PfR 管理の出口リンクとしての VPN IPsec/GRE トンネル インターフェイスの設定

このモジュールには、IP Security（IPsec; IP セキュリティ）/Generic Routing Encapsulation（GRE; 総称ルーティング カプセル化）トンネル インターフェイスを PfR 管理の出口リンクとして設定する方法について説明している Performance Routing（PfR; パフォーマンス ルーティング）ソリューションが記載されています。VPN IPsec/GRE Tunnel Optimization ソリューションは、ネットワークベースの IPsec Virtual Private Network（VPN; バーチャル プライベート ネットワーク）だけをサポートしています。

PfR は、ネットワーク間の複数の接続に対し、自動ルート最適化と負荷分散を行います。PfR は、IP トラフィックを監視してから、プレフィクスのパフォーマンス、リンクの負荷分散、リンク帯域幅の金銭的コスト、およびトラフィック タイプに基づいてポリシーとルールを定義できる、統合型の Cisco IOS ソリューションです。PfR は、アクティブ モニタリング システム、パッシブ モニタリング システム、障害のダイナミック検出、およびパスの自動修正を実行できます。PfR を導入することによって、インテリジェントな負荷分散や、企業ネットワーク内での最適なルート選択が可能になります。

機能情報の確認

お使いのソフトウェア リリースが、このモジュールで説明されている機能の一部をサポートしていないことがあります。最新の機能情報および警告については、ご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、「PfR 管理の出口リンクとしての VPN IPsec/GRE トンネル インターフェイスの設定の機能情報」（P.20）を参照してください。

Cisco Feature Navigator を使用すると、プラットフォーム、および Cisco ソフトウェア イメージの各サポート情報を検索できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

マニュアルの内容

PfR 管理の出口リンクとしての VPN IPsec/GRE トンネル インターフェイスの設定に関する前提条件

- VPN IPsec/GRE トンネル インターフェイスを PfR 管理の出口リンクとして実装するには、PfR の機能および PfR ネットワーク コンポーネントの設定方法について理解する必要があります。詳細については、「Understanding Performance Routing」モジュール、「Configuring Basic Performance Routing」モジュール、および「Configuring Advanced Performance Routing」モジュールを参照してください。その他の PfR 機能モジュールのリストについては、「関連資料」（P.18）を参照してください。
- Cisco Express Forwarding（CEF; シスコ エクスプレス フォワーディング）は、すべての参加ルータでイネーブルにする必要があります。
- ルーティング プロトコル ピアリングまたはスタティック ルーティングが、PfR 管理のネットワークで設定されている必要があります。
- 標準の Cisco PfR ボーダー ルータおよびマスター コントローラ設定が完了している必要があります。

PfR 管理の出口リンクとしての VPN IPsec/GRE トンネル インターフェイスの設定に関する制約事項

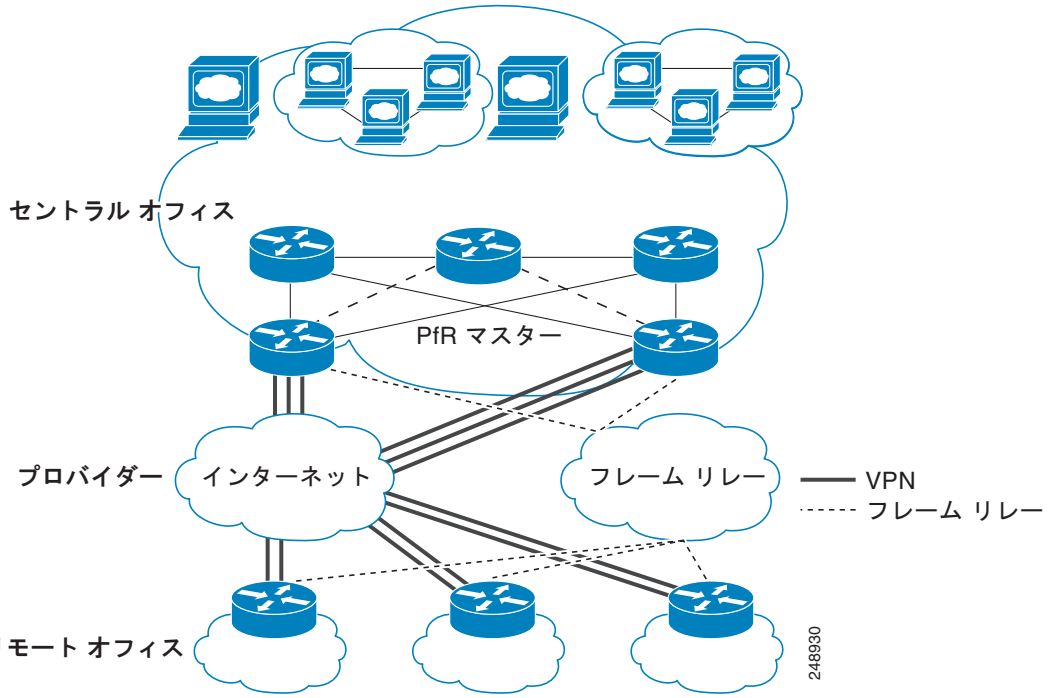
Cisco IOS PfR は、IPsec/GRE トンネル インターフェイスを介してルーティングされるプレフィクスの最適化をサポートします。GRE およびマルチポイント GRE VPN トンネルだけがサポートされています。

