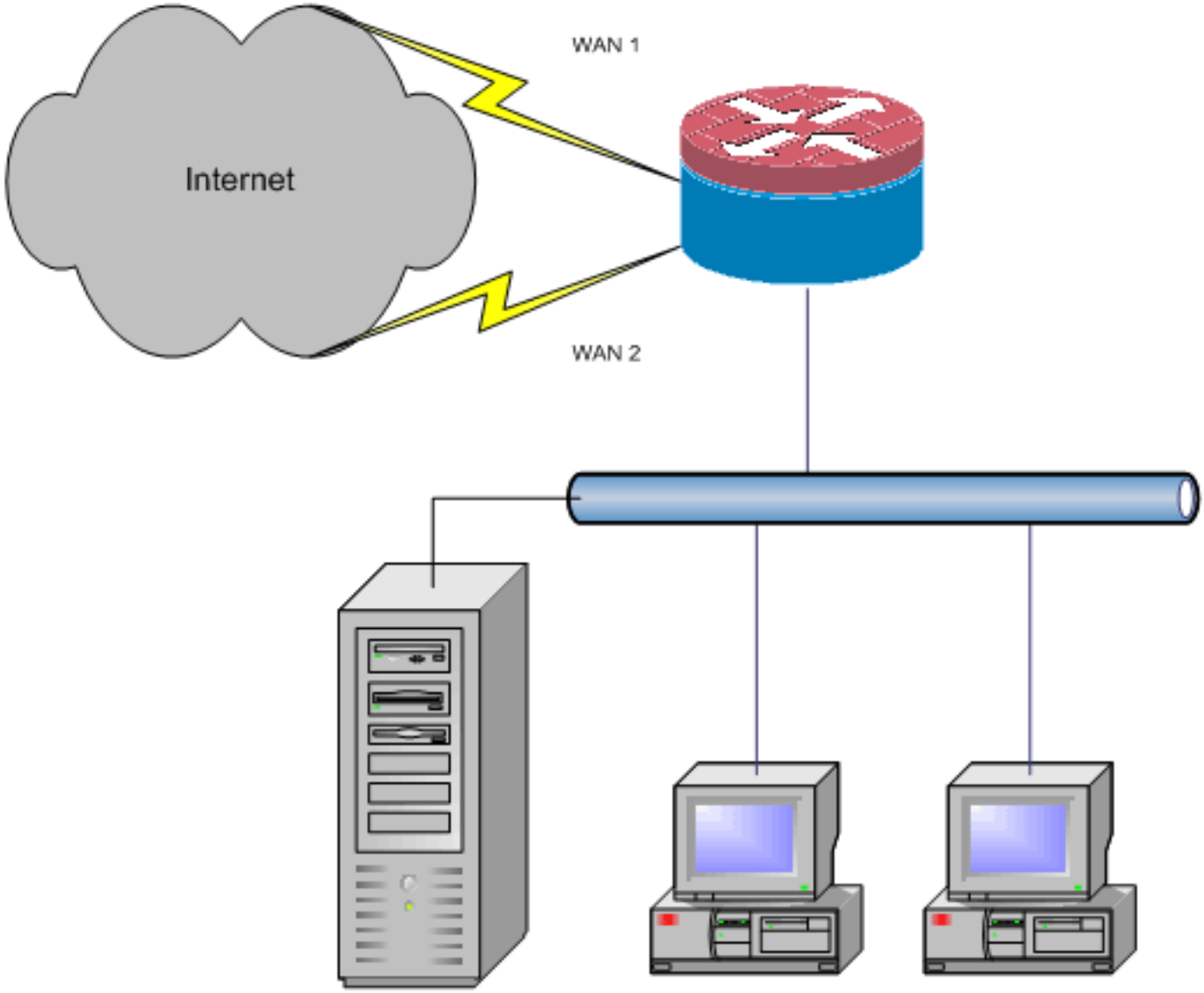
Configuración de Cisco IOS NAT para dos conexiones ISP con OER

Contenido

Introducción

Este documento describe una configuración 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 de 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. En caso de que una de las conexiones deje de utilizarse, se puede utilizar el seguimiento de objetos, un componente de Optimized Edge Routing (OER), para desactivar la ruta hasta que la conexión vuelva a estar disponible, lo que garantiza la disponibilidad de la red en lugar de la inestabilidad o la falta de fiabilidad de una conexión a Internet.



