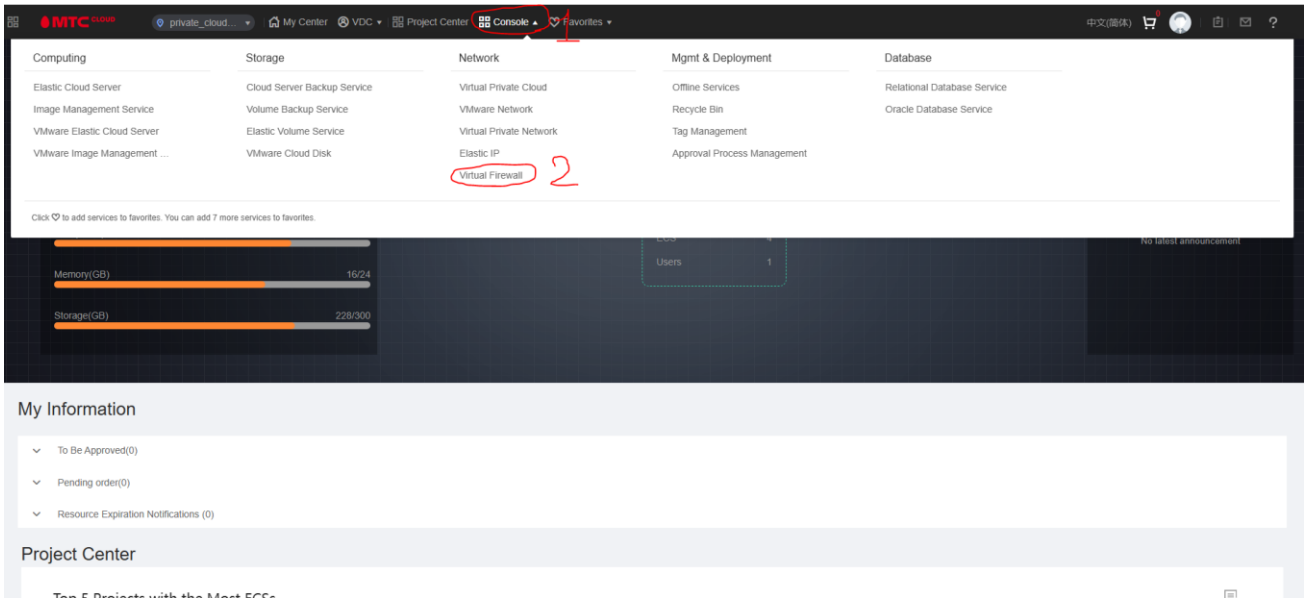
Инструкция по настройке правил Firewall для платформы Huawei

Правильная настройка Firewall необходима для защиты локальной сети от несанкционированного доступа и внешних угроз. Она позволяет чётко определить, какие устройства и пользователи могут выходить в интернет или получать доступ к внутренним ресурсам, а какие — нет.