PfR 管理の出口リンクとしての VPN IPsec/GRE トンネル インターフェイスの設定の概要

VPN IPsec/GRE トンネル インターフェイスの最適化

Cisco IOS PfR は、IPsec/GRE トンネル インターフェイスを介してルーティングされるプレフィクスの最適化をサポートします。VPN トンネル インターフェイスは、マスター コントローラの PfR 外部インターフェイスとして設定されます。図 1 に、VPN トラフィックを最適化するように設定された PfR 管理のネットワークを示します。ここでは、Cisco IOS PfR は、セントラル オフィスおよびリモート オフィスに導入されます。

図 1　　VPN ルーティングが最適化された Cisco IOS PfR ネットワーク



この拡張により、2 方向の VPN 最適化の設定が可能になります。マスター コントローラおよびボーダー ルータ プロセスは、VPN の両側でイネーブルになります。各サイトでは、マスター コントローラ データベースが別々に保持されます。VPN ルートは、トンネル インターフェイスを介してダイナミックに学習したり、または設定したりできます。プレフィクスおよび出口リンク ポリシーは、標準の Cisco IOS PfR 設定を介して VPN プレフィクスで設定されます。

IPsec over GRE トンネルを使用したルート プレフィクスの保護

IPsec-to-GRE モデルでは、サービス プロバイダーは、IP バックボーンを介して VPN サービスを提供できます。セントラルおよびリモート VPN クライアントの両方は、IPsec-to-IPsec モデルに従い終了します。プレフィクスは、GRE トンネルを使用してカプセル化されます。GRE パケットは IPsec により保護されます。カプセル化されたプレフィクスは、セントラル VPN サイトから、GRE のもう一方のエンドポイントであるカスタマー ヘッドエンド ルータに転送されます。IPsec で保護される GRE パケットにより、サービス プロバイダー ネットワークの IP バックボーンに安全な接続が提供されます。

IPsec over GRE トンネルの設定の詳細については、次の URL で公開されている『*Dynamic Multipoint IPsec VPNs (Using Multipoint GRE/NHRP to Scale IPsec VPNs)*』マニュアルを参照してください。

http://www.cisco.com/en/US/tech/tk583/tk372/technologies_white_paper09186a008018983e.shtml

PfR 管理の出口リンクとしての GRE トンネル インターフェイスの設定

ボーダー ルータの GRE トンネル インターフェイスは、マスター コントローラの PfR 外部インターフェイスとして設定します。PfR 管理のネットワークの個別の物理インターフェイスに、少なくとも 2 つの外部トンネル インターフェイスを設定する必要があります。これらのインターフェイスは、単一のボーダー ルータまたは複数のボーダー ルータで設定できます。内部インターフェイスは、通常、ボーダー ルータにあり、マスター コントローラが到達可能な物理インターフェイスを使用して設定します。

PfR 管理の出口リンクとして VPN IPsec/GRE トンネル インターフェイスを設定する方法

GRE トンネルを介した IPsec VPN プレフィクスの監視および制御のための PfR の設定

GRE トンネルを介した IPsec VPN を設定するには、次のタスクを実行します。最初に、IPsec VPN はボーダー ルータで設定され、トンネル インターフェイスはマスター コントローラで PfR 管理の外部インターフェイスとして設定されます。このタスクでは、IKE ポリシーの定義、トランスフォーム セットの設定、クリプト プロファイルおよびクリプト マップの定義、GRE トンネルの設定を行います。

このタスクの GRE トンネルおよび IPsec 保護は、ボーダー ルータで設定されます。このタスクの設定手順は、単一のトンネルの設定方法を示しています。PfR 管理のネットワークのボーダー ルータに、少なくとも 2 つのトンネルを設定する必要があります。IPsec 設定は、各トンネル エンドポイント（セントラルおよびリモート サイト）で適用する必要があります。

