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

Contents

Introduction

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.

Observação: essa configuração não é recomendada como uma configuração permanente porque seria confusa do ponto de vista do gerenciamento de rede.

Prerequisites

Requirements

Não existem requisitos específicos para este documento.

Componentes Utilizados

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

- Router A: Roteador Cisco 3640 executando o software Cisco IOS® versão 12.3(4)T
- Router B: Roteador Cisco 2621 executando o software Cisco IOS® versão 12.3(5)

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

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 Site A acessa o mesmo host com endereço IP no Site B, ele se conecta a um endereço 172.19.1.2 em vez do endereço real 172.16.1.2. Quando o host no Site B acessa o Site A, ele se conecta a um endereço 172.18.1.2. 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 altera 172.16.x.x para parecer com 172.19.x.x.

A função de criptografia em cada roteador criptografa o tráfego traduzido através das interfaces seriais. Observe que o NAT ocorre *antes da* criptografia em um roteador.

Observação: essa configuração permite que as duas redes se comuniquem apenas. Não permite a conectividade com a Internet. Você precisa de caminhos adicionais para a Internet para se conectar a locais diferentes dos dois locais; em outras palavras, você precisa adicionar outro roteador ou firewall em cada lado, com várias rotas configuradas nos hosts.

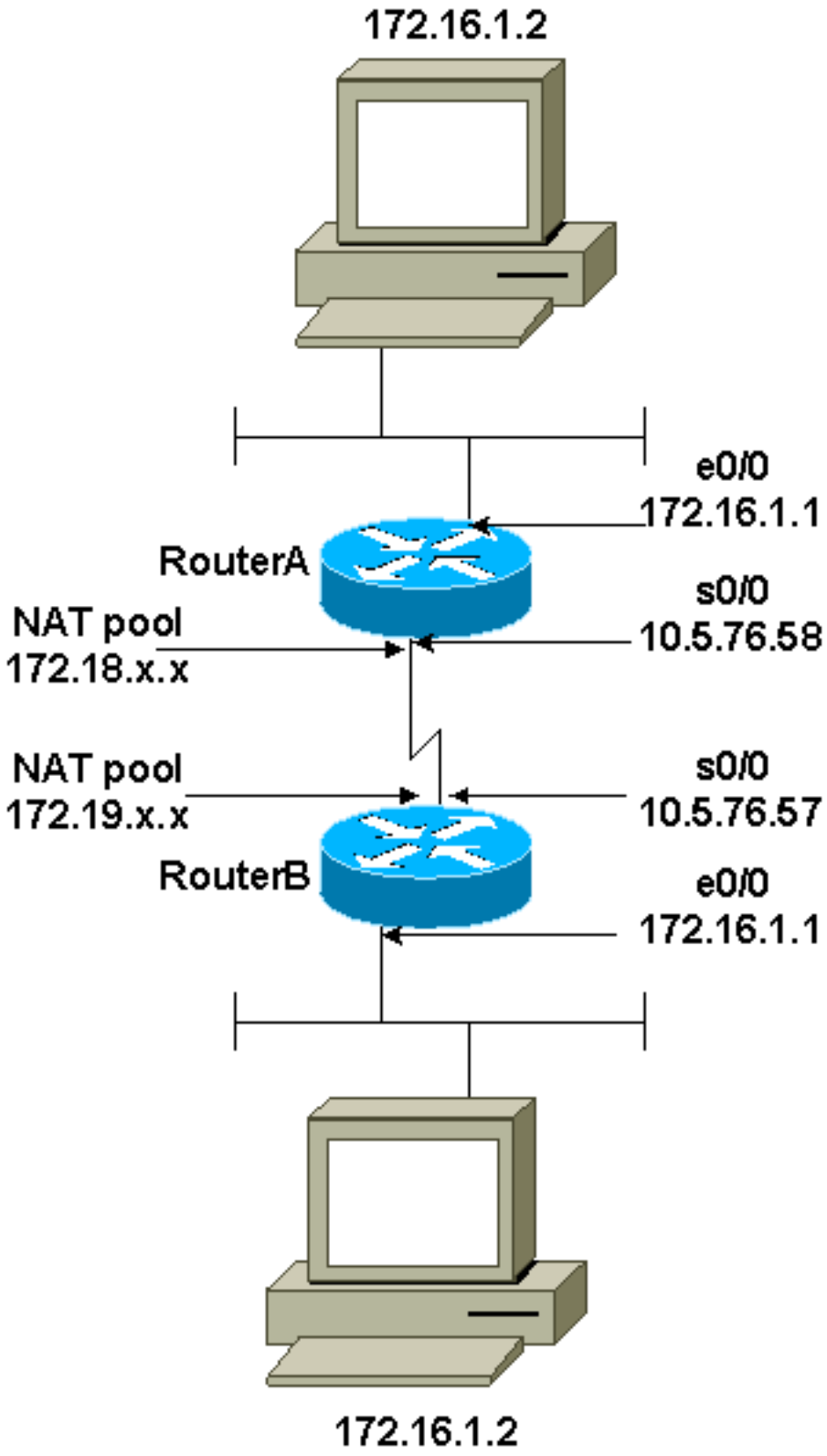
Configurar

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

Observação: para encontrar informações adicionais sobre os comandos usados neste documento, use a ferramenta Command Lookup Tool (somente clientes registrados).

Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:



Configurações

Este documento utiliza as seguintes configurações:

- Router A
- Router B

Router 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
```

Router 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.
- **show ip nat translation** —Mostra as conversões atuais de NAT em uso.

Troubleshoot

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.

Observação: antes de inserir o comando **debug**, consulte Informações importantes sobre os comandos debug.

- **debug crypto ipsec** —Mostra as negociações de IPSec da fase 2.
- **debug crypto isakmp** — Mostra as negociações de Internet Security Association and Key Management Protocol (ISAKMP) da fase 1.
- **debug crypto engine** —Mostra o tráfego que está criptografado.

Informações Relacionadas

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