

IPSec ルータ間の フルメッシュの設定

目次

[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](#)

[トラブルシューティングのためのコマンド](#)

[関連情報](#)

概要

この設定例は、3 台のルータ間のフルメッシュ暗号化を示しています。つまり、各ルータは 2 つのピアそれぞれの背後にあるネットワークに対して、1 つずつ暗号化マップを使用しています。

暗号化は、次の方向で実行されます。

- 160.160.160.x ネットワークから 170.170.170.x ネットワークへ
- 160.160.160.x ネットワークから 180.180.180.x ネットワークへ
- 170.170.170.x ネットワークから 180.180.180.x ネットワークへ

前提条件

要件

このドキュメントに関する固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情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- Cisco IOS® ソフトウェア リリース 12.2.7C および 12.2.8(T)4
- Cisco 2500 および 3600 ルータ

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。このドキュメントで使用するすべてのデバイスは、クリアな (デフォルト) 設定で作業を開始して

います。ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

表記法

ドキュメント表記の詳細は、『[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

この項では、このドキュメントで説明する機能の設定に必要な情報を提供します。

注: このドキュメントで使用されているコマンドの詳細を調べるには、[Command Lookup Tool](#) ([登録ユーザ専用](#)) を使用してください。

ネットワーク図

このドキュメントでは、次の図で示されるネットワーク構成を使用しています。

設定

このドキュメントでは、次の設定を使用します。

- [dr_Whoovie の設定](#)
- [yertle の設定](#)
- [thidwick の設定](#)

注: これらの設定は、ドキュメント内の現在のコード (2003 年 11 月) を使用して最近テストされました。

dr_Whoovie の設定

```
Current configuration:
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname dr_whoovie
!
enable secret 5 $1$KxKv$cbqKsZtQTLJLGPn.tErFZ1
enable password ww
!
ip subnet-zero
!
cns event-service server
!
!--- Internet Key Exchange (IKE) Policies: crypto isakmp
policy 1 authentication pre-share crypto isakmp key
cisco123 address 150.150.150.3 crypto isakmp key
cisco123 address 150.150.150.2 ! !--- IPsec Policies:
crypto ipsec transform-set 170cisco esp-des esp-md5-hmac
crypto ipsec transform-set 180cisco esp-des esp-md5-hmac
! crypto map ETH0 17 ipsec-isakmp set peer 150.150.150.2
set transform-set 170cisco !--- Include the
160.160.160.x to 170.170.170.x network !--- in the
```

```

encryption process. match address 170 crypto map ETH0 18
ipsec-isakmp set peer 150.150.150.3 set transform-set
180cisco !--- Include the 160.160.160.x to 180.180.180.x
network !--- in the encryption process. match address
180 ! interface Ethernet0 ip address 150.150.150.1
255.255.255.0 no ip directed-broadcast no ip route-cache
no ip mroute-cache no mop enabled crypto map ETH0 !
interface Ethernet1 no ip address no ip directed-
broadcast shutdown ! interface Serial0 ip address
160.160.160.1 255.255.255.0 no ip directed-broadcast no
ip mroute-cache no fair-queue ! interface Serial1 no ip
address no ip directed-broadcast clockrate 4000000 ! ip
classless ip route 170.170.170.0 255.255.255.0
150.150.150.2 ip route 180.180.180.0 255.255.255.0
150.150.150.3 no ip http server ! !--- Include the
160.160.160.x to 170.170.170.x network !--- in the
encryption process. access-list 170 permit ip
160.160.160.0 0.0.0.255 170.170.170.0 0.0.0.255 !---
Include the 160.160.160.x to 180.180.180.x network !---
in the encryption process. access-list 180 permit ip
160.160.160.0 0.0.0.255 180.180.180.0 0.0.0.255 dialer-
list 1 protocol ip permit dialer-list 1 protocol ipx
permit ! line con 0 transport input none line aux 0 line
vty 0 4 password ww login ! end

```

yertle の設定

```

Current configuration:
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname yertle
!
enable secret 5 $1$me5Q$2kF5zKlPPTvHEBdGiEZ9m/
enable password ww
!
ip subnet-zero
!
cns event-service server
!
!--- IKE Policies: crypto isakmp policy 1 authentication
pre-share crypto isakmp key cisco123 address
150.150.150.3 crypto isakmp key cisco123 address
150.150.150.1 ! !--- IPSec Policies: crypto ipsec
transform-set 160cisco esp-des esp-md5-hmac crypto ipsec
transform-set 180cisco esp-des esp-md5-hmac ! crypto map
ETH0 16 ipsec-isakmp set peer 150.150.150.1 set
transform-set 160cisco !--- Include the 170.170.170.x to
160.160.160.x network !--- in the encryption process.
match address 160 crypto map ETH0 18 ipsec-isakmp set
peer 150.150.150.3 set transform-set 180cisco !---
Include the 170.170.170.x to 180.180.180.x network !---
in the encryption process. match address 180 ! interface
Ethernet0 ip address 150.150.150.2 255.255.255.0 no ip
directed-broadcast no ip route-cache no ip mroute-cache
no mop enabled crypto map ETH0 ! interface Serial0 no ip
address no ip directed-broadcast no ip mroute-cache
shutdown no fair-queue ! interface Serial1 ip address
170.170.170.1 255.255.255.0 no ip directed-broadcast !
ip classless ip route 160.160.160.0 255.255.255.0
150.150.150.1 ip route 180.180.180.0 255.255.255.0
150.150.150.3 no ip http server ! !--- Include the

