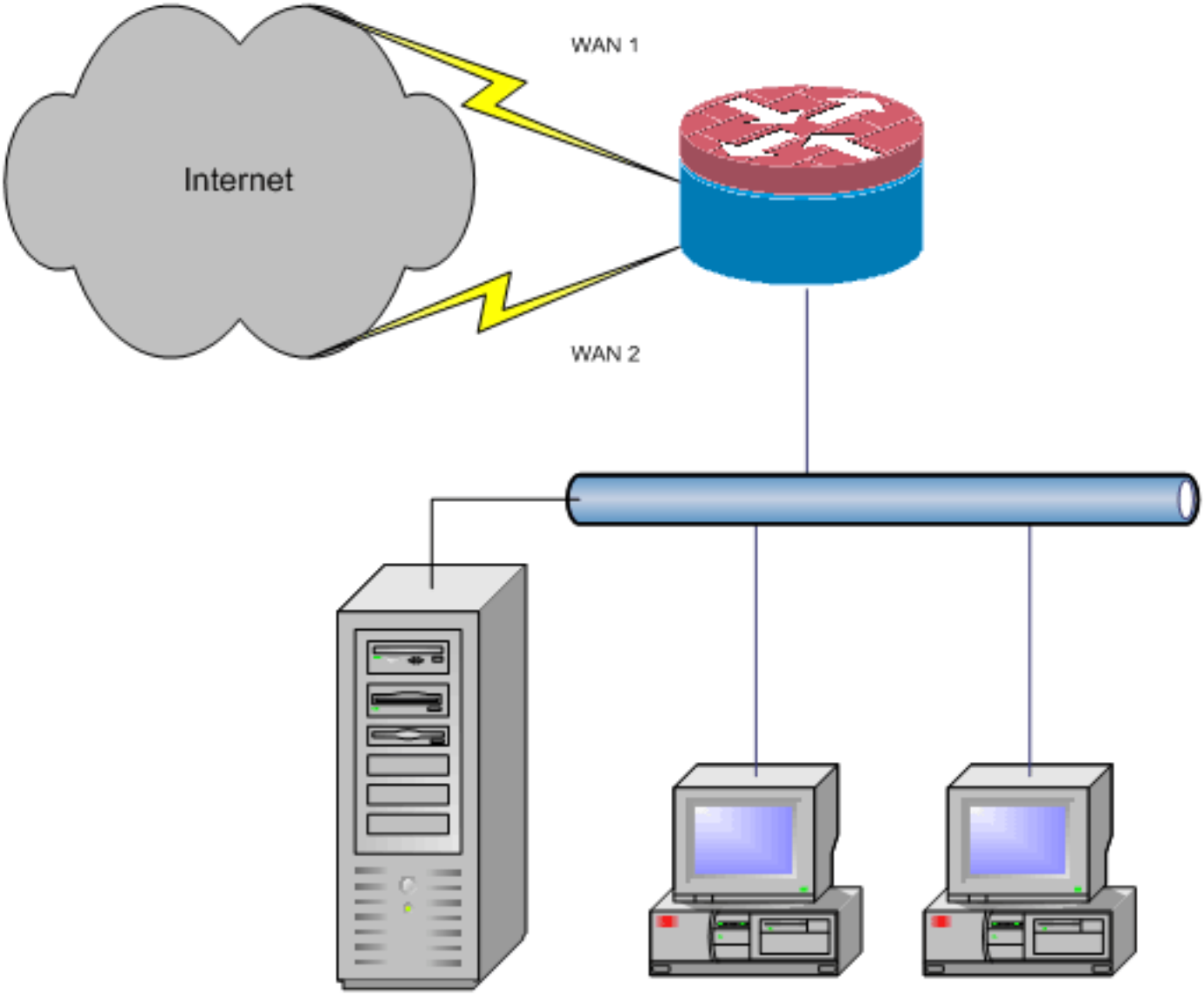
Balanceo de carga IOS NAT y Firewall Zona-basado de la directiva con el Edge Routing optimizado para dos conexiones de Internet

Contenido

Introducción

Este documento describe una configuración para que un router del ® del Cisco IOS conecte una red con Internet con el Network Address Translation (NAT) vía dos Conexiones ISP. El Cisco IOS NAT puede distribuir las conexiones TCP y a las Sesiones UDP subsiguientes sobre las conexiones de Red múltiple si las rutas de igual costo a un destino determinado están disponibles. En caso que una de las conexiones llegue a estar inutilizable, el Rastreo de objetos, un componente del Edge Routing optimizado (OER), se puede utilizar para desactivar la ruta hasta que la conexión esté disponible otra vez, que asegura la disponibilidad de la red a pesar de la inestabilidad o la falta de fiabilidad de una conexión de Internet.



