# Índice



# Introdução

Esta configuração de exemplo mostra como:

- Cifre um 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 o Access Control Lists (ACLs) para dizer o roteador para não fazer o Network Address Translation (NAT) ao tráfego de rede privada-privada, que então está cifrado e colocado no túnel enquanto sae do roteador. Há igualmente um NAT estático para um server interno na rede 10.1.1.x nesta configuração de exemplo. Esta configuração de exemplo usa a opção do mapa de rotas no comando nat pará-la de ser NAT'd se o tráfego para ele é destinado igualmente sobre o túnel criptografado.

# 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(14)T de Cisco IOS®
- Dois Cisco routers

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

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

# Por que o recusar instrução no ACL especifica o tráfego NAT?

Você substitui conceptualmente uma rede com um túnel quando você usa o Cisco IOS IPsec ou um VPN. Você substitui a nuvem do Internet por um túnel do Cisco IOS IPsec que vá de 200.1.1.1 a 100.1.1.1 neste diagrama. Faça esta rede transparente do ponto de vista das duas LAN privadas que são ligadas junto pelo túnel. Você geralmente não quer usar o NAT para o tráfego que vai de uma LAN privada ao LAN privado remota por este motivo. Você quer ver os pacotes que vêm da rede do roteador2 com um endereço IP de origem da rede 10.1.1.0/24 em vez de 200.1.1.1 quando os pacotes alcançam a rede do roteador interno 3.

Refira o ordem de operação NAT para obter mais informações sobre de como configurar um NAT. Este documento mostra que o NAT ocorre antes da verificação cripto quando o pacote vai do interior à parte externa. Eis porque você deve especificar esta informação na configuração.

```
ip nat inside source list 122 interface Ethernet0/1 overloadaccess-list 122 deny ip 10.1.1.0
0.0.0.255 172.16.1.0 0.0.0.255access-list 122 permit ip 10.1.1.0 0.0.0.255 any
```

**Nota:** É igualmente possível construir o túnel e usar ainda o NAT. Você especifica o tráfego NAT como o “tráfego interessante para o IPsec” (referido como o ACL 101 em outras seções deste documento) nesta encenação. Refira configurar um túnel de IPsec entre o Roteadores com sub-redes LAN duplicadas para obter mais informações sobre de como construir um túnel quando o NAT for ativo.

# Que sobre o NAT estático embora, por que não posso eu obter a esse endereço sobre o túnel de IPsec?

Esta instalação igualmente inclui um NAT linear estático para um server em 10.1.1.3. Este é NAT'd a 200.1.1.25 de modo que os usuários do Internet possam o alcançar. Emita este comando:

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

Este NAT estático impossibilita usuários na rede 172.16.1.x de 10.1.1.3 de alcance através do túnel criptografado. Isto é porque você precisa de negar o tráfego criptografado de ser NAT'd com ACL 122. Contudo, o comando static nat toma a precedência sobre a declaração NAT genérica para todas as conexões a e de 10.1.1.3. A indicação do NAT estático não nega especificamente o tráfego criptografado igualmente de ser NAT'd. As respostas de 10.1.1.3 são NAT'd a 200.1.1.25 quando um usuário na rede 172.16.1.x conecta a 10.1.1.3 e consequentemente não vão para trás sobre o túnel criptografado (o NAT acontece antes da criptografia).

Você deve negar o tráfego criptografado de ser NAT'd (mesmo estaticamente NAT'd linear) com um **comando route-map na** indicação do NAT estático.

**Nota:** A opção do **mapa de rotas em um** NAT estático é apoiada somente do Cisco IOS Software Release 12.2(4)T e Mais Recente. Refira o NAT? Capacidade para usar mapas de rota com traduções estáticas para a informação adicional.

Você deve emitir estes comandos adicionais permitir estaticamente o acesso criptografado a 10.1.1.3, o host do NAT'd:

```
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 0.0.0.255access-list 150 permit ip host 10.1.1.3 any!route-map nonat permit 10 match ip address 150
```

Estas indicações dizem o roteador para aplicar somente o NAT estático para traficar esse os fósforos ACL 150. O ACL 150 diz não aplicar o NAT para traficar originado de 10.1.1.3 e destinado sobre o túnel criptografado a 172.16.1.x. Contudo, aplique-o a todo tráfego restante originado de 10.1.1.3 (tráfego Internet-baseado).

