# Configuração de uma Rede Privada para Privada de Túnel IPsec do Roteador com NAT e uma Rede Estática

## Contents



## Introduction

Esta configuração de exemplo mostra como:

- Criptografe o tráfego entre duas redes privadas (10.1.1.x e 172.16.1.x).
- Atribua um endereço IP estático (endereço externo 200.1.1.25) a um dispositivo de rede em 10.1.1.3.

Você usa listas de controle de acesso (ACLs) para dizer ao roteador para não fazer a conversão de endereço de rede (NAT) para o tráfego de rede privada para privada, que é então criptografado e colocado no túnel quando ele sai do roteador. Também há um NAT estático para um servidor interno na rede 10.1.1.x nesta configuração de exemplo. Este exemplo de configuração usa a opção route-map no comando NAT para impedir que ele seja NAT'd se o tráfego para ele também for destinado pelo túnel criptografado.

## 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(14)T
- Dois Cisco 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

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

# Por que a instrução Deny na ACL especifica o tráfego NAT?

Você substitui conceitualmente uma rede por um túnel quando usa o Cisco IOS IPsec ou uma VPN. Você substitui a nuvem da Internet por um túnel IPsec do Cisco IOS que vai de 200.1.1.1 a 100.1.1.1 neste diagrama. Torne essa rede transparente do ponto de vista das duas LANs privadas que estão conectadas pelo túnel. Normalmente, você não quer usar NAT para o tráfego que vai de uma LAN privada para a LAN privada remota por esse motivo. Você deseja ver os pacotes que vêm da rede do Roteador 2 com um endereço IP de origem da rede 10.1.1.0/24 em vez de 200.1.1.1 quando os pacotes chegam à rede interna do Roteador 3.

Consulte a Ordem de Operação do NAT para obter mais informações sobre como configurar um NAT. Este documento mostra que o NAT ocorre antes da verificação de criptografia quando o pacote vai de dentro para fora. É por isso que você deve especificar essas informações na configuração.

```
ip nat inside source list 122 interface Ethernet0/1 overload
```

```
access-list 122 deny ip 10.1.1.0 0.0.0.255 172.16.1.0 0.0.0.255
access-list 122 permit ip 10.1.1.0 0.0.0.255 any
```

**Observação:** também é possível construir o túnel e ainda usar o NAT. Você especifica o tráfego NAT como o "tráfego interessante para IPsec" (conhecido como ACL 101 em outras seções deste documento) neste cenário. Consulte Configurando um Túnel IPsec entre Roteadores com Sub-Redes LAN Duplicadas para obter mais informações sobre como construir um túnel enquanto o NAT está ativo.

# Mas e o NAT estático, por que não posso chegar a esse endereço pelo túnel IPsec?

Essa configuração também inclui um NAT estático de um para um para um servidor em 10.1.1.3. Este é o NAT de 200.1.1.25 para que os usuários da Internet possam acessá-lo. Emita este

comando:

```
ip nat inside source static 10.1.1.3 200.1.1.25
```

Esse NAT estático impede que os usuários da rede 172.16.1.x alcancem 10.1.1.3 através do túnel criptografado. Isso ocorre porque você precisa negar que o tráfego criptografado seja NAT com ACL 122. No entanto, o comando static NAT tem precedência sobre a instrução genérica NAT para todas as conexões de e para 10.1.1.3. A instrução de NAT estático não nega especificamente que o tráfego criptografado também seja de NAT. As respostas de 10.1.1.3 são NAT'd para 200.1.1.25 quando um usuário na rede 172.16.1.x se conecta a 10.1.1.3 e, portanto, não retorna ao túnel criptografado (o NAT acontece antes da criptografia).

Você deve negar que o tráfego criptografado seja NAT'd (mesmo que estaticamente um NAT para um) com um comando **route-map** na instrução de NAT estático.

**Observação:** a opção **route-map** em um NAT estático só é suportada do Cisco IOS Software Release 12.2(4)T e posteriores. Consulte NAT—Habilidade de usar mapas de rota com traduções estáticas para obter informações adicionais.

