瞭解策略路由

目錄

簡介

基於策略的路由提供了一種根據網路管理員定義的策略轉發和路由資料包的工具。實際上，這是一種讓策略替代路由協定決策的方式。基於策略的路由包括基於訪問清單、分組大小或其他標準選擇性地應用策略的機制。所採取的操作包括在使用者定義的路由上路由資料包、設定優先順序、服務位型別等。

在本文檔中，使用防火牆將10.0.0.0/8私有地址轉換為屬於子網172.16.255.0/24的Internet可路由地址。有關直觀說明，請參閱下圖。

如需詳細資訊，請參閱原則型路由。

必要條件

需求

本文件沒有特定需求。

採用元件

本檔案所述內容不限於任何特定硬體或軟體版本。

本文檔中顯示的資訊基於以下軟體和硬體版本。

- Cisco IOS®軟體版本12.3(3)
- Cisco 2500系列路由器

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。如果您在即時網路中工作，請確保在使用任何命令之前瞭解其潛在影響。

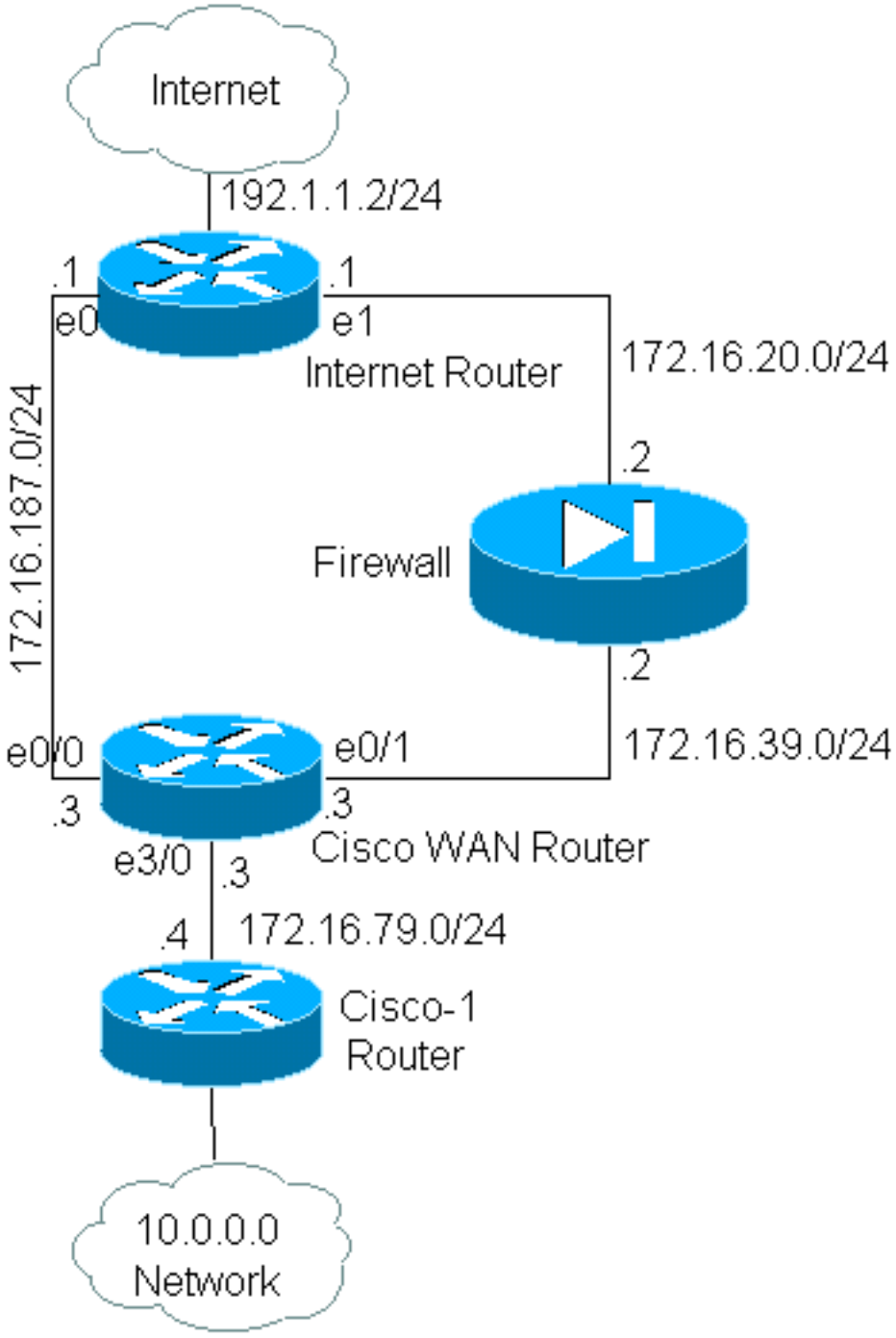
慣例

如需文件慣例的詳細資訊，請參閱思科技術提示慣例。

組態

在本例中，使用普通路由時，從10.0.0.0/8網路到Internet的所有資料包將採用通過Cisco WAN路由器的介面ethernet 0/0的路徑(通過172.16.187.0/24子網)，因為這是具有最少度量值的最佳路徑。對於基於策略的路由，我們希望這些資料包通過防火牆到達網際網路的路徑，正常路由行為必須通過配置策略路由來覆蓋。防火牆將來自10.0.0.0/8網路的所有資料包轉換到Internet，但這對策略路由工作並不必要。