Este documento describe las configuraciones adicionales para aplicar el Firewall Zona-basado Cisco IOS de la directiva para agregar la capacidad de la inspección con estado para aumentar la protección de la red básica proporcionada por el NAT.

prerrequisitos

Requisitos

Este documento asume que usted tiene el LAN y conexiones WAN que funcionen y que no proporciona ya el fondo de la configuración o del troubleshooting para establecer la conectividad inicial.

Este documento no describe una manera de distinguir 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 cualquier Internet ruta-basado en el accesibilidad de los servidores DNS ISP. Usted necesita identificar los host específicos que son accesibles vía solamente uno de las Conexiones ISP y no pudieron estar disponibles si esa Conexión ISP no está disponible.

Componentes Utilizados

Esta configuración fue desarrollada con un Cisco 1811 Router que funciona con el software avanzado 12.4(15)T2 de los Servicios IP. Si se utiliza una diversa versión de software, algunas características pueden no estar disponibles, o los comandos configuration pudieron diferenciar de ésos mostrados en este documento. Las configuraciones similares deben estar disponibles en todas las plataformas del router del Cisco IOS, aunque la configuración de la interfaz varíe probablemente entre diversas Plataformas.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Convenciones

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

Configurar

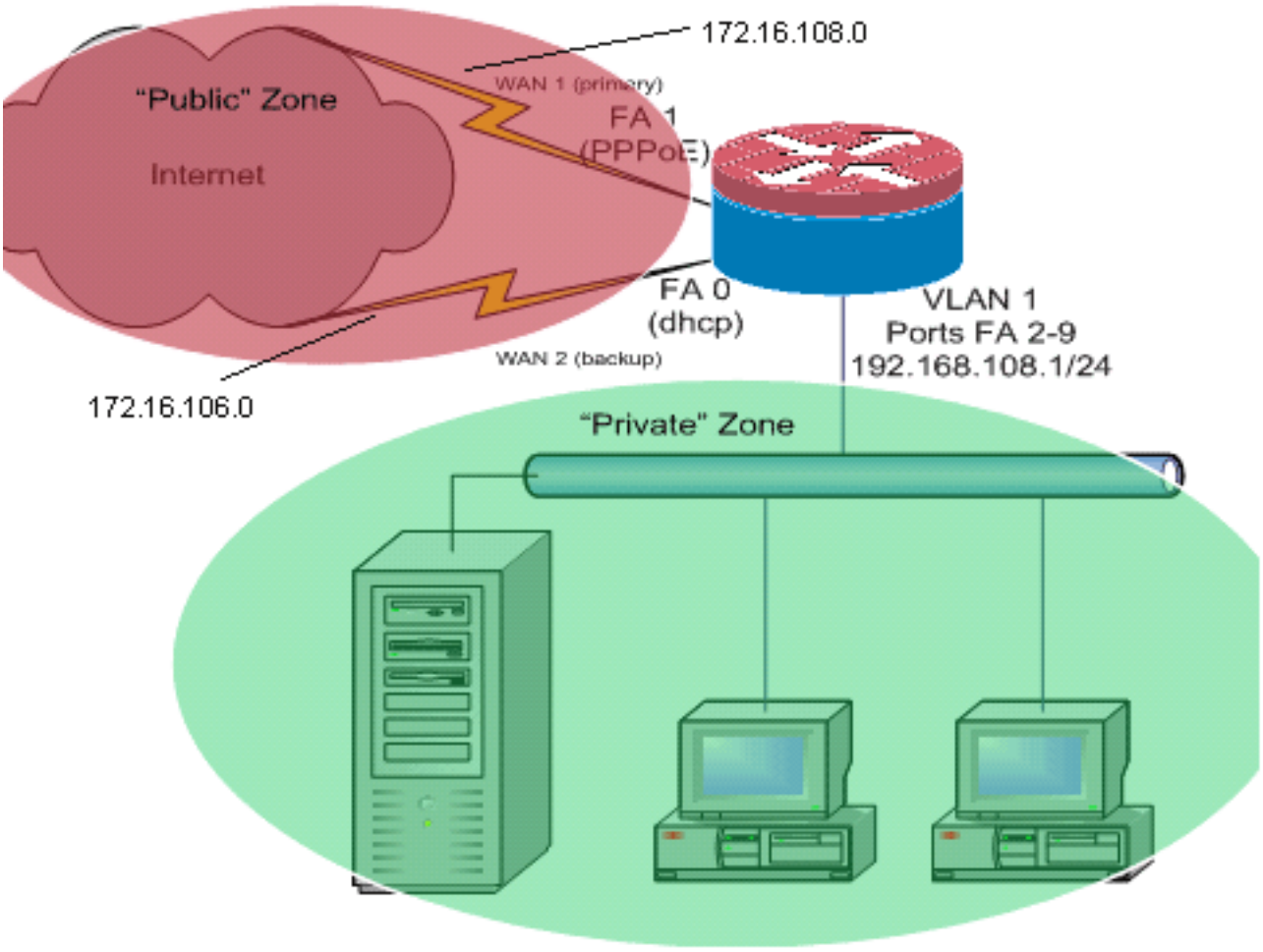
Usted puede ser que necesite agregar el Policy-Based Routing para que el tráfico específico esté seguro que utiliza siempre una Conexión ISP. Los ejemplos del tráfico que pudieron requerir este comportamiento incluyen los clientes del IPSec VPN, los microteléfonos VoIP, y cualquier otro tráfico que deba utilizar siempre solamente uno de las opciones de Conexión ISP para preferir la misma dirección IP, una velocidad más alta, o para bajar el tiempo de espera en la conexión.