Este documento describe configuraciones adicionales para aplicar el firewall de políticas basado en zona del IOS de Cisco para agregar la capacidad de inspección activa (stateful) para aumentar la protección de red básica proporcionada por NAT.

Prerequisites

Requirements

Este documento asume que ya tiene conexiones LAN y WAN que funcionan y que no proporciona información de configuración o resolución de problemas para establecer la conectividad inicial.

Este documento no describe una manera de diferenciar entre las rutas. Por lo tanto, no hay manera de preferir una conexión más deseable sobre una conexión menos deseable.

Este documento describe cómo configurar OER para habilitar o inhabilitar cualquiera de las rutas de Internet basadas en la disponibilidad de los servidores DNS del ISP. Debe identificar hosts específicos a los que se puede acceder a través de una sola de las conexiones ISP y que podrían no estar disponibles si esa conexión ISP no está disponible.

Componentes Utilizados

Esta configuración se desarrolló con un router Cisco 1811 que ejecuta el software 12.4(15)T2 Advanced IP Services. Si se utiliza una versión de software diferente, es posible que algunas funciones no estén disponibles o que los comandos de configuración difieran de los que se muestran en este documento. Configuraciones similares deberían estar disponibles en todas las plataformas del router Cisco IOS, aunque la configuración de la interfaz probablemente varíe 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

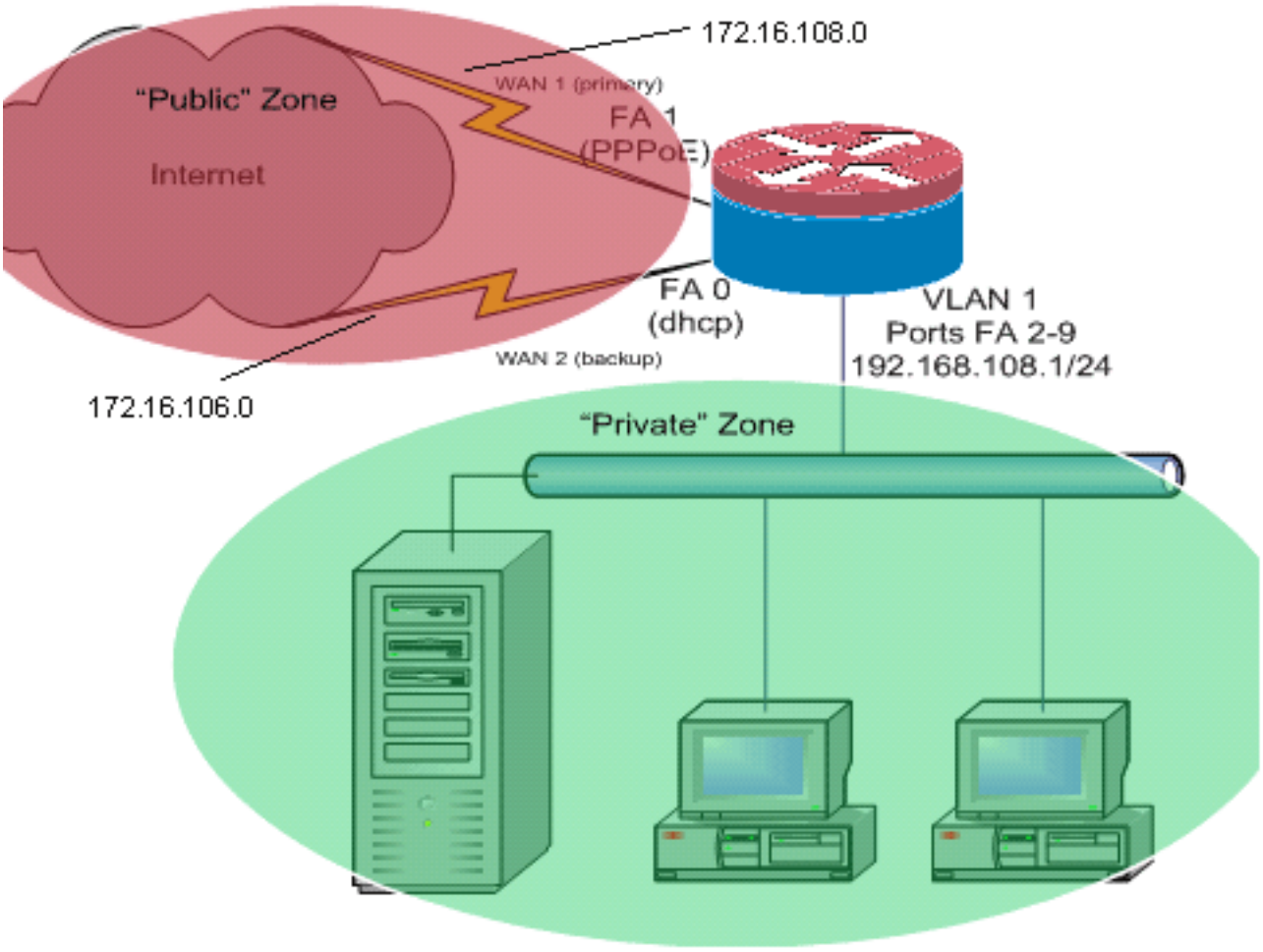
Es posible que deba agregar routing basado en políticas para tráfico específico para asegurarse de que siempre utiliza una conexión ISP. Algunos ejemplos de tráfico que podrían requerir este comportamiento son los clientes VPN IPsec, los auriculares VoIP y cualquier otro tráfico que siempre debería utilizar sólo una de las opciones de conexión ISP para preferir la misma dirección IP, mayor velocidad o menor latencia en la conexión.

