

Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenciones](#)

[Configuraciones](#)

[Diagrama de la red](#)

[Configuración de firewall](#)

[Información Relacionada](#)

[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, un Firewall se está utilizando para traducir a 10.0.0.0/8 direcciones privadas a los direccionamientos del Enrutable por Internet que pertenecen a la subred 172.16.255.0/24. Vea el diagrama a continuación para una explicación visual.

Refiera al [Policy-Based Routing](#) para más información.

[prerrequisitos](#)

[Requisitos](#)

No hay requisitos específicos para este documento.

[Componentes Utilizados](#)

Este documento no se restringe a ningún hardware o versiones de software específico.

La información mostrada en este documento se basa en la siguiente versión de software y hardware.

- Cisco IOS® Software Release 12.3(3)
- Cisco 2500 Series Router

La información que se presenta en este documento se originó a partir de dispositivos dentro de un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se

pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener un comando antes de ejecutarlo.

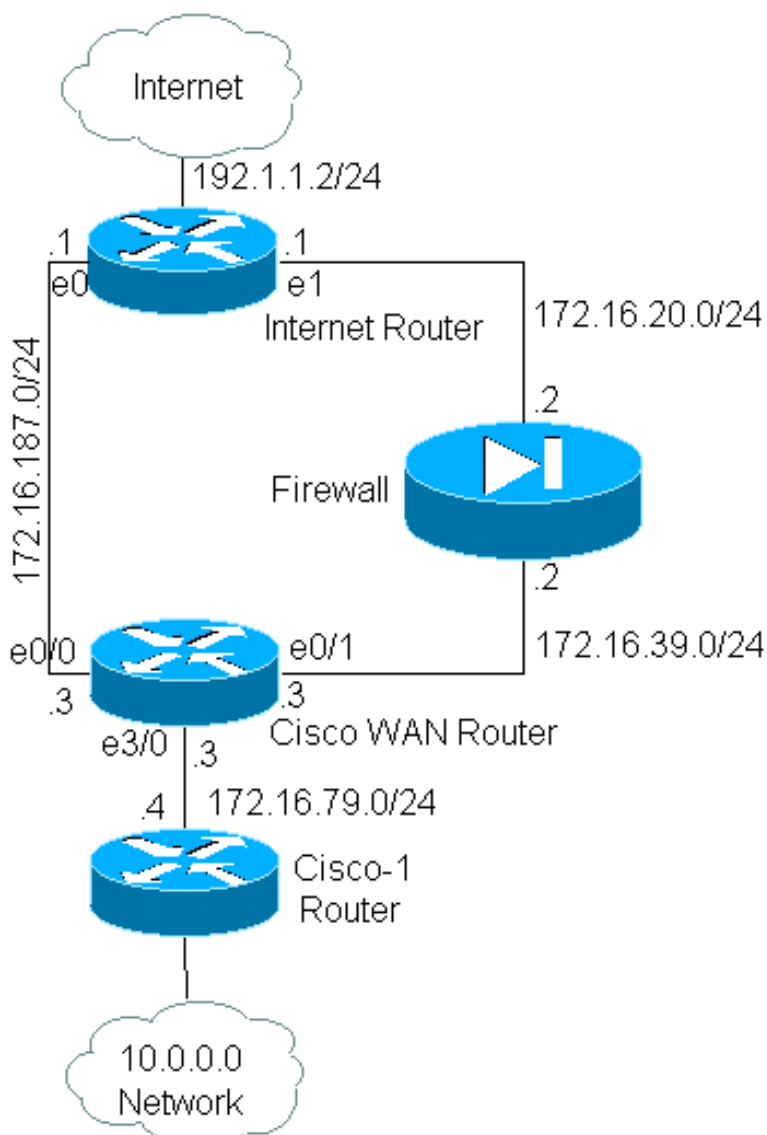
Convenciones

Para obtener más información sobre las convenciones del documento, consulte [Convenciones de Consejos Técnicos de Cisco](#).

Configuraciones

En este ejemplo, con la encaminamiento normal, todos los paquetes a partir de la red el 10.0.0.0/8 a Internet tomarán la trayectoria con las interfaces Ethernet 0/0 del Cisco WAN Router (vía la subred 172.16.187.0/24) pues es el mejor trayecto con el lo más menos posible métrico. Con el Policy-Based Routing quisiéramos que estos paquetes llevaran la trayectoria con el Firewall Internet, comportamiento del ruteo normal tenemos que ser reemplazados configurando el Policy Routing. El Firewall traduce todos los paquetes a partir de la red el 10.0.0.0/8 que va a Internet, que es sin embargo no necesario para que el Policy Routing trabaje.

Diagrama de la red



[Configuración de firewall](#)

La configuración de escudo de protección abajo se incluye para proporcionar una imagen completa. Sin embargo, no es parte de que el problema del Policy Routing explicó en este documento. El Firewall en este ejemplo se podía substituir fácilmente por un PIX u otro dispositivo de firewall.

