CHAPTER 28

IPSec VPN SPA を使用した高度な VPN の設定

この章では、Cisco 7600 シリーズ ルータ上の IPSec VPN SPA に高度な IP Security（IPSec）Virtual Private Network（VPN; バーチャル プライベート ネットワーク）を設定する方法について説明します。具体的な内容は次のとおりです。

（注）

この章に記載された手順は、読者がセキュリティ設定の概念（VLAN、Internet Security Association and Key Management Protocol [ISAKMP] ポリシー、事前共有キー、トランスフォーム セット、Access Control List［ACL; アクセス コントロール リスト］、暗号マップなど）についての知識があることを前提としています。これらの詳細およびその他のセキュリティ設定の概念については、『*Cisco IOS Security Configuration Guide*』および『*Cisco IOS Security Command Reference*』を参照してください。

Cisco 7600 シリーズ ルータへのカードの取り付けについての詳細は、次の URL の『*Cisco 7600 Series Router SIP, SSC, and SPA Hardware Installation Guide*』を参照してください。

http://www.cisco.com/univercd/cc/td/doc/product/core/cis7600/76sipspa/sipspahw/index.htm

システム イメージおよびコンフィギュレーション ファイルの管理については、『*Cisco IOS Configuration Fundamentals Configuration Guide*』および『*Cisco IOS Configuration Fundamentals Command Reference*』を参照してください。

この章で使用するコマンドの詳細については、『*Cisco IOS Software Releases 12.2SR Command Reference*s』および『*Cisco IOS Software Releases 12.2SX Command References*』を参照してください。また、関連する CiscoIOS Release12.2 ソフトウェア コマンド リファレンスおよびマスター インデックスも参照してください。詳細については、「関連資料」（p.lv）を参照してください。

ヒント

IPSec VPN SPA を使用して VPN を正しく設定するために、設定の概要および注意事項にすべて目を通してから設定作業を始めてください。

高度な VPN の概要

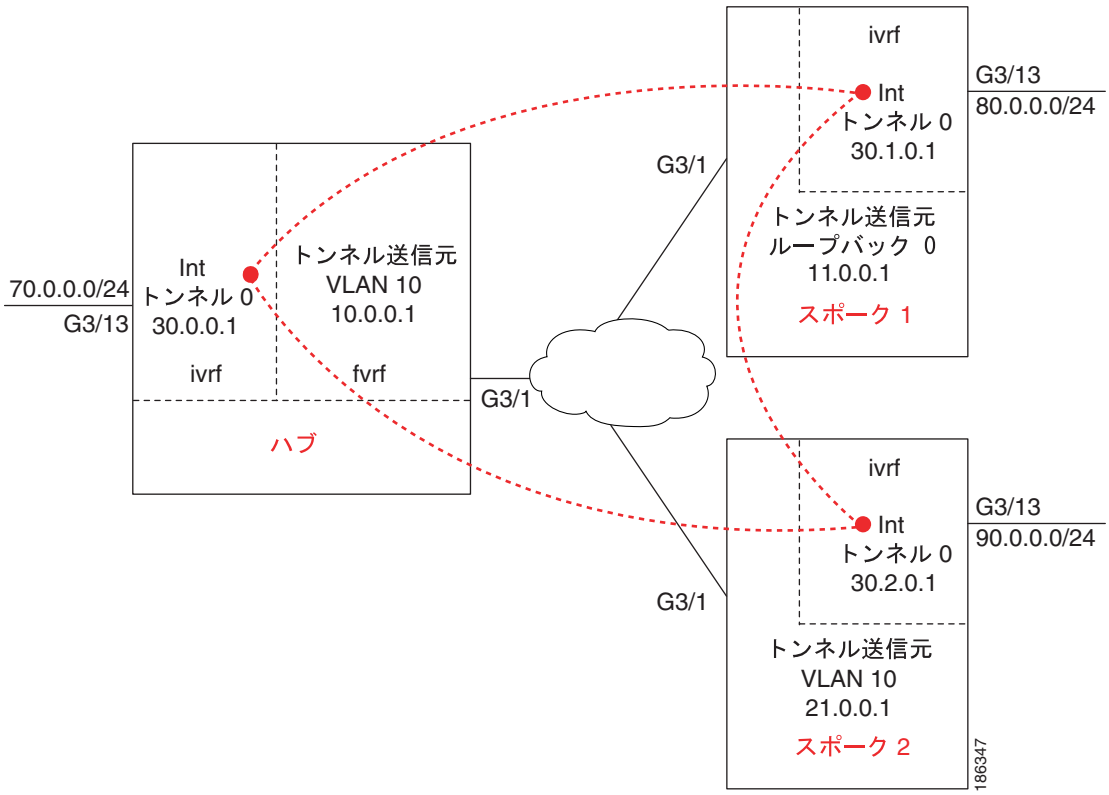
大規模かつ複雑なネットワークに IPSec VPN を設定する作業は、非常に煩雑な場合があります。この章では、高度な環境で IPSec の設定を簡素化する 2 つの機能、Dynamic Multipoint VPN（DMVPN）と Easy VPN について説明します。

DMVPN の設定

DMVPN 機能により、Generic Routing Encapsulation（GRE; 総称ルーティング カプセル化）トンネル、IPSec 暗号化、および Next Hop Resolution Protocol（NHRP）を組み合わせて、IPSec VPN のスケーラビリティを向上させることができます。

図 28-1 に、1 つのハブと 2 つのスポークを持つ DMVPN 構成の例を示します。

図 28-1　DMVPN の設定例



DMVPN 設定時の注意事項および制約事項

DMVPN を設定する場合は、次の注意事項および制約事項に従ってください。

- トンネル キーの設定はできません。トンネル キーを設定すると、PFC3 または IPSec VPN SPA はトンネルを引き継がず、トンネルは CEF スイッチングされます。
- 異なる VRF インスタンスに属する GRE トンネル同士が、同じトンネル送信元を共有することはできません。
- 非 VRF モードでは、mGRE（マルチポイント GRE）トンネル同士は同じトンネル送信元を共有できません。

