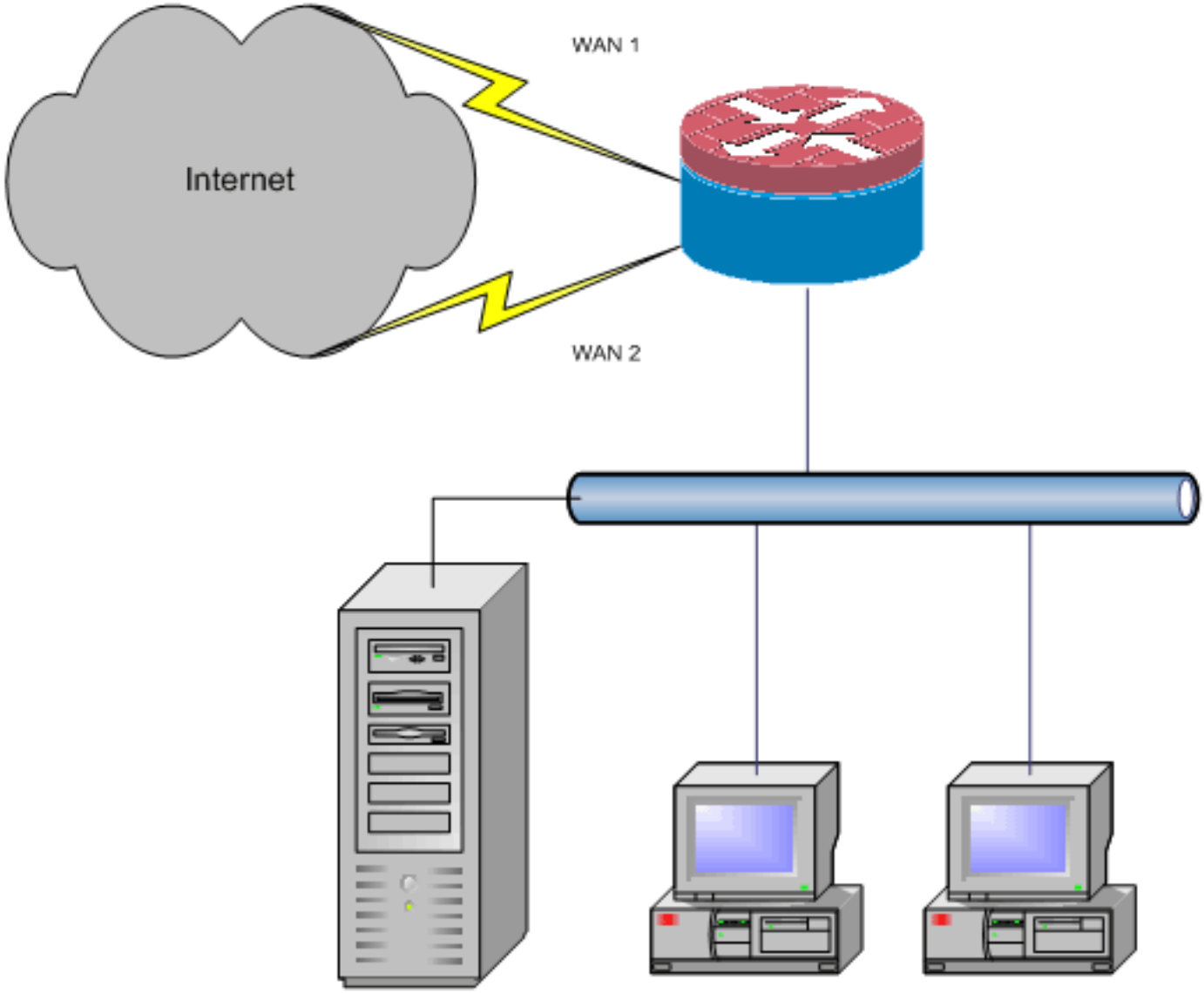
Cisco IOS NAT configureren voor twee ISP-verbindingen met OER

Inhoud

Inleiding

Dit document beschrijft een configuratie voor een Cisco IOS® router om een netwerk met internet te verbinden met Network Address Translation (NAT) via twee ISP-verbindingen. Cisco IOS NAT kan volgende TCP-verbindingen en UDP-sessies via meerdere netwerkverbindingen distribueren als gelijke kostenroutes naar een bepaalde bestemming beschikbaar zijn. In het geval dat een van de verbindingen onbruikbaar wordt, kan object-tracking, een component van Optimized Edge Routing (OER), worden gebruikt om de route te deactiveren totdat de verbinding opnieuw beschikbaar wordt, waardoor de netwerkbeschikbaarheid wordt geïnspireerd op instabiliteit of onbetrouwbaarheid van een internetverbinding.



