О Captive Portal

Captive Portal — это функциональность, используемая в PT NGFW для идентификации и контроля доступа пользователей.

Сценарии применения Captive Portal:

- **Организация гостевого доступа;**
- **Авторизация и применение политик безопасности для пользователей и устройств, находящихся вне домена;**
- **Авторизация и применение политик безопасности для пользователей и серверов на базе ОС Linux.**

Процесс авторизации через Captive Portal в PT NGFW

С точки зрения архитектуры Captive Portal является частью СУ и работает в связке с User-Control агентом, который используется для интеграции с Microsoft AD.

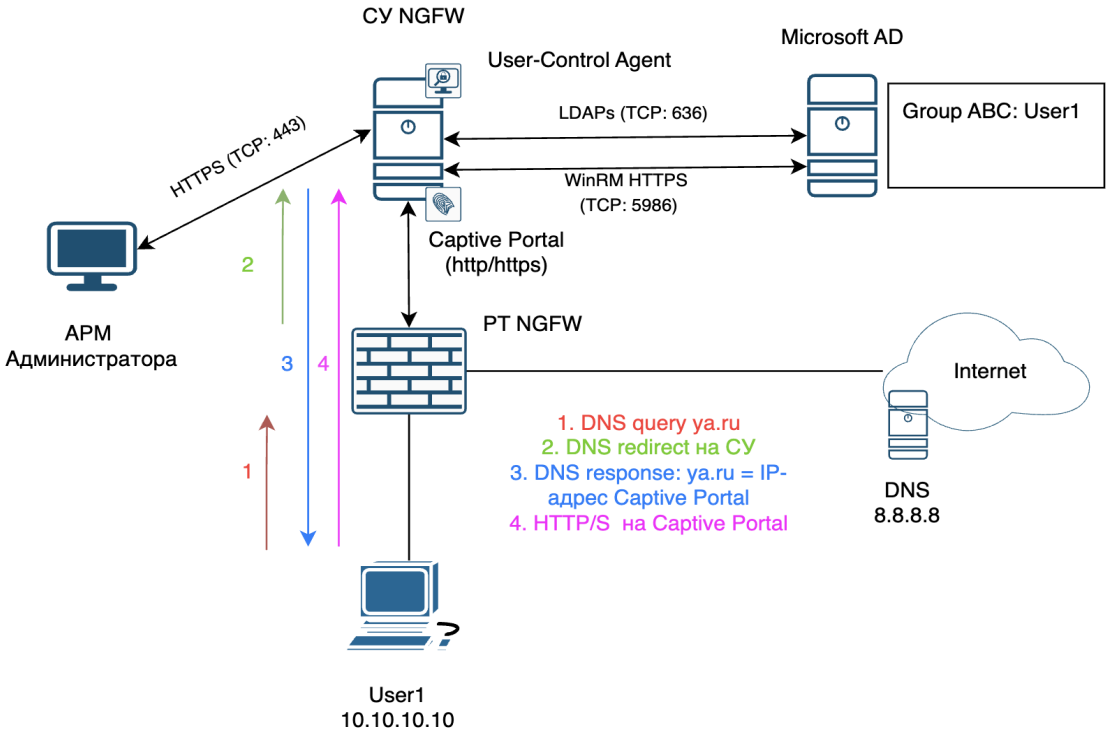

Рисунок 1. Сценарий авторизации пользователя через Captive Portal и User-Control Agent

- **Пользователь User1 инициирует HTTP-запрос к сайту ya.ru, в результате чего формируется DNS-запрос на разрешение доменного имени (ya.ru);**
- **PT NGFW перехватывает запрос от пользователя в сторону DNS-сервера и перенаправляет его в систему управления;**
- **СУ формирует DNS-ответ для пользователя, в котором вместо истинного значения IP-адреса для сайта ya.ru проставляется IP-адрес Captive Portal;**
- **Пользователь User 1 перенаправляется на Captive Portal, на котором он вводит свои учетные данные из Active Directory для прохождения аутентификации;**
- **После ввода пользователем учетных данных Captive Portal с помощью User-Control Agent выполняет авторизацию в AD по протоколу LDAPs. При этом в AD формируется запись авторизации, которая считывается User-Control Agent и передается в PT NGFW. Таким образом, PT NGFW получает информацию о пользователе и его IP-адресе (например, User1: 10.10.10.10).**

  ВАЖНО! Чтобы Captive Portal мог проводить авторизацию пользователей, DNS-запросы от них должны проходить через PT NGFW. Также необходимо обеспечить сетевую доступность до Captive Portal со стороны пользователей, для которых необходимо задействовать эту функциональность.

