# Сведения о маршрутизации на основе политик

## Содержание



## Общие сведения

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 данного документа нет особых требований.

### Используемые компоненты

Сведения, содержащиеся в данном документе, не ограничены определенными версиями программного или аппаратного обеспечения.

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

- Операционная система Cisco IOS® Release 12.3(3);
- Маршрутизаторы серии Cisco 2500.

Сведения, представленные в данном документе, были получены на тестовом оборудовании в специально созданных лабораторных условиях. При написании данного документа использовались только данные, полученные от устройств с конфигурацией по

умолчанию. При работе с реально функционирующей сетью необходимо полностью осознавать возможные результаты использования всех команд.

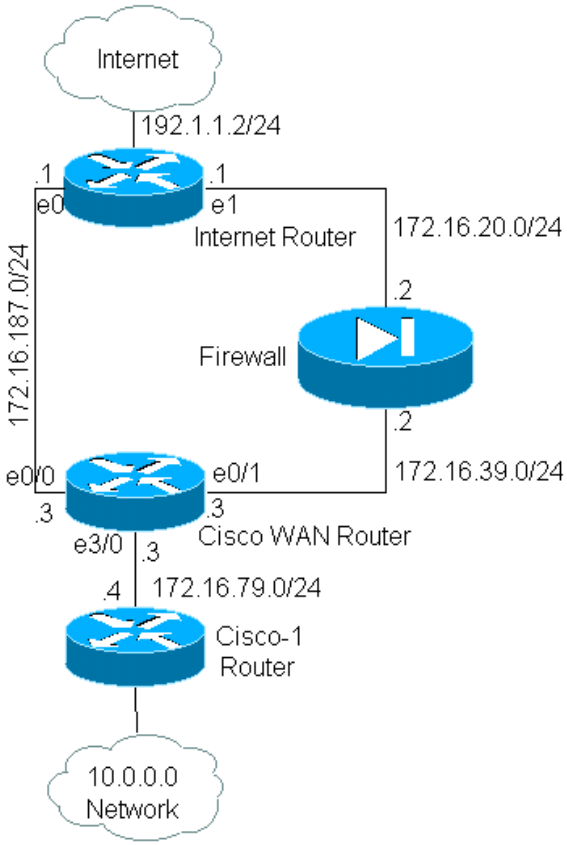
### Условные обозначения

Дополнительные сведения об условных обозначениях см. в разделе "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 брандмауэра

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
```

Сведения о командах, родственных **ip nat**, см. в документе IP-адресация и служебные команды.

В данном примере маршрутизаторы Cisco для WAN используют маршрутизацию на основе политик для обеспечения гарантии того, что IP-пакеты, исходящие из сети 10.0.0.0/8, будут проходить через брандмауэр. 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 команде **route-map**.

**Конфигурация маршрутизатора Cisco-1**

```
!
version 12.3

!

interface Ethernet0

!-- Интерфейс подключается к сети 10.0.0.0


ip address 10.1.1.1 255.0.0.0


!
interface Ethernet1

!-- Интерфейс подключается к 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
!

!--- Выходные данные отключены
```

**Конфигурация для Internet_Router**

```
!
version 12.3

!
interface Ethernet1

!-- Интерфейс подключается к брандмауэру

ip address 172.16.20.1 255.255.255.0

interface Serial0

!--- Интерфейс подключается к Интернету

ip address 192.1.1.2 255.255.255.0
clockrate 64000
no fair-queue
!
interface Ethernet0

!--- Интерфейс подключается к Cisco_Wan_Router

ip address 172.16.187.1 255.255.255.0
!

!
router eigrp 1
redistribute static

!--- Перераспределение статического маршрута по умолчанию на другие
!--- маршрутизаторы для выхода в Интернет

network 172.16.0.0
no auto-summary
!
ip classless
ip route 0.0.0.0 0.0.0.0 192.1.1.1

!-- Статический маршрут по умолчанию, ведущий к
!-- маршрутизатору, подключенному к Интернету

!--- Выходные данные отключены
```

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.


**Внимание.** Использование команды **debug ip packet detail** на производственном маршрутизаторе может привести к высокой загрузке центрального процессора и, как следствие, к серьезному снижению производительности или к выходу сети из строя. Перед использованием команд отладки рекомендуется внимательно прочитать раздел Использование команд отладки документа Общие сведения о командах ping и traceroute.

**Примечание:** Выражение **access-list 101 permit icmp any any** используется для фильтрации результатов выполнения команды **debug ip packet**. Без списка контроля доступа команда **debug ip packet** может генерировать большое количество выходных данных, что блокирует работу маршрутизатора.

```
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

!--- Пакет с исходным адресом в сети 10.0.0.0/8 передается
!--- по инструкции 10 карты маршрутов "net-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

!--- Ранее соответствующие пакеты переадресовывались из
!--- интерфейса Ethernet 0/1 с помощью команды set.
```

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

!--- Пакеты с исходным адресом 10.1.1.1 с помощью брандмауэра переводятся в
!--- адрес 172.16.255.1 перед достижением 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

!--- Пакеты, возвращающиеся из Интернета, приходят на
!--- конечный адрес 172.16.255.1 перед достижением брандмауэра.

*Mar  1 00:06:11.619:
```

Команда **debug ip policy** на маршрутизаторе Cisco WAN показывает, что пакет был перенаправлен на брандмауэр по адресу 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
```

# Дополнительные сведения

- **Страница поддержки IP-маршрутизации**
- **Страница поддержки NAT**
- **Инструменты и ресурсы технической поддержки**
- **Маршрутизация на основе политик**
- **Технологии операционной системы Cisco IOS**
- **Техническая поддержка — Cisco Systems**

---



---

Дата генерации PDF файла: Jan 05, 2010

---

http://www.cisco.com/support/RU/customer/content/9/92073/36.shtml

---