Dit document beschrijft extra configuraties om Cisco IOS Zone-Based Policy Firewall toe te passen om stateful inspection mogelijkheid toe te voegen om de basisnetwerkbescherming die door NAT wordt geboden te verbeteren.

Voorwaarden

Vereisten

Dit document gaat ervan uit dat u al LAN- en WAN-verbindingen hebt die werken en geen configuratie- of achtergrondinformatie biedt voor het instellen van een initiële connectiviteit.

In dit document wordt geen manier beschreven om een onderscheid te maken tussen de routes. Daarom is er geen manier om de voorkeur te geven aan een meer wenselijke connectie boven een minder wenselijke connectie.

Dit document beschrijft hoe u OER moet configureren om een van de internetroutes in of uit te schakelen op basis van de bereikbaarheid van de DNS-servers van de ISP. U moet specifieke hosts identificeren die slechts via één van de ISP-verbindingen bereikbaar zijn en mogelijk niet beschikbaar zijn als de verbinding van die ISP niet beschikbaar is.

Gebruikte componenten

Deze configuratie is ontwikkeld met een Cisco 1811 router met 12.4(15)T2 geavanceerde IP-servicessoftware. Als er een andere softwareversie wordt gebruikt, zijn bepaalde functies mogelijk niet beschikbaar of zijn de configuratieopdrachten mogelijk niet beschikbaar in dit document. Gelijkaardige configuraties zouden beschikbaar moeten zijn op alle Cisco IOS routerplatforms, alhoewel de interfaceconfiguratie waarschijnlijk tussen verschillende platforms zal verschillen.

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 de Cisco Technical Tips Convention voor meer informatie over documentconventies.

Configureren

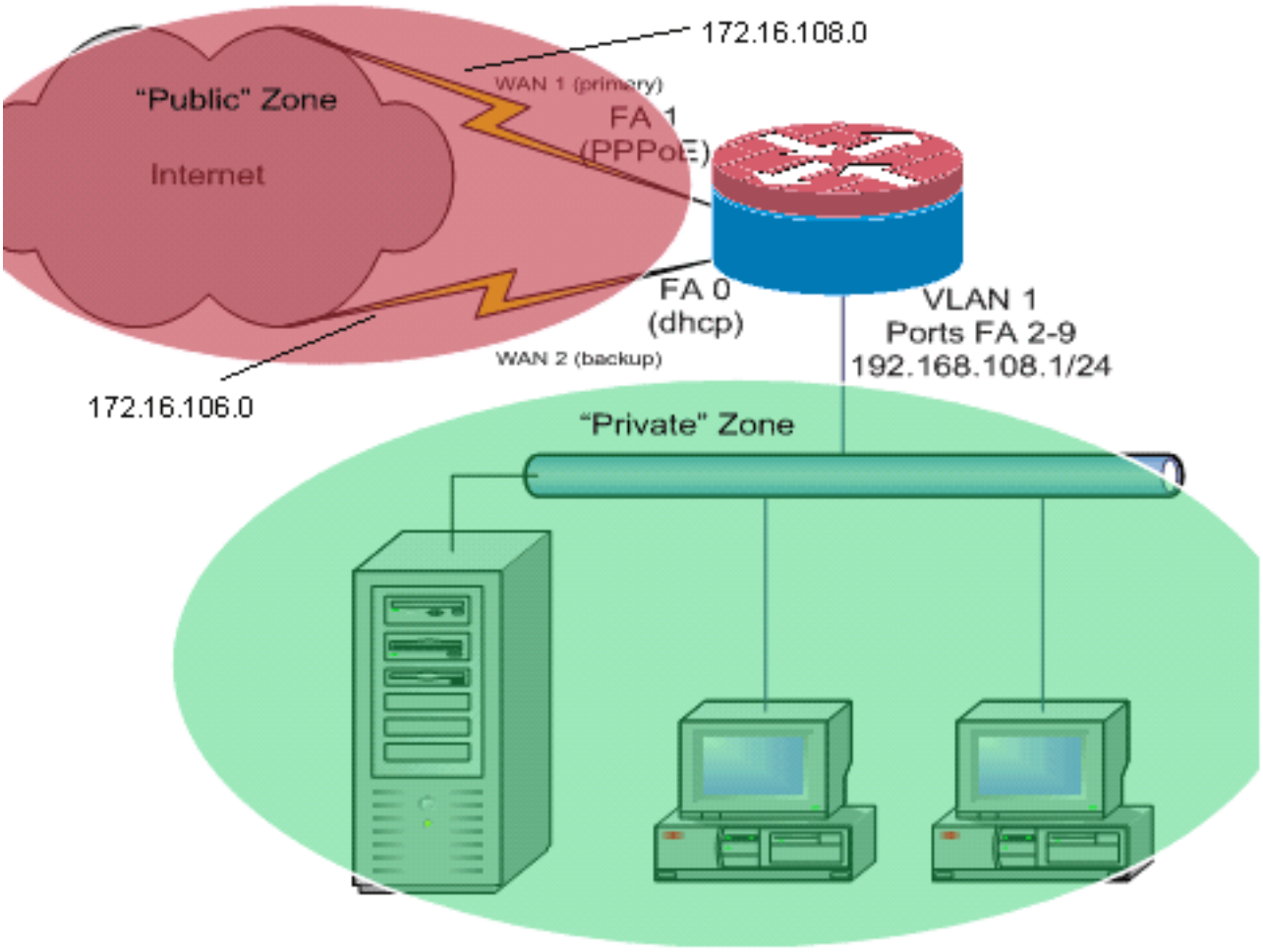
U kunt op beleid gebaseerde routing voor specifiek verkeer toevoegen om er zeker van te zijn dat het altijd één ISP-verbinding gebruikt. Voorbeelden van verkeer die dit gedrag kunnen vereisen zijn IPsec VPN-clients, VoIP-telefoons en elk ander verkeer dat altijd alleen één van de ISP-verbindingsopties zou moeten gebruiken om hetzelfde IP-adres, dezelfde hoge snelheid of een lagere latentie op de verbinding te prefereren.

