逆ルート注入

Reverse Route Injection（RRI; 逆ルート注入）とは、リモート トンネル エンドポイントによって保護されているネットワークおよびホストのルーティング プロセスに、スタティック ルートを自動的に組み込む機能です。保護されているホストおよびネットワークをリモート プロキシ ID といいます。

各ルートはリモート プロキシ ネットワークおよびマスクを基に作成され、このネットワークへのネクストホップがリモート トンネル エンドポイントになります。ネクストホップとして Virtual Private Network（VPN; バーチャル プライベート ネットワーク）のリモート ルータを使い、暗号化プロセスによってトラフィックを強制的に暗号化します。

Cisco IOS Release 12.3(14)T の Reverse Route Injection（RRI）機能に、RRI のデフォルト動作の拡張機能、ルート タグ値の追加、RRI の設定方法の拡張機能が追加されました。

Cisco IOS Release 12.4(15)T には、VPN プロセスによって作成されたルートにディスタンス メトリックを設定する拡張機能が追加されました。この拡張機能により、ルータでダイナミックに学習されたルートを、ローカルに設定されているスタティック ルートより優先されることができます。

この章で紹介する機能情報の入手方法

*ご使用の Cisco IOS ソフトウェア リリースでは、この章で説明されるすべての機能がサポートされているとは限りません。*この章に記載されている特定の機能に関する説明へのリンク、および各機能がサポートされているリリースのリストについては、「RPI の機能情報」（P.18）を参照してください。

プラットフォーム、Cisco IOS ソフトウェア イメージ、および Cisco Catalyst OS ソフトウェア イメージの各サポート情報を検索するには

Cisco Feature Navigator を使用すると、プラットフォーム、Cisco IOS ソフトウェア イメージ、および Cisco Catalyst OS 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://tools.cisco.com/ITDIT/CFN/jsp/index.jsp からアクセスできます。Cisco.com のアカウントは必要ありません。

この章の構成

逆ルート注入の前提条件

- RRI で生成されたスタティック ルートの伝播にダイナミック ルーティング プロトコルを使用する場合は、IP ルーティングをイネーブルにし、スタティック ルートを再配布する必要があります。

逆ルート注入の制約事項

- RRI をクリプト マップに適用する際、そのクリプト マップはルータのインターフェイスごとに一意でなければなりません。つまり、同じクリプト マップは複数のインターフェイスに適用できないということです。複数のクリプト マップを複数のインターフェイスに適用すると、ルートが正しくクリーンアップされないことがあります。複数のインターフェイスに 1 つのクリプト マップが必要な場合は、一意に定義したマップを各インターフェイスで使用する必要があります。この制約があるのは、Cisco IOS Release 12.3(14)T 以前のリリースの RRI だけです。
- スタティック クリプト マップでは、適用済みのクリプト マップに RRI が設定されている場合、必ずルートが存在します。Cisco IOS Release 12.3(14)T では、（スタティック マップに常に存在するルートの）デフォルトの動作は適用されません。ただし、キーワード **static** を **reverse-route** コマンドに追加している場合は除きます。

逆ルート注入に関する情報

逆ルート注入の拡張機能を設定するには、次の概念を理解しておく必要があります。

逆ルート注入

RRI とは、リモート トンネル エンドポイントによって保護されているネットワークとホストのルーティング プロセスに、スタティック ルートを自動的に組み込む機能です。保護されているホストおよびネットワークをリモート プロキシ ID といいます。

各ルートはリモート プロキシ ネットワークおよびマスクを基に作成され、このネットワークへのネクストホップがリモート トンネル エンドポイントになります。ネクストホップとして VPN のリモート ルータを使い、暗号化プロセスによってトラフィックを強制的に暗号化します。

スタティック ルートを VPN ルータ上に作成すると、その情報がアップストリーム デバイスに伝播され、戻されてくるトラフィックの送信先となる適切な VPN ルータが判定可能になることで、IPsec のステート フローを維持します。適切な VPN ルータを判定することができれば、サイトで複数の VPN ルータを使用してロード バランシングやフェールオーバーを実行する場合や、デフォルト ルートでリ

モート VPN デバイスにアクセスできない場合に特に役立ちます。ルートは、グローバル ルーティング テーブルまたは適切な Virtual Route Forwarding（VRF; VPN ルーティングおよび転送）テーブルに作成されます。

