セキュリティ機能の設定

Cisco 3900 シリーズ、2900 シリーズ、および 1900 シリーズ サービス統合型ルータ（ISR）では、次のセキュリティ機能を提供します。

暗号化エンジンのアクセラレータの設定

Services Performance Engine 200 および Services Performance Engine 250 には、SSLVPN プロトコルと IPSec プロトコル間で共有されるオンボードの暗号化エンジン アクセラレータがあります。

デフォルトで、IPSec のパフォーマンスを最大化するために SSL の加速は無効になっています。SSLVPN ゲートウェイとしてルータを設定するには、グローバル コンフィギュレーション モードで **crypto engine accelerator bandwidth-allocation ssl fair** コマンドで SSLVPN のハードウェア アクセラレーションをイネーブルにします。**reload** コマンドを発行します。

SSL VPN の設定

CISCO IOS ソフトウェアの Secure Socket Layer Virtual Private Network（SSL VPN; セキュア ソケット レイヤ バーチャル プライベート ネットワーク）機能（WebVPN とも呼ばれる）を使用すると、リモート ユーザは、どのような場所にいても、インターネット上からエンタープライズ ネットワークにアクセスできるようになります。リモート アクセスは、SSL 対応の SSL VPN ゲートウェイを介して提供されています。SSL VPN ゲートウェイによりリモート ユーザは、Web ブラウザを使用してセキュアな VPN トンネルを確立できます。この機能は、ネイティブ HTTP over SSL（HTTPS）ブラウザ サポートを使用して、幅広い Web リソースおよび Web 対応アプリケーションに簡単にアクセスできる包括的なソリューションを実現します。SSL VPN は、クライアントレス、シンクライアント、フル トンネル クライアント サポートの 3 種類の SSL VPN アクセス モードを提供します。

SSL VPN の設定に関する追加情報については、『*Cisco IOS Security Configuration Guide: Secure Connectivity, Release 12.4T*』の「SSL VPN」（http://www.cisco.com/en/US/docs/ios/sec_secure_connectivity/configuration/guide/12_4t/sec_secure_connectivity_12_4t_book.html）を参照してください。

認証、許可、アカウンティング

認証、許可、アカウンティング（AAA）ネットワーク セキュリティ サービスは、ルータにアクセス コントロールを設定するための主要なフレームワークを提供します。認証は、ログインおよびパスワード ダイアログ、確認要求および応答、メッセージングのサポート、暗号化（選択するセキュリティ プロトコルに応じて）など、ユーザを識別するための方法を提供します。許可は、1 回限りの許可や各サービスに対する許可、各ユーザに対するアカウント リストおよびプロファイル、ユーザ グループのサポート、IP、Internetwork Packet Exchange（IPX; インターネットワーク パケット交換）、AppleTalk Remote Access（ARA; AppleTalk リモート アクセス）、および Telnet のサポートなど、リモート アクセスをコントロールするための方法を提供します。アカウンティングで、ユーザ識別、開始時刻と終了時刻、実行コマンド（PPP など）、パケット数、バイト数などといったセキュリティ サーバ情報の収集と送信を行い、課金、監査、およびレポートに使用する手段を提供します。

AAA では、Remote Authentication Dial-In User Service（RADIUS; リモート認証ダイヤルイン ユーザ サービス）、Terminal Access Controller Access Control System Plus（TACACS+; ターミナル アクセス コントローラ アクセス コントロール システム プラス）、または Kerberos などのプロトコルを使用してセキュリティ機能を管理します。ルータがネットワーク アクセス サーバとして機能している場合、AAA は、ネットワーク アクセス サーバと RADIUS、TACACS+、または Kerberos セキュリティ サーバ間の通信を確立するための手段となります。

AAA サービスおよびサポートされているセキュリティ プロトコル、認証、許可、アカウンティング、RADIUS、TACACS+、または Kerberos の設定については、『*Cisco IOS Security Configuration Guide: Securing User Services, Release 12.4T*』の次の項を参照してください。

http://www.cisco.com/en/US/docs/ios/sec_user_services/configuration/guide/12_4T/sec_securing_user_services_12.4t_book.html

- 『Configuring Authentication』
- 『Configuring Authorization』
- 『Configuring Accounting』
- 『Configuring RADIUS』
- 『Configuring TACACS+』
- 『Configuring Kerberos』

AutoSecure の設定

AutoSecure 機能は、ネットワーク攻撃に悪用される可能性のある一般的な IP サービスをディセーブルにし、攻撃を受けたときはネットワークの防御に役立つ IP サービスおよび機能をイネーブルにできます。この IP サービスは、1 つのコマンドですべてを同時にディセーブル/イネーブルにすることにより、ルータ上のセキュリティ設定を大幅に簡易化しています。AutoSecure 機能の詳細については、*AutoSecure* 機能のマニュアル（http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123_1/ftatosec.htm）を参照してください。

アクセス リストの設定

アクセス リストは、送信元 IP アドレス、宛先 IP アドレス、またはプロトコルに基づいてインターフェイス上のネットワーク トラフィックを許可または拒否します。アクセス リストは、標準版または拡張版のどちらかに設定されます。標準アクセス リストは、指定された送信元からのパケットの通過を許可または拒否します。拡張アクセス リストでは、宛先および送信元の両方を指定できます。また、各プロトコルを指定して、通過を許可または拒否することができます。

アクセス リストの作成の詳細については、『*Cisco IOS Security Configuration Guide: Securing the Data Plane, Release 12.4T*』の「Access Control Lists」（http://www.cisco.com/en/US/docs/ios/sec_data_plane/configuration/guide/12_4t/sec_data_plane_12_4t_book.html）の項を参照してください。

アクセス リストは、一般的なタグによってコマンドがバインドされる一連のコマンドです。タグは、番号または名前のどちらかです。表 1 は、アクセス リストの設定に使用するコマンドのリストです。

表 1　　アクセス リストのコンフィギュレーション コマンド

アクセス コントロール リスト（ACL）タイプ	コンフィギュレーション コマンド
番号形式	
標準	**access-list** {**1-99**}{**permit** | **deny**} *source-addr* [*source-mask*]
拡張	**access-list** {**100-199**}{**permit** | **deny**} *protocol source-addr* [*source-mask*] *destination-addr* [*destination-mask*]
名前形式	
標準	**ip access-list standard** *name* followed by **deny** {*source* | *source-wildcard* | **any**}
拡張	**ip access-list extended** *name* **{permit** | **deny}** *protocol* {*source-addr* [*source-mask*] | **any**}{*destination-addr* [*destination-mask*] | **any**}

