# Entendendo o Roteamento de Política

## Contents



## Introduction

O roteamento com base em políticas fornece uma ferramenta de encaminhamento e roteamento de pacotes de dados com base nas políticas definidas pelos administradores da rede. De fato, é uma maneira de ter as decisões de políticas de protocolo de roteamento de anulação. O roteamento baseado em políticas inclui um mecanismo para aplicação seletiva de políticas com base em lista de acesso, tamanho de pacote ou outros critérios. As ações tomadas podem incluir roteamento de pacotes nas rotas definidas pelo usuário, ajuste da precedência, tipo de bits do serviço etc.

Neste documento, um firewall está sendo usado para converter endereços privados 10.0.0.0/8 em endereços roteáveis pela Internet pertencentes à sub-rede 172.16.255.0/24. Consulte o diagrama abaixo para obter uma explicação visual.

Consulte Roteamento Baseado em Política para obter mais informações.

## Prerequisites

### Requirements

Não existem requisitos específicos para este documento.

### Componentes Utilizados

Este documento não está restrito a nenhuma versão específica de hardware ou software.

As informações mostradas neste documento são baseadas nas versões de software e hardware abaixo.

- Software Cisco IOS® versão 12.3(3)

- Cisco 2500 Series Routers

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. All of the devices used in this document started with a cleared (default) configuration. Se você estiver trabalhando em uma rede ativa, certifique-se de que entende o impacto potencial de qualquer comando antes de utilizá-lo.

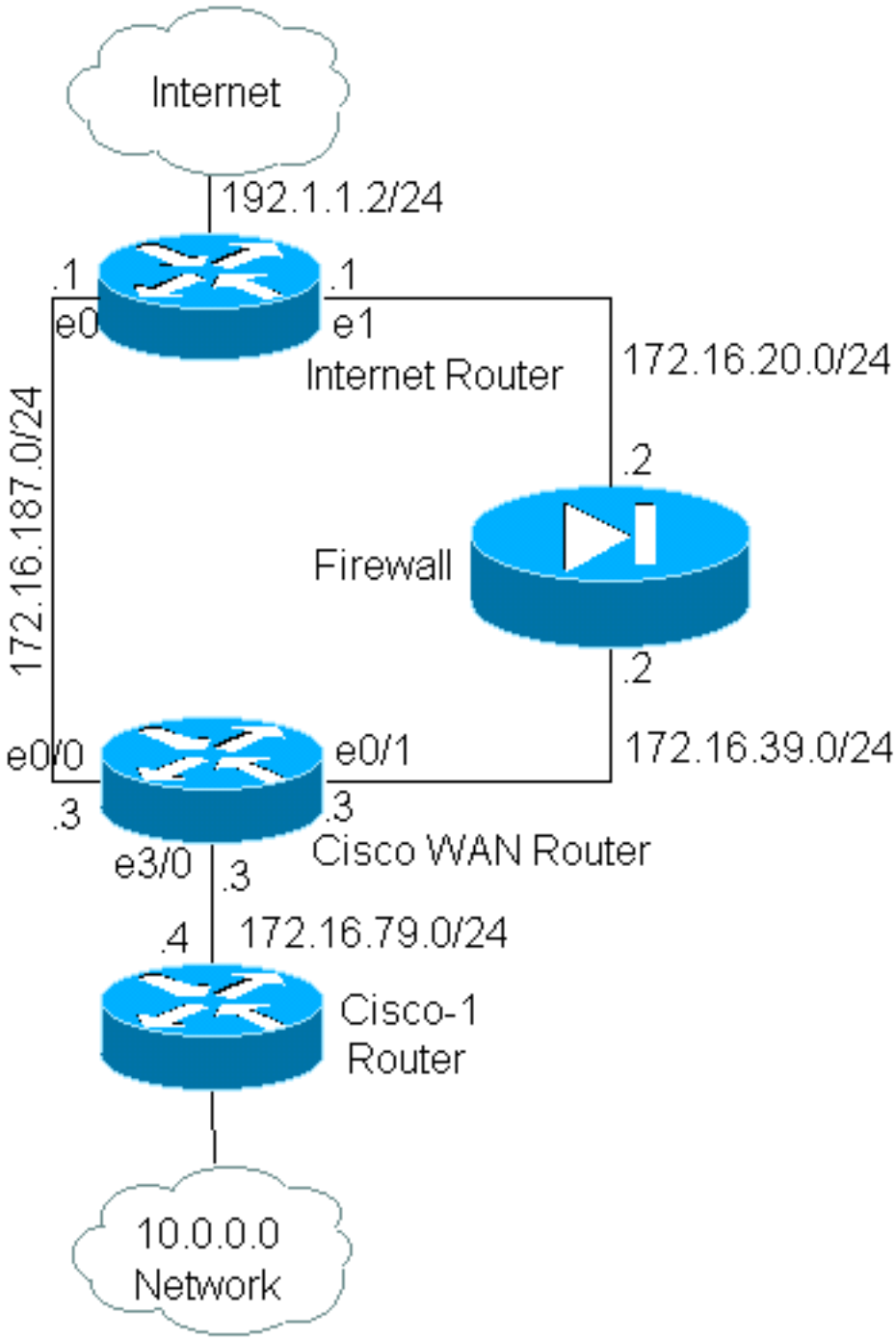
### Conventions

Para obter mais informações sobre convenções de documento, consulte as Convenções de dicas técnicas Cisco.

