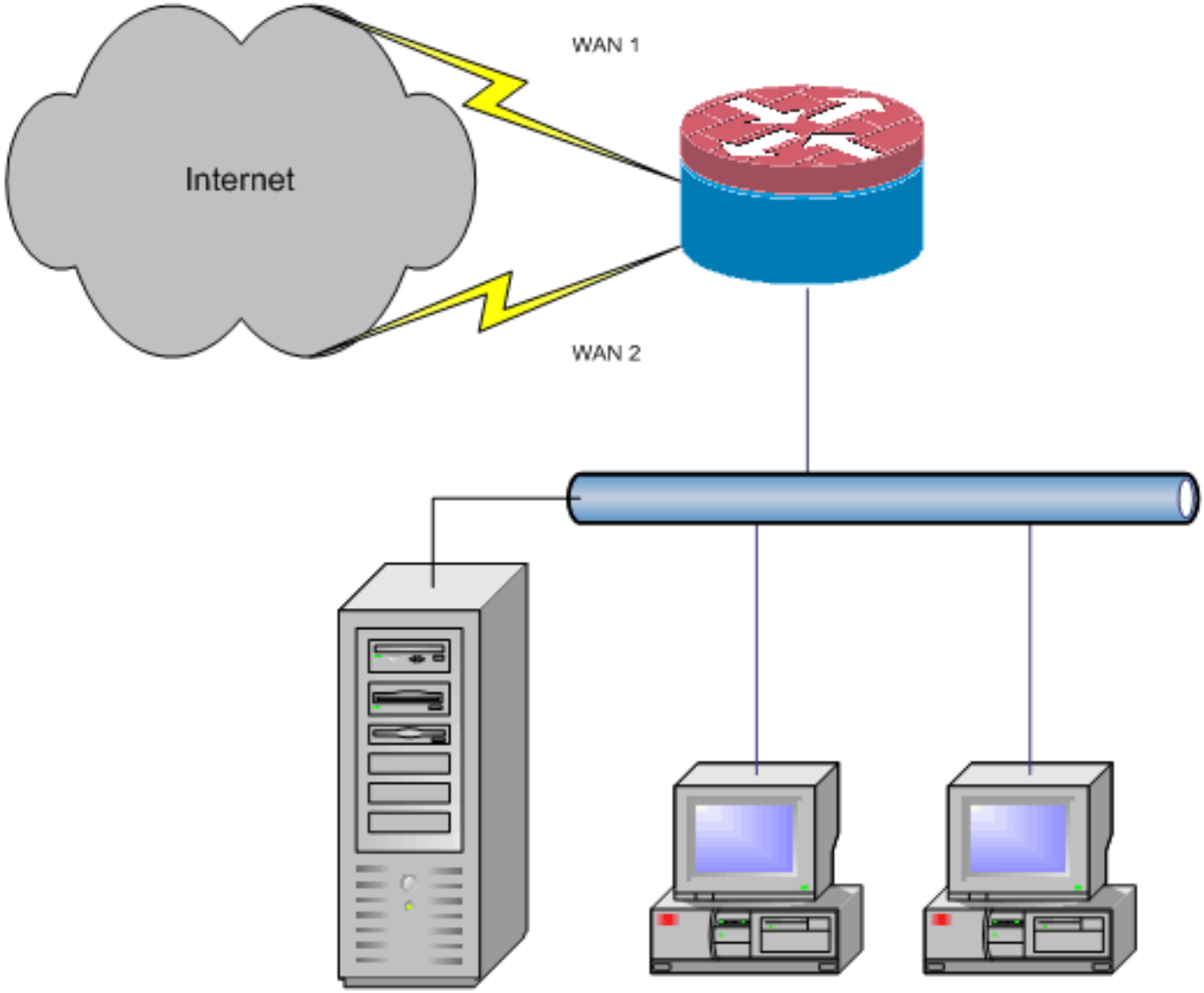
Configurar o NAT do Cisco IOS para duas conexões ISP com OER

Contents

Introduction

Este documento descreve uma configuração para um roteador Cisco IOS® conectar uma rede à Internet com Network Address Translation (NAT) através de duas conexões ISP. A NAT do 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. Caso uma das conexões se torne inutilizável, o rastreamento de objeto, um componente do OER (Otimized Edge Routing, roteamento otimizado de borda), pode ser usado para desativar a rota até que a conexão se torne novamente disponível, o que garante a disponibilidade da rede apesar da instabilidade ou da falta de confiabilidade de uma conexão com a Internet.



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

Prerequisites

Requirements

Este documento pressupõe que você já tem conexões de LAN e WAN que funcionam 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 as rotas. Portanto, não há como preferir uma conexão mais desejável em vez de uma conexão menos desejável.

Este documento descreve como configurar o OER para habilitar ou desabilitar a rota da Internet com base na acessibilidade dos servidores DNS do ISP. Você precisa identificar hosts específicos que podem ser acessados por meio de apenas uma das conexões do ISP e que podem não estar disponíveis se essa conexão do ISP não estiver disponível.

