CHAPTER 5

セキュリティ機能の設定

この章では、Cisco 860 および Cisco 880 シリーズ Integrated Services Routers（ISR; サービス統合型ルータ）で設定可能な特定のセキュリティ機能を実装するシスコの主要なフレームワークである Authentication, Authorization, Accounting（AAA; 認証、許可、アカウンティング）の概要について説明します。

この章で説明する内容は、次のとおりです。

AAA

AAA のネットワーク セキュリティ サービスは、ルータ上でアクセス制御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、ユーザを識別する手段を提供します。これには、ログインおよびパスワード ダイアログ、チャレンジ/応答、メッセージ サポート、および暗号化（選択したセキュリティ プロトコルに基づく）などがあります。許可は、リモート アクセス制御の手段を提供します。これには、一時的な許可またはサービスごとの許可、ユーザ単位のアカウント リストおよびプロファイル、ユーザ グループのサポート、および IP、Internetwork Packet Exchange（IPX）、AppleTalk Remote Access（ARA）、Telnet のサポートなどがあります。アカウンティングは、ユーザ ID、開始時刻および終了時刻、実行されたコマンド（PPP など）、パケット数、およびバイト数などの課金、監査、および報告に使用するセキュリティ サーバ情報の収集および送付を行う手段を提供します。

AAA は RADIUS、TACACS+、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の管理を行います。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 サーバ間で通信を確立する手段となります。

AAA サービスの設定およびサポートされているセキュリティ プロトコルの詳細については、http://www.cisco.com/en/US/docs/ios/security/configuration/guide/12_4t/sec_12_4t_book.html の『*Cisco IOS Release 12.4T Security Configuration Guide*』で次の各セクションを参照してください。

- 「Configuring Authentication」
- 「Configuring Authorization」
- 「Configuring Accounting」
- 「Configuring RADIUS」
- 「Configuring TACACS+」
- 「Configuring Kerberos」

AutoSecure の設定

AutoSecure 機能は、ネットワーク攻撃の対象になる可能性のある一般的な IP サービスを無効にして、攻撃時のネットワークの防御に役立つ IP サービスと機能を有効します。これらの IP サービスは、コマンドを 1 回使用するだけで一度に無効および有効に設定されるため、ルータのセキュリティ設定が大幅に簡素化されます。AutoSecure 機能の詳細については、http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123_1/ftatosec.htm の *AutoSecure* 機能のマニュアル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 ACL 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でネットワーク トラフィックの許可または拒否を行います。アクセス リストは、標準アクセス リストまたは拡張アクセス リストとして設定します。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 リストの場合は、宛先と送信元の両方を指定でき、個別のプロトコルの通過を許可または拒否するように指定できます。

アクセス リストの作成の詳細については、http://www.cisco.com/en/US/docs/ios/security/configuration/guide/12_4/sec_12_4_book.html で『*Cisco IOS Release 12.4 Security Configuration Guide*』の「Access Control Lists: Overview and Guidelines」のセクションを参照してください。

アクセス リストは、共通のタグを使用して結合された一連のコマンドです。タグは番号または名前のいずれかです。表 5-1 は、アクセス リストの設定に使用するコマンドを示しています。

表 5-1　アクセス リストの設定コマンド

ACL タイプ	設定コマンド
番号指定	
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*]
名前指定	
標準	**ip access-list standard** *name* **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 リストを作成、改良、および管理するには、http://www.cisco.com/en/US/docs/ios/security/configuration/guide/12_4t/sec_12_4t_book.html の『*Cisco IOS Release 12.4T Security Configuration Guide*』の「Traffic Filtering, Firewalls, and Virus Detection」で次の各セクション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、共通の名前または番号を使用して統合された一連のアクセス リスト設定です。アクセス グループは、インターフェイスの設定時にインターフェイスに対してイネーブルになります。アクセス グループを作成する際には、次の点に注意します。

- アクセス リスト設定の順序は重要です。パケットはシーケンスの最初のアクセス リストと比較されます。一致しない場合（許可または拒否のいずれでもない場合）、パケットは次のアクセス リストと比較され、以降は同様に処理されます。
- パケットを許可または拒否するには、すべてのパラメータがアクセス リストと一致する必要があります。
- すべてのシーケンスの最後には暗黙的な「deny all」が存在しています。

