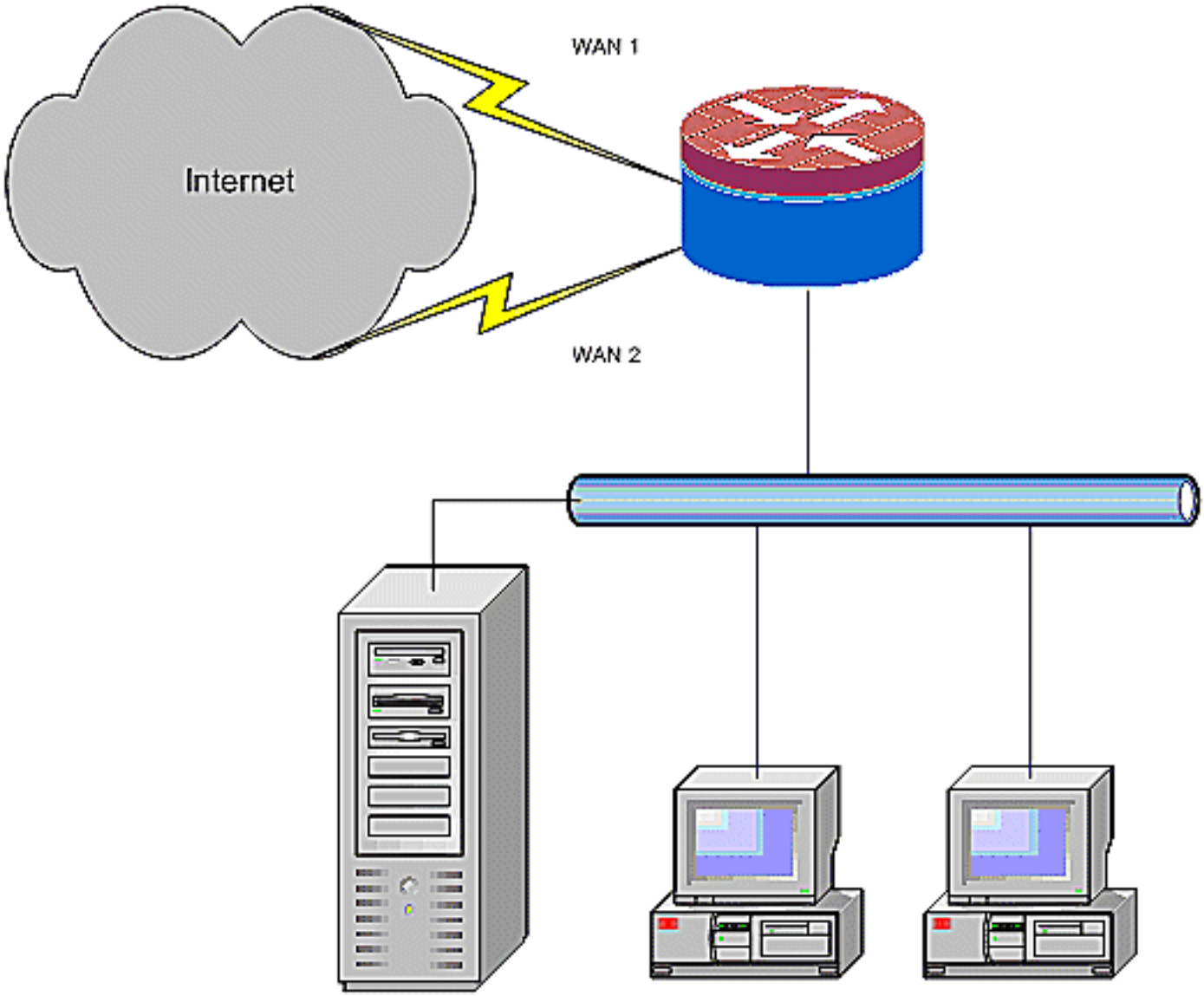
IOS NAT Load Balancing mit zonenbasierter Firewall für zwei ISP-Verbindungen

Inhalt

Einführung

Dieses Dokument enthält eine Beispielkonfiguration für einen Cisco IOS®-Router, um über zwei ISP-Verbindungen ein Netzwerk mit Network Address Translation (NAT) mit dem Internet zu verbinden. Die Cisco IOS-Software NAT kann folgende TCP-Verbindungen und UDP-Sitzungen über mehrere Netzwerkverbindungen verteilen, wenn preiswerte Routen zu einem bestimmten Ziel verfügbar sind.