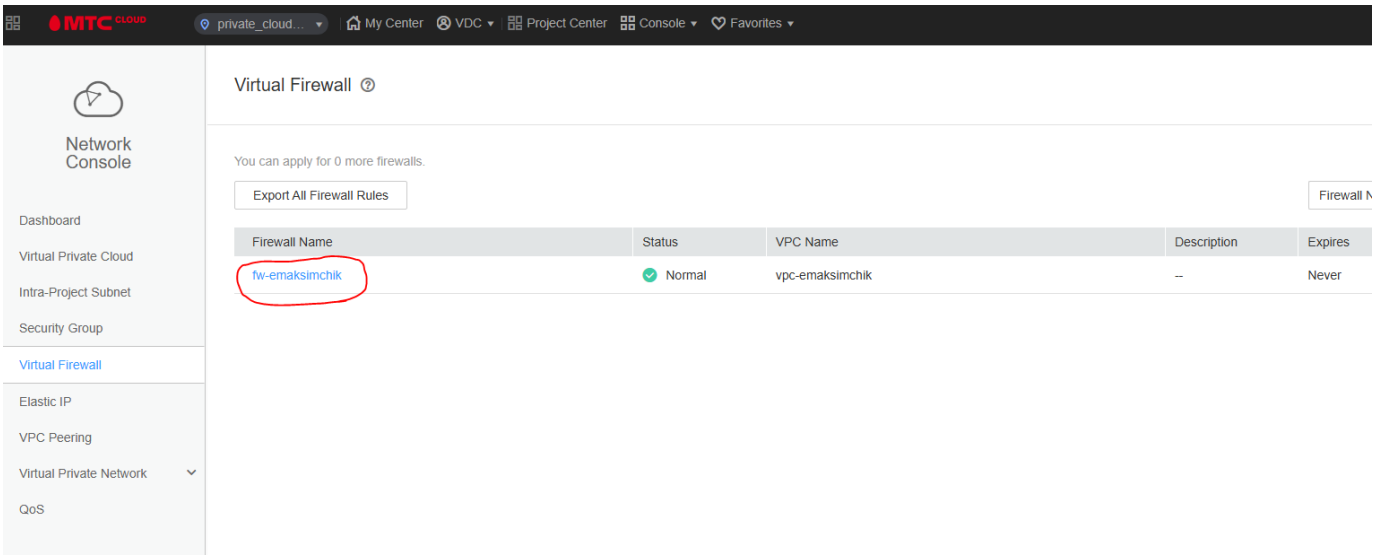
Firewall служит важным инструментом для контроля сетевого трафика, повышения безопасности, соблюдения политики доступа и предотвращения потенциальных атак. Без корректно настроенных правил даже надёжная сеть может оказаться уязвимой.

Добавление правил Firewall

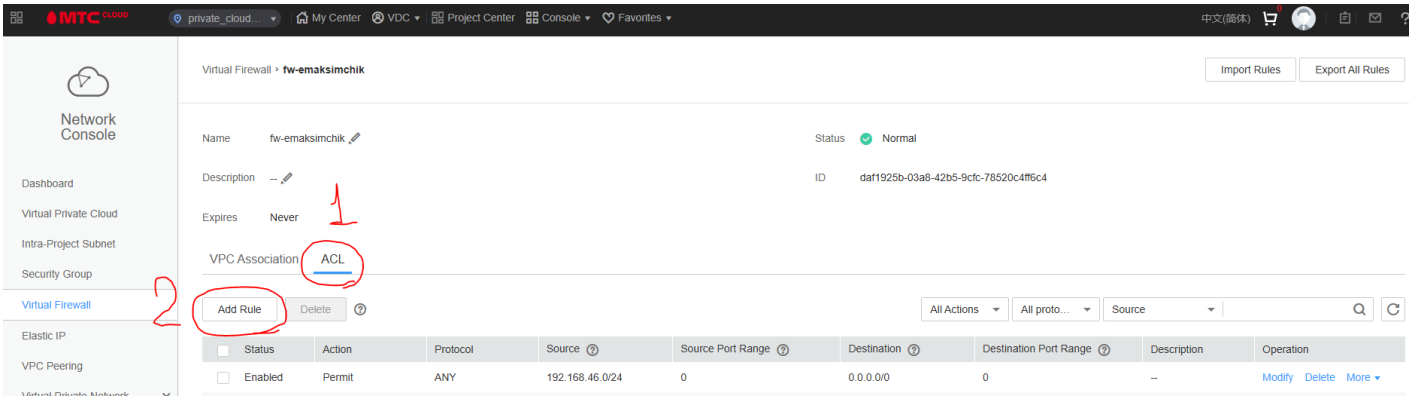
1. Необходимо перейти во вкладку Console (1), после этого перейти в пункт меню Virtual Firewall (2).



