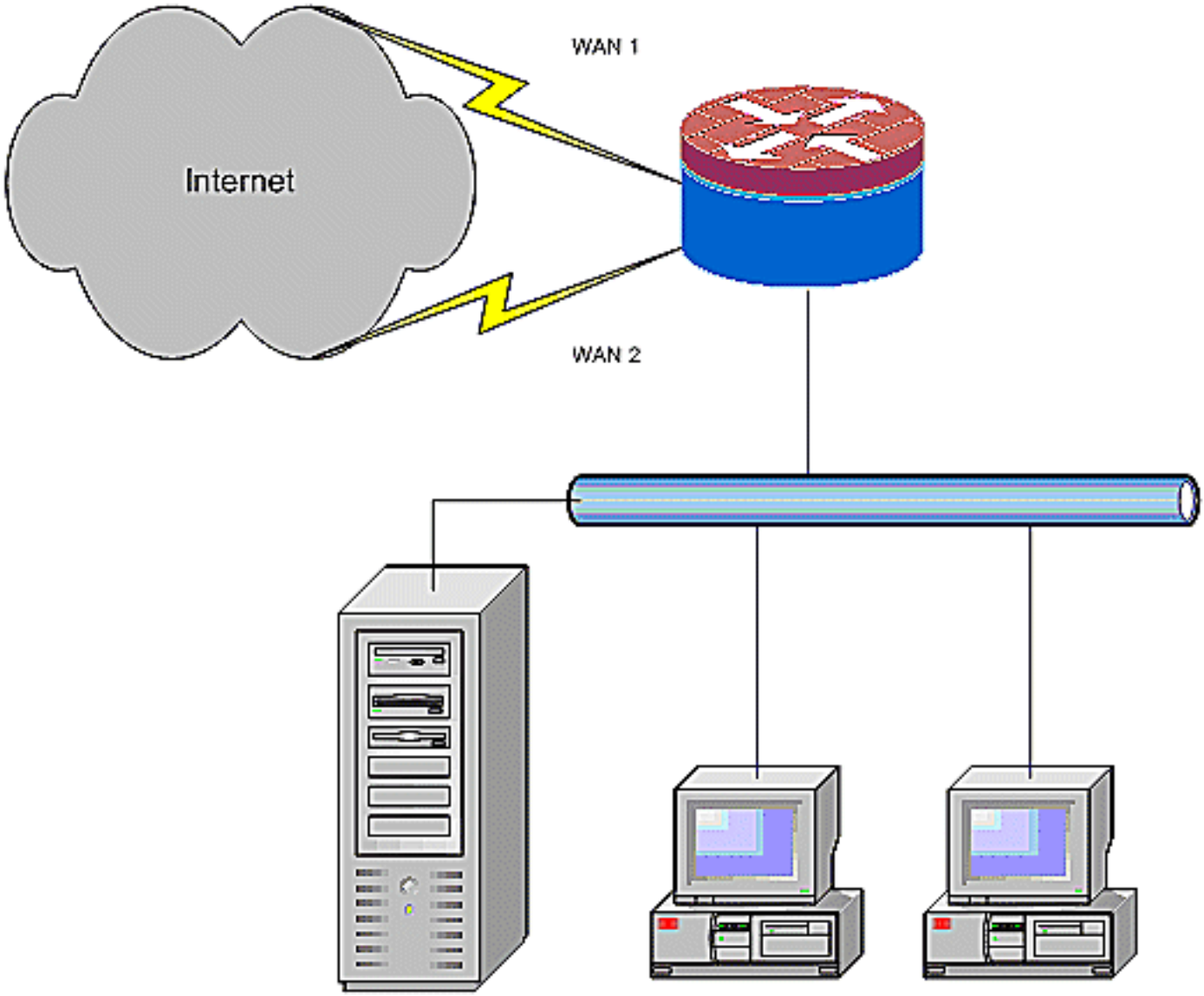
適用於兩個ISP連線的IOS NAT負載平衡（使用基於區域的策略防火牆）

目錄

簡介

本文檔提供通過兩個ISP連線使用網路地址轉換(NAT)將網路連線到Internet的Cisco IOS®路由器的配置示例。如果到給定目標的等價路由可用，Cisco IOS軟體NAT可以通過多個網路連線分發後續TCP連線和UDP會話。