Dieses Dokument beschreibt zusätzliche Konfiguration zur Anwendung der Cisco IOS Zone-Based Policy Firewall (ZFW), um Stateful Inspection-Funktionen zur Verbesserung des grundlegenden Netzwerkschutzes durch NAT hinzuzufügen.

Voraussetzungen

Anforderungen

In diesem Dokument wird davon ausgegangen, dass Sie mit LAN- und WAN-Verbindungen arbeiten und keine Hintergrundinformationen zur Konfiguration oder Fehlerbehebung für die Herstellung der Erstverbindung bereitstellen. In diesem Dokument wird keine Möglichkeit zur Unterscheidung zwischen den Routen beschrieben. Daher ist es nicht möglich, eine wünschenswertere Verbindung einer weniger wünschenswerten Verbindung vorzuziehen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf der Cisco Serie 1811 Router mit Advanced IP

Services Software 12.4(15)T3. Wenn eine andere Softwareversion verwendet wird, sind einige Funktionen nicht verfügbar, oder die Konfigurationsbefehle können von den in diesem Dokument angegebenen abweichen. Eine ähnliche Konfiguration ist auf allen Cisco IOS-Router-Plattformen verfügbar, auch wenn die Schnittstellenkonfiguration zwischen den verschiedenen Plattformen unterschiedlich sein kann.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie in den Cisco Technical Tips Conventions (Technische Tipps zu Konventionen von Cisco).

Konfigurieren

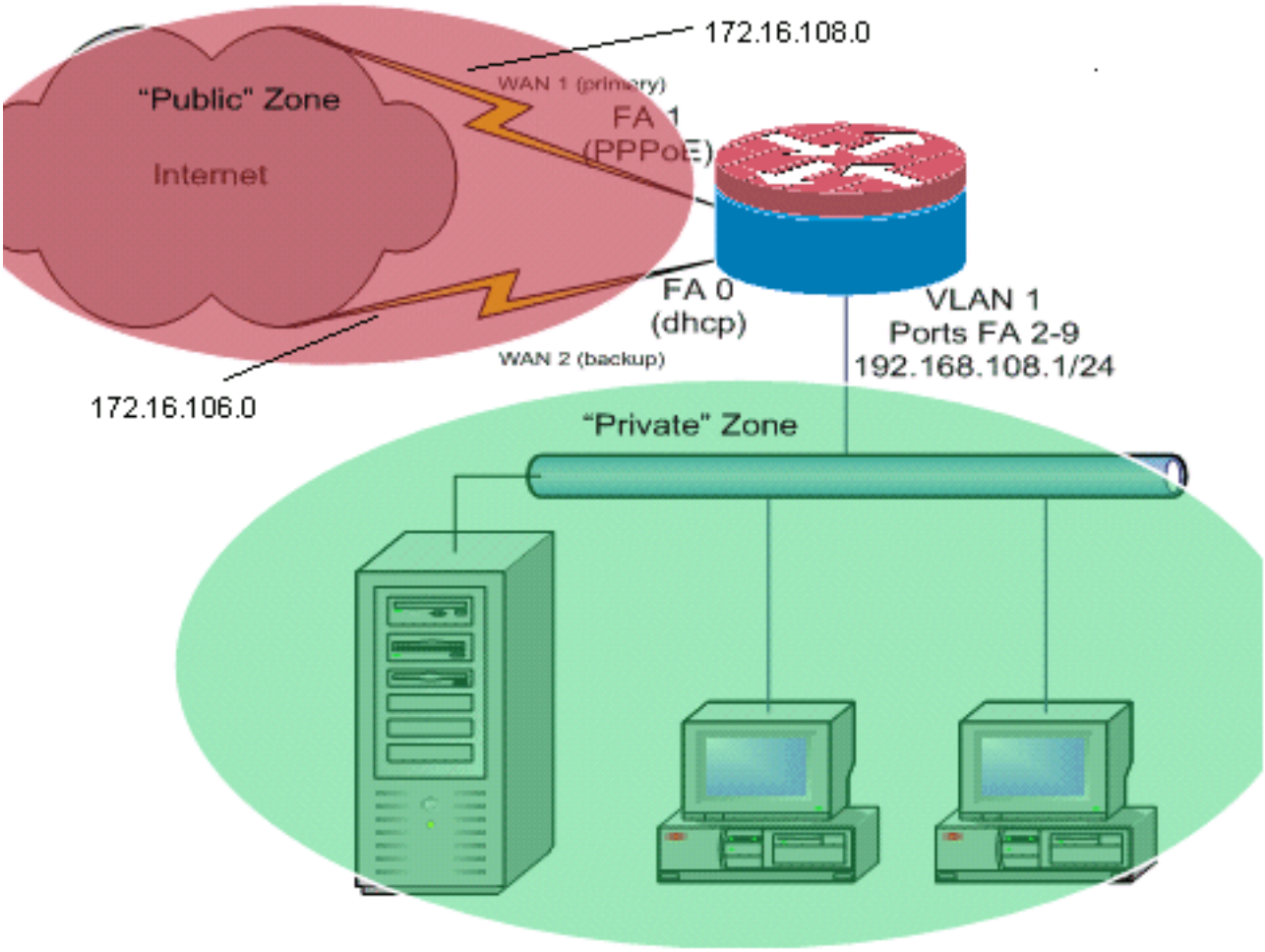
In diesem Abschnitt erhalten Sie Informationen zum Konfigurieren der in diesem Dokument beschriebenen Funktionen.

