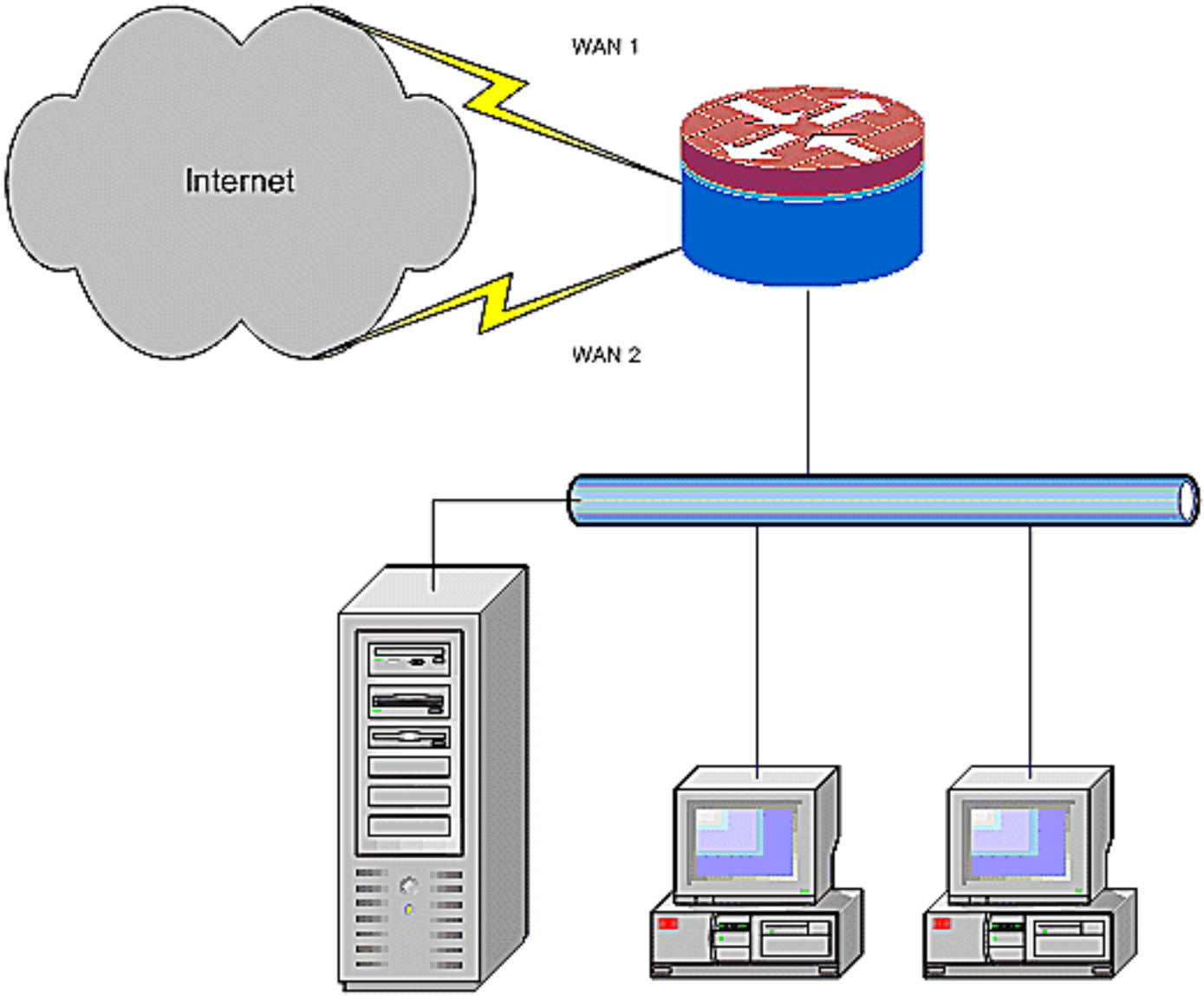
Função de balanceamento de carga IO NAT com o Firewall Zona-baseado da política para duas conexões ISP

Índice

Introdução

Este documento fornece uma configuração de exemplo para que um roteador do ® do Cisco IOS conecte uma rede ao Internet com o Network Address Translation (NAT) através de duas conexões ISP. O Cisco IOS Software NAT pode distribuir conexões de TCP e sessões de UDP subsequentes sobre conexões de rede múltipla se as rotas de custo igual a um destino fornecido estão disponíveis.



Este documento descreve a configuração adicional para aplicar o Firewall Zona-baseado Cisco IOS da política (ZFW) para adicionar a capacidade da inspeção stateful de aumentar a proteção da rede básica fornecida pelo NAT.

