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).

| BB INTC CLOUD @ private_c                                    | cloud 🔹   🛱 My Center 🛛 🕲 VDC 🕶   🔡 Pi | roject Center 🔡 Console 🔺 🏷 Favorites |                             |                             | 中文(简体) 🛱 🎧   🖻   🗹 ?   |
|--|--|---------------------------------------|-----------------------------|-----------------------------|------------------------|
| Computing  | Storage                                | Network                               | Mgmt & Deployment           | Database                    |                        |
| Elastic Cloud Server   | Cloud Server Backup Service            | Virtual Private Cloud                 | Offline Services            | Relational Database Service |                        |
| Image Management Service                                     | Volume Backup Service                  | VMware Network                        | Recycle Bin                 | Oracle Database Service     |                        |
| VMware Elastic Cloud Server                                  | Elastic Volume Service                 | Virtual Private Network               | Tag Management              |                             |                        |
| vinnere intege management                                    | Vinimare Cloud Disk                    | Virtual Firewall                      | Арргочат госсээ манадолгон. |                             |                        |
| Click $\heartsuit$ to add services to favorites. You can add | d 7 more services to favorites.        |                                       |                             |                             |                        |
|  |  |                                       |                             |                             | No latest announcement |
| Memory(GB)   | 16/24                                  |                                       |                             |                             |                        |
| Storane/CB)  |  |                                       |                             |                             |                        |
| Storage(SD)  | 2201000                                |                                       |                             |                             |                        |
|  |  |                                       |                             |                             |                        |
|  |  |                                       |                             |                             |                        |
| My Information   |  |                                       |                             |                             |                        |
| ✓ To Be Approved(0)  |  |                                       |                             |                             |                        |
| <ul> <li>Pending order(0)</li> </ul>                         |  |                                       |                             |                             |                        |
| <ul> <li>Resource Expiration Notifications (0)</li> </ul>    | 0)                                     |                                       |                             |                             |                        |
| Project Center   |  |                                       |                             |                             |                        |
| Ton E Drainste with the                                      | Mast ECCa                              |                                       |                             |                             |                        |

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

| брганизации             | •   |                                    |                 |             |            |
|-------------------------|---|------------------------------------|-----------------|-------------|------------|
|                         | ♥ private_cloud ▼       I 🖨 My Center       ⑧ VDC ▼       Ⅲ   | Project Center  🔡 Console 🔻 🛇 Favo | vrites 🔻        |             |            |
| $\bigcirc$              | Virtual Firewall ③  |                                    |                 |             |            |
| Network<br>Console      | You can apply for 0 more firewalls. Export All Firewall Rules |                                    |                 |             | Firewall N |
| Dashboard               | Firewall Name   | Status                             | VPC Name        | Description | Expires    |
| Virtual Private Cloud   | fw-emaksimchik  | Normal                             | vpc-emaksimchik | -           | Never      |
| Security Group          |   |                                    |                 |             |            |
| Virtual Firewall        |   |                                    |                 |             |            |
| Elastic IP              |   |                                    |                 |             |            |
| VPC Peering             |   |                                    |                 |             |            |
| Virtual Private Network | ~   |                                    |                 |             |            |
| QoS                     |   |                                    |                 |             |            |

