# Руководство по администрированию NetPolice NGFW ($N^2$GFW)

## Оглавление

## 1. Функционал $N^2$GFW

Межсетевой экран нового поколения фильтрует трафик, проходящий через определенные протоколы (например, TCP, UDP, IP), тем самым обеспечивая защиту сети от хакерских атак и разнообразных типов вторжений, основанных на использовании данных протоколов.

Система IDS/IPS позволяет распознавать вредоносную активность внутри сети. Основной задачей системы является обнаружение, протоколирование и предотвращение угроз в режиме реального времени, а также предоставление журналов активности. Администратор может создавать собственные сигнатуры для защиты определенных сервисов и включать их в профили Netpolice NGFW, наряду существующими.

## 2. Лицензирование $N^2$GFW

Для работы $N^2$GFW требуется лицензионный ключ.
Если лицензионный ключ не установлен, система $N^2$GFW работает 24 часа.
После этого, нормальное функционирование будет невозможно.

## 3. Требования к установке N²GFW

Установка N²GFW возможна на

- аппаратную
- или виртуальную платформу (например, Vmware Esxi).

Для установки N²GFW требуется серверная Linux система, с возможностью установки Docker контейнеров.

Существуют следующие варианты установки N²GFW:

- N²GFW с системой управления, WEB интерфейс + БД.
- N²GFW без системы управления
- Только система управления N²GFW, WEB интерфейс + БД.

К системе управления возможно подключение нескольких N²GFW.

## 4. Аппаратные требования к N²GFW

Для установки N²GFW без системы управления:

- CPU не менее 2,5 ГГц, не менее 4 -х ядер
- ОЗУ не менее 8 Гб
- жесткий диск, не менее 128 Гб
- сетевые интерфейсы Ethernet 100/1000 Мбит/с, не менее трех

Система управления N²GFW:

- CPU не менее 3 ГГц, не менее 4-х ядер, с поддержкой SSE 4.2
- ОЗУ не менее 16 Гб
- жесткий диск не менее 512 Гб
- сетевой интерфейс Ethernet 100/1000 Мбит/с

Требования к совмещенной установке такие же, как и к системе управления,
плюс два дополнительных Ethernet интерфейса.

## 5. Установка N²GFW

**Шаг № 1**
Для самостоятельной установки N²GFW необходимо воспользоваться скриптом ***install.sh***
URL для установки https://update.netpolice.ru/install.sh
Получить скрипт можно, например утилитой wget , wget https://update.netpolice.ru/install.sh
Дать скрипту права на исполнение chmod +x ./install.sh
Скрипт запускается из-под пользователя с правами администратора системы, **root**, либо от пользователя с правами sudo.

До запуска скрипта необходимо самостоятельно установить компоненты **Docker** и **docker-compose**.
Скрипт установки сделает это самостоятельно, но только для дистрибутивов на основе ОС Linux Ubuntu, Debian.

Для дистрибутивов на основе Centos Linux, необходима предварительная установка компонентов **docker.**

*Например, для RedOS 8, необходимо выполнить команды:*

***dnf install docker-ce docker-ce-cli***
***systemctl enable docker --now***

*Проверить, что служба docker запущена:*

***systemctl status docker***

Необходимо, так же, проверить, что установлены компоненты **openssl**.
Для дистрибутивов на основе Centos, например RedOS 8 необходимо отключить selinux, **sudo setenforce 0**
Так же, поправить конфигурацию nano /etc/selinux/config
**SELINUX=disabled**

Для дистрибутива Astra Linux 1.7-1.8, так же, желательно предварительно установить **docker**.
```
sudo apt install docker.io
```

После запуска скрипта **./install.sh** он предложит создать ключ:

Выберите тип ключа:

(1) RSA and RSA
(2) DSA and Elgamal
(3) DSA (sign only)
(4) RSA (sign only)
(9) ECC (sign and encrypt) *default*
(10) ECC (только для подписи)
(14) Existing key from card

Выберите необходимый вариант.

Далее, выберите длину ключа, идентификатор пользователя, адрес электронной почты.

Подтвердите выбор:

Сменить (N)Имя, (C)Примечание, (E)Адрес; (O)Принять/(Q)Выход? O

Введите **FQDN** доменное имя, необходимое для **SSL** сертификата сайта управления.

**Шаг № 2**
Далее, скрипт предложит выбрать вариант установки:
1. Install controller
2. Install service
3. Install controller+service

Вариант №1 - устанавливает только интерфейс управления
Вариант №2 - устанавливает только сам $N^2$GFW,
Вариант №3 совмещенный – устанавливает интерфейс управления и $N^2$GFW.

