

Configurando IPSec entre três roteadores usando endereços privados

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Conventions](#)

[Configurar](#)

[Diagrama de Rede](#)

[Configurações](#)

[Verificar](#)

[Troubleshoot](#)

[Comandos para Troubleshooting](#)

[Informações Relacionadas](#)

[Introduction](#)

Este documento descreve uma configuração totalmente em malha com três roteadores que usam endereços privados. O exemplo ilustra estes recursos:

- Payload de Segurança de Encapsulamento (ESP - Encapsulating Security Payload) - Somente DES (Data Encryption Standard)
- Chaves pré-compartilhadas
- Redes privadas atrás de cada roteador: 192.168.1.0, 192.168.2.0 e 192.168.3.0
- política isakmp e configuração de mapa de criptografia
- Tráfego de túnel definido com os comandos **access-list** e **route-map**. Além da Conversão de Endereço de Porta (PAT - Port Address Translation), os mapas de rotas podem ser aplicados a uma Conversão de Endereço de Rede (NAT - Network Address Translation) estática um para um no Cisco IOS® Software Release 12.2(4)T2 e posteriores. Para obter mais informações, consulte [NAT - Ability to Use Route Maps with Static Translations Feature Overview](#).

Observação: a tecnologia de criptografia está sujeita a controles de exportação. É sua responsabilidade conhecer a lei sobre exportação de tecnologia de criptografia. Se você tem alguma dúvida com relação ao controle de exportação, envie um e-mail para export@cisco.com.

[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 12.3.(7)T.
- Roteadores Cisco configurados com IPSec.

