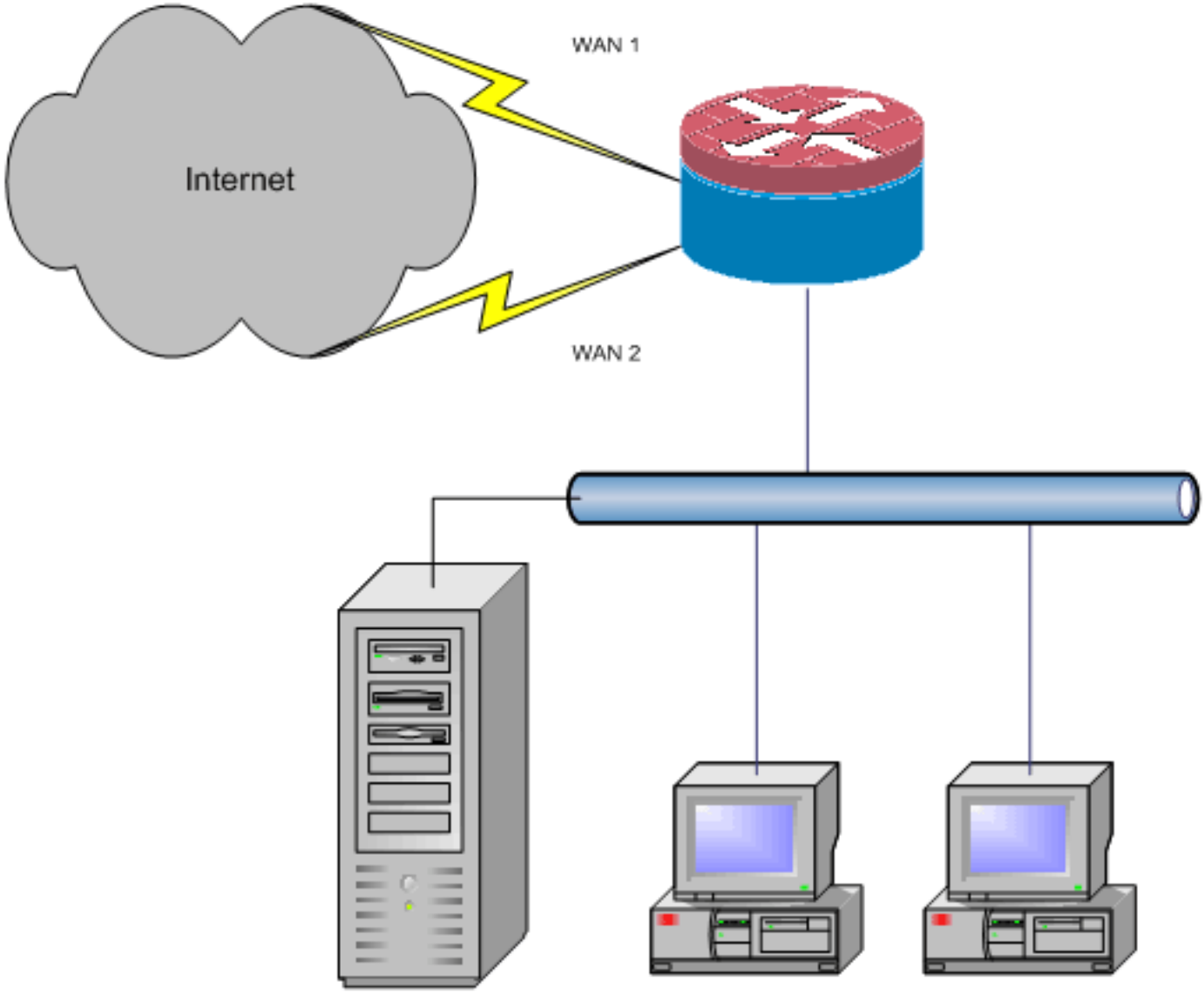
Função de balanceamento de carga IO NAT e Firewall Zona-baseado da política com roteamento de extremidade aperfeiçoado para duas conexões com o Internet

Índice

Introdução

Este documento descreve uma configuração 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 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. Caso uma das conexões se tornar inusável, o Rastreamento de objetos, um componente do roteamento de extremidade aperfeiçoado (OER), pode ser usado para desativar a rota até que a conexão se torne disponível outra vez, que assegura a disponibilidade da rede apesar da instabilidade ou da insegurança de uma conexão com o Internet.



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

Pré-requisitos

Requisitos

Este documento supõe que você já tem o LAN e as conexões de WAN que funcionam e não 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. Consequentemente, não há nenhuma maneira de preferir uma conexão mais desejável sobre uma conexão menos-desejável.

Este documento descreve como configurar OER a fim permitir ou desabilitar um ou outro Internet rota-baseado na alcançabilidade dos servidores DNS do ISP. Você precisa de identificar os anfitriões específicos que são alcançáveis através de somente uma das conexões ISP e não puderam estar disponíveis se essa conexão ISP não está disponível.

