Het configureren van een IPsec Tunnel Private-to-Private Network met NAT en een Static

Inhoud

[Inleiding](#)
[Voorwaarden](#)
[Vereisten](#)
[Gebruikte componenten](#)
[Conventies](#)
[Waarom specificeert de Deny Declaration in ACL het NAT-verkeer?](#)
[Maar hoe zit het met de statische NAT, waarom kan ik dat adres niet bereiken in de IPsec-tunnel?](#)
[Configureren](#)
[Netwerkdiagram](#)
[Configuraties](#)
[Verifiëren](#)
[Problemen oplossen](#)
[Opdrachten voor troubleshooting](#)
[Gerelateerde informatie](#)

Inleiding

Deze voorbeeldconfiguratie toont hoe u:

- Versleutel het verkeer tussen twee particuliere netwerken (10.1.1.x en 172.16.1.x).
- Pas een statisch IP-adres (extern adres 200.1.1.25) aan een netwerkapparaat aan op 10.1.1.3.

U gebruikt toegangscontrolelijsten (ACL's) om de router te vertellen dat u geen netwerkadresomzetting (NAT) wilt uitvoeren naar het privé-to-privé netwerkverkeer, dat vervolgens versleuteld en in de tunnel geplaatst wordt terwijl de router wordt verlaten. Er is ook een statische NAT voor een binnenserver op het 10.1.1.x netwerk in deze voorbeeldconfiguratie. Deze voorbeeldconfiguratie gebruikt de route-map optie op de NAT-opdracht om te voorkomen dat NATd wordt als er verkeer voor is dat ook over de gecodeerde tunnel gaat.

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:

- Cisco IOS®-softwarerelease 12.3(14)T
- twee Cisco-routers

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 Cisco Technical Tips Conventions (Conventies voor technische tips van Cisco) voor meer informatie over documentconventies.

Waarom specificeert de Deny Declaration in ACL het NAT-verkeer?

U vervangt conceptueel een netwerk door een tunnel wanneer u Cisco IOS IPsec of een VPN gebruikt. U vervangt de internetcloud door een Cisco IOS IPsec-tunnel die van 200.1.1.1 tot 10.1.1.1 in dit diagram gaat. Maak dit netwerk transparant vanuit het standpunt van de twee privé LANs die samen door de tunnel worden verbonden. U wilt gewoonlijk geen NAT gebruiken voor het verkeer dat van één privé LAN naar het externe privé LAN gaat om deze reden. U wilt de pakketten zien die van het netwerk van de router 2 met een bron IP adres van het netwerk 10.1.1.0/24 in plaats van 200.1.1 komen wanneer de pakketten het netwerk van de binnenrouter 3 bereiken.

Raadpleeg NAT-operatievolgorde voor meer informatie over het configureren van een NAT. Dit document toont aan dat de NAT plaatsvindt vóór de crypto controle wanneer het pakje van binnenuit naar buiten gaat. Dit is waarom u deze informatie in de configuratie moet specificeren.

```
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
```

Opmerking: Het is ook mogelijk om de tunnel te bouwen en nog steeds NAT te gebruiken. U specificeert in dit scenario het NAT-verkeer als het "interessante verkeer voor IPsec" (aangeduid als ACL 101 in andere secties van dit document). Raadpleeg een IPsec-tunneleffect tussen routers met dubbele LAN-subnetten voor meer informatie over de manier waarop u een tunnel kunt bouwen terwijl NAT actief is.

Maar hoe zit het met de statische NAT, waarom kan ik dat adres niet bereiken in de IPsec-tunnel?

Deze instelling bevat ook een statische één-op-één NAT voor een server op 10.1.1.3. Dit is NAT voor 200.1.1.25 zodat internetgebruikers er toegang toe hebben. Deze opdracht geven:

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

Dit statische NAT belet gebruikers op het 172.16.1.x netwerk om 10.1.1.3 via de gecodeerde tunnel te bereiken. Dit komt doordat u het versleutelde verkeer niet kunt ontkennen door NATd te zijn met ACL 122. De statische NAT-opdracht krijgt echter voorrang op de generieke NAT-verklaring voor alle verbindingen naar en vanaf 10.1.1.3. De statische NAT-verklaring ontkent niet specifiek dat gecodeerde verkeer ook NAT-d is. De antwoorden van 10.1.1.3 zijn NAT'd naar 200.1.1.25 wanneer een gebruiker op het 172.16.1.x-netwerk zich verbindt met 10.1.1.3 en daarom niet terug gaat via de gecodeerde tunnel (NAT gebeurt vóór encryptie).

U moet versleuteld verkeer ontkennen van NAT'd (zelfs statelijk één-op-één NAT'd) met een **route-map-**opdracht op de statische NAT-verklaring.