Настройка Captive Portal

Создание политики аутентификации на Captive Portal

1. **В СУ выделите второй IP-адрес и укажите его в параметрах. Например:**

```
# The primary network interface
auto ens192
allow-hotplug ens192
iface ens192 inet static
address 10.13.107.92/24
gateway 10.13.107.1
dns-domain ptsecurity.ru
dns-nameservers 10.0.52.101 10.10.52.101 10.20.52.101
post-up ip route add 10.13.108.0/24 via 10.13.107.254 dev ens192

auto ens192:0
allow-hotplug ens192:0
iface ens192:0 inet static
address 10.13.107.158/24
```

Рисунок 2. Выделение второго IP-адреса в СУ

2. **Настройте сервис traefik в СУ и укажите новый IP-адрес для сервиса Captive Portal. Например:**

```
sudo nano /opt/pt-ngfw/traefik/config/traefik.yml
.........
entrypoints:
  traefik:
    address: 127.0.0.1:81
    forwardedHeaders:
      trustedips:
        - 127.0.0.0/8
        - 10.0.0.0/8
        - 172.16.0.0/12
        - 192.168.0.0/16
  http:
    address: 10.13.107.92:80
    transport:
      respondingtimeouts:
        idletimeout: 5m
    forwardedHeaders:
      trustedips:
        - 127.0.0.0/8
        - 10.0.0.0/8
        - 172.16.0.0/12
        - 192.168.0.0/16
    http:
      redirections:
        entrypoint:
          to: https
```

```
        scheme: https
  https:
    address: 10.13.107.92:443
    forwardedHeaders:
      trustedips:
        - 127.0.0.0/8
        - 10.0.0.0/8
        - 172.16.0.0/12
        - 192.168.0.0/16
    http:
      tls: {}

  captive-http:
    address: 10.13.107.158:80
    transport:
      respondingtimeouts:
        idletimeout: 5m
    forwardedHeaders:
      trustedips:
        - 127.0.0.0/8
        - 10.0.0.0/8
        - 172.16.0.0/12
        - 192.168.0.0/16
    http:
      redirections:
        entrypoint:
          to: captive-https
          scheme: https

  captive-https:
    address: 10.13.107.158:443
    forwardedHeaders:
      trustedips:
        - 127.0.0.0/8
        - 10.0.0.0/8
        - 172.16.0.0/12
        - 192.168.0.0/16
    http:
      tls: {}
.......
```

В этом примере:

- 10.13.107.92 – IP-адрес, использующийся для интерфейса управления СУ (MGMT)
- 10.13.107.158 – IP-адрес для Captive Portal.

3. **Перезапустите сервис traefik:**

```
sudo systemctl restart pt-ngfw-traefik.service
```

4. **В СУ на странице Objects → Addresses добавьте адресный объект с типом IP-address для Captive Portal. Например:**

