配置IPSec路由器到路由器星型网

目录

简介

本文介绍从一个路由器("hub")到其他三个路由器("spoke")星型网加密。 在中心路由器上有一个加密映射，指定了三个对等路由器身后的网络。在每个分支路由器上的加密映射指定了在中心路由器背后的网络。

加密是在这些网络之间完成：

- 160.160.160.x 网络到 170.170.170.x 网络
- 160.160.160.x 网络到 180.180.180.x 网络
- 160.160.160.x 网络到 190.190.190.x 网络

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- Cisco IOS®软件版本12.0.7.T或更高版本
- Cisco 2500 路由器

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原

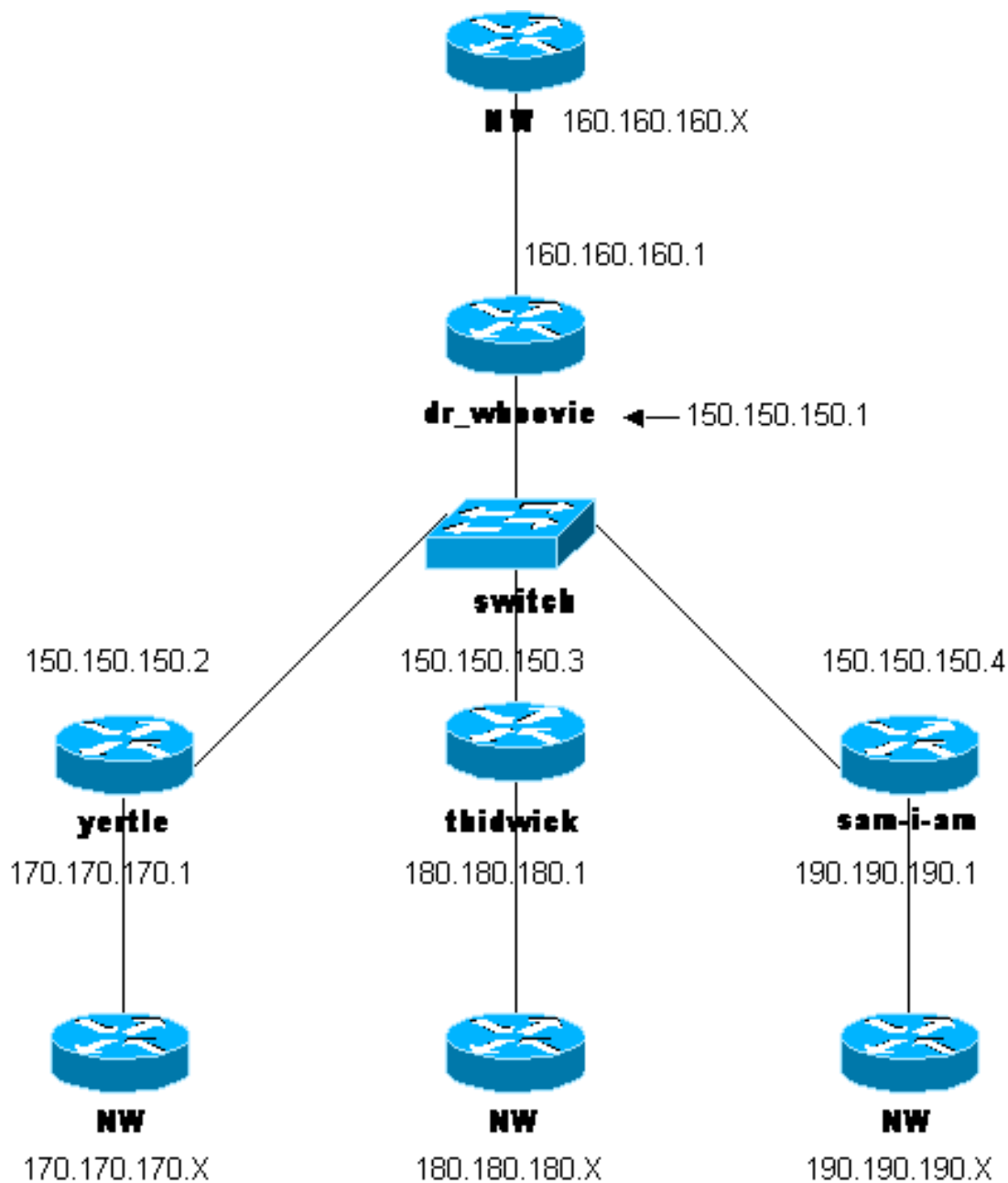始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

配置

本部分提供有关如何配置本文档所述功能的信息。

注：要查找有关本文档中使用的命令的其他信息，请使用命令查找工具(仅注册客户)。

网络图

本文档使用以下网络设置：

配置

本文档使用以下配置：

- [dr_whoovie配置](#)
- [sam-i-am配置](#)
- [thidwick配置](#)
- [分类器配置](#)

dr_whoovie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
```

分类器配置

```
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
```

验证

本部分所提供的信息可用于确认您的配置是否正常工作。

命令输出解释程序工具（仅限注册用户）支持某些 show 命令，使用此工具可以查看对 show 命令输出的分析。

- show crypto ipsec sa - 显示阶段 2 的安全关联。
- show crypto isakmp sa - 显示第 1 阶段的安全关联。

故障排除

本部分提供的信息可用于对配置进行故障排除。

故障排除命令

注意：在发出debug命令之前，请参阅有关Debug命令的重要信息。

- debug crypto ipsec - 显示第 2 阶段的 IPsec 协商。
- debug crypto isakmp - 显示第 1 阶段的 ISAKMP 协商。
- debug crypto engine - 显示已加密的流量。
- clear crypto isakmp - 清除与第 1 阶段相关的安全关联。
- clear crypto sa - 清除与第 2 阶段相关的安全关联。

相关信息

- 配置IPSec网络安全
- 配置Internet密钥交换安全协议
- IPSec 支持页面
- 技术支持 - Cisco Systems