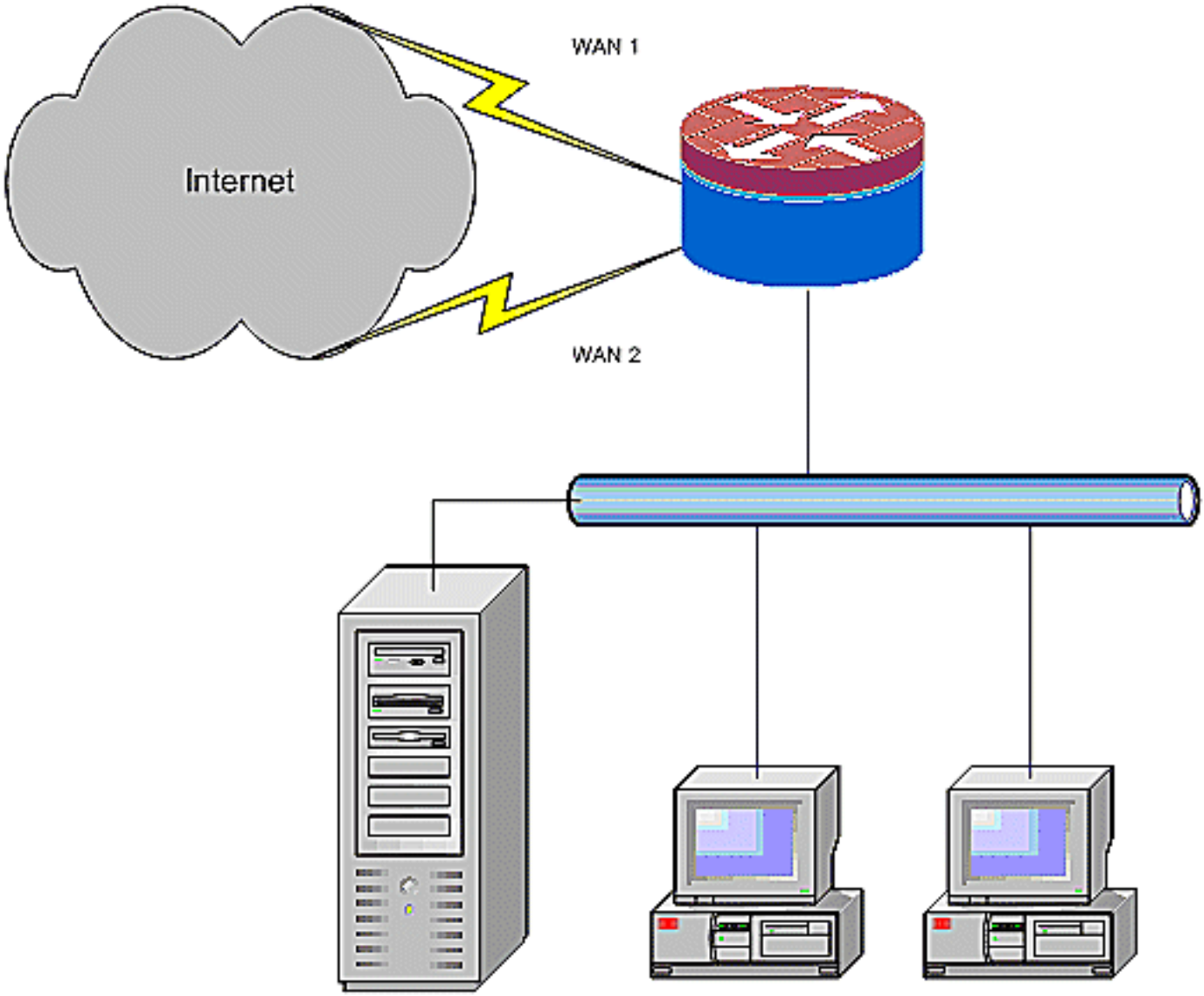
Balanceamento de Carga NAT do IOS com Firewall de Política Baseado em Zona para Duas Conexões ISP

Contents

Introduction

Este documento fornece uma configuração de exemplo para um roteador Cisco IOS® conectar uma rede à Internet com Network Address Translation (NAT) através de duas conexões ISP. A NAT do software Cisco IOS pode distribuir conexões TCP subsequentes e sessões UDP sobre várias conexões de rede se rotas de custo igual para um determinado destino estiverem disponíveis.



Este documento descreve a configuração adicional para aplicar o Cisco IOS Zone-Based Policy Firewall (ZFW) para adicionar o recurso de inspeção stateful para aumentar a proteção básica da rede fornecida pelo NAT.