Você deve emitir esses comandos adicionais para permitir acesso criptografado a 10.1.1.3, o host estaticamente do NAT:

```
ip nat inside source static 10.1.1.3 200.1.1.25 route-map nonat
!
access-list 150 deny   ip host 10.1.1.3 172.16.1.0 0.0.0.255
access-list 150 permit ip host 10.1.1.3 any
!
route-map nonat permit 10
 match ip address 150
```

Essas instruções instruem o roteador a aplicar somente o NAT estático ao tráfego que corresponda à ACL 150. A ACL 150 diz para não aplicar o NAT ao tráfego originado de 10.1.1.3 e destinado pelo túnel criptografado para 172.16.1.x. No entanto, aplique-o a todo o tráfego restante originado de 10.1.1.3 (tráfego baseado na Internet).

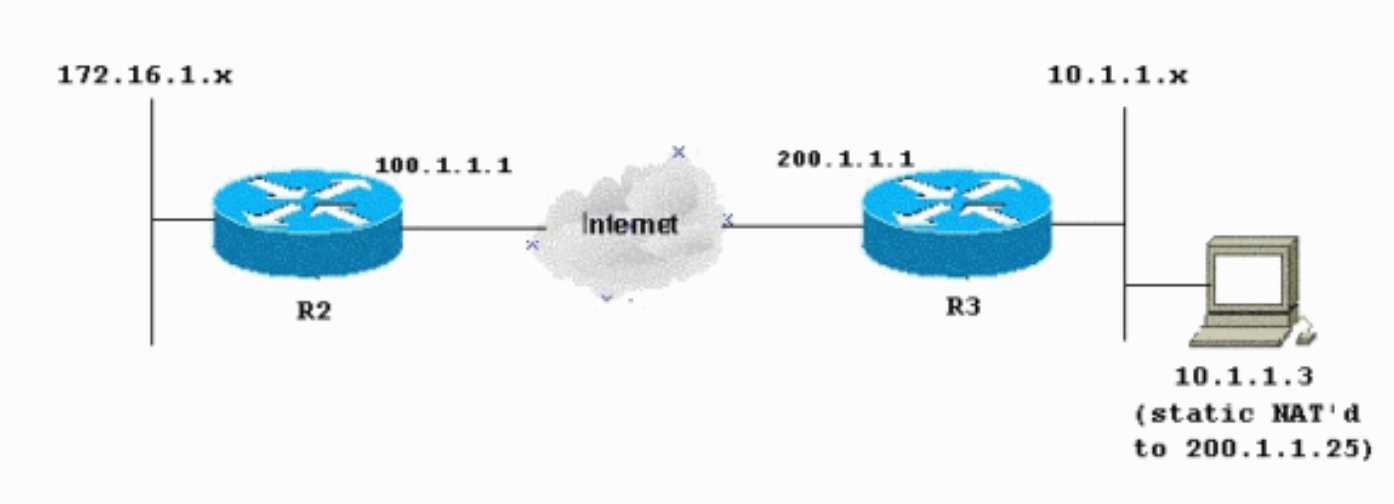
# Configurar

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

Nota:Use a Command Lookup Tool (somente clientes registrados) para obter mais informações sobre os comandos usados neste documento.

## Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:




## Configurações

Este documento utiliza as seguintes configurações:

