Настройка межсетевого экрана Netpolice NGFW в Yandex Cloud

Предварительные требования

Для начала работы с Yandex Cloud необходимо:

- Иметь подключенный аккаунт в статусе ACTIVE или TRIAL_ACTIVE
- Иметь на счету необходимые средства для функционирования ВМ и оплаты за использование NGFW

Примечание: Оплата взимается за:

- Время работы виртуальной машины
- Использование статического IP-адреса
- Лицензию Netpolice NGFW

1. Установка утилиты управления CLI

Для работы с Yandex Cloud через командную строку необходимо установить утилиту CLI.

Подробная инструкция доступна по ссылке: https://yandex.cloud/ru/docs/cli/quickstart#install

2. Создание облачной сети и подсети

Способ №1: через веб-консоль Yandex Cloud

1. На странице каталога в консоли управления нажмите кнопку "Создать ресурс" и выберите пункт "Сеть"
2. Задайте имя сети: nngfw-internal-subnet
3. Включите опцию "Создать подсети"
4. Выберите зону доступности ru-central1-a
5. Задайте имя сети, например, internal, external, management
6. Нажмите кнопку "Создать сеть"
7. Введите CIDR подсети: IP-адрес и маску подсети, например, 10.10.0.0/24.

Необходимо создать три сети:

- Вход для NGWFW
- Выход для NGFW

– Сеть для управления NGFW

Подробная информация о создании сети и подсети доступна по ссылке:
https://yandex.cloud/ru/docs/vpc/quickstart

Способ №2: через CLI

Создание сети:

```
yc vpc network create nngf-internal-subnet
```

Создание подсети:

```
yc vpc subnet create nngfw-internal-subnet \
--zone ru-central1-a \
--network-name usergate-network \
--range 192.168.1.0/24
```

3. Резервирование статического IP-адреса

Способ №1: через веб-консоль Yandex Cloud

1. Перейдите на страницу каталога, в котором нужно зарезервировать адрес
2. В списке сервисов выберите Virtual Private Cloud
3. На панели слева выберите "IP-адреса"
4. Нажмите кнопку "Зарезервировать адрес"
5. В открывшемся окне выберите зону доступности ru-central1-a
6. Нажмите кнопку "Зарезервировать"

Способ №2: через CLI

```
yc vpc address create --external-ipv4 zone=ru-central1-a
```

4. Создание виртуальной машины (ВМ) из образа

Способ №1: через веб-консоль Yandex Cloud

1. На странице каталога в консоли управления нажмите кнопку "Создать ресурс" и выберите "Виртуальная машина"
2. В блоке "Образ загрузочного диска" в поле "Поиск продукта" введите "Netpolice NGFW».

3. В блоке "Расположение" выберите зону доступности ru-central1-a
4. В блоке "Вычислительные ресурсы" перейдите на вкладку "Своя конфигурация" и укажите:
    - Платформа: Intel Ice Lake
    - vCPU: 2
    - Гарантированная доля vCPU: 100%
    - RAM: 8 ГБ

- Введите CIDR подсети: IP-адрес и маску подсети, например, 10.10.0.0/24. Подробнее про диапазоны IP-адресов в подсетях читайте в разделе Облачные сети и подсети.
- Введите CIDR подсети: IP-адрес и маску подсети, например, 10.10.0.0/24. Подробнее про диапазоны IP-адресов в подсетях читайте в разделе Облачные сети и подсети.

Способ №2: через CLI

Предварительно можно просмотреть все доступные образы:

```
yc compute image list --folder-id standard-images
```

5. Создание SSH-ключей для доступа к ВМ

Способ №1: через веб-консоль

Подробная инструкция по созданию SSH-ключей доступна по ссылке:

https://yandex.cloud/ru/docs/compute/operations/vm-connect/ssh#creating-ssh-keys

После создания ключей:

1. В блоке "Доступ" выберите вариант "SSH-ключ"
2. В поле "Логин" введите имя пользователя user (не используйте имя "root")
3. В поле "SSH-ключ" выберите SSH-ключ, сохраненный в вашем профиле