スタティック クリプト マップ テンプレートであってもダイナミック クリプト マップ テンプレートであっても、RRI はクリプト マップごとに適用されます。この 2 つのタイプのマップのデフォルト動作は次のとおりです。

- ダイナミック クリプト マップでは、ルートは、リモート プロキシの IPsec セキュリティ アソシエーション（SA）が正常に確立されるとすぐに作成されます。これらのリモート プロキシに戻るネクストホップは、ダイナミック クリプト マップ テンプレートの作成中に学習、適用されるアドレスのリモート VPN ルータを経由します。このルートは SA の削除後に削除されます。Cisco IOS Release 12.3(14)T には、スタティック クリプト マップの IPsec ソース プロキシを基にしたルート作成が追加されました。この動作がスタティック マップでのデフォルトの動作になり、クリプト ACL を基にしたルート作成（次の黒丸を参照）を無効にしました。
- スタティック クリプト マップでは、クリプト アクセス リストに定義されている宛先情報を基にルートが作成されます。ネクストホップは、クリプト マップにアタッチされている最初の set peer 文から取得します。RRI、ピア、またはアクセス リストがクリプト マップから削除されると、必ずルートも削除されます。この動作は、以降の項で説明するように、RRI の拡張機能を追加することで変わります。

Cisco IOS Release 12.4(15)T の RRI の拡張機能

Cisco IOS Release 12.4(15)T の RRI 機能に次の拡張機能が追加されました。

RRI ディスタンス メトリック

一般に、スタティック ルートはアドミニストレーティブ ディスタンスが 1 で作成されます。これはルーティング テーブルで常にスタティック ルートに優先権があることを意味します。ただし場合によっては、ダイナミックに学習されたルートの方をスタティック ルートより優先させる必要があります（ダイナミックに学習されたルートがない場合はスタティック ルートを使用）。クリプト マップまたは IPsec プロファイルのいずれかで **set reverse-route distance** コマンドを実行すると、VPN で作成されたルートに別のディスタンス メトリックを指定することで、ダイナミック ルートまたは優先度の高いルートを使用できない場合だけそのルートが有効になるようにできます。

ゲートウェイ オプション

この RRI ゲートウェイ オプションを指定できるのはクリプト マップだけです。

このオプションを使用すると、リモート トンネル エンドポイントに対して一意のネクストホップまたはゲートウェイを設定できます。このオプションは、各 VPN トンネルでルートが 2 つ作成されるという点で、Cisco IOS Release 12.3(14)T よりも前の **reverse-route remote-peer** {*ip-address*} コマンドと動作が同じです。1 番目のルートは、リモート トンネル エンドポイントを経由して、宛先が保護されたサブネットに向かいます。2 番目のルートは、このトンネル エンドポイントに到達するためのネクストホップを指定します。この RRI ゲートウェイ オプションを使用すると、ルートの再帰検索をサポートするプラットフォームで、特定のデフォルト パスを VPN 接続の特定のグループに指定できます。

（注） 12.4(15)T 以降のリリースでは、キーワード オプション **gateway** は **reverse-route remote-peer** コマンド（*IP アドレス*の指定なし）に変わっています。Cisco Express Forwarding（CEF; シスコ エクスプレス フォワーディング）に変更があったため、ネクストホップ IP アドレスを追加せずにインターフェイスをネクストホップとしては使用できません。

IPsec プロファイルにおける RRI のサポート

RRI を使用できるのは、以前はクリプト マップ コンフィギュレーションだけでした。Cisco IOS Release 12.4(15)T は、主に仮想トンネル インターフェイスに使用されている、IPsec プロファイルの関連 RRI オプションをサポートしています。トンネル インターフェイスでは、一般的な RRI 機能を使ったディスタンス メトリックとタグ オプションだけが有効です。

（注） Easy VPN クライアントのダイナミック バーチャル インターフェイスでは、RRI を特にイネーブルにする必要はありません。ルート サポートはデフォルトでイネーブルになっています。必要に応じて、タグまたはディスタンス メトリックの値を指定する必要があります。

タグ オプション設定の変更点

タグ オプションは 12.3(14)T でクリプト マップ向けに導入されました。現在このオプションは、IPsec プロファイルでサポート（**set reverse-route tag** コマンド構文）されています。また、**set reverse-route tag** コマンドは、最適化のためにクリプト マップでも使用できます。ただし、従来の **reverse-route tag** コマンドはサポートされていません。

show crypto route コマンド

show crypto route コマンドは、RRI または Easy VPN virtual tunnel interface（VTI; 仮想トンネル インターフェイス）を介して IPsec で作成されたルートを表示します。ルートは 1 つの表で表示されます。**show crypto route** コマンドのサンプル出力については、**「show crypto route コマンドの出力：例」**の項を参照してください。

