変更を VPN のすべてのデバイスに展開します。テストした最初のグループメンバーでは、GET VPN は完全暗号化モードで動作しています。パッシブ SA モードをイネーブルにして追加した新しいメンバーは、暗号化されたトラフィックを受信し、クリアテキストのトラフィックを送信しています。

ステップ8 次の手順を使用して、新しいデバイスを確認し、パッシブモードをオフにします。この手順は、すべての新しいデバイスに対して同時に実行することも、小さなグループに分けて段階的に実行することもできます。また、ネットワークを拡張したときに新しいグループメンバーに対してこの手順を実行することもできます。必要に応じて次の手順を繰り返してください。

- a) 最初のグループメンバーを確認したときと同じ方法を使用して、新しいグループメンバーが正常に動作していることを確認します。
- b) グループメンバーのセットを完全暗号化モードに移行する準備が整ったら、Site-to-Site VPN Manager で GET VPN トポロジを選択して、[グループメンバー (Group Members)]を選択します。

- c) 完全な暗号化を使用する必要があるすべてのパッシブモードのグループメンバーを選択し、右クリックして、[パッシブSAモードの編集 (Edit Passive SA Mode)] を選択します。[パッシブSAモードの有効化 (Enable Passive SA Mode)] オプションの選択を解除して、[OK] をクリックします。
- d) パッシブモードを変更したデバイスだけではなく、VPN のすべてのデバイスに設定を展開します。通常は、VPN 内のすべてのデバイスに展開する必要があります。

GET VPN 設定のトラブルシューティング

Security Manager を使用して GET VPN をプロビジョニングおよび展開したあとに GET VPN が動作しない場合は、次の項目をチェックします。

- すべての協調キー サーバ間で RSA キーが同期されていること、つまり RSA キーが同じであることを確認します。キーの同期方法の詳細については、[RSA キーの生成と同期 \(18 ページ\)](#) を参照してください。
- 目的のトラフィックが暗号化されない場合は、キー サーバのセキュリティ ポリシー ACL (セキュリティ アソシエーション) に目的のトラフィックの permit ACE があることを確認します。非対称の ACE の場合 (送信元アドレスと宛先アドレスが異なる場合) は、対称的な ACE (送信元アドレスと宛先アドレスを入れ替えた ACE) が存在することを確認します。詳細については、[GET VPN セキュリティ ポリシーおよびセキュリティ アソシエーションについて \(13 ページ\)](#) を参照してください。
- マルチキャストのキーの再生成を使用する場合は、ネットワーク、すべてのキーサーバ、およびほとんどのグループメンバーでマルチキャストがイネーブルになっていることを確認します。マルチキャストは、デバイスで直接イネーブルにする必要があります。マルチキャストをイネーブルにするために必要なコマンドは、Security Manager によってプロビジョニングされません。詳細については、[キーの再生成転送メカニズムの選択 \(7 ページ\)](#) を参照してください。
- マルチキャストのキーの再生成を使用する場合は、キー サーバのセキュリティ ACL にマルチキャスト グループ アドレス用の deny ACE があり、マルチキャストのキーの再生成メッセージが暗号化されないことを確認します。
- グループメンバーのローカルセキュリティ ACL には deny ACE だけがあることを確認します。暗号化するトラフィックを特定するために permit ステートメントを含めると、対応する IPsec SA がいないため、一致するトラフィックは実際にはドロップされます。permit エントリがグループメンバーにあるため、キーサーバはそのエントリを認識できず、必要な IPsec SA を生成できません。詳細については、[GET VPN セキュリティ ポリシーおよびセキュリティ アソシエーションについて \(13 ページ\)](#) を参照してください。
- 証明書を使用してグループメンバーを認可する場合は、ISAKMP 認証で証明書が使用されており、PKI ポリシーが設定されていることを確認します。グループメンバーおよびキーサーバの ISAKMP アイデンティティは、Distinguished Name (DN; 識別名) を使用するように設定する必要があります。

- 通常、GET VPNが展開されるタイプのWAN環境では、ネットワークアドレス変換 (NAT) は使用されません。ただし、NATを使用する場合には、変換されるアドレス用の permit ステートメントがセキュリティ ポリシー ACLにあることを確認します。また、Network Address Translation-Traversal (NAT-T; ネットワーク アドレス変換通過) を使用する場合、GDOI プロトコル ポートは 4500 に変更されます。
- Cisco IOS ソフトウェア Release 12.4(15)T10、12.4(22)T3、12.4(24)T2、15.0(1)M、および 12.2(33)XNEには、コントロールプレーンリプライ保護メカニズムが追加されました。このメカニズムは下位互換性がないため、ネットワーク内のいずれかの GET VPN グループ メンバーがこれらのいずれかの (またはそれ以上の) リリースを実行している場合には、すべてのキーサーバをこれらの (またはそれ以上の) リリースにアップグレードする必要があります。アップグレードしない場合は、キーの再生成に失敗してネットワークが切断される可能性があります。この場合、次のいずれかのシステム ロギング (syslog) メッセージが表示されます。
 - %GDOI-3-GDOI_REKEY_SEQ_FAILURE: Failed to process rekey seq # 2 in seq payload for group get-group, last seq # 6
 - %GDOI-3-PSEUDO_TIME_TOO_OLD: Rekey received in group get-group is too old and failed PST check: my_pst is 184 sec, peer_pst is 25 sec, allowable_skew is 10 sec



ヒント 便利な **show** コマンドの情報を含む、CLI 設定の観点からの追加のトラブルシューティングのヒントについては、Cisco.com の『[Cisco Group Encrypted Transport VPN](#)』を参照してください。

関連項目

- [Group Encrypted Transport \(GET\) VPN について \(1 ページ\)](#)
- [GET VPN の設定 \(16 ページ\)](#)

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。