- mGRE では、次のコマンドはサポートされません。
  - **ip tcp adjust-mss**
  - **qos pre-classify**
  - **tunnel path-mtu-discovery**
- Cisco 7600 シリーズ ルータに搭載された DMVPN では、マルチキャスト ストリーミングはサポートされていません。ルーティング プロトコルなどのコントロール プレーンからのマルチキャスト パケットだけがサポートされます。
- VRF 対応の DMVPN 構成で、CE/DMVPN スポークが MPLS クラウド経由で他の CE と通信する必要がある場合、**mls mpls tunnel-recir** コマンドを PE/ ハブでグローバルに設定する必要があります。
- DMVPN とともに NAT 透過対応の拡張機能を使用するには、トランスフォーム セットで IPSec トランスポート モードを使用する必要があります。また、NAT 透過機能（IKE および IPSec）では、2 つのピア（IKE および IPSec）を同じ IP アドレスに変換できますが（これらを区別する User Datagram Protocol［UDP; ユーザ データグラム プロトコル］ポートを使用［ピア アドレス変換と同義］）、この機能は DMVPN ではサポートされません。NAT 変換後は、すべての DMVPN スポークが一意の IP アドレスを持つ必要があります。NAT 変換される前は、同じ IP アドレスを持っていてもかまいません。
- この機能にスポーク ツー スポーク トンネルの動的な作成を利用する場合、IKE 証明書またはワイルドカード事前共有キーを ISAKMP 認証に使用する必要があります。

（注）　ワイルドカード事前共有キーは使用しないことを強く推奨します。いずれか 1 台のスポーク ルータが脆弱化されると、VPN 全体のアクセスが脆弱化されます。

- GRE トンネル キープアライブ（GRE インターフェイスに適用される **keepalive** コマンド）は、mGRE トンネルではサポートされません。

ハブおよびスポーク ルータで mGRE および IPSec トンネリングをイネーブルにするには、次の手順で、グローバル IPSec ポリシー テンプレートを使用する暗号マップを設定し、mGRE トンネルに IPSec 暗号化を設定する必要があります。

DMVPN サポートの詳しい設定情報は、次の URL を参照してください。

http://www.cisco.com/en/US/docs/ios/12_2t/12_2t13/feature/guide/ftgreips.html

DMVPN 要件

IPSec プロファイルを設定する前に、**crypto ipsec transform-set** コマンドを使用してトランスフォーム セットを定義する必要があります。

IPSec プロファイルの設定

IPSec プロファイルの設定に使用するコマンドは、暗号マップを設定する場合に使用するコマンドと大部分が同じですが、IPSec プロファイルで有効なのはこれらのコマンドのサブセットだけです。IPSec プロファイルでは、IPSec ポリシーに対応するコマンドのみ発行できます。IPSec ピア アドレスや、暗号化するパケットを照合するための ACL を指定することはできません。

IPSec プロファイルを設定するには、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	説明
ステップ 1	`Router(config)# crypto ipsec profile` *name*	「スポークとハブ」および「スポークとスポーク」ルータ間での IPSec 暗号化に使用する IPSec パラメータを定義します。このコマンドにより、暗号マップ コンフィギュレーション モードが開始されます。 • *name* — IPSec プロファイルの名前
ステップ 2	`Router(config-crypto-map)# set transform-set` *transform-set-name*	IPSec プロファイルとともに使用するトランスフォーム セットを指定します。 • *transform-set-name* — トランスフォーム セットの名前
ステップ 3	`Router(config-crypto-map)# set identity`	（任意）IPSec プロファイルで使用するアイデンティティ制限を指定します。
ステップ 4	`Router(config-crypto-map)# set security association lifetime {`***seconds*** *seconds* | ***kilobytes*** *kilobytes*`}`	（任意）IPSec プロファイルのグローバル ライフタイムを上書きします。 • *seconds* — SA（セキュリティ アソシエーション）が満了するまでの秒数 • *kilobytes* — SA が満了するまでに、その SA を使用して IPSec ピア間で送受信できるトラフィック量（キロバイト）
ステップ 5	`Router(config-crypto-map)# set pfs [`***group1*** | ***group2***`]`	（任意）この IPSec プロファイルの新しい SA を要求するときに、IPSec が Perfect Forward Secrecy（PFS）を要求するかどうかを指定します。このコマンドを指定しない場合、デフォルト（group1）がイネーブルになります。 • ***group1*** —（任意）新しい Diffie-Hellman（DH）交換を実行するとき、IPSec が 768 ビット DH プライム モジュール グループを使用することを指定します。 • ***group2*** — 1,024 ビット DH プライム モジュール グループを指定します。

VRF モードでのハブへの DMVPN の設定

VPN VRF モードで mGRE および IPSec 統合のハブ ルータを設定する（前述の手順で設定した IPSec プロファイルをトンネルに対応付ける）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	説明
ステップ 1	`Router(config)# interface tunnel tunnel-number`	トンネル インターフェイスを設定し、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。 • *tunnel-number* — 作成または設定するトンネル インターフェイスの番号。作成できるトンネル インターフェイスの数に制限はありません。
ステップ 2	`Router(config)# ip vrf vrf-name`	VRF ルーティング テーブルを設定し、VRF コンフィギュレーション モードを開始します。 • *vrf-name* — VRF に割り当てられた名前
ステップ 3	`Router(config-if)# ip address ip-address mask [secondary]`	トンネル インターフェイスのプライマリまたはセカンダリ IP アドレスを設定します。 • *address* — IP アドレス • *mask* — サブネット マスク • *secondary* — セカンダリ IP アドレス
ステップ 4	`Router(config-if)# ip mtu bytes`	（任意）インターフェイスで伝送される IP パケットの MTU サイズ（バイト）を設定します。 • *bytes* — MTU サイズ（バイト）
ステップ 5	`Router(config-if)# ip nhrp authentication string`	NHRP を使用するインターフェイスの認証ストリングを設定します。 • *string* — 認証ストリングのテキストこのストリングは、同じ DMVPN に属するすべてのトンネルで同じでなければなりません。
ステップ 6	`Router(config-if)# ip nhrp map multicast dynamic`	NHRP により、マルチキャスト NHRP マッピングにスポーク ルータを自動的に追加します。
ステップ 7	`Router(config-if)# ip nhrp network-id number`	インターフェイスで NHRP をイネーブルにします。 • *number* — NBMA ネットワークに属する、このシャーシ内で一意の 32 ビット ネットワーク識別子。範囲は 1 ～ 4,294,967,295 です。
ステップ 8	`Router(config-if)# tunnel source {ip-address | type number}`	トンネル インターフェイスの送信元アドレスを設定します。 • *ip-address* — トンネル内のパケットの送信元アドレスとして使用する IP アドレス • *type number* — インターフェイスのタイプおよび番号（VLAN2 など）
ステップ 9	`Router(config-if)# tunnel mode gre multipoint`	トンネル インターフェイスのカプセル化モードを mGRE に設定します。
ステップ 10	`Router(config-if)# tunnel vrf vrf-name`	（任意）特定のトンネル宛先、インターフェイス、またはサブインターフェイスに VRF インスタンスを関連付けます。この手順が必要になるのは、FVRF を設定する場合のみです。 • *vrf-name* — VRF に割り当てられた名前