RRI の設定方法

ここでは、Cisco IOS ソフトウェアのリリース 12.4(15)T 以前およびリリース 12.4(15)T の RRI の設定方法を説明します。

12.4(15)T 以前の Cisco IOS リリースのクリプト マップにおける RRI の設定

ここでは、次の作業について説明します。

スタティック クリプト マップにおける RRI の設定

リリース 12.4(15)T よりも前の Cisco IOS ソフトウェアのスタティック クリプト マップで RRI を設定するには、以下の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto map** {*map-name*} {*seq-name*} **ipsec-isakmp**
4. **reverse-route** [**static** | **tag** *tag-id* [**static**] | **remote-peer** [**static**] | **remote-peer** *ip-address* [**static**]]

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 map** {*map-name*} {*seq-name*} **ipsec-isakmp** **例：** `Router (config)# crypto map mymap 1 ipsec-isakmp`	クリプト マップ エントリを作成または変更し、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。
ステップ 4	**reverse-route** [**static** | **tag** *tag-id* [**static**] | **remote-peer** [**static**] | **remote-peer** *ip-address* [**static**]] **例：** `Router (config-crypto-map)# reverse-route remote peer 10.1.1.1`	クリプト マップ エントリのソース プロキシ情報を作成します。

ダイナミック マップ テンプレートでの RRI の設定

リリース 12.4(15)T よりも前の Cisco IOS ソフトウェアのダイナミック マップ テンプレートで RRI を設定するには、以下の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto dynamic-map** *dynamic-map-name dynamic-seq-name*
4. **reverse-route** [**static** | **tag** *tag-id* [**static**] | **remote-peer** [**static**] | **remote-peer** *ip-address* [**static**]]

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 dynamic-map** *dynamic-map-name dynamic-seq-name* **例：** `Router (config)# crypto dynamic-map mymap 1`	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 コマンド モードを開始します。
ステップ 4	**reverse-route** [**static** | **tag** *tag-id* [**static**] | **remote-peer** [**static**] | **remote-peer** *ip-address* [**static**]] **例：** `Router (config-crypto-map)# reverse-route remote peer 10.1.1.1`	クリプト マップ エントリのソース プロキシ情報を作成します。

Cisco IOS Release 12.4(15)T に追加された拡張機能による RRI の設定

ここでは、Cisco IOS Release 12.4(15)T に追加された RRI 拡張機能を設定する方法について説明します。

- 「スタティック クリプト マップにおける RRI 拡張機能の設定」（P.6）
- 「ダイナミック マップ テンプレートにおける RRI および拡張機能の設定」（P.7）
- 「IPsec プロファイルにおける RRI ディスタンス メトリックの設定」（P.8）
- 「RRI または Easy VPN VTI を介して IPsec で作成されたルートの確認」（P.9）

スタティック クリプト マップにおける RRI 拡張機能の設定

スタティック クリプト マップで RRI 拡張機能を設定するには（Cisco IOS Release 12.4(15)T 以降のリリース）、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto map** *map-name seq-name* **ipsec-isakmp**
4. **reverse-route** [**static** | **remote-peer** *ip-address* [**gateway**] [**static**]]
5. **set reverse-route** [**distance** *number* | **tag** *tag-id*]

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 map** *map-name seq-name* **ipsec-isakmp** **例：** `Router (config)# crypto map mymap 1 ipsec-isakmp`	クリプト マップ エントリを作成または変更し、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。
ステップ 4	**reverse-route** [**static** | **remote-peer** *ip-address* [**gateway**] [**static**]] **例：** `Router (config-crypto-map)# reverse-route`	クリプト マップ エントリのソース プロキシ情報を作成します。 **（注）** キーワード **gateway** を追加すると、デュアル ルート機能をイネーブルにしてデフォルト ゲートウェイをサポートできます。
ステップ 5	**set reverse-route** [**distance** *number* | **tag** *tag-id*] **例：** `Router (config-crypto-map)# set reverse-route distance 20`	使用するディスタンス メトリック、またはルートに関連づけるタグ値を指定します。

