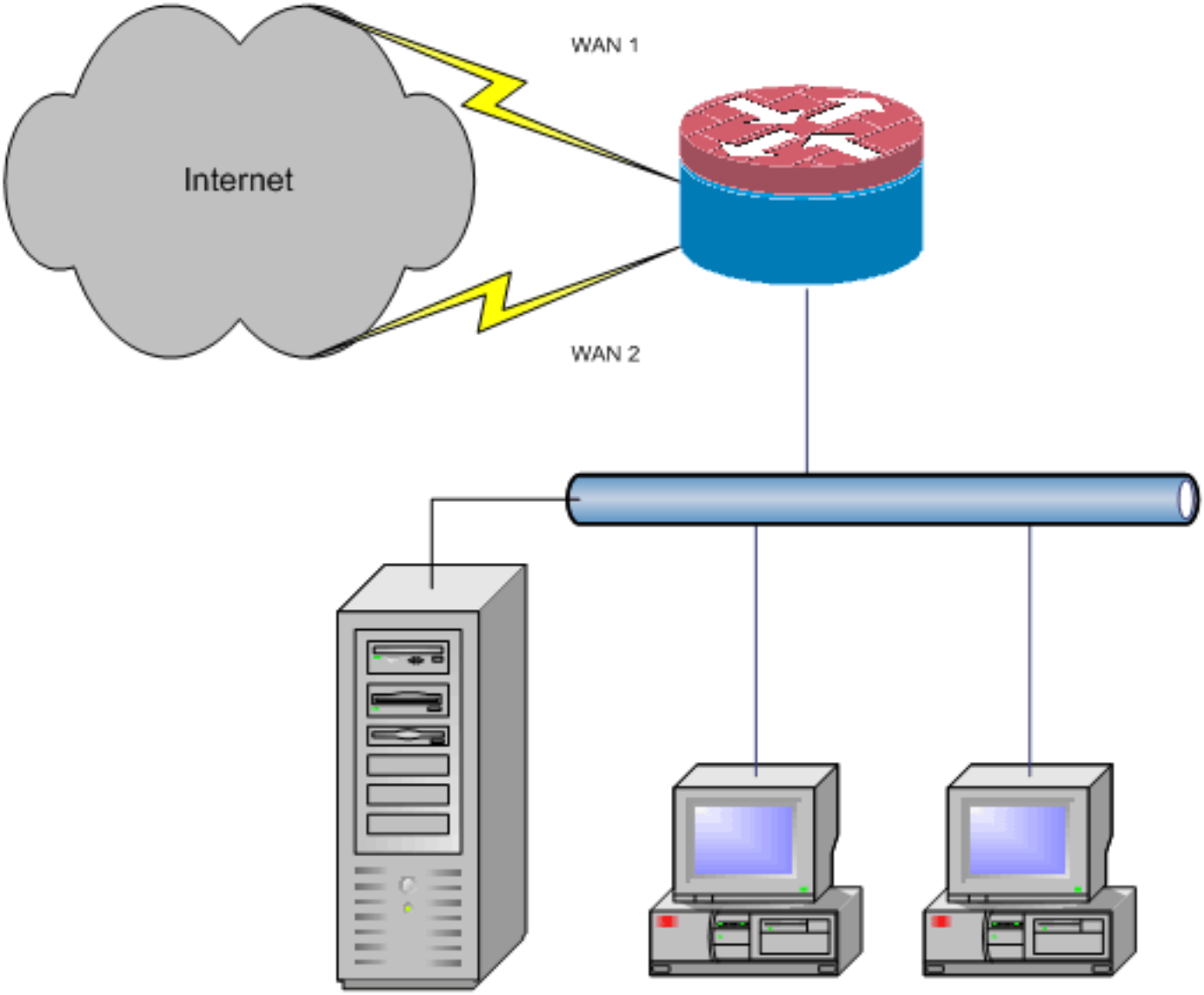
使用OER為兩個ISP連線配置Cisco IOS NAT

目錄

簡介

本檔案將說明Cisco IOS®路由器的配置，該路由器通過兩個ISP連線將網路通過網路地址轉換(NAT)連線到Internet。如果到給定目標的等價路由可用，Cisco IOS NAT可以通過多個網路連線分發後續TCP連線和UDP會話。當其中一個連線變得不可用時，最佳化邊緣路由(OER)的一個元件對象跟蹤可用於停用該路由，直到該連線再次可用，這樣儘管網際網路連線不穩定或不可靠，但仍能確保網路可用性。



本文檔介紹應用Cisco IOS基於區域的策略防火牆以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

本文檔假定您已有LAN和WAN連線可用，並且不提供用於建立初始連線的配置或故障排除背景。

本文檔未介紹區分路由的方法。因此，沒有辦法優先選擇更期望的連線而不是更期望的連線。

本文檔介紹如何配置OER，以便根據ISP的DNS伺服器的可達性啟用或禁用Internet路由。您需要確定只能通過其中一個ISP連線訪問的特定主機，如果該ISP連線不可用，這些主機可能不可用。

採用元件

此配置由運行12.4(15)T2 Advanced IP Services軟體的Cisco 1811路由器開發。如果使用不同的軟體版本，則某些功能可能不可用，或者配置命令可能與本文檔中顯示的有所不同。所有Cisco IOS路由器平台都應提供類似的配置，但介面配置可能會因平台不同而不同。