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

Nota: Utilice la herramienta Command Lookup Tool (clientes registrados solamente) 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 la red, describe un router de acceso que utilice una conexión IP DHCP-configurada a un ISP (como se muestra por el FastEthernet 0) y una conexión PPPoE sobre la otra Conexión ISP. Los Tipos de conexión no tienen ningún impacto determinado en la configuración, a menos que se vaya el Rastreo de objetos y el Edge Routing optimizado (OER) y/o el Policy-Based Routing a ser utilizado con una conexión de Internet DHCP-asignada. En estos casos, puede ser muy difícil definir a un Next Hop Router para el Policy Routing u OER.

Discusión de políticas del firewall

Este ejemplo de configuración describe las políticas del firewall que permiten las conexiones simples TCP, UDP, y ICMP de la zona de Seguridad del “interior” a la zona de Seguridad del “exterior” y acomodan las conexiones FTP salientes y el tráfico de datos correspondientes para las transferencias del active y del FTP pasivo. Cualquier tráfico de la aplicación compleja (por ejemplo, señalización VoIP y los media) que no es dirigido por esta política básica actuará probablemente con la capacidad disminuida, o puede fallar totalmente. Estas políticas del firewall bloquean todas las conexiones de la zona de Seguridad “pública” a la zona “privada”, que incluye todas las conexiones que sean acomodadas por la expedición del puerto de NAT. Usted debe construir las configuraciones adicionales de las políticas del firewall para acomodar el tráfico adicional que no es manejado por esta configuración básica.

Si usted tiene preguntas sobre el diseño y la configuración de políticas del firewall de la directiva Zona-Basar, refiera al diseño del Firewall de la directiva y a la guía Zona-basados de la aplicación.

Configuración de CLI

Configuración del Cisco IOS CLI

```
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 DHCP-asignado de la ruta:

Configuración del Cisco IOS CLI
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.

- **muestre a IP la traducción nacional** — Actividad de las visualizaciones NAT entre los host interiores NAT y los host exteriores NAT. Este comando proporciona la verificación que los host interiores 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#`
- **ruta de IP de la demostración** — Verifica que las rutas múltiples a Internet estén disponibles.`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`
- **el tipo del directiva-mapa de la demostración examina las sesiones de los zona-pares** — Actividad del examen del Firewall de las visualizaciones entre los host de la soldado-zona y los host de la público-zona. Este comando proporciona la verificación que el tráfico en los host interiores está examinado mientras que los host comunican con los servicios en la zona de seguridad externa.

Troubleshooting

Verifique estos elementos si las conexiones no trabajan después de que usted configure al router del Cisco IOS con el NAT:

- El NAT se aplica apropiadamente en el exterior y las interfaces interiores.
- La configuración del NAT es completa, y los ACL reflejan el tráfico que debe ser NATed.
- Las rutas múltiples al Internet/WAN están disponibles.
- Si usted utiliza la ruta que sigue, marque el estado de la ruta que sigue para asegurarse que las conexiones de Internet están disponibles.
- Las políticas del firewall reflejan exactamente la naturaleza del tráfico que usted desea

permitir a través del router.

Información Relacionada

- Cisco IOS Firewall
- Referencia de comandos de los Servicios de direccionamiento IP del Cisco IOS - Comandos nat
- Diseño del Firewall de la directiva y guía Zona-basados de la aplicación
- Guía de configuración optimizada Cisco IOS del Edge Routing, versión 12.4T
- Soporte Técnico y Documentación - Cisco Systems