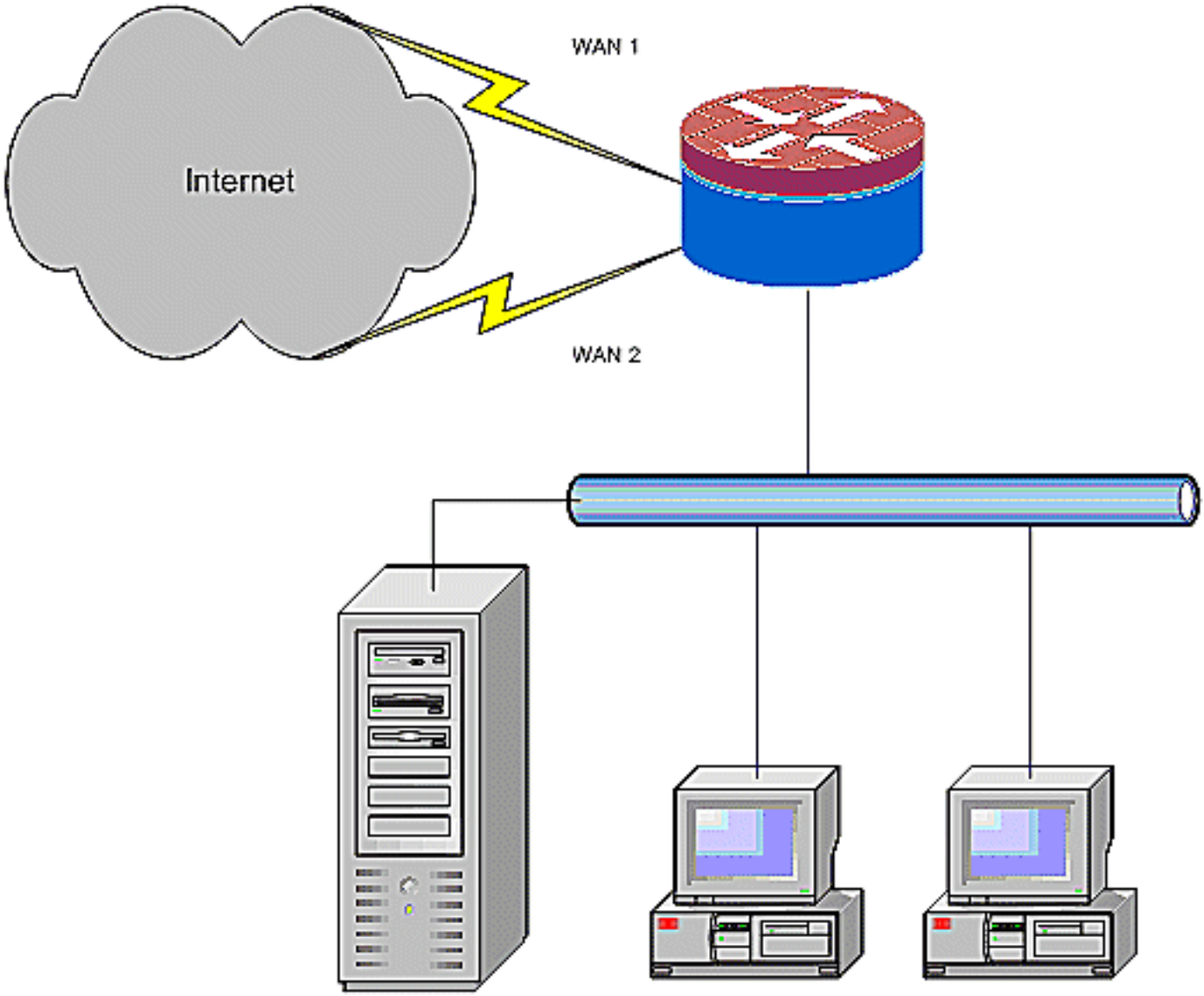
使用基于区域的策略防火墙的 IOS NAT 负载平衡（用于两个 ISP 连接）

目录

简介

本文档提供了Cisco IOS®路由器的示例配置，该路由器通过两个ISP连接通过网络地址转换(NAT)将网络连接到Internet。如果存在指向某个给定目标的等价路由，Cisco IOS 软件 NAT 可以将随后的 TCP 连接和 UDP 会话分配到多个网络连接。