ダイナミック マップ テンプレートにおける RRI および拡張機能の設定

ダイナミック マップ テンプレートで RRI 拡張機能を設定するには（Cisco IOS Release 12.4(15)T 以降のリリースの場合）、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto dynamic-map** *dynamic-map-name dynamic-seq-name*
4. **reverse-route** [**static** | **remote-peer** *ip-address* [**gateway**] [**static**]]
5. **set reverse-route** [**distance** *number* | **tag** *tag-id*]

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 dynamic-map** *dynamic-map-name dynamic-seq-name* **例：** `Router (config)# crypto dynamic-map mymap 1`	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 コマンド モードを開始します。
ステップ 4	**reverse-route** [**static** | **remote-peer** *ip-address* [**gateway**] [**static**]] **例：** `Router (config-crypto-map)# reverse-route remote peer 10.1.1.1 gateway`	クリプト マップ エントリのソース プロキシ情報を作成します。
ステップ 5	**set reverse-route** [**distance** *number* | **tag** *tag-id*] **例：** `Router (config-crypto-map)# set reverse-route distance 20`	使用するディスタンス メトリック、またはルートに関連づけるタグ値を指定します。

IPsec プロファイルにおける RRI ディスタンス メトリックの設定

IPsec プロファイルで Cisco IOS Release 12.4(15)T 以降のリリースの RRI ディスタンス メトリックを設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto ipsec profile** *name*
4. **set reverse-route** [**distance** *number* | **tag** *tag-id*]

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 profile** *name* **例：** `Router (config)# crypto ipsec profile myprofile`	IPsec プロファイルを作成または変更し、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。
ステップ 4	**set reverse-route** [**distance** *number* | **tag** *tag-id*] **例：** `Router (config-crypto-profile)# set reverse-route distance 20`	各スタティック ルートのディスタンス メトリックを定義するか、RRI によって作成されたルートにタグを設定します。 • **distance**：各スタティック ルートのディスタンス メトリックを定義します。 • **tag**：ルート マップを使用した分散を制御するための「照合」値として使用可能なタグ値を設定します。

RRI または Easy VPN VTI を介して IPsec で作成されたルートの確認

RRI または Easy VPN VTI を介して IPsec で作成されたルートを表示するには、次の手順を実行します。

手順の概要

1. **enable**
2. **show crypto route**

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	**show crypto route** **例：** `Router# show crypto route`	RRI または Easy VPN VTI を介して IPsec で作成されたルートを表示します。

トラブルシューティングのヒント

RRI の動作と IPsec SA の作成および削除との関係を確認するには、**debug crypto ipsec** コマンド（『*Cisco IOS Debug Command Reference*』を参照）を使用します。

RRI の設定例

ここでは、次の各手順について説明します。

Cisco IOS Release 12.3(14)T よりも前の RRI の設定：例

次に、Cisco IOS Release 12.3(14)T よりも前の RRI の設定および出力の例を示します。

Crypto ACL が存在する場合の RRI の設定：例

次に、すべてのリモート VPN ゲートウェイを 192.168.0.3 でルータに接続している例を示します。RRI がスタティック クリプト マップに追加され、crypto access control list（ACL; アクセス コントロール リスト）で定義されている発信元ネットワークおよび発信元ネットマスクを基にルートを作成します。

```
crypto map mymap 1 ipsec-isakmp
 set peer 10.1.1.1
 reverse-route
 set transform-set esp-3des-sha
 match address 102

Interface FastEthernet 0/0
 ip address 192.168.0.2 255.255.255.0
 standby name group1
 standby ip 192.168.0.3
 crypto map mymap redundancy group1

access-list 102 permit ip 192.168.1.0 0.0.0.255 10.0.0.0 0.0.255.255
```

Cisco IOS Release 12.3(14)T 以降のリリースの場合、クリプト ACL の内容を基にスタティック マップでルート作成と同じ動作を維持するには、キーワード **static** が必要です（**reverse-route static**）。

（注） この場合の **reverse-route** コマンドは、次のスタティック ルート Command-Line Interface（CLI; コマンドライン インターフェイス）コマンド（**ip route**）を使った場合と似たルートを作成します。