Prerequisites

Requirements

Este documento pressupõe que você trabalhe com conexões de LAN e WAN e não fornece configuração ou plano de fundo de solução de problemas para estabelecer a conectividade inicial. Este documento não descreve uma maneira de diferenciar entre as rotas, portanto, não há como preferir uma conexão mais desejável em vez de uma conexão menos desejável.

Componentes Utilizados

As informações neste documento são baseadas no Cisco Series 1811 Router com software de Serviços IP Avançados 12.4(15)T3. Se uma versão de software diferente for usada, alguns

recursos não estarão disponíveis ou os comandos de configuração poderão ser diferentes dos mostrados neste documento. Configuração semelhante está disponível em todas as plataformas do roteador Cisco IOS, embora a configuração da interface provavelmente varie entre plataformas diferentes.

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.

Conventions

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

Configurar

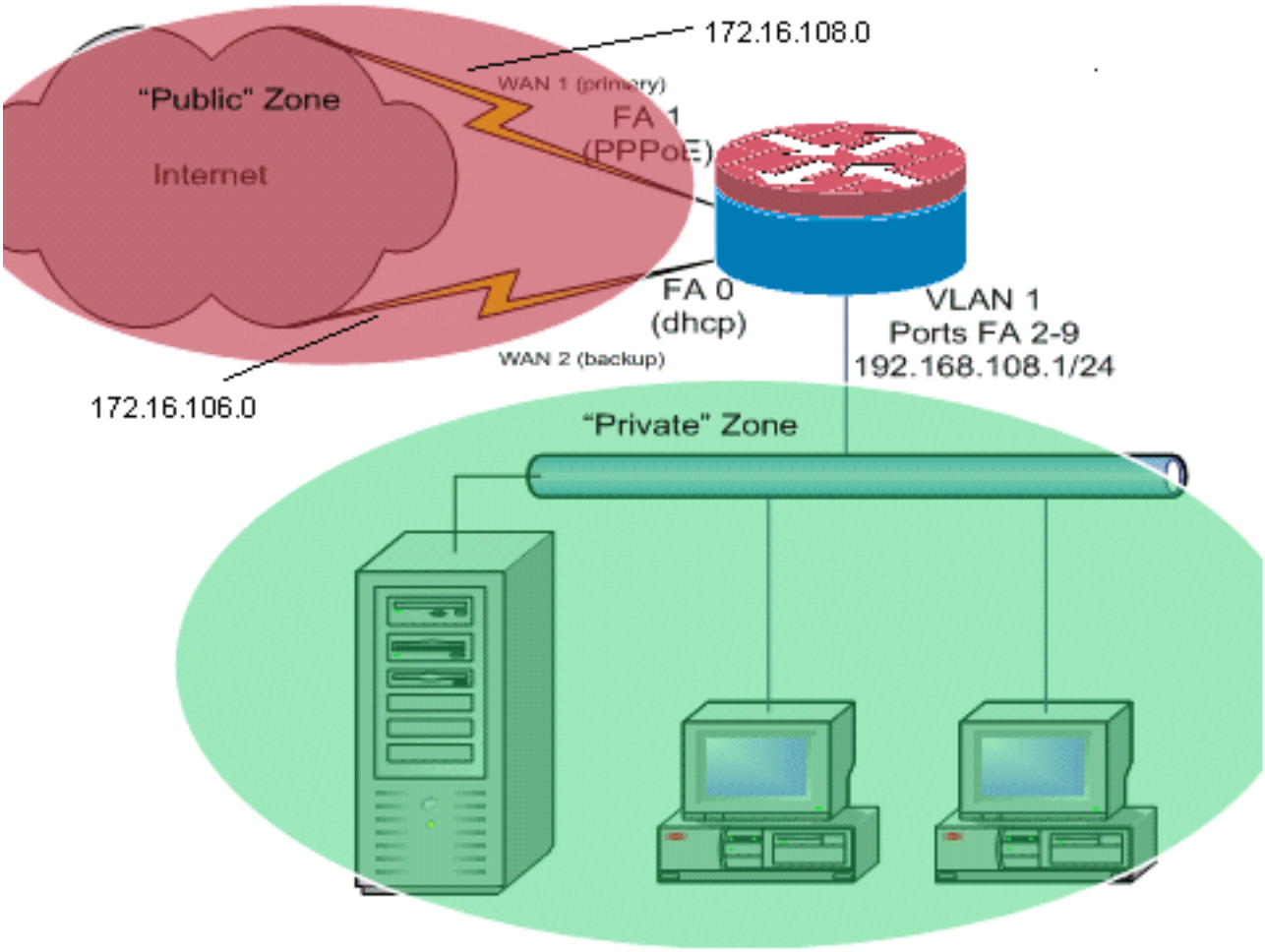
Nesta seção, você encontrará informações para configurar os recursos descritos neste documento.

