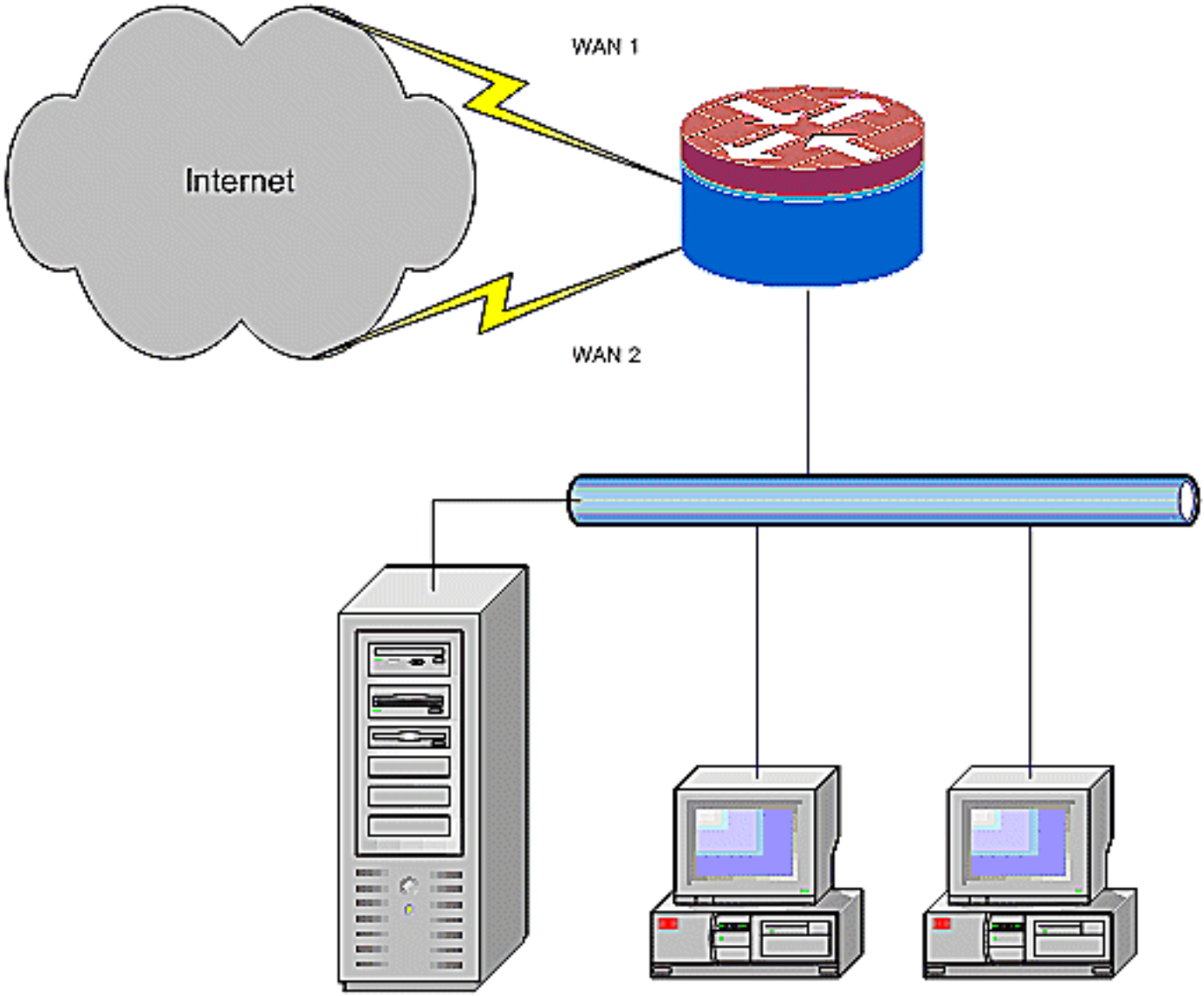
Balanceo de carga IOS NAT con el Firewall Zona-basado de la directiva para dos Conexiones ISP

Contenido

Introducción

Este documento proporciona una configuración de muestra para que un router del ® del Cisco IOS conecte una red con Internet con el Network Address Translation (NAT) a través de dos Conexiones ISP. El Cisco IOS Software 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.