網路圖表



防火牆配置

包含下列防火牆配置以提供完整檢視。但是，這不是本文檔中介紹的策略路由問題的一部分。本示例中的防火牆可以輕鬆地由PIX或其他防火牆裝置替換。

```
!
ip nat pool net-10 172.16.255.1 172.16.255.254 prefix-length 24
ip nat inside source list 1 pool net-10
!
interface Ethernet0
 ip address 172.16.20.2 255.255.255.0
 ip nat outside
!
interface Ethernet1
 ip address 172.16.39.2 255.255.255.0
 ip nat inside
!
router eigrp 1
 redistribute static
 network 172.16.0.0
 default-metric 10000 100 255 1 1500
!
ip route 172.16.255.0 255.255.255.0 Null0
access-list 1 permit 10.0.0.0 0.255.255.255
!
end
```

有關**ip nat**相關命令的詳細資訊，請參閱IP編址和服務命令

在本示例中，Cisco WAN路由器正在運行策略路由，以確保通過防火牆傳送來自10.0.0.0/8網路的IP資料包。以下配置包含一條訪問清單語句，用於將來自10.0.0.0/8網路的資料包傳送到防火牆。

Cisco_WAN_Router的組態

```
!
interface Ethernet0/0
 ip address 172.16.187.3 255.255.255.0
 no ip directed-broadcast
!
interface Ethernet0/1
 ip address 172.16.39.3 255.255.255.0
 no ip directed-broadcast
!
interface Ethernet3/0
 ip address 172.16.79.3 255.255.255.0
 no ip directed-broadcast
 ip policy route-map net-10
!
router eigrp 1
 network 172.16.0.0
!

access-list 111 permit ip 10.0.0.0 0.255.255.255 any
!
route-map net-10 permit 10
 match ip address 111
 set interface Ethernet0/1
!
route-map net-10 permit 20
```

```
!
end
```

請參閱route-map命令文檔，瞭解有關路由對映相**關命令的**詳細資訊。

註：PBR不支援**access-list**命令中的**log關鍵字。**如果配置了**log**關鍵字，則不會顯示任何命中。

Cisco-1路由器的配置

```
!
version 12.3

!

interface Ethernet0

!-- Interface connecting to 10.0.0.0 network ip address 10.1.1.1 255.0.0.0 ! interface Ethernet1
!-- Interface connecting to Cisco_Wan_Router ip address 172.16.79.4 255.255.255.0 ! router eigrp
1 network 10.0.0.0 network 172.16.0.0 no auto-summary ! !---Output Suppressed
```

Internet_Router的配置

```
!
version 12.3

!
interface Ethernet1

!-- Interface connecting to Firewall ip address 172.16.20.1 255.255.255.0 interface Serial0 !---
Interface connecting to Internet ip address 192.1.1.2 255.255.255.0 clockrate 64000 no fair-
queue ! interface Ethernet0 !--- Interface connecting to Cisco_Wan_Router ip address
172.16.187.1 255.255.255.0 ! ! router eigrp 1 redistribute static !--- Redistributing the static
default route for other routers to reach Internet network 172.16.0.0 no auto-summary ! ip
classless ip route 0.0.0.0 0.0.0.0 192.1.1.1 !-- Static default route pointing to the router
connected to Internet !---Output Suppressed
```

在測試此範例時，來源為10.1.1.1（位於Cisco-1路由器上）的ping會使用extended ping命令傳送到Internet上的主機。在本示例中，192.1.1.1用作目的地址。為了檢視Internet路由器上發生的情況，在使用**debug ip packet 101 detail**命令時關閉了快速交換。

警告：在生產路由器上使用**debug ip packet detail**指令可能會造成CPU使用率高，進而導致效能嚴重下降或網路中斷。建議在使用debug指令之前，仔細閱讀瞭解Ping和Traceroute指令的使用Debug指令一節。

注意：**access-list 101 permit icmp any any語**句用於過濾**debug ip packet輸**出。如果沒有此存取清單，**debug ip packet**指令可能會產生大量輸出到主控台，使路由器鎖定。配置PBR時使用擴展ACL。如果沒有配置ACL以建立匹配條件，則會導致所有流量進行策略路由。

```
Results of ping from Cisco_1 to 192.1.1.1/internet taken from Internet_Router:
Packet never makes it to Internet_Router

Cisco_1# ping
Protocol [ip]:
Target IP address: 192.1.1.1
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
```

```
Source address or interface: 10.1.1.1
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.1.1.1, timeout is 2 seconds:
Packet sent with a source address of 10.1.1.1
.....
Success rate is 0 percent (0/5)
```