Componentes Utilizados

Essa configuração foi desenvolvida com um roteador Cisco 1811 que executa o software 12.4(15)T2 Advanced IP Services. Se uma versão de software diferente for usada, alguns recursos podem não estar disponíveis ou os comandos de configuração podem ser diferentes dos mostrados neste documento. Configurações semelhantes devem estar disponíveis 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

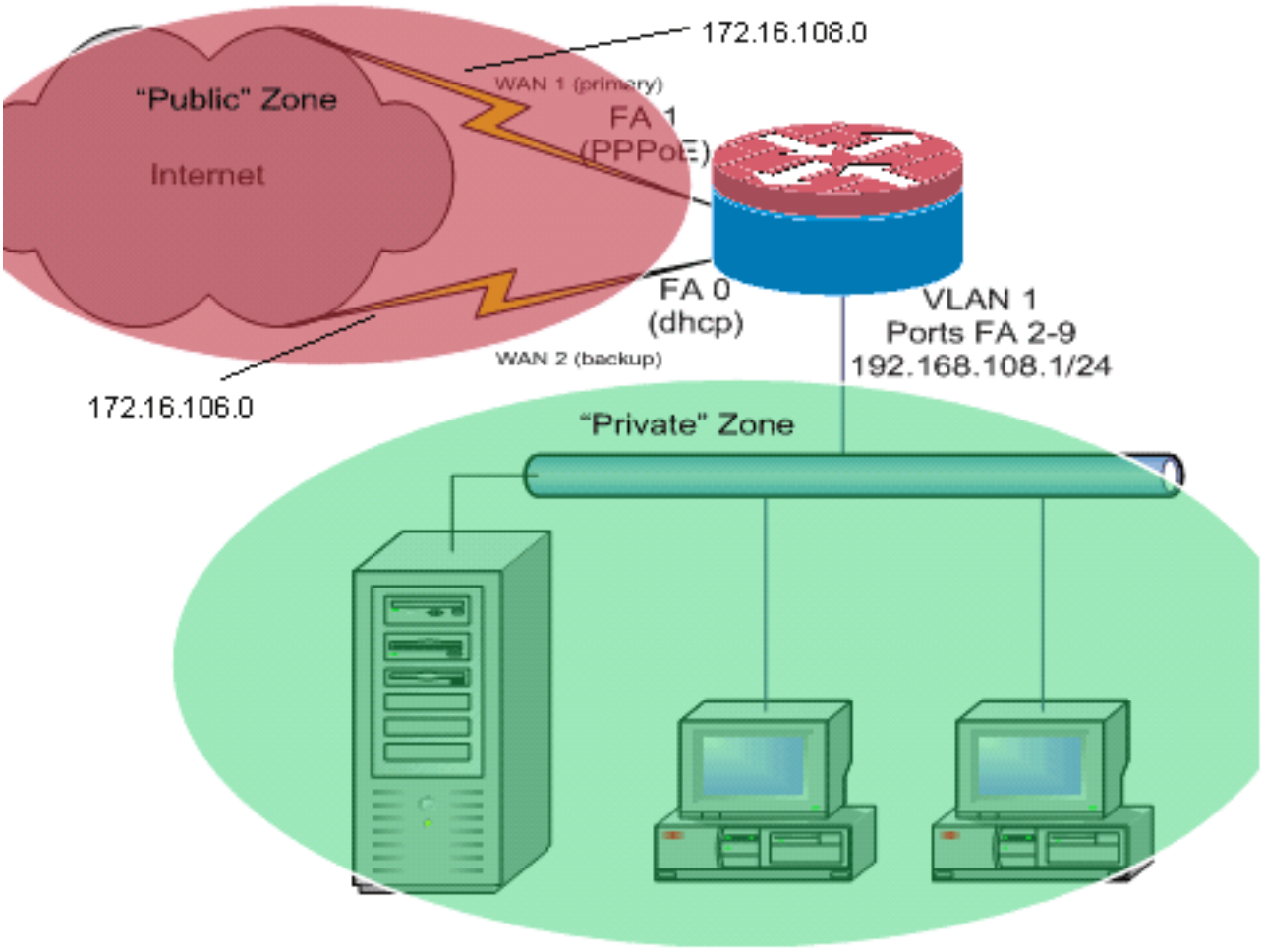
Você pode precisar adicionar roteamento baseado em políticas para tráfego específico para ter certeza de que ele sempre usa uma conexão ISP. Exemplos de tráfego que podem exigir esse comportamento incluem clientes VPN IPsec, aparelhos VoIP e qualquer outro tráfego que sempre deve usar apenas uma das opções de conexão do ISP para preferir o mesmo endereço IP, velocidade mais alta ou latência mais baixa 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 de rede, 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, a menos que o rastreamento de objeto e o OER (Otimized Edge Routing, roteamento de borda otimizada) e/ou o roteamento baseado em políticas sejam usados com uma conexão de Internet atribuída por DHCP. Nesses casos, pode ser muito difícil definir um roteador de próximo salto para roteamento de política ou OER.

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 correspondente 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 funcionará com capacidade reduzida ou poderá 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. Você deve construir configurações adicionais de política de firewall para acomodar tráfego adicional que não seja tratado por essa configuração básica.

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.

Configuração de CLI

Configuração da CLI do Cisco IOS

```
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
```

Usar rastreamento de rota atribuído por dhcp:

Configuração da CLI do Cisco IOS
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 (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 estão sendo convertidos para ambos os endereços externos de 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#
```

- **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 nos hosts internos é inspecionado como hosts que se comunicam com serviços na zona de segurança externa.

Troubleshoot

Verifique esses itens se as conexões não funcionarem depois de configurar o roteador Cisco IOS com NAT:

- 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.
- Se você usar o rastreamento de rota, verifique o estado do rastreamento de rota para garantir que as conexões de Internet estejam disponíveis.
- A política de firewall reflete precisamente a natureza do tráfego que você deseja permitir através do roteador.

Informações Relacionadas

- Cisco IOS Firewall
- Referência de comando do Cisco IOS IP Addressing Services - Comandos NAT
- Guia de aplicativos e design de firewall de política baseada em zona
- Guia de Configuração de Roteamento Edge Otimizado do Cisco IOS, Versão 12.4T
- Suporte Técnico e Documentação - Cisco Systems