Este documento describe la configuración adicional para aplicar el Firewall Zona-basado Cisco IOS de la directiva (ZFW) 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 le asume trabajo con el LAN y las conexiones WAN y no proporciona el fondo de la configuración o del troubleshooting para establecer la conectividad inicial. Este documento no describe una manera de distinguir entre las rutas, tan allí no es ninguna manera de preferir una conexión más deseable sobre una conexión menos deseable.

Componentes Utilizados

La información en este documento se basa en el 1811 Router del Cisco Series con el software avanzado 12.4(15)T3 de los Servicios IP. Si se utiliza una diversa versión de software, algunas

características no están disponibles, o los comandos configuration pueden diferenciar de ésos mostrados en este documento. La configuración similar está disponible 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

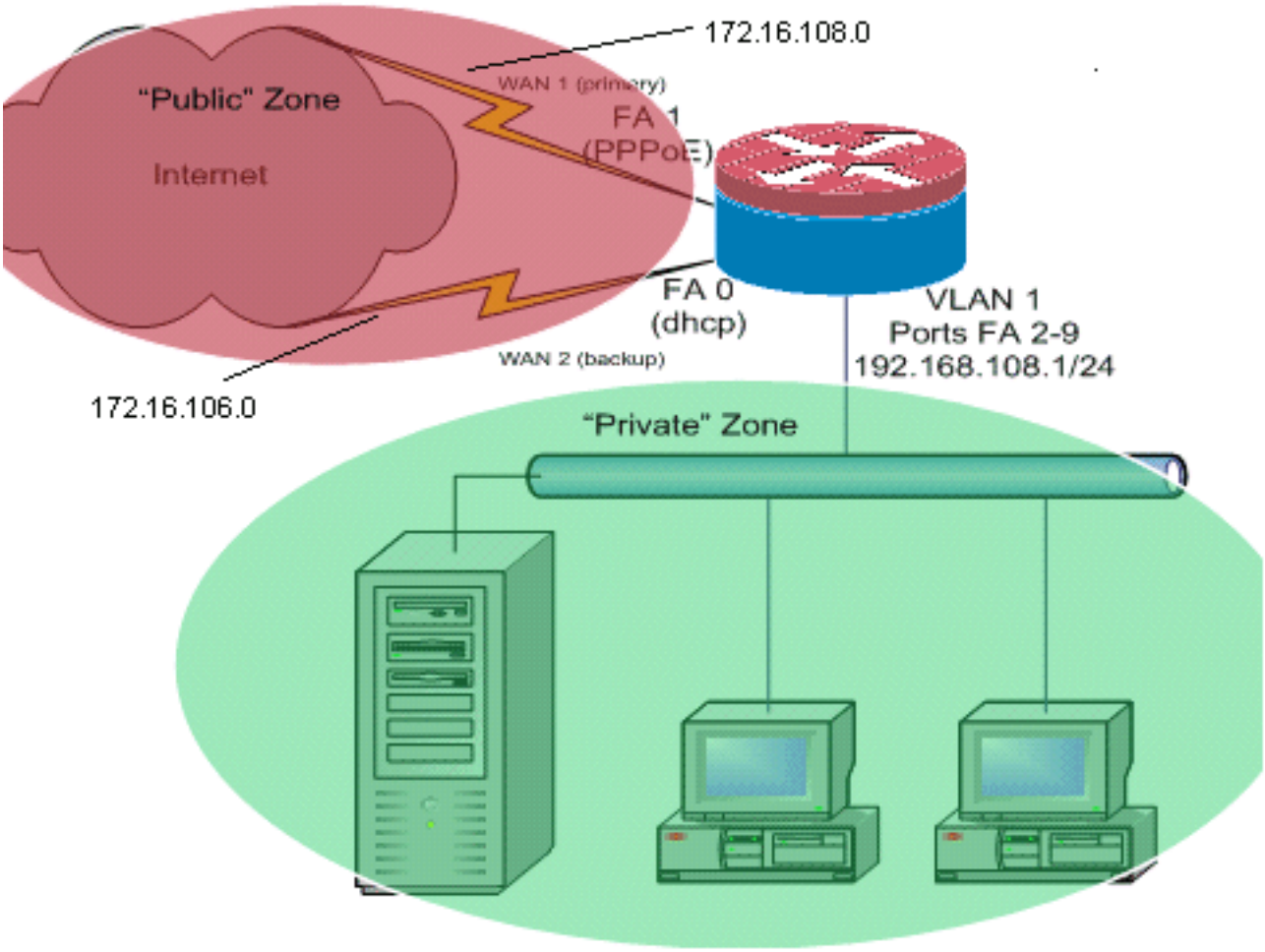
En esta sección encontrará la información para configurar las funciones descritas en este documento.