您可以看到，封包從未到達網際網路路由器。以下debug命令（從Cisco WAN路由器獲取）顯示了發生這種情況的原因。

```
Debug commands run from Cisco_WAN_Router:
"debug ip policy"
*Mar  1 00:43:08.367: IP: s=10.1.1.1 (Ethernet3/0), d=192.1.1.1, len 100, policy match
*Mar  1 00:43:08.367: IP: route map net-10, item 10, permit
 !--- Packet with source address belonging to 10.0.0.0/8 network !--- is matched by route-map
"net-10" statement 10. *Mar 1 00:43:08.367: IP: s=10.1.1.1 (Ethernet3/0), d=192.1.1.1
(Ethernet0/1), len 100, policy routed *Mar 1 00:43:08.367: Ethernet3/0 to Ethernet0/1 192.1.1.1
!--- matched packets previously are forwarded out of interface !--- ethernet 0/1 by the set
command.
```

資料包按照預期與net-10策略對映中的策略條目10匹配。那麼，為什麼資料包沒有到達Internet路由器？

```
"debug arp"
*Mar  1 00:06:09.619: IP ARP: creating incomplete entry for IP address: 192.1.1.1 interface
Ethernet0/1
*Mar  1 00:06:09.619: IP ARP: sent req src 172.16.39.3 00b0.64cb.eab1,
                 dst 192.1.1.1 0000.0000.0000 Ethernet0/1
*Mar  1 00:06:09.635: IP ARP rep filtered src 192.1.1.1 0010.7b81.0b19, dst 172.16.39.3
                 00b0.64cb.eab1 wrong cable, interface Ethernet0/1

Cisco_Wan_Router# show arp
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  172.16.39.3             -   00b0.64cb.eab1  ARPA   Ethernet0/1
Internet  172.16.39.2             3   0010.7b81.0b19  ARPA   Ethernet0/1
Internet  192.1.1.1               0   Incomplete      ARPA
```

debug arp輸出會顯示此情況。Cisco WAN路由器會嘗試按照指示執行操作，並嘗試將資料包直接放在ethernet 0/1介面上。這要求路由器傳送一個地址解析協定(ARP)請求來獲取目的地址192.1.1.1，但路由器意識到該地址並不在此介面上，因此該地址的ARP條目是「不完整」，如**show arp**命令所示。然後會出現封裝故障，因為路由器無法將資料包放在沒有ARP條目的線路上。

通過將防火牆指定為下一跳，我們可以防止此問題，並使路由對映按預期工作：

```
Config changed on Cisco_WAN_Router:
!
route-map net-10 permit 10
 match ip address 111
 set ip next-hop 172.16.39.2
!
```

現在，在Internet路由器上使用相同的**debug ip packet 101 detail**命令，我們可以看到資料包的路徑

是正確的。我們還可以看到，防火牆已將資料包轉換為172.16.255.1，正在執行ping的電腦192.1.1.1已做出響應：

```
Cisco_1# ping
Protocol [ip]:
Target IP address: 192.1.1.1
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 10.1.1.1
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.1.1.1, timeout is 2 seconds:
Packet sent with a source address of 10.1.1.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 68/70/76 ms

Results of ping from Cisco_1 to 192.1.1.1/internet taken from Internet_Router:
Internet_Router#
*Mar  1 00:06:11.619: IP: s=172.16.255.1 (Ethernet1), d=192.1.1.1 (Serial0), g=192.1.1.1, len
100, forward
*Mar  1 00:06:11.619:     ICMP type=8, code=0
!--- Packets sourced from 10.1.1.1 are getting translated to 172.16.255.1 by !--- the Firewall
before it reaches the Internet_Router. *Mar 1 00:06:11.619: *Mar 1 00:06:11.619: IP: s=192.1.1.1
(Serial0), d=172.16.255.1 (Ethernet1), g=172.16.20.2, len 100, forward *Mar 1 00:06:11.619: ICMP
type=0, code=0 !--- Packets returning from Internet arrive with the destination !--- address
172.16.255.1 before it reaches the Firewall. *Mar 1 00:06:11.619:
```

Cisco WAN路由器上的**debug ip policy**命令顯示資料包已轉發到防火牆172.16.39.2:

從Cisco_WAN_Router運行的Debug命令

```
"debug ip policy"
*Mar  1 00:06:11.619: s=10.1.1.1 (Ethernet3/0), d=192.1.1.1, len 100, policy match
*Mar  1 00:06:11.619: IP: route map net-10, item 20, permit
*Mar  1 00:06:11.619: s=10.1.1.1 (Ethernet3/0), d=192.1.1.1 (Ethernet0/1), len 100, policy
routed
*Mar  1 00:06:11.619: Ethernet3/0 to Ethernet0/1 172.16.39.2
```

適用於加密流量的原則型路由

將解密的流量轉發到環回介面，以便根據策略路由路由加密流量，然後在該介面上執行PBR。如果加密流量通過VPN隧道傳遞，則在該介面上禁用`ip cef`，並終止vpn隧道。

相關資訊

- IP 路由支援頁面
- NAT支援頁面
- 技術支援工具和資源
- 原則型路由

- Cisco IOS技術
- 技術支援與文件 - Cisco Systems