リモート トンネル エンドポイント

```
ip route 10.1.1.1 255.255.255.255 192.168.1.1
```

VPNSM

ip route 10.1.1.1 255.255.255.255 vlan0.1

2 つのルート（リモート エンドポイント用とルート再帰用）を作成する場合の RRI の設定：例

次に、クリプト マップが設定されているインターフェイスを介して、リモート エンドポイント用とリモート エンドポイントへのルート再帰用の 2 つのルートを作成する場合の例を示します。

```
reverse-route remote-peer
```

Cisco IOS Release 12.3(14)T に追加された拡張機能による RRI の設定：例

次に、Cisco IOS Release 12.3(14)T に追加された RRI 拡張機能の設定および出力の例を示します。

- 「Crypto ACL が存在する場合の RRI の設定：例」（P.11）
- 「ルート タグを使った RRI の設定：例」（P.11）
- 「ユーザが定義したネクストホップを介したリモート プロキシへのルートを 1 つ作成する RRI の設定：例」（P.11）

Crypto ACL が存在する場合の RRI の設定：例

次に、ACL が既に存在する状況で RRI を設定する例を示します。

```
crypto map mymap 1 ipsec-isakmp
   set peer 172.17.11.1
   reverse-route static
   set transform-set esp-3des-sha
   match address 101

access-list 101 permit ip 192.168.1.0 0.0.0.255 172.17.11.0 0.0.0.255
```

ルート タグを使った RRI の設定：例

次に、RRI で作成されたルートにタグ番号付きでタグを設定した後、タグを設定したそのルートをルーティング プロセスで使用してルート マップを介して再配布する方法の例を示します。

```
crypto dynamic-map ospf-clients 1
 reverse-route tag 5

router ospf 109
 redistribute rip route-map rip-to-ospf

route-map rip-to-ospf permit
 match tag 5
 set metric 5
 set metric-type type1

Router# show ip eigrp topology

P 10.81.7.48/29, 1 successors, FD is 2588160, tag is 5
     via 192.168.82.25 (2588160/2585600), FastEthernet0/1
```

ユーザが定義したネクストホップを介したリモート プロキシへのルートを 1 つ作成する RRI の設定：例

（注） このオプションを適用できるのはクリプト マップだけです。

上記の例では、ユーザが定義したネクストホップを介したリモート プロキシへのルートを 1 つ作成しました。このネクストホップでは、デフォルト ルートに再帰する場合を除き、再帰ルート検索は必要ありません。

```
reverse-route remote-peer 10.4.4.4
```

Cisco IOS Release 12.3(14)T よりも前のリリースでは、上記の例は次のような出力になります。

```
10.0.0.0/24 via 10.1.1.1 (in the VRF table if VRFs are configured)
10.1.1.1/32 via 10.4.4.4 (in the global route table)
```

また、RRI 拡張機能を使うと次のような結果になります。

```
10.0.0.0/24 via 10.4.4.4 (in the VRF table if VRFs are configured, otherwise in the global
table)
```

Cisco IOS Release 12.4(15)T に追加された拡張機能による RRI の設定：例

次に、Cisco IOS Release 12.4(15)T に追加された RRI 拡張機能の設定および出力の例を示します。

クリプト マップにおける RRI ディスタンス メトリックの設定：例

次に、RRI ディスタンス メトリックがクリプト マップに設定されているサーバおよびクライアントの設定を示します。

サーバ

```
crypto dynamic-map mymap
 set security-association lifetime seconds 300
 set transform-set 3dessha
 set isakmp-profile profile1
 set reverse-route distance 20
 reverse-route
```

クライアント

```
crypto ipsec client ezvpn ez
 connect auto
 group cisco key cisco
 mode client
 peer 10.0.0.119
 username XXX password XXX
 xauth userid mode local
```

ルート タグを使った RRI の設定：例

次に、RRI で作成されたルートにタグ番号付きでタグを設定した後、タグを設定したそのルートをルーティング プロセスで使用してルート マップを介して再配布する方法の例を示します。

```
crypto dynamic-map ospf-clients 1
 set reverse-route tag 5

router ospf 109
 redistribute rip route-map rip-to-ospf

route-map rip-to-ospf permit
 match tag 5
 set metric 5
 set metric-type type1

Router# show ip eigrp topology

P 10.81.7.48/29, 1 successors, FD is 2588160, tag is 5
  via 192.168.82.25 (2588160/2585600), FastEthernet0/1
```