```

```
170.170.170.x to 160.160.160.x network !--- in the
encryption process. access-list 160 permit ip
170.170.170.0 0.0.0.255 160.160.160.0 0.0.0.255 !---
Include the 170.170.170.x to 180.180.180.x network !---
in the encryption process. access-list 180 permit ip
170.170.170.0 0.0.0.255 180.180.180.0 0.0.0.255 dialer-
list 1 protocol ip permit dialer-list 1 protocol ipx
permit ! line con 0 transport input none line aux 0 line
vty 0 4 password ww login ! end
```

thidwick の設定

```
Current configuration:
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname thidwick
!
enable secret 5 $1$Pcpo$fj4FNS1dEDY9lGg3Ne6FK1
enable password ww
!
ip subnet-zero
!
isdn switch-type basic-5ess
isdn voice-call-failure 0
cns event-service server
!
!--- IKE Policies: crypto isakmp policy 1 authentication
pre-share crypto isakmp key cisco123 address
150.150.150.1 crypto isakmp key cisco123 address
150.150.150.2 ! !--- IPsec Policies: crypto ipsec
transform-set 160cisco esp-des esp-md5-hmac crypto ipsec
transform-set 170cisco esp-des esp-md5-hmac ! crypto map
ETH0 16 ipsec-isakmp set peer 150.150.150.1 set
transform-set 160cisco !--- Include the 180.180.180.x to
160.160.160.x network !--- in the encryption process.
match address 160 crypto map ETH0 17 ipsec-isakmp set
peer 150.150.150.2 set transform-set 170cisco !---
Include the 180.180.180.x to 170.170.170.x network !---
in the encryption process. match address 170 ! interface
Ethernet0 ip address 150.150.150.3 255.255.255.0 no ip
directed-broadcast no ip route-cache no ip mroute-cache
no mop enabled crypto map ETH0 ! interface Serial0 no ip
address no ip directed-broadcast no ip mroute-cache no
fair-queue clockrate 4000000 ! interface Serial1 ip
address 180.180.180.1 255.255.255.0 no ip directed-
broadcast clockrate 4000000 ! interface BRI0 no ip
address no ip directed-broadcast shutdown isdn switch-
type basic-5ess ! ip classless ip route 160.160.160.0
255.255.255.0 150.150.150.1 ip route 170.170.170.0
255.255.255.0 150.150.150.2 no ip http server ! !---
Include the 180.180.180.x to 160.160.160.x network !---
in the encryption process. access-list 160 permit ip
180.180.180.0 0.0.0.255 160.160.160.0 0.0.0.255 !---
Include the 180.180.180.x to 170.170.170.x network !---
in the encryption process. access-list 170 permit ip
180.180.180.0 0.0.0.255 170.170.170.0 0.0.0.255 dialer-
list 1 protocol ip permit dialer-list 1 protocol ipx
permit ! line con 0 transport input none line aux 0 line
vty 0 4 password ww login ! end
```

確認

このセクションでは、設定が正常に動作しているかどうかを確認する際に役立つ情報を提供しています。

特定の show コマンドは、[Output Interpreter Tool](#) ([登録ユーザ専用](#)) によってサポートされています。このツールを使用すると、show コマンド出力の分析を表示できます。

- `show crypto ipsec sa` : 現在の IPsec セキュリティ アソシエーションで使用されている設定を表示します。
- `show crypto isakmp sa` : ピアにおける現在の IKE セキュリティ アソシエーションをすべて表示します。

トラブルシューティング

ここでは、設定のトラブルシューティングに役立つ情報について説明します。

トラブルシューティングのためのコマンド

注: debug コマンドを使用する前に、[『debug コマンドの重要な情報』](#)を参照してください。

- `debug crypto ipsec` : フェーズ 2 の IPsec ネゴシエーションを表示します。
- `debug crypto isakmp` - フェーズ 1 の Internet Security Association and Key Management Protocol (ISAKMP) ネゴシエーションを表示します。
- `debug crypto engine` : 暗号化されたトラフィックを表示します。
- `clear crypto isakmp` : フェーズ 1 に関連したセキュリティ アソシエーションをクリアします。
- `clear crypto sa` : フェーズ 2 に関連したセキュリティ アソシエーションをクリアします。

関連情報

- [IPsec に関するサポート ページ](#)
- [IPsec ネットワーク セキュリティの設定](#)
- [インターネット キー交換セキュリティ プロトコルの設定](#)
- [テクニカルサポート - Cisco Systems](#)