アクセス リストの作成、改良、管理については、『*Cisco IOS Security Configuration Guide: Securing the Data Plane, Release 12.4T*』の「Access Control Lists」（http://www.cisco.com/en/US/docs/ios/sec_data_plane/configuration/guide/12_4t/sec_data_plane_12_4t_book.html）を参照してください。

- 『Creating an IP Access List and Applying It to an Interface』
- 『Creating an IP Access List to Filter IP Options, TCP Flags, Noncontiguous Ports, or TTL Values』
- 『Refining an IP Access List』
- 『Displaying and Clearing IP Access List Data Using ACL Manageability』

アクセス グループ

アクセス グループとは、一般的な名前または番号にバインドされている一連のアクセス リストの定義のことです。アクセス グループは、インターフェイスを設定するときに、インターフェイスに対してイネーブルにされます。アクセス グループを作成する場合は、次の注意事項に従ってください。

- アクセス リストの定義の順序は重要です。パケットは、最初のアクセス リストから順に照合されます。一致するものがない場合（つまり、許可または拒否が発生しない場合）は、次のアクセス リストに照合され、さらに次のアクセス リストへと順に進められます。
- パケットが許可または拒否される前に、すべてのパラメータがアクセス リストに一致する必要があります。
- すべてのシーケンスの末尾には、暗黙的に「deny all」が付きます。

アクセス グループの設定および管理に関する情報については、『*Cisco IOS Security Configuration Guide: Securing the Data Plane, Release 12.4T*』の「Access Control Lists」の項の「Creating an IP Access List to Filter IP Options, TCP Flags, Noncontiguous Ports, or TTL Values」の項（http://www.cisco.com/en/US/docs/ios/sec_data_plane/configuration/guide/12_4t/sec_data_plane_12_4t_book.html）を参照してください。

Cisco IOS ファイアウォールの設定

Cisco IOS ファイアウォールでは、ステートフルなファイアウォールを設定できます。ステートフルなファイアウォールでは、パケットが内部的に検査され、ネットワーク接続の状態が監視されます。アクセス リストは各パケットに基づいたトラフィックの許可または拒否に制限され、パケットの流れには基づいていないため、ステートフルなファイアウォールの方が静的アクセス リストよりも優れています。また、Cisco IOS ファイアウォールでは、パケットを検査するため、アプリケーション層のデータを検証してトラフィックの許可または拒否を決定できます。静的アクセス リストでは、これは検証不可能です。

Cisco IOS ファイアウォールを設定するには、インターフェイス コンフィギュレーション モードで次のコマンドを使用して、検証するプロトコルを指定します。

ip inspect name *inspection-name protocol* **timeout** *seconds*

指定したプロトコルがファイアウォールを通過していることがインスペクションで検出された場合、ダイナミック アクセス リストが作成され、リターン トラフィックの通過を許可します。timeout パラメータは、リターン トラフィックがルータを通過せずに、ダイナミック アクセス リストがアクティブの状態を保つ時間を指定します。タイムアウト値が指定値に達すると、ダイナミック アクセス リストが削除され、後続のパケット（有効なパケットの場合もある）が許可されなくなります。

複数のステートメントで同一のインスペクション名を使用して、1 つのルール セットにまとめてください。ファイアウォールにインターフェイスを設定するときに、**ip inspect inspection-name { in | out }** コマンドを使用して、このルール セットを設定の別の場所でアクティブ化できます。

Cisco IOS ファイアウォールの設定に関する追加情報については、『*Cisco IOS Firewall Overview*』（http://www.cisco.com/en/US/docs/ios/security/configuration/guide/sec_ios_firewall_ov.html）を参照してください。

また、Cisco IOS ファイアウォールは、Session Initiated Protocol（SIP）アプリケーションでの音声セキュリティを提供するようにも設定できます。SIP インスペクションでは、基本的な検査機能（ピンホール開口部の SIP パケット インスペクションおよび検出）に加え、プロトコルの適合性やアプリケーション セキュリティを提供します。詳細については、『*Cisco IOS Firewall: SIP Enhancements: ALG and AIC*』（http://www.cisco.com/en/US/docs/ios/security/configuration/guide/sec_sip_alg_aic.html）を参照してください。

ゾーンベース ポリシー ファイアウォール

Cisco IOS ゾーンベース ポリシー ファイアウォールを使用すると、インターフェイスを異なるゾーンに割り当て、ポリシーを設定することでセキュリティ ポリシーを展開し、これらのゾーン間を行き来するトラフィックを検査できるようになります。ポリシーでは、定義したトラフィック クラスに適用する一連のアクションを指定します。

ゾーン ベース ポリシー ファイアウォールの設定に関する詳細情報については、『*Cisco IOS Security Configuration Guide: Securing the Data Plane, Release 12.4T*』の「Zone-Based Policy Firewall」（http://www.cisco.com/en/US/docs/ios/sec_data_plane/configuration/guide/12_4t/sec_data_plane_12_4t_book.html）を参照してください。

Cisco IOS IPS の設定

Cisco IOS Intrusion Prevention System（IPS; 侵入防御システム）テクノロジーは、セキュリティ ポリシーに違反したり悪意のあるネットワーク アクティビティを表すパケットおよびフローを適切に処理することで、境界ファイアウォール保護を強化します。

Cisco IOS IPS では、「シグネチャ」を使用して、ネットワーク トラフィック内における誤使用のパターンを検出します。Cisco IOS IPS は、インライン侵入検出センサーとして機能し、ルータを通過するパケットおよびセッションを監視して、現在アクティブな（ロードされている）アタック シグネチャのいずれかと一致するかどうかについてそれぞれをスキャンします。Cisco IOS IPS により不審なアクティビティが検出されると、ネットワーク セキュリティが損なわれる前に対応し、イベントを記録します。また、検出されたシグニチャに対して設定されたアクションに基づいて、次の操作を実行します。

- syslog フォーマットでアラームを送信する、または Secure Device Event Exchange（SDEE; セキュア デバイス イベント交換）フォーマットでアラームのログを取る
- 不審なパケットを廃棄する
- 接続を再設定する
- 攻撃者の発信元 IP アドレスからのトラフィックを一定時間拒否する
- シグニチャが見つかった接続のトラフィックを一定時間拒否する

