

GRE トンネルでの CET 暗号化の設定

内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[表記法](#)

[設定](#)

[ネットワーク図](#)

[設定](#)

[確認](#)

[トラブルシューティング](#)

[関連情報](#)

概要

トンネルで Cisco Encryption Technology (CET) 暗号化を設定するには、トンネルのインターフェイスで暗号化を設定する必要があります。また、トンネルの最終的な接続先に向う物理インターフェイスでも暗号化を設定する必要があります。

注：CET暗号化は[サポート終了](#)です。移行のためには、暗号化方式として IP Security (IPSec) をお勧めします。

前提条件

要件

このドキュメントに特有の要件はありません。

使用するコンポーネント

このドキュメントの内容は、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

表記法

ドキュメントの表記法の詳細は、「[シスコ テクニカル ティップスの表記法](#)」を参照してください。

設定

このセクションでは、このドキュメントで説明する機能を設定するために必要な情報を提供しています。

注：この文書で使用されているコマンドの詳細を調べるには、「Command Lookup ツール」を使用してください（登録ユーザのみ）。

ネットワーク図

このドキュメントでは、次のネットワーク セットアップを使用します。



ネットワーク構成図に関する注記

- r3-4k の背後の 8.8.8.8、および R6-2500 の背後の 7.7.7.4 は端末です。これらが互いに ping を実行すると、トラフィックはトンネルを通過します。
- Generic Routing Encapsulation (GRE; 総称ルーティング カプセル化) トンネルは、トンネルの発信元および送信先としてループバック インターフェイスが設定されています。
- トンネルを通過するトラフィックも暗号化を行います。この機能を実行するにはトンネルトラフィックを暗号化するために、トンネル インターフェイスと物理送信インターフェイスの両方において暗号化マップを結びつける必要があります。

設定

このドキュメントでは、次の構成を使用します。

- [r3-4k](#)
- [R1-AGS](#)
- [R6-2500](#)

r3-4k

```
hostname r3-4k
!
crypto public-key r6-2500 02014544
  F3681B5D 32372A19 0C0CCC4B E707F829 D882CF30 A9B4DBE3
E1911E9C F6A9E162
  732558DF A20FEFAD 2ACC400E 8DDB10B1 3566FA3A E55A9BBE
00916AAD 20A0C75C
quit
!
crypto map my_crypto_map 10
  set algorithm 40-bit-des
  set peer r6-2500
  match address 128
!
interface Loopback0
```

```

ip address 1.1.6.1 255.255.255.0
!
interface Tunnel0
ip address 5.5.5.1 255.255.255.0
tunnel source Loopback0
tunnel destination 2.2.6.3
crypto map my_crypto_map
!
interface Ethernet0
ip address 1.1.1.1 255.255.255.0
description inside interface
media-type 10BaseT
crypto map my_crypto_map
!
!
interface Serial0
encapsulation frame-relay
no ip route-cache
!
interface Serial0.1 point-to-point
description outside interface
ip address 8.8.8.1 255.255.255.0
frame-relay interface-dlci 100
!
!ip classless
ip route 0.0.0.0 0.0.0.0 1.1.1.2
ip route 7.0.0.0 255.0.0.0 5.5.5.2

access-list 128 permit gre host 1.1.6.1 host 2.2.6.3
!

```

R1-AGS

```

!
hostname R1-AGS
!
interface Ethernet0
ip address 1.1.1.2 255.255.255.0
!
interface Serial1
ip address 2.2.5.2 255.255.255.0
!
ip classless
ip route 1.0.0.0 255.0.0.0 1.1.1.1
ip route 2.0.0.0 255.0.0.0 2.2.5.3

```

R6-2500

```

hostname R6-2500
!
crypto public-key r3-4k 04D6265A
512A7D84 43C348B7 959D2FE2 3122B285 FDA2A362 7272A835
84D03134 DB160DE1
27CA2D24 D6C23EFE 3BE25A95 D62EA30B 0F2C3BA8 9AB6DB82
D8127238 266AC987
quit
!
crypto map my_crypto_map 10
set algorithm 40-bit-des
set peer r3-4k
match address 128
!
interface Loopback0

```

```
ip address 2.2.6.3 255.255.255.0
!
interface Tunnel0
ip address 5.5.5.2 255.255.255.0
tunnel source Loopback0
tunnel destination 1.1.6.1
crypto map my_crypto_map
!
interface Ethernet 0
description inside interface
ip address 7.7.7.3 255.255.255.0
!
interface Serial0
description outside interface
ip address 2.2.5.3 255.255.255.0
crypto map my_crypto_map
!
ip classless
ip route 0.0.0.0 0.0.0.0 2.2.5.2
ip route 7.0.0.0 255.0.0.0 7.7.7.0
ip route 8.0.0.0 255.0.0.0 5.5.5.1
!
access-list 128 permit gre host 2.2.6.3 host 1.1.6.1
```

確認

現在、この設定に使用できる確認手順はありません。

トラブルシューティング

現在、この設定に関する特定のトラブルシューティング情報はありません。

関連情報

- [IPSec に関するサポート ページ](#)
- [テクニカルサポート - Cisco Systems](#)