了解策略路由

目录

简介

基于策略的路由提供了一种工具，可用于根据网络管理员定义的策略转发和路由数据包。实际上，这是一种使策略覆盖路由协议决策的方法。基于策略的路由包括一种机制，该机制可根据访问列表、数据包大小或其他标准有选择性地应用策略。采取的措施包括按用户定义的路线路由数据包以及设置优先级和服务位类型等。

在本文档中，防火墙用于将 10.0.0.0/8 专用地址转换成属于子网 172.16.255.0/24 并且可在 Internet 上路由的地址。下图给出了较为直观的说明。

有关详细信息，请参阅基于策略的路由。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档不限于任何特定的硬件或软件版本。

本文档中显示的信息基于以下软件和硬件版本。

- Cisco IOS® 软件版本 12.3(3)
- Cisco 2500 系列路由器

本文档中的信息都是基于特定实验室环境中的设备创建的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您是在真实网络上操作，请确保您在使用任何命令前已经了解其潜在影响。

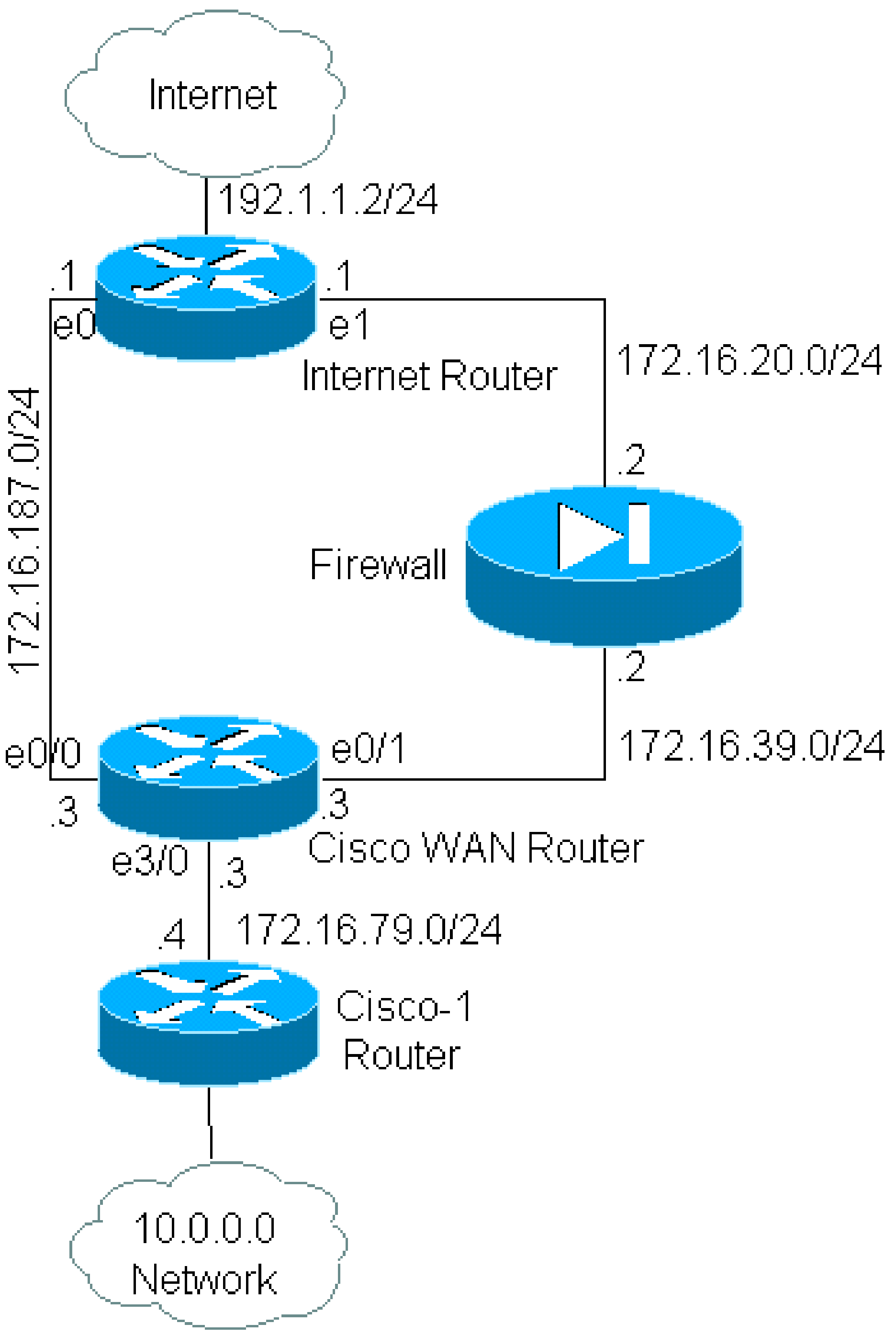
规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

