IPSec トンネルと汎用ルーティング カプセル化を使用した VPN の設定

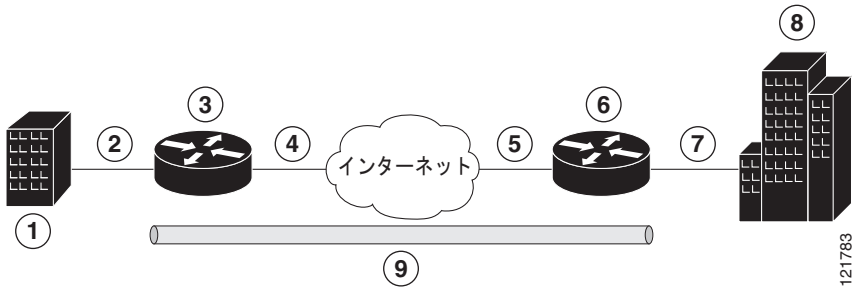
Cisco 1800 シリーズ サービス統合型固定構成ルータは Virtual Private Network（VPN; バーチャル プライベート ネットワーク）の作成をサポートします。

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、IPSec と 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、支店オフィスと企業ネットワーク間の接続をセキュアにするサイト間 VPN の設定を示します。図 7-1 は、一般的な構成例を示します。

図 7-1　　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 1800 シリーズ サービス統合型ルータ
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：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	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

GRE トンネル

GRE トンネルは通常、Cisco ルータと、企業ネットワークなどのプライベート ネットワークへのアクセスを制御するリモート デバイス間で VPN を確立するために使用されます。GRE トンネルから転送されたトラフィックはカプセル化され、ルータの物理インターフェイスにルーティングされます。GRE インターフェイスが使用されている場合、Cisco ルータと、企業ネットワークへのアクセスを制御するルータは、トンネルを介してルーティング更新情報を交換し、IP マルチキャスト トラフィックをイネーブルにするダイナミック IP ルーティング プロトコルをサポートできます。サポートされる IP ルーティング プロトコルには、Enhanced Interior Gateway Routing Protocol（EIGRP）、Routing Information Protocol（RIP; ルーティング情報プロトコル）、Intermediate System-to-Intermediate System（IS-IS）、Open Shortest Path First（OSPF）、および Border Gateway Protocol（BGP; ボーダー ゲートウェイ プロトコル）が含まれます。

（注） IP Security（IPSec; IP セキュリティ）が GRE とともに使用される場合は、トラフィックを暗号化するためのアクセス リストに、必要なエンド ネットワークとアプリケーションが示されず、代わりに送信方向の GRE トンネルの許可された送信元と送信先が示されます。追加の Access Control Llist（ACL; アクセス コントロール リスト）がトンネル インターフェイスに適用されない場合は、GRE トンネルに転送されたすべてのパケットが暗号化されます。

VPN

VPN 設定情報は、両方のエンドポイント（Cisco ルータ側とリモート ユーザ側、Cisco ルータ側と別のルータ側など）で設定する必要があります。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。

設定作業

次の作業を実行して、このネットワーク シナリオを設定します。

- 「VPN の設定」
- 「GRE トンネルの設定」

これらの設定作業の結果を示す例は、「設定例」の項に示されています。

（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は、使用しているルータに応じて第 1 章「ルータの基本設定」、第 3 章「PPP over Ethernet と NAT の設定」、第 4 章「PPP over ATM と NAT の設定」、および第 5 章「DHCP および VLAN による LAN の設定」を参照してください。

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」
- 「グループ ポリシー情報の設定」
- 「ポリシー ルックアップのイネーブル化」
- 「IPSec トランスフォームおよびプロトコルの設定」
- 「IPSec 暗号方式およびパラメータの設定」
- 「物理インターフェイスへの暗号マップの適用」

IKE ポリシーの設定

Internet Key Exchange（IKE; インターネット キー エクスチェンジ）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。

	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が 1 です。
		
		また、Internet Security Association Key and Management Protocol（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）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 Data Encryption Standard（DES; データ暗号化規格）を使用します。

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、事前共有キーを使用します。

	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 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 モードを開始し、次の手順を実行します。

	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含む IKE ポリシー グループを作成します。
		
		また、Internet Security Association Key and Management Protocol（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）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 Domain Name System（DNS; ドメイン ネーム システム）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。

	コマンドまたはアクション	目的

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。

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。

	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*』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)#`
		PPP を含むすべてのネットワーク関連サービス要求の AAA 許可と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*』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、そのトランスフォーム セットが選択され、両方のピアの設定の一部として、保護する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。

	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 セキュリティ アソシエーションのネゴシエーション時に使用されるグローバル ライフタイム値を設定します。
		
		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

ダイナミック暗号マップ ポリシーでは、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。

	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、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 エントリで使用できるトランスフォーム 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。

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 モードを開始します。

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。

物理インターフェイスへの暗号マップの適用

暗号マップは、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暗号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 モードを開始し、次の手順を実行します。

	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 0`
	`Router(config-if)#`
		暗号マップを適用するインターフェイスに対し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	**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-if)# exit`
	`Router(config)#`
		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。

GRE トンネルの設定

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 モードを開始し、次の手順を実行します。

	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。

ステップ 3	**tunnel source** *interface-type number*
	
	例：
	`Router(config-if)# tunnel source fastethernet 2`
	`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)#`
		トンネルに暗号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*』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。

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 2

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
!
crypto isakmp policy 1 ! defines the key association and authentication for ipsec tunnel.
hash md5
authentication pre-share
crypto isakmp key cisco123 address 200.1.1.1
!
!
crypto ipsec transform-set set1 esp-3des esp-md5-hmac ! defines encryption and transform
set for the ipsec tunnel.
!
crypto map to_corporate 1 ipsec-isakmp ! associates all crypto values and peering address
for the ipsec tunnel.
 set peer 200.1.1.1
 set transform-set set1
 match address 105
!
!!
interface vlan 1 ! VLAN 1 is the internal home network
 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
!
interface fastethernet 0! FE0 is the outside or internet exposed interface
 ip address 210.110.101.21 255.255.255.0
 ip access-group 103 in ! acl 103 permits ipsec traffic from the corp. router as well as
denies internet initiated traffic inbound.
 ip nat outside
 no cdp enable
 crypto map to_corporate ! applies the ipsec tunnel to the outside interface.
!
ip nat inside source list 102 interface Ethernet1 overload ! utilize nat overload in order
to make best use of the single address provided by the isp.
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
access-list 103 permit icmp any any ! allow icmp for debugging but should be disabled due
to security implications.
access-list 103 deny ip any any ! prevents internet initiated traffic inbound.
! acl 105 matches addresses for the ipsec tunnel to/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
```