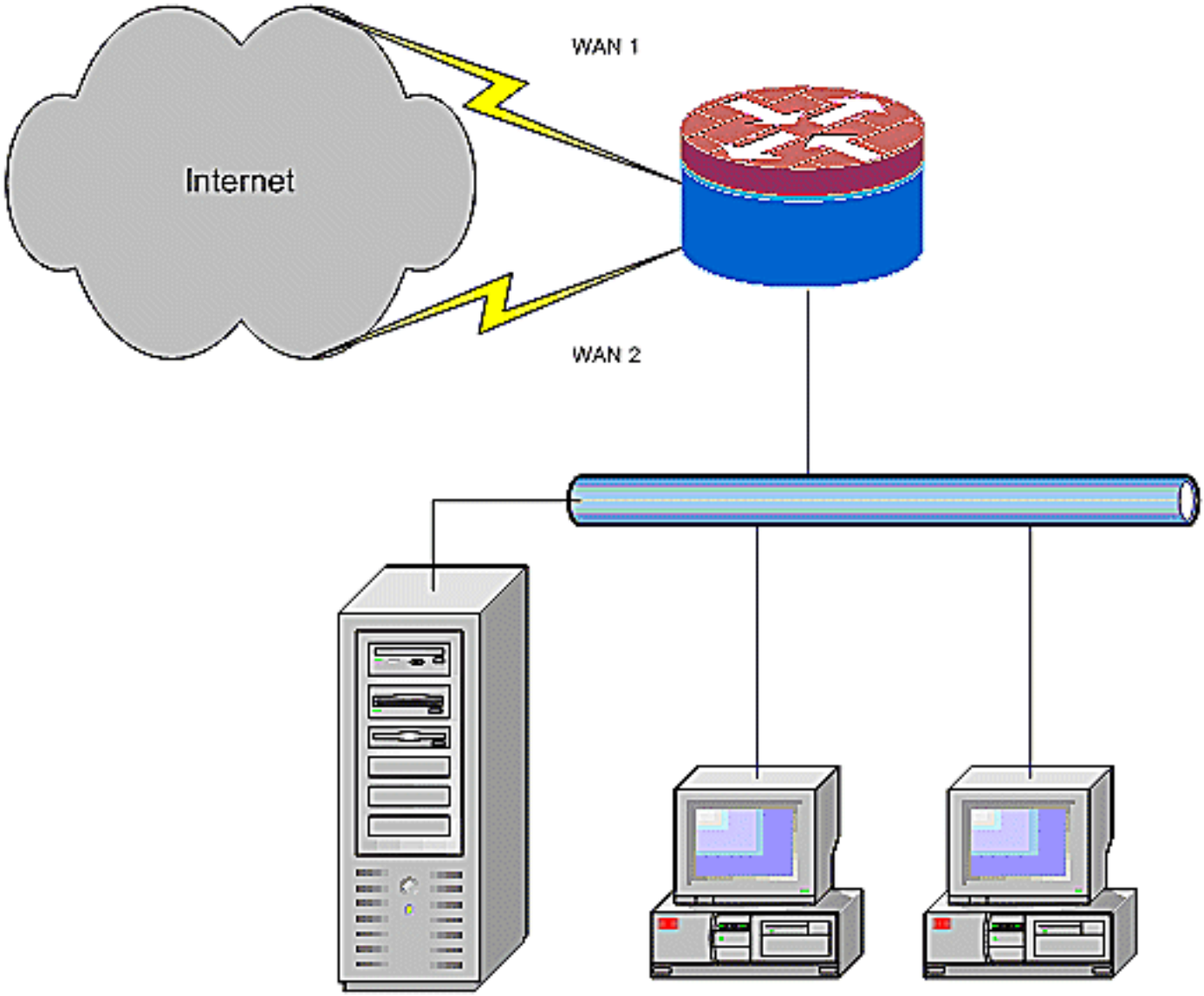
IOS NAT-taakverdeling met Zone-gebaseerde beleidsfirewall voor twee ISP-verbindingen

Inhoud

Inleiding

Dit document biedt een voorbeeldconfiguratie voor een Cisco IOS®-router om een netwerk met Internet te verbinden met Netwerkadresomzetting (NAT) door twee ISP-verbindingen. De Cisco IOS software NAT kan volgende TCP-verbindingen en UDP-sessies via meerdere netwerkverbindingen distribueren als de gelijke-kostenroutes naar een bepaalde bestemming beschikbaar zijn.



Dit document beschrijft extra configuratie om de Cisco IOS Zone-Based Policy Firewall (ZFW) toe te passen om stateful inspection mogelijkheid toe te voegen om de basale netwerkbescherming te verbeteren die door NAT wordt geboden.

