IPSec ルータ間にハブとスポークの設定

目次

はじめに

このドキュメントでは、1 つのルータ (「ハブ」) と 3 つの他のルータ (「スポーク」) の間で行う、ハブとスポークの暗号化について説明します。 ハブ ルータには、3 つの各ピアの背後にあるネットワークを指定した暗号マップが 1 つあります。 各スポーク ルータの暗号マップでは、ハブ ルータの背後のネットワークが指定されています。

暗号化はこれらのネットワークの間で行われます:

- 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
- 160.160.160.x ネットワークから 190.190.190.x ネットワーク

前提条件

要件

このドキュメントに関しては個別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 12.0.7.T または それ 以降
- Cisco 2500 ルータ

本書の情報は、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、初期（デフォルト）設定の状態から起動しています。 稼働中のネットワークで作業を行う場合、コマンドの影響について十分に理解したうえで作業してください。

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
- sam-I-am の設定
- thidwick の設定
- yertle の設定

dr_whoovie の設定

```
Current configuration:
!
version 12.0
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
!--- Configure the Internet Key Exchange (IKE) !---
policy and preshared key for each peer: !--- IKE policy
defined for peers. crypto isakmp policy 1
authentication pre-share
!--- Preshared keys for different peers. crypto isakmp
key cisco170 address 150.150.150.2
crypto isakmp key cisco180 address 150.150.150.3
```

```
crypto isakmp key cisco190 address 150.150.150.4
!--- Configure the IPSec parameters: !--- IPSec
transform sets. crypto ipsec transform-set 170cisco esp-
des esp-md5-hmac
crypto ipsec transform-set 180cisco esp-des esp-md5-hmac
crypto ipsec transform-set 190cisco esp-des esp-md5-hmac
!
crypto map ETH0 17 ipsec-isakmp
!--- Set the peer. set peer 150.150.150.2
!--- The IPSec transform set is used for this tunnel.
set transform-set 170cisco
!--- Interesting traffic for peer 150.150.150.2. match
address 170
crypto map ETH0 18 ipsec-isakmp
!--- Set the peer. set peer 150.150.150.3
!--- The IPSec transform set is used for this tunnel.
set transform-set 180cisco
!--- Interesting traffic for peer 150.150.150.3. match
address 180
crypto map ETH0 19 ipsec-isakmp
!--- Set the peer. set peer 150.150.150.4
!--- The IPSec transform set is used for this tunnel.
set transform-set 190cisco
!--- Interesting traffic for peer 150.150.150.4. match
address 190
!
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
!--- Apply crypto map on the interface. crypto map ETH0
!
interface Serial0
ip address 160.160.160.1 255.255.255.0
no ip directed-broadcast
no ip mroute-cache
no fair-queue
!
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
ip route 190.190.190.0 255.255.255.0 150.150.150.4
no ip http server
!
!--- Access list that shows traffic to encryption from
yertle. access-list 170 permit ip 160.160.160.0
0.0.0.255 170.170.170.0 0.0.0.255
!--- Access list that shows traffic to encryption from
thidwick. access-list 180 permit ip 160.160.160.0
0.0.0.255 180.180.180.0 0.0.0.255
!--- Access list that shows traffic to encryption from
sam-i-am. access-list 190 permit ip 160.160.160.0
0.0.0.255 190.190.190.0 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
```

sam-I-am の設定

```
Current configuration:
!
```

```
version 12.0
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Sam-I-am
!
enable secret 5 $1$HDyw$qubSJdqfIC0f1VLvHmg/P0
enable password ww
!
ip subnet-zero
!
isdn switch-type basic-5ess
isdn voice-call-failure 0
cns event-service server
!--- Configure the IKE policy and preshared key for the
hub: crypto isakmp policy 1
authentication pre-share
crypto isakmp key cisco190 address 150.150.150.1
!--- Configure the IPSec parameters: !--- IPSec
transform set. crypto ipsec transform-set 190cisco esp-
des esp-md5-hmac
!--- Crypto map definition for the hub site. crypto map
ETH0 19 ipsec-isakmp
!--- Set the peer. set peer 150.150.150.1
!--- IPSec transform set. set transform-set 190cisco
!--- Interesting traffic for peer 150.150.150.1 (hub
site). match address 190
!
interface Ethernet0
ip address 150.150.150.4 255.255.255.0
no ip directed-broadcast
no ip route-cache
no ip mroute-cache
no mop enabled
!--- Apply crypto map on the interface. crypto map ETH0
!
interface Serial0
ip address 190.190.190.1 255.255.255.0
no ip directed-broadcast
no ip mroute-cache
no fair-queue
!
ip classless
ip route 160.160.160.0 255.255.255.0 150.150.150.1
no ip http server
!--- Access list that shows traffic to encryption !---
for the hub site (dr_whoovie). access-list 190 permit ip
190.190.190.0 0.0.0.255 160.160.160.0 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 12.0
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
!--- Configure the IKE policy and preshared key for the
hub: crypto isakmp policy 1
authentication pre-share
crypto isakmp key cisco180 address 150.150.150.1
!--- Configure the IPSec parameters: !--- IPSec
transform set. crypto ipsec transform-set 180cisco esp-
des esp-md5-hmac
!--- Crypto map definition for the hub site. crypto map
ETH0 18 ipsec-isakmp
!--- Set the peer. set peer 150.150.150.1
!--- IPSec transform set. set transform-set 180cisco
!--- Interesting traffic for peer 150.150.150.1 (hub
site). match address 180
!
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
!--- Apply crypto map on the interface. crypto map ETH0
!
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
no ip http server
!--- Access list that shows traffic to encryption !---
for the hub site (dr_whoovie). access-list 180 permit ip
180.180.180.0 0.0.0.255 160.160.160.0 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 12.0
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
!--- Configure the IKE policy and preshared key for the
hub: crypto isakmp policy 1
authentication pre-share
crypto isakmp key cisco170 address 150.150.150.1
!--- Configure the IPSec parameters: !--- IPSec
transform set. crypto ipsec transform-set 170cisco esp-
des esp-md5-hmac
!--- Crypto map definition for the hub site. crypto map
ETH0 17 ipsec-isakmp
!--- Set the peer. set peer 150.150.150.1
!--- IPSec transform set. set transform-set 170cisco
!--- Interesting traffic for peer 150.150.150.1 (hub
site). match address 170
!
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
!--- Apply crypto map on the interface. 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
no ip http server
!--- Access list that shows traffic to encryption for !-
-- the hub site (dr_whoovie). access-list 170 permit ip
170.170.170.0 0.0.0.255 160.160.160.0 0.0.0.255
dialer-list 1 protocol ip permit
dialer-list 1 protocol ipx permit
!
```

```
tftp-server flash:/c2500-jos56i-l.120-7.T
tftp-server flash:c2500-jos56i-l.120-7.T
tftp-server flash:
!
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**：フェーズ 2 のセキュリティ アソシエーションを表示します。
- **show crypto isakmp sa**：フェーズ 1 のセキュリティ アソシエーションを表示します。

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 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 ネットワーク セキュリティを設定して下さい
- インターネットキー交換セキュリティプロトコルを設定して下さい
- IPSec に関するサポート ページ
- テクニカルサポート - Cisco Systems