逆ルート注入

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。保護されているこれらのホストおよびネットワークは、リモート プロキシ アイデンティティと呼ばれます。

各ルートは、リモート プロキシ ネットワークとマスクを基にして作成され、リモート トンネル エンドポイントがこのネットワークへのネクスト ホップとなります。ネクスト ホップとしてバーチャル プライベート ネットワーク（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。

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

- 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。スタティックマップに常に表示されるルートのデフォルト動作は、**static** キーワードが **reverse-route** コマンドに追加されない限り適用されません。

- RIB のプレフィックスに、手動で設定されたタグ付きのスタティックルートと、RRI を介して挿入されたタグのないルートがあるとします。このようなシナリオでは、ルート選択に一貫性がなくなり、手動設定ルートまたはRRIルートのいずれかが選択される可能性があります。

  そのような一貫性のなさを回避するには、次の作業のいずれかを行う必要があります。

  - ルータのすべてのピア VPN ネットワークへのスタティックルートを手動で設定する場合は、暗号マップからリバースルート設定を削除することでRRIを無効にします。
  - RRI を介して挿入されたルートの暗号マップに同一のタグを設定します。

逆ルート注入に関する情報

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。保護されているこれらのホストおよびネットワークは、リモート プロキシ アイデンティティと呼ばれます。

各ルートは、リモート プロキシ ネットワークとマスクを基にして作成され、リモート トンネル エンドポイントがこのネットワークへのネクスト ホップとなります。リモート VPN ルータをネクストホップとして使用することによって、トラフィックは強制的に暗号プロセスを通して暗号化されます。

VPN ルータでスタティック ルートが作成されたあと、この情報がアップストリーム デバイスに伝播されます。これにより、アップストリーム デバイスでは、IPsec 状態フローを維持するためのリターン トラフィックの送信先として適切なVPNルータを特定できるようになります。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 Routing and Forwarding（VRF）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。リモート プロキシへのネクスト ホップは、リモートVPNルータ経由となります。リモートVPNルータのアドレスは、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および適用されます。ルートは、SA が削除されたあとに削除されます。スタティック クリプト マップの IPsec 送信元プロキシで作成されたルートは、スタティック マップのデフォルト動作であり、クリプト ACL（次の項目を参照）に基づいたルートの作成よりも優先されます。

- 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。

RRI の設定方法

スタティック クリプト マップを使用した RRI の設定

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 モードを有効にします。 • パスワードを入力します（要求された場合）。
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

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 モードを有効にします。 • パスワードを入力します（要求された場合）。
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。

RRI の設定例

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 アクセス コントロール リスト（ACL）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 0/0/1
 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
```

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
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『*Cisco IOS Master Commands List, All Releases*』
セキュリティ コマンド	• 『*Cisco IOS Security Command Reference Commands A to C*』 • 『*Cisco IOS Security Command Reference Commands D to L*』 • 『*Cisco IOS Security Command Reference Commands M to R*』 • 『*Cisco IOS Security Command Reference Commands S to Z*』
推奨される暗号化アルゴリズム	『Next Generation Encryption』

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。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。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

RRI の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。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。

プラットフォームのサポートおよびシスコ 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 にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

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	Cisco IOS XE Release 2.1	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。保護されているこれらのホストおよびネットワークは、リモート プロキシ アイデンティティと呼ばれます。 各ルートは、リモート プロキシ ネットワークとマスクを基にして作成され、リモート トンネル エンドポイントがこのネットワークへのネクスト ホップとなります。ネクスト ホップとしてバーチャル プライベート ネットワーク（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。 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**。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。