Если в профиле нет сохраненных SSH-ключей или вы хотите добавить новый ключ:

1. Нажмите кнопку "Добавить ключ"
2. Задайте имя SSH-ключа
3. Загрузите или вставьте содержимое открытого SSH-ключа
4. Нажмите кнопку "Добавить"

Способ №2: через CLI

```
yc compute instance create \
--name netpolice-ngfw \
--memory 8 \
--cores 2 \
--zone ru-central1-a \
--create-boot-disk image-folder-id=standard-images,image-family=usergate-ngfw \
--ssh-key <путь_к_открытой_части_SSH-ключа> \
--public-address=<зарезервированный_IP_адрес>
```

6. Подключение к ВМ и получение учетных данных

После создания и запуска ВМ подключитесь к ней по протоколу SSH:

```
ssh user@<публичный IP-адрес ВМ>
```

Для получения паролей доступа к веб-интерфейсу выполните команду:

```
grep -i api /etc/nngf/docker-compose.yml && grep -i admin /etc/nngf/docker-compose.yml
```

Вы получите два пароля:

- ADMIN_PASSWORD - для доступа к веб-интерфейсу
- API_KEY - для доступа к системе управления

7. Настройка Netpolice NGFW через веб-интерфейс

1. Откройте в браузере: https://<публичный IP-адрес ВМ>
2. Войдите, используя:

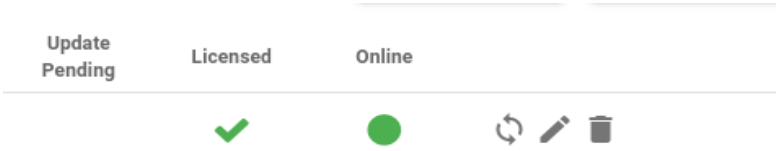
- Имя пользователя: admin@email.com
- Пароль: значение переменной ADMIN_PASSWORD

8. Детальная настройка NGFW через веб-интерфейс

Настройка устройства

1. Войдите в веб-интерфейс управления через HTTPS
2. Выберите меню **DEVICES**

3. Нажмите на иконку редактирования (в виде "ручки")



4. Заполните параметры устройства:
    - **Device name**: уникальное имя устройства NGFW
    - **Description**: описание (например, место установки)
    - **Password**: пароль для подключения к устройству NGFW (API_KEY)
    - **Address**: IP-адрес устройства
    - **Variable set**: параметры конфигурации устройства
    - **Assign policy**: название политики IPS/IDS
    - **Assign Firewall**: название политики IP-файрвола
5. В правом верхнем углу активируйте опцию **L3 mode**
6. После установки всех параметров нажмите **UPDATE**, затем **CLOSE**

Настройка параметров конфигурации

1. Выберите **PROFILES**

2. Нажмите на иконку редактирования
3. Установите следующие параметры:

- **NETFLOW_DST**: IP-адрес и порт NetFlow коллектора для сбора статистики по трафику
- **NETFLOW_PROTO**: протокол NetFlow (по умолчанию "10", IPFIX)
- **INTERNAL_IF**: имя внутреннего интерфейса NGFW (куда подключаются абоненты)
- **EXTERNAL_IF**: имя внешнего интерфейса NGFW
- **CONTROL_IF**: имя интерфейса управления (должен иметь доступный для системы управления IPv4-адрес)
- **INTERFACE**: параметр стыковки интерфейсов NGFW (обычно не требует редактирования)
- **BRIDGE_IF**: имя бриджа L2 интерфейса
- **HOME_NET**: IP-адресация внутренней сети (например, 192.168.0.0/16)
- **EXTERNAL_NET**: внешние сети (например, !192.168.0.0/16 - всё, что не входит в "домашнюю" сеть)
- **INLINE**: вид услуги (L3)