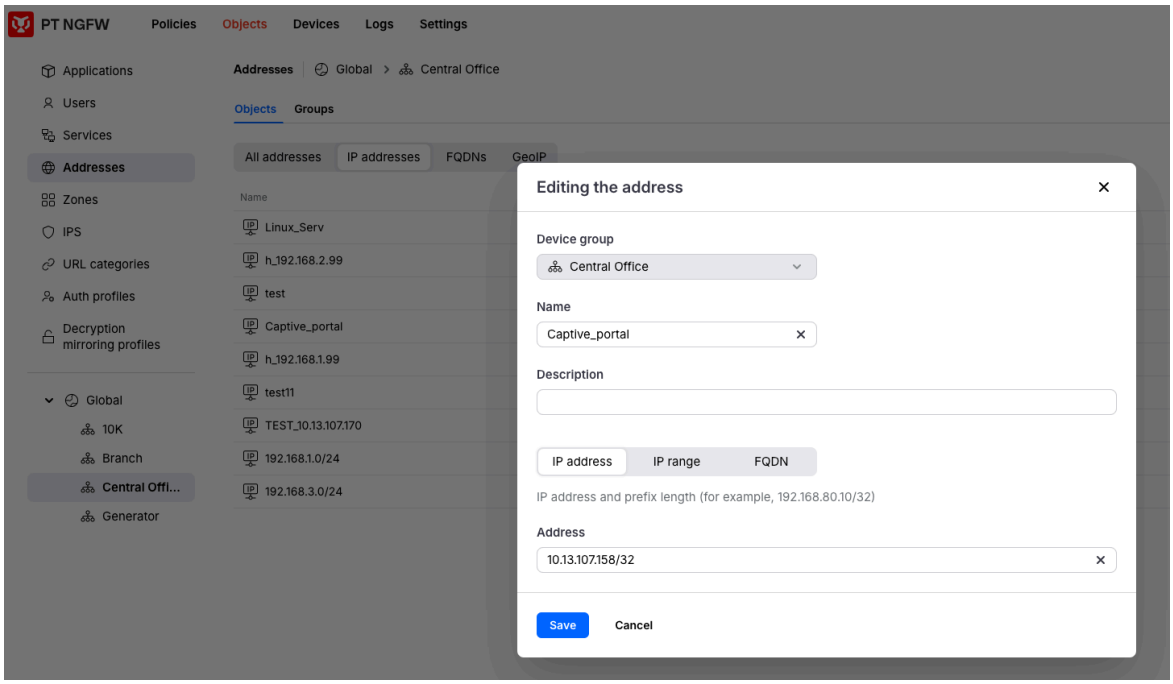

Рисунок 3. Добавление адресного объекта для Captive Portal

5. **На странице Objects → Auth Profiles добавьте Authentication profile и выберите в нем созданный ранее адрес для Captive Portal. Например:**

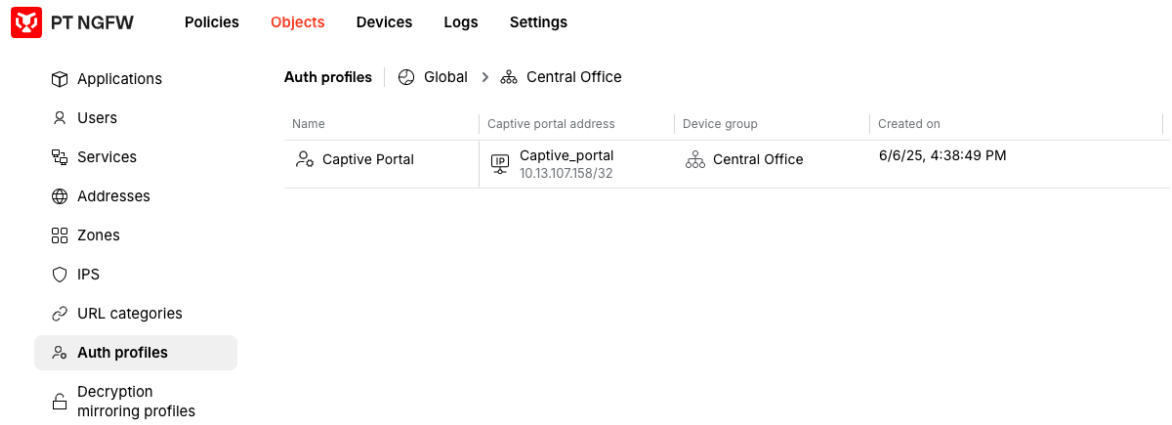

Рисунок 4. Добавление профиля аутентификации

6. **Обеспечьте сетевую доступность к Captive Portal для выбранных компьютеров и серверов.**

7. **Если требуется, на странице Policies → Security добавьте разрешающие политики безопасности.**

8. **Добавьте правило аутентификации для доступа к IP-адресу Captive Portal без аутентификации — Without authentication, чтобы перенаправленные от пользователей запросы могли доходить до Captive Portal.**

   Если требуется, выберите режим журналирования при срабатывании правила — Logging Mode At rule hit. Например:

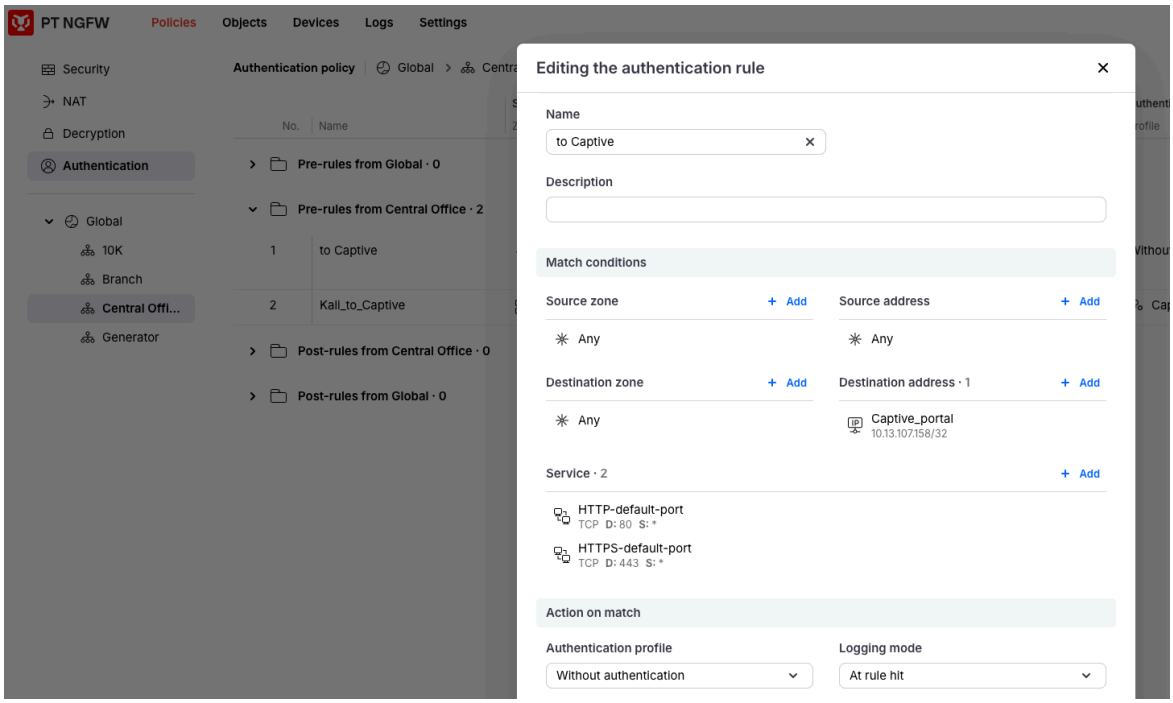

Рисунок 5. Добавление правила аутентификации (without authentication)

9. **Для выбранных компьютеров и серверов в соответствующих зонах безопасности выберите ранее созданный профиль аутентификации Authentication Profile.**

   Выберите необходимый режим журналирования при срабатывании правила, например Logging Mode At rule hit.