## Configurações

Neste exemplo, com o roteamento normal, todos os pacotes da rede 10.0.0.0/8 para a Internet seguirão o caminho através da interface ethernet 0/0 do Cisco WAN Router (através da sub-rede 172.16.187.0/24), pois é o melhor caminho com a menor métrica. Com o roteamento baseado em políticas, queremos que esses pacotes sigam o caminho pelo Firewall até a Internet, o comportamento normal de roteamento deve ser substituído pela configuração do roteamento de política. O firewall converte todos os pacotes da rede 10.0.0.0/8 indo para a Internet, o que, no entanto, não é necessário para que o roteamento de política funcione.

### Diagrama de Rede




## Configuração para firewall

A configuração de firewall abaixo está incluída para fornecer uma imagem completa. No entanto, ele não faz parte do problema de roteamento de política explicado neste documento. O firewall neste exemplo pode ser facilmente substituído por um PIX ou outro 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
```

Consulte Endereçamento IP e Comandos de Serviços para obter mais informações sobre comandos relacionados ao **ip nat**

Neste exemplo, o Cisco WAN Router está executando o roteamento de política para garantir que os pacotes IP originários da rede 10.0.0.0/8 serão enviados através do firewall. A configuração abaixo contém uma instrução de lista de acesso que envia pacotes originados da rede 10.0.0.0/8 para o firewall.

### Configuração do 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 a documentação do comando **route-map** para obter mais informações sobre os comandos relacionados ao **mapa de rota**.

**Observação:** a palavra-chave **log** no comando **access-list** não é suportada pelo PBR. Se a palavra-chave **log** estiver configurada, ela não mostrará nenhum acerto.

### Configuração do roteador 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
```

## Configuração 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
```

Ao testar este exemplo, um ping originado de 10.1.1.1 no Cisco-1 Router, usando o comando **ping estendido**, foi enviado a um host na Internet. Neste exemplo, 192.1.1.1 foi usado como o endereço de destino. Para ver o que está acontecendo no Internet Router, a comutação rápida foi desativada enquanto o comando **debug ip packet 101 detail** foi usado.

**Aviso:** o uso do comando **debug ip packet detail** em um roteador de produção pode causar alta utilização da CPU, o que pode resultar em uma grave degradação do desempenho ou em uma interrupção da rede. Recomendamos que você leia cuidadosamente a seção Using the Debug Command de Understanding the Ping and Traceroute Commands antes de usar os comandos debug.

**Observação:** a instrução **access-list 101 permit icmp any any any** é usada para filtrar a saída do **pacote debug ip**. Sem essa lista de acesso, o comando **debug ip packet** pode gerar tanta saída para o console que o roteador trava. Use ACLs estendidas ao configurar o PBR. Se nenhuma ACL for configurada para estabelecer os critérios de correspondência, isso resultará em todo o tráfego que está sendo roteado por 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 você pode ver, o pacote nunca chegou ao Roteador de Internet. Os comandos debug abaixo, retirados do Cisco WAN Router, mostram por que isso aconteceu.

```
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.
```

O pacote correspondeu à entrada de política 10 no mapa de política net-10, conforme esperado. Então por que o pacote não chegou ao Roteador 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
```

A saída **debug arp** mostra isso. O roteador WAN da Cisco tenta fazer o que foi instruído e tenta colocar os pacotes diretamente na interface ethernet 0/1. Isso exige que o roteador envie uma solicitação do Address Resolution Protocol (ARP) para o endereço destino 192.1.1.1, que o roteador percebe que não está nessa interface, e, portanto, a entrada ARP para esse endereço é "Incompleto", como visto pelo comando **show arp**. Uma falha de encapsulamento ocorre quando o roteador não consegue colocar o pacote no fio sem entrada ARP.

Ao especificar o firewall como o próximo salto, podemos evitar esse problema e fazer com que o mapa de rotas funcione como o esperado:

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

Usando o mesmo comando **debug ip packet 101 detail** no Roteador Internet, agora vemos que o pacote está tomando o caminho correto. Também podemos ver que o pacote foi traduzido para

172.16.255.1 pelo firewall, e que a máquina que está fazendo ping, 192.1.1.1, respondeu:

```
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:
```

O comando debug ip policy no Roteador Cisco WAN mostra que o pacote foi encaminhado ao firewall, 172.16.39.2:

### Execução de comandos de depuração do 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
```

### Roteamento baseado em políticas para tráfego criptografado

Encaminhe o tráfego descriptografado para uma interface de loopback para rotear o tráfego criptografado com base no roteamento de política e faça o PBR nessa interface. Se o tráfego criptografado for passado por um túnel VPN, `desative ip cef` na interface e termine o túnel vpn.

## Informações Relacionadas

- Página de Suporte do IP Routing
- Página de suporte de NAT
- Ferramentas e recursos de suporte técnico

- Roteamento baseado em políticas
- Tecnologias Cisco IOS
- Suporte Técnico e Documentação - Cisco Systems