Een IPSec-tunnel configureren tussen routers met dubbele LAN-subnetten

Inhoud

Inleiding

Dit document biedt een netwerkvoorbeeld dat twee fuserende ondernemingen met dezelfde IP-adresseringsregeling simuleert. Twee routers worden aangesloten met een VPN-tunnel en de netwerken achter elke router zijn hetzelfde. Voor één site om hosts op de andere site te bereiken, wordt Network Address Translation (NAT) op de routers gebruikt om zowel de bron- als de doeladressen aan verschillende subnetwerken te wijzigen.

Opmerking: Deze configuratie wordt niet aanbevolen als een permanente installatie, omdat de configuratie verwarrend is vanuit een netwerkbeheerstandpunt.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- router A: Cisco 3640 router met Cisco IOS®-softwarerelease 12.3(4)T
- router B: Cisco 2621 router met Cisco IOS®-softwarerelease 12.3(5)S

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Conventies

Raadpleeg voor meer informatie over documentconventies de technische Tips van Cisco.

Achtergrondinformatie

In dit voorbeeld, wanneer host 172.16.1.2 op Site A toegang heeft tot dezelfde IP-adresserende host op Site B, sluit deze zich aan op een 172.19.1.2-adres in plaats van op het werkelijk 172.16.1.2-adres. Wanneer de host op Site B toegang heeft tot Site A, sluit hij zich aan op een 172.18.1.2-adres. NAT op router A vertaalt elk 172.16.x.x adres om er als de bijbehorende 172.18.x.x host-ingang uit te zien. NAT op router B verandert 172.16.x.x om er als 172.19.x.x uit te zien.

De crypto functie op elke router versleutel het vertaalde verkeer over de seriële interfaces. Merk op dat NAT *vóór* encryptie op een router voorkomt.

Opmerking: Deze configuratie stelt alleen de twee netwerken in staat te communiceren. Het maakt internetconnectiviteit onmogelijk. U hebt extra paden naar het internet nodig voor connectiviteit op andere locaties dan de twee sites; met andere woorden , u moet een andere router of firewall aan elke kant toevoegen , met meerdere routes die op de hosts zijn geconfigureerd .

