

Configurando o roteador para roteador do IPsec, Pre-shared, sobrecarga NAT entre redes privadas

Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenções](#)

[Configurar](#)

[Diagrama de Rede](#)

[Configurações](#)

[Verificar](#)

[Troubleshooting](#)

[Comandos para Troubleshooting](#)

[Informações Relacionadas](#)

Introdução

Esta configuração de exemplo mostra como criptografar um tráfego entre duas redes privadas (10.50.50.x e 10.103.1.x) que usam o IPsec. As redes se conhecem por seus endereços privados.

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 12.3.1a de Cisco IOS®
- Cisco 2691 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](#).

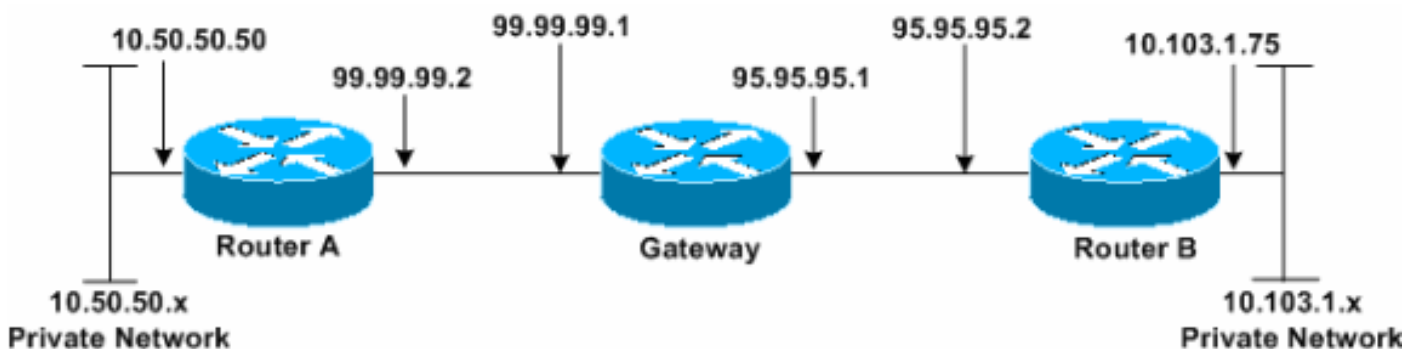
Configurar

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 configuração de rede mostrada neste diagrama.



Configurações

Este documento utiliza estas configurações.

- [Roteador A](#)
- [roteador B](#)

Roteador A

```
Router_A#write terminal
Building configuration...
Current configuration : 1638 bytes
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Router_A
!
boot system flash:c2691-ik9o3s-mz.123-1a.bin
!
ip subnet-zero
!
ip audit notify log
ip audit po max-events 100
no ftp-server write-enable
```

```
!  
crypto isakmp policy 1  
hash md5  
authentication pre-share  
crypto isakmp key cisco123 address 95.95.95.2  
!  
crypto ipsec transform-set rtpset esp-des esp-md5-hmac  
!  
crypto map rtp 1 ipsec-isakmp  
set peer 95.95.95.2  
set transform-set rtpset  
!--- Include the private network to private network  
traffic !--- in the encryption process. match address  
115  
!  
no voice hpi capture buffer  
no voice hpi capture destination  
!  
interface FastEthernet0/0  
ip address 99.99.99.2 255.255.255.0  
ip nat outside  
duplex auto  
speed auto  
crypto map rtp  
!  
interface FastEthernet0/1  
ip address 10.50.50.50 255.255.255.0  
ip nat inside  
duplex auto  
speed auto  
!  
!--- Except the private network traffic from the !---  
Network Address Translation (NAT) process. ip nat inside  
source route-map nonat interface FastEthernet0/0  
overload  
ip http server  
no ip http secure-server  
ip classless  
ip route 0.0.0.0 0.0.0.0 99.99.99.1  
!  
!--- Except the private network traffic from the NAT  
process. access-list 110 deny ip 10.50.50.0 0.0.0.255  
10.103.1.0 0.0.0.255  
access-list 110 permit ip 10.50.50.0 0.0.0.255 any  
!--- Include the private network to private network  
traffic !--- in the encryption process. access-list 115  
permit ip 10.50.50.0 0.0.0.255 10.103.1.0 0.0.0.255  
!  
!--- Except the private network traffic from the NAT  
process. route-map nonat permit 10  
match ip address 110  
!  
dial-peer cor custom  
!  
line con 0  
exec-timeout 0 0  
line aux 0  
line vty 0 4  
login  
!  
end  
  
Router_A#
```

roteador B

```
Router_B#write terminal
Building configuration...
Current configuration : 1394 bytes
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Router_B
!
boot system flash:c2691-ik9o3s-mz.123-1a.bin
!
ip subnet-zero
!
ip audit notify log
ip audit po max-events 100
no ftp-server write-enable
!
crypto isakmp policy 1
hash md5
authentication pre-share
crypto isakmp key cisco123 address 99.99.99.2
!
crypto ipsec transform-set rtpset esp-des esp-md5-hmac
!
crypto map rtp 1 ipsec-isakmp
set peer 99.99.99.2
set transform-set rtpset
!--- Include the private network to private network
traffic !--- in the encryption process. match address
115
!
no voice hpi capture buffer
no voice hpi capture destination
!
interface FastEthernet0/0
ip address 95.95.95.2 255.255.255.0
ip nat outside
duplex auto
speed auto
crypto map rtp
!
interface FastEthernet0/1
ip address 10.103.1.75 255.255.255.0
ip nat inside
duplex auto
speed auto
!
!--- Except the private network traffic from the NAT
process. ip nat inside source route-map nonat interface
FastEthernet0/0 overload
ip http server
no ip http secure-server
ip classless
ip route 0.0.0.0 0.0.0.0 95.95.95.1
!
!--- Except the private network traffic from the NAT
process. access-list 110 deny ip 10.103.1.0 0.0.0.255
10.50.50.0 0.0.0.255
access-list 110 permit ip 10.103.1.0 0.0.0.255 any
!--- Include the private network to private network
```

```
traffic !--- in the encryption process. access-list 115
permit ip 10.103.1.0 0.0.0.255 10.50.50.0 0.0.0.255
!
!--- Except the private network traffic from the NAT
process. route-map nonat permit 10
match ip address 110
!
dial-peer cor custom
!
line con 0
exec-timeout 0 0
line aux 0
line vty 0 4
login
!
end
Router_B#
```

Verificar

No momento, não há procedimento de verificação disponível para esta configuração.

Troubleshooting

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 de depuração, consulte as informações importantes sobre eles.](#)

- **debug crypto ipsec sa** — Indica as negociações de IPSEC de fase 2.
- **debug crypto isakmp sa** — Indica as negociações do Internet Security Association and Key Management Protocol (ISAKMP) da fase 1.
- **motor do debug crypto** — Indica as sessões de criptografia.

Informações Relacionadas

- [Troubleshooting de Segurança de IP - Entendendo e Utilizando Comandos debug](#)
- [Página de suporte do IPSec](#)
- [Suporte Técnico - Cisco Systems](#)