Información sobre el ruteo de políticas

Contenido

Introducción

El ruteo basado en políticas proporciona una herramienta para reenviar y rutear paquetes de datos basados en las políticas definidas por los administradores de red. En efecto, es una manera de que la política invalide las decisiones del protocolo de ruteo. El ruteo basado en políticas incluye un mecanismo para aplicar selectivamente políticas basadas en la lista de acceso, el tamaño de los paquetes u otros criterios. Las medidas que se toman pueden incluir el ruteo de paquetes en rutas definidas por el usuario, el establecimiento de la precedencia, el tipo de los bits de servicio, etc.

En este documento, se utiliza un firewall para traducir direcciones privadas 10.0.0.0/8 a direcciones enrutables a Internet que pertenecen a la subred 172.16.255.0/24. Consulte el diagrama siguiente para obtener una explicación visual.

Consulte Ruteo Basado en Políticas para obtener más información.

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

Este documento no se limita a ninguna versión específica de hardware o software.

La información que se muestra en este documento se basa en las siguientes versiones de software y hardware.

- Cisco IOS® Software Release 12.3(3)

- Cisco 2500 Series Routers

La información que se presenta en este documento se originó a partir de dispositivos dentro de un ambiente de laboratorio específico. All of the devices used in this document started with a cleared (default) configuration. Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener un comando antes de ejecutarlo.

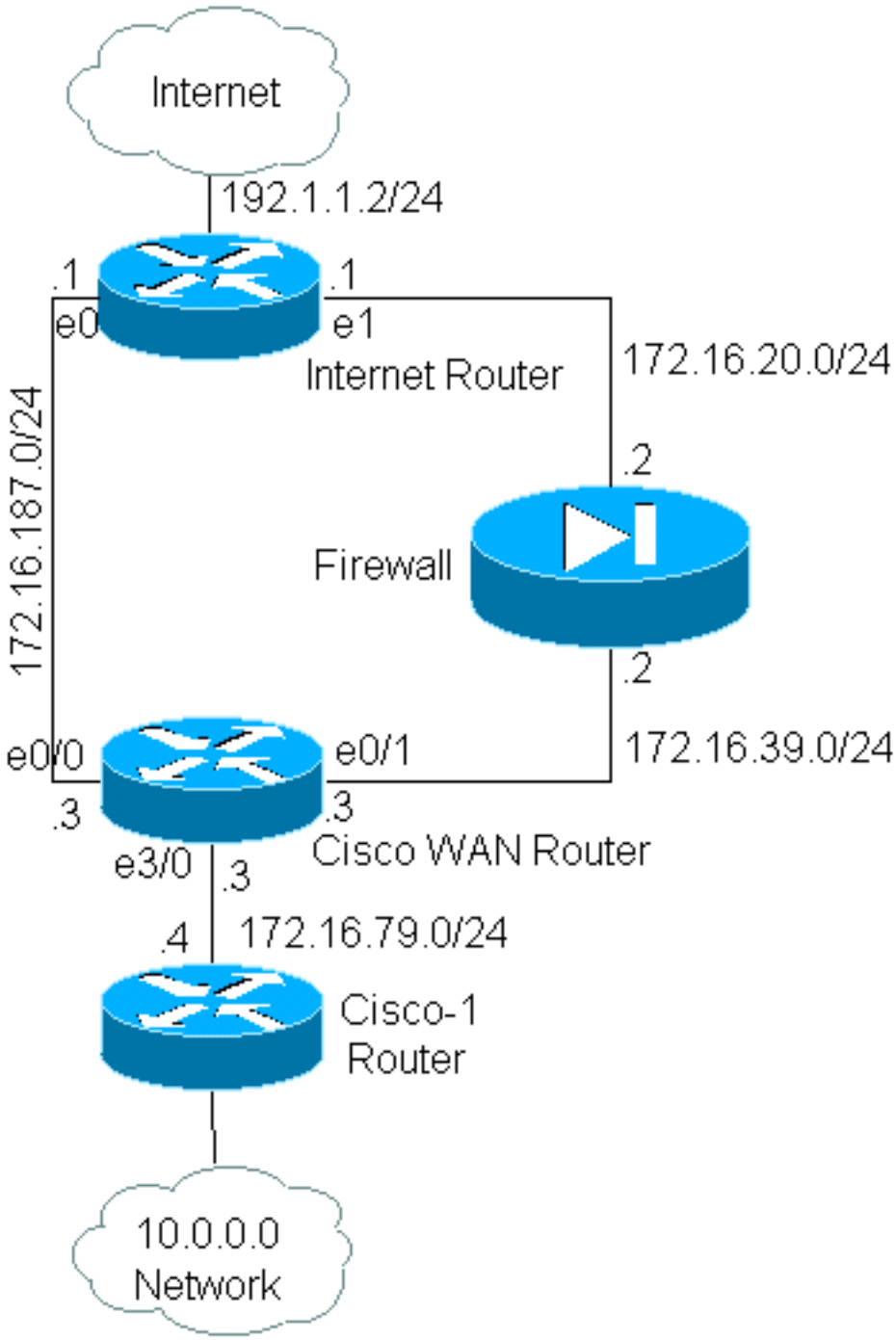
Convenciones

Para obtener más información sobre las convenciones del documento, consulte Convenciones de Consejos Técnicos de Cisco.