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

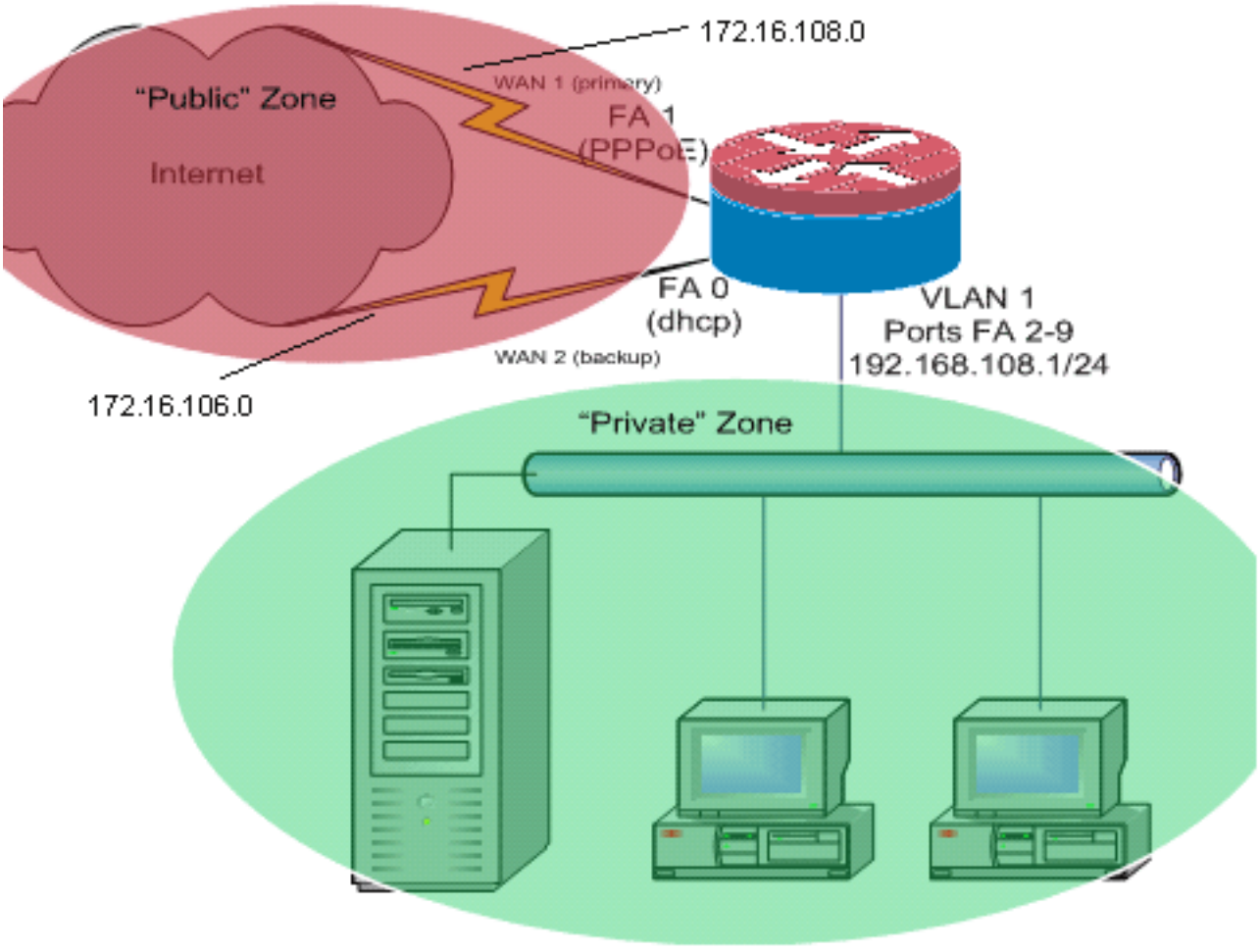
您可能需要為特定流量新增基於策略的路由，以確保它始終使用一個ISP連線。可能需要此行為的流量示例包括IPsec VPN客戶端、VoIP手持機和任何其它流量，這些流量應始終只使用其中一個ISP連線選項，以便在連線上優先使用相同的IP地址、更高的速度或更低的延遲。

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。

網路圖表

本檔案會使用以下網路設定：



如網路圖所示，此配置示例描述了一個接入路由器，該路由器使用到一個ISP的DHCP配置IP連線（如FastEthernet 0所示）和通過另一個ISP連線的PPPoE連線。連線型別對配置沒有特殊影響，除非對象跟蹤和最佳化邊緣路由(OER)和/或基於策略的路由與DHCP分配的Internet連線一起使用。在這些情況下，可能很難為策略路由或OER定義下一跳路由器。

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傳輸的對應資料流量。未由此基本策略處理的任何複雜應用流量（例如VoIP信令和媒體）都可能以功能降低的方式運行，或者可能完全失敗。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。您必須構建其他防火牆策略配置，以適應此基本配置未處理的額外流量。

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。

CLI組態

Cisco IOS CLI組態

```
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分配的路由跟蹤：

Cisco IOS CLI組態

```
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
```

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正在被轉換為兩個NAT外部地址。

```
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** — 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，是否檢查內部主機上的流量。

疑難排解

如果在使用NAT配置Cisco IOS路由器後連線不起作用，請驗證以下各項：

- 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。
- 如果使用路由跟蹤，請檢查路由跟蹤的狀態，以確保Internet連線可用。
- 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

- Cisco IOS 防火牆
- Cisco IOS IP編址服務命令參考 — NAT命令
- 基於區域的策略防火牆設計和應用指南
- Cisco IOS最佳化邊緣路由組態設定指南12.4T版
- 技術支援與文件 - Cisco Systems