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

Opmerking: Gebruik het Opname Gereedschap (alleen geregistreerde klanten) om meer informatie te verkrijgen over de opdrachten die in deze sectie worden gebruikt.

Netwerkdiagram

Het netwerk in dit document is als volgt opgebouwd:



Dit configuratievoorbeeld, zoals in het netwerkdiagram wordt geïllustreerd, beschrijft een toegangsrouter die een door DHCP geconfigureerd IP-verbinding naar één ISP gebruikt (zoals getoond door Fast Ethernet 0) en een PPPoE-verbinding via de andere ISP-verbinding. De verbindingstypes hebben geen bijzonder effect op de configuratie, tenzij object-tracking en Optimized Edge Routing (OER) en/of op beleid gebaseerde routing gebruikt moeten worden met een DHCP-toegewezen internetverbinding. In deze gevallen kan het zeer moeilijk zijn om een volgende-hoprouter voor beleidsrouting of OER te definiëren.

Firewallbeleidsdiscussie

Dit configuratievoorbeeld beschrijft een firewallbeleid dat eenvoudige TCP-, UDP- en ICMP-verbindingen van de "binnenkant" veiligheidszone naar de "buiten" veiligheidszone toestaat en uitgaande FTP-verbindingen en het corresponderende gegevensverkeer voor zowel actieve als passieve FTP-overdrachtsbetalingen toestaat. Elk complex toepassingsverkeer (bijvoorbeeld VoIP-signalering en media) dat niet door dit basisbeleid wordt afgehandeld, zal waarschijnlijk met minder mogelijkheden werken of kan geheel falen. Dit firewallbeleid blokkeert alle verbindingen van het "publieke" veiligheidsgebied naar het "particuliere" gebied, dat alle verbindingen omvat die door NAT poorttransport worden ondergebracht. U moet extra firewallbeleidsformaties bouwen om extra verkeer mogelijk te maken dat niet door deze basisconfiguratie wordt verwerkt.

Als u vragen hebt over het ontwerp en de configuratie van het beleid van de Firewall op basis van een zone, raadpleeg dan de Zone-Based Policy Firewall Design and Application Guide.