Voorwaarden

Vereisten

Dit document gaat ervan uit dat u met LAN- en WAN-verbindingen werkt en biedt geen configuratie- of probleemoplossing voor de basisconnectiviteit. In dit document wordt geen manier beschreven om een onderscheid te maken tussen de routes, dus er is geen manier om de voorkeur te geven aan een meer wenselijke verbinding boven een minder wenselijke verbinding.

Gebruikte componenten

De informatie in dit document is gebaseerd op de Cisco Series 1811 router met 12.4(15)T3 geavanceerde IP-servicessoftware. Als een andere softwareversie wordt gebruikt, zijn bepaalde

functies niet beschikbaar of de configuratieopdrachten kunnen verschillen van de opdrachten in dit document. Gelijkaardige configuratie is beschikbaar op alle Cisco IOS routerplatforms, alhoewel de interfaceconfiguratie waarschijnlijk tussen verschillende platforms verschilt.

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

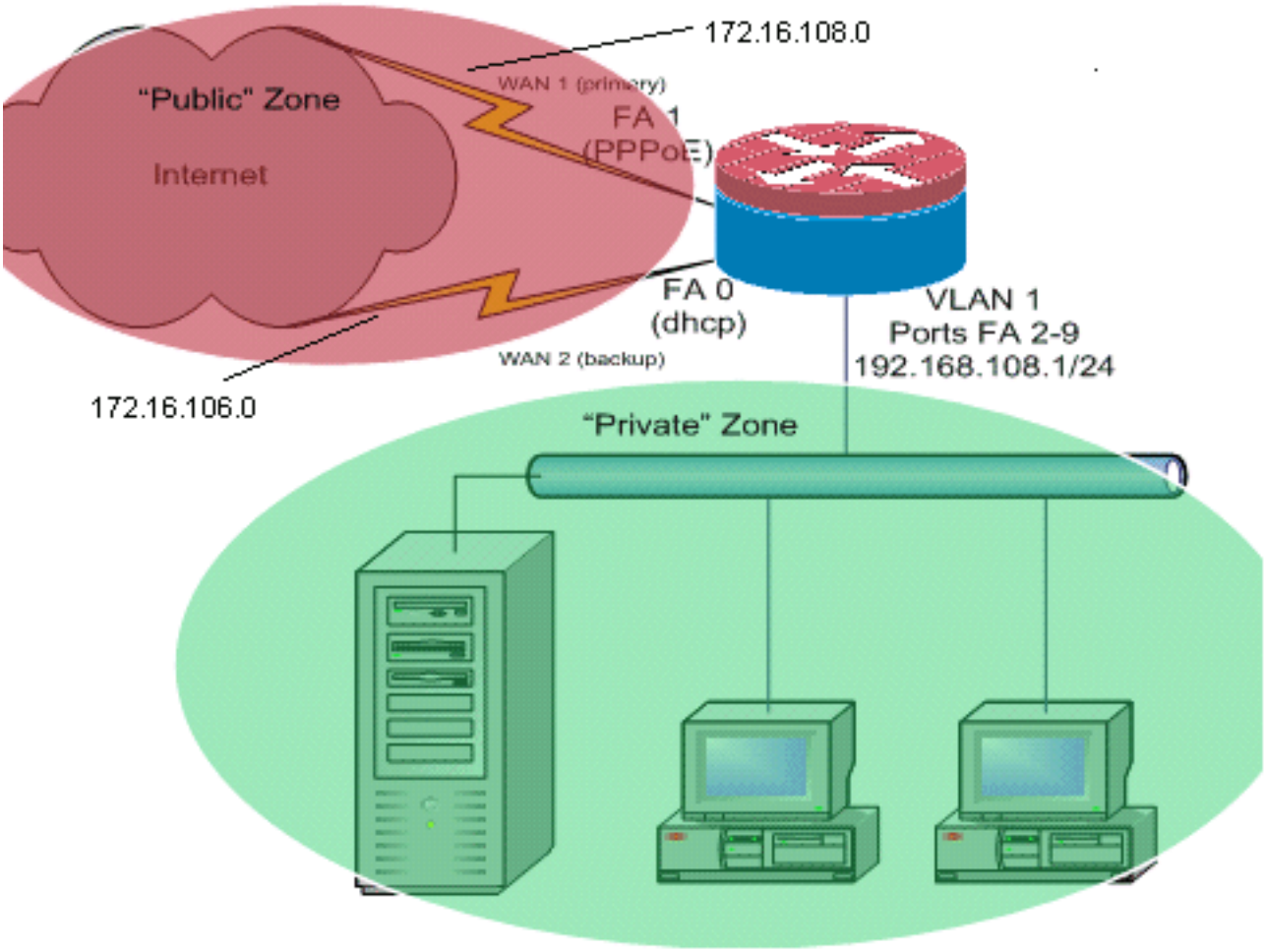
Deze sectie bevat informatie over het configureren van de functies die in dit document worden beschreven.

