Configurando a túnel IPSec de red privada a privada del router con el NAT y los parásitos atmosféricos

Contenido

Introducción

Esta configuración de ejemplo muestra cómo:

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

Usted utiliza el Listas de control de acceso (ACL) para decir al router no hacer el Network Address Translation (NAT) al tráfico de red de privada a privada, que después se cifra y se pone en el túnel mientras que sale del router. Hay también un NAT estático para un servidor interior en la red 10.1.1.x en esta configuración de muestra. Esta configuración de muestra utiliza la opción del route-map en el comando nat de pararla de ser NAT'd si el tráfico para él también se destina sobre el túnel encriptado.

prerrequisitos

Requisitos

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.

- Software Release 12.3(14)T de Cisco IOS®
- 'Dos routers de Cisco'

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Convenciones

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

¿Por qué Enunciado de negación en el ACL especifica el tráfico NAT?

Usted substituye conceptual una red por un túnel cuando usted utiliza el Cisco IOS IPsec o un VPN. Usted substituye la nube de Internet por un túnel del Cisco IOS IPsec que vaya de 200.1.1.1 a 100.1.1.1 en este diagrama. Haga esta red transparente desde el punto de vista de los dos LAN privados que son conectados juntos por el túnel. Usted no quiere generalmente utilizar el NAT para el tráfico que va a partir de un LAN privado al LAN privado remoto por este motivo. Usted quiere ver los paquetes que vienen de la red del router2 con una dirección IP de origen de la red 10.1.1.0/24 en vez de 200.1.1.1 cuando los paquetes alcanzan la red del router interno 3.

Refiera al Orden NAT de funcionamiento para más información sobre cómo configurar un NAT. Este documento muestra que el NAT ocurre antes del control crypto cuando el paquete va desde adentro al exterior. Esta es la razón por la cual usted 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: Es también posible construir el túnel y todavía utilizar el NAT. Usted especifica el tráfico NAT como el "tráfico interesante para el IPSec" (referido como ACL 101 en otras secciones de esto documento) en este escenario. Refiera a configurar un túnel IPsec entre el Routers con las subredes LAN duplicadas para más información sobre cómo construir un túnel mientras que el NAT es activo.

¿Qué sobre el NAT estático sin embargo, por qué no puedo conseguir a ese direccionamiento sobre el túnel IPsec?

Esta configuración también incluye un NAT uno por estático para un servidor en 10.1.1.3. Éste es NAT'd a 200.1.1.25 de modo que los usuarios de Internet puedan accederlo. Ejecutar este

comando:

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

Este NAT estático impide a los usuarios en la red 172.16.1.x de 10.1.1.3 que alcanza vía el túnel encriptado. Esto es porque usted necesita negar el tráfico encriptado de ser NAT'd con el ACL 122. Sin embargo, el comando static nat toma la precedencia sobre la sentencia NAT genérica para todas las conexiones a y desde 10.1.1.3. La declaración NAT estática no niega específicamente el tráfico encriptado también de ser NAT'd. Las contestaciones de 10.1.1.3 son NAT'd a 200.1.1.25 cuando un usuario en la red 172.16.1.x conecta con 10.1.1.3 y por lo tanto no pasan detrás el túnel encriptado (el NAT sucede antes del cifrado).

Usted debe negar el tráfico encriptado de ser NAT'd (incluso estáticamente NAT'd uno por) con un **comando route-map** en la declaración NAT estática.

Nota: La opción del **route-map** en un NAT estático se soporta solamente del Cisco IOS Software Release 12.2(4)T y Posterior. Refiera al NAT — Capacidad de utilizar el Route Maps con las traducciones estáticas para la información adicional.

Usted debe publicar estos comandos adicionales de permitir el acceso encriptado a 10.1.1.3, estáticamente el host del 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 0.0.0.255
access-list 150 permit ip host 10.1.1.3 any
!
route-map nonat permit 10
 match ip address 150
```

Estas declaraciones dicen al router aplicar solamente el NAT estático para traficar que las coincidencias ACL 150. El ACL 150 dice para no aplicar el NAT para traficar originado de 10.1.1.3 y destinado sobre el túnel encriptado a 172.16.1.x. Sin embargo, apliqúelo al resto del tráfico originado de 10.1.1.3 (tráfico Internet-basado).

Configurar

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

Nota: Use la herramienta Command Lookup Tool (clientes registrados solamente) para encontrar más información sobre los comandos usados 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.

Troubleshooting

Use esta sección para resolver problemas de configuración.

Refiera al Troubleshooting de IP Security - Entendiendo y con los comandos debug para la 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 de Debug antes de usar un **comando debug**.

- **debug crypto ipsec sa** — Visualiza los IPSec Negotiations de la fase 2.
- **debug crypto isakmp sa** — Vea negociaciones ISAKMP de la fase 1.
- **motor del debug crypto** — Visualiza a las sesiones encriptadas.

Información Relacionada

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