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

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

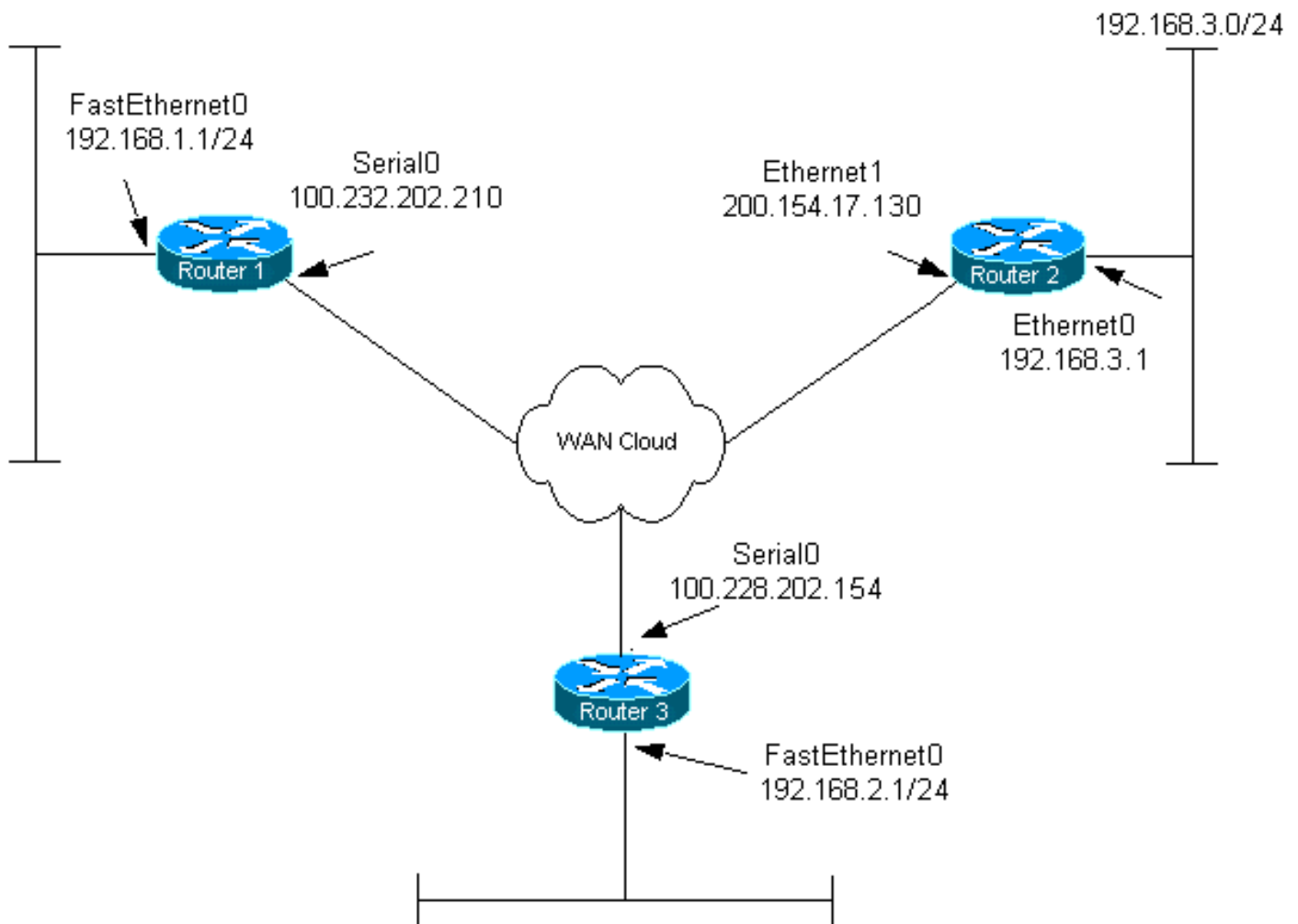
Configurar

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

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 seguinte configuração de rede:



Configurações

Este documento utiliza as seguintes configurações:

- [Roteador 1](#)
- [Roteador 2](#)
- [Roteador 3](#)

Roteador 1

```
Current configuration:
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname router1
!
boot-start-marker
boot-end-marker
!
!
clock timezone EST 0
no aaa new-model
ip subnet-zero
!
!
```

```
ip audit po max-events 100
no ftp-server write-enable
!

!--- Configure Internet Key Exchange (IKE) policy and !-
-- pre-shared keys for each peer. !--- IKE policy
defined for peers. crypto isakmp policy 4
authentication pre-share

!--- Pre-shared keys for different peers. crypto isakmp
key xxxxxx1234 address 100.228.202.154
crypto isakmp key xxxxxx1234 address 200.154.17.130
!
!

!--- IPsec policies: crypto ipsec transform-set encrypt-
des esp-des
!
!
crypto map combined local-address Serial0

!--- Set the peer, transform-set and encryption traffic
for tunnel peers. crypto map combined 20 ipsec-isakmp
    set peer 100.228.202.154
    set transform-set encrypt-des
    match address 106
crypto map combined 30 ipsec-isakmp
    set peer 200.154.17.130
    set transform-set encrypt-des
    match address 105
!
!
interface Serial0
    ip address 100.232.202.210 255.255.255.252
    ip nat outside
    serial restart-delay 0

!--- Apply the crypto map to the interface. crypto map
combined
!
interface FastEthernet0
    ip address 192.168.1.1 255.255.255.0
    ip nat inside
!
ip classless
ip route 0.0.0.0 0.0.0.0 100.232.202.209
no ip http server
no ip http secure-server
!

!--- Define traffic for NAT. ip nat inside source route-
map nonat interface Serial0 overload

!--- Access control list (ACL) that shows traffic to
encrypt over the tunnel. access-list 105 permit ip
192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255
access-list 106 permit ip 192.168.1.0 0.0.0.255
192.168.2.0 0.0.0.255

!--- ACL to avoid the traffic through NAT over the
tunnel. access-list 150 deny ip 192.168.1.0 0.0.0.255
192.168.2.0 0.0.0.255
access-list 150 deny ip 192.168.1.0 0.0.0.255
192.168.3.0 0.0.0.255
```

```
!--- ACL to perform NAT on the traffic that does not go
over the tunnel. access-list 150 permit ip 192.168.1.0
0.0.0.255 any

!--- Do not perform NAT on the IPSec traffic. route-map
nonat permit 10
  match ip address 150
!
control-plane
!
!
line con 0
line aux 0
line vty 0 4
!
!
end
```

Roteador 2

```
Current configuration:
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname router2
!
boot-start-marker
boot-end-marker
!
!
clock timezone EST 0
no aaa new-model
ip subnet-zero
!
!
ip audit po max-events 100
no ftp-server write-enable
!

!--- Configure IKE policy and pre-shared keys for each
peer. !--- IKE policy defined for peers. crypto isakmp
policy 4
  authentication pre-share

!--- Pre-shared keys for different peers. crypto isakmp
key xxxxxx1234 address 100.228.202.154
crypto isakmp key xxxxxx1234 address 100.232.202.210
!
!

!--- IPSec policies. crypto ipsec transform-set encrypt-
des esp-des
!
!
crypto map combined local-address Ethernet1

!--- Set the peer, transform-set and encryption traffic
for tunnel peers. crypto map combined 7 ipsec-isakmp
set peer 100.232.202.210
```

```

    set transform-set encrypt-des
    match address 105

crypto map combined 8 ipsec-isakmp
    set peer 100.228.202.154
    set transform-set encrypt-des
    match address 106
!
!
!
interface Ethernet0
    ip address 192.168.3.1 255.255.255.0
    ip nat inside
!
interface Ethernet1
    ip address 200.154.17.130 255.255.255.224
    ip nat outside

!--- Apply the crypto map to the interface. crypto map
combined
!
ip classless
ip route 0.0.0.0 0.0.0.0 200.154.17.129
no ip http server
no ip http secure-server
!

!--- Define traffic for NAT. ip nat inside source route-
map nonat interface Ethernet1 overload

!--- ACL shows traffic to encrypt over the tunnel.
access-list 105 permit ip 192.168.3.0 0.0.0.255
192.168.1.0 0.0.0.255
access-list 106 permit ip 192.168.3.0 0.0.0.255
192.168.2.0 0.0.0.255

!--- ACL to avoid the traffic through NAT over the
tunnel. access-list 150 deny ip 192.168.3.0 0.0.0.255
192.168.1.0 0.0.0.255
access-list 150 deny ip 192.168.3.0 0.0.0.255
192.168.2.0 0.0.0.255

!--- ACL to perform NAT on the traffic that does not go
over the tunnel. access-list 150 permit ip any any

!--- Do not perform NAT on the IPsec traffic. route-map
nonat permit 10
    match ip address 150
!
!
!
control-plane
!
!
line con 0
line aux 0
line vty 0 4
!
!
end