- Roteador 2
- Roteador 3

**R2 - Configuração do roteador**

```
R2#write terminal
Building configuration...
Current configuration : 1412 bytes
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R2
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
!
resource policy
!
clock timezone EST 0
ip subnet-zero
no ip domain lookup
!
!
crypto isakmp policy 10
 authentication pre-share
!
crypto isakmp key ciscokey address 200.1.1.1
!
!
crypto ipsec transform-set myset esp-3des esp-md5-hmac
!
crypto map myvpn 10 ipsec-isakmp
 set peer 200.1.1.1
 set transform-set myset
```

```
!--- Include the private-network-to-private-network
traffic !--- in the encryption process: match address
101
!
!
!
interface Ethernet0/0
 ip address 172.16.1.1 255.255.255.0
 ip nat inside
 ip virtual-reassembly
!
interface Ethernet1/0
 ip address 100.1.1.1 255.255.255.0
 ip nat outside
 ip virtual-reassembly
 crypto map myvpn
!
ip classless
ip route 0.0.0.0 0.0.0.0 100.1.1.254
!
ip http server
no ip http secure-server
!
!--- Except the private network from the NAT process: ip
nat inside source list 175 interface Ethernet1/0
overload
!
!--- Include the private-network-to-private-network
traffic !--- in the encryption process: access-list 101
permit ip 172.16.1.0 0.0.0.255 10.1.1.0 0.0.0.255
!--- Except the private network from the NAT process:
access-list 175 deny   ip 172.16.1.0 0.0.0.255 10.1.1.0
0.0.0.255
access-list 175 permit ip 172.16.1.0 0.0.0.255 any
!
!
!
control-plane
!
!
line con 0
 exec-timeout 0 0
line aux 0
line vty 0 4
 login
!
end
```

## R3 - Configuração do roteador

```
R3#write terminal
Building configuration...
Current configuration : 1630 bytes
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R3
!
boot-start-marker
boot-end-marker
```

```
!
!
no aaa new-model
!
resource policy
!
clock timezone EST 0
ip subnet-zero
no ip domain lookup
!
crypto isakmp policy 10
 authentication pre-share
crypto isakmp key ciscokey address 100.1.1.1
!
!
crypto ipsec transform-set myset esp-3des esp-md5-hmac
!
crypto map myvpn 10 ipsec-isakmp
 set peer 100.1.1.1
 set transform-set myset
!--- Include the private-network-to-private-network
traffic !--- in the encryption process: match address
101
!
!
!
interface Ethernet0/0
 ip address 10.1.1.1 255.255.255.0
 ip nat inside
 ip virtual-reassembly
!
interface Ethernet1/0
 ip address 200.1.1.1 255.255.255.0
 ip nat outside
 ip virtual-reassembly
 crypto map myvpn
!
!
ip classless
ip route 0.0.0.0 0.0.0.0 200.1.1.254
!
no ip http server
no ip http secure-server
!
!--- Except the private network from the NAT process: ip
nat inside source list 122 interface Ethernet1/0
overload
!--- Except the static-NAT traffic from the NAT process
if destined !--- over the encrypted tunnel: ip nat
inside source static 10.1.1.3 200.1.1.25 route-map nonat
!
access-list 101 permit ip 10.1.1.0 0.0.0.255 172.16.1.0
0.0.0.255
!--- Except the private network from the NAT process:
access-list 122 deny   ip 10.1.1.0 0.0.0.255 172.16.1.0
0.0.0.255
access-list 122 permit ip 10.1.1.0 0.0.0.255 any
!--- Except the static-NAT traffic from the NAT process
if destined !--- over the encrypted tunnel: access-list
150 deny   ip host 10.1.1.3 172.16.1.0 0.0.0.255
access-list 150 permit ip host 10.1.1.3 any
!
route-map nonat permit 10
 match ip address 150
```

```
!
!
!
control-plane
!
!
line con 0
 exec-timeout 0 0
line aux 0
line vty 0 4
 login
!
end
```

# Verificar

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

# Troubleshoot

Use esta seção para resolver problemas de configuração.

Consulte IP Security Troubleshooting - Understanding and Using debug Commands para obter informações adicionais.

## Comandos para Troubleshooting

A Output Interpreter Tool ( somente clientes registrados) (OIT) oferece suporte a determinados comandos show. Use a OIT para exibir uma análise da saída do comando show.

**Nota:Consulte Informações Importantes sobre Comandos de Depuração antes de usar comandos debug.**

- **debug crypto ipsec sa** — Exibe as negociações de IPsec da Fase 2.
- **debug crypto isakmp sa** — Veja as negociações ISAKMP da Fase 1.
- **debug crypto engine** — Exibe as sessões criptografadas.

# Informações Relacionadas

- Negociação IPsec/Protocolos IKE - Cisco Systems
- Suporte Técnico e Documentação - Cisco Systems