Het begrip beleidsrouting

Inhoud

Inleiding

Op beleid gebaseerde routing biedt een gereedschap voor het verzenden en routeren van gegevenspakketten die zijn gebaseerd op beleid dat door netwerkbeheerders wordt gedefinieerd. In feite is het een manier om het beleid te hebben om het routingprotocol besluiten te vernietigen. Op beleid gebaseerde routing omvat een mechanisme voor het selectief toepassen van beleid op basis van toegangslijsten, pakketgrootte of andere criteria. De genomen acties kunnen het verzenden van pakketten op door gebruikers bepaalde routes omvatten, het plaatsen van de voorrang, type van de dienstbits, enz.

In dit document wordt een firewall gebruikt om 10.0.0.0/8 privé adressen in Internet-routeerbare adressen te vertalen die tot 172.16.255.0/24 behoren. Zie het diagram hieronder voor een visuele uitleg.

Raadpleeg Op beleid gebaseerde routing voor meer informatie.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

Dit document is niet beperkt tot specifieke hardware- of softwareversies.

De informatie in dit document is gebaseerd op de hieronder genoemde software- en hardwareversies.

- Cisco IOS-softwarerelease 12.3(3)S

- Cisco 2500 Series routers

De informatie in dit document is gebaseerd op apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als u in een levend netwerk werkt, zorg er dan voor dat u de potentiële impact van om het even welke opdracht begrijpt alvorens het te gebruiken.

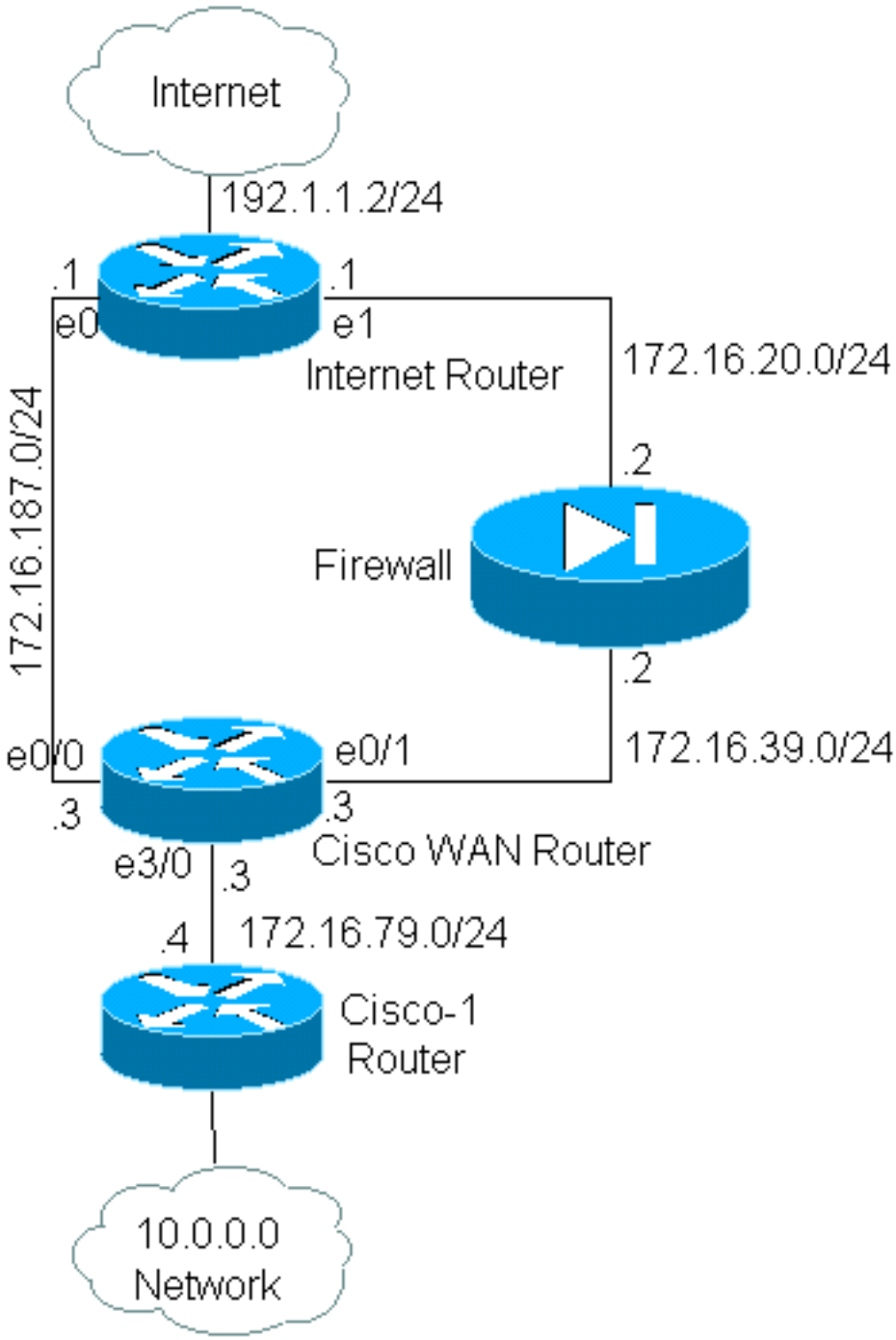
Conventies

Zie de Cisco Technical Tips Convention voor meer informatie over documentconventies.

