Entendendo o Roteamento de Política

Índice

Introdução

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 traduzir 10.0.0.0/8 endereços privados nos endereços do Internet roteável que pertencem à sub-rede 172.16.255.0/24. Veja o diagrama abaixo para uma explicação visual.

Refira o roteamento baseado em política para mais informação.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

Este documento não é restringido a nenhuma hardware ou versões de software específica.

A informação mostrada neste documento é baseada nas versões de software e hardware abaixo.

- Liberação do Cisco IOS ® Software 12.3(3)

- Cisco 2500 Series Routers

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se você estiver trabalhando em uma rede ativa, certifique-se de que entende o impacto potencial de qualquer comando antes de utilizá-lo.

Convenções

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

Configurações

Neste exemplo, com roteamento normal, todos os pacotes da rede 10.0.0.0/8 ao Internet tomarão o trajeto com os Ethernet de interface 0/0 do Cisco WAN Router (através da sub-rede 172.16.187.0/24) porque é o melhor caminho com menos métrica. Com roteamento baseado em política que nós queremos estes pacotes tomar o trajeto com o Firewall ao Internet, comportamento de roteamento normal tem que ser cancelado configurando o roteamento de política. O Firewall traduz todos os pacotes da rede 10.0.0.0/8 que vai ao Internet, que é contudo não necessário para que o roteamento de política trabalhe.

Diagrama de Rede

Configuração para firewall

A configuração de firewall abaixo é incluída para fornecer uma imagem completa. Contudo, não é parte da edição do roteamento de política explicada neste documento. O Firewall neste exemplo podia facilmente ser substituído por um PIX ou por um 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
```

Refira o endereçamento de IP e preste serviços de manutenção a comandos para obter mais informações sobre dos comandos relacionados **nat IP**

Neste exemplo, o Cisco WAN Router é roteamento de política running para assegurar-se de que

os pacotes IP que originam da rede 10.0.0.0/8 estejam enviados com o Firewall. A configuração abaixo contém uma instrução de lista de acesso que envie os pacotes que originam da rede 10.0.0.0/8 ao 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
```

Refira a documentação do comando route-map para obter mais informações sobre dos comandos relacionados do **mapa de rotas**.

Nota: A palavra-chave do **log no comando access-list** não é apoiada pelo PBR. Se a palavra-chave do **log** configurada, ele não mostra nenhuma batidas.

Configuração para o Cisco 1 Router

```
!
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
```

Em testar este exemplo, um sibilo originado de 10.1.1.1 no Cisco 1 Router, utilização Neste exemplo, 192.1.1.1 foi usado como o endereço de destino. Para considerar o que está acontecendo no roteador de Internet, o interruptor rápido foi desligado quando o **comando debug ip packet 101 detail** foi usado.

aviso: Usar o **comando debug ip packet detail em um** roteador de produção pode causar a utilização elevada da CPU, que pode conduzir a uma degradação séria do desempenho ou a uma parada de rede. Nós recomendamos que você lê com cuidado a utilização da seção de comando Debug de compreender os comandos ping and traceroute antes que você use comandos debug.

Nota: O ICMP da licença do access-list 101 toda a qualquer indicação é usado para filtrar a saída do **pacote debugar IP**. Sem esta lista de acessos, o **comando debug ip packet** pode gerar tanto a saída ao console que o roteador trava acima. Use ACL extendido quando você configura o PBR. Se nenhum ACL é configurado a fim estabelecer os critérios de verificação de repetição de dados, conduz a todo o tráfego que é política-roteado.

```
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 fê-lo ao roteador de Internet. Os comandos debug abaixo, tomado do Cisco WAN Router, mostra porque isto 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 combinou a entrada de política 10 no mapa de política net-10, como esperado. Assim porque o pacote não o fez 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 **arp debugar** mostra esta. As tentativas do Cisco WAN Router de fazer o que foi instruído

e tenta pôr os pacotes diretamente nos Ethernet 0/1 de relação. Isto exige que o roteador envia uma requisição de protocolo de resolução de endereço (ARP) para o endereço de destino de 192.1.1.1, que o roteador realiza não está nesta relação, e daqui a entrada de ARP para este endereço está “incompleta,” como visto pelo **comando show arp**. Uma falha de encapsulamento ocorre então porque o roteador é incapaz de pôr o pacote sobre o fio sem a entrada de ARP.

Especificando o Firewall como o salto seguinte, nós podemos impedir este problema e fazer o mapa de rotas trabalhar como pretendido:

```
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 de Internet, nós vemos agora que o pacote está tomando o trajeto correto. Nós podemos igualmente ver que o pacote esteve traduzido a 172.16.255.1 pelo Firewall, e que a máquina que está sendo sibilada, 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
```

A política baseou o roteamento para o tráfego criptografado

Envie o tráfego decifrado a uma interface de loopback a fim distribuir o tráfego criptografado baseado no roteamento de política e fazer então o PBR nessa relação. Se o tráfego enrypted é passado sobre um túnel VPN a seguir o `cef do desabilitação IP na` relação, e termina o túnel do vpn.

Informações Relacionadas

- Página de Suporte do IP Routing

- Página de suporte de NAT
- Ferramentas de suporte técnico e recursos
- Roteamento baseado em política
- Tecnologias do IOS da Cisco
- Suporte Técnico e Documentação - Cisco Systems