2. Выбрать Firewall из списка, название Firewall будет аналогично названию организации



3. Перейти во вкладку ACL (1), где можно просмотреть существующие правила, отредактировать/удалить правила, а также создать новые правила (2)

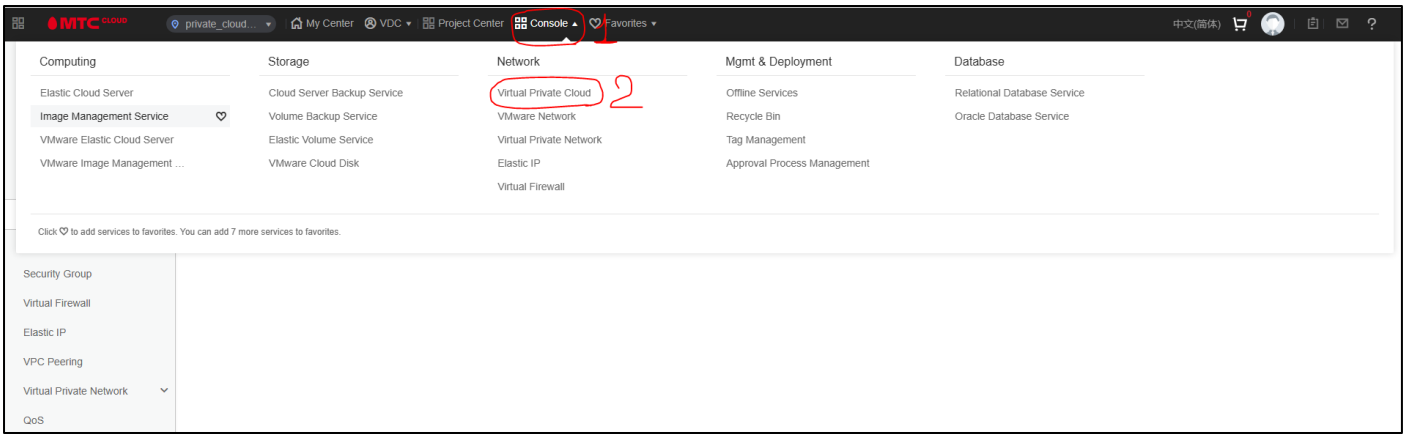


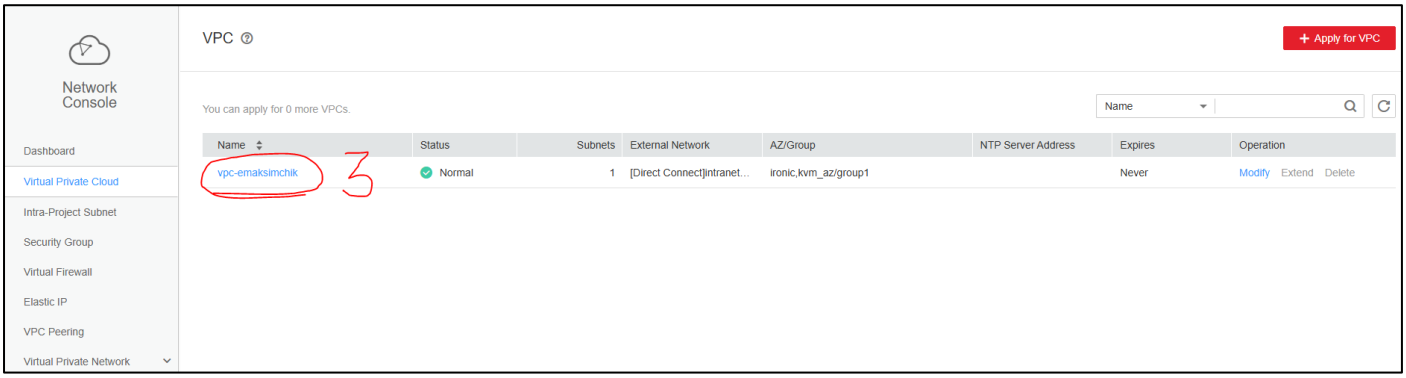
Пример формирования правил Firewall

1. Разрешение доступа в интернет из локальной сети

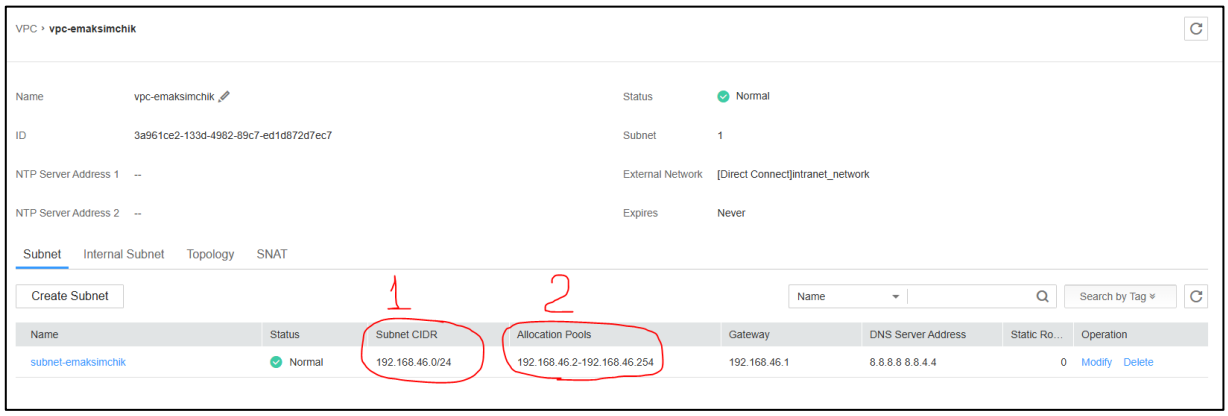
Данное правило разрешает виртуальным машинам из внутренней *локальной* сети `192.168.46.0/24` (адрес