Hinweis: Verwenden Sie das Command Lookup Tool (nur registrierte Kunden), um weitere Informationen zu den in diesem Abschnitt verwendeten Befehlen zu erhalten.

Sie müssen richtlinienbasiertes Routing für bestimmten Datenverkehr hinzufügen, um sicherzustellen, dass immer eine ISP-Verbindung verwendet wird. Beispiele für Datenverkehr, der dieses Verhalten erfordern kann, sind IPSec VPN-Clients, VoIP-Telefonie-Datenverkehr und jeder andere Datenverkehr, der nur eine der ISP-Verbindungsoptionen verwendet, um dieselbe IP-Adresse, höhere Geschwindigkeit oder geringere Latenz für die Verbindung vorzuziehen.

Netzwerkdiagramm

In diesem Dokument wird die folgende Netzwerkeinrichtung verwendet:



In diesem Konfigurationsbeispiel wird ein Access Router beschrieben, der eine DHCP-konfigurierte IP-Verbindung mit einem ISP (wie durch FastEthernet 0 dargestellt) und eine PPPoE-Verbindung mit der anderen ISP-Verbindung verwendet. Die Verbindungstypen haben keine besonderen Auswirkungen auf die Konfiguration, aber einige Verbindungstypen können die Verwendbarkeit dieser Konfiguration in bestimmten Fehlerszenarien verhindern. Dies gilt insbesondere für Fälle, in denen IP-Verbindungen über einen Ethernet-verbundenen WAN-Dienst verwendet werden, z. B. Kabelmodem oder DSL-Dienste, bei denen ein zusätzliches Gerät die WAN-Verbindung beendet und eine Ethernet-Übergabe an den Cisco IOS-Router ermöglicht. In Fällen, in denen statische IP-Adressierung angewendet wird, im Gegensatz zu DHCP-zugewiesenen Adressen oder PPPoE und ein WAN-Fehler, in dem der Ethernet-Port weiterhin eine Ethernet-Verbindung zum WAN-Verbindungsgerät unterhält, versucht der Router weiterhin, die Lastverteilung zwischen den guten und schlechten WAN-Verbindungen auszugleichen. Wenn bei Ihrer Bereitstellung inaktive Routen aus dem Lastenausgleich entfernt werden müssen, lesen Sie die Konfiguration in Cisco IOS NAT Load Balancing und Zone-Based Policy Firewall mit Optimized Edge Routing for Two Internet Connections, in der das Hinzufügen von Optimized Edge Routing zur Überwachung der Routenvalidierung beschrieben wird.

