Cisco IOS XR ソフトウェアでのトンネル インターフェイスの設定

ここでは、Cisco IOS XR ソフトウェアをサポートするルータで Tunnel-IPSec インターフェイスを設定する方法について説明します。トンネル インターフェイスは、別のトランスポート プロトコル内に任意のパケットのカプセル化を提供する仮想インターフェイスです。保護されていない公開ルートでも、Tunnel-IPSec インターフェイスによってセキュアな通信が可能になります。

仮想インターフェイスは、ルータ内部の論理パケット スイッチング エンティティです。仮想インターフェイスは、グローバル スコープを持ちますが、関連付けられた位置は持ちません。Cisco IOS XR ソフトウェアでは、物理インターフェイスを識別するために *rack/slot/module/port* 表記を使用していますが、インターフェイス名で仮想インターフェイスを識別した後は、グローバルに一意な数字による ID を使用します。この数字による ID は、たとえば、Loopback 0、Loopback 1、Null99999 です。Loopback 0 と Null 0 を同時に使用できるように、各仮想インターフェイス タイプの ID は一意です。

仮想インターフェイスのコントロール プレーンは、アクティブ RP 上に存在します。設定とコントロール プレーンは、スタンバイ RP 上にミラーリングされ、スイッチオーバーが発生した場合には、仮想インターフェイスがそれまでのスタンバイ RP に移り、このスタンバイ RP が新たにアクティブ RP となります。

（注） 親インターフェイスに応じて、サブインターフェイスは物理インターフェイスまたは仮想インターフェイスになります。

仮想トンネルは、任意の RP または DRP で*設定*されますが、作成および操作は RP からだけ実行されます。

（注） トンネルには、モジュラ サービス カードとの 1 対 1 の関連付けはありません。

Cisco IOS XR ソフトウェアのトンネル インターフェイス設定機能の履歴

リリース	変更点
リリース 2.0	Cisco CRS-1 ルータにこの機能が追加されました。
リリース 3.0	変更ありません。
リリース 3.2	変更ありません。
リリース 3.3.0	変更ありません。
リリース 3.4.0	変更ありません。
リリース 3.5.0	変更ありません。
リリース 3.6.0	変更ありません。

リリース 3.7.0	変更ありません。
リリース 3.8.0	変更ありません。

この章の構成

トンネル インターフェイスを設定するための前提事項

この設定作業を行うには、Cisco IOS XR ソフトウェアのシステム管理者が、対応するコマンド タスク ID を含むタスク グループに関連付けられたユーザ グループにユーザを割り当てる必要があります。すべてのコマンド タスク ID は、各コマンド リファレンスおよび『*Cisco IOS XR Task ID Reference Guide*』に記載されています。

タスク グループの割り当てについてサポートが必要な場合は、システム管理者に連絡してください。ユーザ グループおよびタスク ID の詳細については、『*Cisco IOS XR Software System Security Configuration Guide*』の「*Configuring AAA Services on Cisco IOS XR Software* 」モジュールを参照してください。

トンネル インターフェイスの設定に関する情報

トンネル インターフェイスを設定するには、次の概念を理解しておく必要があります。

トンネル インターフェイスの概要

トンネリングによって、トランスポート プロトコル内の任意のパケットをカプセル化できるようになります。この機能は、設定用の単純なインターフェイスを用意するために、仮想インターフェイスとして実装されます。トンネル インターフェイスは特定の「パッセンジャ」プロトコルや「トランスポート」プロトコルに関連付けられません。トンネル インターフェイスは、任意の標準のポイントツーポ

イント カプセル化スキームを実装するために必要なサービスを提供できるように設計されたアーキテクチャです。サポートされるトンネルはポイントツーポイント リンクなので、リンクごとに個別のトンネルを設定する必要があります。

トンネル インターフェイスを設定するには、必須の手順が 3 つあります。

1. トンネル インターフェイスを設定します。**interface tunnel-ipsec** *ID を指定します。*
2. トンネルの発信元を設定します。**tunnel source** {*ip-address* | *interface-id*} を指定します。
3. トンネルの宛先を設定します。**tunnel destination** {*ip-address* | *tunnel-id*} を指定します。

