Configuração de um túnel IPSec entre roteadores com sub-redes LAN duplicadas

Índice

Introdução

Este documento fornece um exemplo de rede que simula duas empresas fundidas com o mesmo esquema de endereçamento de IP. Dois roteadores são conectados com um túnel VPN, e as redes atrás de cada roteador são as mesmas. Para que um local acesse hosts no outro local, a Tradução de Endereço de Rede (NAT) é usada nos roteadores para alterar os endereços de origem e de destino para sub-redes diferentes.

Note: Esta configuração não é recomendada como uma instalação permanente porque seria desconcertante de um ponto de vista do Gerenciamento de redes.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

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

- Roteador A: Cisco 3640 Router que executa o Software Release 12.3(4)T de Cisco IOS®
- Roteador B: Cisco 2621 Router que executa o Software Release 12.3(5) de Cisco IOS®

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.

Informações de Apoio

Neste exemplo, quando o host 172.16.1.2 no local A alcança o mesmos host IP-endereçado no local B, conectam a 172.19.1.2 um endereço um pouco do que ao endereço real de 172.16.1.2. Quando o host no local B aos acessos situa A, conecta a 172.18.1.2 um endereço. NAT no roteador A converte qualquer endereço 172.16.x.x para ficar semelhante à entrada de host 172.18.x.x correspondente. O NAT no roteador B muda 172.16.x.x para olhar como 172.19.x.x.

A função cripto em cada roteador cifra o tráfego traduzido através das interfaces serial. Note que o NAT ocorre *antes da* criptografia em um roteador.

Note: Esta configuração permite somente que as duas redes comuniquem-se. Não permite a conectividade de Internet. Você precisa trajetos adicionais aos internet de conectividade aos lugar diferentes dos dois locais; ou seja você precisa de adicionar um outro roteador ou Firewall em cada lado, com as rotas múltiplas configuradas nos anfitriões.