アクセス グループの設定および管理の詳細については、http://www.cisco.com/en/US/docs/ios/security/configuration/guide/12_4t/sec_12_4t_book.html の『*Cisco IOS Release 12.4T Security Configuration Guide*』の「Creating an IP Access List to Filter IP Options, TCP Flags, Noncontiguous Ports, or TTL Values」のセクションを参照してください。

Cisco IOS ファイアウォールの設定

Cisco IOS ファイアウォールを使用すると、パケットを内部で検査し、ネットワーク接続の状態を監視する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 ファイアウォールは、スタティックなアクセス リストよりも優れています。アクセス リストは、パケットのストリームに基づくのではなく、個別のパケットに基づいてトラフィックを許可または拒否するだけだからです。また、Cisco IOS ファイアウォールはパケットの検査を行うため、アプリケーション レイヤのデータを調べてトラフィックの許可または拒否を判断できます。スタティックなアクセス リストでは、このような検査を行うことはできません。

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、検査するプロトコルを指定します。

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

検査によって指定され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検出されると、ダイナミックなアクセス リストが作成されて、戻りトラフィックの通過が許可されます。timeout パラメータでは、ルータを通過する戻りトラフィックが存在しない場合にダイナミック アクセス リストをアクティブにしておく時間を指定します。所定のタイムアウト値が経過すると、ダイナミック アクセス リストは削除されるため、後続のパケット（通常、有効なパケット）は許可されません。

複数のステートメントで同じ検査名を使用すると、それらは 1 つのルール セットにまとめられます。コンフィギュレーションの別の場所でこのルールを有効にするには、ファイアウォールのインターフェイスを設定する際に **ip inspect inspection-name in | out** コマンドを使用します。

Cisco IOS ファイアウォールの設定の詳細については、http://www.cisco.com/en/US/docs/ios/security/configuration/guide/12_4/sec_12_4_book.html で『*Cisco IOS Release 12.4 Security Configuration Guide*』の「Cisco IOS Firewall Overview」のセクションを参照してください。

Cisco IOS ファイアウォールは、Session Initiated Protocol（SIP）アプリケーションのボイス セキュリティを提供するように設定することもできます。SIP 検査は、プロトコルの適合性およびアプリケーションの保護に加え、基本的な検査機能（SIP パケット検査およびピンホールの開きの検出）が提供されます。詳細については、http://www.cisco.com/en/US/docs/ios/security/configuration/guide/sec_sip_alg_aic.html で、「Cisco IOS Firewall: SIP Enhancements: ALG and AIC」を参照してください。

Cisco IOS IPS の設定

Cisco 880 シリーズ ISR で利用可能な 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、不正なネットワーク動作を示したりするパケットおよびフローに適切に対処することによって、境界部分のファイアウォール保護を強化します。

Cisco IOS IPS は、「シグネチャ」を使用してネットワーク トラフィックの悪用パターンを検出します。Cisco IOS IPS は、インライン型の侵入検知装置として機能し、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、既知の IPS シグニチャとの比較を行います。Cisco IOS IPS は、不審な動作を検出すると、ネットワーク セキュリティが破られる前に対処してイベントを記録します。また、設定に応じて、次のいずれかを行います。

- アラームの送信
- 疑わしいパケットの破棄
- 接続のリセット
- 攻撃者のソース IP アドレスからのトラフィックを一定の期間拒否する
- シグネチャが確認された接続のトラフィックを一定の期間拒否する

Cisco IOS IPS の設定の詳細については、http://www.cisco.com/en/US/docs/ios/security/configuration/guide/12_4t/sec_12_4t_book.html で『*Cisco IOS Release 12.4T Security Configuration Guide*』の「Configuring Cisco IOS Intrusion Prevention System (IPS)」のセクションを参照してください。

URL フィルタリング

Cisco 860 シリーズおよび Cisco 880 シリーズ ISR には、URL フィルタリングに基づいたカテゴリがあります。ユーザは、許可またはブロックする Web サイトのカテゴリを選択することで、ISR で URL フィルタリングをプロビジョニングします。サード パーティで管理されている外部のサーバを使用して、それぞれのカテゴリの URL を調べます。許可ポリシーおよび拒否ポリシーは ISR で保守管理します。サービスは加入ベースで、各カテゴリの URL はサード パーティのベンダーが保守管理します。