配置

在本示例中，使用正常路由时，从 10.0.0.0/8 网络到 Internet 的所有数据包都将采用通过 Cisco 广域网路由器接口以太网 0/0 的路径（通过 172.16.187.0/24 子网），因为这是度量值最小的最佳路径。使用基于策略的路由时，我们希望这些数据包采用通过防火墙到 Internet 的路径，因此需要通过配置策略路由来覆盖正常路由行为。防火墙对从 10.0.0.0/8 网络传到 Internet 的所有数据包进行转换，但是此操作对于策略路由的运行而言是没有必要的。

网络图



防火墙配置

以下防火墙配置有助于您进行全面了解。但是，这不包括在本文档说明的策略路由问题中。本示例中的防火墙可由 PIX 或其他防火墙设备轻松替换。

```
!
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
```

请参阅 IP 编址和服务命令，获取有关 **ip nat** 相关命令的详细信息

在本示例中，Cisco 广域网路由器运行策略路由，确保从 10.0.0.0/8 网络发出的 IP 数据包将通过防火墙进行发送。以下配置包含一个访问列表语句，可将从 10.0.0.0/8 网络发出的数据包发送到防火墙。

Cisco_WAN_Router 的配置

```
!
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
```

请参阅 route-map 命令文档，获取有关 route-map 相关命令的详细信息。

注意： PBR 不支持 access-list 命令中的**日志关键字**。如果已配置**日志关键字**，它不会显示任何命中。

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
```

在测试本示例的过程中，在 Cisco-1 路由器上使用扩展 ping 命令从 10.1.1.1 中发出的 ping 发送到了 Internet 上的主机中。在本示例中，使用 192.1.1.1 作为目标地址。为查看 Internet 路由器上发生的情况，在使用 **debug ip packet 101 detail** 命令的同时关闭了快速交换。

警告： 在生产路由器上使用 **debug ip packet detail** 命令会大量占用 CPU，从而导致性能严重下降或网络中断。建议在使用 debug 命令之前仔细阅读了解 ping 和 traceroute 命令中的使用 debug 命令部分。

注意： **access-list 101 permit icmp any any** 语句用于过滤 debug ip packet 输出。如果没有此访问列表，**debug ip packet** 命令将生成过多的输出并传送到控制台，导致路由器锁定。配置 PBR 时，请使用扩展 ACL。如果没有为建立匹配标准而配置 ACL，将导致对所有流量采取策略路由方式。

```
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)
```

如您所见，数据包未曾传送到 Internet 路由器。以下 debug 命令（来自 Cisco 广域网路由器）说明了发生这种情况的原因。

```
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.
```

正如预期的那样，数据包与 net-10 策略映射中的策略条目 10 相匹配。但是为何数据包未传送到 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 输出说明了其中原由。Cisco 广域网路由器尝试执行接收到的指示，并尝试将数据包直接置于以太网 0/1 接口上。这要求路由器为目标地址 192.1.1.1 发送一个 Address Resolution Protocol (ARP) 请求，然后路由器意识到该目标地址不在此接口上，因此，该地址的 ARP 条目“不完整”，使用 **show arp** 命令即可了解这些。由于路由器无法将数据包置于没有 ARP 条目的线路上，因此随后发生封装故障。

通过将防火墙指定为下一跳可避免此问题，从而使 route-map 按预期方式发挥作用：

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

通过在 Internet 路由器上使用相同的 **debug ip packet 101 detail** 命令，可以看到数据包选择采用了正确的路径。此外，还可看到防火墙已将数据包转换到 172.16.255.1，而正在 ping 的计算机 192.1.1.1 已作出答复：

```
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 广域网路由器上的 **debug ip policy** 命令显示，已将数据包转发到防火墙 172.16.39.2：

从 Cisco_WAN_Router 运行的 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
```

对加密数据流进行的基于策略的路由

将解密的数据流转发到回环接口，以便根据策略路由对加密的数据流进行路由，然后在此接口上执行 PBR。如果解密的数据流通过 VPN 隧道进行传输，则在接口上 disable ip cef，并终止 vpn 隧道。

相关信息

- IP 路由支持页
- NAT 支持页
- 技术支持工具和资源
- 基于策略的路由
- Cisco IOS技术
- 技术支持和文档 - Cisco Systems