

Configurando o hub and spoke do roteador para roteador do IPsec

Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenções](#)

[Configurar](#)

[Diagrama de Rede](#)

[Configurações](#)

[Verificar](#)

[Troubleshooting](#)

[Comandos para Troubleshooting](#)

[Informações Relacionadas](#)

[Introdução](#)

Este documento mostra a criptografia hub e spoke de um roteador (o hub) para três outros roteadores (os spokes). Não existe um mapa de criptografia no roteador hub que especifique as redes atrás de cada um de seus três peers. Os mapas de criptografia em cada um dos roteadores spoke especificam a rede atrás do roteador de hub.

A criptografia é feita entre estas redes:

- Rede 160.160.160.x para rede 170.170.170.x
- Rede 160.160.160.x para rede 180.180.180.x
- rede 160.160.160.x para rede 190.190.190.x

[Pré-requisitos](#)

[Requisitos](#)

Não existem requisitos específicos para este documento.

[Componentes Utilizados](#)

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

- Software Release 12.0.7.T ou Mais Recente de Cisco IOS®

- Cisco 2500 Router

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Convenções

Para obter mais informações sobre convenções de documento, consulte as [Convenções de dicas técnicas Cisco](#).

Configurar

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

Nota: Para localizar informações adicionais sobre os comandos usados neste documento, utilize a Ferramenta Command Lookup (somente clientes [registrados](#)).

Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:

Configurações

Este documento utiliza as seguintes configurações:

- [configuração de dr_whoovie](#)
- [Configuração sam-I-am](#)
- [configuração de thidwick](#)
- [configuração do yertle](#)

configuração de dr_whoovie

```
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.tErFZl
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

```

Configuração sam-I-am

```

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

```

configuração de thidwick

```

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

```

configuração do yertle

```

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-
1.120-7.T tftp-server flash:c2500-jos56i-1.120-7.T tftp-
server flash: ! 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 associações de segurança da fase 2.
- show crypto isakmp sa - Mostra as associações de segurança da fase 1.

Troubleshooting

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

Comandos para Troubleshooting

Nota: Antes de emitir comandos de depuração, consulte as informações importantes sobre eles.

- **IPsec do debug crypto** — Indica as negociações de IPSEC de fase 2.
- **isakmp do debug crypto** — Indica as negociações de ISAKMP de 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

- [Configurar a Segurança de rede IPSec](#)
- [Configurar o protocolo de segurança do intercâmbio chave de Internet](#)
- [Página de suporte do IPSec](#)
- [Suporte Técnico - Cisco Systems](#)