Pré-requisitos

Requisitos

Este documento supõe-no trabalho com LAN e conexões de WAN e não o fornece o fundo da configuração ou do Troubleshooting para estabelecer a conectividade inicial. Este documento não descreve uma maneira de diferenciar-se entre as rotas, tão lá é nenhuma maneira de preferir uma conexão mais desejável sobre uma conexão menos desejável.

Componentes Utilizados

A informação neste documento é baseada no 1811 Router do Cisco Series com software avançado 12.4(15)T3 dos Serviços IP. Se uma versão de software diferente é usada, algumas

características não estão disponíveis, ou os comandos configuration podem diferir daqueles mostrados neste documento. A configuração similar está disponível em todas as plataformas de roteador do Cisco IOS, embora a configuração da interface varie provavelmente entre Plataformas diferentes.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Convenções

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

Configurar

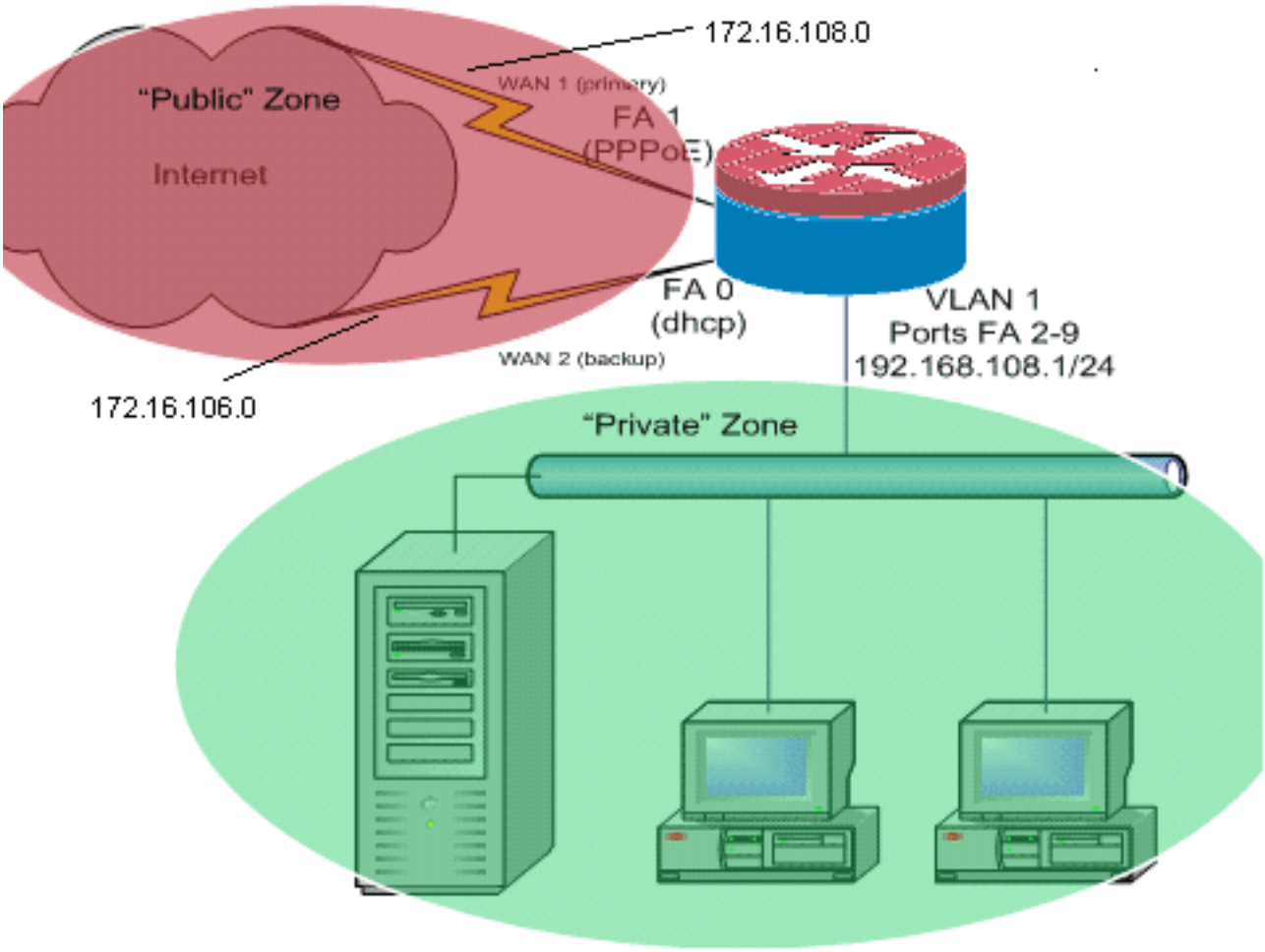
Nesta seção, você encontrará informações para configurar os recursos descritos neste documento.