Opmerking: de **route-map-**optie op een statische NAT wordt alleen ondersteund door Cisco IOS-softwarerelease 12.2(4)T en hoger. Raadpleeg NAT-mogelijkheid voor routekaarten met statische omzettingen voor meer informatie.

U moet deze extra opdrachten uitgeven om gecodeerde toegang tot 10.1.1.3 toe te staan, de statische NAT's host:

```
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
```

Deze verklaringen vertellen de router om alleen de statische NAT op verkeer toe te passen dat ACL 150 overeenkomt. ACL 150 zegt om NAT niet toe te passen op verkeer dat uit 10.1.1.3 komt en over de gecodeerde tunnel aan 172.16.1.x is bestemd. Pas het echter toe op al het andere verkeer dat afkomstig is van 10.1.1.3 (internetverkeer).

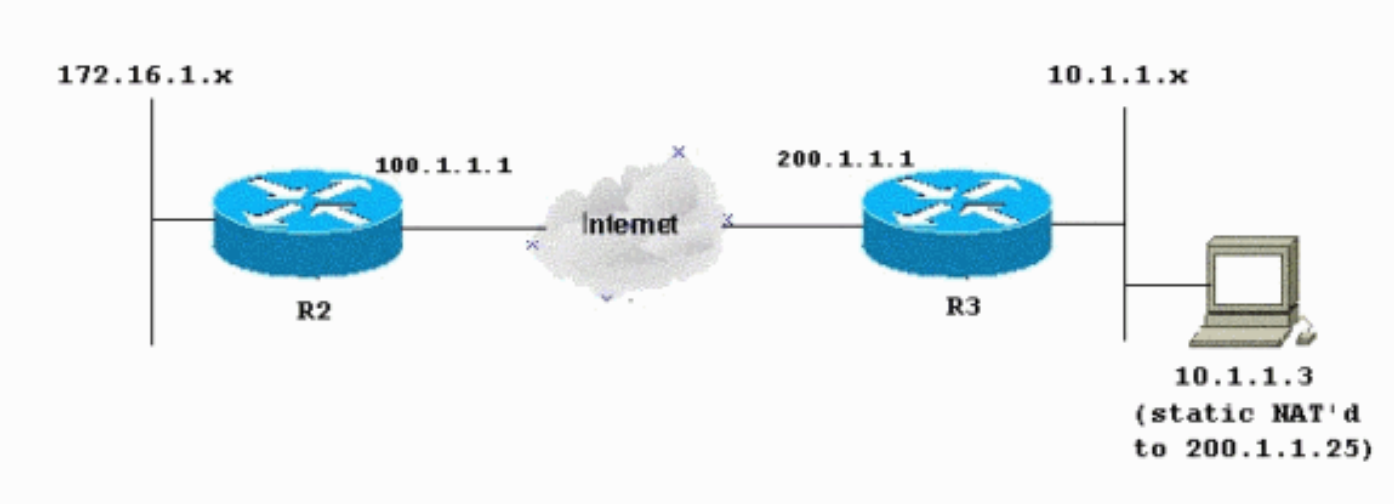
Configureren

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

N.B.: Gebruik het Opdrachtupgereedschap (alleen geregistreerde klanten) om meer informatie te vinden over de opdrachten die in dit document worden gebruikt.

Netwerkdiagram

Het netwerk in dit document is als volgt opgebouwd:



Configuraties

Dit document gebruikt deze configuraties:

- router 2
- router 3

R2 - routerconfiguratie

```
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 - routerconfiguratie

```
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
```

Verifiëren

Er is momenteel geen verificatieprocedure beschikbaar voor deze configuratie.

Problemen oplossen

Gebruik dit gedeelte om de configuratie van het probleem op te lossen.

Raadpleeg het gedeelte IP-beveiligingsprobleemoplossing - Opdrachten begrijpen en gebruiken voor extra informatie.

Opdrachten voor troubleshooting

Het Uitvoer Tolk (uitsluitend geregistreerde klanten) (OIT) ondersteunt bepaalde **show** opdrachten. Gebruik de OIT om een analyse van **tonen** opdrachtoutput te bekijken.

Opmerking: Raadpleeg Belangrijke informatie over debug Commands voordat u **debug-**opdrachten gebruikt.

- **debug crypto ipsec sa** — Hiermee worden de IPsec-onderhandelingen van fase 2 weergegeven.
- **debug crypto isakmp sa** — Zie de ISAKMP-onderhandelingen van fase 1.
- **debug-encryptie-motor** — Hiermee worden de versleutelde sessies weergegeven.

Gerelateerde informatie

- IPsec-onderhandeling/IKE-protocollen - Cisco-systemen
- Technische ondersteuning en documentatie – Cisco Systems