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

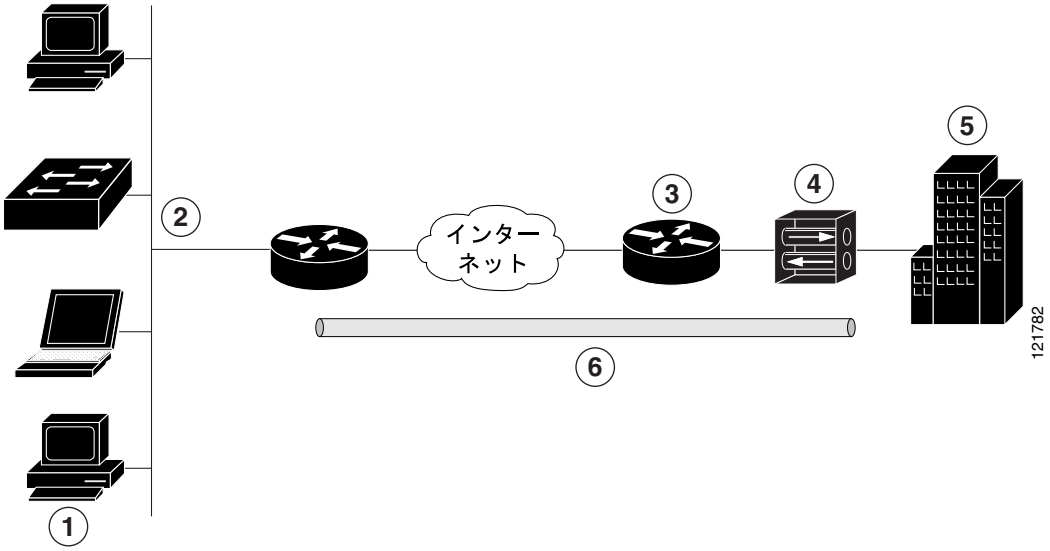
VPN の設定

Virtual Private Network（VPN; 仮想私設網）接続を使用すると、インターネットなどのパブリック ネットワーク上で 2 つのネットワーク間のセキュアな接続を実現できます。Cisco 860 および Cisco 880 シリーズ ISR は、サイト間 VPN およびリモート アクセス VPN の 2 種類の VPN をサポートしています。サイト間 VPN は、ブランチ オフィスとコーポレート オフィスを接続する場合などに使用します。リモート アクセス VPN は、リモート クライアントが企業ネットワークにログインする場合に使用します。リモート アクセス VPN およびサイト間 VPN の両方についてこのセクションで 2 つの例を挙げて説明します。

リモート アクセス VPN

リモート アクセス VPN の設定では、Cisco Easy VPN および IP Security（IPSec）トンネリングを使用して、リモート クライアントと企業のネットワーク間の接続を設定および保護します。図 5-1 は、一般的なネットワーク構成例を示しています。

図 5-1　IPSec トンネルを使用したリモート アクセス VPN



1	リモート ネットワークに接続されたユーザ
2	VPN クライアント：Cisco 880 シリーズ アクセス ルータ
3	ルータ：本社オフィスへのネットワーク 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 アドレスを 210.110.101.1 に設定した Cisco VPN 3000 コンセントレータなど）
5	本社オフィス（ネットワーク アドレス 10.1.1.1 を使用）
6	IPSec トンネル

Cisco Easy VPN クライアントの機能を使用すると、Cisco Unity Client プロトコルを実行して、面倒な設定作業の多くを省略することができます。このプロトコルを使用すると、大半の 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 Services（WINS）サーバ アドレス、およびスプリットトンネリング フラグなど）を VPN サーバ（IPSec サーバとして動作する Cisco VPN 3000 シリーズ コンセントレータなど）で定義できます。

Cisco Easy VPN サーバ対応デバイスは、PC 上で Cisco Easy VPN リモート ソフトウェアを使用しているモバイル ユーザやリモート ユーザが起動した VPN トンネルを終端できます。Cisco Easy VPN サーバ対応装置により、リモート ルータが Easy VPN リモート ノードとして機能することができます。

Cisco Easy VPN クライアントの機能は、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のモードで設定できます。クライアント モードはデフォルト設定です。クライアント モードを使用すると、クライアント サイトのデバイスだけが中央サイトにあるリソースにアクセスできます。クライアント サイトにあるリソースは、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を使用すると、（VPN 3000 シリーズ コンセントレータが配置された）中央サイトのユーザがクライアント サイトのネットワーク リソースにアクセスできます。

IPSec サーバが設定されている場合は、サポート対象の Cisco 880 シリーズ ISR といった IPSec クライアント上で最小限の設定を行うことにより、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 クライアントに IPSec ポリシーを設定し、対応する VPN トンネル接続を作成します。