Refiera al [IP Addressing y mantiene los comandos](#) para más información sobre los Comandos relacionados **nacionales del IP**

En este ejemplo, el Cisco WAN Router es Policy Routing corriente para asegurarse de que los paquetes del IP que originan de la red 10.0.0.0/8 serán enviados con el Firewall. La configuración abajo contiene una sentencia de lista de acceso que envíe los paquetes que originan a partir de la red el 10.0.0.0/8 al Firewall.

Configuración de Cisco_WAN_Router

Refiera a la documentación del [comando route-map](#) para más información sobre los Comandos relacionados del **route-map**.

Nota: La palabra clave del **registro** en el **comando access-list** no es soportada por el PBR. Si la palabra clave del **registro** configurada, él no muestra ninguna golpes.

[Configuración para el Cisco 1 Router](#)

[Configuración para Internet Router](#)

En la prueba de este ejemplo, un ping originado de 10.1.1.1 en el Cisco 1 Router, usando el [comando extended ping](#), fue enviado a un host en el Internet. En este ejemplo, 192.1.1.1 fue utilizado como la dirección destino. Para considerar qué está sucediendo en el router de Internet, la transferencia rápida fue apagada mientras que utilizaron al **comando debug ip packet 101 detail**.



Advertencia: Usando el **comando debug ip packet detail** en un router de producción puede causar CPU elevada la utilización, que puede dar lugar a una degradación grave del rendimiento o a una interrupción de la red. Recomendamos que usted lee cuidadosamente [usar la](#) sección de [comando Debug de entender los comandos ping and traceroute](#) antes de que usted utilice los comandos debug.

Nota: El ICMP del permiso del **access-list 101** cualquier cualquier declaración se utiliza para filtrar la salida de paquetes del IP del debug. Sin esta lista de acceso, el **comando debug ip packet** puede generar tanto la salida a la consola que el router bloquea para arriba. Utilice los ACL ampliados cuando usted configura el PBR. Si no se configura ningún ACL para establecer los criterios de concordancia, da lugar a todo el tráfico directiva-que es ruteado.

```
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# pingProtocol [ip]:Target IP address: 192.1.1.1Repeat count
[5]:Datagram size [100]:Timeout in seconds [2]:Extended commands [n]: ySource address or
interface: 10.1.1.1Type 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 usted puede ver, el paquete nunca lo hizo al router de Internet. Los comandos debug abajo, tomado del Cisco WAN Router, demostración porqué sucedió 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 correspondió con la entrada de política 10 en la correspondencia de políticas net-10, como se esperaba. ¿Tan porqué el paquete no lo hizo 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 Ethernet0/1Cisco_Wan_Router# show arpProtocol Address Age (min) Hardware Addr Type InterfaceInternet 172.16.39.3 - 00b0.64cb.eab1 ARPA Ethernet0/1Internet 172.16.39.2 3 0010.7b81.0b19 ARPA Ethernet0/1Internet 192.1.1.1 0 Incomplete ARPA
```

La salida **arp del debug** muestra esto. Las tentativas del Cisco WAN Router de hacer lo que fue dada instrucciones e intenta para poner los paquetes directamente sobre los Ethernets 0/1 interfaz. Esto requiere que el router envíe una petición de Address Resolution Protocol (ARP) para la dirección destino de 192.1.1.1, que el router realiza no está en esta interfaz, y por lo tanto la entrada ARP para este direccionamiento es "incompleta," según lo visto por el comando **show arp**. Una falla de encapsulación entonces ocurre pues el router no puede poner el paquete en el alambre sin la entrada ARP.

Especificando el Firewall como el Next-Hop, podemos prevenir este problema y hacer el trabajo del route-map según lo previsto:

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

Usando el mismo comando **debug ip packet 101 detail** en el router de Internet, ahora vemos que el paquete está tomando la trayectoria correcta. Podemos también ver que el paquete ha sido traducido a 172.16.255.1 por el Firewall, y que la máquina que era hecha ping, 192.1.1.1, ha contestado:

```
Cisco_1# pingProtocol [ip]:Target IP address: 192.1.1.1Repeat count [5]:Datagram size [100]:Timeout in seconds [2]:Extended commands [n]: ySource address or interface: 10.1.1.1Type 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 msResults 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

```
Cisco_1# ping Protocol [ip]:Target IP address: 192.1.1.1Repeat count [5]:Datagram size [100]:Timeout in seconds [2]:Extended commands [n]: ySource address or interface: 10.1.1.1Type 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 msResults 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:
```

[La directiva basó la encaminamiento para el tráfico encriptado](#)

Transmita al tráfico desencriptado un Loopback Interface para rutear el tráfico encriptado basado en el Policy Routing y después hacer el PBR en esa interfaz. Si el tráfico encriptado se pasa sobre un túnel VPN después el `cef` del IP de la neutralización en la interfaz, y termina el túnel del vpn.

[Información Relacionada](#)

- [Página de Soporte de IP Routing](#)
- [Página de Soporte de NAT](#)
- [Herramientas de soporte técnico y recursos](#)
- [Ruteo basado en políticas](#)
- [Cisco IOS Technologies](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)