仮想インターフェイスの命名規則

仮想インターフェイス名では、インターフェイスのラック、スロット、モジュール、およびポートを識別するために、*rack/slot/module/port* という物理インターフェイスの表記方法を使用しません。仮想インターフェイスは、物理的なインターフェイスやサブインターフェイスには関連付けられないためです。

仮想インターフェイスでは、仮想インターフェイス タイプごとに、グローバルに一意な数字による ID を使用します。

仮想インターフェイスの表記例：

```
Interface                  IP-Address      Status Protocol
Loopback0                  10.9.0.0         Up           Up
Loopback10                 10.7.0.0         Up           Up
Tunnel-TE5000              172.18.189.38    Down         Down
Null10                     10.8.0.0          Up           Up
```

Tunnel-IPSec の概要

IP Security（IPSec; IP セキュリティ）は、インターネット上のプライベート通信のセキュリティを確保するためのオープン スタンダードのフレームワークです。IPSec は、パブリック ネットワークやセキュアではないネットワークでデータを送信する必要がある、仮想プライベート ネットワーク（VPN）やファイアウォールなどのアプリケーションをサポートするために使用できます。ルータ IPSec プロトコル スイートには、IP レイヤにプライバシ、完全性、および認証サービスを提供するために使用できる一連の標準が用意されています。また、IPSec プロトコル スイートには、ネットワーク レイヤ セキュリティの主要な管理要件をサポートする暗号化技術も含まれます。

IPSec を使用すると、Secure Shell（SSH; セキュア シェル）または Secure Socket Layer（SSL; セキュア ソケット レイヤ）を使用する必要はありません。使用すると、同じデータの暗号化と復号化が 2 回実行され、不要なオーバーヘッドが生じます。IPSec デーモンは、RP と DRP の両方で実行されます。IPSec はルータのオプションの機能です。IPSec は、セキュアなトランスポートが必要なアプリケーションが複数あるユーザに適しています。クライアント側では、Cisco VPN 3000 Client や他のサードパーティ製 IPSec クライアント ソフトウェアを使用して、IPSec VPN を構築できます。

（注） IPSec トンネルはコントロール プレーンに存在するため、トンネルを始動または終了する必要はありません。IPSec トンネルへの送信は、RP または DRP からローカルで発信されたトラフィックの場合だけであり、Tunnel-IPSec に適用するプロファイルの一部として設定されたアクセス制御リスト（ACL）によって検出されます。

Tunnel-IPSec の命名規則

プロファイルは、インターフェイスの tunnel-ipsec のインターフェイス設定サブモードから入力されます。例：

```
interface tunnel-ipsec 30
     profile <profile name>
```

クリプト プロファイル セット

クリプト プロファイル セットを設定し、トンネル インターフェイス（またはクリプト IPSec トランスポート）に適用する必要があります。クリプト IPSec トランスポートの使用の詳細については、「その他の参考資料」（P.483）に記載されているリンクを参照してください。2 つの IPSec ピア間で IPSec が正常に動作するには、両方のピアのクリプト プロファイル エントリに互換性のある設定ステートメントを含める必要があります。

2 つのピアがセキュリティ アソシエーションの確立を試行するには、相手側ピアのクリプト プロファイル エントリのいずれかと互換性のあるクリプト プロファイル エントリが、各ピアに 1 つ以上必要です。2 つのクリプト プロファイル エントリに互換性があると判断するには、少なくとも次の基準を満たす必要があります。

- 互換性のあるクリプト アクセス リストを含む必要があります。応答側のピアが動的クリプト プロファイルを使用している場合、ローカルのクリプト アクセス リストのエントリは、ピアのクリプト アクセス リストから「許可」される必要があります。
- 各ピアは、相手側ピアを識別する必要があります（ただし、応答側ピアが動的クリプト プロファイルを使用している場合を除きます）。
- 少なくとも 1 つのトランスフォーム セットが共通している必要があります。

（注） クリプト プロファイルは共有できません。つまり、複数のインターフェイスに同じプロファイルは設定できません。

トンネル インターフェイスの設定方法

ここでは、次の手順について説明します。

- 「Tunnel-IPSec インターフェイスの設定」（P.480）（必須）

Tunnel-IPSec インターフェイスの設定

ここでは、Tunnel-IPSec インターフェイスの設定方法について説明します。

前提条件

profile コマンドを使用するには、クリプト コマンドの適切なタスク ID を含むタスク グループに関連付けられたユーザ グループに属している必要があります。**tunnel destination** コマンドを使用するには、インターフェイス コマンドの適切なタスク ID を含むタスク グループに関連付けられたユーザ グループに属している必要があります。

