

配置路由器间 IPSec 全网状连接

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[规则](#)

[配置](#)

[网络图](#)

[配置](#)

[验证](#)

[故障排除](#)

[故障排除命令](#)

[相关信息](#)

简介

此配置示例显示通过在二对等体中每一个后使用一个加密映射器到每一个路由器到网络的三个路由器之间的全网状加密。

加密是完成从：

- 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
- 170.170.170.x对180.180.180.x网络的网络

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12.2.7C和12.2.8(T)4
- Cisco2500和3600个路由器

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](#)。

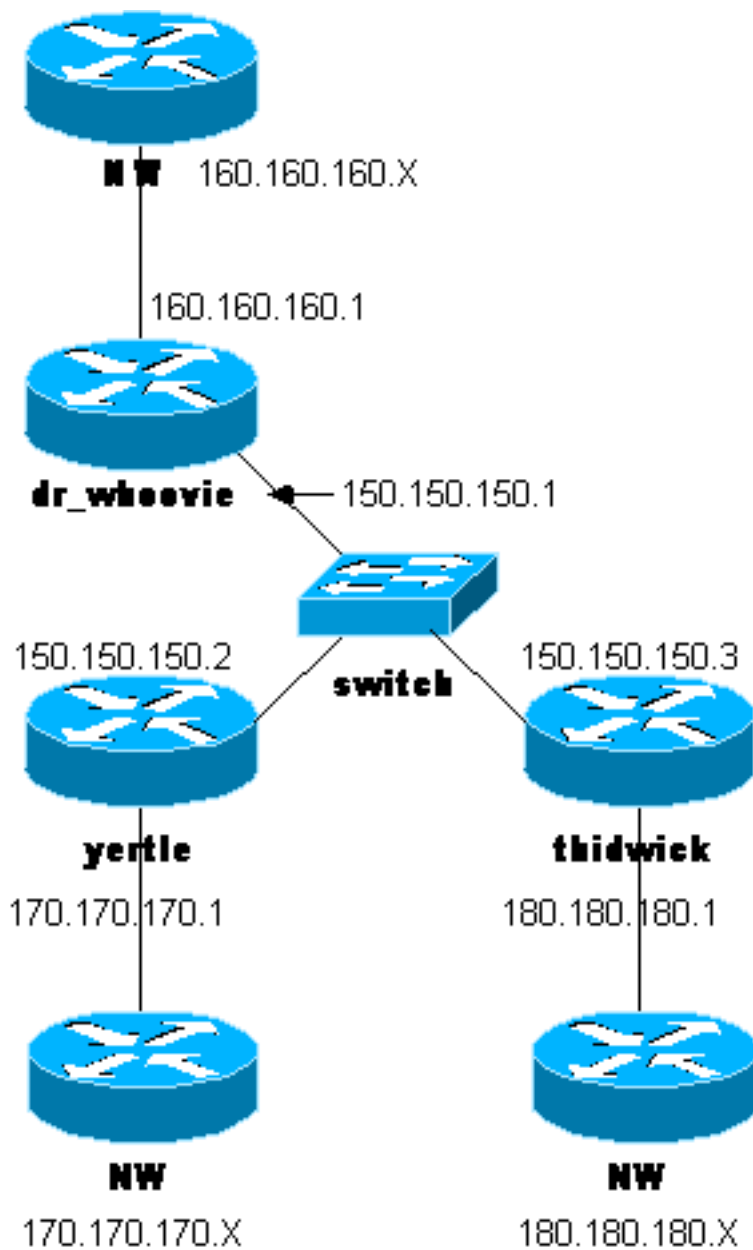
配置

本部分提供有关如何配置本文档所述功能的信息。

注意：要查找本文档所用命令的其他信息，请使用 [命令查找工具](#)（[仅限注册用户](#)）。

网络图

本文档使用此图所示的网络设置。



配置

本文档使用以下配置。

- [Dr_whoovie配置](#)
- [Yertle配置](#)
- [Thidwick配置](#)

注意：这些配置用当前代码(十一月最近测试2003)在本文内。

Dr_whoovie配置

```
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配置

```
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配置

```

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
```

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** - 显示当前 [IPSec] 安全关联所使用的设置。
- **show crypto isakmp sa** —显示所有当前IKE安全关联在对等体。

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 Internet 安全连接和密钥管理协议 (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

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