

# Configuración de un túnel IPSec entre routers con subredes LAN duplicadas.

## Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Convenciones](#)

[Antecedentes](#)

[Configurar](#)

[Diagrama de la red](#)

[Configuraciones](#)

[Verificación](#)

[Troubleshoot](#)

[Comandos para resolución de problemas](#)

[Información Relacionada](#)

## Introducción

Este documento proporciona un ejemplo de conexión en red que simula dos compañías en proceso de fusión con el mismo esquema de direccionamiento de IP. Dos routers están conectados con un túnel VPN, y las redes detrás de cada router son las mismas. Para que un sitio acceda a los hosts del otro sitio, la Traducción de Dirección de Red (NAT) se utiliza en los routers para cambiar las direcciones de origen y destino a subredes diferentes.

**Nota:** Esta configuración no se recomienda como configuración permanente porque sería confusa desde el punto de vista de la administración de la red.

## Prerequisites

### Requirements

No hay requisitos específicos para este documento.

### Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Router A: Router Cisco 3640 que ejecuta Cisco IOS® Software Release 12.3(4)T

- Router B: Router Cisco 2621 que ejecuta Cisco IOS® Software Release 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.

## Convenciones

Para obtener más información sobre las convenciones del documento, consulte [Convenciones de Consejos Técnicos de Cisco](#).

## Antecedentes

En este ejemplo, cuando el host 172.16.1.2 en el Sitio A accede al mismo host con dirección IP en el Sitio B, se conecta a una dirección 172.19.1.2 en lugar de a la dirección real 172.16.1.2. Cuando el host en el Sitio B accede al Sitio A, se conecta a una dirección 172.18.1.2. El NAT en el Router A traduce cualquier dirección 172.16.x.x para que se vea como la entrada de host 172.18.x.x correspondiente. NAT en el Router B cambia 172.16.x.x a 172.19.x.x.

La función crypto en cada router cifra el tráfico traducido a través de las interfaces seriales. Tenga en cuenta que la NAT se produce *antes del* cifrado en un router.

**Nota:** Esta configuración sólo permite que las dos redes se comuniquen. No permite la conectividad a Internet. Necesita rutas de acceso adicionales a Internet para la conectividad a ubicaciones distintas de los dos sitios; en otras palabras, debe agregar otro router o firewall en cada lado, con varias rutas configuradas en los hosts.