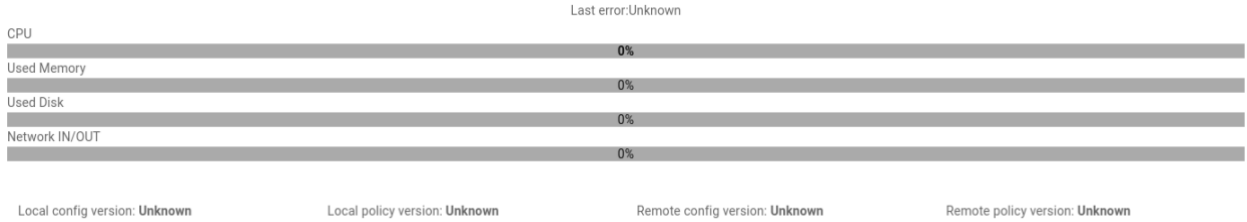
4. Сохраните параметры, нажав UPDATE, затем CLOSE

<u>Настройка политик IDS/IPS</u>

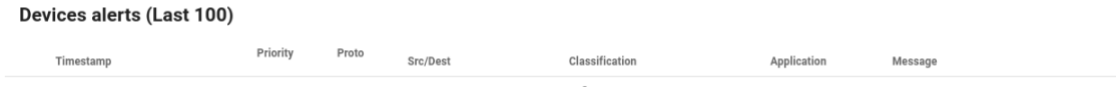
1. Выберите **POLICIES** в верхнем меню
2. В меню **Search Policy** выберите существующую политику или добавьте новую

3. В меню **Search Group** выберите необходимую группу или создайте новую через + и **Add Rule Group**
    - Здесь также можно загрузить собственные правила IDS/IPS
4. Выберите группу и через меню **CHANGE RULES** добавьте или удалите сигнатуры
5. Для настройки правил фильтрации используйте флажок **Restrict Access** вверху списка групп

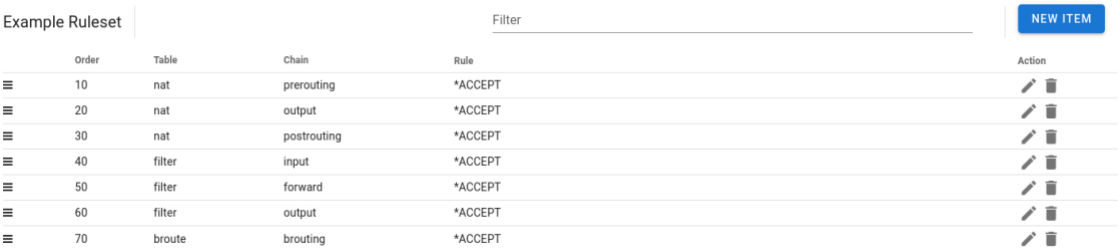
Мониторинг и уведомления



- Вкладка **MONITORING** позволяет наблюдать за состоянием CPU, RAM, диска, сетевых интерфейсов и сообщения из SysLog NGFW
- Вкладка **ALERTS** позволяет получать сообщения о срабатывании политик IPS/IDS



- Вкладка **FIREWALL** позволяет настроить политики IP-фильтрации в цепочках входящего и исходящего трафика, а также создавать собственные цепочки фильтрации



9. Настройка сетевого режима и маршрутизации

Для доступа в Интернет необходимо:

1. Перевести Netpolice NGFW в режим **L3 Mode** и **L3 NAT**

   На ВМ, подключенной к NGFW, необходимо установить статический маршрут в сторону IP-адреса NGFW:

2. На вкладке **ROUTES(L3 MODE)** проверить статическую маршрутизацию.
3. Настройка статистической маршрутизации через WEB интерфейс описана в документации Yandex Cloud https://yandex.cloud/ru/docs/vpc/operations/static-route-create#console_1

Через CLI интерфейс:

```
# Получите ID таблицы маршрутизации:
yc vpc route-table list
# Добавьте статический маршрут
yc vpc route-table update --id <ID_таблицы> --route destination=0.0.0.0/0,next-hop=192.168.1.5
# Для Linux-дистрибутивов можно использовать утилиту Network Manager (nmcli).
```