10. **Нажмите Сохранить.**

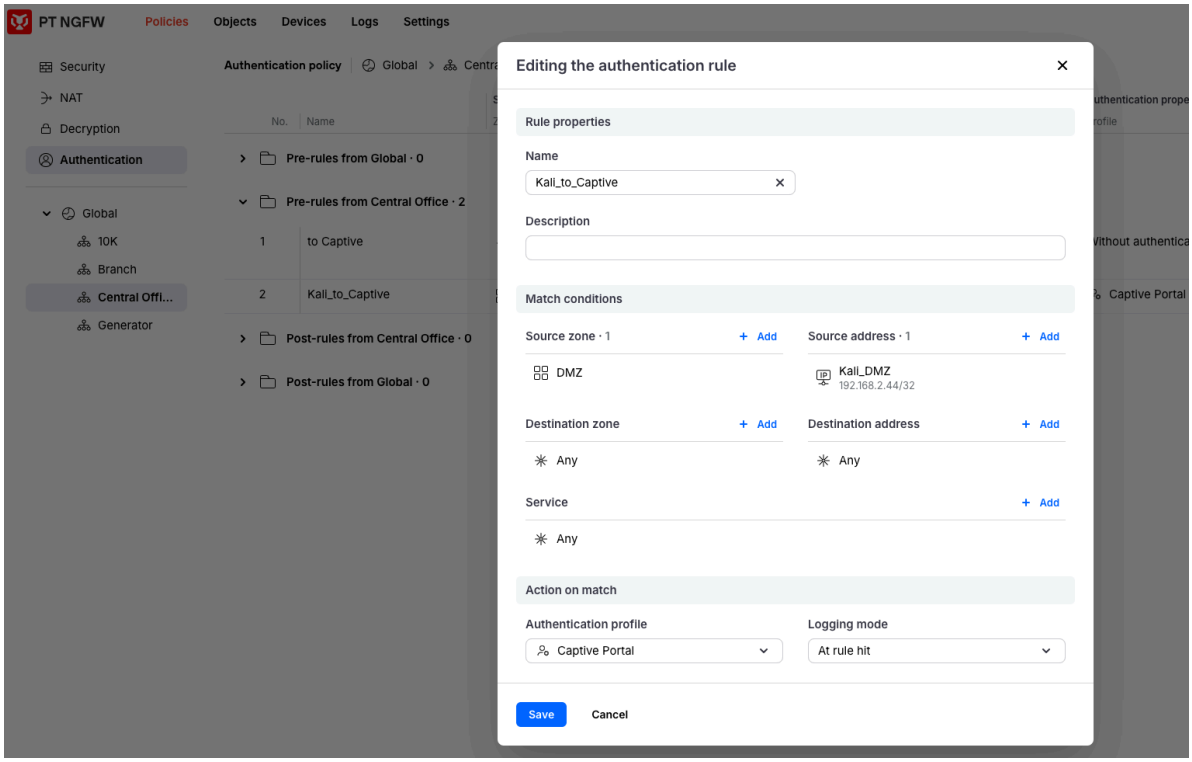

Рисунок 6. Выбор профиля аутентификации и сохранение правила

11. **Примените конфигурацию с СУ на PT NGFW, нажав Push to devices.**

12. **На тестовом ПК удостоверьтесь, что DNS-запросы перехватываются Captive Portal. Например:**

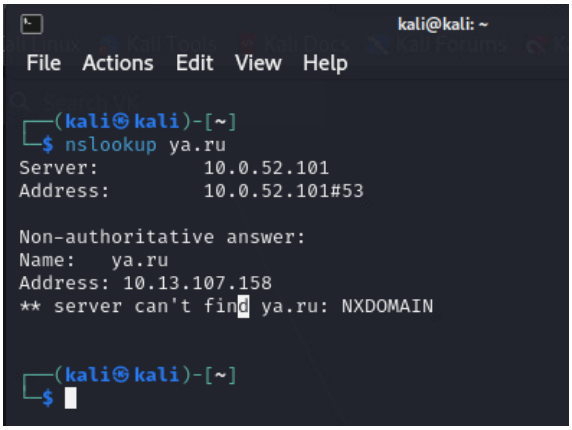

Рисунок 7. Проверка DNS-запросов

Если все настроено корректно, то в ответе на DNS-запрос должен отобразиться IP-адрес настроенного Captive Portal.

13. **В браузере перейдите на тестовый веб-сайт и убедитесь, что Captive Portal перехватил запрос пользователя и выдал страницу авторизации. Например:**

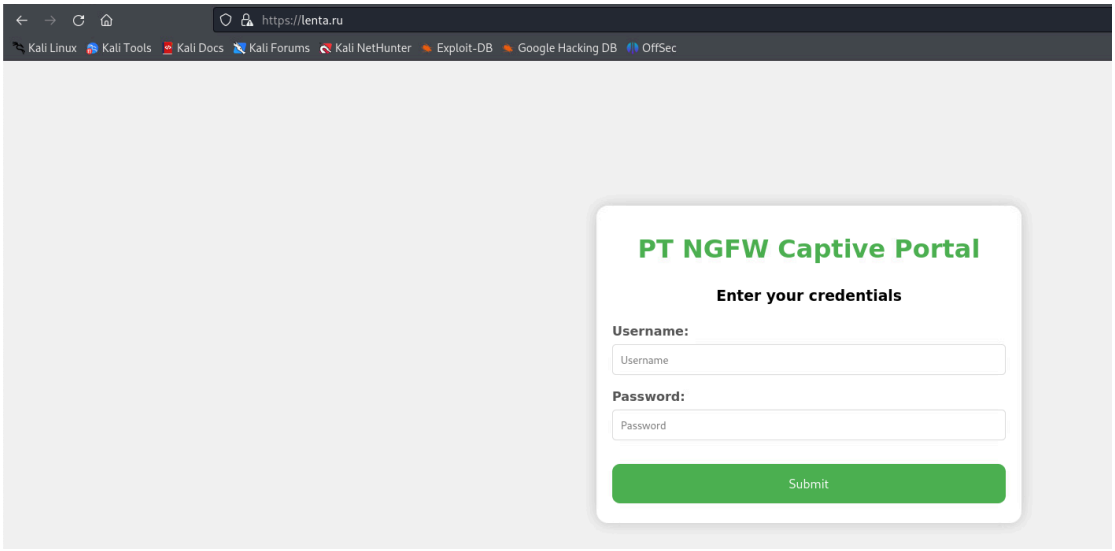

Рисунок 8. Страница авторизации

14. Введите доменные учетные данные из Microsoft AD, с которым предварительно настроена интеграция. Формат ввода в поле Username: user@domain.local

15. При успешной авторизации Captive Portal вернет сообщение Success с указанием IP-адреса, который был считан из записей AD для этой сессии аутентификации.