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

Você precisa de adicionar para ter certeza o roteamento baseado em política para o tráfego específico que usa sempre uma conexão ISP. Os exemplos do tráfego que podem exigir este comportamento incluem o tráfego dos clientes do IPSec VPN, da telefonia de VoIP, e o todo o outro tráfego que usar somente uma das opções de conexão ISP para preferir o mesmo endereço IP de Um ou Mais Servidores Cisco ICM NT, uma velocidade mais alta, ou para abaixar a latência na conexão.

Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:



Este exemplo de configuração descreve um roteador de acesso que use uma conexão IP DHCP-configurada a um ISP (como mostrado pelos FastEthernet 0), e uma conexão PPPoE sobre a outra conexão ISP. Os tipos de conexão não têm nenhum impacto particular na configuração, mas os tipos de algumas conexões podem impedir a usabilidade desta configuração em cenários de falha específicos. Isto ocorre particularmente nos casos onde a conectividade IP sobre um serviço MACILENTO Ethernet-conectado é usada, por exemplo, modem a cabo ou serviços DSL onde um dispositivo adicional termina a conectividade de WAN e fornece a mão-fora dos Ethernet ao roteador do Cisco IOS. Nos casos onde o endereçamento do IP Estático é aplicado, ao contrário dos endereços DHCP-atribuídos ou do PPPoE, e uma falha WAN ocorre, tal que a porta Ethernet ainda mantém ligações de Ethernet ao dispositivo da conectividade de WAN, o roteador continua a tentar à Conectividade do balanceamento de carga através das boas e conexões de WAN ruins. Se seu desenvolvimento exige que as rotas inativas estejam removidas da função de balanceamento de carga, refira a configuração fornecida na função de balanceamento de carga do Cisco IOS NAT e no Firewall Zona-baseado da política com o roteamento de extremidade aperfeiçoado para duas conexões com o Internet que descreve a adição de roteamento de extremidade aperfeiçoado para monitorar a validez da rota.

Discussão de política de firewall

Este exemplo de configuração descreve uma política de firewall que permita conexões simples TCP, UDP, e ICMP da zona de Segurança do “interior” à zona de Segurança da “parte externa”, e acomoda conexões de FTP de partida e o tráfego de dados equivalente para transferências do active e do FTP passivo. Todo o tráfego do aplicativo complexo, por exemplo, sinalização voip e media, que não é segurado por esta política básica provavelmente opera-se com capacidade diminuída ou pode-se falhar inteiramente. Esta política de firewall obstrui todas as conexões da zona de Segurança “pública” à zona “privada”, que inclui todas as conexões que são acomodadas

pela porta-transmissão NAT. Caso necessário, você precisa de ajustar a política da inspeção do Firewall para refletir seus perfil do aplicativo e política de segurança.

Se você tem perguntas no projeto e na configuração de política de firewall da política Zona-Basear, refira o guia Zona-baseado do projeto e do aplicativo do Firewall da política.

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 (apenas para clientes registrados) (OIT) suporta determinados comandos show. Use a OIT para exibir uma análise da saída do comando show.

- **mostre a IP a tradução nat** — Atividade dos indicadores NAT entre host internos NAT e host exteriores NAT. Este comando fornece a verificação que os host internos estão traduzidos a ambos os endereços exteriores 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#
```

- **mostre a rota IP** — Verifica que as rotas múltiplas ao 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`
- **o tipo do mapa de política da mostra inspeciona sessões dos zona-pares** — Atividade da inspeção do Firewall dos indicadores entre “privado” - divida anfitriões e “público” - divida anfitriões. Este comando fornece a verificação que o tráfego dos host internos está inspecionado enquanto os anfitriões se comunicam com os serviços na zona de Segurança da “parte externa”.

Troubleshooting

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

Depois que você configura o roteador do Cisco IOS com NAT, se as conexões não trabalham, seja certo destes:

- O NAT é aplicado apropriadamente na parte externa e nas interfaces internas.
- A configuração de NAT está completa, e os ACL refletem o tráfego que deve ser NATed.
- As rotas múltiplas ao Internet/WAN estão disponíveis.
- A política de firewall reflete exatamente a natureza do tráfego que você deseja permitir através do roteador.

Informações Relacionadas

- Suporte à Tecnologia de Voz
- Suporte ao Produto de Voz e Comunicações Unificadas
- Troubleshooting da Telefonia IP Cisco
- Projeto do Firewall da política e guia Zona-baseados do aplicativo
- Suporte Técnico e Documentação - Cisco Systems