выданный для тенанта) выходить в интернет. Оно разрешает весь исходящий трафик по любому протоколу и порту.

Для просмотра адреса локальной сети необходимо перейти во вкладку Console (1), после этого перейти в пункт Virtual Private Cloud (2) и выбрать существующий VPC (3).

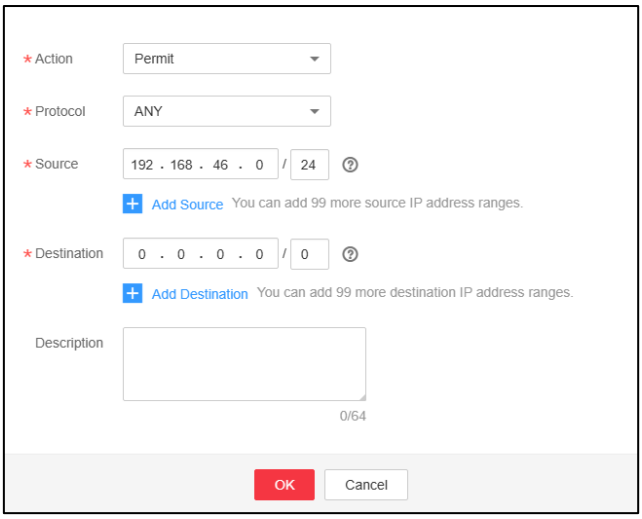




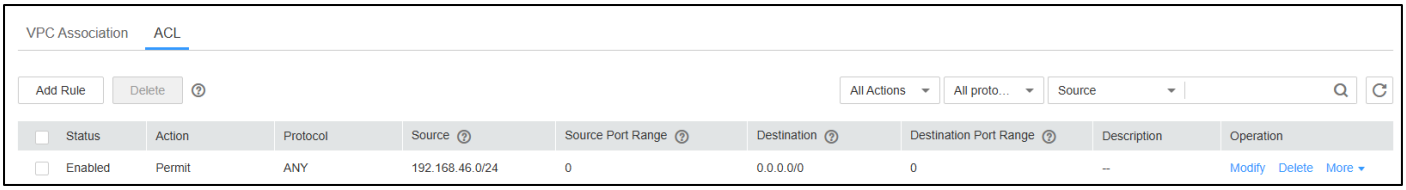
После перехода в VPC можно посмотреть адрес внутренней *локальной* сети в формате CIDR (1), диапазон адресов доступных к использованию для виртуальных машин (2).