CLI-configuratie

Cisco IOS CLI-configuratie

```
track timer interface 5
!
!
track 123 rtr 1 reachability
 delay down 15 up 10
!
track 345 rtr 2 reachability
 delay down 15 up 10
!
!---Configure timers on route tracking class-map type
inspect match-any priv-pub-traffic match protocol ftp
match protocol tcp match protocol udp match protocol
icmp ! policy-map type inspect priv-pub-policy class
type inspect priv-pub-traffic inspect class class-
default ! zone security public zone security private
zone-pair security priv-pub source private destination
public service-policy type inspect priv-pub-policy ! !
interface FastEthernet0 ip address dhcp ip dhcp client
route track 345
 ip nat outside
 ip virtual-reassembly
 zone security public
!
!---Use "ip dhcp client route track [number]" !--- to
monitor route on DHCP interfaces !--- Define ISP-facing
interfaces with "ip nat outside" interface FastEthernet1
no ip address pppoe enable no cdp enable ! interface
FastEthernet2 no cdp enable ! interface FastEthernet3 no
cdp enable ! interface FastEthernet4 no cdp enable !
interface FastEthernet5 no cdp enable ! interface
FastEthernet6 no cdp enable ! interface FastEthernet7 no
cdp enable ! interface FastEthernet8 no cdp enable !
interface FastEthernet9 no cdp enable ! ! interface
Vlan1 description LAN Interface ip address 192.168.108.1
255.255.255.0 ip nat inside ip virtual-reassembly ip tcp
adjust-mss 1452 zone security private !--- Define LAN-
facing interfaces with "ip nat inside" ! ! Interface
Dialer 0 description PPPoX dialer ip address negotiated
ip nat outside ip virtual-reassembly ip tcp adjust-mss
zone security public !---Define ISP-facing interfaces
with "ip nat outside" ! ip route 0.0.0.0 0.0.0.0 dialer
0 track 123 ! ! ip nat inside source route-map fixed-nat
interface Dialer0 overload ip nat inside source route-
map dhcp-nat interface FastEthernet0 overload !---
Configure NAT overload (PAT) to use route-maps ! ! ip
sla 1 icmp-echo 172.16.108.1 source-interface Dialer0
timeout 1000 threshold 40 frequency 3 !---Configure an
OER tracking entry to monitor the !---first ISP
connection ! ! ! ip sla 2 icmp-echo 172.16.106.1 source-
interface FastEthernet0 timeout 1000 threshold 40
frequency 3 !--- Configure a second OER tracking entry
to monitor !---the second ISP connection ! ! ! ip sla
schedule 1 life forever start-time now ip sla schedule 2
life forever start-time now !---Set the SLA schedule and
duration ! ! ! access-list 110 permit ip 192.168.108.0
0.0.0.255 any !--- Define ACLs for traffic that will be
!--- NATed to the ISP connections ! ! ! route-map fixed-
nat permit 10 match ip address 110 match interface
Dialer0 ! route-map dhcp-nat permit 10 match ip address
110 match interface FastEthernet0 !--- Route-maps
associate NAT ACLs with NAT !--- outside on the ISP-
facing interfaces
```

Gebruik dhcp-toegewezen route volgen:

Cisco IOS CLI-configuratie
interface FastEthernet0 description Internet Intf ip dhcp client route track 123 ip address dhcp ip nat outside ip virtual-reassembly speed 100 full-duplex no cdp enable

Verifiëren

Gebruik dit gedeelte om te bevestigen dat de configuratie correct werkt.

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

- **toon ip nationaal vertalen**-Toont NAT-activiteit tussen NAT binnen hosts en NAT buiten hosts. Deze opdracht verschaft verificatie dat interne hosts naar beide NAT-adressen worden vertaald.

```
Router#show ip nat tra
Pro Inside global      Inside local       Outside local      Outside global
tcp 172.16.108.44:54486 192.168.108.3:54486 172.16.104.10:22 172.16.104.10:22
tcp 172.16.106.42:49620 192.168.108.3:49620 172.16.102.11:80 172.16.102.11:80
tcp 172.16.108.44:1623 192.168.108.4:1623 172.16.102.11:445  172.16.102.11:445
Router#
```

- **toon ip route**—verifieert dat de meerdere routes naar het internet beschikbaar zijn.

```
Router#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is 172.16.108.1 to network 0.0.0.0

C    192.168.108.0/24 is directly connected, Vlan1
     172.16.0.0/24 is subnetted, 2 subnets
C       172.16.108.0 is directly connected, FastEthernet4
C       172.16.106.0 is directly connected, Vlan106
S*   0.0.0.0/0 [1/0] via 172.16.108.1
               [1/0] via 172.16.106.1
```

- **toon beleid-kaart type inspecteert zone-paar sessies**-Beeldt de inspectie van de firewall tussen privé zonehosts en openbaar zonegastheren. Deze opdracht verstrekt verificatie dat het verkeer op de binnenhosts wordt geïnspecteerd als hosts communiceren met de diensten in de externe veiligheidszone.

Problemen oplossen

Controleer deze items als de verbindingen niet werken nadat u de Cisco IOS router met NAT configureren:

- NAT wordt correct toegepast op buiten- en binneninterfaces.
- NAT-configuratie is voltooid en ACL's geven het verkeer weer dat NATed moet zijn.
- Er zijn meerdere routes naar internet/WAN beschikbaar.
- Als u route tracking gebruikt, controleer dan de staat van de route die volgt om er zeker van te zijn dat de internetverbindingen beschikbaar zijn.
- Het firewallbeleid reflecteert nauwkeurig de aard van het verkeer dat u door de router wilt toestaan.

Gerelateerde informatie

- Cisco IOS Firewall
- Cisco IOS IP-adresseringsopdracht voor services - NAT-opdrachten
- Zone-Based Policy Firewall Design and Application Guide
- Cisco IOS geoptimaliseerde Edge-routinggids, release 12.4T
- Technische ondersteuning en documentatie – Cisco Systems