	コマンド	説明
ステップ 11	`Router(config-if)# tunnel protection ipsec profile name`	トンネル インターフェイスを IPSec プロファイルに対応付けます。 • *name* — IPSec プロファイルの名前。この値は、**crypto ipsec profile** コマンドで指定した値と同じである必要があります。
ステップ 12	`Router(config-if)# crypto engine slot slot inside`	内部インターフェイスに指定した暗号エンジンを割り当てます。 • *slot* は IPSec VPN SPA が搭載されたスロットを入力します。
ステップ 13	`Router(config-if)# interface type slot/subslot/port`	DMVPN 物理出力インターフェイスを設定します。
ステップ 14	`Router(config-if)# ip vrf forwarding vrf-name`	（任意）インターフェイスまたはサブインターフェイスに VRF を関連付けます。この手順が必要になるのは、FVRF を設定する場合のみです。 • *vrf-name* — VRF に割り当てられた名前
ステップ 15	`Router(config-if)# ip address address mask`	インターフェイスのプライマリまたはセカンダリ IP アドレスを設定します。 • *address* — IP アドレス • *mask* — サブネット マスク
ステップ 16	`Router(config-if)# crypto engine slot slot outside`	インターフェイスに指定した暗号エンジンを割り当てます。 • *slot* は IPSec VPN SPA が搭載されたスロットを入力します。

暗号接続モードでのハブへの DMVPN の設定

暗号接続モードで mGRE および IPSec 統合のハブ ルータを設定する（前述の手順で設定した IPSec プロファイルをトンネルに対応付ける）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	説明
ステップ 1	`Router(config)# interface tunnel tunnel-number`	トンネル インターフェイスを設定し、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。 • *tunnel-number* — 作成または設定するトンネル インターフェイスの番号。作成できるトンネル インターフェイスの数に制限はありません。
ステップ 2	`Router(config-if)# ip address ip-address mask [secondary]`	トンネル インターフェイスのプライマリまたはセカンダリ IP アドレスを設定します。 • *address* — IP アドレス • *mask* — サブネット マスク • *secondary* — セカンダリ IP アドレス
ステップ 3	`Router(config-if)# ip mtu bytes`	（任意）インターフェイスで伝送される IP パケットの MTU サイズ（バイト）を設定します。 • *bytes* — MTU サイズ（バイト）

	コマンド	説明
ステップ 4	`Router(config-if)# ip nhrp authentication string`	NHRP を使用するインターフェイスの認証ストリングを設定します。 • *string* — 認証ストリングのテキストこのストリングは、同じ DMVPN に属するすべてのトンネルで同じでなければなりません。
ステップ 5	`Router(config-if)# ip nhrp map multicast dynamic`	NHRP により、マルチキャスト NHRP マッピングにスポーク ルータを自動的に追加します。
ステップ 6	`Router(config-if)# ip nhrp network-id number`	インターフェイスで NHRP をイネーブルにします。 • *number* — NBMA ネットワークに属する、このシャーシ内で一意の 32 ビット ネットワーク識別子。範囲は 1 ～ 4,294,967,295 です。
ステップ 7	`Router(config-if)# tunnel source {ip-address | type number}`	トンネル インターフェイスの送信元アドレスを設定します。 • *ip-address* — トンネル内のパケットの送信元アドレスとして使用する IP アドレス • *type number* — インターフェイスのタイプおよび番号（VLAN2 など）
ステップ 8	`Router(config-if)# tunnel mode gre multipoint`	トンネル インターフェイスのカプセル化モードを mGRE に設定します。
ステップ 9	`Router(config-if)# tunnel protection ipsec profile name`	トンネル インターフェイスを IPSec プロファイルに対応付けます。 • *name* — IPSec プロファイルの名前。この値は、**crypto ipsec profile** コマンドで指定した値と同じである必要があります。
ステップ 10	`Router(config-if)# crypto engine slot slot`	インターフェイスに指定した暗号エンジンを割り当てます。 • *slot* は IPSec VPN SPA が搭載されたスロットを入力します。
ステップ 11	`Router(config)# interface vlan ifvlan`	DMVPN 内部 VLAN を設定します。
ステップ 12	`Router(config-if)# ip address address mask`	インターフェイスのプライマリまたはセカンダリ IP アドレスを設定します。 • *address* — IP アドレスステップ 7 で指定した値を入力します。 • *mask* — サブネット マスク
ステップ 13	`Router(config-if)# crypto engine slot slot`	インターフェイスに指定した暗号エンジンを割り当てます。 • *slot* は IPSec VPN SPA が搭載されたスロットを入力します。
ステップ 14	`Router(config-if)# interface type slot/subslot/port`	DMVPN 物理出力インターフェイスを設定します。
ステップ 15	`Router(config-if)# no ip address`	インターフェイスに IP アドレスを割り当てません。
ステップ 16	`Router(config-if)# crypto connect vlan ifvlan`	外部アクセス ポート VLAN を内部インターフェイス VLAN に接続し、暗号接続モードを開始します。 • *ifvlan* — DMVPN 内部 VLAN の識別子

VRF モードでのスポークへの DMVPN の設定

VRF モードで mGRE および IPSec 統合のスポーク 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 モードから次の作業を行います。