本文檔介紹應用Cisco IOS基於區域的策略防火牆(ZFW)新增狀態檢測功能來增強NAT提供的基本網路保護的其他配置。

必要條件

需求

本文檔假定您使用LAN和WAN連線，不提供用於建立初始連線的配置或故障排除背景。本文檔沒有描述區分路由的方法，因此沒有方法優先使用更理想的連線而非次理想的連線。

採用元件

本檔案中的資訊是根據搭載12.4(15)T3進階IP服務軟體的Cisco系列1811路由器。如果使用不同的軟體版本，則某些功能不可用，或者配置命令可能與本文檔中顯示的有所不同。所有Cisco IOS路由器平台都提供類似的配置，但介面配置可能因平台不同而不同。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設

）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

慣例

請參閱思科技術提示慣例以瞭解更多有關文件慣例的資訊。

設定

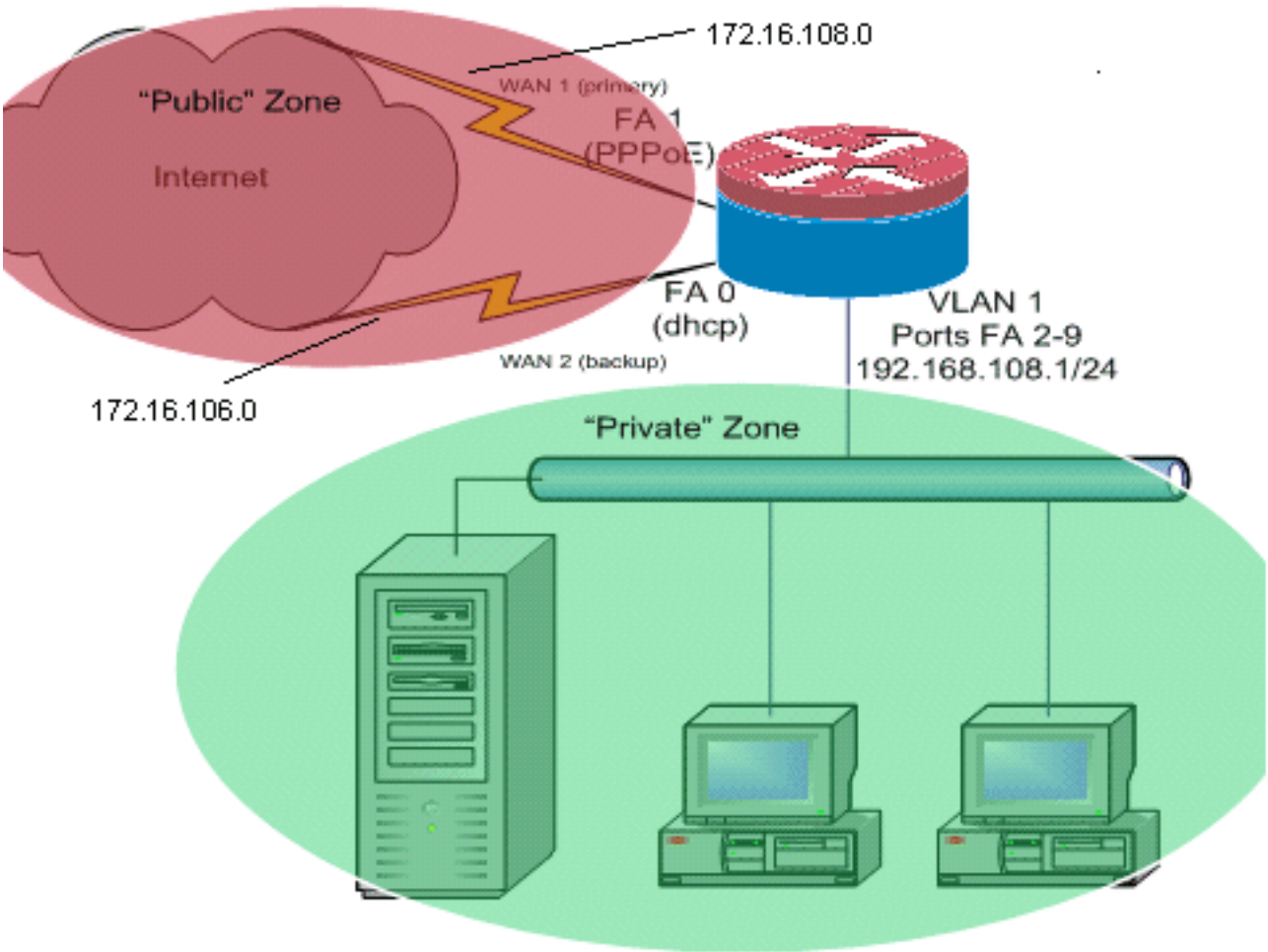
本節提供用於設定本文件中所述功能的資訊。

註：使用Command Lookup Tool(僅供已註冊客戶使用)可獲取本節中使用的命令的詳細資訊。

您需要為特定流量新增基於策略的路由，以確保它始終使用一個ISP連線。需要此行為的流量示例包括IPSec VPN客戶端、VoIP電話流量以及僅使用其中一個ISP連線選項以優先使用相同IP地址、速度較高或連線延遲較低的任何其他流量。

網路圖表

本檔案會使用以下網路設定：



此配置示例描述了一個接入路由器，它使用一個ISP的DHCP配置IP連線（如FastEthernet 0所示）和另一個ISP連線的PPPoE連線。連線型別對配置沒有特殊影響，但某些連線型別可能會影響在特定故障情況下此配置的可用性。當使用通過乙太網連線的WAN服務的IP連線時（例如，電纜數據機或DSL服務），當其他裝置終止WAN連線並提供乙太網切換到Cisco IOS路由器時，情況尤其如此。如果應用靜態IP編址（而不是DHCP分配的地址或PPPoE），並且發生WAN故障，因此乙太網

埠仍然保持與WAN連線裝置的乙太網鏈路，則路由器會繼續嘗試在正常和錯誤的WAN連線之間實現負載均衡連線。如果您的部署要求從負載均衡中移除非活動路由，請參閱Cisco IOS NAT負載均衡和基於區域的策略防火牆（具有針對兩個Internet連線的最佳化邊緣路由）中提供的配置，其中介紹了新增最佳化邊緣路由以監控路由有效性。