Пример создания правила:



Добавленное правило отобразиться в списке всех правил:



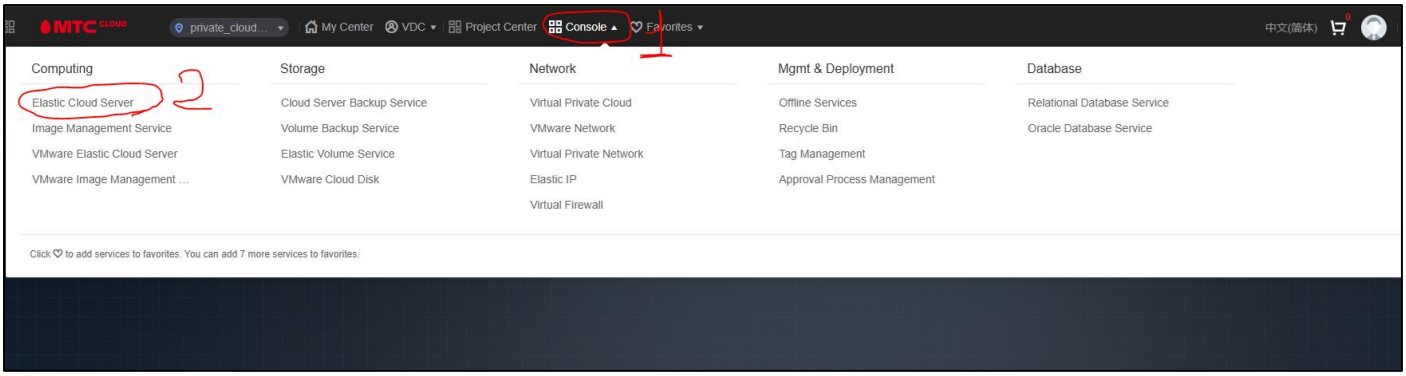
Описание использованных полей:

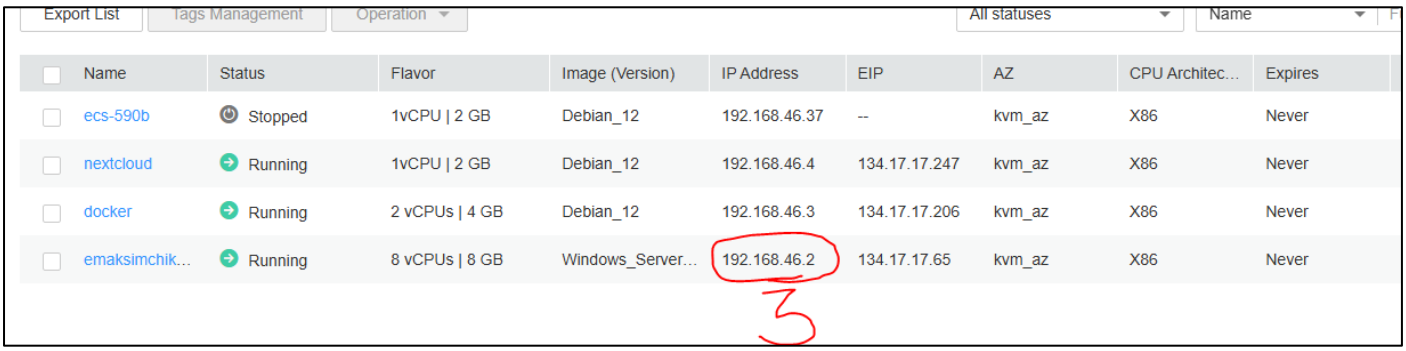
Поле	Значение	Описание
Action	Permit	Разрешает прохождение трафика, попадающего под условие правила
Protocol	ANY	Разрешены все протоколы (TCP, UDP, ICMP и т.д.).
Source	192.168.46.0/24	Указывает исходную подсеть, с которой разрешён доступ. В данном случае — вся внутренняя сеть.
Destination	0.0.0.0/0	Любой внешний адрес (весь интернет). Это универсальная запись для всех адресов

