Présentation du routage basé sur une stratégie

Contenu

Introduction

Le PBR (Policy-Based Routing) fournit un outil pour transmettre et router des paquets de données selon des politiques définies par des administrateurs réseau. En effet, cela permet d'avoir une politique qui ignore les décisions de protocole de routage. Le PBR (Policy-Based Routing) inclut un mécanisme d'application sélective des stratégies basé sur la liste d'accès, la taille de paquet ou d'autres critères. Les mesures prises peuvent inclure le routage de paquets sur des routes définies par l'utilisateur, le paramétrage de la priorité, le type de bits de service, etc.

Dans ce document, un pare-feu est utilisé pour traduire l'adresse privée 10.0.0.0/8 en adresses routables sur l'Internet appartenant au sous-réseau 172.16.255.0/24. Voyez le diagramme ci-dessous pour une explication visuelle.

Référez-vous au PBR (Policy-Based Routing) pour plus d'informations.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Components Used

Ce document n'est pas limité à des versions de matériel ou de logiciel spécifiques.

Les informations fournies dans ce document sont basées sur les versions de logiciel et de matériel ci-dessous.

- Logiciel Cisco IOS® Version 12.3(3)

- Routeurs de la gamme Cisco 2500

Les informations présentées dans ce document ont été créées à partir de périphériques dans un environnement de laboratoire spécifique. All of the devices used in this document started with a cleared (default) configuration. Si vous travaillez dans un réseau opérationnel, assurez-vous de bien comprendre l'impact potentiel de toute commande avant de l'utiliser.

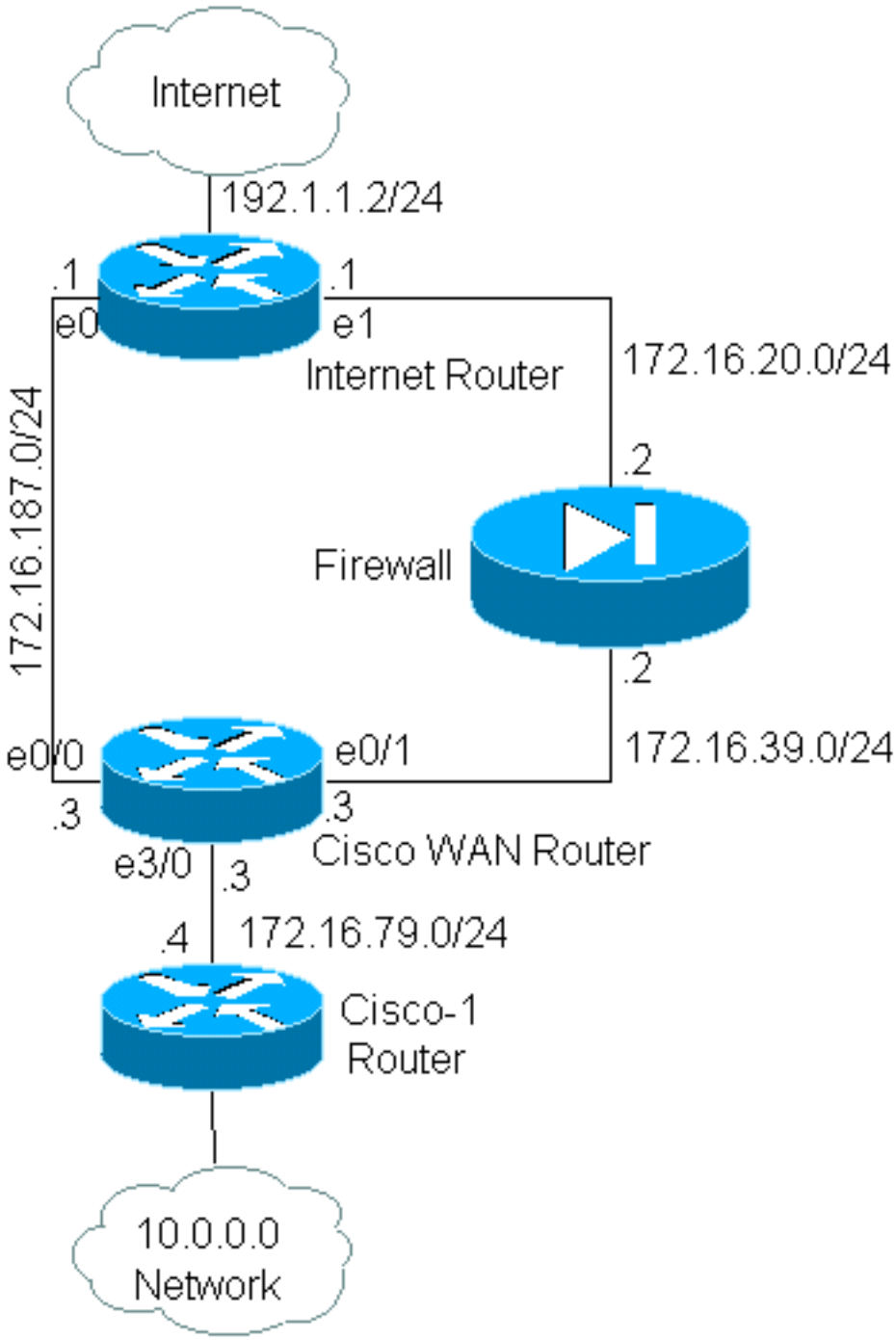
Conventions

Pour plus d'informations sur les conventions des documents, référez-vous aux Conventions utilisées pour les conseils techniques de Cisco.