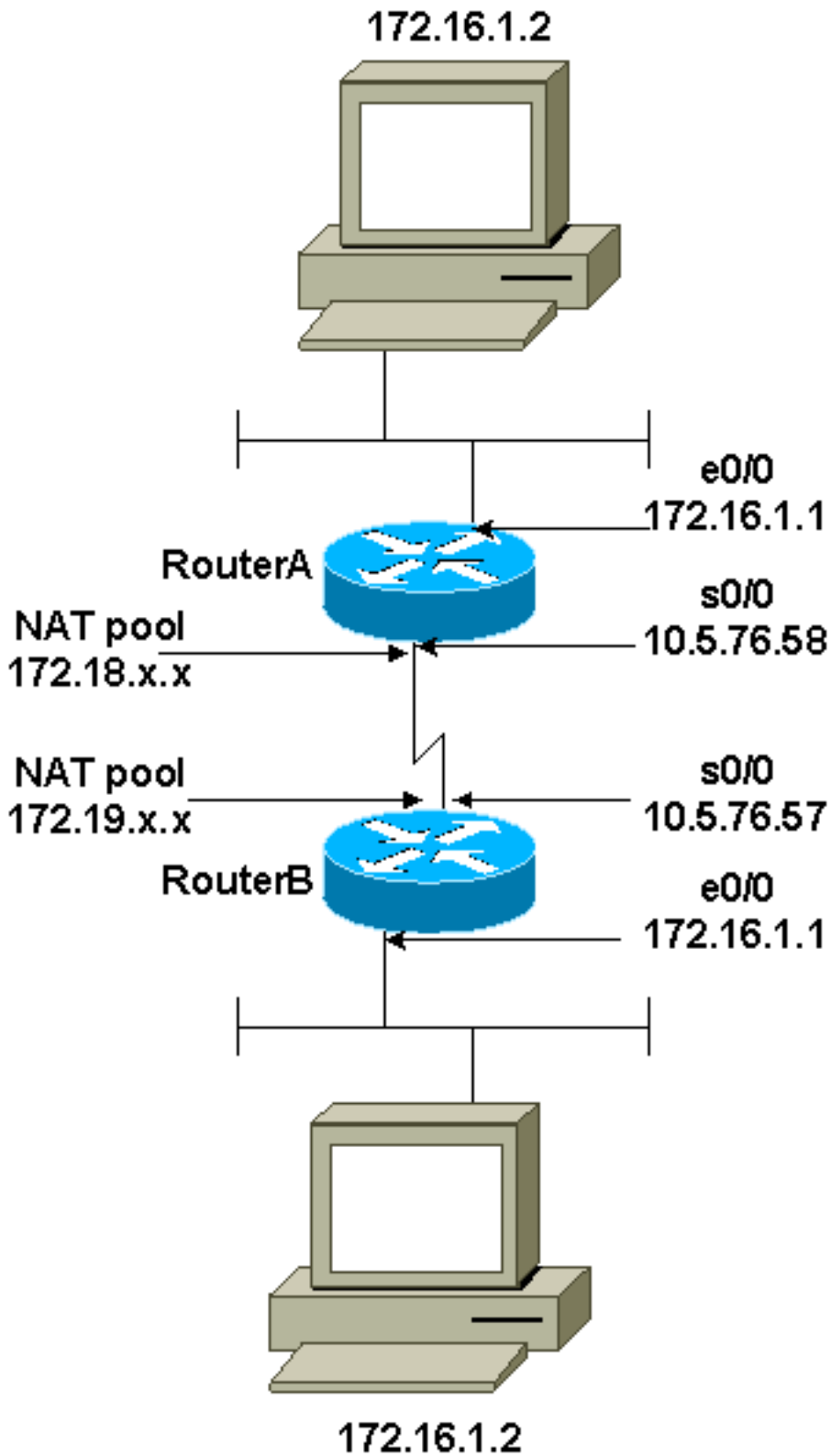
## Configurar

En esta sección encontrará la información para configurar las funciones descritas en este documento.

**Nota:** Para encontrar información adicional sobre los comandos usados en este documento, utilice la [Command Lookup Tool](#) ([sólo](#) clientes registrados) .

## Diagrama de la red

En este documento, se utiliza esta configuración de red:



## Configuraciones

En este documento, se utilizan estas configuraciones:

- [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
```

## Verificación

En esta sección encontrará información que puede utilizar para confirmar que su configuración esté funcionando correctamente.

La herramienta [Output Interpreter](#) (sólo para clientes registrados) permite utilizar algunos comandos “show” y ver un análisis del resultado de estos comandos.

- **show crypto ipsec sa:** muestra las asociaciones de seguridad de la fase 2.
- **show crypto isakmp sa** — Muestra las asociaciones de seguridad de la fase 1.
- **show ip nat translation:** muestra las traducciones NAT actuales en uso.

## Troubleshoot

En esta sección encontrará información que puede utilizar para solucionar problemas de configuración.

### Comandos para resolución de problemas

La herramienta [Output Interpreter](#) (sólo para clientes registrados) permite utilizar algunos comandos “show” y ver un análisis del resultado de estos comandos.

**Nota:** Antes de ejecutar un comando **debug**, consulte [Información Importante sobre Comandos Debug](#).

- **depuración crypto ipsec** — Muestra los IPSec Negotiations de la Fase 2.
- **debug crypto isakmp** — muestra las negociaciones de fase 1 del protocolo Asociación de seguridad en Internet y administración de claves (ISAKMP).
- **debug crypto engine** — muestra el tráfico codificado.

## Información Relacionada

- [Página de soporte de IPSec](#)
- [Configuración de seguridad de red IPSec](#)
- [Configuración del protocolo de seguridad de intercambio de claves de Internet](#)
- [Soporte Técnico - Cisco Systems](#)