本文档还说明了另外一种应用 Cisco IOS 区域策略防火墙 (ZFW) 的配置，这种配置可添加状态检查功能以加强 NAT 提供的基本网络保护。

先决条件

要求

本文档假定您使用 LAN 和 WAN 连接，因此不提供用于建立初始连接的配置或故障排除背景。本文档不提供区分路由的方法，因此没有办法挑选比较满意的连接。

使用的组件

本文档中的信息以运行 12.4(15)T3 Advanced IP Services 软件的 Cisco 系列 1811 路由器为基准。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。尽管接口配置在不同的平台之间可能会有变化，但是类似的配置在所有 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

有关文档约定的更多信息，请参考 Cisco 技术提示约定。

配置

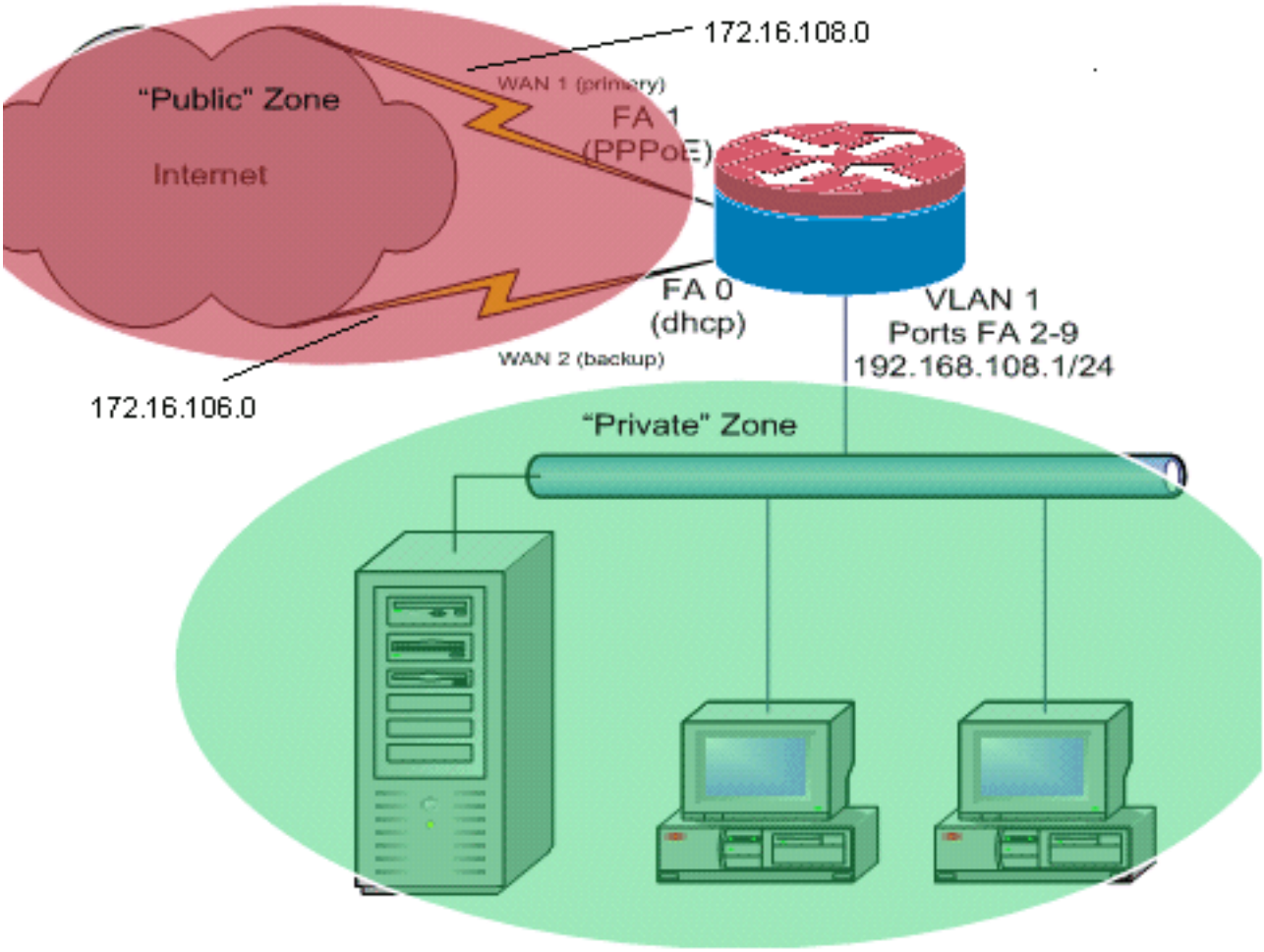
本部分提供有关如何配置本文档所述功能的信息。

注意：使用命令查找工具(仅限注册客户)可获取有关本节中使用的命令的详细信息。

您需要为特定数据流添加基于策略的路由，以确保该数据流始终使用同一个 ISP 连接。可能需要这种行为的数据流示例包括：IPSec VPN 客户端，VoIP 电话数据流，以及仅使用一个 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任何其他数据流。

网络图

本文档使用以下网络设置：



此配置示例说明的接入路由器对一个 ISP（显示为 FastEthernet 0）使用一个 DHCP 配置 IP 连接，对另一个 ISP 连接使用 PPPoE 连接。连接类型对配置没有特定的影响，但有些连接类型在特定故障情况下可能会影响此配置的可用性。这种问题主要出现在通过连接以太网的 WAN 服务使用 IP 连接时，例如，电缆调制解调器或由附加设备终止 WAN 连接并为 Cisco IOS 路由器提供以太网移