	コマンド	説明
ステップ 1	`Router(config)# interface tunnel` *tunnel-number*	トンネル インターフェイスを設定し、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。 • *tunnel-number* — 作成または設定するトンネル インターフェイスの番号。作成できるトンネル インターフェイスの数に制限はありません。
ステップ 2	`Router(config)# ip vrf` *vrf-name*	VRF ルーティング テーブルを設定し、VRF コンフィギュレーション モードを開始します。 • *vrf-name* — VRF に割り当てられた名前
ステップ 3	`Router(config-if)# ip address` *ip-address mask* [*secondary*]	トンネル インターフェイスのプライマリまたはセカンダリ IP アドレスを設定します。 • *address* — IP アドレス • *mask* — サブネット マスク • *secondary* — セカンダリ IP アドレス
ステップ 4	`Router(config-if)# ip mtu` *bytes*	（任意）インターフェイスで伝送される IP パケットの MTU サイズ（バイト）を設定します。 • *bytes* — MTU サイズ（バイト）
ステップ 5	`Router(config-if)# ip nhrp authentication` *string*	NHRP を使用するインターフェイスの認証ストリングを設定します。 • *string* — 認証ストリングのテキストこのストリングは、同じ DMVPN に属するすべてのトンネルで同じでなければなりません。
ステップ 6	`Router(config-if)# ip nhrp map` *hub-tunnel-ip-address hub-physical-ip-address*	NonBroadcast MultiAccess（NBMA; 非ブロードキャスト マルチアクセス））ネットワークに接続する宛先 IP アドレスの IP/NBMA アドレス マッピングをスタティックに設定します。 • *hub-tunnel-ip-address* — ハブでの NHRP サーバを定義します。これはハブのスタティックなパブリック IP アドレスに、永続的にマッピングされます。 • *hub-physical-ip-address* — ハブのスタティックなパブリック IP アドレスを定義します。
ステップ 7	`Router(config-if)# ip nhrp map multicast` *hub-physical-ip-address*	スポークとハブの間でダイナミック ルーティング プロトコルの使用をイネーブルにし、ハブ ルータにマルチキャスト パケットを送信します。 • *hub-physical-ip-address* — ハブのスタティックなパブリック IP アドレスを定義します。
ステップ 8	`Router(config-if)# ip nhrp nhs` *hub-tunnel-ip-address*	ハブ ルータを NHRP ネクストホップ サーバとして設定します。 • *hub-tunnel-ip-address* — ハブでの NHRP サーバを定義します。これはハブのスタティックなパブリック IP アドレスに、永続的にマッピングされます。

	コマンド	説明
ステップ 9	`Router(config-if)# ip nhrp network-id number`	インターフェイスで NHRP をイネーブルにします。 • *number* — NBMA ネットワークに属する、このシャーシ内で一意の 32 ビット ネットワーク識別子。範囲は 1 ～ 4,294,967,295 です。
ステップ 10	`Router(config-if)# tunnel source {ip-address | type number}`	トンネル インターフェイスの送信元アドレスを設定します。 • *ip-address* — トンネル内のパケットの送信元アドレスとして使用する IP アドレス • *type number* — インターフェイスのタイプおよび番号（VLAN2 など）
ステップ 11	`Router(config-if)# tunnel mode gre multipoint`	トンネル インターフェイスのカプセル化モードを mGRE に設定します。データ トラフィックがダイナミックなスポークツースポーク トラフィックを使用する場合に、このコマンドを使用します。
ステップ 12	`Router(config-if)# tunnel protection ipsec profile name`	トンネル インターフェイスを IPSec プロファイルに対応付けます。 • *name* — IPSec プロファイルの名前。この値は、**crypto ipsec profile** コマンドで指定した値と同じである必要があります。
ステップ 13	`Router(config-if)# crypto engine slot slot inside`	内部インターフェイスに指定した暗号エンジンを割り当てます。 • *slot* は IPSec VPN SPA が搭載されたスロットを入力します。
ステップ 14	`Router(config-if)# interface type slot/subslot/port`	DMVPN 物理出力インターフェイスを設定します。
ステップ 15	`Router(config-if)# ip address address mask`	インターフェイスのプライマリまたはセカンダリ IP アドレスを設定します。 • *address* — IP アドレス • *mask* — サブネット マスク
ステップ 16	`Router(config-if)# crypto engine slot slot outside`	インターフェイスに指定した暗号エンジンを割り当てます。 • *slot* は IPSec VPN SPA が搭載されたスロットを入力します。

暗号接続モードでのスポークへの DMVPN の設定

暗号接続モードで mGRE および IPSec 統合のスポーク 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 モードから次の作業を行います。

	コマンド	説明
ステップ 1	`Router(config)# interface tunnel` *tunnel-number*	トンネル インターフェイスを設定し、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。 • *tunnel-number* — 作成または設定するトンネル インターフェイスの番号。作成できるトンネル インターフェイスの数に制限はありません。
ステップ 2	`Router(config-if)# ip address` *ip-address mask* [*secondary*]	トンネル インターフェイスのプライマリまたはセカンダリ IP アドレスを設定します。 • *address* — IP アドレス • *mask* — サブネット マスク • *secondary* — セカンダリ IP アドレス
ステップ 3	`Router(config-if)# ip mtu` *bytes*	（任意）インターフェイスで伝送される IP パケットの MTU サイズ（バイト）を設定します。 • *bytes* — MTU サイズ（バイト）
ステップ 4	`Router(config-if)# ip nhrp authentication` *string*	NHRP を使用するインターフェイスの認証ストリングを設定します。 • *string* — 認証ストリングのテキストこのストリングは、同じ DMVPN に属するすべてのトンネルで同じでなければなりません。
ステップ 5	`Router(config-if)# ip nhrp map` *hub-tunnel-ip-address hub-physical-ip-address*	NonBroadcast MultiAccess（NBMA; 非ブロードキャスト マルチアクセス））ネットワークに接続する宛先 IP アドレスの IP/NBMA アドレス マッピングをスタティックに設定します。 • *hub-tunnel-ip-address* — ハブでの NHRP サーバを定義します。これはハブのスタティックなパブリック IP アドレスに、永続的にマッピングされます。 • *hub-physical-ip-address* — ハブのスタティックなパブリック IP アドレスを定義します。
ステップ 6	`Router(config-if)# ip nhrp map multicast` *hub-physical-ip-address*	スポークとハブの間でダイナミック ルーティング プロトコルの使用をイネーブルにし、ハブ ルータにマルチキャスト パケットを送信します。 • *hub-physical-ip-address* — ハブのスタティックなパブリック IP アドレスを定義します。
ステップ 7	`Router(config-if)# ip nhrp nhs` *hub-tunnel-ip-address*	ハブ ルータを NHRP ネクストホップ サーバとして設定します。 • *hub-tunnel-ip-address* — ハブでの NHRP サーバを定義します。これはハブのスタティックなパブリック IP アドレスに、永続的にマッピングされます。