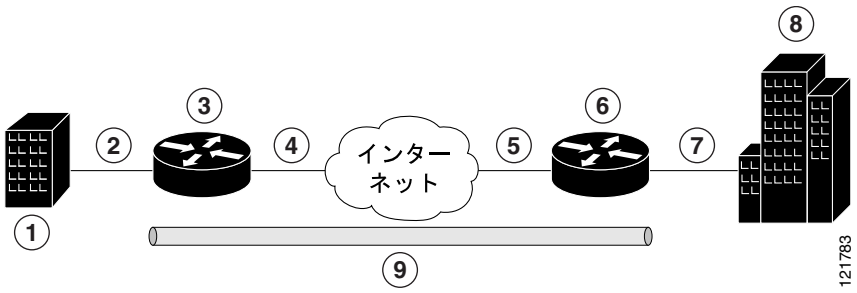
（注）　Cisco Easy VPN クライアントの機能は、宛先ピアを 1 つだけ使用する構成をサポートしています。アプリケーションで複数の VPN トンネルを作成する必要がある場合には、クライアントとサーバの両方で IPSec VPN および Network Address Translation/Peer Address Translation（NAT/PAT; ネットワーク アドレス変換 / ポート アドレス変換）パラメータを手動で設定する必要があります。

Cisco 860 および Cisco 880 シリーズ ISR は、Cisco Easy VPN サーバとして動作するように設定することもでき、この機能を使用すると、許可された Cisco Easy VPN クライアントは接続されたネットワークに対してダイナミックな VPN トンネルを確立できます。Cisco Easy VPN サーバの設定の詳細については、http://www.cisco.com/en/US/docs/ios/12_2t/12_2t8/feature/guide/ftunity.html の「*Easy VPN Server*」の機能のマニュアル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 トンネルと Generic Routing Encapsulation（GRE; 総称ルーティング カプセル化）プロトコルを使用して、ブランチ オフィスと企業ネットワーク間の接続を保護します。図 5-2 は、一般的なネットワーク構成例を示しています。

図 5-2　IPSec トンネルおよび GRE によるサイト間 VPN



1	複数の LAN および VLAN を持つブランチ オフィス
2	ファスト イーサネット LAN インターフェイス：アドレス 192.165.0.0/16（NAT の内部インターフェイス）
3	VPN クライアント：Cisco 860 または Cisco 880 シリーズ ISR
4	ファスト イーサネット ATM インターフェイス：アドレス 200.1.1.1（NAT の内部インターフェイス）

5	LAN インターフェイス：インターネットと接続（外部インターフェイス アドレス 210.110.101.1）
6	VPN クライアント：もう 1 つのルータ（企業ネットワークへのアクセスを制御）
7	LAN インターフェイス：企業ネットワークと接続（内部インターフェイス アドレス 10.1.1.1）
8	本社オフィス 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、http://www.cisco.com/en/US/docs/ios/security/configuration/guide/12_4t/sec_12_4t_book.html で『*Cisco IOS Release 12.4T Security Configuration Guide*』の「Configuring Security for VPNs with IPSec」の章を参照してください。

設定例

設定例ではいずれも「IPSec トンネル上での VPN の設定」（P.5-7）の手順を使用して、IPSec トンネル上に VPN を設定します。その後、リモート アクセス設定、サイト間設定という順にそれぞれの特定の手順を行います。

この章の設定例は、Cisco 860 および Cisco 880 の ISR のエンドポイント設定にだけ適用されます。いずれの VPN 接続も、両端のエンドポイントが適切に機能するように設定されている必要があります。他のルータ モデルで VPN を設定するために、必要に応じてソフトウェア設定マニュアルを参照してください。

VPN の設定情報は、両端のエンドポイントに設定される必要があります。設定する必要のあるパラメータは、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、および Network Address Translation（NAT; ネットワーク アドレス変換）などです。

- 「IPSec トンネル上での VPN の設定」（P.5-7）
- 「Cisco Easy VPN リモート設定の作成」（P.5-14）
- 「GRE トンネルでの Site-to-Site の設定」（P.5-17）

IPSec トンネル上での VPN の設定

次の作業を行って IPSec トンネル上で VPN を設定します。

- 「IKE ポリシーの設定」（P.5-8）
- 「グループ ポリシー情報の設定」（P.5-9）
- 「暗号マップに対するモード設定の適用」（P.5-10）
- 「ポリシー検索のイネーブル化」（P.5-10）
- 「IPSec トランスフォームおよびプロトコルの設定」（P.5-11）
- 「IPSec 暗号方式およびパラメータの設定」（P.5-12）
- 「暗号マップの物理インターフェイスへの適用」（P.5-13）
- 「次の作業」（P.5-14）

