

# ???????????? UDP/TCP ???????? (L3-L4) ?????????????? ???????? Nginx

Информация, приведенная на данной странице, является разработкой команды pre-sales и/или community KUMA и **НЕ** является официальной рекомендацией вендора.

Официальная документация по данному разделу приведена в Онлайн-справке на продукт: [Управление потоком событий с помощью nginx \(kaspersky.com\)](https://kaspersky.com)

Чтобы настроить балансировку трафика между коллекторами KUMA:

1. Установите nginx на сервере, предназначенном для управления потоком событий (предпочтительно выделенные сервера, не менее двух)

- Команда для установки в Oracle Linux 8.6:

```
$sudo dnf install nginx
```

- Команда для установки в Ubuntu 20.4:

```
$sudo apt-get install nginx
```

При установке из sources, необходимо собрать с параметром `-with-stream`:

```
$sudo ./configure -with-stream -without-http_rewrite_module -without-http_gzip_module
```

2. Подготавливаем конфигурационный файл nginx.conf, где блоки выделенные красным меняем (название\ip адреса\порт) под свою задачу.

```
{  
    upstream back_FW_ASA {  
        server 10.11.17.145:514;  
        server 10.11.18.145:514;  
    }  
}
```

и

```
server {  
    listen 514 udp;  
    proxy_pass back_FW_ASA;  
    proxy_bind $remote_addr transparent;  
}
```

При помощи данного файла nginx будет "прозрачно" для коллекторов пробрасывать оригинальный сетевой пакет трафика, позволяя передать реальный адрес(ия устройства, которое передало лог. При необходимости прослушивания TCP убираем в 16 строке udp.

```
user nginx;
worker_processes auto;
error_log /var/log/nginx/error.log;
pid /run/nginx.pid;
# Load dynamic modules. See /usr/share/doc/nginx/README.dynamic.
include /usr/share/nginx/modules/*.conf;
events {
    worker_connections 1024;
}
stream {
    upstream back_FW_ASA {
        server 10.11.17.145:514;
        server 10.11.18.145:514;
    }
    server {
        listen 514 udp;
        proxy_pass back_FW_ASA;
        proxy_bind $remote_addr transparent;
    }
}
```

3. Укажите адреса коллекторов KUMA и порт, в примере их адреса\порты - 10.11.17.145:514 ? 10.11.18.145:514, ????????????? ????????? ????????? ????? ????????? ? ????????????? 50:50 (??? ????????????? ????? ?????????????).

4. Служба балансировщика будет "прослушивать" 514 порт со всех IP адресов сервера, для большей отказоустойчивости служб предлагается использовать службу [keepalived](#) на двух серверах. Настройка [keepalived](#)

---

Revision #8

Created 2023-12-05 17:31:31 UTC

Updated 2026-05-04 08:02:35 UTC by Anton