交的 DSL 服务。在应用静态 IP 寻址的情况下（与 DHCP 分配地址或 PPPoE 相反），如果发生 WAN 故障，使得以太网端口仍保持与 WAN 连接设备的以太网链路，路由器将继续尝试对正常 WAN 连接和故障 WAN 连接进行连接负载均衡。如果您的部署要求从负载均衡中删除非活动路由，请参阅采用两个 Internet 连接的优化边缘路由的 Cisco IOS NAT 负载均衡和区域策略防火墙，该文档说明如何添加优化的边缘路由以监控路由有效性。

防火墙策略讨论

此配置示例描述防火墙策略，该策略允许从“内部”安全区到“外部”安全区的简单TCP、UDP和ICMP连接，并为主动和被动FTP传输提供出站FTP连接和等效数据流量。无法由这种基本策略进行处理的任何复杂应用数据流（例如，VoIP 信令和媒体）都可能导致能力下降，甚至可能完全失败。此防火墙策略阻止从“公共”安全区域到“私有”区域的所有连接，其中包括NAT端口转发所支持的所有连接。如有必要，您需要调整防火墙检查策略以反映应用配置文件和安全策略。

如果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。

配置

本文档使用以下配置：

配置

```
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
```

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。**此命令用于验证内部主机是否同时转换为两个 NAT 外部地址。

```
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—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。此命令可验证当主机与“外部”安全区域中的服务通信时，会检查内部主机的流量。

故障排除

本部分提供的信息可用于对配置进行故障排除。

使用 NAT 配置 Cisco IOS 路由器之后，如果连接无法正常工作，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。
- 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

- 语音技术支持

- 语音和统一通信产品支持
- Cisco IP 电话故障排除
- 区域策略防火墙设计和应用指南
- 技术支持和文档 - Cisco Systems