Nota: Use a Command Lookup Tool (somente clientes registrados) para obter mais informações sobre os comandos usados nesta seção.

Você precisa adicionar roteamento baseado em políticas para tráfego específico para ter certeza de que ele sempre usa uma conexão ISP. Exemplos de tráfego que podem exigir esse comportamento incluem clientes VPN IPSec, tráfego de telefonia VoIP e qualquer outro tráfego que use apenas uma das opções de conexão do ISP para preferir o mesmo endereço IP, maior velocidade ou menor latência na conexão.

Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:



Este exemplo de configuração descreve um roteador de acesso que usa uma conexão IP configurada por DHCP para um ISP (como mostrado pela FastEthernet 0) e uma conexão PPPoE sobre a outra conexão do ISP. Os tipos de conexão não têm nenhum impacto particular na configuração, mas alguns tipos de conexões podem impedir a usabilidade dessa configuração em cenários de falha específicos. Isso ocorre principalmente nos casos em que a conectividade IP sobre um serviço de WAN conectado a Ethernet é usada, por exemplo, modem a cabo ou serviços DSL em que um dispositivo adicional termina a conectividade de WAN e fornece entrega Ethernet para o roteador Cisco IOS. Nos casos em que o endereçamento IP estático é aplicado, ao contrário dos endereços atribuídos por DHCP ou PPPoE, e ocorre uma falha na WAN, de modo que a porta Ethernet ainda mantém o enlace Ethernet para o dispositivo de conectividade da WAN, o roteador continua tentando balancear a carga da conectividade em conexões WAN boas e ruins. Se sua implantação exigir que as rotas inativas sejam removidas do balanceamento de carga, consulte a configuração fornecida no Cisco IOS NAT Load-Balancing e Zone-Based Policy Firewall com Otimized Edge Routing For Two Internet Connections que descreve a adição de Otimized Edge Routing para monitorar a validade da rota.

Discussão sobre política de firewall

Este exemplo de configuração descreve uma política de firewall que permite conexões TCP, UDP e ICMP simples da zona de segurança "interna" para a zona de segurança "externa" e acomoda conexões FTP de saída e o tráfego de dados equivalente para transferências FTP ativas e passivas. Qualquer tráfego de aplicativo complexo, por exemplo, sinalização e mídia VoIP, que não seja tratado por essa política básica, provavelmente opera com capacidade reduzida ou pode falhar completamente. Essa política de firewall bloqueia todas as conexões da zona de segurança "pública" para a zona "privada", que inclui todas as conexões acomodadas pelo encaminhamento de portas NAT. Se necessário, você precisa ajustar a política de inspeção de firewall para refletir

o perfil do aplicativo e a política de segurança.

Se tiver dúvidas sobre o design e a configuração da política do firewall de política baseada em zona, consulte o Guia de design e aplicação do firewall de política baseado em zona.

Configurações

Este documento utiliza as seguintes configurações:

Configuração

```
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
```

Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

A Output Interpreter Tool (somente clientes registrados) (OIT) oferece suporte a determinados comandos show. Use a OIT para exibir uma análise da saída do comando show.

- **show ip nat translation** —Exibe a atividade de NAT entre os hosts internos de NAT e os hosts externos de NAT. Esse comando fornece verificação de que os hosts internos são convertidos para ambos os endereços externos de 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 se várias rotas para a Internet estão disponíveis.

```
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** — Exibe a atividade de inspeção de firewall entre hosts de zona "privada" e hosts de zona "pública". Esse comando fornece verificação de que o tráfego de hosts internos é inspecionado como hosts que se comunicam com serviços na zona de segurança "externa".

Troubleshoot

Esta seção fornece informações que podem ser usadas para o troubleshooting da sua configuração.

Depois de configurar o roteador Cisco IOS com NAT, se as conexões não funcionarem, certifique-se dos seguintes:

- O NAT é aplicado adequadamente em interfaces internas e externas.
- A configuração de NAT está completa e as ACLs refletem o tráfego que deve ser NAT.
- Várias rotas para a Internet/WAN estão disponíveis.
- A política de firewall reflete precisamente a natureza do tráfego que você deseja permitir através do roteador.

Informações Relacionadas

- Suporte à Tecnologia de Voz
- Suporte aos produtos de Voz e Comunicações Unificadas
- Troubleshooting da Telefonia IP Cisco
- Guia de aplicativos e design de firewall de política baseada em zona
- Suporte Técnico e Documentação - Cisco Systems