IKE ポリシーの設定

Internet Key Exchange（IKE; インターネット鍵交換）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、次の作業を行います。

	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 ネゴシエーションで使用する IKE ポリシーを作成します。プライオリティは 1 ～ 10000 の番号（1 が最高）です。
		このとき、Internet Security Association and Key Management Protocol（ISAKMP）ポリシー コンフィギュレーション モードが開始されます。

ステップ 2	**encryption** {**des** | **3des** | **aes** | **aes 192** | **aes 256**}
	
	例：
	`Router(config-isakmp)# encryption 3des`
	`Router(config-isakmp)#`
		IKE ポリシーで使用する暗号化アルゴリズムを指定します。
		例では、168 ビットの Data Encryption Standard（DES; データ暗号規格）が指定されています。

ステップ 3	**hash** {**md5** | **sha**}
	
	例：
	`Router(config-isakmp)# hash md5`
	`Router(config-isakmp)#`
		IKE ポリシーで使用するハッシュ アルゴリズムを指定します。
		例では、Message Digest 5（MD5）アルゴリズムが指定されています。デフォルトは Secure Hash standard（SHA-1）です。

ステップ 4	**authentication** {**rsa-sig** | **rsa-encr** | **pre-share**}
	
	例：
	`Router(config-isakmp)# authentication pre-share`
	`Router(config-isakmp)#`
		IKE ポリシーで使用する認証方式を指定します。
		例では、事前共有鍵が指定されています。

ステップ 5	**group** {**1** | **2** | **5**}
	
	例：
	`Router(config-isakmp)# group 2`
	`Router(config-isakmp)#`
		IKE ポリシーで使用する 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 Security Association（SA; セキュリティ アソシエーション）のライフタイム（60 ～ 86400 秒）を指定します。

ステップ 7	**exit**
	
	例：
	`Router(config-isakmp)# exit`
	`Router(config)#`
		IKE ポリシーの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 モードに切り替えます。

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、次の作業を行います。

	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格納する IKE ポリシー グループを作成します。
		このとき、Internet Security Association Key and Management Protocol（ISAKMP）グループ ポリシー コンフィギュレーション モードが開始されます。

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 事前共有鍵を指定します。

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 Domain Name System（DNS; ドメイン ネーム システム）サーバを指定します。
		wins コマンドを使用して、グループの Windows Internet Naming Service（WINS）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 ポリシーの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 モードに切り替えます。

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。
		このコマンドの詳細および設定可能なその他の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。

暗号マップに対するモード設定の適用

暗号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、次の作業を行います。

	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)#`
		暗号マップにモード設定を適用し、Authentication, Authorization, Accounting（AAA; 認証、許可、アカウンティング）サーバからのグループ ポリシーの鍵検索（IKE 要求）を有効にします。

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応答するようにルータを設定します。

ポリシー検索のイネーブル化

AAA によるポリシー検索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、次の作業を行います。

	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 アクセス制御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)#`
		特定のユーザに関するログイン時の AAA 認証を設定し、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が使用されます。ここで RADIUS サーバを使用することもできます。詳しくは、『*Cisco IOS Security Configuration Guide*』および『*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 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)#`
		すべてのネットワーク関連サービス要求（PPP など）に関する AAA 許可を設定し、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が使用されます。ここで RADIUS サーバを使用することもできます。詳しくは、『*Cisco IOS Security Configuration Guide*』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 Cisco password 0 Cisco`
	`Router(config)#`
		ユーザ名に基づく認証システムを確立します。
		
		この例では、ユーザ名 *Cisco* と暗号化パスワード *Cisco* を指定しています。

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、セキュリティ プロトコルとアルゴリズムの特定の組み合わせです。IKE ネゴシエーションの実行時に、両ピアはデータ フローを保護するために特定のトランスフォーム セットの使用に同意します。

IKE ネゴシエーションの実行時に、両ピアは、複数のトランスフォーム セットから両ピアに共通するトランスフォームを検索します。このようなトランスフォームを含むトランスフォーム セットが見つかると、そのセットが選択され、両ピアのコンフィギュレーションの一部として、そのセットが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、次の作業を行います。

	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)#`
		トンネルに暗号化が適用されるように IPSec プロファイルを設定します。