Cisco IOS IPS の設定に関する追加情報については、『*Cisco IOS Security Configuration Guide: Securing the Data Plane, Release 12.4T*』の「Cisco IOS IPS 5.x Signature Format Support and Usability Enhancements」（http://www.cisco.com/en/US/docs/ios/sec_data_plane/configuration/guide/12_4t/sec_data_plane_12_4t_book.html）を参照してください。

コンテンツのフィルタリング

Cisco 3900 シリーズ、2900 シリーズ、および 1900 シリーズ ISR では、カテゴリベースの URL フィルタリングを提供しています。ユーザは、許可または拒否する Web サイトのカテゴリを選択し、ISR 上で URL フィルタリングを準備します。各カテゴリの URL のチェックには、サードパーティが保守する外部サーバが使用されています。ポリシーの許可および拒否は、ISR 上で保守されています。サービスは、加入ベースで提供され、各カテゴリの URL はサードパーティ ベンダーによってメンテナンスされています。

URL フィルタリング設定の詳細については、『Subscription-based Cisco IOS Content Filtering』（http://www.cisco.com/en/US/docs/ios/security/configuration/guide/sec_url_filtering.html）を参照してください。

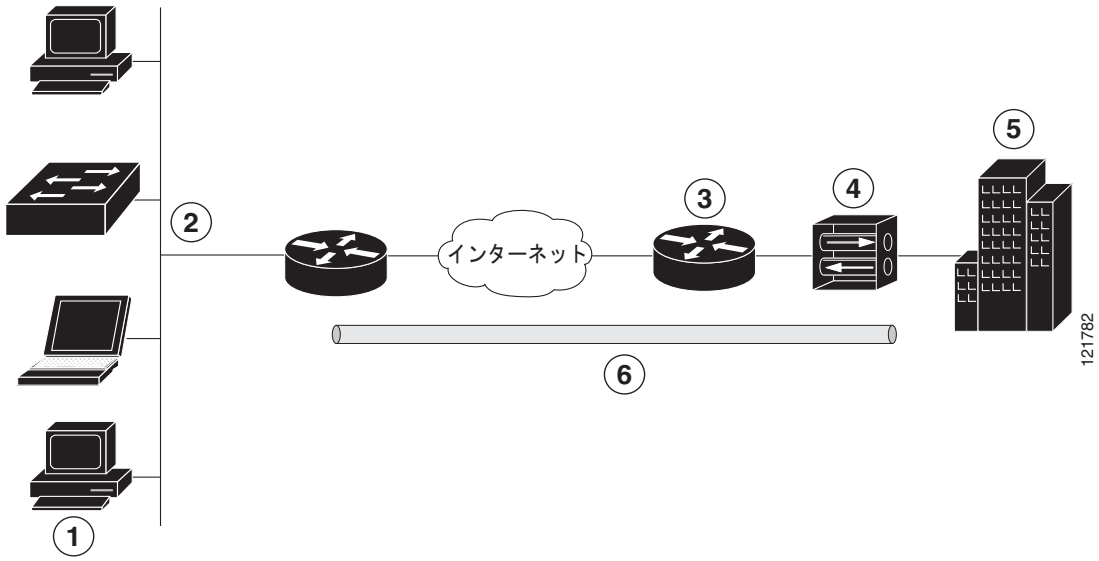
VPN の設定

バーチャル プライベート ネットワーク（VPN）接続は、インターネットなどのパブリック ネットワークを介して、2 つのネットワーク間に安全な接続を提供します。Cisco 3900 シリーズ、2900 シリーズ、および 1900 シリーズ ISR では、サイト間およびリモート アクセスという 2 つのタイプの VPN をサポートしています。リモート アクセス VPN は、企業ネットワークにログインする際にリモート クライアントによって使用されます。サイト間 VPN は、たとえば、ブランチ オフィスと企業オフィスを接続する際に使用されます。この項では、それぞれの例を示します。

リモート アクセス VPN の例

リモート アクセス VPN コンフィギュレーションでは、Cisco Easy VPN および IP Security（IPSec）トンネルを使用して、リモート クライアントとコーポレート ネットワーク間の接続を設定および保護します。図 1 は、一般的な構成例を示します。

図 1　　IPSec トンネルを使用したリモート アクセス VPN



1	リモート ネットワークで接続されたユーザ
2	VPN クライアント：Cisco 3900 シリーズ、2900 シリーズ、または 1900 シリーズ ISR
3	ルータ：コーポレート オフィスのネットワーク アクセスを提供
4	VPN サーバ：Easy VPN サーバ（外部インターフェイス アドレスが 210.110.101.1 の Cisco VPN 3000 コンセントレータなど）
5	ネットワーク アドレスが 10.1.1.1 のコーポレート オフィス
6	IPSec トンネル

Cisco Easy VPN クライアント機能は、Cisco Unity Client プロトコルを実装することにより、面倒な設定作業の大部分を排除します。このプロトコルでは、ほとんどの VPN パラメータ（内部 IP アドレス、内部サブネット マスク、DHCP サーバ アドレス、Windows Internet Naming Service（WINS; Windows インターネット ネーミング サービス）サーバ アドレス、スプリットトンネリング フラグなど）を、VPN サーバ（IPSec サーバとして機能している Cisco VPN 3000 シリーズ コンセントレータなど）に定義することできます。

Cisco Easy VPN サーバ対応のデバイスでは、PC 上で Cisco Easy VPM リモート ソフトウェアを実行しているモバイルおよびリモート作業者が開始した VPN トンネルを終了できます。Cisco Easy VPN サーバ対応のデバイスでは、リモート ルータを Cisco Easy VPN リモート ノードとして動作させることができます。

Cisco Easy VPN クライアント機能は、2 つのモード（クライアント モードまたはネットワーク拡張モード）のいずれかに設定できます。デフォルト設定はクライアント モードで、クライアント サイトの装置だけが中央サイトのリソースにアクセスできます。クライアント サイトのリソースは、中央サイトでは利用できません。ネットワーク拡張モードでは、Cisco VPN 3000 シリーズ コンセントレータが配置されている中央サイトのユーザは、クライアント サイトのネットワーク リソースにアクセスできます。

IPSec サーバの設定を完了すると、IPSec クライアント上で最小限の設定を行って VPN 接続を作成できます。IPSec クライアントが VPN トンネル接続を開始すると、IPSec サーバは IPSec ポリシーを IPSec クライアントに転送し、対応する VPN トンネル接続を作成します。

