Configuración de una Red Privada a Privada del Túnel IPsec del Router con NAT y una Red Estática

Contenido

[Introducción](#)
[Prerequisites](#)
[Requirements](#)
[Componentes Utilizados](#)
[Convenciones](#)
[¿Por qué la instrucción Deny en la ACL especifica el tráfico NAT?](#)
[Pero, ¿por qué no puedo llegar a esa dirección a través del túnel IPsec?](#)
[Configurar](#)
[Diagrama de la red](#)
[Configuraciones](#)
[Verificación](#)
[Troubleshoot](#)
[Comandos para resolución de problemas](#)
[Información Relacionada](#)

Introducción

Esta configuración de ejemplo muestra cómo:

- Cifre el tráfico entre dos redes privadas (10.1.1.x y 172.16.1.x).
- Asigne una dirección IP estática (dirección externa 200.1.1.25) a un dispositivo de red en 10.1.1.3.

Las listas de control de acceso (ACL) se utilizan para indicar al router que no realice la traducción de direcciones de red (NAT) al tráfico de red privado a privado, que se cifra y se coloca en el túnel cuando sale del router. También hay una NAT estática para un servidor interno en la red 10.1.1.x en esta configuración de ejemplo. Esta configuración de ejemplo utiliza la opción route-map en el comando NAT para evitar que se convierta en NATd si el tráfico para él también está destinado a través del túnel cifrado.

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.

- Versión 12.3(14)T del software del IOS® de Cisco
- 'Dos routers de Cisco'

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

Consulte Convenciones de Consejos TécnicosCisco para obtener más información sobre las convenciones del documento.

¿Por qué la instrucción Deny en la ACL especifica el tráfico NAT?

Conceptualmente, reemplaza una red por un túnel cuando utiliza Cisco IOS IPsec o una VPN. En este diagrama, reemplaza la nube de Internet por un túnel IPsec de Cisco IOS que va de 200.1.1.1 a 100.1.1.1. Haga que esta red sea transparente desde el punto de vista de las dos LAN privadas que están conectadas por el túnel. Por este motivo, no suele querer utilizar NAT para el tráfico que va de una LAN privada a la LAN privada remota. Desea ver los paquetes que vienen de la red del Router 2 con una dirección IP de origen de la red 10.1.1.0/24 en lugar de 200.1.1.1 cuando los paquetes alcanzan la red interna del Router 3.

Consulte Orden de Funcionamiento de NAT para obtener más información sobre cómo configurar una NAT. Este documento muestra que la NAT tiene lugar antes de la verificación de criptografía cuando el paquete va del interior al exterior. Esta es la razón por la que debe especificar esta información en la configuración.

```
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
```

Nota: También es posible construir el túnel y seguir utilizando NAT. El tráfico NAT se especifica como el "tráfico interesante para IPSec" (denominado ACL 101 en otras secciones de este documento) en este escenario. Consulte Configuración de un Túnel IPSec entre Routers con Subredes LAN Duplicadas para obtener más información sobre cómo construir un túnel mientras NAT está activo.

Pero, ¿por qué no puedo llegar a esa dirección a través del túnel IPsec?

Esta configuración también incluye una NAT estática uno a uno para un servidor en 10.1.1.3. Esto es NAT'd a 200.1.1.25 para que los usuarios de Internet puedan acceder a él. Ejecutar este comando:

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

Esta NAT estática impide que los usuarios de la red 172.16.1.x alcancen 10.1.1.3 a través del túnel cifrado. Esto se debe a que debe impedir que el tráfico cifrado sea NAT'd con ACL 122. Sin embargo, el comando static NAT tiene precedencia sobre la sentencia NAT genérica para todas las conexiones hacia y desde 10.1.1.3. La sentencia NAT estática no niega específicamente que el tráfico cifrado también sea NAT'd. Las respuestas de 10.1.1.3 son NAT'd a 200.1.1.25 cuando un usuario en la red 172.16.1.x se conecta a 10.1.1.3 y, por lo tanto, no regresa por el túnel cifrado (la NAT se produce antes del cifrado).

Debe negar que el tráfico cifrado sea NAT'd (incluso NAT'd estáticamente uno a uno) con un comando **route-map** en la sentencia NAT estática.

