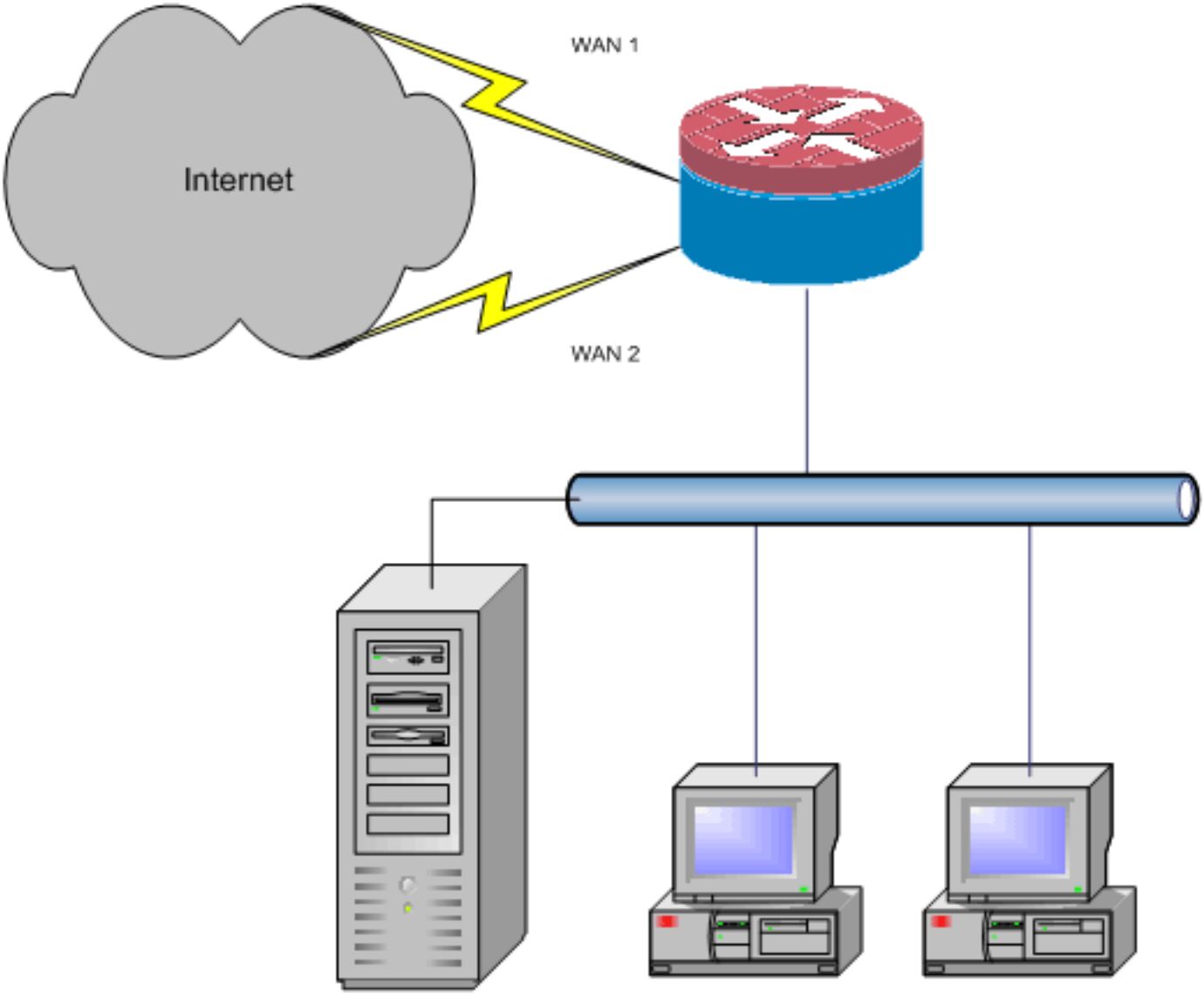
IOS NAT 负载平衡和基于区域的策略防火墙（针对两个 Internet 连接优化边界路由）

目录

简介

本文档介绍了 Cisco IOS 路由器的一种配置，该配置允许使用两个 ISP 连接通过网络地址转换 (NAT) 将网络连接到 Internet。如果存在通往给定目标的等价路由，则 Cisco IOS NAT 可以将随后的 TCP 连接和 UDP 会话分配到多个网络连接。在其中一连接变得不可用情况下，对象跟踪，组件优化边缘路由(OER)，可以用于撤销路由，直到连接再变得可用，保证互联网连接的网络可用性竟管不稳定性或不确实。



