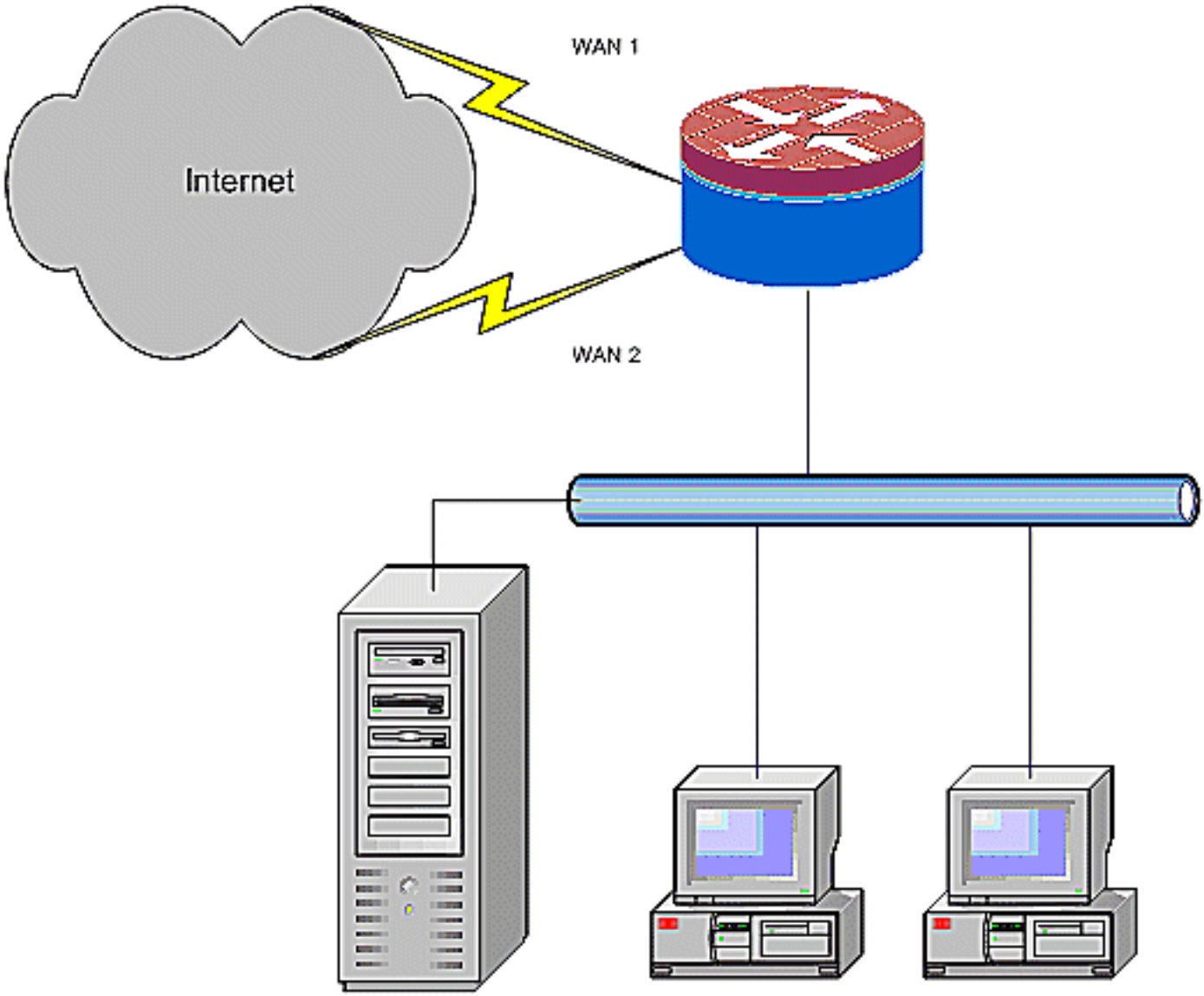
Equilibrio de carga NAT de IOS con firewall de políticas basado en zona para dos conexiones ISP

Contenido

Introducción

Este documento proporciona una configuración de ejemplo para que un router Cisco IOS® conecte una red a Internet con traducción de direcciones de red (NAT) a través de dos conexiones ISP. La NAT del software Cisco IOS puede distribuir las conexiones TCP subsiguientes y las sesiones UDP a través de varias conexiones de red si hay disponibles rutas de igual costo a un destino dado.



Este documento describe la configuración adicional para aplicar el firewall de políticas basado en zona (ZFW) de Cisco IOS para agregar la capacidad de inspección activa (stateful) a fin de aumentar la protección de red básica proporcionada por NAT.