Configuraties

In dit voorbeeld, met normale routing, zullen alle pakketten van het 10.0.0.0/8 netwerk naar het internet het pad door interface Ethernet 0/0 van Cisco WAN Router (via 172.16.187.0/24 subnet) nemen aangezien het het beste pad met minste metrische snelheid is. Met op beleid gebaseerde routing willen we dat deze pakketten het pad door de firewall naar het internet nemen, dan moet het normale routinggedrag worden gecorrigeerd door het configureren van beleidsrouting. De firewall vertaalt alle pakketten van het netwerk 10.0.0.0/8 naar het internet, wat echter niet nodig is voor het beleid routing om te werken.

Netwerkdiagram



Configuratie voor firewall

De configuratie van de firewall is hieronder opgenomen om een volledig beeld te geven. Het maakt echter geen deel uit van de beleidsroutingkwestie die in dit document wordt toegelicht. De firewall in dit voorbeeld kan eenvoudig door een PIX of een ander firewallapparaat worden vervangen.

```
!
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
```

Raadpleeg de opdrachten voor IP-adressering en -services voor meer informatie over **IP-**gerelateerde opdrachten

In dit voorbeeld, voert de Cisco WAN router beleid in dat routing om te verzekeren dat IP-pakketten van het 10.0.0.0/8 netwerk door de firewall zullen worden verzonden. De configuratie hieronder bevat een verklaring van de toegangslijst die pakketten van 10.0.0.0/8 netwerk naar de firewall stuurt.

Configuratie van 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
```

Raadpleeg de documentatie van de route-map voor meer informatie over **route-map** gerelateerde opdrachten.

Opmerking: het **logsleutelwoord** in de **toegangslijst** opdracht wordt niet ondersteund door PBR. Als het **logsleutelwoord** gevormd wordt, toont het geen hits.

Configuratie van 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
```

Configuratie van 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
```

In het testen van dit voorbeeld, werd een ping gesourcet van 10.1.1.1 op de router Cisco-1, die het **uitgebreide** pingopdracht gebruikt, naar een host op het internet verzonden. In dit voorbeeld werd 192.1.1.1 gebruikt als bestemmingsadres. Om te zien wat op de router van Internet gebeurt, werd de snelle omschakeling uitgeschakeld toen het **debug IP pakket 101 detail** bevel werd gebruikt.

Waarschuwing: het gebruik van **de debug IP-pakketdetailopdracht** op een productierouter kan een hoog CPU-gebruik veroorzaken, wat kan leiden tot een ernstige verslechtering van de prestaties of een netwerkstoring. Wij raden u aan om zorgvuldig de sectie van de Debug Opdracht gebruiken van het Beginnen van de Opdrachten Ping en Traceroute lezen voordat u debug opdrachten gebruikt.

Opmerking: De **toegangslijst 101** staat **icmp om het even welke** verklaring gebruikt om de **debug IP-pakketuitvoer** te filteren. Zonder deze toegangslijst, kan het **debug IP-pakketbevel** zoveel output naar de console genereren dat de router vastloopt. Gebruik uitgebreide ACL's wanneer u PBR-systemen vormt. Als er geen ACL is ingesteld om de wedstrijdcriteria vast te stellen, resulteert dit in al het verkeer dat politiek wordt routeerd.

```
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)
```

Zoals u kunt zien, heeft het pakje het nooit op de Internet router gebracht. De debug opdrachten hieronder, die van de Cisco WAN-router zijn genomen, tonen waarom dit is gebeurd.

```
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.
```

Het pakje kwam overeen met beleidstitel 10 in de netto-10 beleidskaart, zoals verwacht. Waarom heeft het pakket het niet gemaakt op de Internet Router?

```
"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
```

De **debug arp** uitvoer toont dit. De router van Cisco WAN probeert te doen wat hij heeft geleerd en probeert de pakketten rechtstreeks op de Ethernet 0/1-interface te zetten. Dit vereist dat de router een verzoek van het Protocol van de Resolutie van het Adres (ARP) voor het bestemmingsadres van 192.1.1.1 verzenden, wat de router zich realiseert is niet op deze interface en daarom is de ARP ingang voor dit adres "Onvolledig," zoals gezien door het bevel van de **show arp**. Een insluitingsfout komt dan voor aangezien de router het pakket niet op de draad zonder ARP-ingang kan plaatsen.

Door de firewall als de volgende-hop te specificeren, kunnen we dit probleem voorkomen en de route-kaart werk maken zoals bedoeld:

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

Met het zelfde **debug IP pakket 101 detail** bevel op de router van Internet, zien wij nu dat het

pakket het juiste pad neemt. We kunnen ook zien dat het pakje vertaald is naar 172.16.255.1 door de firewall en dat de machine die gepingd wordt, 192.1.1.1, geantwoord heeft:

```
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:
```

Het opdracht **ip-beleid** op de Cisco WAN-router toont aan dat het pakket naar de firewall is doorgestuurd, 172.16.39.2:

Debug Commons uitvoeren vanuit 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
```

Op beleid gebaseerde routing voor versleuteld verkeer

Doorsturen van het gedecrypteerde verkeer naar een loopback interface om het gecodeerde verkeer te leiden gebaseerd op beleid routing en dan PBR op die interface. Als het versleutelde verkeer via een VPN-tunnel wordt doorgegeven, `schakelt` u `ip-cef` op de interface `uit` en sluit u de VPN-tunnel af.

Gerelateerde informatie

- Ondersteuningspagina voor IP-routing

- NAT-ondersteuningspagina
- Tools en bronnen voor technische ondersteuning
- Op beleid gebaseerde routing
- Cisco IOS-technologieën
- Technische ondersteuning en documentatie – Cisco Systems