	コマンド	説明
ステップ 8	`Router(config-if)# ip nhrp network-id number`	インターフェイスで NHRP をイネーブルにします。 • *number* — NBMA ネットワークに属する、このシャーシ内で一意の 32 ビット ネットワーク識別子。範囲は 1 ～ 4,294,967,295 です。
ステップ 9	`Router(config-if)# tunnel source {ip-address | type number}`	トンネル インターフェイスの送信元アドレスを設定します。 • *ip-address* — トンネル内のパケットの送信元アドレスとして使用する IP アドレス • *type number* — インターフェイスのタイプおよび番号（VLAN2 など）
ステップ 10	`Router(config-if)# tunnel mode gre multipoint`	トンネル インターフェイスのカプセル化モードを mGRE に設定します。データ トラフィックがダイナミックなスポークツースポーク トラフィックを使用する場合に、このコマンドを使用します。
ステップ 11	`Router(config-if)# tunnel protection ipsec profile name`	トンネル インターフェイスを IPSec プロファイルに対応付けます。 • *name* — IPSec プロファイルの名前。この値は、**crypto ipsec profile** コマンドで指定した値と同じである必要があります。
ステップ 12	`Router(config-if)# crypto engine slot slot`	インターフェイスに指定した暗号エンジンを割り当てます。 • *slot* は IPSec VPN SPA が搭載されたスロットを入力します。
ステップ 13	`Router(config)# interface vlan ifvlan`	DMVPN 内部 VLAN を設定します。
ステップ 14	`Router(config-if)# ip address address mask`	インターフェイスのプライマリまたはセカンダリ IP アドレスを設定します。 • *address* — IP アドレスステップ 7 で指定した値を入力します。 • *mask* — サブネット マスク
ステップ 15	`Router(config-if)# crypto engine slot slot`	インターフェイスに指定した暗号エンジンを割り当てます。 • *slot* は IPSec VPN SPA が搭載されたスロットを入力します。
ステップ 16	`Router(config-if)# interface type slot/subslot/port`	DMVPN 物理出力インターフェイスを設定します。
ステップ 17	`Router(config-if)# no ip address`	インターフェイスに IP アドレスを割り当てません。
ステップ 18	`Router(config-if)# crypto connect vlan ifvlan`	外部アクセス ポート VLAN を内部インターフェイス VLAN に接続し、暗号接続モードにします。 • *ifvlan* — DMVPN 内部 VLAN の識別子

DMVPN 設定の確認

DMVPN コンフィギュレーションが正常に機能しているかどうかを確認するには、**show crypto isakmp sa**、**show crypto map**、および **show ip nhrp** コマンドを入力します。

show crypto isakmp sa コマンドは、ピアの現在の IKE SA をすべて表示します。

ハブと 2 つのスポーク間で IKE ネゴシエーションが正常に終了すると、図 28-1（p.28-2）に示すように、次のような出力が表示されます

```
HUB# show crypto isakmp sa
dst             src             state          conn-id slot status
10.0.0.1        11.0.0.1        QM_IDLE          68001 ACTIVE
10.0.0.1        21.0.0.1        QM_IDLE          68002 ACTIVE


SPOKE1# show crypto isakmp sa
dst             src             state          conn-id slot status
11.0.0.1        21.0.0.1        QM_IDLE          68002 ACTIVE
21.0.0.1        11.0.0.1        QM_IDLE          68003 ACTIVE
10.0.0.1        11.0.0.1        QM_IDLE          68001 ACTIVE

SPOKE2# show crypto isakmp sa
dst             src             state          conn-id slot status
10.0.0.1        21.0.0.1        QM_IDLE          68001 ACTIVE
11.0.0.1        21.0.0.1        QM_IDLE          68003 ACTIVE
21.0.0.1        11.0.0.1        QM_IDLE          68002 ACTIVE
```

show crypto map コマンドは、暗号マップの設定を表示します。

暗号マップが設定されている場合、次のような出力が表示されます。

```
HUB# show crypto map
Crypto Map "Tunnel0-head-0" 65536 ipsec-isakmp
        Profile name: VPN-PROF
        Security association lifetime: 4608000 kilobytes/3600 seconds
        PFS (Y/N): N
        Transform sets={
                ts,
        }

Crypto Map "Tunnel0-head-0" 65537 ipsec-isakmp
        Map is a PROFILE INSTANCE.
        Peer = 11.0.0.1
        Extended IP access list
            access-list  permit gre host 10.0.0.1 host 11.0.0.1
        Current peer: 11.0.0.1
        Security association lifetime: 4608000 kilobytes/3600 seconds
        PFS (Y/N): N
        Transform sets={
                ts,
        }

Crypto Map "Tunnel0-head-0" 65538 ipsec-isakmp
        Map is a PROFILE INSTANCE.
        Peer = 21.0.0.1
        Extended IP access list
            access-list  permit gre host 10.0.0.1 host 21.0.0.1
        Current peer: 21.0.0.1
        Security association lifetime: 4608000 kilobytes/3600 seconds
        PFS (Y/N): N
        Transform sets={
                ts,
        }
        Interfaces using crypto map Tunnel0-head-0:
                Tunnel0
 using crypto engine SPA-IPSEC-2G[4/0]
```

```
SPOKE1# show crypto map
Crypto Map "Tunnel0-head-0" 65536 ipsec-isakmp
        Profile name: VPN-PROF
        Security association lifetime: 4608000 kilobytes/3600 seconds
        PFS (Y/N): N
        Transform sets={
                ts,
        }

Crypto Map "Tunnel0-head-0" 65537 ipsec-isakmp
        Map is a PROFILE INSTANCE.
        Peer = 10.0.0.1
        Extended IP access list
            access-list  permit gre host 11.0.0.1 host 10.0.0.1
        Current peer: 10.0.0.1
        Security association lifetime: 4608000 kilobytes/3600 seconds
        PFS (Y/N): N
        Transform sets={
                ts,
        }

Crypto Map "Tunnel0-head-0" 65538 ipsec-isakmp
        Map is a PROFILE INSTANCE.
        Peer = 21.0.0.1
        Extended IP access list
            access-list  permit gre host 11.0.0.1 host 21.0.0.1
        Current peer: 21.0.0.1
        Security association lifetime: 4608000 kilobytes/3600 seconds
        PFS (Y/N): N
        Transform sets={
                ts,
        }
        Interfaces using crypto map Tunnel0-head-0:
                Tunnel0
 using crypto engine SPA-IPSEC-2G[4/0]


SPOKE2# show crypto map
Crypto Map "Tunnel0-head-0" 65536 ipsec-isakmp
        Profile name: VPN-PROF
        Security association lifetime: 4608000 kilobytes/3600 seconds
        PFS (Y/N): N
        Transform sets={
                ts,
        }

Crypto Map "Tunnel0-head-0" 65537 ipsec-isakmp
        Map is a PROFILE INSTANCE.
        Peer = 10.0.0.1
        Extended IP access list
            access-list  permit gre host 21.0.0.1 host 10.0.0.1
        Current peer: 10.0.0.1
        Security association lifetime: 4608000 kilobytes/3600 seconds
        PFS (Y/N): N
        Transform sets={
                ts,
        }

Crypto Map "Tunnel0-head-0" 65538 ipsec-isakmp
        Map is a PROFILE INSTANCE.
        Peer = 11.0.0.1
        Extended IP access list
            access-list  permit gre host 21.0.0.1 host 11.0.0.1
        Current peer: 11.0.0.1
        Security association lifetime: 4608000 kilobytes/3600 seconds
        PFS (Y/N): N
```

```
        Transform sets={
                ts,
        }
        Interfaces using crypto map Tunnel0-head-0:
                Tunnel0
 using crypto engine SPA-IPSEC-2G[4/0]
```

