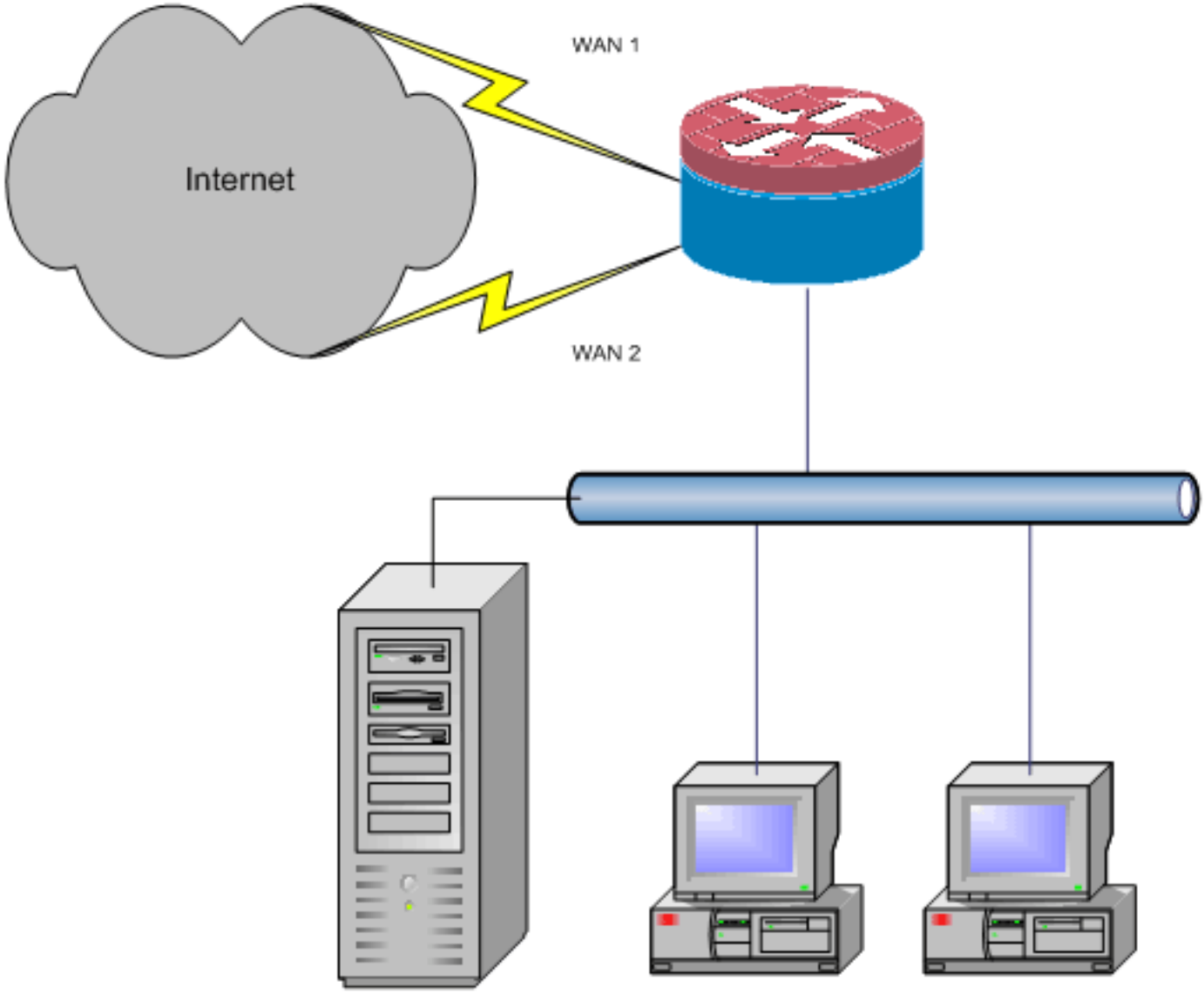
Konfigurieren von Cisco IOS NAT für zwei ISP-Verbindungen mit OER

Inhalt

Einleitung

Dieses Dokument beschreibt eine Konfiguration für einen Cisco IOS®-Router, der über zwei ISP-Verbindungen eine Netzwerkverbindung mit dem Internet mit Network Address Translation (NAT) herstellt. Cisco IOS NAT kann nachfolgende TCP-Verbindungen und UDP-Sitzungen über mehrere Netzwerkverbindungen verteilen, wenn Routen zu einem bestimmten Ziel mit gleichen Kosten verfügbar sind. Falls eine der Verbindungen unbrauchbar wird, kann die Objektverfolgung, eine Komponente von Optimized Edge Routing (OER), verwendet werden, um die Route zu deaktivieren, bis die Verbindung wieder verfügbar wird. Dadurch wird die Netzwerkverfügbarkeit sichergestellt, die von Instabilität oder Unzuverlässigkeit einer Internetverbindung inspiriert ist.