Configurations

Dans cet exemple, avec un routage normal, tous les paquets du réseau 10.0.0.0/8 vers l'Internet passeront par l'interface ethernet 0/0 du routeur WAN Cisco (par l'intermédiaire du sous-réseau 172.16.187.0/24) car c'est le meilleur chemin avec la plus petite métrique. Avec le PBR (Policy-Based Routing), nous voulons que des paquets passent par le pare-feu pour accéder à Internet, le comportement de routage normal doit être ignoré en configurant le routage spécifique. Le pare-feu traduit tous les paquets du réseau 10.0.0.0/8 allant vers Internet, ce qui n'est cependant pas nécessaire pour que le routage spécifique fonctionne.

Diagramme du réseau



Configuration pour le pare-feu

La configuration de pare-feu ci-dessous est incluse pour fournir une représentation complète. Cependant, ce n'est pas une partie de la question du routage spécifique expliquée dans ce document. Le pare-feu dans cet exemple pourrait facilement être remplacé par un PIX ou un périphérique de pare-feu différent.

```
!
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
```

Référez-vous à Adressage IP et commandes de services pour plus d'informations sur les commandes associées à **ip nat**

Dans cet exemple, le routeur WAN Cisco exécute un routage spécifique pour s'assurer que les paquets IP provenant du réseau 10.0.0.0/8 seront envoyés par le pare-feu. La configuration ci-dessous contient une instruction de liste d'accès qui envoie des paquets provenant du réseau 10.0.0.0/8 au pare-feu.

Configuration pour 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
```

Référez-vous à la documentation sur la commande route-map pour plus d'informations sur les commandes associées à route-map.

Remarque : Le mot clé **log** de la commande **access-list** n'est pas pris en charge par PBR. Si le **mot clé log est configuré, il n'affiche aucun résultat.**

Configuration pour routeur 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
```

Configuration pour 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 testant cet exemple, un ping originaire de 10.1.1.1 sur le routeur Cisco-1, utilisant la commande extended ping, a été envoyé à un hôte sur l'Internet. Dans cet exemple, 192.1.1.1 a été utilisé comme adresse de destination. Pour voir ce qui se produit sur le routeur Internet, la commutation rapide a été désactivée tandis que la commande **debug ip packet 101 detail** était utilisée.

Avertissement : L'utilisation de la commande **debug ip packet detail** sur un routeur de production peut entraîner une utilisation élevée du CPU, ce qui peut entraîner une grave dégradation des performances ou une panne de réseau. Nous recommandons que vous lisiez soigneusement la section Utilisation de la commande Debug de la Compréhension des commandes Ping et Traceroute avant d'utiliser des commandes de débogage.

Remarque : La **liste d'accès 101 permit icmp any any any** est utilisée pour filtrer la sortie du **paquet ip debug**. Sans cette liste d'accès, la commande **debug ip packet peut produire tellement en sortie de console que le routeur se bloque.** Utilisez des ACL étendues quand vous configurez PBR. Si aucun ACL n'est configuré afin d'établir les critères de correspondance, cela a comme conséquence d'appliquer un routage spécifique à tout le trafic.

```
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)
```

Comme vous pouvez voir, le paquet n'a jamais atteint le routeur Internet. Les commandes de débogage ci-dessous, prises du routeur WAN Cisco, montrent pourquoi ceci s'est produit.

```
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.
```

Le paquet a apparié l'entrée de stratégie 10 dans la carte de stratégie net-10, comme prévu. Alors pourquoi le paquet n'a-t-il pas atteint le routeur 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 sortie **debug arp montre ceci.** Le routeur WAN Cisco essaye d'exécuter les instructions qui lui ont été envoyées et essaye de mettre les paquets directement sur l'interface ethernet 0/1. Ceci exige que le routeur envoie une demande de Protocole de résolution d'adresse (ARP) pour l'adresse de destination de 192.1.1.1, ce que le routeur fait n'est pas sur cette interface, et par conséquent l'entrée ARP pour cette adresse est « Incomplete », comme vu par la commande **show arp.** Une défaillance d'encapsulation se produit alors car le routeur ne peut pas mettre le paquet sur le réseau sans entrée ARP.

En spécifiant le pare-feu en tant que prochain saut, nous pouvons empêcher ce problème et faire fonctionner la commande route-map comme prévu :

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

!

Utilisant la même commande **debug ip packet 101 detail sur le routeur Internet, nous voyons maintenant que le paquet prend le bon chemin.** Nous pouvons également voir que le paquet a été traduit à 172.16.255.1 par le pare-feu, et que la machine à laquelle un ping a été envoyé, 192.1.1.1, a répondu :

```
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:
```

La commande **debug ip policy sur le routeur WAN Cisco montre que le paquet a été transmis au pare-feu, 172.16.39.2 :**

Commandes de débogage exécutées depuis le 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
```

PBR (Policy-Based Routing) pour trafic crypté

Transmettez le trafic décrypté à une interface de bouclage afin de router le trafic crypté en fonction du routage spécifique, puis appliquez PBR à cette interface. Si le trafic crypté passe par un tunnel VPN, alors exécutez `disable ip cef sur l'interface, et terminez le tunnel vpn.`

Informations connexes

- Page de support pour le routage IP
- Page de support NAT
- Outils et ressources d'assistance technique
- Policy-based routing
- Technologies Cisco IOS
- Support et documentation techniques - Cisco Systems