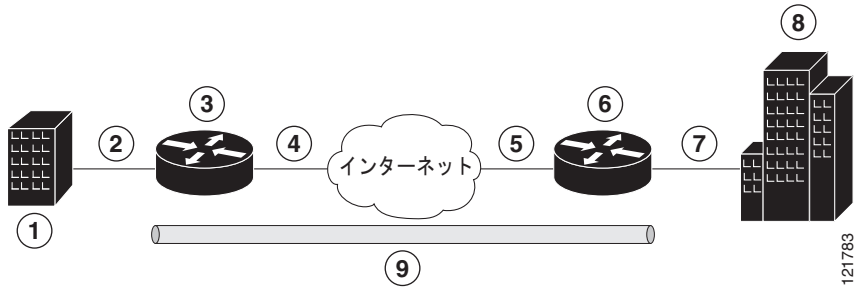
（注） Cisco Easy VPN クライアント機能に設定できるのは、1 つの宛先ピアだけです。アプリケーションで複数の VPN トンネルを作成する必要がある場合、手動でクライアントおよびサーバ側の両方に IPSec VPN および Network Address Translation/Peer Address Translation（NAT/PAT; ネットワーク アドレス変換 / ピア アドレス変換）パラメータを設定する必要があります。

また、Cisco 3900 シリーズ、2900 シリーズ、および 1900 シリーズ ISR を Cisco Easy VPN サーバとして機能するように設定すると、承認されている Cisco Easy VPN クライアントで接続先ネットワークへの 動的 VPN トンネルを確立できるようになります。Cisco Easy VPN サーバの設定については、『*Easy VPN Server*』機能（http://www.cisco.com/en/US/docs/ios/12_2t/12_2t8/feature/guide/ftunity.html）を参照してください。

サイト間 VPN

サイト間 VPN の設定では、IPSec および Generic Routing Encapsulation（GRE; 汎用ルーティング カプセル化）プロトコルを使用して、ブランチ オフィスとコーポレート ネットワーク間の接続を保護します。図 2 は、一般的な構成例を示します。

図 2　IPSec トンネルおよび GRE を使用したサイト間の VPN



1	複数の LAN および VLAN を使用しているブランチ オフィス
2	ファスト イーサネット LAN インターフェイス（NAT 用の内部インターフェイス、アドレスは 192.165.0.0/16）
3	VPN クライアント：Cisco 3900 シリーズ、2900 シリーズ、または 1900 シリーズ ISR
4	ファスト イーサネットまたは ATM インターフェイス（NAT 用の外部インターフェイス、アドレスは 200.1.1.1）
5	LAN インターフェイス（外部インターフェイス アドレスは 210.110.101.1）：インターフェイスに接続
6	VPN クライアント：企業ネットワークへのアクセスを制御する別のルータ
7	LAN インターフェイス（内部インターフェイス アドレスは 10.1.1.1）：企業ネットワークに接続
8	コーポレート オフィス ネットワーク
9	GRE を使用した IPSec トンネル

IPSec および GRE の設定の詳細については、『*Cisco IOS Security Configuration Guide: Secure Connectivity, Release 12.4T*』の「Configuring Security for VPNs with IPSec」（http://www.cisco.com/en/US/docs/ios/sec_secure_connectivity/configuration/guide/12_4t/sec_secure_connectivity_12_4t_book.html）を参照してください。

設定例

各例では、「IPSec トンネル上での VPN の設定」（P.8）の手順を使用して IPSec トンネル上に VPN を設定します。次に、リモート アクセス設定およびサイト間設定の具体的な手順を順番に説明します。

この章の例は、Cisco 3900 シリーズ、2900 シリーズ、および 1900 シリーズ ISR のエンドポイント設定にだけ適用されます。VPN 接続では、機能するためには両方のエンドポイントが正しく設定されていることが必要です。他のルータ モデルでの VPN 設定については、必要に応じてソフトウェア コンフィギュレーション マニュアルを参照してください。

VPN コンフィギュレーション情報は、両方のエンドポイントに設定する必要があります。内部 IP アドレス、内部サブネット マスク、DHCP サーバ アドレス、ネットワーク アドレス変換（NAT）などのパラメータを指定する必要があります。

- 「IPSec トンネル上での VPN の設定」（P.8）
- 「Cisco Easy VPN リモート コンフィギュレーションの作成」（P.17）
- 「サイト間 GRE トンネルの設定」（P.20）

IPSec トンネル上での VPN の設定

IPSec トンネル上に VPN を設定するには、次の作業を行います。

- 「IKE ポリシーの設定」（P.9）
- 「グループ ポリシー情報の設定」（P.10）
- 「クリプト マップへのモード設定の適用」（P.12）
- 「ポリシー ルックアップのイネーブル化」（P.13）
- 「IPSec トランスフォームおよびプロトコルの設定」（P.14）
- 「IPSec 暗号方式およびパラメータの設定」（P.15）
- 「物理インターフェイスへのクリプト マップの適用」（P.16）

- 「次の作業」（P.17）

IKE ポリシーの設定

インターネット キー交換（IKE）ポリシーを設定するには、グローバル コンフィギュレーション モードから始め、次の手順を実行します。

手順の概要

1. **crypto isakmp policy** *priority*
2. **encryption** {**des** | **3des** | **aes** | **aes 192** | **aes 256**}
3. **hash** {**md5** | **sha**}
4. **authentication** {**rsa-sig** | **rsa-encr** | **pre-share**}
5. **group** {**1** | **2** | **5**}
6. **lifetime** *seconds*
7. **exit**
8.