Diskussionen über Firewall-Richtlinien

In diesem Konfigurationsbeispiel wird eine Firewall-Richtlinie beschrieben, die einfache TCP-, UDP- und ICMP-Verbindungen von der "internen" Sicherheitszone zur "externen" Sicherheitszone zulässt und ausgehende FTP-Verbindungen sowie den entsprechenden Datenverkehr für aktive und passive FTP-Übertragungen unterstützt. Jeder komplexe Anwendungsdatenverkehr, z. B. VoIP-Signalisierung und Medien, der von dieser grundlegenden Richtlinie nicht behandelt wird, funktioniert wahrscheinlich mit eingeschränkter Funktionalität oder kann gänzlich ausfallen. Diese Firewall-Richtlinie blockiert alle Verbindungen von der "öffentlichen" Sicherheitszone zur "privaten"

Zone, die alle Verbindungen umfasst, die durch die NAT-Port-Weiterleitung unterstützt werden. Bei Bedarf müssen Sie die Firewall-Überprüfungsrichtlinie an Ihr Anwendungsprofil und Ihre Sicherheitsrichtlinien anpassen.

Wenn Sie Fragen zum Design und zur Konfiguration von zonenbasierten Richtlinien-Firewall-Richtlinien haben, lesen Sie den zonenbasierten Firewall-Design- und Anwendungshandbuch.

Konfigurationen

In diesem Dokument werden folgende Konfigurationen verwendet:

Konfiguration

```
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
```

Überprüfen

In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Das Output Interpreter Tool (nur registrierte Kunden) (OIT) unterstützt bestimmte **show**-Befehle. Verwenden Sie das OIT, um eine Analyse der **Ausgabe des** Befehls **show anzuzeigen**.

- **show ip nat translation**: Zeigt die NAT-Aktivität zwischen NAT innerhalb von Hosts und NAT außerhalb von Hosts an. Mit diesem Befehl wird überprüft, ob interne Hosts in beide NAT-

externen Adressen übersetzt werden.

```
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#
```

- **show ip route** - Überprüft, ob mehrere Routen zum Internet verfügbar sind.

```
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
```

- **show policy-map type inspect zone-pair sessions** - Zeigt die Firewall-Inspection-Aktivität zwischen Hosts in "privaten" Zonen und Hosts in "öffentlichen" Zonen an. Dieser Befehl stellt sicher, dass der Datenverkehr der internen Hosts überprüft wird, wenn Hosts mit Diensten in der "externen" Sicherheitszone kommunizieren.

Fehlerbehebung

Dieser Abschnitt enthält Informationen zur Fehlerbehebung in Ihrer Konfiguration.

Wenn Sie den Cisco IOS-Router mit NAT konfiguriert haben, sollten Sie folgende Punkte beachten, wenn die Verbindungen nicht funktionieren:

- NAT wird auf Außen- und Innenschnittstellen angemessen angewendet.
- Die NAT-Konfiguration ist abgeschlossen, und die ACLs spiegeln den Verkehr wider, der NATed sein muss.
- Es stehen mehrere Routen zum Internet/WAN zur Verfügung.
- Die Firewall-Richtlinie spiegelt genau die Art des Datenverkehrs wider, den Sie über den Router zulassen möchten.

Zugehörige Informationen

- Unterstützung von Sprachtechnologie
- Produkt-Support für Sprach- und Unified Communications
- Fehlerbehebung bei Cisco IP-Telefonie
- Firewall-Design und Anwendungshandbuch für zonenbasierte Richtlinien
- Technischer Support und Dokumentation - Cisco Systems