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

U moet op beleid gebaseerde routing voor specifiek verkeer toevoegen om er zeker van te zijn dat het altijd één ISP-verbinding gebruikt. Voorbeelden van verkeer dat dit gedrag kan vereisen zijn de cliënten van IPSec VPN, het telefoonverkeer van VoIP en elk ander verkeer dat slechts één van de ISP verbindingsopties gebruikt om het zelfde IP adres, hogere snelheid, of lagere latentie op de verbinding te prefereren.

Netwerkdiagram

Het netwerk in dit document is als volgt opgebouwd:



Dit configuratievoorbeeld 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 connectiviteitstypes hebben geen specifieke impact op de configuratie, maar sommige connectiviteitstypes kunnen de bruikbaarheid van deze configuratie in specifieke mislukkingsscenario's verhinderen. Dit gebeurt in het bijzonder in gevallen waar IP-connectiviteit via een Ethernet-verbonden WAN-service wordt gebruikt, bijvoorbeeld kabelmodems of DSL-services waar een extra apparaat de WAN-connectiviteit eindigt en Ethernet-overdracht naar de Cisco IOS-router biedt. In gevallen waar statische IP-adressering wordt toegepast, in tegenstelling tot DHCP-toegewezen adressen of PPPoE, en een WAN-storing optreedt, zodat de Ethernet-poort nog steeds Ethernet-link naar het WAN-aansluitingsapparaat onderhoudt, blijft de router proberen de connectiviteit in evenwicht te brengen via zowel de goede als de slechte WAN-verbindingen. Als uw plaatsing vereist dat inactieve routes van lading-in-evenwicht worden verwijderd, verwijs naar de configuratie die in Cisco IOS NAT taakverdeling en Zone-Based Policy Firewall met Geoptimaliseerde Rand Routing voor twee Internet-verbindingen die de toevoeging van Geoptimaliseerde Rand Routing beschrijft om de geldigheid van de route te controleren.

Firewallbeleidsdiscussie

Dit configuratievoorbeeld beschrijft een firewallbeleid dat eenvoudige TCP-, UDP- en ICMP-verbindingen van de "binnen" veiligheidszone naar de "buiten" veiligheidszone toestaat en uitgaande FTP-verbindingen en het equivalente gegevensverkeer voor zowel actieve als passieve FTP-overdrachtsbetalingen toestaat. Elk complex toepassingsverkeer, bijvoorbeeld VoIP-signalering en media, dat niet door dit basisbeleid wordt afgehandeld, werkt waarschijnlijk met minder mogelijkheden of kan geheel falen. Dit firewallbeleid blokkeert alle verbindingen van de "publieke" veiligheidszone naar de "private" zone, die alle verbindingen omvat die worden opgevangen door NAT port-expediteur. Indien nodig moet u het beleid voor firewallinspectie

aanpassen om uw toepassingsprofiel en uw beveiligingsbeleid weer te geven.

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

Configuraties

Dit document gebruikt deze configuraties:

Configuratie

```
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 nat outside ip virtual-
reassembly zone security public ! interface
FastEthernet1 no ip address pppoe enable no cdp enable !
interface FastEthernet2 no cdp enable !--- Output
Suppressed 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 ! 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 ! 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
```

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 worden vertaald naar beide NAT-adressen buiten.

  ```
  Router# show ip nat translation
  ```

```
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 inspecteer zone-paar sessies**-Toont firewallinspectie tussen "private"-zone hosts en "openbare"-zone hosts. Deze opdracht geeft verificatie dat het verkeer van binnenhosts is geïnspecteerd als hosts communiceren met de diensten in de "externe" veiligheidszone.

Problemen oplossen

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

Nadat u de Cisco IOS-router met NAT hebt configureren, als de verbindingen niet werken, zorg er dan voor dat deze:

- 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.
- Het firewallbeleid reflecteert nauwkeurig de aard van het verkeer dat u door de router wilt toestaan.

Gerelateerde informatie

- Ondersteuning voor spraaktechnologie
- Productondersteuning voor spraak en Unified Communications
- Probleemoplossing voor Cisco IP-telefonie
- Zone-Based Policy Firewall Design and Application Guide
- Technische ondersteuning en documentatie – Cisco Systems