制約事項

Cisco IOS PfR は、IPsec/GRE VPN だけをサポートします。他の VPN タイプはサポートされていません。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto ipsec security-association lifetime** {**seconds** *seconds* | **kilobytes** *kilobytes*}
4. **crypto ipsec transform-set** *transform-set-name transform1* [*transform2*] [*transform3*] [*transform4*]
5. **mode** [**tunnel** | **transport**]
6. **exit**
7. **crypto map** *map-name seq-num* [**ipsec-isakmp**]
8. **set peer** {*host-name* [**dynamic**] [**default**] | *ip-address* [**default**]}
9. **set transform-set** *transform-set-name* [*transform-set-name2...transform-set-name6*]
10. **match address** [*access-list-id* | *name*]
11. **exit**
12. **crypto ipsec profile** *name*
13. **set transform-set** *transform-set-name* [*transform-set-name2...transform-set-name6*]
14. **exit**
15. **crypto map** *map-name* **local-address** *interface-id*
16. **crypto isakmp key** *encryption-level key-string* {**address** *peer-address* [*mask*] | **hostname** *name*} [**no-xauth**]
17. **crypto isakmp keepalive** *seconds* [*retries*] [**periodic** | **on-demand**]
18. **crypto isakmp policy** *priority*
19. **encryption** {**des** | **3des** | **aes** | **aes 192** | **aes 256**}
20. **authentication** {**rsa-sig** | **rsa-encr** | **pre-share**}
21. **exit**
22. **interface** *type number* [*name-tag*]
23. **ip address** *ip-address mask* [**secondary**]
24. **crypto map** *map-name* [**redundancy** *standby-name*]
25. exit
26. **interface** *type number* [*name-tag*]
27. **ip address** *ip-address mask* [**secondary**]
28. **keepalive** [*period* [*retries*]]
29. **bandwidth** {*kbps* | **inherit** [*kbps*]}
30. **tunnel mode gre ip**
31. **tunnel source** {*ip-address* | *interface-type interface-number*}
32. **tunnel destination** {*host-name* | *ip-address*}
33. **tunnel protection ipsec profile** *name* [**shared**]
34. **exit**
35. **ip route** *prefix mask* {*ip-address* | *interface-type interface-number* [*ip-address*]} [**dhcp**] [*distance*] [*name*] [**permanent**] [**tag** *tag*]

36. **access-list** *access-list-number* [**dynamic** *dynamic-name* [**timeout** *minutes*]] {**deny** | **permit**} *protocol source source-wildcard destination destination-wildcard* [**precedence** *precedence*] [**tos** *tos*] [**log** | **log-input**] [**time-range** *time-range-name*] [**fragments**]
37. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	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 3	**crypto ipsec security-association lifetime** {**seconds** *seconds* | **kilobytes** *kilobytes*} **例：** `Router(config)# crypto ipsec security-association lifetime kilobytes 530000000`	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。 • この例では、このセキュリティ アソシエーションの IPsec ピア間で転送できるトラフィックのボリュームを KB 単位で設定しています。
ステップ 4	**crypto ipsec transform-set** *transform-set-name transform1* [*transform2*] [*transform3*] [*transform4*] **例：** `Router(config)# crypto ipsec transform-set VPN_1 esp-des esp-3des esp-sha-hmac`	クリプト トランスフォーム コンフィギュレーション モードを開始して、トランスフォーム セット（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）を作成または変更します。 • この例では、認証に 56 ビット Data Encryption Standard（DES; データ暗号規格）、168 ビット DES、または Secure Hash Algorithm（SHA）を指定します。
ステップ 5	**mode** [**tunnel** | **transport**] **例：** `Router(cfg-crypto-trans)# mode transport`	トランスフォーム セットのモードを設定します。 • この例では、モードを transport に設定します。デフォルト モードは、tunnel です。tunnel モードでは、パケット全体が保護されます。transport モードでは、ペイロードだけが保護されます。カプセル化は GRE により実行されます。
ステップ 6	**exit** **例：** `Router(cfg-crypto-trans)# exit`	クリプト トランスフォーム コンフィギュレーション モードを終了して、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 7	**crypto map** *map-name seq-num* [**ipsec-isakmp**] **例：** `Router(config)# crypto map TUNNEL 10 ipsec-isakmp`	クリプト マップ コンフィギュレーション モードを開始して、クリプト マップを作成または変更します。 • この例では、TUNNEL という名前のクリプト マップを作成し、セキュリティ アソシエーションを確立するように IKE を設定します。

	コマンドまたはアクション	目的
ステップ 8	**set peer** {*host-name* [**dynamic**] [**default**] | *ip-address* [**default**]} **例：** `Router(config-crypto-map)# set peer 10.4.9.81`	クリプト マップ エントリで IPsec ピアを指定します。
ステップ 9	**set transform-set** *transform-set-name* [*transform-set-name2...transform-set-name6*] **例：** `Router(config-crypto-map)# set transform-set VPN_1`	クリプト 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 4 で設定した、トランスフォーム セット VPN_1 を指定します。
ステップ 10	**match address** [*access-list-id* | *name*] **例：** `Router(config-crypto-map)# match address 100`	拡張アクセス リストを指定して、クリプト マップ エントリの IPsec ピアを定義します。 • アクセス リストは、ステップ 36 で定義します。
ステップ 11	**exit** **例：** `Router(config-crypto-map)# exit`	クリプト マップ コンフィギュレーション モードを終了して、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 12	**crypto ipsec profile name** **例：** `Router(config)# crypto ipsec profile PFR`	2 つの IPsec ルータ間の IPsec 暗号化に使用される IPsec パラメータを定義して、IPsec プロファイル コンフィギュレーション モードを開始します。 • この例では、PFR という名前のプロファイルを作成します。
ステップ 13	**set transform-set** *transform-set-name* [*transform-set-name2...transform-set-name6*] **例：** `Router(ipsec-profile)# set transform-set VPN_1`	クリプト 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 4 で設定した、トランスフォーム セット VPN_1 を指定します。
ステップ 14	**exit** **例：** `Router(ipsec-profile)# exit`	IPsec プロファイル コンフィギュレーション モードを終了して、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 15	**crypto map** *map-name* **local-address** *interface-id* **例：** `Router(config)# crypto map TUNNEL local-address FastEthernet 0/0`	定義したクリプト マップを指定のインターフェイスに適用します。 • この例では、TUNNEL という名前のクリプト マップをインターフェイス FastEthernet 0/0 に適用します。
ステップ 16	**crypto isakmp key** *encryption-level key-string* {**address** *peer-address* [*mask*] | **hostname** *name*} [**no-xauth**] **例：** `Router(config)# crypto isakmp key 0 CISCO address 10.4.9.81 no-xauth`	事前共有認証キーを作成します。 • この例では、暗号化レベル 0 を設定して、拡張認証に IPsec ピアを要求しないようにルータを設定します。ただし、暗号化レベルまたは認証レベルは指定できます。

