配置IPSec路由器到路由器的中心輻射點

目錄

簡介

本文顯示從一台路由器（「集線器」）到另外三台路由器（「輻條」）的星型和中心加密。 集線器路由器上有一個加密對映，指定三個對等點後方的網路。每個分支路由器上的加密對映指定中心路由器後面的網路。

加密在這些網路之間完成：

- 160.160.160.x網路到170.170.170.x網路
- 160.160.160.x網路到180.180.180.x網路
- 160.160.160.x網路到190.190.190.x網路

必要條件

需求

本文件沒有特定需求。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Cisco IOS®軟體版本12.0.7.T或更高版本
- Cisco 2500路由器

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設

) 的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

慣例

如需文件慣例的詳細資訊，請參閱思科技術提示慣例。

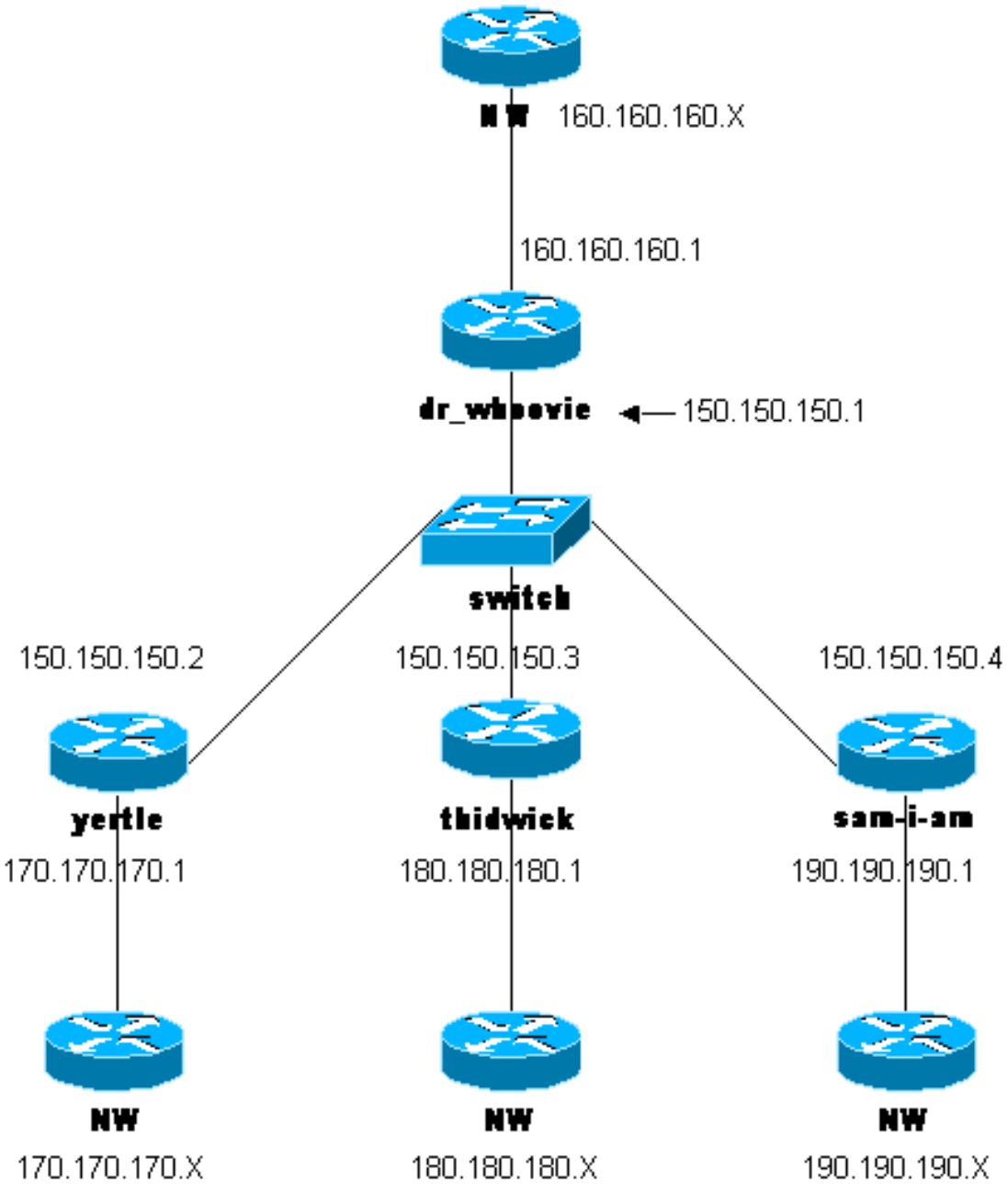
設定

本節提供用於設定本文件中所述功能的資訊。

注意：要查詢有關本文檔中使用的命令的其他資訊，請使用命令查詢工具(僅限註冊客戶)。

網路圖表

本檔案會使用以下網路設定：



組態

本檔案會使用以下設定：

- dr_who配置
- sam-I-am配置
- thidwick配置
- yertle配置

dr_who配置

```
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配置

```
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配置

```
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配置

```
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
```

驗證

本節提供的資訊可用於確認您的組態是否正常運作。

輸出直譯器工具(僅供註冊客戶使用)支援某些show命令，此工具可讓您檢視show命令輸出的分析。

- show crypto ipsec sa — 顯示第2階段安全關聯。
- show crypto isakmp sa — 顯示第1階段安全關聯。

疑難排解

本節提供的資訊可用於對組態進行疑難排解。

疑難排解指令

注意：發出debug命令之前，請參閱有關Debug命令的重要資訊**。**

- debug crypto ipsec — 顯示第2階段的IPSec協商。
- debug crypto isakmp — 顯示第1階段的ISAKMP協商。
- debug crypto engine — 顯示加密的流量。
- clear crypto isakmp — 清除與第1階段相關的安全關聯。
- clear crypto sa — 清除與第2階段相關的安全關聯。

相關資訊

- **配置IPSec網路安全**
- **配置網際網路金鑰交換安全協定**
- IPSec支援頁面
- 技術支援 - Cisco Systems