

# Configurando IPSec entre três roteadores usando endereços privados

## Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenções](#)

[Configurar](#)

[Diagrama de Rede](#)

[Configurações](#)

[Verificar](#)

[Troubleshooting](#)

[Comandos para Troubleshooting](#)

[Informações Relacionadas](#)

## [Introdução](#)

Este documento descreve uma configuração inteiramente engrenada com três Roteadores que usa endereços privados. O exemplo ilustra estas características:

- Encapsulating Security Payload (ESP) - Data Encryption Standard (DES) somente
- Chaves pré-compartilhada
- Redes privadas atrás de cada roteador: 192.168.1.0, 192.168.2.0, e 192.168.3.0
- política do isakmp e configuração do crypto map
- Tráfego de túnel definido com os **comandos access-list e route-map**. Além do que a tradução de endereço de porta (PAT), os mapas de rota podem ser aplicados a uma tradução de endereço da rede estática linear (NAT) no Software Release 12.2(4)T2 e Mais Recente de Cisco IOS®. Para mais informação refira o [NAT - Capacidade para usar mapas de rota com visão geral de características das traduções estáticas](#).

**Nota:** A tecnologia de criptografia está sujeita a controles de exportação. É sua responsabilidade conhecer a lei em relação à exportação de tecnologia de criptografia. [Se você tem alguma dúvida com relação ao controle de exportação, envie um e-mail para export@cisco.com.](#)

## [Pré-requisitos](#)

### [Requisitos](#)

Não existem requisitos específicos para este documento.

## Componentes Utilizados

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

- Cisco IOS Software Release 12.3.(7)T.
- Roteadores Cisco configurados com IPsec.

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:

- [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 roteador3

```

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 no correspondente.
- mostre IPsec crypto sa — Mostra os ajustes usados (IPsec) por SA atuais.

## Troubleshooting

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.

**Nota:** Antes de emitir **comandos debug**, consulte [Informações importantes sobre comandos debug](#).

**Nota:** As seguintes depurações devem estar executando nos dois roteadores de IPSec (peers). Cancelar SA 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 de criptografia atualmente em andamento. As sessões de criptografia terminarem normalmente quando o tempo de sessão para fora. Utilize o comando `show crypto cisco connections` para saber o valor da connection-id.
- **cancele o isakmp cripto** — Cancela a fase 1 SA.
- **cancele o sa cripto** — Cancela a fase 2 SA.

## [Informações Relacionadas](#)

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