	コマンドまたはアクション	目的
ステップ 17	**crypto isakmp keepalive** *seconds* [*retries*] [**periodic** | **on-demand**] **例：** `Router(config)# crypto isakmp keepalive 10`	ゲートウェイからピアに Dead Peer Detection（DPD）メッセージを送信できるようにします。
ステップ 18	**crypto isakmp policy** *priority* **例：** `Router(config)# crypto isakmp policy 1`	Internet Key Exchange（IKE; インターネット キー エクスチェンジ）ポリシーを定義して、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 19	**encryption** {**des** | **3des** | **aes** | **aes 192** | **aes 256**} **例：** `Router(config-isakmp)# encryption 3des`	IKE ポリシー内での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 暗号化を指定します。
ステップ 20	**authentication** {**rsa-sig** | **rsa-encr** | **pre-share**} **例：** `Router(config-isakmp)# authentication pre-share`	IKE ポリシー内での認証方式を指定します。 • この例では、事前共有キーが使用されるように指定します。
ステップ 21	**exit** **例：** `Router(config-isakmp)# exit`	ISAKMP ポリシー コンフィギュレーション モードを終了して、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 22	**interface** *type number* [*name-tag*] **例：** `Router(config)# interface FastEthernet0/0`	インターフェイス タイプを設定し、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。 • 物理インターフェイスは、ここで定義されます。
ステップ 23	**ip address** *ip-address mask* [**secondary**] **例：** `Router(config-if)# ip address 10.4.9.14 255.255.255.0`	インターフェイスに対するプライマリ IP アドレスまたはセカンダリ IP アドレスを設定します。
ステップ 24	**crypto map** *map-name* [**redundancy** *standby-name*] **例：** `Router(config-if)# crypto map TUNNEL`	クリプト マップ セットをインターフェイスに適用します。 • この例では、ステップ 7 で定義された、TUNNEL という名前のクリプト マップを指定します。
ステップ 25	**exit** **例：** `Router(config-if)# exit`	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 26	**interface** *type number* [*name-tag*] **例：** `Router(config)# interface Tunnel0`	インターフェイス タイプを設定し、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。 • トンネル インターフェイスは、ここで定義されます。

	コマンドまたはアクション	目的
ステップ 27	**ip address** *ip-address mask* [**secondary**] **例：** `Router(config-if) ip address 10.100.2.1 255.255.0.0`	インターフェイスに対するプライマリ IP アドレスまたはセカンダリ IP アドレスを設定します。
ステップ 28	**keepalive** [*period* [*retries*]] **例：** `Router(config-if) keepalive 30 5`	キープアライブ パケットをイネーブルにし、Cisco IOS ソフトウェアがインターフェイスをダウンさせる前に、またはトンネル プロトコルを特定のインターフェイスでダウンさせる前に応答なしでキープアライブ パケットを送信する回数を指定します。

ステップ 29	**bandwidth** {*kbps* | **inherit** [*kbps*]}
	
	例：
	`Router(config-if)# bandwidth 500`
	
	`Router(config-if)# bandwidth inherit`
		インターフェイスの現在の帯域幅値をより高いレベルのプロトコルに設定し通信します。