防火牆策略討論

此組態範例說明一個防火牆原則，允許簡單的TCP、UDP和ICMP連線從「內部」安全區域到「外部」安全區域，並適用於傳出FTP連線以及主動和被動FTP傳輸的同等資料流量。任何未由此基本策略處理的複雜應用流量（例如VoIP信令和媒體）都可能在功能降低的情況下運行，或者可能會完全失敗。此防火牆策略阻止從「公共」安全區域到「專用」區域的所有連線，該區域包括NAT埠轉發所容納的所有連線。如有必要，您需要調整防火牆檢測策略以反映您的應用配置檔案和安全策略。

如果您對基於區域的策略防火牆策略設計和配置有疑問，請參閱基於區域的策略防火牆設計和應用指南。

組態

本檔案會使用以下設定：

組態

```
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
```

驗證

使用本節內容，確認您的組態是否正常運作。

輸出直譯器工具(僅供已註冊客戶使用)(OIT)支援某些show命令。使用OIT檢視show命令輸出的分析。

- show ip nat translation — 顯示內部主機與NAT外部主機之間的NAT活動。此命令用於驗證內部主機是否被轉換為兩個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 — 驗證是否有多條通往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 — 顯示「專用」區域主機和「公共」區域主機之間的防火牆檢查活動。此命令可驗證當主機與「外部」安全區域中的服務通訊時，是否檢查內部主機的流量。

疑難排解

本節提供的資訊可用於對組態進行疑難排解。

使用NAT配置Cisco IOS路由器後，如果連線不起作用，請確認以下各項：

- NAT會適當地應用於外部和內部介面。
- NAT配置已完成，ACL反映必須進行NAT處理的流量。
- 提供多條通往網際網路/廣域網的路由。
- 防火牆策略準確地反映了您希望允許通過路由器的流量的性質。

相關資訊

- 語音技術支援

- 語音和整合通訊產品支援
- Cisco IP電話故障排除
- 基於區域的策略防火牆設計和應用指南
- 技術支援與文件 - Cisco Systems