show ip nhrp コマンドは、NHRP キャッシュを表示します。

次の出力例は、NHRP 登録が行われたことを示します。スポーク間の NHRP は動的ですが、ハブとスポーク間の NHRP は静的です。

```
Router# show ip nhrp
HUB# show ip nhrp
30.1.0.1/32 via 30.1.0.1, Tunnel0 created 00:18:13, expire 01:41:46
  Type: dynamic, Flags: authoritative unique registered
  NBMA address: 11.0.0.1
30.2.0.1/32 via 30.2.0.1, Tunnel0 created 00:11:55, expire 01:48:04
  Type: dynamic, Flags: authoritative unique registered
  NBMA address: 21.0.0.1


SPOKE1# show ip nhrp
30.0.0.1/32 via 30.0.0.1, Tunnel0 created 00:23:39, never expire
  Type: static, Flags: authoritative used
  NBMA address: 10.0.0.1
30.2.0.1/32 via 30.2.0.1, Tunnel0 created 00:04:27, expire 01:47:59
  Type: dynamic, Flags: router
  NBMA address: 21.0.0.1


SPOKE2# show ip nhrp
30.0.0.1/32 via 30.0.0.1, Tunnel0 created 00:12:02, never expire
  Type: static, Flags: authoritative used
  NBMA address: 10.0.0.1
30.1.0.1/32 via 30.1.0.1, Tunnel0 created 00:04:29, expire 01:41:40
  Type: dynamic, Flags: router
  NBMA address: 11.0.0.1
```

DMVPN の設定例は、「DMVPN の設定例」（p.28-18）を参照してください。

Easy VPN サーバの設定

Easy VPN サーバは、Cisco VPN Client Release 4.x 以降のソフトウェア クライアントおよび Cisco VPN ハードウェア クライアントに対してサーバ サポートを提供します。この機能により、リモートのエンド ユーザは、任意の Cisco IOS VPN ゲートウェイと IPSec を使用して通信できます。集中管理される IPSec ポリシーがサーバによってクライアントに「プッシュ」されるので、エンド ユーザによる設定は最小限で済みます。

Easy VPN サーバには次の機能があります。

- モード設定および Xauth サポート
- ユーザ ベースのポリシー制御
- VPN グループ アクセスに関するセッション モニタリング
- RADIUS サーバ サポート
- **backup-gateway** コマンド
- **pfs** コマンド
- 仮想 IPsec インターフェイス サポート
- バナー、自動更新、およびブラウザ プロキシ
- コンフィギュレーション マネジメント拡張機能（モード設定交換によるコンフィギュレーション URL のプッシュ）
- Public Key Infrastructure（PKI; 公開鍵インフラストラクチャ）によるユーザ単位の AAA ポリシーのダウンロード
- Syslog メッセージ拡張機能
- Network Admission Control（NAC）サポート

Easy VPN サーバ設定時の注意事項および制約事項

Easy VPN サーバを設定する場合は、次の注意事項および制約事項に従ってください。

- 次の IPSec プロトコル オプションおよびアトリビュートは、現在 Cisco VPN クライアントではサポートされていません。したがって、これらのクライアントに対応するルータには、これらのオプションおよびアトリビュートを設定しないでください。
  - 公開鍵暗号化を使用する認証
  - Digital Signature Standard（DSS）
  - Diffie-Hellman（DH）グループ（1）
  - IPSec プロトコル識別子（IPSEC_AH）
  - IPSec プロトコル モード（トランスポート モード）
  - 手動キー
  - Perfect Forward Secrecy（PFS）

Easy VPN サーバ機能および拡張機能に関する詳しい設定情報は、次の URL を参照してください。

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t8/ftunity.htm

Easy VPN リモートの設定

Easy VPN 機能により、リモートのエンド ユーザは、任意の Cisco IOS VPN ゲートウェイと IPSec を使用して通信できます。集中管理される IPSec ポリシーがサーバによってクライアントに「プッシュ」されるので、エンド ユーザによる設定は最小限で済みます。

Easy VPN リモートには次の機能があります。

- 仮想 IPsec インターフェイス サポート
- バナー、自動更新、およびブラウザ プロキシ
- デュアル トンネル サポート
- コンフィギュレーション マネジメント拡張機能（モード設定交換によるコンフィギュレーション URL のプッシュ）
- プライマリ ピアの再アクティブ化

Easy VPN リモート設定時の注意事項

IPSec VPN SPA に Easy VPN を設定する場合は、次の注意事項に従ってください。

注意　IPSec VPN SPA への接続に使用している Cisco IOS ベースの Easy VPN クライアントでは、他のすべての暗号設定を実行コンフィギュレーションから削除する必要があります。ISAKMP ポリシーが設定されていると、プリインストールされた Easy VPN ISAKMP ポリシーよりも優先され、接続が失敗します。Easy VPN を実行する VPN3000 や PIX システムなどのクライアントがあると、暗号設定をすべて削除しないかぎり、Easy VPN を設定できません。Easy VPN クライアント サポートの詳しい設定情報は、次の URL を参照してください。