ステップ 30	**tunnel mode gre ip** **例：** `Router(config-if)# tunnel mode gre ip`	トンネル インターフェイスの暗号化モードを設定します。 **（注）** ここでは構文の一部だけを示します。詳細については、『*Cisco IOS Interface and Hardware Component Command Reference*』を参照してください。
ステップ 31	**tunnel source** {*ip-address* | *interface-type interface-number*} **例：** `Router(config-if)# tunnel source 10.4.9.14`	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。 • この例の送信元インターフェイスは、ステップ 22 で定義しました。インターフェイス名または IP アドレスを指定できます。
ステップ 32	**tunnel destination** {*host-name* | *ip-address*} **例：** `Router(config-if)# tunnel destination 10.4.9.81`	トンネル インターフェイスの宛先を指定します。 • リモート トンネル エンドポイントが接続される物理インターフェイスの IP アドレスをここで設定します。
ステップ 33	**tunnel protection ipsec profile** *name* [**shared**] **例：** `Router(config-if)# tunnel protection ipsec profile PFR`	トンネル インターフェイスを IPsec プロファイルに関連付けます。 • この例で設定する PFR という名前の IPsec プロファイルは、ステップ 19 で定義しています。
ステップ 34	**exit** **例：** `Router(config-if)# exit`	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 35	**ip route** *prefix mask* {*ip-address* | *interface-type interface-number* [*ip-address*]} [**dhcp**] [*distance*] [*name*] [**permanent**] [**tag** *tag*] **例：** `Router(config)# ip route 10.2.2.2 255.255.255.255 Tunnel0`	スタティック ルートを確立します。 • トンネル宛先ホストまたはネットワークのデフォルト ルートを設定します。

	コマンドまたはアクション	目的
ステップ 36	**access-list** *access-list-number* [**dynamic** *dynamic-name* [**timeout** *minutes*]] {**deny** | **permit**} *protocol source source-wildcard destination destination-wildcard* [**precedence** *precedence*] [**tos** *tos*] [**log** | **log-input**] [**time-range** *time-range-name*] [**fragments**] **例：** `Router(config)# access-list 100 permit gre host 10.4.9.14 host 10.4.9.81`	拡張 IP アクセス リストを作成または設定します。 • 拡張アクセス リストは、GRE ホストだけを許可するように定義します。 • この例のアクセス リストは、ステップ 10 の **match address** ステートメントで参照されます。
ステップ 37	**end** **例：** `Router(config)# end`	グローバル コンフィギュレーション モードを終了して、特権 EXEC モードを開始します。

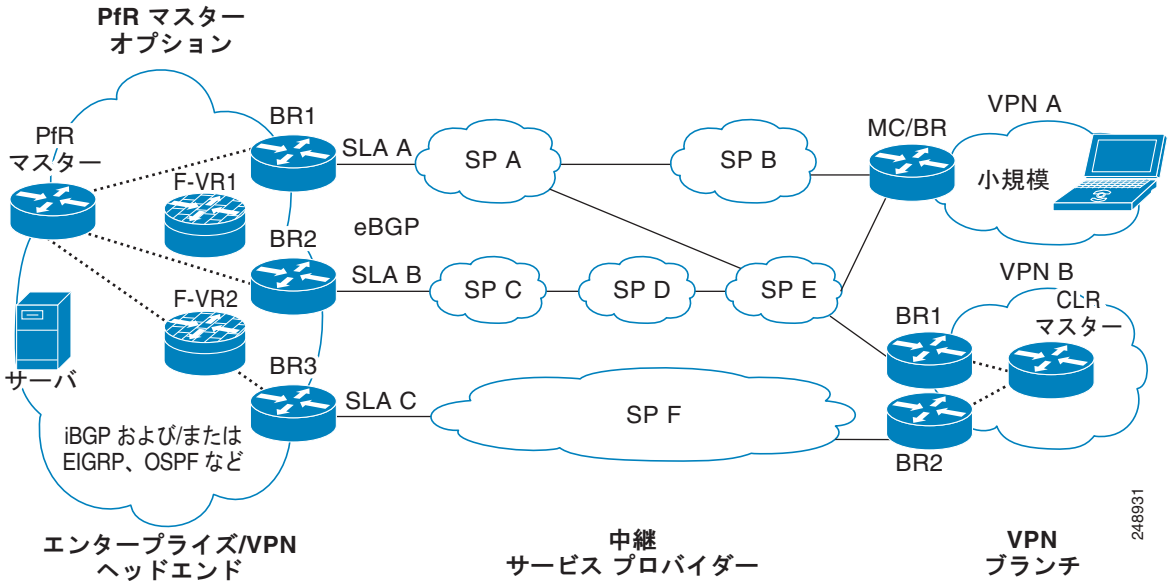
PfR 管理の出口リンクとしての VPN IPsec/GRE トンネル インターフェイスの設定例

• 「例：GRE/IPsec VPN プレフィクスの監視および制御のための PfR の設定」（P.10）

例：GRE/IPsec VPN プレフィクスの監視および制御のための PfR の設定

図 2 に、1 つのセントラル VPN サイトと 2 つのリモート VPN サイトを示します。VPN ピアリングは、サービス プロバイダー クラウドを介して確立されます。PfR 管理のネットワークは、Cisco IOS PfR 設定が個別に適用される各サイトで設定します。各サイトには、個別のマスター コントローラおよびボーダー ルータ プロセスがあり、個別のマスター コントローラ データベースを保持します。

図 2　PfR 管理のネットワークにより制御される VPN サイト



各リモート サイトとセントラル サイトの間に 2 つの GRE トンネルが設定されています。VPN プレフィクスは、GRE トンネルで暗号化され、暗号化されたプレフィクスは、IPsec 暗号化で保護されます。この例では、セントラル VPN サイト、VPN A および VPN B の設定を示しています。