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

Usted necesita agregar el Policy-Based Routing para que el tráfico específico esté seguro que utiliza siempre una Conexión ISP. Los ejemplos del tráfico que pueden requerir este comportamiento incluyen el tráfico de los clientes del IPSec VPN, de la telefonía VoIP, y cualquier otro tráfico que utilice 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.

Diagrama de la red

En este documento, se utiliza esta configuración de red:



Este ejemplo de configuración 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, pero los tipos de algunas conexiones pueden obstaculizar la utilidad de esta configuración en los escenarios de falla específicos. Esto ocurre determinado en caso de que la conectividad del IP sobre un servicio PÁLIDO Ethernet-conectado se utiliza, por ejemplo, módem de cable o los servicios DSL donde un dispositivo adicional termina la conectividad WAN y proporciona la mano-apagado de los Ethernetes al router del Cisco IOS. En caso de que IP estático la dirección sea aplicada, en comparación con los direccionamientos DHCP-asignados o el PPPoE, y ocurre una Falla de WAN, tal que el acceso de Ethernet todavía mantiene el link Ethernet al dispositivo de la conectividad WAN, el router continúa intentando a la Conectividad del balance de la carga a través de las buenas y malas conexiones WAN. Si su despliegue requiere que las rutas inactivas estén quitadas del balanceo de carga, refiera a la configuración proporcionada en el balanceo de carga del Cisco IOS NAT y el Firewall Zona-basado de la directiva del Edge Routing optimizado para dos conexiones de Internet que describe la adición de Edge Routing optimizado para monitorear la validez de la ruta.

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 acomoda las conexiones FTP salientes y el tráfico de datos equivalentes para las transferencias del active y del FTP pasivo. Cualquier tráfico de la aplicación compleja, por ejemplo, señalización VoIP y el media, que no es manejado por esta política básica actúa con la capacidad disminuida o puede probablemente 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 puerto-expedición NAT. En caso necesario, usted necesita ajustar la directiva del examen del Firewall para reflejar su perfil de aplicación y política de seguridad.

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

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.

- **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 están traducidos 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#`

- **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 el “soldado” - divida los host y el “público en zonas” - divida los host en zonas. Este comando proporciona la verificación que el tráfico de los host interiores está examinado mientras que los host comunican con los servicios en la zona de Seguridad del “exterior”.

Troubleshooting

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

Después de que usted configure al router del Cisco IOS con el NAT, si las conexiones no trabajan, esté seguro de éstos:

- 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.
- Las políticas del firewall reflejan exactamente la naturaleza del tráfico que usted 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
- Diseño del Firewall de la directiva y guía Zona-basados de la aplicación
- Soporte Técnico y Documentación - Cisco Systems