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**crypto isakmp policy** *priority*
	
	例：
	`Router(config)# crypto isakmp policy 1`
	`Router(config-isakmp)#`
		IKE ネゴシエーション時に使用される IKE ポリシーを作成します。プライオリティ番号の範囲は 1 ～ 10000 で、プライオリティが最も高いのは 1 です。
		また、ISAKMP[1] 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 2	**encryption** {**des**	**3des**	**aes**	**aes 192**	**aes 256**}
					
					例：
					`Router(config-isakmp)# encryption 3des`
					`Router(config-isakmp)#`
						IKE ポリシーに使用される暗号化アルゴリズムを指定します。
						この例では、168 ビット DES[2] を指定します。

ステップ 3	**hash** {**md5**	**sha**}
		
		例：
		`Router(config-isakmp)# hash md5`
		`Router(config-isakmp)#`
			IKE ポリシーに使用されるハッシュ アルゴリズムを指定します。
			この例では、MD5[3] アルゴリズムを指定します。デフォルト値は SHA-1 です[4]。

ステップ 4	**authentication** {**rsa-sig**	**rsa-encr**	**pre-share**}
			
			例：
			`Router(config-isakmp)# authentication pre-share`
			`Router(config-isakmp)#`
				IKE ポリシーに使用される認証方式を指定します。
				この例では、事前共有キーを指定します。

	コマンドまたはアクション	目的

ステップ 5	**group** {**1** | **2** | **5**}
	
	例：
	`Router(config-isakmp)# group 2`
	`Router(config-isakmp)#`
		IKE ポリシーに使用される Diffie-Hellman グループを指定します。

ステップ 6	**lifetime** *seconds*
	
	例：
	`Router(config-isakmp)# lifetime 480`
	`Router(config-isakmp)#`
		IKE SA[5] のライフタイムを 60 ～ 86400 秒に指定します。

ステップ 7	**exit**
	
	例：
	`Router(config-isakmp)# exit`
	`Router(config)#`
		IKE ポリシー コンフィギュレーション モードを終了します。続いて、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。

1. ISAKMP = インターネット セキュリティ アソシエーション キーおよび管理プロトコル
2. DES = データ暗号規格
3. MD5 = メッセージ ダイジェスト 5
4. SHA-1 = Secure Hash 標準
5. SA = セキュリティ アソシエーション

グループ ポリシー情報の設定

グループ ポリシーを設定するには、グローバル コンフィギュレーション モードから始め、次の手順を実行します。

手順の概要

1. **crypto isakmp client configuration group** {*group-name* | *default*}
2. **key** ***name***
3. **dns** ***primary-server***
4. **domain** ***name***
5. **exit**
6. **ip local pool {default | *poolname*} [*low-ip-address* [*high-ip-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	**crypto isakmp client configuration group** {*group-name* | *default*}
	
	例：
	`Router(config)# crypto isakmp client configuration group rtr-remote`
	`Router(config-isakmp-group)#`
		リモート クライアントにダウンロードされる属性を含む IKE ポリシー グループを作成します。
		また、ISAKMP グループ 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 2	**key** *name*
	
	例：
	`Router(config-isakmp-group)# key secret-password`
	`Router(config-isakmp-group)#`
		グループ ポリシーの IKE 事前共有キーを指定します。

ステップ 3	**dns** *primary-server*
	
	例：
	`Router(config-isakmp-group)# dns 10.50.10.1`
	`Router(config-isakmp-group)#`
		グループのプライマリ DNS[1] サーバを指定します。
		wins コマンドを使用して、グループ用の WINS[2] サーバを指定することもできます。

ステップ 4	**domain** *name*
	
	例：
	`Router(config-isakmp-group)# domain company.com`
	`Router(config-isakmp-group)#`
		グループのドメイン メンバーシップを指定します。

ステップ 5	**exit**
	
	例：
	`Router(config-isakmp-group)# exit`
	`Router(config)#`
		IKE グループ ポリシー コンフィギュレーション モードを終了します。続いて、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 6	**ip local pool** {**default** | *poolname*} [*low-ip-address* [*high-ip-address*]]
	
	例：
	`Router(config)# ip local pool dynpool 30.30.30.20 30.30.30.30`
	`Router(config)#`
		グループのローカル アドレス プールを指定します。
		このコマンドの詳しい説明およびその他の設定可能なパラメータについては、『*Cisco IOS Dial Technologies Command Reference*』を参照してください。

1. DNS = ドメイン ネーム システム
2. WINS = Windows インターネット ネーム サービス

クリプト マップへのモード設定の適用

クリプト マップにモード設定を適用するには、グローバル コンフィギュレーション モードから始め、次の手順を実行します。

手順の概要

1. **crypto map** *map-name* **isakmp authorization list** *list-name*
2. **crypto map** *tag* **client configuration address** [**initiate** | **respond**]

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**crypto map** *map-name* **isakmp authorization list** *list-name*
	
	例：
	`Router(config)# crypto map dynmap isakmp authorization list rtr-remote`
	`Router(config)#`
		クリプト マップにモード設定を適用し、AAA サーバからのグループ ポリシーのキー ルックアップ（IKE クエリ）をイネーブルにします。

ステップ 2	**crypto map** *tag* **client configuration address** [**initiate**	**respond**]
		
		例：
		`Router(config)# crypto map dynmap client configuration address respond`
		`Router(config)#`
			リモート クライアントからのモード設定要求にルータが応答するように設定します。

ポリシー ルックアップのイネーブル化

AAA 経由でポリシー ルックアップをイネーブルにするには、グローバル コンフィギュレーション モードから始め、次の手順を実行します。

手順の概要

1. **aaa new-model**
2. **aaa authentication login** {**default** | *list-name*} *method1* [*method2...*]
3. **aaa authorization** {**network** | **exec** | **commands** *level* | **reverse-access** | **configuration**} {**default** | *list-name*} [*method1* [*method2...*]]
4. **username** *name* {**nopassword** | **password** *password* | **password** *encryption-type encrypted-password*}

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**aaa new-model**
	
	例：
	`Router(config)# aaa new-model`
	`Router(config)#`
		AAA アクセス コントロール モデルをイネーブルにします。

ステップ 2	**aaa authentication login** {**default**	*list-name*} *method1* [*method2...*]
		
		例：
		`Router(config)# aaa authentication login rtr-remote local`
		`Router(config)#`
			選択したユーザのログイン時の AAA 認証を指定し、使用する方式を指定します。
			
			この例では、ローカル認証データベースを使用します。RADIUS サーバを使用することもできます。詳細については、『*Cisco IOS Security Configuration Guide: Securing User Services, Release 2.4T*』および『*Cisco IOS Security Command Reference*』を参照してください。

ステップ 3	**aaa authorization** {**network**	**exec**	**commands** *level*	**reverse-access**	**configuration**} {**default**	*list-name*} [*method1* [*method2...*]]
						
						例：
						`Router(config)# aaa authorization network rtr-remote local`
						`Router(config)#`
							PPP を含むすべてのネットワーク関連サービス要求の AAA 許可を指定してから、さらに許可方式を指定します。
							
							この例では、ローカル許可データベースを使用します。RADIUS サーバを使用することもできます。詳細については、『*Cisco IOS Security Configuration Guide: Securing User Services, Release 2.4T*』および『*Cisco IOS Security Command Reference*』を参照してください。