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

Voraussetzungen

Anforderungen

In diesem Dokument wird davon ausgegangen, dass Sie bereits über funktionierende LAN- und WAN-Verbindungen verfügen, und es werden keine Hintergrundinformationen zur Konfiguration oder Fehlerbehebung bereitgestellt, um die erste Verbindung herzustellen.

Dieses Dokument beschreibt keine Möglichkeit zur Unterscheidung zwischen den Routen. Daher ist es nicht möglich, eine wünschenswertere Verbindung einer weniger wünschenswerten Verbindung vorzuziehen.

In diesem Dokument wird beschrieben, wie OER konfiguriert wird, um entweder die Internetroute je nach Erreichbarkeit der DNS-Server des ISP zu aktivieren oder zu deaktivieren. Sie müssen bestimmte Hosts identifizieren, die nur über eine der ISP-Verbindungen erreichbar sind und möglicherweise nicht verfügbar sind, wenn diese ISP-Verbindung nicht verfügbar ist.

Verwendete Komponenten

Diese Konfiguration wurde mit einem Cisco 1811-Router entwickelt, auf dem die Software 12.4(15)T2 Advanced IP Services ausgeführt wird. Wenn eine andere Softwareversion verwendet wird, sind möglicherweise einige Funktionen nicht verfügbar, oder die Konfigurationsbefehle unterscheiden sich möglicherweise von den in diesem Dokument angegebenen. Ähnliche Konfigurationen sollten auf allen Cisco IOS-Router-Plattformen verfügbar sein, auch wenn die Schnittstellenkonfiguration zwischen den verschiedenen Plattformen variieren kann.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netz Live ist, überprüfen Sie, ob Sie die mögliche Auswirkung jedes möglichen Befehls verstehen.

Konventionen

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

Konfigurieren

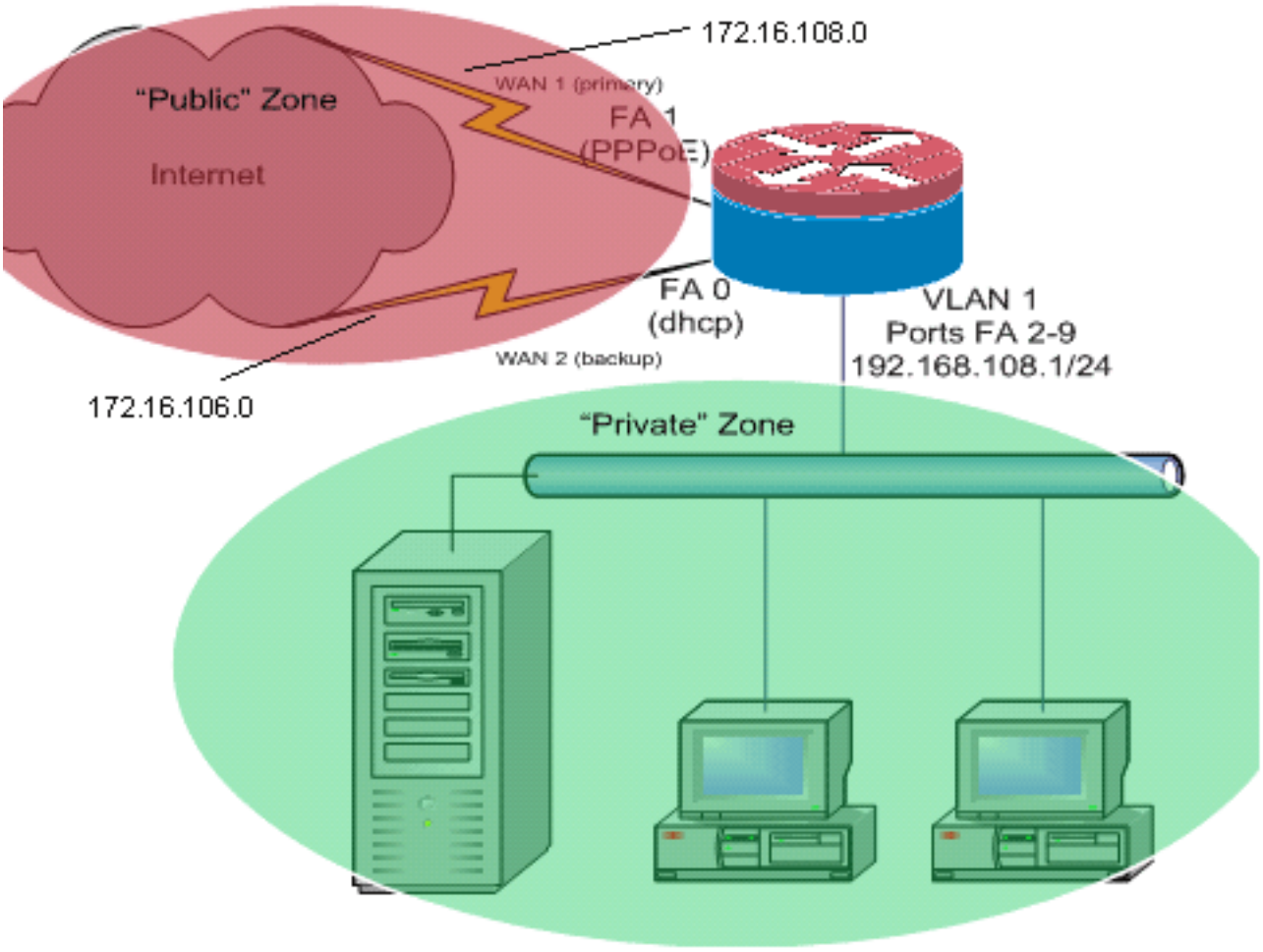
Möglicherweise müssen Sie richtlinienbasiertes Routing für bestimmten Datenverkehr hinzufügen, um sicherzustellen, dass immer eine ISP-Verbindung verwendet wird. Beispiele für Datenverkehr, der dieses Verhalten erfordern könnte, sind IPsec-VPN-Clients, VoIP-Telefone und jeder andere Datenverkehr, der immer nur eine der ISP-Verbindungsoptionen verwenden sollte, um dieselbe IP-Adresse, eine höhere Geschwindigkeit oder eine niedrigere Latenz in der Verbindung vorzuziehen.