セントラル VPN 設定：PfR マスター コントローラ

セントラル VPN サイトは、VPN A および VPN B とのピアを確立します。各サイトでは、PfR マップを使用して個別のポリシーを定義します。VPN A プレフィクスでは、80 ms の遅延ポリシーが設定され、ポリシー違反プレフィクスは、ポリシー準拠の最初の出口に送られます。VPN B プレフィクスでは、40 ms の遅延ポリシーおよび相対損失ポリシーが設定され、ポリシー違反プレフィクスは、利用可能な最良の出口に送られます。

```
key chain PFR
 key 1
  key-string CISCO
!
pfr master
 logging
 border 10.4.9.6 key-chain PFR
  interface Ethernet 0/0 external
  interface Ethernet 0/1 internal
!
 border 10.4.9.7 key-chain PFR
  interface Ethernet 0/0 external
  interface Ethernet 0/1 internal
!
 mode route control
 mode monitor both
 exit
!
ip prefix VPN A permit 10.4.9.25
pfr-map VPNA
 match ip address prefix-list VPNB
 set delay 800
 set mode select-exit good
 exit
!
ip prefix VPNB permit 10.4.9.254
```

```
pfr-map VPNB
 match ip address prefix-list VPNC
 set delay 400
 set loss relative 100
 set resolve loss priority 1 variance 10
 set mode select-exit best
 end
```

セントラル VPN 設定：BR1

次に、BR1 のセントラル VPN 設定の例（グローバル コンフィギュレーション モード）を示します。

```
key chain PFR
 key 1
  key-string CISCO
!
pfr border
 local serial 0/1
 master 10.4.9.4 key-chain PFR
!
ip route 10.70.1.0 255.255.255.0
!
route-map REDISTRIBUTE_STATIC
 match tag 5000
 set metric -10
 exit
!
router eigrp 1
 network 10.70.0.0 0.0.0.255
 redistribute static route-map REDISTRIBUTE_STATIC
 exit
!
crypto ipsec security-association lifetime kilobytes 530000000
crypto ipsec security-association lifetime second 14400
crypto ipsec transform-set VPN_1 esp-3des esp-sha-hmac
 mode transport
 exit
!
crypto map TUNNEL 10 ipsec-isakmp
 set peer 10.4.9.81
 set transform-set VPN_1
 match address 100
!
crypto ipsec profile PFR
 set transform-set VPN_1
 exit
crypto map TUNNEL local-address Ethernet 0/0
!
crypto isakmp key 0 CISCO address 10.4.9.81 no-xauth
crypto isakmp keepalive 10
crypto isakmp policy 1
 encryption 3des
 authentication pre-share
 exit
!
interface Ethernet0/0
 ip address 10.4.9.14 255.255.255.0
 crypto map TUNNEL
 exit
!
interface Tunnel0
 ip address 10.100.2.1 255.255.0.0
 keepalive 30 5
 bandwidth 500
```

```
 bandwidth inherit
 tunnel mode gre ip
 tunnel source 10.4.9.14
 tunnel destination 10.4.9.81
 tunnel protection ipsec profile PFR
 exit
```

セントラル VPN 設定：BR2

次に、BR2 のセントラル VPN 設定の例（グローバル コンフィギュレーション モード）を示します。

```
key chain PFR
 key 1
  key-string CISCO
!
pfr border
 local Ethernet 0/1
 master 10.4.9.4 key-chain PFR
!
ip route 10.70.1.0 255.255.255.0
!
route-map REDISTRIBUTE_STATIC
 match tag 5000
 set metric -10
 exit
!
router eigrp 1
 network 10.70.0.0 0.0.0.255
 redistribute static route-map REDISTRIBUTE_STATIC
!
crypto ipsec security-association lifetime kilobytes 530000000
crypto ipsec security-association lifetime second 14400
crypto ipsec transform-set VPN_1 esp-3des esp-sha-hmac
 mode transport
 exit
!
crypto map TUNNEL 10 ipsec-isakmp
 set peer 10.4.9.82
 set transform-set VPN_1
 match address 100
!
crypto ipsec profile PFR
 set transform-set VPN_1
 exit
crypto map TUNNEL local-address Ethernet 0/0
!
crypto isakmp key 0 CISCO address 10.4.9.82 no-xauth
crypto isakmp keepalive 10
crypto isakmp policy 1
 encryption 3des
 authentication pre-share
 exit
!
interface Ethernet0/0
 ip address 10.4.9.15 255.255.255.0
 crypto map TUNNEL
 exit
!
interface Tunnel0
 ip address 10.100.2.2 255.255.0.0
 keepalive 30 5
 bandwidth 500
 bandwidth inherit
 tunnel mode gre ip
```

```
 tunnel source 10.4.9.15
 tunnel destination 10.4.9.82
 tunnel protection ipsec profile PFR
 end
```

