Сведения о маршрутизации на основе политик

Содержание

Введение

Маршрутизация на основе политик является инструментом для переадресации и маршрутизации пакетов данных, в котором используются политики, определяемые сетевым администратором. В реальности это позволяет обладать политикой принятия решений переопределения протокола маршрутизации. Маршрутизация на основе политик включает в себя механизм для выборочного применения политик, основанных на списке контроля доступа, размере пакета или других критериях. Выполняемыми действиями могут являться — маршрутизация пакетов по маршрутам, определяемым пользователем, установка приоритетов, установка битов типа обслуживания и т.д.

В данном документе брандмауэр используется для преобразования частных адресов 10.0.0.0/8 в адреса, маршрутизируемые в Интернет и принадлежащие к подсети 172.16.255.0/24. Для получения наглядного представления см. нижеприведенную схему.

Дополнительные сведения см. в документе Маршрутизация на основе политик.

Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

Этот документ не ограничен никакими определенными аппаратными средствами или версиями программного обеспечения.

Сведения, содержащиеся в данном документе, приведены для следующих версий программного и аппаратного обеспечения.

- Cisco IOS® Software Release 12.3(3)
- Маршрутизаторы Cisco серии 2500

Сведения, содержащиеся в данном документе, были получены с устройств в специальной лабораторной среде. Все устройства, описанные в данном документе, были запущены с конфигурацией по умолчанию. При работе с реальной сетью необходимо полностью осознавать возможные результаты использования всех команд.

Условные обозначения

Дополнительные сведения об условных обозначениях см. в документе Технические рекомендации Cisco. Условные обозначения.

Конфигурации

В этом примере с помощью нормальной маршрутизации все пакеты, направляемые из сети 10.0.0.0/8 в Интернет, будут проходить через интерфейс Ethernet 0/0 маршрутизатора Cisco WAN (через подсеть 172.16.187.0/24), так как это наилучший путь с наименьшей метрикой. С помощью маршрутизации на основе политик эти пакеты направляются через брандмауэр в Интернет, при этом нормальная маршрутизация должна быть переопределена путем настройки маршрутизации на основе политик. Брандмауэр транслирует все пакеты, передаваемые из сети 10.0.0.0/8 в Интернет, что, однако, не требуется для работы маршрутизации на основе политик.

Схема сети

Конфигурация межсетевого экрана

Нижеприведенная конфигурация брандмауэра приводится для полноты картины. Однако это не является частью проблемы маршрутизации на основе политик, рассматриваемой в данном документе. Брандмауэр в этом примере может быть легко заменен PIX или другим межсетевым устройством.

```
!
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
```

См. IP-адресацию и Команды Сервисов для получения дополнительной информации о связанных командах **ip nat**

В данном примере Маршрутизатор Cisco WAN выполняет маршрутизацию в соответствии с политикой, чтобы гарантировать, что пакеты IP, происходящие из 10.0.0.0/8 сети, будут переданы через межсетевой экран. Нижеприведенная конфигурация содержит выражение списка контроля доступа, которое отправляет на брандмауэр пакеты, исходящие из сети 10.0.0.0/8.

Конфигурация для 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
```

Дополнительные сведения о командах, родственных route-map, см. в документации по командеroute-map.

Примечание: Регистрационное ключевое слово в **команде access-list** не поддерживается PBR. Если **регистрационное** ключевое слово настроило, оно не показывает соответствий.

Конфигурация маршрутизатора 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
```

Конфигурация для 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
```

При проверке этого примера, тестовый запрос от адреса 10.1.1.1 маршрутизатора Cisco-1, формируемый с помощью команды extended ping, был послан на узел Интернета. В этом примере в качестве адреса места назначения использовался адрес 192.1.1.1. **Чтобы увидеть, что происходит в Интернет-маршрутизаторе, во время использования команды debug ip packet 101 detail была отключена быстрая коммутация.**

% Warning: Использование **команды debug ip packet detail** на производственном маршрутизаторе может вызвать высокую загрузку ЦП, которая может привести к значительному снижению производительности или выходу сети из строя. Перед использованием команд отладки рекомендуется внимательно прочитать раздел Использование команд отладки документа Общие сведения о командах ping и traceroute.

Примечание: Icmp разрешения access-list 101 любой любой оператор используется для фильтрации **выходных данных debug ip packet**. **Без списка контроля доступа команда debug ip packet может генерировать большое количество выходных данных, что блокирует работу маршрутизатора.** Используйте расширенные списки ACL при настройке PBR. Если никакой ACL не настроен для установления условий соответствия, это приводит ко всему маршрутизировавшему политикой трафику.

```
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)
```

Как можно видеть, пакеты никогда не приводят к этому в Интернет-маршрутизаторе. Нижеприведенные команды отладки, взятые для маршрутизатора Cisco WAN, показывают почему это происходит.

```
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.
```

Как и ожидалось, пакет согласовал запись политики 10 в схеме политик net-10 . Почему

пакет не сделал это в Интернет-маршрутизаторе?

```
"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
```

Это понятно из выходных данных команды debug arp. Маршрутизатор Cisco для WAN пытается сделать то, что ему предписано, и переслать пакеты напрямую интерфейсу Ethernet 0/1. **Это требует, чтобы маршрутизатор отправил ARP-запрос на адрес назначения 192.1.1.1, который маршрутизатор распознает как не соответствующий этому интерфейсу, и, следовательно, ARP-запись для этого адреса является неполной ("Incomplete"), как это показано с помощью команды show arp.** Затем происходит неудачная инкапсуляция, так как маршрутизатор не может поместить пакет в канал без ARP-записи.

Задавая брандмауэр в качестве следующего узла, можно не допустить возникновения этой проблемы и сделать так, чтобы схема маршрутизации работала надлежащим образом:

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

Используя ту же самую команду debug ip packet 101 detail для Интернет-маршрутизатора, теперь можно увидеть, что пакет пересылается по верному пути. Можно также видеть, что этот пакет отправлен брандмауэром на адрес 172.16.255.1, а машина с адресом 192.1.1.1 при проверке формирует следующий отклик:

```
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:
```

Команда debug ip policy на маршрутизаторе Cisco WAN показывает, что пакет был перенаправлен на межсетевой экран, 172.16.39.2:

Команды Debug, запускаемые с 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
```

Маршрутизация на основе политик для зашифрованного потока данных

Передайте дешифрованный трафик к интерфейсу обратной связи, чтобы направить зашифрованный поток данных на основе маршрутизации в соответствии с политикой и затем сделать PBR на том интерфейсе. Если enrypted трафик передан по VPN-туннелю тогда `disable ip cef` на интерфейсе, и завершите туннель vpn.

Дополнительные сведения

- Страница поддержки IP-маршрутизации
- Страница поддержки NAT
- Технический Suppport Tools и Resouces
- Маршрутизация на основе политик
- Технологии Cisco IOS
- Cisco Systems – техническая поддержка и документация