debug コマンドおよび show コマンドによる、クリプト マップにおける RRI ディスタンス メトリックの設定の出力：例

次に、**debug** コマンドおよび **show** コマンドを使って出力した、サーバのクリプト マップにおける RRI ディスタンス メトリックの設定を示します。

```
Router# debug crypto ipsec

00:23:37: IPSEC(validate_proposal_request): proposal part #1,
  (key eng. msg.) INBOUND local= 10.0.0.119, remote= 10.0.0.14,
    local_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4),
    remote_proxy= 192.168.6.1/255.255.255.255/0/0 (type=1),
    protocol= ESP, transform= esp-3des esp-sha-hmac  (Tunnel),
    lifedur= 0s and 0kb,
    spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x0
00:23:37: IPSEC(key_engine): got a queue event with 1 KMI message(s)
00:23:37: IPSEC(rte_mgr): VPN Route Event create routes for peer or rekeying for
 10.0.0.128
00:23:37: IPSEC(rte_mgr): VPN Route Refcount 1 FastEthernet0/0
00:23:37: IPSEC(rte_mgr): VPN Route Added 192.168.6.1 255.255.255.255 via 10.0.0.14 in IP
DEFAULT TABLE with tag 0 distance 20
00:23:37: IPSEC(policy_db_add_ident): src 0.0.0.0, dest 192.168.6.1, dest_port 0

Router# show ip route

Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is 10.0.0.14 to network 0.0.0.0

C    192.200.200.0/24 is directly connected, Loopback0
     10.20.20.20/24 is subnetted, 1 subnets
C       10.30.30.30 is directly connected, Loopback4
C    192.168.5.0/24 is directly connected, Loopback3
     10.20.20.20/24 is subnetted, 2 subnets
S       10.3.1.0 [1/0] via 10.0.0.113
```

```
C       10.20.20.20 is directly connected, FastEthernet0/0
     192.168.6.0/32 is subnetted, 1 subnets
S       192.168.6.1 [20/0] via 10.0.0.14
C    192.168.3.0/24 is directly connected, Loopback2
     10.15.0.0/24 is subnetted, 1 subnets
C       10.15.0.0 is directly connected, Loopback6
S*   0.0.0.0/0 [1/0] via 10.0.0.14
```

VTI の RRI ディスタンス メトリックの設定：例

次に、VTI に RRI ディスタンス メトリックが設定されているサーバおよびクライアントの設定を示します。

サーバの設定

```
crypto isakmp profile profile1
 keyring mykeyring
 match identity group cisco
 client authentication list authenlist
 isakmp authorization list autholist
 client configuration address respond
 virtual-template 1
crypto ipsec profile vi
 set transform-set 3dessha
 set reverse-route distance 20
 set isakmp-profile profile1
!
interface Virtual-Template1 type tunnel
 ip unnumbered
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile vi
```

クライアントの設定

```
crypto ipsec client ezvpn ez
 connect auto
 group cisco key cisco
 mode client
 peer 10.0.0.119
 username XXX password XXX
 virtual-interface 1
```