**Шаг № 3**
Далее, строка Enter **ADMIN password for UI п**редлагает ввести пароль администратора для интерфейса управления, либо воспользоваться автоматически созданным паролем.
Пароль необходимо сохранить в защищенном месте.

**Шаг № 4**
Затем, происходит автоматическая установка всех сервисов $N^2$GFW, в зависимости от заданной конфигурации.

При завершении установки, скрипт выдает учетные данные для входа в интерфейс управления.

**Authorization https://»доменное имя»**
**admin@email.com/пароль администратора**
**user@email.com/user**
**operator@email.com/operator"**

На этом, предварительная настройка сервисов $N^2$GFW закончена.
Необходимо переходить к настройке через WEB интерфейс управления.

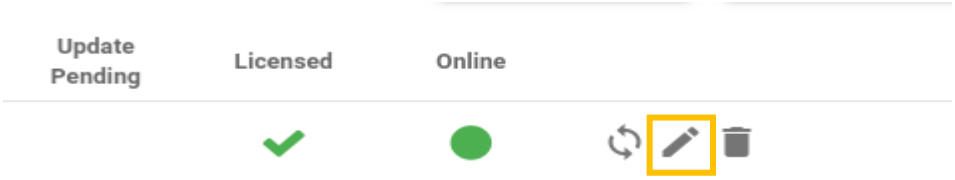
## 6. Настройка N²GFW через WEB интерфейс управления

Для входа в WEB интерфейс управления, вам необходимо зайти по ссылке https://доменное-имя. Доменное имя должно иметь DNS A запись, доступную для администратора.

Если нет возможность установить корректный FQDN домен, можно зайти по IP адресу Linux сервера. При этом, согласится со всеми исключениями безопасности, которые от вас потребует браузер.

**Шаг №1**
В интерфейсе управления выберете меню DEVICES.


**Шаг №2**
Необходимо выбрать редактирование устройства NGFW, меню в виде «ручки».
Здесь же отображается состояние лицензии. Нормальное состояние - зеленый цвет иконки.




Редактируем параметры устройства NGFW:

1. **Device name:** задаём уникальное имя устройства NGFW
2. **Description:** описание, например место установки
3. **Password:** пароль, необходимый для подключения к устройству NGFW.

   Пароль можно получить в командной строке сервера, командой

   *grep -i API_KEY /etc/nngf/docker-compose.yml | cut -d ":" -f2*
4. **Address:** IP адрес устройства, для локальной установки оставить по умолчанию.
5. **Variable set:** параметры конфигурации устройства
6. **Assign policy:** Название политики IPS/IDS
7. **Assign Firewall:** Название политики IP файрвола.

Возможно, так же выбрать режим работы NGFW L2 или L3.
В правом верхнем углу выбрать активным меню «L3 mode».

Появляется дополнительная вкладка «ROUTES (L3 MODE)», где можно настроить параметры статической маршрутизации.

После установки всех необходимых параметров, нажмите внизу «UPDATE», затем «CLOSE»

**Шаг №3**
После данной настройки, переходим в параметры конфигурации.

Выбираем «PROFILES», далее меню редактирования, или удаления конфигурации, если необходимо.


Устанавливаем параметры:

1. **NETFLOW_DST** — IP адрес и порт NetFlow коллектора для сбора статистики по трафику.
2. **NETFLOW_PROTO** - Протокол NetFlow, по умолчанию «10», IPFIX.
3. **INTERNAL_IF** - Имя внутреннего интерфейса NGFW в системе (куда подключаются абоненты).
4. **EXTERNAL_IF** -Имя внешнего интерфейса NGWF в системе
5. **CONTROL_IF -** Имя интерфейса управления в системе.
   Он должен иметь доступный для системы управления IPV4 адрес.
6. **INTERFACE** — параметр стыковки интерфейсов NGFW, в основном редактировать нет необходимости.
7. **BRIDGE_IF** - имя бриджа L2 интерфейса в системе.
8. **HOME_NET** — IP адресация «домашней», т.е. внутренней сети. Если указать неверно, фильтрация IPS/IDS работать не будет. Например, 192.168.0.0/16
9. **EXTERNAL_NET** — внешние сети. Например !192.168.0.0/16 Все, что не попадает в «домашнюю» сеть считается внешней.
10. **INLINE** — вид услуги, L2 или L3.

Далее, сохраняем параметры «UPDATE», «CLOSE».