#### организации

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

|                       | 🛛 private_cloud 🔹 🛛 🛱 My Center 🛛 🕲 VDC | 、 ▼   믬 Project Center   믬 Con | nsole 🔹 🛇 Favorites 🔹 |                       |                      |                            | 中文(简体)      | ı ( 💭 🛱       | 1 ⊠ ?       |
|-----------------------|---|--------------------------------|-----------------------|-----------------------|----------------------|----------------------------|-------------|---------------|-------------|
| Ó                     | Virtual Firewall > fw-emaksimchik       |                                |                       |                       |                      |                            | Import R    | ules Expor    | t All Rules |
| Network<br>Console    | Name fw-emaksimchik 🖋                   |                                |                       | Stati                 | us 🥑 Normal          |                            |             |               |             |
| Dashboard             | Description 🖋                           |                                |                       | ID                    | daf1925b-03a8-42b5-9 | cfc-78520c4ff6c4           |             |               |             |
| Virtual Private Cloud | Expires Never                           |                                |                       |                       |                      |                            |             |               |             |
| Intra-Project Subnet  | VPC Association ACL                     |                                |                       |                       |                      |                            |             |               |             |
| Security Group        |   |                                |                       |                       |                      |                            |             |               |             |
| Virtual Firewall      | Add Rule Delete (?)                     |                                |                       |                       | All Actic            | ns 👻 All proto 👻 Sour      | ce 👻        |               | QC          |
| Elastic IP            | Status Action                           | Protocol So                    | ource @               | Source Port Range (2) | Destination (?)      | Destination Port Range (2) | Description | Operation     |             |
| VPC Peering           | Enabled Permit                          | ANY 192                        |                       | 0                     | 0.0.0.0/0            | 0                          | -           | Modify Delete | More •      |

### 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).

| 88 | • MTC CLOUD • private_cloud                                   | . 🔹 🖌 My Center 🛛 VDC 🕶 🔡 Project C | center 🔡 Console 🔺 🛇 Favorites 🔹 |                             |                             | 中文(简体) 🕂 🎧   🖻   🗹 ? |
|----|---|-------------------------------------|----------------------------------|-----------------------------|-----------------------------|----------------------|
|    | Computing   | Storage                             | Network                          | Mgmt & Deployment           | Database                    |                      |
|    | Elastic Cloud Server  | Cloud Server Backup Service         | Virtual Private Cloud            | Offline Services            | Relational Database Service |                      |
|    | Image Management Service                                      | Volume Backup Service               | VMware Network                   | Recycle Bin                 | Oracle Database Service     |                      |
|    | VMware Elastic Cloud Server                                   | Elastic Volume Service              | Virtual Private Network          | Tag Management              |                             |                      |
|    | VMware Image Management                                       | VMware Cloud Disk                   | Elastic IP                       | Approval Process Management |                             |                      |
|    |   |                                     | Virtual Firewall                 |                             |                             |                      |
|    | Click ${f O}$ to add services to favorites. You can add 7 mor | re services to favorites.           |                                  |                             |                             |                      |
| s  | ecurity Group   |                                     |                                  |                             |                             |                      |
| V  | /irtual Firewall  |                                     |                                  |                             |                             |                      |
| E  | lastic IP   |                                     |                                  |                             |                             |                      |
| V  | /PC Peering   |                                     |                                  |                             |                             |                      |
| N  | rirtual Private Network                                       |                                     |                                  |                             |                             |                      |
| C  | loS   |                                     |                                  |                             |                             |                      |

| Ø                       | VPC @                         |            |         |                          |                      |                    |         |   | + Apply for          | VPC |
|-------------------------|-------------------------------|------------|---------|--------------------------|----------------------|--------------------|---------|---|----------------------|-----|
| Network<br>Console      | You can apply for 0 more VPCs | S.         |         |                          |                      |                    | Name    | Ŧ | Q                    | C   |
| Dashboard               | Name 🜲                        | Status     | Subnets | External Network         | AZ/Group             | NTP Server Address | Expires |   | Operation            |     |
| Virtual Private Cloud   | vpc-emaksimchik               | S Normal   | 1       | [Direct Connect]intranet | ironic,kvm_az/group1 |                    | Never   |   | Modify Extend Delete |     |
| Intra-Project Subnet    |                               | $\bigcirc$ |         |                          |                      |                    |         |   |                      |     |
| Security Group          |                               |            |         |                          |                      |                    |         |   |                      |     |
| Virtual Firewall        |                               |            |         |                          |                      |                    |         |   |                      |     |
| Elastic IP              |                               |            |         |                          |                      |                    |         |   |                      |     |
| VPC Peering             |                               |            |         |                          |                      |                    |         |   |                      |     |
| Virtual Private Network |                               |            |         |                          |                      |                    |         |   |                      |     |