セントラル VPN 設定：内部ピア

次の例に、ボーダー ルータと内部ピアとのピアを確立する EIGRP ルーティング プロセスを示します。

```
router eigrp 1
 network 10.50.1.0 0.0.0.255
 redistribute static route-map REDISTRIBUTE_STATIC
 end
```

VPN A 設定：MC/BR

次に、VPN A 設定の設定例（グローバル コンフィギュレーション モード）を示します。VPN A は、Small Office Home Office（SOHO）クライアント用に設定されるリモート サイトです。ルータは 1 つ導入されます。このルータは、サービス プロバイダー B およびサービス プロバイダー E とのピアを確立します。このネットワークには Interior Gateway Protocol（IGP）は導入されず、セントラル サイトのリモート トンネル エンドポイントにスタティック ルートだけが設定されています。遅延ポリシー、損失ポリシー、および最良の出口リンク選択が設定され、トラフィックは、常に、最も低い遅延時間およびパケット損失の ISP を経由するようにルーティングされます。解決ポリシーは、損失の優先順位が最高になるように設定されています。この例では、物理インターフェイス設定もルータ IGP ピアリング設定も示されていません。

```
key chain BR1
 key 1
  key-string CISCO
!
```

（注） ローカル ボーダー ルータ プロセスはイネーブルです。ボーダー ルータおよびマスター コントローラ プロセスは同じルータでイネーブルであるため、ループバック インターフェイス（192.168.0.1）は、ローカル インターフェイスとして設定されます。

```
pfr border
 local Loopback0
 master 192.168.0.1 key-chain BR1
!
pfr master
 learn
 delay
 mode route control
 delay threshold 100
 loss relative 200
 periodic 300
 mode select-exit good
resolve loss priority 1 variance 20
resolve delay priority 2 variance 10
!
 border 192.168.0.1 key-chain BR1
  interface Serial0/0 internal
  interface Tunnel0 external
  interface Tunnel0 external
  exit
!
crypto ipsec security-association lifetime kilobytes 530000000
crypto ipsec security-association lifetime second 14400
crypto ipsec transform-set VPN_1 esp-3des esp-sha-hmac
 mode transport
 exit
```

```
!
crypto map TUNNEL 10 ipsec-isakmp
 set peer 10.4.9.81
 set transform-set VPN_1
 match address 100
!
crypto ipsec profile PFR
 set transform-set VPN_1
 exit
crypto map TUNNEL local-address Ethernet 0/0
!
crypto isakmp key 0 CISCO address 10.4.9.81 no-xauth
crypto isakmp keepalive 10
crypto isakmp policy 1
 encryption 3des
 authentication pre-share
 exit
!

interface Ethernet0/0
 ip address 10.4.9.14 255.255.255.0
 crypto map TUNNEL
 exit
!
interface Tunnel0
 ip address 10.100.2.1 255.255.0.0
 keepalive 30 5
 bandwidth 500
 bandwidth inherit
 tunnel mode gre ip
 tunnel source 10.4.9.14
 tunnel destination 10.4.9.81
 tunnel protection ipsec profile PFR
 exit
!
```

（注） この例では、単一のトンネル設定が示されています。VPN 最適化を設定するには、トンネルは 2 つ必要です。

VPN B 設定：PfR マスター コントローラ

次に、VPN B でのマスター コントローラ設定の例（グローバル コンフィギュレーション モード）を示します。負荷分散およびルート制御モードはイネーブルです。ポリシー違反プレフィクスは、ポリシー準拠の最初の出口に送られるように設定されています。

```
key chain PFR
 key 1
  key-string CISCO
!
pfr master
 logging
 border 10.4.9.6 key-chain PFR
  interface Ethernet 0/0 external
  interface Ethernet 0/1 internal
!
 border 10.4.9.7 key-chain PFR
  interface Ethernet 0/0 external
  interface Ethernet 0/1 internal
!
mode route control
mode select-exit good
max-range utilization
```

```
!
 learn
  delay
  end
```

VPN B 設定：BR1

次に、BR1 の VPN B 設定の例（グローバル コンフィギュレーション モード）を示します。

```
key chain PFR
 key 1
  key-string CISCO
!
pfr border
 local Ethernet 0/1
 master 10.4.9.4 key-chain PFR
!
route-map REDISTRIBUTE_STATIC
 match tag 5000
 set metric -10
 exit
!
router rip
 network 10.60.1.0
 redistribute static route-map REDISTRIBUTE_STATIC
 end
!
crypto ipsec security-association lifetime kilobytes 530000000
crypto ipsec security-association lifetime second 14400
crypto ipsec transform-set VPN_1 esp-3des esp-sha-hmac
 mode transport
 exit
!
crypto map TUNNEL 10 ipsec-isakmp
 set peer 10.4.9.82
 set transform-set VPN_1
 match address 100
!
crypto ipsec profile PFR
 set transform-set VPN_1
 exit
crypto map TUNNEL local-address Ethernet 0/0
!
crypto isakmp key 0 CISCO address 10.4.9.82 no-xauth
crypto isakmp keepalive 10
crypto isakmp policy 1
 encryption 3des
 authentication pre-share
 exit
!
interface Ethernet0/0
 ip address 10.4.9.15 255.255.255.0
 crypto map TUNNEL
 exit
!
interface Tunnel0
 ip address 10.100.2.2 255.255.0.0
 keepalive 30 5
 bandwidth 500
 bandwidth inherit
 tunnel mode gre ip
 tunnel source 10.4.9.15
 tunnel destination 10.4.9.82
 tunnel protection ipsec profile PFR
```

```
 end
```