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t_7/ftezvpnr.htm

Easy VPN サーバの設定例は、「Easy VPN サーバ（ルータ側）の設定例」（p.28-23）を参照してください。

Easy VPN Remote RSA シグニチャ ストレージの設定

Easy VPN Remote Rivest, Shamir, and Adelman（RSA）シグニチャ サポート機能を使用すると、Easy VPN リモート デバイスで RSA シグニチャをサポートできます。このサポートは、リモート デバイスの内外に保存可能な RSA 証明書を通して実現されます。

（注）　Easy VPN Remote RSA シグニチャ サポート機能は、Cisco IOS Release 12.2(33)SRA 以降でのみサポートされています。

Easy VPN Remote RSA シグニチャ サポート設定時の注意事項および制約事項

Easy VPN Remote RSA シグニチャ サポートを設定する場合は、次の注意事項および制約事項に従ってください。

- Cisco VPN リモート デバイスを配置し、デバイスの設定について理解しておく必要があります。
- この相互運用性機能を設定する前に、ネットワークで CA を使用可能にする必要があります。CA はシスコシステムズの PKI プロトコルの Simple Certificate Enrollment Protocol（SCEP）（従来は Certificate Enrollment Protocol [CEP]）をサポートする必要があります。
- この機能を設定する必要があるのは、ネットワークに IPSec および IKE を両方とも設定する場合のみです。
- Cisco IOS ソフトウェアは、2,048 ビットを超える CA サーバ公開鍵をサポートしません。

Easy VPN Remote RSA シグニチャ サポートの設定

Easy VPN リモート デバイスの RSA シグニチャの設定方法は、その他のシスコ製デバイスの RSA シグニチャの設定方法と同じです。

RSA シグニチャの設定方法については、『*Cisco IOS Security Configuration Guide*』を参照してください。

RSA シグニチャをイネーブルにするには、Easy VPN リモートを設定し、発信インターフェイスに設定を割り当てるときに、**group** コマンドを省略する必要があります。最初の Organizational Unit（OU）フィールドの内容が、グループとして使用されます。

Cisco Easy VPN リモート デバイスの設定方法については、次の URL にある機能マニュアル『*Easy VPN Remote RSA Signature Support*』を参照してください。

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t_7/gtevcrsa.htm

設定例

ここでは、次の設定例を示します。

DMVPN の設定例

ここでは、DMVPN の設定例を示します。

DMVPN の設定例は図 28-1（p.28-2）に示す実装に基づいており、次の設定パラメータを使用しています。

- ハブ ルータ（HUB）は、内部 VRF（IVRF）および前面扉 VRF（FVRF）を使用し、VRF モードで設定されています。
- 1 つのスポーク ルータ（SPOKE1）が IVRF を使用し、FVRF を使用せずに VRF モードで設定されています。
- 1 つのスポーク ルータ（SPOKE2）が、暗号接続モードで設定されています。
- EIGRP はトンネル経由でルートを配送するように設定されています。
- すべてのルータにおいて、インターフェイス gi3/1 はプロバイダ ネットワークへのインターフェイスです。
- すべてのルータにおいて、インターフェイス gi3/13 はプライベート LAN へのインターフェイスです。

VRF モードを使用する DMVPN ハブの設定例

（注）　トンネル送信元が物理出力ポートの場合、両方を同じ IP アドレスで設定してください。トンネル送信元が物理出力ポートでない場合、トンネル送信元と送受信するトラフィックが物理出力ポートを通過するようにします。

次に、内部 VRF および前面扉 VRF（FVRF）を使用し、VRF モードで DMVPN ハブとして動作する IPSec VPN SPA の設定例を示します。

```
hostname HUB
!
ip vrf fvrf
 rd 1000:1
!
ip vrf ivrf
 rd 1:1
!
crypto engine mode vrf
!
crypto keyring RING1 vrf fvrf
  pre-shared-key address 0.0.0.0 0.0.0.0 key abcdef
!
crypto isakmp policy 10
 encr 3des
 hash md5
 authentication pre-share
crypto isakmp keepalive 60
!
crypto ipsec transform-set ts esp-3des esp-md5-hmac
!
crypto ipsec profile VPN-PROF
 set transform-set ts
!
!
interface Tunnel0
! EIGRP uses the configured bandwidth to allocate bandwidth for its routing update
mechanism
 bandwidth 1000000
 ip vrf forwarding ivrf
 ip address 30.0.0.1 255.0.0.0
 ip nhrp authentication cisco123
 ip nhrp map multicast dynamic
 ip nhrp network-id 1000
! For a large number of tunnels, the following two commands are recommended
! EIGRP timers are adjusted to match the default timers for a WAN interface
 ip hello-interval eigrp 200 60
 ip hold-time eigrp 200 180
! The following two EIGRP commands are necessary to allow spoke-to-spoke communication
 no ip next-hop-self eigrp 200
 no ip split-horizon eigrp 200
 tunnel source Vlan10
 tunnel mode gre multipoint
 tunnel vrf fvrf
 tunnel protection ipsec profile VPN-PROF
 crypto engine slot 4/0 inside
!
interface Vlan10
 ip vrf forwarding fvrf
 ip address 10.0.0.1 255.255.255.0
 crypto engine slot 4/0 outside
!
interface GigabitEthernet3/1
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 10
 switchport mode trunk

interface GigabitEthernet3/13
 description Local LAN interface
 ip vrf forwarding ivrf
 ip address 70.0.0.1 255.255.255.0

router eigrp 10
 no auto-summary
 !
```

```
 address-family ipv4 vrf ivrf
 redistribute connected
 network 30.0.0.0
 no auto-summary
 autonomous-system 200
 exit-address-family
!
! In this example, tunnel destination reachability is provided by static routes
! A routing protocol could also be used
ip route vrf fvrf 11.0.0.0 255.0.0.0 10.0.0.2
ip route vrf fvrf 21.0.0.0 255.0.0.0 10.0.0.2

end
```

VRF モードを使用する DMVPN スポークの設定例

（注）　トンネル送信元が物理出力ポートの場合、両方を同じ IP アドレスで設定してください。トンネル送信元が物理出力ポートでない場合、トンネル送信元と送受信するトラフィックが物理出力ポートを通過するようにします。