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

| VPC > vpc-emaksime   | lik                                  |                 |                     |                  |                |                  |                    |           |                 | С |
|----------------------|--------------------------------------|-----------------|---------------------|------------------|----------------|------------------|--------------------|-----------|-----------------|---|
| Name                 | vpc-emaksimchik 🖋                    |                 |                     | Status           | Normal         |                  |                    |           |                 |   |
| ID                   | 3a961ce2-133d-4982-89c7-ed1d872d7ec7 | ,               |                     | Subnet           | 1              |                  |                    |           |                 |   |
| NTP Server Address 1 |                                      |                 |                     | External Network | [Direct Connec | t]intranet_netwo | ork                |           |                 |   |
| NTP Server Address 2 |                                      |                 |                     | Expires          | Never          |                  |                    |           |                 |   |
| Subnet Interna       | Subnet Topology SNAT                 |                 |                     |                  |                |                  |                    |           |                 |   |
| Create Subnet        |                                      | 1               | 2                   |                  |                | Name             | -                  | Q         | Search by Tag ¥ | С |
| Name                 | Status                               | Subnet CIDR     | Allocation Pools    |                  | Gateway        |                  | DNS Server Address | Static Ro | Operation       |   |
| subnet-emaksimchi    | Normal                               | 192.168.46.0/24 | 192.168.46.2-192.16 | 8.46.254         | 192.168.46.    | 1                | 8.8.8.8 8.8.4.4    | 0         | Modify Delete   |   |
|                      |                                      |                 |                     |                  |                |                  |                    |           |                 |   |

### Пример создания правила:

| * Action      | Permit 👻   |
|---------------|--|
| * Protocol    | ANY  |
| * Source      | 192 . 168 . 46 . 0 / 24 🕐  |
|               | + Add Source You can add 99 more source IP address ranges.           |
| * Destination | 0 . 0 . 0 . 0 / 0 @  |
|               | + Add Destination You can add 99 more destination IP address ranges. |
| Description   |  |
|               | 0/64   |
|               | OK Cancel  |

### Добавленное правило отобразиться в списке всех правил:

| VPC Association | ACL    |          |                 |                     |                 |             |                         |             |               |        |
|-----------------|--------|----------|-----------------|---------------------|-----------------|-------------|-------------------------|-------------|---------------|--------|
| Add Rule        | elete  |          |                 |                     |                 | All Actions | ✓ All proto ▼ Source    | e 👻         |               | QC     |
| Status          | Action | Protocol | Source 🕥        | Source Port Range 👩 | Destination (?) | De          | estination Port Range 👩 | Description | Operation     |        |
| Enabled         | Permit | ANY      | 192.168.46.0/24 | 0                   | 0.0.0/0         | 0           |                         |             | Modify Delete | More - |

### 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         | Любой внешний адрес (весь<br>интернет). Это универсальная запись<br>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 BM располагается в колонке **IP Address** напротив названия BM (3)

| oud 🔹 🛱 My Center 🔕 VDC 🕶 嘂 Pri | oject Center 🔡 Console 🔺 🌣 Favorites 🔻  |  |  | 中文(简体) 🛱 🂭  |
|---------------------------------|---|--|--|---|
| Storage                         | Network   | Mgmt & Deployment  | Database   |   |
| Cloud Server Backup Service     | Virtual Private Cloud   | Offline Services   | Relational Database Service  |   |
| Volume Backup Service           | VMware Network  | Recycle Bin  | Oracle Database Service  |   |
| Elastic Volume Service          | Virtual Private Network   | Tag Management   |  |   |
| VMware Cloud Disk               | Elastic IP  | Approval Process Management  |  |   |
|                                 | Virtual Firewall  |  |  |   |
| 7 more services to favorites.   |   |  |  |   |
|                                 |   |  |  |   |
|                                 |   |  |  |   |
|                                 |   |  |  |   |
|                                 | Nud ♥ I A My Center ♥ VDC ♥ I Pr<br>Storage<br>Cloud Server Backup Service<br>Volume Backup Service<br>Elastic Volume Service<br>VMware Cloud Disk<br>7 more services to favorites. | Storage       Network         Cloud Server Backup Service       Virtual Private Cloud         Volume Backup Service       Virtual Private Cloud         Volume Service       Virtual Private Network         Elastic Volume Service       Virtual Private Network         Virtual Private Network       Elastic IP         Virtual Firewall       Virtual Firewall | Storage       Network       Mgmt & Deployment         Cloud Server Backup Service       Virual Private Cloud       Offine Services         Volume Backup Service       Virual Private Cloud       Offine Services         Volume Service       Virual Private Network       Recycle Bin         Elastic Volume Service       Virual Private Network       Tag Management         Virual Private Network       Elastic IP       Approval Process Management         Virual Firewall       Virtual Firewall       Virtual Firewall | Storage       Network       Mgmt & Deployment       Database         Cloud Server Backup Service       Virual Private Cloud       Offline Services       Relational Database Service         Volume Backup Service       Virual Private Network       Recycle Bin       Oracle Database Service         Volume Service       Virual Private Network       Tag Management         Virual Firewalt       Elastic IP       Approval Process Management         Virual Firewalt       Virual Firewalt       Virual Firewalt |