**Шаг №4**
Настраиваем политики IDS/IPS, выбираем «POLICIES» в верхнем меню.

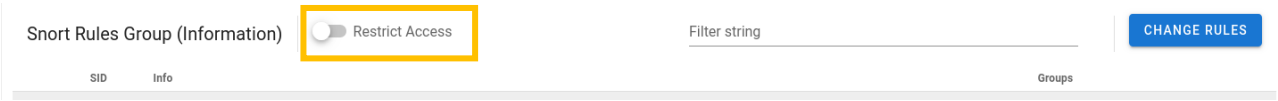
Слева «Search Policy», выбираем существующую политику или добавляем новую.

В меню «Search Group» выбираем необходимую группу, или создаем через меню «+» и «Add Rule Group».

Здесь же можно загрузить свою собственные правила IDS/IPS.

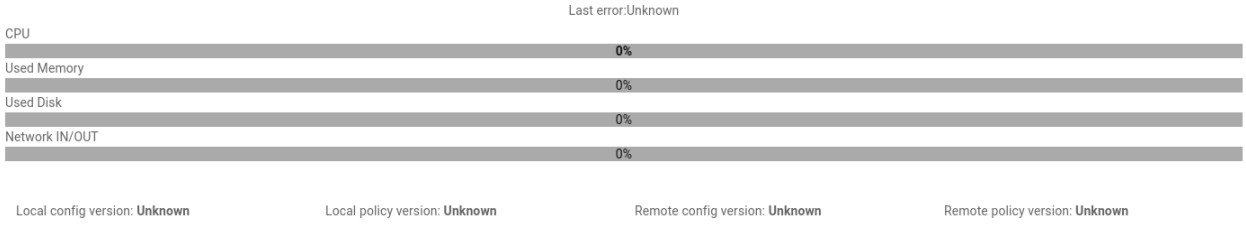
Указателем мыши можно выбрать группу, через меню «CHANGE RULES» добавить или удалить сигнатуры.

Так же, можно задать правила фильтрации, вверху списка групп флажок «Restrict Access».

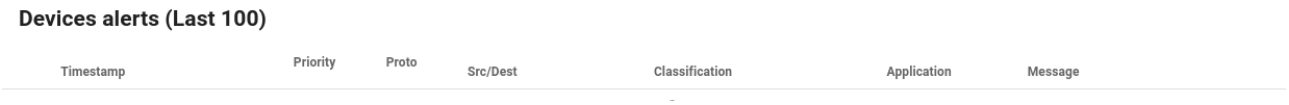



## Шаг №5

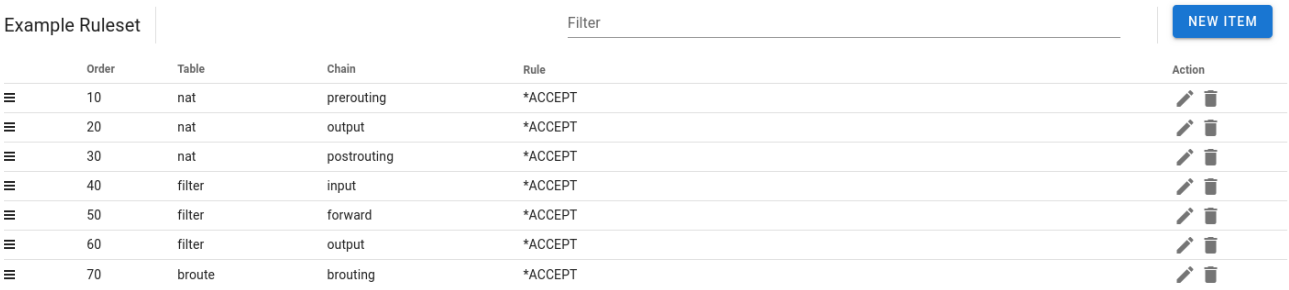
Вкладка «MONITORING» в верхнем меню позволяет наблюдать за состоянием процессора CPU, памяти RAM, диска, сетевых интерфейсов, сообщения из SysLog NGFW.




Вкладка «ALERTS» в верхнем меню позволяет получать сообщения NGFW о срабатывании политик IPS/IDS.




Вкладка в верхнем меню «FIREWALL» позволяет настроить политики IP фильтрации в цепочках входящего, исходящего трафика. Либо создать свои цепочки фильтрации.




## Дополнительные возможности N²GFW

N²GFW имеет гибкую структуру, и позволяет подключать дополнительные системы. Например, система контентной фильтрации с собственной базой сайтов и фильтрацией HTTP/HTTPS трафика.

Дополнительные расширение нагрузочной способности N²GFW возможно включением нескольких N²GFW с балансировкой трафика, по L2 или L3, используя протоколы динамической маршрутизации.