Prerequisites

Requirements

Este documento asume que usted trabaja con conexiones LAN y WAN y no proporciona antecedentes de configuración o resolución de problemas para establecer la conectividad inicial. Este documento no describe una manera de diferenciar entre las rutas, por lo que no hay manera de preferir una conexión más deseable sobre una menos deseable.

Componentes Utilizados

La información de este documento se basa en el Cisco Series 1811 Router con el software 12.4(15)T3 Advanced IP Services. Si se utiliza una versión de software diferente, algunas

funciones no están disponibles o los comandos de configuración pueden diferir de los que se muestran en este documento. Existe una configuración similar disponible en todas las plataformas del router Cisco IOS, aunque la configuración de la interfaz probablemente varía entre las diferentes plataformas.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Convenciones

Consulte Convenciones de Consejos Técnicos de Cisco para obtener más información sobre las convenciones sobre documentos.

Configurar

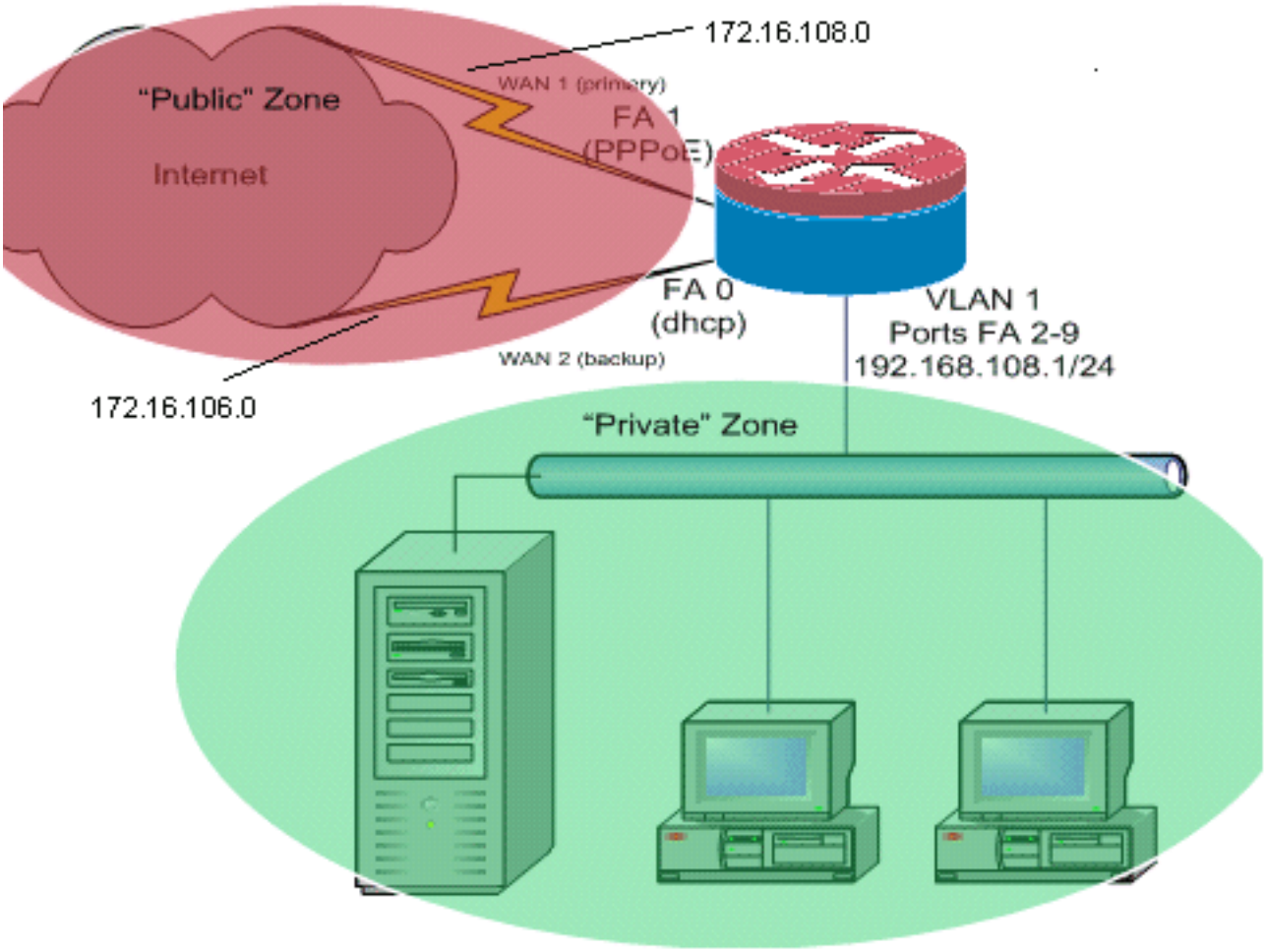
En esta sección encontrará la información para configurar las funciones descritas en este documento.