ステップ 4	**username** *name* {**nopassword**	**password** *password*	**password** *encryption-type encrypted-password*}
			
			例：
			`Router(config)# username username1 password 0 password1`
			`Router(config)#`
				ユーザ名をベースとした認証システムを構築します。
				
				この例では、暗号化パスワード *password1* を使用して、ユーザ名 *username1* を実装します。

IPSec トランスフォームおよびプロトコルの設定

トランスフォーム セットは、特定のセキュリティ プロトコルとアルゴリズムを組み合わせたものです。IKE のネゴシエーション中に、ピアは特定のトランスフォーム セットを使用してデータ フローを保護することに合意します。

IKE のネゴシエーション中に、ピアは、複数のトランスフォーム セットの中から両方のピアで同一のトランスフォーム セットを検索します。このようなトランスフォームが含まれているトランスフォーム セットが検出された場合は、両方のピアの設定の一部として選択され、保護対象トラフィックに適用されます。

IPSec トランスフォーム セットおよびプロトコルを指定するには、グローバル コンフィギュレーション モードから始め、次の手順を実行します。

手順の概要

1. **crypto ipsec profile** ***profile-name***
2. **crypto ipsec transform-set** *transform-set-name*
3. **crypto ipsec security-association lifetime** {**seconds** *seconds* | **kilobytes** *kilobytes*}

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**crypto ipsec profile** *profile-name*
	
	例：
	`Router(config)# crypto ipsec profile pro1`
	`Router(config)#`
		IPSec プロファイルを設定し、暗号化用にトンネル上で保護を適用します。

ステップ 2	**crypto ipsec transform-set** *transform-set-name transform1* [*transform2*] [*transform3*] [*transform4*]
	
	例：
	`Router(config)# crypto ipsec transform-set vpn1 esp-3des esp-sha-hmac`
	`Router(config)#`
		トランスフォーム セット（IPSec セキュリティ プロトコルとアルゴリズムの有効な組み合わせ）を定義します。
		有効なトランスフォームおよび組み合わせの詳細については、『*Cisco IOS Security Command Reference*』を参照してください。

ステップ 3	**crypto ipsec security-association lifetime** {**seconds** *seconds*	**kilobytes** *kilobytes*}
		
		例：
		`Router(config)# crypto ipsec security-association lifetime seconds 86400`
		`Router(config)#`
			IPSec SA ネゴシエーション時のグローバル ライフタイム値を指定します。
			詳細については、『*Cisco IOS Security Command Reference*』を参照してください。

IPSec 暗号方式およびパラメータの設定

ダイナミック クリプト マップ ポリシーでは、ルータがすべてのクリプト マップ パラメータ（IP アドレスなど）を認識していない場合でも、リモート IPSec ピアからの新規の SA のネゴシエーション要求を処理します。

IPSec 暗号方式を設定するには、グローバル コンフィギュレーション モードから始め、次の手順を実行します。

手順の概要

1. **crypto dynamic-map** *dynamic-map-name dynamic-seq-num*
2. **set transform-set** ***transform-set-name*** **[*transform-set-name2...transform-set-name6*]**
3. **reverse-route**
4. **exit**
5. **crypto map** ***map-name seq-num*** **[ipsec-isakmp] [dynamic** ***dynamic-map-name*****] [discover] [profile** ***profile-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	**crypto dynamic-map** *dynamic-map-name dynamic-seq-num*
	
	例：
	`Router(config)# crypto dynamic-map dynmap 1`
	`Router(config-crypto-map)#`
		ダイナミック クリプト マップ エントリを作成し、クリプト マップ コンフィギュレーション モードを開始します。
		
		このコマンドの詳細については、『*Cisco IOS Security Command Reference*』を参照してください。

ステップ 2	**set transform-set** *transform-set-name* [*transform-set-name2...transform-set-name6*]
	
	例：
	`Router(config-crypto-map)# set transform-set vpn1`
	`Router(config-crypto-map)#`
		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 3	**reverse-route**
	
	例：
	`Router(config-crypto-map)# reverse-route`
	`Router(config-crypto-map)#`
		クリプト マップ エントリの送信元プロキシ情報を作成します。
		
		詳細については、『*Cisco IOS Security Command Reference*』を参照してください。

	コマンドまたはアクション	目的

ステップ 4	**exit**
	
	例：
	`Router(config-crypto-map)# exit`
	`Router(config)#`
		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 5	**crypto map** *map-name seq-num* [**ipsec-isakmp**] [**dynamic** *dynamic-map-name*] [**discover**] [**profile** *profile-name*]
	
	例：
	`Router(config)# crypto map static-map 1 ipsec-isakmp dynamic dynmap`
	`Router(config)#`
		クリプト マップ プロファイルを作成します。

物理インターフェイスへのクリプト マップの適用

クリプト マップは、IPSec トラフィックが通過する各インターフェイスに適用されている必要があります。物理インターフェイスにクリプト マップを適用することにより、ルータがすべてのトラフィックを SA データベースに照合するようになります。デフォルト設定では、ルータはリモート サイト間に送信されるトラフィックを暗号化して、安全な接続を提供します。ただし、パブリック インターフェイスでは他のトラフィックの通過を許可し、インターネットへの接続を提供しています。

インターフェイスにクリプト マップを適用するには、グローバル コンフィギュレーション モードから始め、次の手順を実行します。

手順の概要

1. **interface** *type number*
2. **crypto map** *map-name*
3. **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	**interface** *type number*
	
	例：
	`Router(config)# interface fastethernet 4`
	`Router(config-if)#`
		クリプト マップを適用するインターフェイスのインターフェイス コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的

ステップ 2	**crypto map** *map-name*
	
	例：
	`Router(config-if)# crypto map static-map`
	`Router(config-if)#`
		クリプト マップをインターフェイスに適用します。
		
		このコマンドの詳細については、『*Cisco IOS Security Command Reference*』を参照してください。

ステップ 3	**exit**
	
	例：
	`Router(config-crypto-map)# exit`
	`Router(config)#`
		グローバル コンフィギュレーション モードに戻ります。

次の作業

Cisco Easy VPN リモート コンフィギュレーションを作成する場合は、「Cisco Easy VPN リモート コンフィギュレーションの作成」（P.17）を参照してください。