本文档描述另一种应用了 Cisco IOS 区域策略防火墙的配置，这种配置添加了状态检查功能，可加强 NAT 提供的基本网络保护。

先决条件

要求

本文档假设您已经拥有能够正常使用的 LAN 和 WAN 连接，因此不提供建立初始连接所需的配置或故障排除背景。

本文档不介绍区分路由的方式。因此，没有办法选出更喜欢的连接。

本文档介绍如何配置 OER，使其根据 ISP 的 DNS 服务器的可达性来启用或禁用 Internet 路由。您需要识别出只能通过一个 ISP 连接到达并且当此 ISP 连接不可用时也不可用的特定主机。

使用的组件

此配置使用其上运行 12.4(15)T2 版 Advanced IP Services 软件的 Cisco 1811 路由器开发。如果使用的是其他软件版本，有些功能可能不可用，配置命令也可能与本文档中所示有所不同。虽然接口配置在不同的平台之间很可能会有变化，但是相似的配置应该在所有 Cisco IOS 路由器平台上都是

可用的。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

配置

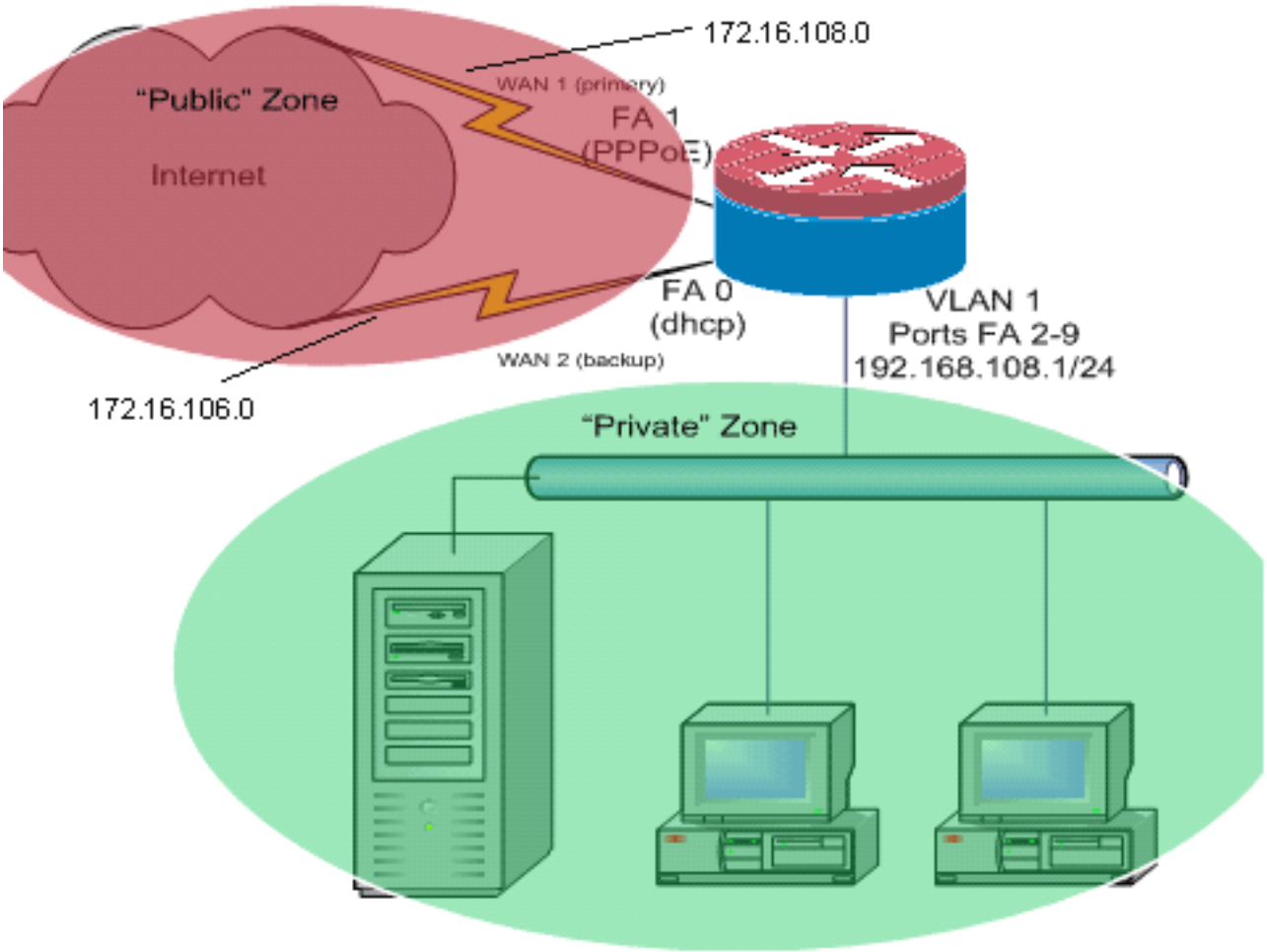
您可能需要为特定的流量添加基于策略的路由，确保此流量始终使用同一个 ISP 连接。可能需要这种行为的流量示例包括：IPsec VPN 客户端，VoIP 听筒，以及应该始终使用同一个 ISP 连接选项以便在连接中获得相同 IP 地址、更高速度或更低延时的其他任何流量。