Nota: Utilice la herramienta Command Lookup (sólo para clientes registrados) para obtener más información sobre los comandos utilizados en esta sección.

Debe agregar el ruteo basado en políticas para tráfico específico para asegurarse de que siempre utiliza una conexión ISP. Entre los ejemplos de tráfico que pueden requerir este comportamiento se incluyen los clientes VPN IPSec, el tráfico de telefonía VoIP y cualquier otro tráfico que utilice sólo una de las opciones de conexión ISP para preferir la misma dirección IP, mayor velocidad o menor latencia en la conexión.

Diagrama de la red

En este documento, se utiliza esta configuración de red:



Este ejemplo de configuración describe un router de acceso que utiliza una conexión IP configurada por DHCP a un ISP (como se muestra en FastEthernet 0) y una conexión PPPoE a través de la otra conexión ISP. Los tipos de conexión no tienen un impacto particular en la configuración, pero algunos tipos de conexiones pueden dificultar el uso de esta configuración en escenarios de fallas específicos. Esto ocurre especialmente en los casos en que se utiliza la conectividad IP a través de un servicio WAN conectado a Ethernet, por ejemplo, los servicios de módem por cable o DSL donde un dispositivo adicional termina la conectividad WAN y proporciona la transferencia Ethernet al router Cisco IOS. En los casos en que se aplica el direccionamiento IP estático, a diferencia de las direcciones asignadas por DHCP o PPPoE, y se produce un error de WAN, de modo que el puerto Ethernet todavía mantiene el link Ethernet al dispositivo de conectividad WAN, el router continúa intentando equilibrar la carga de la conectividad tanto en las conexiones WAN buenas como en las malas. Si su implementación requiere que las rutas inactivas se quiten del balanceo de carga, consulte la configuración proporcionada en Cisco IOS NAT Load-Balancing y Zone-Based Policy Firewall con Optimized Edge Routing para Dos Conexiones de Internet que describe la adición de Optimized Edge Routing para monitorear la validez de la ruta.

Debate sobre la política de firewall

Este ejemplo de configuración describe una política de firewall que permite conexiones simples TCP, UDP e ICMP desde la zona de seguridad "interna" a la zona de seguridad "externa", y acomoda las conexiones FTP salientes y el tráfico de datos equivalente para las transferencias FTP activas y pasivas. Cualquier tráfico de aplicaciones complejo, por ejemplo, la señalización VoIP y los medios, que no se gestiona mediante esta política básica probablemente funcione con una capacidad reducida o pueda fallar por completo. Esta política de firewall bloquea todas las conexiones de la zona de seguridad "pública" a la zona "privada", que incluye todas las

conexiones que se acomodan mediante el reenvío de puertos NAT. Si es necesario, debe ajustar la política de inspección del firewall para reflejar su perfil de aplicación y su política de seguridad.

Si tiene preguntas sobre el diseño y la configuración de políticas de firewall de políticas basadas en zonas, consulte la Guía de diseño y aplicación de firewall de políticas basadas en zonas.

Configuraciones

En este documento, se utilizan estas configuraciones:

Configuración

```
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
```

Verificación

Use esta sección para confirmar que su configuración funciona correctamente.

La herramienta Output Interpreter Tool (clientes registrados solamente) (OIT) soporta ciertos comandos show. Utilice la OIT para ver un análisis del resultado del comando show.

- **show ip nat translation**—Muestra la actividad NAT entre los hosts internos NAT y los hosts externos NAT. Este comando proporciona la verificación de que los hosts internos se traducen a ambas direcciones externas NAT.

```
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**: verifica que estén disponibles varias rutas a Internet.

```
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**: muestra la actividad de inspección del firewall entre hosts de zona "privada" y hosts de zona "pública". Este comando proporciona la verificación de que el tráfico de los hosts internos se inspecciona mientras los hosts se comunican con los servicios en la zona de seguridad "externa".

Troubleshoot

En esta sección encontrará información que puede utilizar para solucionar problemas de configuración.

Después de configurar el router Cisco IOS con NAT, si las conexiones no funcionan, asegúrese de lo siguiente:

- La NAT se aplica correctamente en interfaces externas e internas.
- La configuración NAT está completa y las ACL reflejan el tráfico que se debe NATed.
- Hay disponibles varias rutas a Internet/WAN.
- La política de firewall refleja con precisión la naturaleza del tráfico que desea permitir a través del router.

Información Relacionada

- Soporte de tecnología de voz
- Soporte de Productos de Voice and Unified Communications
- Troubleshooting de Cisco IP Telephony
- Guía de Aplicación y Diseño de Zone-Based Policy Firewall
- Soporte Técnico y Documentación - Cisco Systems