IPSec トンネルおよび GRE を使用してサイト間 VPN を作成する場合は、「サイト間 GRE トンネルの設定」（P.20）を参照してください。

Cisco Easy VPN リモート コンフィギュレーションの作成

Cisco Easy VPN クライアントとして動作しているルータでは、Cisco Easy VPN リモート コンフィギュレーションを作成し、それを発信インターフェイスに割り当てる必要があります。

リモート コンフィギュレーションを作成するには、グローバル コンフィギュレーション モードから始め、次の手順を実行します。

手順の概要

1. **crypto ipsec client ezvpn** *name*
2. **group** ***group-name*** **key** ***group-key***
3. **peer** {***ipaddress*** | ***hostname***}
4. **mode {client | network-extension | network extension plus}**
5. **exit**
6. **crypto isakmp keepalive** *seconds*
7. **interface** ***type number***
8. **crypto ipsec client ezvpn** ***name*** **[outside | inside]**
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	**crypto ipsec client ezvpn** *name*
	
	例：
	`Router(config)# crypto ipsec client ezvpn ezvpnclient`
	`Router(config-crypto-ezvpn)#`
		Cisco Easy VPN リモート コンフィギュレーションを作成します。続いて、Cisco Easy VPN リモート コンフィギュレーション モードを開始します。

ステップ 2	**group** *group-name* **key** *group-key*
	
	例：
	`Router(config-crypto-ezvpn)# group ezvpnclient key secret-password`
	`Router(config-crypto-ezvpn)#`
		VPN 接続の IPSec グループおよび IPSec キー値を指定します。

ステップ 3	**peer** {*ipaddress* | *hostname*}
	
	例：
	`Router(config-crypto-ezvpn)# peer 192.168.100.1`
	`Router(config-crypto-ezvpn)#`
		VPN 接続のピア IP アドレスまたはホスト名を指定します。
		
		（注） ホスト名を指定できるのは、ルータから DNS サーバを介してホスト名解決を行える場合だけです。
		
		（注） このコマンドを使用して、バックアップとして使用する複数のピアを設定します。1 つのピアがダウンすると、次に使用可能なピアを用いて Easy VPN トンネルが確立されます。プライマリ ピアが再起動すると、プライマリ ピアを用いてトンネルが再確立されます。

ステップ 4	**mode** {**client** | **network-extension** | **network extension plus**}
	
	例：
	`Router(config-crypto-ezvpn)# mode client`
	`Router(config-crypto-ezvpn)#`
		VPN 動作モードを指定します。

ステップ 5	**exit**
	
	例：
	`Router(config-crypto-ezvpn)# exit`
	`Router(config)#`
		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 6	**crypto isakmp keepalive** *seconds*
	
	例：
	`Router(config-crypto-ezvpn)# crypto isakmp keepalive 10`
	`Router(config)#`
		デッド ピア検出メッセージがイネーブルになります。メッセージ間の時間は、秒単位で 10 ～ 3600 の範囲で指定します。

	コマンドまたはアクション	目的

ステップ 7	**interface** *type number*
	
	例：
	`Router(config)# interface fastethernet 4`
	`Router(config-if)#`
		Cisco Easy VPN リモート コンフィギュレーションを適用するインターフェイスでインターフェイス コンフィギュレーション モードを開始します。
		（注） ATM WAN インターフェイスを使用しているルータの場合、このコマンドは **interface atm 0** になります。

ステップ 8	**crypto ipsec client ezvpn** *name* [**outside** | **inside**]
	
	例：
	`Router(config-if)# crypto ipsec client ezvpn ezvpnclient outside`
	`Router(config-if)#`
		WAN インターフェイスに Cisco Easy VPN リモート コンフィギュレーションを割り当てることにより、ルータが VPN 接続に必要な NAT または PAT[1]、およびアクセス リスト コンフィギュレーションを自動作成します。

ステップ 9	**exit**
	
	例：
	`Router(config-crypto-ezvpn)# exit`
	`Router(config)#`
		グローバル コンフィギュレーション モードに戻ります。

1. PAT = ポート アドレス変換

設定例

次の設定例は、この章で説明した VPN および IPSec トンネルのコンフィギュレーション ファイルの一部を示します。

```
!
aaa new-model
!
aaa authentication login rtr-remote local
aaa authorization network rtr-remote local
aaa session-id common
!
username username1 password 0 password1
!
crypto isakmp policy 1
    encryption 3des
    authentication pre-share
    group 2
    lifetime 480
!
crypto isakmp client configuration group rtr-remote
    key secret-password
    dns 10.50.10.1 10.60.10.1
    domain company.com
    pool dynpool
!
crypto ipsec transform-set vpn1 esp-3des esp-sha-hmac
!
crypto ipsec security-association lifetime seconds 86400
!
crypto dynamic-map dynmap 1
    set transform-set vpn1
    reverse-route
!
crypto map static-map 1 ipsec-isakmp dynamic dynmap
```

```
crypto map dynmap isakmp authorization list rtr-remote
crypto map dynmap client configuration address respond

crypto ipsec client ezvpn ezvpnclient
    connect auto
    group 2 key secret-password
    mode client
    peer 192.168.100.1
!

interface fastethernet 4
    crypto ipsec client ezvpn ezvpnclient outside
    crypto map static-map
!
interface vlan 1
    crypto ipsec client ezvpn ezvpnclient inside
!
```

サイト間 GRE トンネルの設定

サイト間 GRE トンネルを設定するには、グローバル コンフィギュレーション モードから始め、次の手順を実行します。

手順の概要

1. **interface** *type number*
2. **ip address** ***ip-address mask***
3. **tunnel source** ***interface-type number***
4. **tunnel destination** ***default-gateway-ip-address***
5. **crypto map** ***map-name***
6. **exit**
7. **ip access-list {standard | extended}** ***access-list-name***
8. **permit** ***protocol source source-wildcard destination destination-wildcard***
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	**interface** *type number*
	
	例：
	`Router(config)# interface tunnel 1`
	`Router(config-if)#`
		トンネル インターフェイスを作成します。続いて、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 2	**ip address** *ip-address mask*
	
	例：
	`Router(config-if)# 10.62.1.193 255.255.255.252`
	`Router(config-if)#`
		トンネルにアドレスを割り当てます。

	コマンドまたはアクション	目的

ステップ 3	**tunnel source** *interface-type number*
	
	例：
	`Router(config-if)# tunnel source fastethernet 0`
	`Router(config-if)#`
		GRE トンネルにルータの送信元エンドポイントを指定します。