	コマンドまたはアクション	目的

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 プロトコルおよびアルゴリズムの使用可能な組み合わせ）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 セキュリティ アソシエーション（SA）のネゴシエート時に使用されるグローバル ライフタイムの値を指定します。
		
		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

ダイナミック暗号マップ ポリシーは、ルータがすべての暗号マップ 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 ピアからの新しいセキュリティ アソシエーション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、次の作業を行います。

	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)#`
		ダイナミック暗号マップ エントリを作成して、暗号マップ 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)#`
		暗号マップ 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)#`
		暗号マップ 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)#`
		暗号マップ プロファイルを作成します。

暗号マップの物理インターフェイスへの適用

暗号マップは、IPSec トラフィックが流れる各インターフェイスに適用する必要があります。物理インターフェイスに暗号マップを適用すると、ルータはすべてのトラフィックをセキュリティ アソシエーション データベースに対して評価するようになります。デフォルト設定の場合、ルータは接続を保護するためにリモート サイト間で送信されるトラフィックを暗号化します。この場合、パブリック インターフェイスを使用して、他のトラフィックの伝送やインターネットとの接続を利用することが可能です。

インターフェイスに暗号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、次の作業を行います。

	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)#`
		暗号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。

ステップ 2	**crypto map** *map-name*
	
	例：
	`Router(config-if)# crypto map static-map`
	`Router(config-if)#`
		暗号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 リモート設定を作成している場合は、「Cisco Easy VPN リモート設定の作成」（P.5-14）の作業を行います。

IPSec トンネルおよび GRE を使用したサイト間 VPN を作成している場合は、「GRE トンネルでの Site-to-Site の設定」（P.5-17）の作業を行います。

Cisco Easy VPN リモート設定の作成

Cisco Easy VPN クライアントとして機能するルータでは、Cisco Easy VPN リモートの設定を作成して、発信インターフェイスにこの設定を関連付ける必要があります。

リモートの設定を作成するには、グローバル コンフィギュレーション モードから、次の作業を行います。

	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 リモートの設定を作成し、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 接続用の IPSec グループおよび IPSec キーの値を指定します。

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、ルータが DNS サーバを使用してホスト名を解決できる場合だけです。
		（注） このコマンドを使用して両ピアをバックアップとして使用するように設定します。一方のピアがダウンすると、利用可能な 2 番目のピアで Easy VPN トンネルが確立されます。最初のピアが復旧したら、トンネルは最初のピアで再確立されます。

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

	コマンドまたはアクション	目的

ステップ 5	**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)#`
		不能になったピアの検出メッセージをイネーブルにします。メッセージの時間間隔は、10 ～ 3600 の *seconds* 単位で指定します。

ステップ 7	**interface** *type number*
	
	例：
	`Router(config)# interface fastethernet 4`
	`Router(config-if)#`
		Cisco Easy VPN リモートの設定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備え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)#`
		Cisco Easy VPN リモートの設定を WAN インターフェイスに関連付けます。これにより、ルータは VPN 接続に必要な NAT または Port Address Translation（PAT; ポート アドレス変換）、およびアクセス リストの設定を自動的に作成します。

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。

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 ファイルの一部です。

```
!
aaa new-model
!
aaa authentication login rtr-remote local
aaa authorization network rtr-remote local
aaa session-id common
!
username Cisco password 0 Cisco
!
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
!
```

GRE トンネルでの Site-to-Site の設定

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、次の作業を行います。

	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、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。

ステップ 3	**tunnel source** *interface-type number*
	
	例：
	`Router(config-if)# tunnel source fastethernet 0`
	`Router(config-if)#`
		GRE トンネルに対する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 トンネルに対する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)#`
		トンネルに暗号マップを割り当てます。
		
		（注） サイト間で接続を確立するには、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 ルートを設定する必要があります。詳細については、『*Cisco IOS Security Configuration Guide*』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。

	コマンドまたはアクション	目的

ステップ 7	**ip access-list** {**standard** | **extended**} *access-list-name*
	
	例：
	`Router(config)# ip access-list extended vpnstatic1`
	`Router(config-acl)#`
		暗号マップで使用される名前付き ACL 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上で GRE トラフィックだけを許可するように設定します。

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。

設定例

次の設定例は、前述の各項で説明した GRE トンネルによる VPN のコンフィギュレーション ファイルの一部です。

```
!
aaa new-model
!
aaa authentication login rtr-remote local
aaa authorization network rtr-remote local
aaa session-id common
!
username cisco password 0 cisco
!
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
```