CHAPTER 13

Easy VPN および IPSec トンネルを使用した VPN の設定

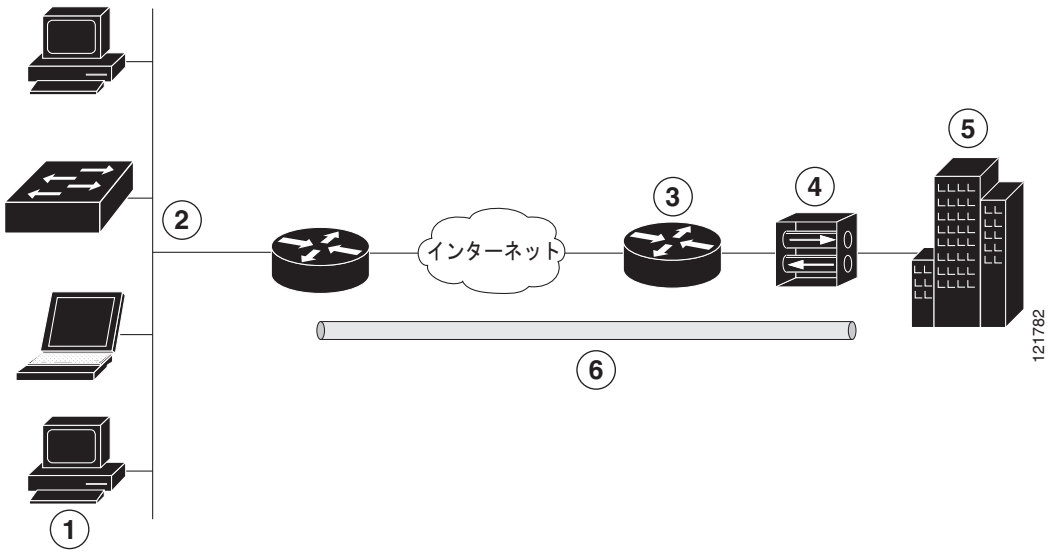
この章では、Cisco 819 サービス統合型ルータ（ISR）で設定できるバーチャル プライベート ネットワーク（VPN）の作成の概要について説明します。

Cisco ルータと他のブロードバンド デバイスは、インターネットへの高パフォーマンスな接続を提供しますが、多くのアプリケーションでは、高レベルの認証を実行し、2 つの特定のエンドポイント間でデータを暗号化する VPN 接続のセキュリティも必要です。

サイト間とリモート アクセスの 2 種類の VPN がサポートされます。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、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。

この章の例は、Cisco Easy VPN と IPSec トンネルを使用してリモート クライアントと企業ネットワーク間の接続を設定し、セキュアにするリモート アクセス VPN の構成を示しています。図 13-1 は、一般的な構成例を示します。

図 13-1　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 819 ISR
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
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

Cisco Easy VPN クライアント機能を使用し、Cisco Unity Client プロトコルを実装することにより、面倒な設定作業が大幅に削減されます。このプロトコルでは、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、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、ほとんどの VPN パラメータを IPSec サーバとして機能している VPN サーバで定義できます。

Easy VPN サーバ対応のデバイスでは、PC 上で Cisco Easy VPN 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。Easy VPN サーバ対応のデバイスでは、リモート ルータを 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、クライアント モードとネットワーク拡張モードの 2 つの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、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 サーバを設定したら、サポート対象の Cisco 819 ISR などの 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 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 クライアント機能で設定できるのは、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 およびネットワーク アドレス変換 / ピア アドレス変換（NAT/PAT）パラメータを設定する必要があります。

設定作業

このネットワーク シナリオのルータを設定するには、次の作業を実行します。

- 「IKE ポリシーの設定」（P.13-3）
- 「グループ ポリシー情報の設定」（P.13-5）
- 「クリプト マップへのモード設定の適用」（P.13-6）
- 「ポリシー ルックアップのイネーブル化」（P.13-7）
- 「IPSec トランスフォームおよびプロトコルの設定」（P.13-8）
- 「IPSec 暗号方式およびパラメータの設定」（P.13-9）
- 「物理インターフェイスへのクリプト マップの適用」（P.13-10）
- 「Easy VPN リモート コンフィギュレーションの作成」（P.13-11）

この設定タスクの結果を示す例は「設定例」（P.13-13）で提供されます。

（注）　この章の手順では、基本的なルータ機能と、NAT、DCHP、および VLAN を使用した PPPoE または PPPoA がすでに設定されていることを前提とします。これらの設定作業を実行していない場合、「ルータの基本設定」（P.5-1）を参照してください。

（注）　この章の例は、Cisco 819 ルータのエンドポイント設定だけを示しています。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。

IKE ポリシーの設定

インターネット キー交換（IKE）を設定するには、グローバル コンフィギュレーション モードを開始し、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**

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、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（ISAKMP）ポリシー コンフィギュレーション モードを開始します。

ステップ 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 データ暗号規格（DES）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、Message Digest 5（MD5）アルゴリズムを指定します。デフォルトは、Secure Hash 標準（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。

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。

	コマンドまたはアクション	目的

ステップ 6	**lifetime** *seconds*
	
	例：
	`Router(config-isakmp)# lifetime 480`
	`Router(config-isakmp)#`
		IKE セキュリティ アソシエーション（SA）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 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。

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 モードを開始し、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。

	コマンドまたはアクション	目的

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 ドメイン ネーム システム（DNS）サーバを指定します。
		（注） **wins** コマンドを使用して、グループに 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 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。

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 モードを開始し、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、認証、許可、アカウンティング（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 を使用してポリシー 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 モードを開始し、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、『*Securing User Services Configuration Guide Library, Cisco IOS Release 12.4T*』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、『*Securing User Services Configuration Guide Library, Cisco IOS Release 12.4T*』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 Cisco password 0 Cisco`
	`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、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、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 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 セットが検出された場合は、それが選択され、両方のピアの設定の一部として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 セットと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 モードを開始し、次の手順を実行します。

手順の概要

1. **crypto ipsec transform-set** *transform-set-name transform1* [*transform2*] [*transform3*] [*transform4*]
2. **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 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 2	**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。

（注）　手動で確立したセキュリティ アソシエーションの場合は、ピアとのネゴシエーションが存在しないため、両方に同じトランスフォーム セットを指定する必要があります。

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 モードを開始し、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。

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、IP セキュリティ（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 モードを開始し、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。

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。

Easy VPN リモート コンフィギュレーションの作成

IPSec リモート ルータとして機能するルータは、Easy VPN リモート コンフィギュレーションを作成し、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 モードを開始し、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. **interface** *type number*
7. **crypto ipsec client ezvpn** *name* [**outside** | **inside**]
8. **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 Remote コンフィギュレーションを作成し、Cisco Easy VPN Remote 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。

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	**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。

	コマンドまたはアクション	目的

ステップ 7	**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 またはポート アドレス変換（PAT）、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 8	**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。

Easy VPN の設定の検証

次の例では、Easy VPN の接続を確認します。

```
Router# show crypto ipsec client ezvpn

Tunnel name :ezvpnclient
Inside interface list:vlan 1
Outside interface:fastethernet 4
Current State:IPSEC_ACTIVE
Last Event:SOCKET_UP
Address:8.0.0.5
Mask:255.255.255.255
Default Domain:cisco.com
```

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 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
!
```