Configuraciones

En este ejemplo, con el ruteo normal, todos los paquetes de la red 10.0.0.0/8 a Internet tomarán la ruta a través de la interfaz Ethernet 0/0 del router WAN de Cisco (a través de la subred 172.16.187.0/24) ya que es la mejor trayectoria con la menor métrica. Con el ruteo basado en políticas, queremos que estos paquetes tomen el trayecto a través del firewall a Internet, el comportamiento de ruteo normal debe ser invalidado mediante la configuración del ruteo de políticas. El firewall traduce todos los paquetes de la red 10.0.0.0/8 a Internet, lo que sin embargo no es necesario para que funcione el ruteo de políticas.

Diagrama de la red



Configuración de firewall

La siguiente configuración del firewall se incluye para proporcionar una imagen completa. Sin embargo, no es parte del problema de ruteo de políticas explicado en este documento. El firewall de este ejemplo podría reemplazarse fácilmente por un PIX u otro dispositivo de firewall.

```
!
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
```

Refiérase a Comandos de Direccionamiento IP y Servicios para obtener más información sobre los comandos relacionados **ip nat**

En este ejemplo, el router WAN de Cisco está ejecutando el ruteo de políticas para asegurarse de que los paquetes IP que se originan en la red 10.0.0.0/8 se envíen a través del firewall. La siguiente configuración contiene una sentencia de lista de acceso que envía los paquetes que se originan en la red 10.0.0.0/8 al firewall.

Configuración de Cisco_WAN_Router

```
!
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
```

Consulte la documentación del comando **route-map** para obtener más información sobre los comandos **route-map** relacionados.

Nota: PBR no soporta la palabra clave **log** en el comando **access-list**. Si la palabra clave **log** está configurada, no muestra ningún resultado.

Configuración para el router Cisco-1

```
!
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
```

Configuración para Internet_Router

```
!
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
```

En la prueba de este ejemplo, un ping originado en 10.1.1.1 en el router Cisco-1, usando el comando **ping extendido**, se envió a un host en Internet. En este ejemplo, se utilizó 192.1.1.1 como dirección de destino. Para ver lo que está sucediendo en el router de Internet, se desactivó el fast switching mientras se utilizó el comando **debug ip packet 101 detail**.

Advertencia: El uso del comando **debug ip packet detail** en un router de producción puede causar una alta utilización de la CPU, lo que puede dar lugar a una degradación grave del rendimiento o a una interrupción de la red. Le recomendamos que lea detenidamente la sección Uso del Comando Debug de Comprensión de los Comandos Ping y Traceroute antes de utilizar los comandos debug.

Nota: La **sentencia permit icmp any any** se utiliza para filtrar la salida **debug ip packet**. Sin esta lista de acceso, el comando **debug ip packet** puede generar tanto resultado en la consola que el router bloquea. Utilice ACL extendidas cuando configure PBR. Si no se configura ninguna ACL para establecer los criterios de coincidencia, da como resultado que todo el tráfico se rutee mediante políticas.

```
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)
```

Como puede ver, el paquete nunca llegó al router de Internet. Los siguientes comandos de depuración, tomados del router WAN de Cisco, muestran por qué ocurrió esto.

```
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.
```

El paquete coincidió con la entrada de política 10 en el mapa de política net-10, como se esperaba. Entonces, ¿por qué el paquete no llegó al router de Internet?

```
"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
```

La salida **debug arp** muestra esto. El router WAN de Cisco intenta hacer lo que se le indicó e intenta colocar los paquetes directamente en la interfaz Ethernet 0/1. Esto requiere que el router envíe una solicitud de protocolo de resolución de direcciones (ARP) para la dirección de destino de 192.1.1.1, que el router se da cuenta que no está en esta interfaz, y por lo tanto la entrada ARP para esta dirección es "Incompleta", como se ve en el comando **show arp**. Luego ocurre una falla de encapsulación ya que el router no puede poner el paquete en el cable sin entrada ARP.

Si especificamos el firewall como el salto siguiente, podemos evitar este problema y hacer que el mapa de ruta funcione de la forma prevista:

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

Con el mismo comando **debug ip packet 101 detail** en el router de Internet, ahora vemos que el paquete está tomando el trayecto correcto. También podemos ver que el paquete ha sido

traducido a 172.16.255.1 por el firewall, y que la máquina a la que se hace ping, 192.1.1.1, ha respondido:

```
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:
```

El comando debug ip policy del router WAN de Cisco muestra que el paquete se reenvió al firewall, 172.16.39.2:

Comandos de depuración ejecutados desde Cisco_WAN_Router

```
"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
```

Routing basado en políticas para tráfico cifrado

Reenviar el tráfico descifrado a una interfaz de loopback para rutear el tráfico cifrado basado en el ruteo de políticas y luego hacer PBR en esa interfaz. Si el tráfico cifrado se pasa a través de un túnel VPN, `inhabilite ip cef` en la interfaz y termine el túnel vpn.

Información Relacionada

- Página de Soporte de IP Routing
- Página de Soporte de NAT

- Recursos y herramientas de soporte técnico
- Policy-Based Routing
- Cisco IOS Technologies
- Soporte Técnico y Documentación - Cisco Systems