2. Разрешение доступа к виртуальной машине из глобальной сети

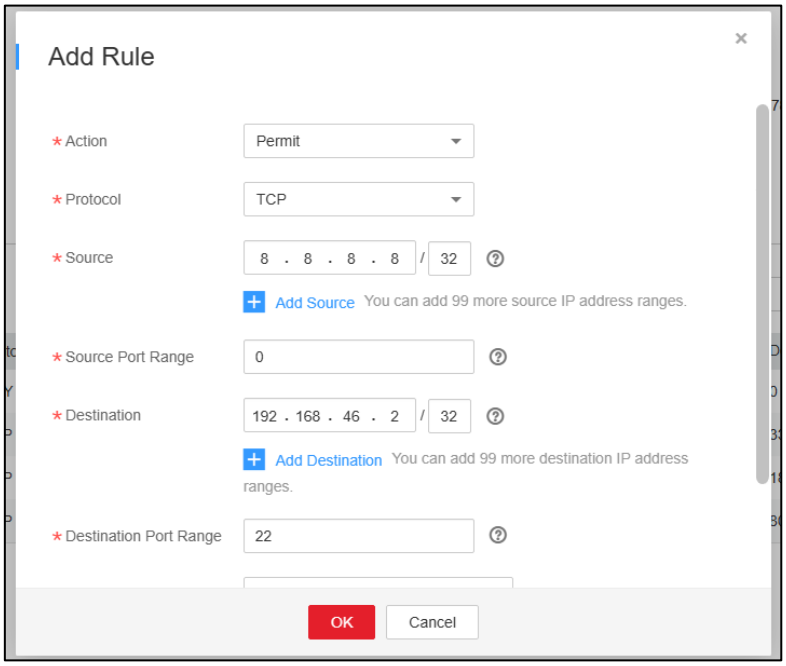
Данное правило позволяет устройству из глобальной сети (Internet), в данном случае `8.8.8.8`, получать доступ по 22 порту (SSH) к виртуальной машине с адресом `192.168.46.2` (задаётся при создании виртуальной машины). Оно разрешает подключение по SSH к виртуальной машине с локальным адресом `192.168.46.2`.

Для просмотра локального адреса виртуальной машины необходимо перейти во вкладку Console (1), после этого перейти в пункт Elastic Cloud Server (2). В данной вкладке отображаются все созданные виртуальные машины. Локальной адрес ВМ располагается в колонке **IP Address** напротив названия ВМ (3)

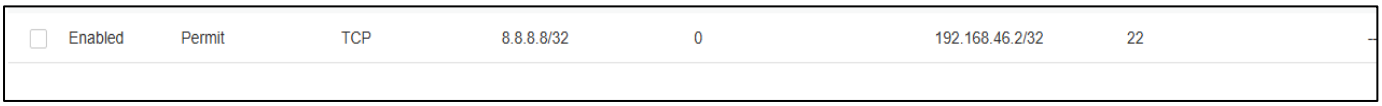




Пример создания правила:



Добавленное правило отобразиться в списке всех правил:



Описание использованных полей:

Поле	Значение	Описание
Action	Permit	Разрешает прохождение трафика, попадающего под условие правила
Protocol	TCP	Разрешает подключения с использованием протокола TCP
Source	8.8.8.8/32	Указывается IP адрес или подсеть в формате CIDR из которой будет доступно подключение к виртуальной машине. (/32 – в случае конкретного статического IP адреса)
Source Port Range	0	Список портов с которых будет доступно подключение. **Указывать 0**
Destination	192.168.46.2/32	Конкретный IP адрес виртуальной машины. Необходимо указывать адрес с использованием /32 сетевой маски
Destination Port Range	22	Список портов доступных для подключения. 22 – стандартный порт для подключения по SSH.