Ограничение трафика

Использование IP Source Guard

Для портов OpenStack можно указать список IP-адресов, которые будут использоваться IP Source Guard. Через порт будет отправлен только тот трафик, IP-адрес источника которого содержится в этом списке. Это помогает защититься от атак с подменой IP-адреса.

Например, можно разрешить:

- Только трафик с виртуальной машины, которая использует порт OpenStack.
- Весь трафик, который проходит через виртуальную машину (0.0.0.0\0). Это может быть полезно, когда виртуальная машина участвует в обработке трафика и является промежуточным узлом сети (например, маршрутизатором, файерволом или VPN-шлюзом).

Использование файервола и групп безопасности

С помощью файервола можно ограничивать трафик в виртуальных сетях.

Файервол обрабатывает трафик в соответствии с заданными группами безопасности. Эти группы содержат правила обработки входящего и исходящего трафика и работают по принципу «все, что не разрешено, запрещено». Одну или несколько групп безопасности можно назначить:

- в личном кабинете VK Cloud (только на порты OpenStack, с которыми связаны виртуальные машины);
- с помощью OpenStack CLI (на любые порты OpenStack).

Можно как создавать свои группы безопасности, так и использовать преднастроенные группы, которые нельзя изменить.

Для корректной работы групп безопасности:

- Либо настройте для них не только входящие, но и исходящие правила.
- Либо используйте их в комбинации с группой безопасности по умолчанию, разрешающей любой исходящий трафик. Это касается как преднастроенных, так и пользовательских групп безопасности.

Группы безопасности по умолчанию:

- default — для сетей SDN Neutron;
- default-sprut — для сетей SDN Sprut.

Преднастроенные группы безопасности

В проекте по умолчанию доступна только группа default. Остальные группы будут доступны после создания ВМ с такими группами.

default

Группа безопасности по умолчанию. Эта группа назначается на все создаваемые в рамках сети порты OpenStack, в том числе:

- порты, к которым подключаются виртуальные машины и другие сервисы платформы;
- служебные порты, которые создаются, например, для маршрутизатора или балансировщика нагрузки.

> При использовании OpenStack CLI возможно создать порт OpenStack:
> - либо с группами безопасности, которые отличаются от группы по умолчанию;
> - либо вообще без группы безопасности.

Разрешены:

- любой исходящий трафик;
- любой входящий трафик в пределах группы безопасности.

ssh

Группа безопасности, разрешающая SSH-трафик.

Разрешен входящий трафик с любых IP-адресов на TCP-порт 22.

ssh+www

Группа безопасности, разрешающая SSH- и HTTP(S)-трафик.

Разрешен входящий трафик с любых IP-адресов на TCP-порты:

- 22
- 80
- 443

rdp

Группа безопасности, разрешающая RDP-трафик.

Разрешен входящий трафик с любых IP-адресов на TCP-порт 3389.

rdp+www

Группа безопасности, разрешающая RDP- и HTTP(S)-трафик.

Разрешен входящий трафик с любых IP-адресов на TCP-порты:

- 3389
- 80
- 443

all

Разрешен любой входящий трафик с любых IP-адресов.