debug コマンドおよび show コマンドによる、VTI が設定されている RRI メトリックの設定の出力：例

次に、**debug** コマンドおよび **show** コマンドを使って出力した、サーバの VTI の RRI メトリックの設定を示します。

```
Router# debug crypto ipsec

00:47:56: IPSEC(key_engine): got a queue event with 1 KMI message(s)
00:47:56: Crypto mapdb : proxy_match
        src addr     : 0.0.0.0
        dst addr     : 192.168.6.1
        protocol     : 0
        src port     : 0
        dst port     : 0
00:47:56: IPSEC(crypto_ipsec_sa_find_ident_head): reconnecting with the same pro
xies and peer 10.0.0.14
00:47:56: IPSEC(rte_mgr): VPN Route Event create routes for peer or rekeying for
 10.0.0.14
```

```
00:47:56: IPSEC(rte_mgr): VPN Route Refcount 1 Virtual-Access2
00:47:56: IPSEC(rte_mgr): VPN Route Added 192.168.6.1 255.255.255.255 via Virtua
l-Access2 in IP DEFAULT TABLE with tag 0 distance 20
00:47:56: IPSEC(policy_db_add_ident): src 0.0.0.0, dest 192.168.6.1, dest_port 0

00:47:56: IPSEC(create_sa): sa created,
  (sa) sa_dest= 10.0.0.110, sa_proto= 50,
    sa_spi= 0x19E1175C(434181980),
    sa_trans= esp-3des esp-sha-hmac , sa_conn_id= 87
00:47:56: IPSEC(create_sa): sa created,
  (sa) sa_dest= 10.0.0.14, sa_proto= 50,
    sa_spi= 0xADC90C5(182227141),
    sa_trans= esp-3des esp-sha-hmac , sa_conn_id= 88
00:47:56: %LINEPROTO-5-UPDOWN: Line protocol on Interface Virtual-Access2, chang
ed state to up
00:47:56: IPSEC(key_engine): got a queue event with 1 KMI message(s)
00:47:56: IPSEC(key_engine_enable_outbound): rec'd enable notify from ISAKMP
00:47:56: IPSEC(key_engine_enable_outbound): enable SA with spi 182227141/50
00:47:56: IPSEC(update_current_outbound_sa): updated peer 10.0.0.14 current outb
ound sa to SPI ADC90C5

Router# show ip route

Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is 10.0.0.14 to network 0.0.0.0

C    192.200.200.0/24 is directly connected, Loopback0
     10.20.20.20/24 is subnetted, 1 subnets
C       10.30.30.30 is directly connected, Loopback4
C    192.168.5.0/24 is directly connected, Loopback3
     10.20.20.20/24 is subnetted, 2 subnets
S       10.3.1.0 [1/0] via 10.0.0.113
C       10.20.20.20 is directly connected, FastEthernet0/0
     192.168.6.0/32 is subnetted, 1 subnets
S       192.168.6.1 [20/0] via 0.0.0.0, Virtual-Access2
C    192.168.3.0/24 is directly connected, Loopback2
     10.15.0.0/24 is subnetted, 1 subnets
C       10.15.0.0 is directly connected, Loopback6
S*   0.0.0.0/0 [1/0] via 10.0.0.14
```

show crypto route コマンドの出力：例

次に、RRI または Easy VPN VTI を介して IPsec で作成されたルート（1 テーブル）の出力例を示します。

```
Router# show crypto route

VPN Routing Table: Shows RRI and VTI created routes
Codes: RRI - Reverse-Route, VTI- Virtual Tunnel Interface
        S - Static Map ACLs

Routes created in table GLOBAL DEFAULT
192.168.6.2/255.255.255.255 [0/0] via 10.0.0.133
                                  on Virtual-Access3 RRI
10.1.1.0/255.255.255.0 [10/0] via Virtual-Access2 VTI
```

```
192.168.6.1/255.255.255.255 [0/0] via Virtual-Access2 VTI
```

その他の参考資料

ここでは、RRI 拡張機能の関連資料について説明します。

関連資料

内容	参照先
Cisco IOS セキュリティ コマンド	『*Cisco IOS Security Command Reference*』
その他の Cisco IOS コマンド	『*Cisco IOS Master Command List*』

規格

規格	タイトル
なし	—

MIB

MIB	MIB リンク
なし	選択したプラットフォーム、Cisco IOS ソフトウェア リリース、および機能セットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
なし	—

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/techsupport

コマンド リファレンス

次のコマンドは、このモジュールに記載されている機能または機能群において、新たに導入または変更されたものです。

- **reverse-route**
- **set reverse-route**
- **show crypto route**

これらのコマンドの詳細については、『Cisco IOS Security Command Reference』（http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_book.html）を参照してください。

Cisco IOS の全コマンドを参照する場合は、Command Lookup Tool（http://tools.cisco.com/Support/CLILookup）にアクセスするか、または『*Master Command List*』を参照してください。

RPI の機能情報

表 1 に、この機能のリリース履歴を示します。

ご使用の Cisco IOS ソフトウェア リリースによっては、コマンドの中に一部使用できないものがあります。特定のコマンドに関するリリース情報については、コマンド リファレンス マニュアル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ソフトウェア イメージのサポート情報を検索できます。Cisco Feature Navigator を使用すると、Cisco IOS および Catalyst OS 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://tools.cisco.com/ITDIT/CFN/jsp/index.jsp からアクセスできます。Cisco.com のアカウントは必要ありません。

（注） 表 1 には、一連の Cisco IOS 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 Cisco IOS 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 Cisco IOS ソフトウェア リリースでもサポートされます。