ユーザ グループとタスク ID の詳細については、『*Cisco IOS XR System Security Configuration Guide*』の「*Configuring AAA Services on Cisco IOS XR Software*」モジュールを参照してください。

次のタスクは、Tunnel-IPSec インターフェイスを作成するために必要です。

- IPSec セキュリティ アソシエーションのグローバルな存続期間を設定する
- チェックポイント処理を設定する
- クリプト プロファイルを設定する

前提条件のチェックポイント処理とクリプト プロファイルの設定方法、および IPSec セキュリティ アソシエーションのグローバルな存続期間を設定する方法の詳細については、『*Cisco IOS XR System Security Configuration Guide*』の「*Implementing IPSec Network Security on Cisco IOS XR Software* 」モジュールを参照してください。

クリプト プロファイルの設定後は、IPSec トラフィックが通過する各トンネル インターフェイスにクリプト プロファイルを適用する必要があります。トンネル インターフェイスにクリプト プロファイル セットを適用すると、ルータは、クリプトで保護されるトラフィックの代理として、接続またはセキュリティ アソシエーションのネゴシエーション中に、クリプト プロファイル セットと照合してすべてのインターフェイスの トラフィックを評価し、指定したポリシーを使用するようになります。

手順の概要

1. **configure**
2. **interface tunnel-ipsec** *identifier*
3. **profile** *profile-name*
4. **tunnel source** {*ip-address* | *interface-id*}
5. **tunnel destination** {*ip-address* | *tunnel-id*}
6. **end**
   または
   commit
7. **show ip route**

詳細手順

	コマンドまたはアクション	目的
ステップ 1	**configure** **例：** `RP/0/RP0/CPU0:router# configure`	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 2	**interface tunnel-ipsec** *identifier* **例：** `RP/0/RP0/CPU0:router(config)# interface tunnel-ipsec 30`	クリプト プロファイルを適用する IPSec インターフェイスを特定し、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。
ステップ 3	**profile** *profile-name* **例：** `RP/0/RP0/CPU0:router(config-if)# profile user1`	IPSec プロセスのトンネルに適用するクリプト プロファイル名を割り当てます。 • 同じクリプト プロファイルは、異なる IPSec モードで共有できません。

	コマンドまたはアクション	目的
ステップ 4	**tunnel source** (*ip-address* | *interface-id*) **例：** `RP/0/RP0/CPU0:router(config-if)# tunnel source Ethernet0/1/1/2`	トンネルの発信元 IP アドレスまたはインターフェイス ID を指定します。 • このコマンドは、静的プロファイルと動的プロファイルのどちらにも必要です。
ステップ 5	**tunnel destination** {*ip-address* | *tunnel-id*} **例：** `RP/0/RP0/CPU0:router(config-if)# tunnel destination 192.168.164.19`	(任意) トンネルの宛先 IP アドレスを指定します。 • 動的プロファイルの場合、このコマンドは不要です。

ステップ 6	**end**
	または
	commit
	
	例：
	`RP/0/RP0/CPU0:router(config-if)# end`
	または
	`RP/0/RP0/CPU0:router(config-if)# commit`
		設定変更を保存します。
		• **end** コマンドを発行すると、変更のコミットを求めるプロンプトが表示されます。
		`Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]:`
		– **yes** と入力すると、実行コンフィギュレーション ファイルに設定変更が保存され、コンフィギュレーション セッションが終了し、ルータが EXEC モードに戻ります。
		– **no** と入力すると、設定変更をコミットせずにコンフィギュレーション セッションが終了し、ルータが EXEC モードに戻ります。
		– **cancel** と入力すると、コンフィギュレーション セッションの終了や設定変更のコミットは行われず、ルータでは現在のコンフィギュレーション セッションが継続されます。
		• 設定変更を実行コンフィギュレーション ファイルに保存し、コンフィギュレーション セッションを継続するには、**commit** コマンドを使用します。