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.

Diagrama de la red

En este documento, se utiliza esta configuración de red:



Este ejemplo de configuración, como se ilustra en el diagrama de red, 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 sobre la otra conexión ISP. Los tipos de conexión no tienen un impacto particular en la configuración, a menos que se utilicen el seguimiento de objetos y el enrutamiento de borde optimizado (OER) o basado en políticas con una conexión a Internet asignada por DHCP. En estos casos, puede ser muy difícil definir un router de salto siguiente para el ruteo de políticas u OER.

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 correspondiente para las transferencias FTP activas y pasivas. Cualquier tráfico de aplicaciones complejo (por ejemplo, medios y señalización VoIP) que no se gestione mediante esta política básica probablemente funcionará con una capacidad reducida o puede que falle 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 con el reenvío de puertos NAT. Debe construir configuraciones de políticas de firewall adicionales para alojar el tráfico adicional que no se controla con esta configuración básica.

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 basado en zonas.

Configuración de CLI

Configuración de CLI de Cisco IOS

```
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

Utilice el seguimiento de la ruta asignada por dhcp:

Configuración de CLI de Cisco IOS

```
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
```

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 están traduciendo a ambas direcciones externas NAT.

```
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**: 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 en los hosts interiores se inspecciona mientras los hosts se comunican con los servicios en la zona de seguridad externa.

Troubleshoot

Verifique estos elementos si las conexiones no funcionan después de configurar el router Cisco IOS con NAT:

- 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.
- Si utiliza el seguimiento de rutas, verifique el estado del seguimiento de rutas para asegurarse de que las conexiones de Internet estén disponibles.
- La política de firewall refleja con precisión la naturaleza del tráfico que desea permitir a través del router.

Información Relacionada

- Cisco IOS Firewall
- Referencia de Comandos de IP Addressing Services de Cisco IOS - Comandos NAT
- Guía de Aplicación y Diseño de Zone-Based Policy Firewall
- Guía de Configuración de Optimized Edge Routing de Cisco IOS, Versión 12.4T
- Soporte Técnico y Documentación - Cisco Systems