# Configurando IPSec de roteador para roteador totalmente engrenado

## Contents



## Introduction

Este exemplo de configuração mostra a criptografia totalmente em malha entre três roteadores através do uso de um mapa de criptografia em cada roteador para as redes atrás de cada um de seus dois pares.

A criptografia deve ser feita de:

- Rede 160.160.160.x para rede 170.170.170.x
- Rede 160.160.160.x para rede 180.180.180.x
- rede 170.170.170.x para rede 180.180.180.x

## Prerequisites

### Requirements

Não existem requisitos específicos para este documento.

### Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Software Cisco IOS® versão 12.2.7C e 12.2.8(T)4
- Cisco 2500 and 3600 routers

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

### Conventions

For more information on document conventions, refer to the Cisco Technical Tips Conventions.

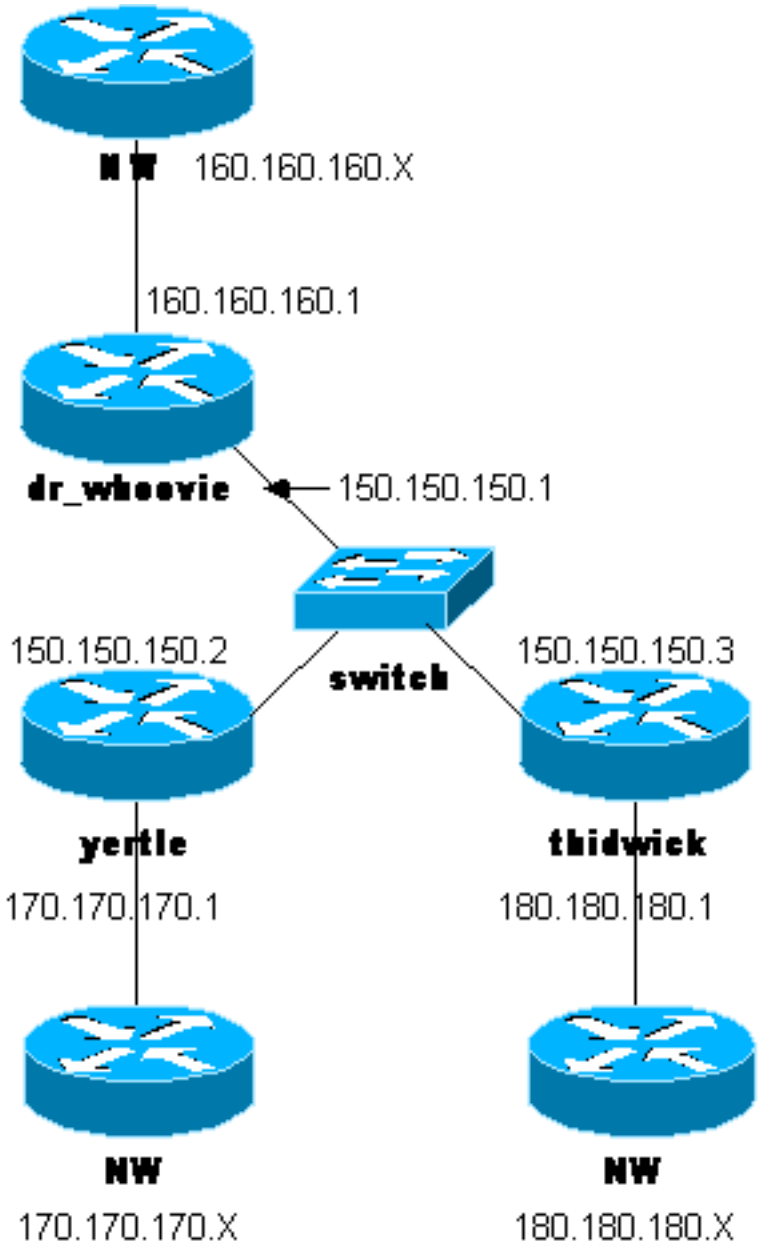
## Configurar

Nesta seção, você encontrará informações para configurar os recursos descritos neste documento.

**Observação:** para encontrar informações adicionais sobre os comandos usados neste documento, use a ferramenta Command Lookup Tool (somente clientes registrados).

### Diagrama de Rede

Este documento utiliza a configuração de rede mostrada neste diagrama.




## Configurações

Este documento utiliza estas configurações.

- configuração de dr_whoovie
- Configuração yertle
- Configuração de thidwick

**Observação:** essas configurações foram testadas recentemente com o código atual (novembro de 2003) no documento.

| configuração de dr_whoovie |
| --- |
| Current configuration:<br>!<br>version 12.2<br>service timestamps debug uptime<br>service timestamps log uptime<br>no service password-encryption<br>! |

```
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
```

## Configuração yertle

```
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
```

## Configuração de thidwick

```
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
```

# Verificar

Esta seção fornece informações que você pode usar para confirmar se sua configuração está funcionando adequadamente.

A Output Interpreter Tool (somente clientes registrados) oferece suporte a determinados comandos show, o que permite exibir uma análise da saída do comando show.

- **show crypto ipsec sa** — Mostra as configurações usadas pelas associações de segurança atuais do [IPSec].
- **show crypto isakmp sa** — Mostra todas as associações de segurança IKE atuais em um peer.

# Troubleshoot

Esta seção fornece informações que podem ser usadas para o troubleshooting da sua configuração.

## Comandos para Troubleshooting

**Observação:** antes de inserir o comando **debug**, consulte Informações importantes sobre os comandos debug.

- **debug crypto ipsec — Exibe as negociações de IPSec de fase 2**
- **debug crypto isakmp** — Exibe as negociações de Internet Security Association and Key Management Protocol (ISAKMP) da fase 1.
- **debug crypto engine — Exibe o tráfego que está criptografado.**
- **clear crypto isakmp — Limpa as associações de segurança relacionadas à fase 1.**
- **clear crypto sa — Limpa as associações de segurança relacionadas à fase 2.**

# Informações Relacionadas

- Página de suporte do IPSec
- Configuração da segurança de rede IPSec
- Configurando o protocolo de segurança do intercâmbio chave de Internet
- Suporte Técnico - Cisco Systems