VPN B 設定：BR2

次に、BR2 の VPN B 設定の例（グローバル コンフィギュレーション モード）を示します。

```
key chain PFR
 key 1
  key-string CISCO
!
pfr border
 local Ethernet 0/1
 master 10.4.9.4 key-chain PFR
 exit
!
route-map REDISTRIBUTE_STATIC
 match tag 5000
 set metric -10
 exit
!
router rip
 network 10.60.1.0
 redistribute static route-map REDISTRIBUTE_STATIC
 exit
!
crypto ipsec security-association lifetime kilobytes 530000000
crypto ipsec security-association lifetime second 14400
crypto ipsec transform-set VPN_1 esp-3des esp-sha-hmac
 mode transport
 exit
!
crypto map TUNNEL 10 ipsec-isakmp
 set peer 10.4.9.82
 set transform-set VPN_1
 match address 100
!
crypto ipsec profile PFR
 set transform-set VPN_1
 exit
crypto map TUNNEL local-address Ethernet 0/0
!
crypto isakmp key 0 CISCO address 10.4.9.82 no-xauth
crypto isakmp keepalive 10
crypto isakmp policy 1
 encryption 3des
 authentication pre-share
 exit
!
interface Ethernet0/0
 ip address 10.4.9.15 255.255.255.0
 crypto map TUNNEL
 exit
!
interface Tunnel0
 ip address 10.100.2.2 255.255.0.0
 keepalive 30 5
 bandwidth 500
 bandwidth inherit
 tunnel mode gre ip
 tunnel source 10.4.9.15
 tunnel destination 10.4.9.82
 tunnel protection ipsec profile PFR
 end
```

VPN B 設定：内部ピア

次の例に、ボーダー ルータと内部ピアとのピアリングを確立する Routing Information Protocol（RIP; ルーティング情報プロトコル）ルーティング プロセスを示します。

```
router rip
 network 10.60.1.0
 end
```

次の作業

このモジュールは、VPN IPsec/GRE トンネル インターフェイスを PfR 管理の出口リンクとして設定する方法について説明しており、PfR テクノロジーを熟知していることを前提としています。PfR の詳細については、「関連資料」（P.18）に記載された資料を参照してください。

参考資料

関連資料

関連項目	参照先
Cisco IOS コマンド	『*Cisco IOS Master Commands List, All Releases*』
Cisco PfR コマンド（コマンド構文の詳細、コマンド モード、コマンド履歴、デフォルト、使用上の注意事項、および例）	『*Cisco IOS Performance Routing Command Reference*』
ベーシック PfR 設定	「Configuring Basic Performance Routing」モジュール
アドバンスド PfR の設定	「Configuring Advanced Performance Routing」モジュール
パフォーマンス ルーティングの運用フェーズを理解するために必要な概念	「Understanding Performance Routing」モジュール
PfR 機能の位置	「Cisco IOS Performance Routing Features Roadmap」モジュール
キー チェーン認証：Cisco IOS ソフトウェアでの認証キー設定および管理に関する情報	『*Cisco IOS IP Routing: Protocol-Independent Configuration Guide*』の「Configuring IP Routing Protocol-Independent Features」の章の「Managing Authentication Keys」の項

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。 以下を含むさまざまな作業にこの Web サイトが役立ちます。 ・テクニカル サポートを受ける ・ソフトウェアをダウンロードする ・セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける ・ツールおよびリソースへアクセスする - Product Alert の受信登録 - Field Notice の受信登録 - Bug Toolkit を使用した既知の問題の検索 ・Networking Professionals（NetPro）コミュニティで、技術関連のディスカッションに参加する ・トレーニング リソースへアクセスする ・TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

PfR 管理の出口リンクとしての VPN IPsec/GRE トンネル インターフェイスの設定の機能情報

表 1 に、この機能のリリース履歴を示します。

プラットフォームのサポートおよびソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator を使用すると、ソフトウェア イメージがサポートする特定のソフトウェア リリース、機能セット、またはプラットフォームを確認できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスしてください。Cisco.com のアカウントは必要ありません。

（注） 表 1 には、一連のソフトウェア リリースのうち、特定の機能が初めて導入されたソフトウェア リリースだけが記載されています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

表 1　VPN IPsec/GRE トンネル インターフェイス最適化の機能情報

機能名	リリース	機能情報
VPN IPsec/GRE トンネル最適化	12.3(11)T	IPsec/GRE トンネル インターフェイスを PfR 管理の出口リンクとして設定できる機能を導入しました。