本部分提供有关如何配置本文档所述功能的信息。

注意： 使用命令查找工具（仅限注册用户）可获取有关本部分所使用命令的详细信息。

网络图

本文档使用以下网络设置：



如网络图所示，此配置示例描述一个访问路由器，该路由器对一个 ISP（如 FastEthernet 0 所示）使用由 DHCP 配置的 IP 连接，并通过另一个 ISP 连接使用 PPPoE 连接。连接类型没有在配置

的特定的影响，除非对象跟踪和优化边缘路由(OER)并且/或者基于策略的路由将与DHCP分配的互联网连接一起使用。在这些情况下，很难为策略路由或 OER 定义下一跳的路由器。

防火墙策略讨论

本配置示例描述一种防火墙策略，这种防火墙策略允许从安全区“内部”与安全区“外部”建立简单的 TCP、UDP 和 ICMP 连接，并且能够容纳出站 FTP 连接以及主动和被动 FTP 传输的相应数据流量。任何不能由这种基本策略处理的复杂应用流量（例如，VoIP 信令和媒体）都可能会导致能力下降，甚至可能完全失败。此防火墙策略阻止从“公共”安全区与“专用”安全区建立的所有连接，包括由 NAT 端口转发容纳的所有连接。您必须构建更多的防火墙策略配置来容纳不能由这种基本配置处理的其他流量。

如果您对区域策略防火墙策略设计和配置有疑问，请参阅区域策略防火墙设计和应用指南。

CLI 配置

Cisco IOS CLI 配置

```
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
```

使用 DHCP 分配的路由跟踪：

Cisco IOS CLI 配置

```
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
```

验证

使用本部分可确认配置能否正常运行。

命令输出解释程序（仅限注册用户）(OIT) 支持某些 **show** 命令。使用 OIT 可查看对 show 命令输出的分析。

- **show ip nat translation** — 显示 NAT 内部主机与 NAT 外部主机之间的 NAT 活动。此命令为转换为两个 NAT 外部地址的内部主机提供验证。`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** — 验证是否存在多个通往 Internet 的路由。`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**—显示专用区域主机和公共区域主机之间的防火墙检查活动。此命令为内部主机（作为与外部安全区中的服务进行通信的主机进行检查）上的通信提供验证。

故障排除

在您用 NAT 配置 Cisco IOS 路由器之后，如果连接还不能正常使用，请验证以下各项：

- 在外部和内部接口上正确应用了 NAT。
- NAT 配置已完成，并且 ACL 反映了必须进行 NAT 处理的流量。
- 存在多个通往 Internet/WAN 的路由。
- 如果使用了路由跟踪，请检查路由跟踪的状态，确保 Internet 连接是可用的。
- 防火墙策略准确反映了您希望允许通过路由器的流量的性质。

相关信息

- Cisco IOS 防火墙
- Cisco IOS IP 编址服务命令参考 - NAT 命令
- 区域策略防火墙设计和应用指南
- Cisco IOS 优化的边缘路由配置指南，12.4T 版
- 技术支持和文档 - Cisco Systems