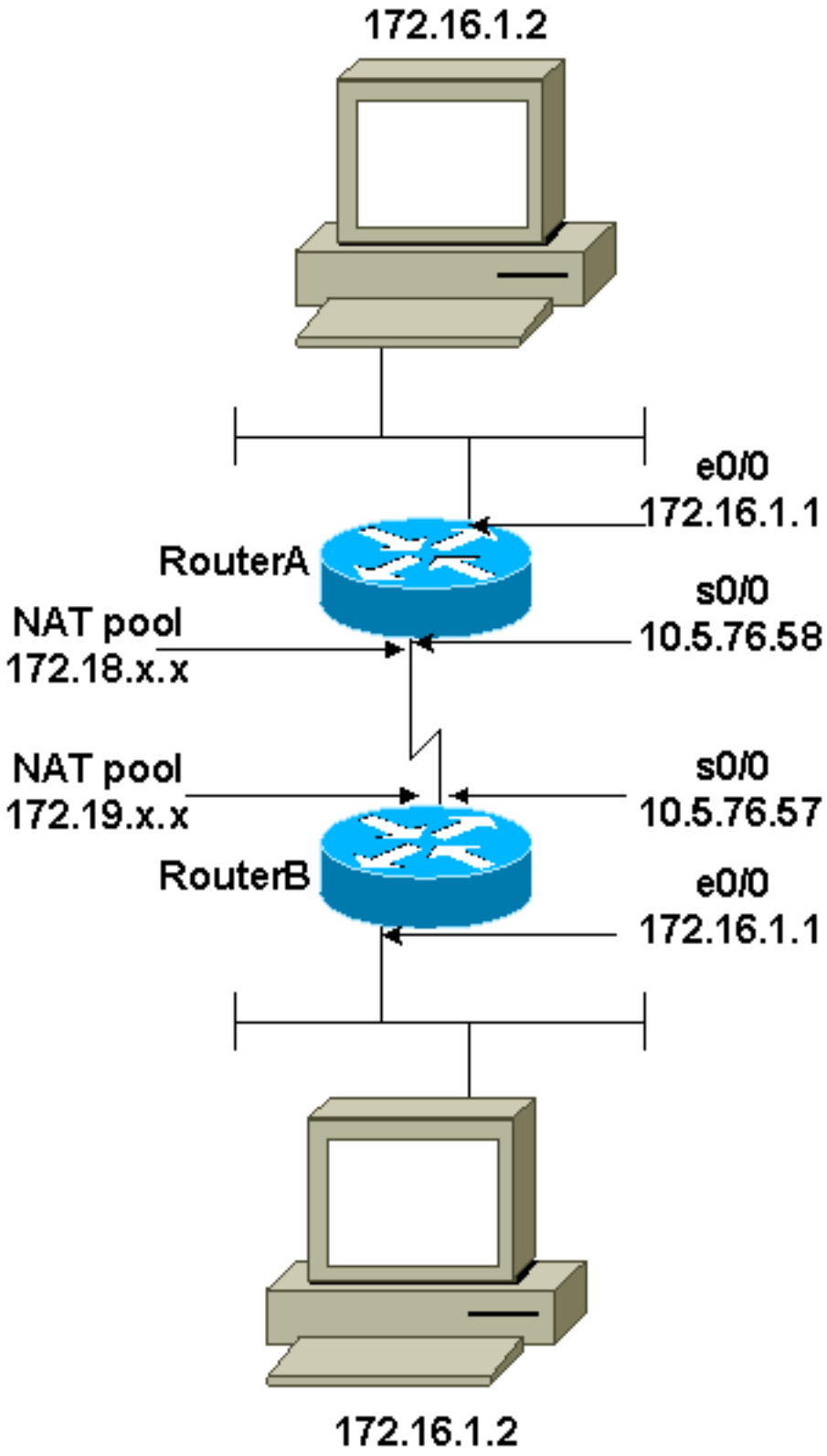
Configureren

Deze sectie bevat informatie over het configureren van de functies die in dit document worden beschreven.

N.B.: Als u aanvullende informatie wilt vinden over de opdrachten in dit document, gebruikt u het Opdrachtplanningprogramma (alleen geregistreerd klanten).

Netwerkdiagram

Het netwerk in dit document is als volgt opgebouwd:



Configuraties

Dit document gebruikt deze configuraties:

- 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
```

Verifiëren

Deze sectie verschaft informatie die u kunt gebruiken om te bevestigen dat uw configuratie correct werkt.

Bepaalde opdrachten met **show worden ondersteund door de tool** Output Interpreter (alleen voor geregistreerde klanten). Hiermee kunt u een analyse van de output van opdrachten met **show genereren.**

- **toon crypto ipsec sa**-shows the fase 2 security associaties.
- **toon crypto isakmp sa** - toont de fase 1 veiligheidsassociaties.
- **toon ip nat vertaling** - toont de huidige NAT vertalingen in gebruik.

Problemen oplossen

Deze sectie bevat informatie waarmee u problemen met de configuratie kunt oplossen.

Opdrachten voor troubleshooting

Bepaalde opdrachten met **show worden ondersteund door de tool** Output Interpreter (alleen voor geregistreerde klanten). Hiermee kunt u een analyse van de output van opdrachten met **show genereren.**

Opmerking: Voordat u **debug-**opdrachten afgeeft, raadpleegt u Belangrijke informatie over Debug Commands.

- **debug crypto ipsec** — toont de IPSec onderhandelingen van fase 2.
- **debug crypto isakmp** — toont de onderhandelingen over fase 1 van de Internet Security Association en Key Management Protocol (ISAKMP).
- **debug crypto motor** - toont het verkeer dat wordt versleuteld.

Gerelateerde informatie

- IPsec-ondersteuningspagina
- IPsec-netwerkbeveiliging configureren
- Het configureren van Internet Key Exchange-beveiligingsprotocol
- Technische ondersteuning - Cisco-systemen