ステップ 4	**tunnel destination** *default-gateway-ip-address*
	
	例：
	`Router(config-if)# tunnel destination 192.168.101.1`
	`Router(config-if)#`
		GRE トンネルにルータの宛先エンドポイントを指定します。

ステップ 5	**crypto map** *map-name*
	
	例：
	`Router(config-if)# crypto map static-map`
	`Router(config-if)#`
		トンネルにクリプト マップを割り当てます。
		（注） トンネル インターフェイスへのダイナミック ルーティングまたはスタティック ルートは、サイト間の接続を確立するために設定しておく必要があります。詳細については、『*Cisco IOS Security Configuration Guide: Secure Connectivity, Release 12.4T*』を参照してください。

ステップ 6	**exit**
	
	例：
	`Router(config-if)# exit`
	`Router(config)#`
		インターフェイス 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	**ip access-list** {**standard** | **extended**} *access-list-name*
	
	例：
	`Router(config)# ip access-list extended vpnstatic1`
	`Router(config-acl)#`
		クリプト マップに使用されている名前付き ACL[1] の ACL 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	**permit** *protocol source source-wildcard destination destination-wildcard*
	
	例：
	`Router(config-acl)# permit gre host 192.168.100.1 host 192.168.101.1`
	`Router(config-acl)#`
		発信インターフェイスでは GRE トラフィックだけが許可されるように指定します。

ステップ 9	**exit**
	
	例：
	`Router(config-acl)# exit`
	`Router(config)#`
		グローバル コンフィギュレーション モードに戻ります。

1. ACL = アクセス コントロール リスト

設定例

次の設定例は、これまでの項で説明してきた GRP トンネルを使用した、サイト間 VPN のコンフィギュレーション ファイルの一部を示します。

```
!
aaa new-model
!
aaa authentication login rtr-remote local
aaa authorization network rtr-remote local
aaa session-id common
!
username username1 password 0 password1
!
interface tunnel 1
    ip address 10.62.1.193 255.255.255.252

tunnel source fastethernet 0

tunnel destination interface 192.168.101.1

ip route 20.20.20.0 255.255.255.0 tunnel 1

crypto isakmp policy 1
    encryption 3des
    authentication pre-share
    group 2
!
crypto isakmp client configuration group rtr-remote
    key secret-password
    dns 10.50.10.1 10.60.10.1
    domain company.com
    pool dynpool
!
crypto ipsec transform-set vpn1 esp-3des esp-sha-hmac
!
crypto ipsec security-association lifetime seconds 86400
!
crypto dynamic-map dynmap 1
    set transform-set vpn1
    reverse-route
!
crypto map static-map 1 ipsec-isakmp dynamic dynmap
crypto map dynmap isakmp authorization list rtr-remote
crypto map dynmap client configuration address respond
!
! Defines the key association and authentication for IPsec tunnel.
crypto isakmp policy 1
hash md5
authentication pre-share
crypto isakmp key cisco123 address 200.1.1.1
!
!
! Defines encryption and transform set for the IPsec tunnel.
crypto ipsec transform-set set1 esp-3des esp-md5-hmac
!
! Associates all crypto values and peering address for the IPsec tunnel.
crypto map to_corporate 1 ipsec-isakmp
 set peer 200.1.1.1
 set transform-set set1
 match address 105
!
!
```

```
! VLAN 1 is the internal home network.
interface vlan 1
 ip address 10.1.1.1 255.255.255.0
 ip nat inside
 ip inspect firewall in ! Inspection examines outbound traffic.
    crypto map static-map
    no cdp enable
!
! FE4 is the outside or Internet-exposed interface
interface fastethernet 4
 ip address 210.110.101.21 255.255.255.0
 ! acl 103 permits IPsec traffic from the corp. router as well as
 ! denies Internet-initiated traffic inbound.
 ip access-group 103 in
 ip nat outside
 no cdp enable
 crypto map to_corporate ! Applies the IPsec tunnel to the outside interface.
!
! Utilize NAT overload in order to make best use of the
! single address provided by the ISP.
ip nat inside source list 102 interface Ethernet1 overload
ip classless
ip route 0.0.0.0 0.0.0.0 210.110.101.1
no ip http server
!
!
! acl 102 associated addresses used for NAT.
access-list 102 permit ip 10.1.1.0 0.0.0.255 any
! acl 103 defines traffic allowed from the peer for the IPsec tunnel.
access-list 103 permit udp host 200.1.1.1 any eq isakmp
access-list 103 permit udp host 200.1.1.1 eq isakmp any
access-list 103 permit esp host 200.1.1.1 any
! Allow ICMP for debugging but should be disabled because of security implications.
access-list 103 permit icmp any any
access-list 103 deny ip any any ! Prevents Internet-initiated traffic inbound.
! acl 105 matches addresses for the IPsec tunnel to or from the corporate network.
access-list 105 permit ip 10.1.1.0 0.0.0.255 192.168.0.0 0.0.255.255
no cdp run
```

ダイナミック マルチポイント VPN の設定

Dynamic Multipoint VPN（DMVPN; ダイナミック マルチポイント VPN）機能を使用すると、ユーザは、GRE トンネル、IPsec 暗号化、および Next Hop Resolution Protocol（NHRP; ネクスト ホップ レゾリューション プロトコル）を組み合わせて大規模および小規模な IP セキュリティ（IPsec）VPN を設定できるようになります。

DMVPN の設定に関する追加情報については、『*Cisco IOS Security Configuration Guide: Secure Connectivity, Release 12.4T*』の「Dynamic Multipoint VPN」（http://www.cisco.com/en/US/docs/ios/sec_secure_connectivity/configuration/guide/12_4t/sec_secure_connectivity_12_4t_book.html）を参照してください。

グループ暗号化トランスポート VPN の設定

Group Encrypted Transport（GET; グループ暗号化トランスポート）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 プロトコル Group Domain of Interpretation（GDOI; グループ ドメイン オブ インタープリテーション）と IPsec 暗号化を組み合わせ、IP マルチキャスト 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の効率的な方法をユーザに提供します。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。

ポイント間トンネルが不要になるため、QoS、ルーティング、およびマルチキャストなどの音声およびビデオ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しながら、メッシュ ネットワークをより大規模に設定できます。GET VPN 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、新しい標準ベースの IP セキュリティ（IPsec）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。

GET VPN の設定に関する追加情報については、『*Cisco Group Encrypted Transport VPN*』（http://www.cisco.com/en/US/docs/ios/12_4t/12_4t11/htgetvpn.html）を参照してください。