Nota: La opción **route-map** en una NAT estática sólo se soporta desde la versión 12.2(4)T y posteriores del software del IOS de Cisco. Refiérase a NAT: Capacidad de Utilizar Mapas de Ruta con Traducciones Estáticas para obtener información adicional.

Debe ejecutar estos comandos adicionales para permitir el acceso cifrado a 10.1.1.3, el host NAT'd estáticamente:

```
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
```

Estas declaraciones indican al router que aplique solamente la NAT estática al tráfico que coincide con la ACL 150. La ACL 150 indica que no se debe aplicar la NAT al tráfico originado desde 10.1.1.3 y destinado a través del túnel cifrado a 172.16.1.x. Sin embargo, aplíquelo al resto del tráfico originado en 10.1.1.3 (tráfico basado en Internet).

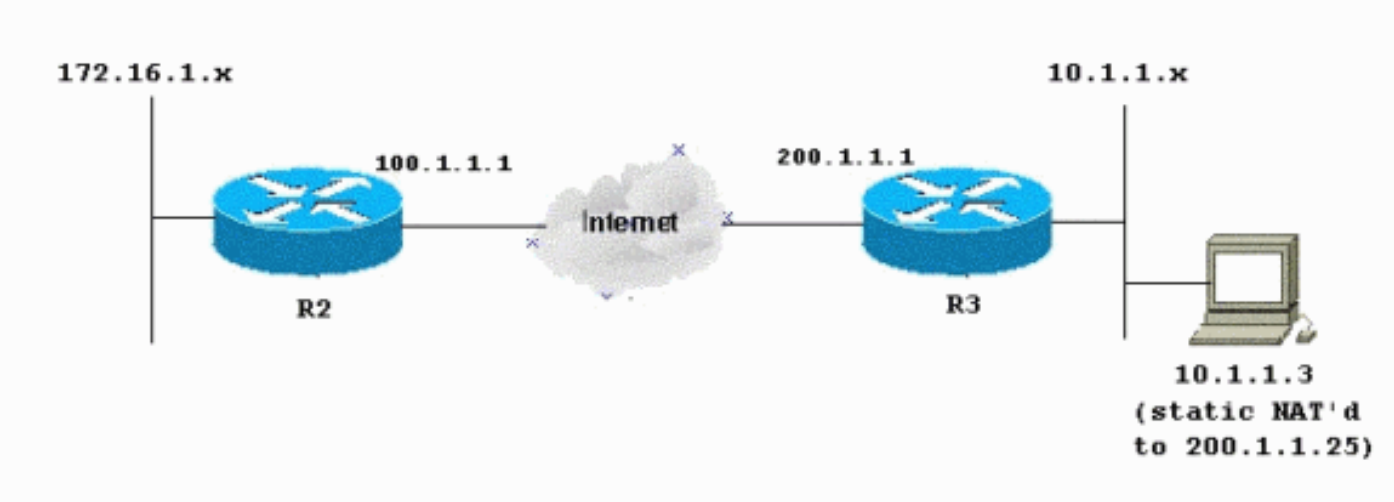
Configurar

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

Nota: Use la Command Lookup Tool (sólo clientes registrados) para obtener más información sobre los comandos utilizados en este documento.

Diagrama de la red

En este documento, se utiliza esta configuración de red:



Configuraciones

En este documento, se utilizan estas configuraciones:

- Router 2
- Router 3

R2: Configuración del router

```
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 - Configuración del router

```
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
```

Verificación

Actualmente, no hay un procedimiento de verificación disponible para esta configuración.

Troubleshoot

Use esta sección para resolver problemas de configuración.

Refiérase a Troubleshooting de Seguridad IP - Comprensión y Uso de los Comandos debug para obtener información adicional.

Comandos para resolución de problemas

La herramienta Output Interpreter Tool (clientes registrados solamente) (OIT) soporta ciertos comandos show. Utilice la OIT para ver un análisis del resultado del comando show.

Nota: Consulte Información Importante sobre Comandos Debug antes de utilizar los comandos **debug**.

- **debug crypto ipsec sa**: muestra las negociaciones IPSec de la Fase 2.
- **debug crypto isakmp sa**: vea las negociaciones ISAKMP de la Fase 1.
- **debug crypto engine**: muestra las sesiones cifradas.

Información Relacionada

- Negociación IPsec/Protocolos IKE - Cisco Systems
- Soporte Técnico y Documentación - Cisco Systems