In diesem Abschnitt erfahren Sie, wie Sie die in diesem Dokument beschriebenen Funktionen konfigurieren können.

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

Netzwerkdiagramm

In diesem Dokument wird die folgende Netzwerkeinrichtung verwendet:



In diesem Konfigurationsbeispiel wird, wie im Netzwerkdiagramm gezeigt, ein Access Router beschrieben, der eine DHCP-konfigurierte IP-Verbindung mit einem ISP (wie durch FastEthernet 0 dargestellt) und eine PPPoE-Verbindung über die andere ISP-Verbindung verwendet. Die Verbindungstypen haben keine besonderen Auswirkungen auf die Konfiguration, es sei denn, die Objektverfolgung und das Optimized Edge Routing (OER) und/oder das richtlinienbasierte Routing sollen mit einer DHCP-zugewiesenen Internetverbindung verwendet werden. In diesen Fällen kann es sehr schwierig sein, einen Next-Hop-Router für Richtlinien-Routing oder OER zu definieren.

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. Komplexer Anwendungsdatenverkehr (z. B. VoIP-Signalisierung und Medien), der von dieser grundlegenden Richtlinie nicht behandelt wird, wird wahrscheinlich mit eingeschränkter Funktionalität betrieben 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. Sie müssen zusätzliche Firewall-Richtlinienkonfigurationen erstellen, um zusätzlichen Datenverkehr aufzunehmen, der von dieser Basiskonfiguration nicht verarbeitet wird.

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

CLI-Konfiguration

Cisco IOS CLI-Konfiguration

```
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

Verwenden der mit DHCP zugewiesenen Routenverfolgung:

Cisco IOS CLI-Konfiguration

```
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
```

Überprüfung

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. Dieser Befehl stellt sicher, dass interne Hosts in beide NAT-externen Adressen übersetzt werden.

```
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#
```

- **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-Inspektionstätigkeit zwischen Hosts in privaten Zonen und Hosts in öffentlichen Zonen an. Dieser Befehl stellt sicher, dass der Datenverkehr auf den internen Hosts überprüft wird, wenn Hosts mit Diensten in der externen Sicherheitszone kommunizieren.

Fehlerbehebung

Überprüfen Sie diese Elemente, wenn die Verbindungen nach der Konfiguration des Cisco IOS-Routers mit NAT 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.
- Wenn Sie die Routenverfolgung verwenden, überprüfen Sie den Status der Routenverfolgung, um sicherzustellen, dass die Internetverbindungen verfügbar sind.
- Die Firewall-Richtlinie spiegelt genau die Art des Datenverkehrs wider, den Sie über den Router zulassen möchten.

Zugehörige Informationen

- Cisco IOS Firewall
- Befehlsreferenz für Cisco IOS IP Addressing Services - NAT-Befehle
- Firewall-Design und Anwendungshandbuch für zonenbasierte Richtlinien
- Cisco IOS Optimized Edge Routing Configuration Guide, Version 12.4T
- Technischer Support und Dokumentation für Cisco Systeme