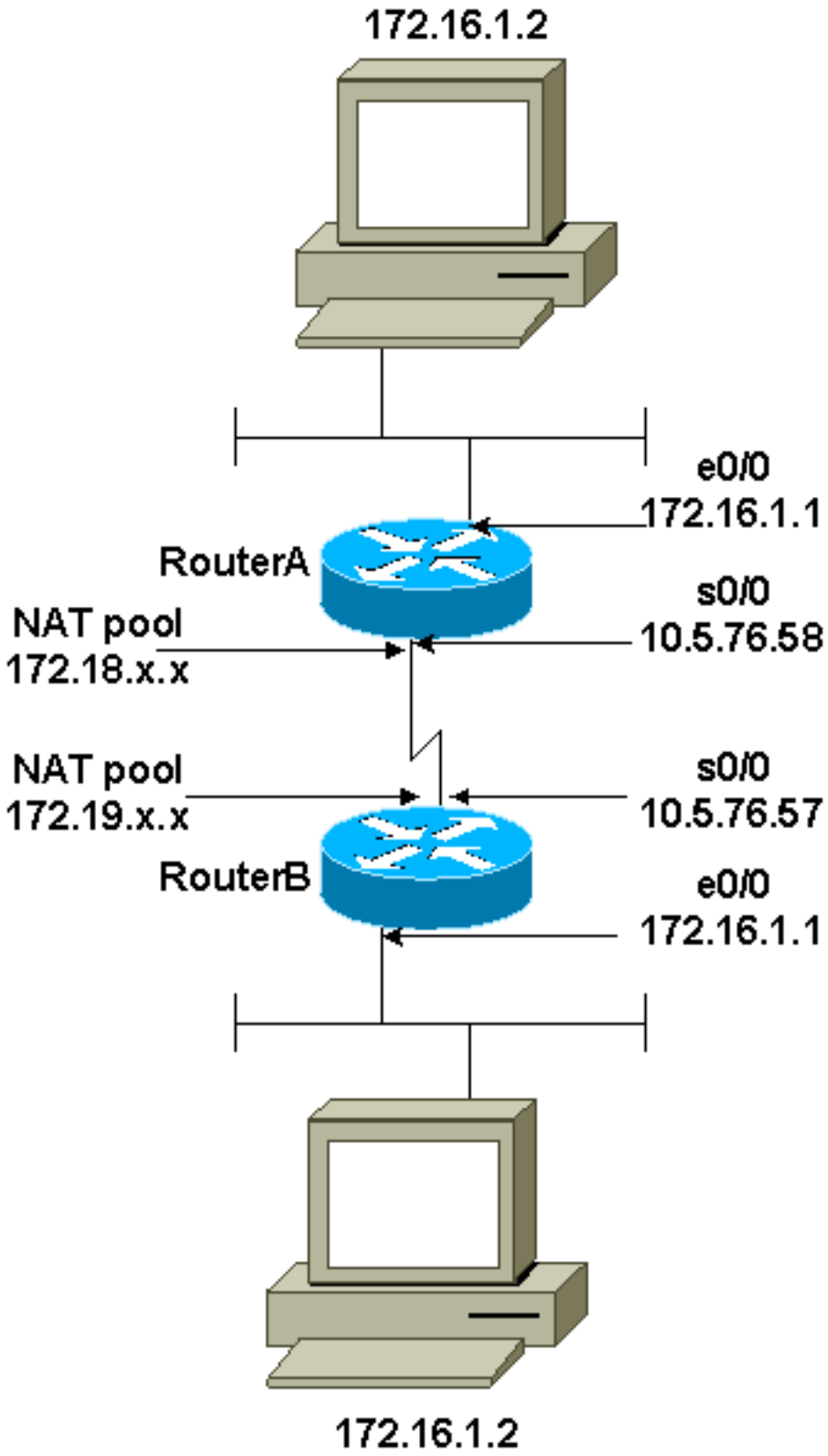
Configurar

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

Note: 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 A
- roteador B

Roteador A

```
Current configuration : 1404 bytes
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname SV3-2
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
ip subnet-zero
!
!
!
!
ip audit notify log
ip audit po max-events 100
ip ssh break-string
no ftp-server write-enable
!
!
!--- These are the Internet Key Exchange (IKE)
parameters. crypto isakmp policy 10
 encr 3des
 hash md5
 authentication pre-share
crypto isakmp key cisco123 address 10.5.76.57
!
!--- These are the IPSec parameters. crypto ipsec
transform-set myset1 esp-3des esp-md5-hmac
!
!
crypto map mymap 10 ipsec-isakmp
 set peer 10.5.76.57
 set transform-set myset1
 !--- Encrypt traffic to the other side. match address
100
!
!
!
interface Serial0/0
 description Interface to Internet
 ip address 10.5.76.58 255.255.0.0
 ip nat outside
 clockrate 128000
 crypto map mymap
!
interface Ethernet0/0
 ip address 172.16.1.1 255.255.255.0
 no ip directed-broadcast
 ip nat inside
 half-duplex
!
!
!--- This is the NAT traffic. ip nat inside source
static network 172.16.0.0 172.18.0.0 /16 no-alias
ip http server
no ip http secure-server
ip classless
ip route 0.0.0.0 0.0.0.0 Serial0/0
```

```
!
!--- Encrypt traffic to the other side. access-list 100
permit ip 172.18.0.0 0.0.255.255 172.19.0.0 0.0.255.255
!
control-plane
!
!
line con 0
line aux 0
line vty 0 4
!
!
end
```

roteador B

```
Current configuration : 1255 bytes
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname SV3-15
!
boot-start-marker
boot-end-marker
!
!
memory-size iomem 15
no aaa new-model
ip subnet-zero
!
!
!
ip audit notify log
ip audit po max-events 100
!
!--- These are the IKE parameters. crypto isakmp policy
10
 encr 3des
 hash md5
 authentication pre-share
crypto isakmp key cisco123 address 10.5.76.58
!
!--- These are the IPSec parameters. crypto ipsec
transform-set myset1 esp-3des esp-md5-hmac
!
crypto map mymap 10 ipsec-isakmp
 set peer 10.5.76.58
 set transform-set myset1
!--- Encrypt traffic to the other side.  match address
100
!
!
interface FastEthernet0/0
 ip address 172.16.1.1 255.255.255.0
 ip nat inside
 duplex auto
 speed auto
!
interface Serial0/0
 description Interface to Internet
```

```
 ip address 10.5.76.57 255.255.0.0
 ip nat outside
 crypto map mymap
!
!--- This is the NAT traffic. ip nat inside source
static network 172.16.0.0 172.19.0.0 /16 no-alias
ip http server
no ip http secure-server
ip classless
ip route 0.0.0.0 0.0.0.0 Serial0/0
!
!--- Encrypt traffic to the other side. access-list 100
permit ip 172.19.0.0 0.0.255.255 172.18.0.0 0.0.255.255
!
!
line con 0
line aux 0
line vty 0 4
!
!
!
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 ipsec sa – Mostra as associações de segurança da fase 2.
- show crypto isakmp sa - Mostra as associações de segurança da fase 1.
- **mostre a IP a tradução nat** — Mostra as traduções de NAT atual no uso.

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.

Note: Antes de emitir comandos de depuração, consulte as informações importantes sobre eles.

- **IPsec do debug crypto** — Mostra as negociações de IPSEC de fase 2.
- **isakmp do debug crypto** — Mostra as negociações do Internet Security Association and Key Management Protocol (ISAKMP) da fase 1.
- **motor do debug crypto** — Mostra o tráfego que é cifrado.

Informações Relacionadas

- Página de suporte do IPSec
- Configurando a segurança da rede IPSec
- Configurando o protocolo de segurança do intercâmbio chave de Internet
- Suporte Técnico - Cisco Systems