表 1　RRI の機能情報

機能名	リリース	機能情報
逆ルート注入	12.1(9)E 12.2(8)T 12.2(8)YE	Reverse Route Injection（RRI; 逆ルート注入）とは、リモート トンネル エンドポイントによって保護されているネットワークおよびホストのルーティング プロセスに、スタティック ルートを自動的に組み込む機能です。保護されているホストおよびネットワークをリモート プロキシ ID といいます。 各ルートはリモート プロキシ ネットワークおよびマスクを基に作成され、このネットワークへのネクストホップがリモート トンネル エンドポイントになります。ネクストホップとして VPN のリモート ルータを使い、暗号化プロセスによってトラフィックを強制的に暗号化します。 この機能に関する詳細については、次の各項を参照してください。 • 「逆ルート注入」（P.2） この機能により、次のコマンドが導入または変更されました。 **reverse-route**
逆ルート リモート ピア オプション	12.2(13)T 12.2(14)S	リモート VPN デバイスへの明示的なネクストホップとしてインターフェイスまたはアドレスを指定できる拡張機能が RRI に追加されました。この機能を使用すると、デフォルトのルート指定を変更して、暗号化された発信パケットを正しく転送できます。 リモート ピア オプションの詳細については、次の各項を参照してください。 • 「Cisco IOS Release 12.4(15)T の RRI の拡張機能」（P.3）

表 1　RRI の機能情報 （続き）

機能名	リリース	機能情報
RRI の拡張機能	12.3(14)T 12.2(33)SRA 12.2(33)SXH	以下の拡張機能が RRI 機能に追加されました。 • スタティック クリプト マップのデフォルト動作とダイナミック クリプト マップのデフォルト動作が同じ。ただし、**reverse-route** コマンドおよびキーワード **static** を使用する場合を除きます。 • RRI を使って作成されたルートすべてにルート タグ値を追加。 • 複数のルータ インターフェイスに適用されている同じクリプト マップで RRI が設定可能。 • **reverse-route remote-peer** {*ip-address*} コマンド、キーワード、引数で設定された RRI によって作成されるルートは 2 つではなく 1 つ。 RRI の機能拡張の詳細については、次の各項を参照してください。 • 「逆ルート注入」（P.2） • 「12.4(15)T 以前の Cisco IOS リリースのクリプト マップにおける RRI の設定」（P.4） • 「Cisco IOS Release 12.4(15)T に追加された拡張機能による RRI の設定」（P.6） • 「Crypto ACL が存在する場合の RRI の設定：例」（P.10） • 「ルート タグを使った RRI の設定：例」（P.11） • 「ユーザが定義したネクストホップを介したリモート プロキシへのルートを 1 つ作成する RRI の設定：例」（P.11） これらの機能拡張により、**reverse-route** コマンドが変更されました。
ゲートウェイ オプション	12.4(15)T	このオプションを使用すると、リモート トンネル エンドポイントに対して一意のネクストホップまたはゲートウェイを設定できます。 ゲートウェイ オプションの詳細については、次の各項を参照してください。 • 「ゲートウェイ オプション」（P.3）

表 1　RRI の機能情報 （続き）

機能名	リリース	機能情報
RRI ディスタンス メトリック	12.4(15)T	この機能拡張を使用すると、スタティック ルートそれぞれにメトリック ディスタンスを定義できます。 RRI ディスタンス メトリックの機能拡張の詳細については、次の各項を参照してください。 • 「RRI ディスタンス メトリック」（P.3） • 「IPsec プロファイルにおける RRI ディスタンス メトリックの設定」（P.8） • 「クリプト マップにおける RRI ディスタンス メトリックの設定：例」（P.12） • 「debug コマンドおよび show コマンドによる、VTI が設定されている RRI メトリックの設定の出力：例」（P.14） この機能により、次のコマンドが導入または変更されました。 **reverse-route** および **set reverse-route**
show crypto route コマンド	12.4(15)T	このコマンドは、RRI または Easy VPN VTI を介して IPsec で作成されたルートを表示します。
IPsec プロファイルにおける RRI のサポート	12.4(15)T	この機能では、主に VTI で使用されている IPsec プロファイルの、対応する RRI オプションに対してサポートが提供されます。 IPsec プロファイルにおける RRI のサポートの機能の詳細については、次の各項を参照してください。 • 「IPsec プロファイルにおける RRI のサポート」（P.4）
タグ オプション設定の変更点	12.4(15)T	現在タグ オプション、IPsec プロファイル（**set reverse-route tag** コマンド）でサポートされています。 この拡張機能に関する詳細については、次の各項を参照してください。 • 「タグ オプション設定の変更点」（P.4）