次に、内部 VRF および前面扉 VRF（FVRF）を使用し、VRF モードで DMVPN スポークとして動作する IPSec VPN SPA の設定例を示します。

```
hostname SPOKE1
!
ip vrf ivrf
 rd 1:1
!
crypto engine mode vrf
!
!
crypto isakmp policy 10
 encr 3des
 hash md5
 authentication pre-share
crypto isakmp key abcdef address 0.0.0.0 0.0.0.0
crypto isakmp keepalive 60
!
!
crypto ipsec transform-set ts esp-3des esp-md5-hmac
!
crypto ipsec profile VPN-PROF
 set transform-set ts
!
interface Tunnel0
 bandwidth 100000
 ip vrf forwarding ivrf
 ip address 30.1.0.1 255.0.0.0
 ip nhrp authentication cisco123
 ip nhrp map 30.0.0.1 10.0.0.1
 ip nhrp map multicast 10.0.0.1
 ip nhrp network-id 1701
 ip nhrp nhs 30.0.0.1
 ip hello-interval eigrp 200 60
 ip hold-time eigrp 200 180
 tunnel source Loopback0
 tunnel mode gre multipoint
 tunnel protection ipsec profile VPN-PROF
 crypto engine slot 4/0 inside
!
interface Loopback0
 ip address 11.0.0.1 255.255.255.0
!

interface GigabitEthernet3/1
 ip address 11.255.255.1 255.255.255.0
 crypto engine slot 4/0 outside
!
interface GigabitEthernet3/13
 ip vrf forwarding ivrf
 ip address 80.0.0.1 255.255.255.0

router eigrp 10
 no auto-summary
 !
 address-family ipv4 vrf ivrf
 autonomous-system 200
 network 30.0.0.0
 no auto-summary
 redistribute connected
 exit-address-family

ip route 10.0.0.0 255.0.0.0 11.255.255.2
ip route 21.0.0.0 255.0.0.0 11.255.255.2

end
```

暗号接続モードを使用した DMVPN スポークの設定例

以下に、暗号接続モードを使用し、DMVPN スポークとして動作する IPSec VPN SPA の設定例を示します。

```
hostname SPOKE2
!
crypto isakmp policy 10
 encr 3des
 hash md5
 authentication pre-share
crypto isakmp key abcdef address 0.0.0.0 0.0.0.0
crypto isakmp keepalive 60
!
!
crypto ipsec transform-set ts esp-3des esp-md5-hmac
!
crypto ipsec profile VPN-PROF
 set transform-set ts
!
interface Tunnel0
 bandwidth 1000000
 ip address 30.2.0.1 255.0.0.0
 ip nhrp authentication cisco123
 ip nhrp map 30.0.0.1 10.0.0.1
 ip nhrp map multicast 10.0.0.1
 ip nhrp network-id 1000
 ip nhrp nhs 30.0.0.1
 ip hello-interval eigrp 200 60
 ip hold-time eigrp 200 180
 tunnel source Vlan10
 tunnel mode gre multipoint
 tunnel protection ipsec profile VPN-PROF
 crypto engine slot 4/0
!
interface Vlan10
 ip address 21.0.0.1 255.255.255.0
 no mop enabled
 crypto engine slot 4/0
!
interface GigabitEthernet3/1
 no ip address
 crypto connect vlan 10
!
interface GigabitEthernet3/13
 ip vrf forwarding ivrf
 ip address 90.0.0.1 255.255.255.0

router eigrp 200
 redistribute connected
 network 30.0.0.0
 network 90.0.0.0
 no auto-summary

ip route 10.0.0.0 255.0.0.0 21.0.0.2
ip route 11.0.0.0 255.0.0.0 21.0.0.2

end
```

Easy VPN サーバ（ルータ側）の設定例

以下に、Easy VPN サーバのルータ側の設定例を示します。

```
!
version 12.2
!
hostname sanjose
!
logging snmp-authfail
logging buffered 1000000 debugging
aaa new-model
aaa authentication login authen local
aaa authorization network author local
!
username unity password 0 uc
ip subnet-zero
no ip source-route
!
mpls ldp logging neighbor-changes
mls flow ip destination
mls flow ipx destination
!
crypto isakmp policy 1
 encr 3des
 hash md5
 authentication pre-share
 group 2
crypto isakmp key 12345 address 0.0.0.0 0.0.0.0
crypto isakmp keepalive 10 2
!
crypto isakmp client configuration group group1
 key 12345
 domain cisco.com
 pool pool1
!
crypto isakmp client configuration group default
 key 12345
 domain cisco.com
 pool pool2
!
crypto ipsec transform-set myset3 esp-3des esp-md5-hmac
!
crypto dynamic-map test_dyn 1
 set transform-set myset3
 reverse-route
!
! Static client mapping
crypto map testtag client authentication list authen
crypto map testtag isakmp authorization list author
crypto map testtag client configuration address respond
crypto map testtag 10 ipsec-isakmp
 set peer 10.5.1.4
 set security-association lifetime seconds 900
 set transform-set myset3
 match address 109
!
! Dynamic client mapping
crypto map test_dyn client authentication list authen
crypto map test_dyn isakmp authorization list author
crypto map test_dyn client configuration address respond
crypto map test_dyn 1 ipsec-isakmp dynamic test_dyn
!
!
no spanning-tree vlan 513
!
redundancy
  main-cpu
  auto-sync running-config
  auto-sync standard
```

```
!
interface GigabitEthernet2/1
 no ip address
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,513,1002-1005
 switchport mode trunk
!
interface GigabitEthernet2/2
 no ip address
 shutdown
!
interface GigabitEthernet6/1/1
 no ip address
 flowcontrol receive on
 flowcontrol send off
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,513,1002-1005
 switchport mode trunk
 cdp enable
!
interface GigabitEthernet6/1/2
 no ip address
 flowcontrol receive on
 flowcontrol send off
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,2,1002-1005
 switchport mode trunk
 cdp enable
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan2
 no ip address
 crypto connect vlan 513
!
interface Vlan513
 ip address 10.5.1.1 255.255.0.0
 crypto map test_dyn
 crypto engine slot 6/1
!
ip local pool pool1 22.0.0.2
ip local pool pool2 23.0.0.3
ip classless
ip pim bidir-enable
!
access-list 109 permit ip host 10.5.1.1 host 22.0.0.2
arp 127.0.0.12 0000.2100.0000 ARPA
!
snmp-server enable traps tty
snmp-server enable traps ipsec tunnel start
snmp-server enable traps ipsec tunnel stop
!
line con 0
line vty 0 4
 password lab
 transport input lat pad mop telnet rlogin udptn nasi
!
end
```