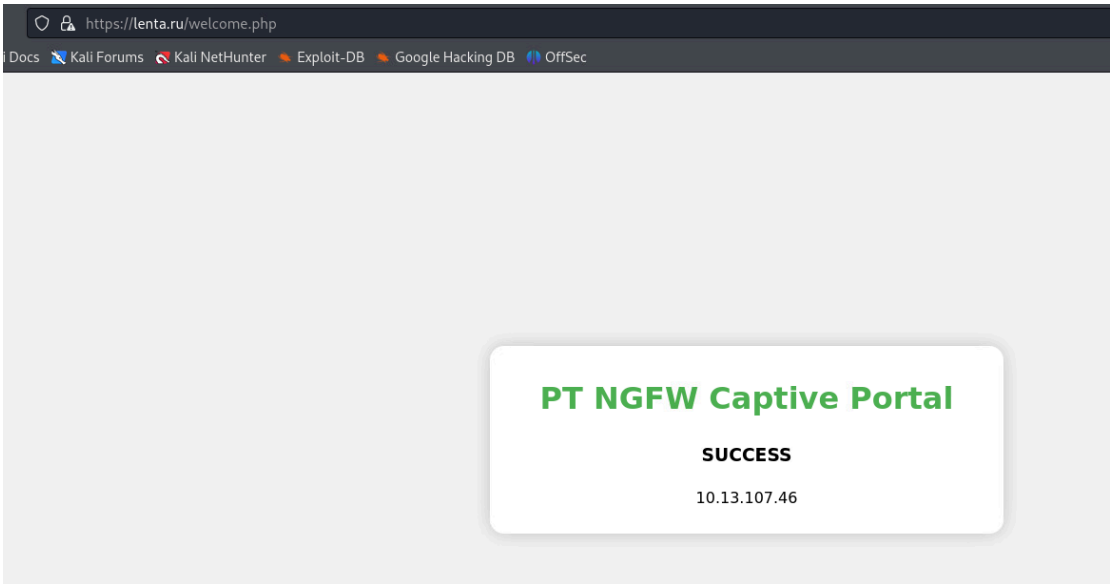

Рисунок 9. Успешная авторизация

ВАЖНО! Если Captive Portal в сообщении успешной авторизации выводит некорректный IP-адрес, то необходимо провести отладку. Одна из возможных причин — попадание трафика от ПК до Captive Portal под политики NAT, которые изменяют IP-адрес источника.

16. **Убедитесь в наличии соответствующих записей на странице Logs → Authentication policy.**
    Для трафика в сторону Captive Portal ожидаемое значение в колонке Action — bypass, для трафика в сторону Internet Action — redirect (в соответствии с политиками аутентификации, см. пункты 7-8).

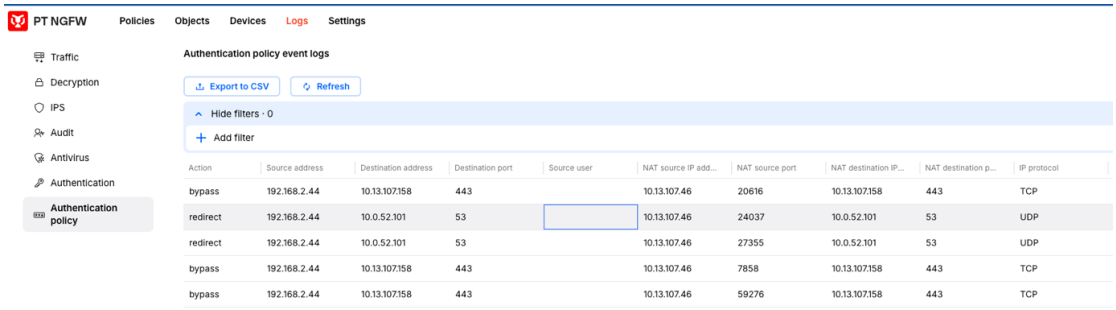

Рисунок 10. Страница Журналы → Аутентификация