ステップ 7	**show ip route** **例：** `RP/0/RP0/CPU0:router# show ip route`	トンネルのフォワーディング情報を表示します。 • **show ip route** コマンドで、アドバタイズの内容、および静的ルートと自動ルートが表示されます。

トンネル インターフェイスの設定例

ここでは、次の例について説明します。

「Tunnel-IPSec：例」（P.482）

Tunnel-IPSec：例

次に、プロファイルを作成し、IPSec トンネルに適用するプロセスの例を示します。必要な準備手順についても示します。まずトランスフォーム セットを定義し、プロファイルを作成してから、IPSec トンネルを設定します。

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# crypto ipsec transform-set tset1
RP/0/RP0/CPU0:router(config-transform-set tset1)# transform esp-sha-hmac
RP/0/RP0/CPU0:router(config-transform-set tset1)# end
Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]: yes

RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# crypto ipsec profile user1
RP/0/RP0/CPU0:router(config-user1)# match sampleac1 transform-set tset1
RP/0/RP0/CPU0:router(config-user1)# set pfs group5
RP/0/RP0/CPU0:router(config-user1)# set type dynamic
RP/0/RP0/CPU0:router(config-user1)# exit

RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface tunnel-ipsec 30
RP/0/RP0/CPU0:router(config-if)# profile user1
RP/0/RP0/CPU0:router(config-if)# tunnel source MgmtEth 0/RP0/CPU0/0
RP/0/RP0/CPU0:router(config-if)# tunnel destination 192.168.164.19
RP/0/RP0/CPU0:router(config-if)# end
Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]: yes
```

関連情報

次に、各トランスポートにクリプト プロファイルを適用する必要があります。トランスポートにクリプト プロファイル セットを適用すると、ルータは、クリプトで保護されるトラフィックの代理として、接続またはセキュリティ アソシエーションのネゴシエーション中に、クリプト プロファイル セットと照合してすべてのインターフェイスの トラフィックを評価し、指定したポリシーを使用するようになります。

各トランスポートにクリプト プロファイルを適用する方法の詳細については、『*Cisco IOS XR System Security Configuration* Guide』の「*Implementing IPSec Network Security on Cisco IOS XR* Software」モジュールを参照してください。

その他の参考資料

ここでは、トンネル インターフェイスの設定に関連する参考資料を示します。

関連資料

内容	参照先
Cisco IOS XR マスター コマンド リファレンス	『*Cisco IOS XR Master Commands List*』
Cisco IOS XR インターフェイス コンフィギュレーション コマンド	『*Cisco IOS XR Interface and Hardware Component Command Reference*』
IPSec とクリプト プロファイルに関する情報	『*Cisco IOS XR System Security Configuration Guide*』
MPLS-TE 用にトンネル インターフェイスを設定する方法など、MPLS トラフィック エンジニアリングに関する情報	『*Cisco IOS XR Multiprotocol Label Switching Configuration Guide*』

内容	参照先
ユーザ グループとタスク ID に関する情報	『*Cisco IOS XR Interface and Hardware Component Command Reference*』
リモートの Craft Works Interface（CWI）クライアント管理アプリケーションからの、Cisco CRS-1 ルータ上のインターフェイスとその他のコンポーネントの設定に関する情報	『*Cisco Craft Works Interface Configuration Guide*』

規格

規格	タイトル
この機能によりサポートされた新規規格または改訂規格はありません。またこの機能による既存規格のサポートに変更はありません。	-

MIB

MIB	MIB リンク
このモジュールに適用できる MIB はありません。	Cisco IOS XR ソフトウェアを使用して選択したプラットフォームの MIB を検索およびダウンロードするには、次の URL の Cisco MIB Locator を使用します。 http://cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

RFC

RFC	タイトル
この機能によりサポートされた新規 RFC または改訂 RFC はありません。またこの機能による既存 RFC のサポートに変更はありません。	-

シスコのテクニカル サポート

説明	リンク
シスコのテクニカル サポート Web サイトでは、製品、テクノロジー、ソリューション、テクニカル ヒント、ツールへのリンクなど、さまざまな技術的コンテンツを検索可能な形で提供しています。Cisco.com に登録されている場合は、次のページからログインしてさらに多くのコンテンツにアクセスできます。	http://www.cisco.com/techsupport