```

Configuração do Roteador 3

```
Current configuration:
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname router3
!
boot-start-marker
boot-end-marker
!
!
clock timezone EST 0
no aaa new-model
ip subnet-zero
!
!
ip audit po max-events 100
no ftp-server write-enable
!

!--- Configure IKE policy and pre-shared keys for each
peer. !--- IKE policy defined for peers. crypto isakmp
policy 4
  authentication pre-share

!--- Pre-shared keys for different peers. crypto isakmp
key xxxxxx1234 address 100.232.202.210
crypto isakmp key xxxxxx1234 address 200.154.17.130
!
!

!--- IPsec policies: crypto ipsec transform-set encrypt-
des esp-des
!
!

!--- Set the peer, transform-set and encryption traffic
for tunnel peers. crypto map combined local-address
Serial0
crypto map combined 7 ipsec-isakmp
  set peer 100.232.202.210
  set transform-set encrypt-des
  match address 106
crypto map combined 8 ipsec-isakmp
  set peer 200.154.17.130
  set transform-set encrypt-des
  match address 105
!
!
interface Serial0
  ip address 100.228.202.154 255.255.255.252
  ip nat outside
  serial restart-delay 0

!--- Apply the crypto map to the interface. crypto map
combined
!
  interface FastEthernet0
  ip address 192.168.2.1 255.255.255.0
  ip nat inside
!
```

```

ip classless
ip route 0.0.0.0 0.0.0.0 100.228.202.153
no ip http server
no ip http secure-server
!

!--- Define traffic for NAT. ip nat inside source route-
map nonat interface Serial0 overload

!--- ACL that shows traffic to encrypt over the tunnel.
access-list 105 permit ip 192.168.2.0 0.0.0.255
192.168.3.0 0.0.0.255
access-list 106 permit ip 192.168.2.0 0.0.0.255
192.168.1.0 0.0.0.255

!--- ACL to avoid the traffic through NAT over the
tunnel. access-list 150 deny ip 192.168.2.0 0.0.0.255
192.168.3.0 0.0.0.255
access-list 150 deny ip 192.168.2.0 0.0.0.255
192.168.1.0 0.0.0.255

!--- ACL to perform NAT on the traffic that does not go
over the tunnel. access-list 150 permit ip 192.168.2.0
0.0.0.255 any

!--- Do not perform NAT on the IPSec traffic. route-map
nonat permit 10
    match ip address 150
!
!
!
control-plane
!
!
line con 0
line aux 0
line vty 0 4
    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 engine connections active** – Exibe os pacotes criptografados e decodificados entre os peers IPSec.
- **show crypto isakmp sa** — Mostra todas as associações de segurança (SAs) IKE atuais em um peer.
- **show crypto ipsec sa** —Mostra as configurações usadas por SAs atuais (IPSec).

Troubleshoot

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

[Comandos para Troubleshooting](#)

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

Observação: antes de emitir comandos `debug`, consulte [Informações importantes sobre comandos debug](#).

Observação: as depurações a seguir devem ser executadas em ambos os roteadores IPsec (peers). Limpar SAs deve ser feito em ambos os pares.

- `debug crypto isakmp` — Exibe erros durante a Fase 1.
- `debug crypto ipsec` — Exibe erros durante a Fase 2.
- `debug crypto engine` — Exibe informações a partir do cripto mecanismo.
- `clear crypto connection connection-id [slot] | rsm | vip` — Termina uma sessão criptografada em andamento no momento. As sessões criptografadas normalmente terminam quando a sessão expira. Utilize o comando `show crypto cisco connections` para saber o valor da `connection-id`.
- `clear crypto isakmp` — Limpa as SAs da Fase 1.
- `clear crypto sa` — Limpa as SAs da Fase 2.

[Informações Relacionadas](#)

- [Página de suporte do IPsec](#)
- [Suporte Técnico - Cisco Systems](#)