Componentes Utilizados

Esta configuração foi desenvolvida com um Cisco 1811 Router que executasse o software avançado 12.4(15)T2 dos Serviços IP. Se uma versão de software diferente é usada, algumas características não podem estar disponíveis, ou os comandos configuration puderam diferir daqueles mostrados neste documento. As configurações similares devem estar disponíveis 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

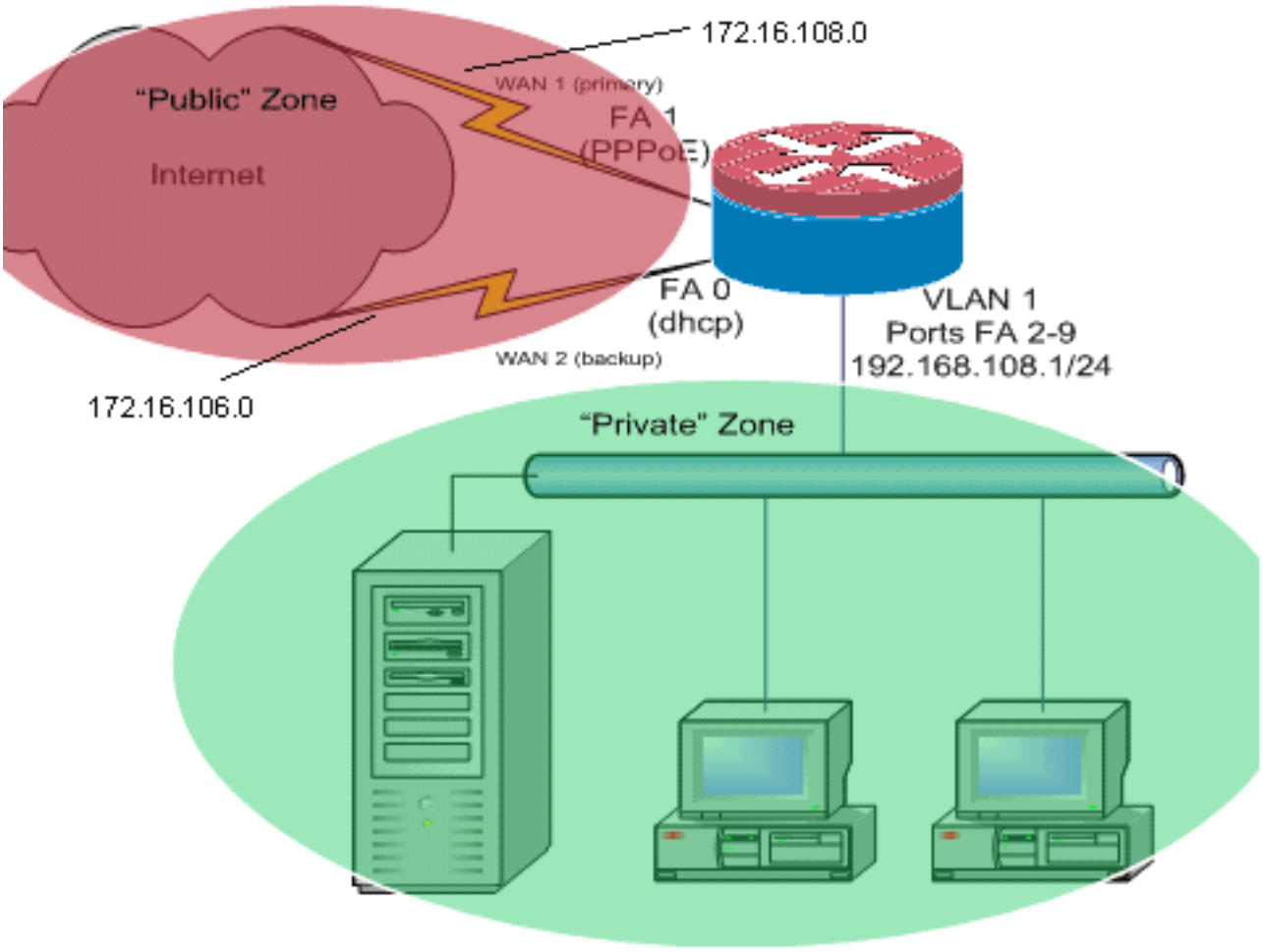
Você pôde precisar de adicionar para ter certeza o roteamento baseado em política para o tráfego específico que usa sempre uma conexão ISP. Os exemplos do tráfego que puderam exigir este comportamento incluem clientes do IPSec VPN, monofones de VoIP, e todo o outro tráfego que dever sempre usar somente 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.

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.

Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:



Este exemplo de configuração, como ilustrado no diagrama da rede, 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, a menos que o Rastreamento de objetos e o roteamento de extremidade aperfeiçoado (OER) e/ou o roteamento baseado em política deverem ser usada com uma conexão com o Internet DHCP-atribuída. Nesses casos, pode ser muito difícil definir um roteador de próximo salto para o roteamento de política ou o OER.

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 acomode conexões de FTP de partida e o tráfego de dados correspondentes 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 operar-se-á provavelmente com capacidade diminuída, ou pode 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 transmissão da porta NAT. Você deve construir configurações adicionais da política de firewall para acomodar o tráfego adicional que não é segurado por esta configuração básica.

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

Configuração de CLI

Configuração do IOS Cisco 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
```

Use o seguimento DHCP-atribuído da rota:

Configuração do IOS Cisco 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
```

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 sendo traduzidos a ambos os endereços exteriores 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#`
- **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 anfitriões da privado-zona e anfitriões da público-zona. Este comando fornece a verificação que o tráfego nos host internos está inspecionado enquanto os anfitriões se comunicam com os serviços na zona de segurança externa.

Troubleshooting

Verifique estes artigos se as conexões não trabalham depois que você configura o roteador do Cisco IOS com NAT:

- 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.
- Se você usa a rota que segue, verifique o estado da rota que segue a fim assegurar-se de que as conexões com o Internet estejam disponíveis.
- A política de firewall reflete exatamente a natureza do tráfego que você deseja permitir através do roteador.

Informações Relacionadas

- Cisco IOS Firewall
- Referência de comandos dos Serviços de endereçamento IP do Cisco IOS - Comandos nat
- Projeto do Firewall da política e guia Zona-baseados do aplicativo
- Manual de configuração aperfeiçoado Cisco IOS do roteamento de extremidade, liberação 12.4T
- Suporte Técnico e Documentação - Cisco Systems