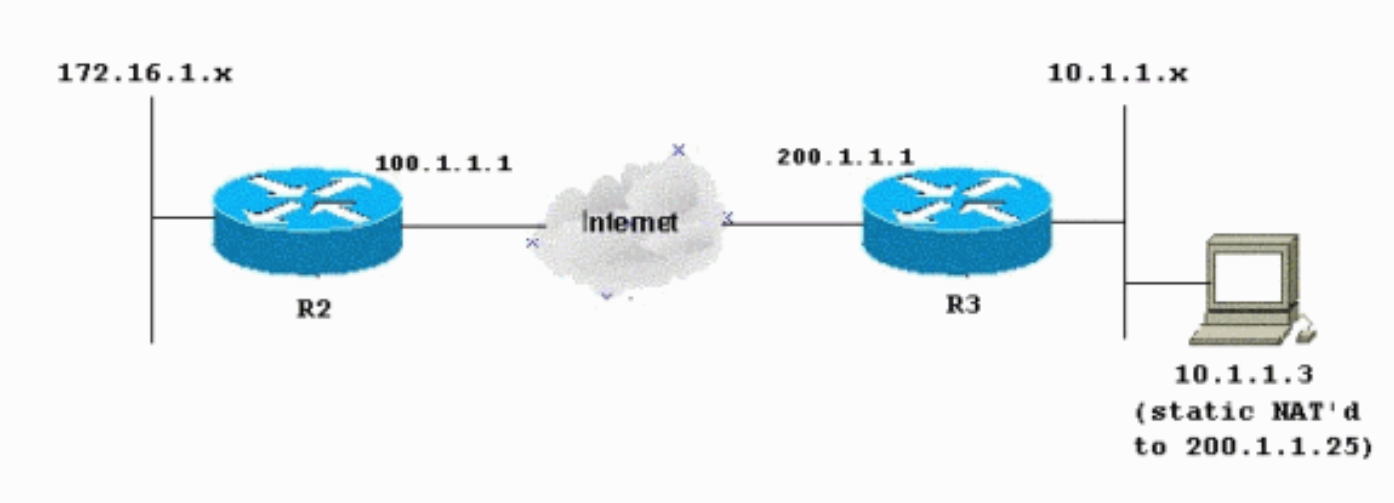
# Configurar

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

**Nota:** Use a ferramenta Command Lookup Tool (apenas para 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 de roteador |
| --- |
| R2#**write terminal**Building configuration...Current configuration : 1412 bytes!version 12.3service |

```
timestamps debug datetime msecservice timestamps log
datetime msecno service password-encryption!hostname
R2!boot-start-markerboot-end-marker!!no aaa new-
model!resource policy!clock timezone EST 0ip subnet-
zerono 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 classlessip route
0.0.0.0 0.0.0.0 100.1.1.254!ip http serverno 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 0.0.0.255access-list 175 permit ip
172.16.1.0 0.0.0.255 any!!!control-plane!!line con 0
exec-timeout 0 0line aux 0line vty 0 4 login!end
```

## R3- configuração de roteador

```
R3#write terminalBuilding configuration...Current
configuration : 1630 bytes!version 12.3service
timestamps debug datetime msecservice timestamps log
datetime msecno service password-encryption!hostname
R3!boot-start-markerboot-end-marker!!no aaa new-
model!resource policy!clock timezone EST 0ip subnet-
zerono ip domain lookup!crypto isakmp policy 10
authentication pre-sharecrypto 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 classlessip
route 0.0.0.0 0.0.0.0 200.1.1.254!no ip http serverno 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 0.0.0.255access-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 0.0.0.255access-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
0line aux 0line vty 0 4 login!end
```

# Verificar

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

# Troubleshooting

Use esta seção para resolver problemas de configuração.

Refira o Troubleshooting de Segurança IP - Compreendendo e usando comandos debug para a informação adicional.

## Comandos para Troubleshooting

A Output Interpreter Tool (apenas para clientes registrados) (OIT) suporta 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**? Indica as negociações de IPSEC de fase 2.
- **debug crypto isakmp sa**? Veja as negociações de ISAKMP de fase 1.
- **motor do debug crypto**? Indica as sessões de criptografia.

# Informações Relacionadas

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