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

Contenido

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 de un punto de vista de la Administración de redes.

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.

- Router A: Cisco 3640 Router que funciona con el Software Release 12.3(4)T de Cisco IOS®

- Router B: Cisco 2621 Router que funciona con el Software Release 12.3(5) de Cisco IOS®

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

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 el mismo host direccionado por IP en el sitio B, conecta con 172.19.1.2 un direccionamiento bastante que con el direccionamiento real de 172.16.1.2. Cuando el host en el sitio B a los accesos localiza A, conecta con 172.18.1.2 un direccionamiento. 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. El NAT en el router B cambia 172.16.x.x para parecer 172.19.x.x.

La función crypto en cada router cifra el tráfico traducido a través de las interfaces seriales. Observe que el NAT ocurre *antes del* cifrado en un router.

Nota: Esta configuración permite solamente que las dos redes comuniquen. No permite la conectividad a Internet. Usted necesita las trayectorias adicionales al Internet para la conectividad a las ubicaciones con excepción de los dos sitios; es decir usted necesita agregar otro router o Firewall en cada lado, con las rutas múltiples configuradas en los host.

Configurar

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

Nota: Para obtener información adicional sobre los comandos que se utilizan en este documento, use la Command Lookup Tool (solo para 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.
- **muestre a IP la traducción nacional** — Muestra las Traducciones NAT actuales funcionando.

Troubleshooting

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 de depuración, consulte Información importante sobre comandos de depuración.

- 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