| Exp | oort List Tags | Management Op | eration 🔻      |                 |               | ŀ             | All statuses | <ul> <li>Name</li> </ul> | ▼   F   |
|-----|----------------|---------------|----------------|-----------------|---------------|---------------|--------------|--------------------------|---------|
|     | Name           | Status        | Flavor         | Image (Version) | IP Address    | EIP           | AZ           | CPU Architec             | Expires |
|     | ecs-590b       | Stopped       | 1vCPU   2 GB   | Debian_12       | 192.168.46.37 |               | kvm_az       | X86                      | Never   |
|     | nextcloud      | Running       | 1vCPU   2 GB   | Debian_12       | 192.168.46.4  | 134.17.17.247 | kvm_az       | X86                      | Never   |
|     | docker         | Running       | 2 vCPUs   4 GB | Debian_12       | 192.168.46.3  | 134.17.17.206 | kvm_az       | X86                      | Never   |
|     | emaksimchik    | Running       | 8 vCPUs   8 GB | Windows_Server  | 192.168.46.2  | 134.17.17.65  | kvm_az       | X86                      | Never   |
|     |                |               |                |                 | 3             |               |              |                          |         |

#### Пример создания правила:

|    | Add Rule                 |  | × |
|----|--------------------------|--|---|
|    | * Action                 | Permit 💌   |   |
|    | * Protocol               | TCP  |   |
|    | * Source                 | 8 . 8 . 8 . 8 / 32 (2)   |   |
|    |                          | + Add Source You can add 99 more source IP address ranges.           |   |
| tc | * Source Port Range      | 0 ⑦  | D |
| Y  | * Destination            | 192 . 168 . 46 . 2   | 3 |
| Р  |                          | + Add Destination You can add 99 more destination IP address ranges. | 1 |
| P  | * Destination Port Range | 22 ②   | 3 |
|    |                          | OK Cancel  |   |

| Enabled | Permit | ТСР | 8.8.8.8/32 | 0 | 192.168.46.2/32 | 22 |
|---------|--------|-----|------------|---|-----------------|----|
|         |        |     |            |   |                 |    |

# Описание использованных полей:

| Поле                      | Значение        | Описание  |  |  |
|---------------------------|-----------------|---|--|--|
| Action                    | Permit          | Разрешает прохождение трафика, попадающего под условие правила  |  |  |
| Protocol                  | ТСР             | Разрешает подключения с<br>использованием протокола ТСР   |  |  |
| Source                    | 8.8.8/32        | Указывается IP адрес или подсеть в<br>формате CIDR из которой будет<br>доступно подключение к виртуальной<br>машине. (/32 – в случае конкретного<br>статического IP адреса) |  |  |
| Source Port<br>Range      | 0               | Список портов с которых будет<br>доступно подключение. Указывать 0  |  |  |
| Destination               | 192.168.46.2/32 | Конкретный IP адрес виртуальной<br>машины. Необходимо указывать<br>адрес с использованием /32 сетевой<br>маски  |  |  |
| Destination<br>Port Range | 22              | Список портов доступных для<br>подключения. 22 – стандартный порт<br>для подключения по SSH.  |  |  |