



# **Инспектор сетевого фильтра NFI v1.1**

**Руководство пользователя**  
на 17 листах

**Москва  
2021г.**

## **Контактная информация**

127106, г. Москва, ул. Гостиничная,  
д.5Тел.: +7 (495) 988-92-25

E-mail: [office@avsw.ru](mailto:office@avsw.ru)

[www.avsw.ru/about/contacts](http://www.avsw.ru/about/contacts)

## **Авторское право**

ООО «АВ Софт»

[www.avsw.ru](http://www.avsw.ru)

© 2010-2021 ООО «АВ Софт»

## **Версия документа**

Март 20, 2021.

Настоящий документ является собственностью ООО «АВ Софт» (далее — «АВ Софт») и защищен законодательством Российской Федерации и международными соглашениями об авторских правах и интеллектуальной собственности.

Копирование документа либо его фрагментов в любой форме, распространение, в том числе в переводе, а также их передача третьим лицам возможны только с письменного разрешения «АВ Софт».

## СОДЕРЖАНИЕ

<b>1</b>	<b>Термины и определения .....</b>	<b>4</b>
<b>2</b>	<b>Введение.....</b>	<b>6</b>
<b>2.1</b>	<b>Назначение и условия применения.....</b>	<b>6</b>
<b>2.2</b>	<b>Функциональные ограничения .....</b>	<b>6</b>
<b>3</b>	<b>Подготовка к работе .....</b>	<b>7</b>
<b>4</b>	<b>Описание операций .....</b>	<b>11</b>
<b>5</b>	<b>Нештатные ситуации .....</b>	<b>13</b>
<b>6</b>	<b>Интеграция с внешним SIEM.....</b>	<b>16</b>

## 1 Термины и определения

В настоящем документе используются термины и определения, представленные в таблице .

**Таблица 1. Термины и определения**

№ п/п	Термин	Определение
1.	Вурасс режим	Режим питания нагрузки сетевым напряжением в обход основной схемы системы бесперебойного питания

В настоящем документе используется перечень сокращений, представленный в таблице.

**Таблица 2. Перечень сокращений**

<b>№ п/п</b>	<b>Сокращение</b>	<b>Расшифровка</b>
1.	IPFW	Ipfirewall
2.	NFI	Network Filter Inspector
3.	NGFW	Next-Generation Firewall
4.	VGA	Video Graphics Array
5.	НСД	Несанкционированный доступ
6.	ПО	Программное обеспечение

## **2 Введение**

Инспектор сетевого фильтра NFI (далее – NFI) является программным комплексом (далее – ПО) для контроля сетевого оборудования, включая межсетевые экраны нового поколения (NGFW), на предмет выявления компрометации и несанкционированного подключения к внешним ресурсам.

Область применения ПО включает в себя защиту информационной инфраструктуры от несанкционированного доступа (далее – НСД) сетевого оборудования во внешнюю сеть Интернет.

Уровень знаний пользователя ПО должен соответствовать уровню администратора ПО.

### **2.1 Назначение и условия применения**

ПО предназначено для решения задач контроля подключений к внешним ресурсам сети Интернет со стороны сетевых устройств корпоративной или ведомственной сети, включая NFW, в целях усиления безопасности информационной инфраструктуры организации.

ПО может использоваться как для контроля NGFW, так и в качестве самостоятельного межсетевого экрана.

### **2.2 Функциональные ограничения**

В ПО присутствует ограничение на минимальное количество интерфейсов, которых должно быть не менее 4-х. Данное разграничение необходимо для удобного контроля проходящих пакетов. В случае, когда сетевых интерфейсов пять и более, NFI назначает NGFW1 и NGFW2 на интерфейсы по середине, интерфейсы с номером меньше половины от их количества работают аналогично интерфейсу LAN, а интерфейсы с номером больше половины от их количества работают аналогично интерфейсу WAN. При нечетном количестве интерфейсов LAN интерфейсов назначается на 1 больше.

### 3 Подготовка к работе

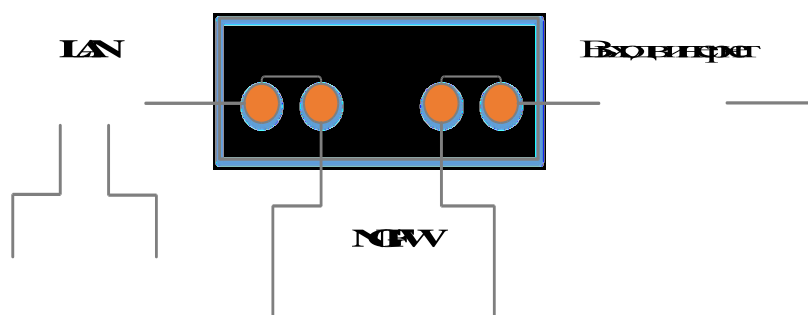
Для подготовки NFI к работе необходимо выполнить следующую последовательность действий:

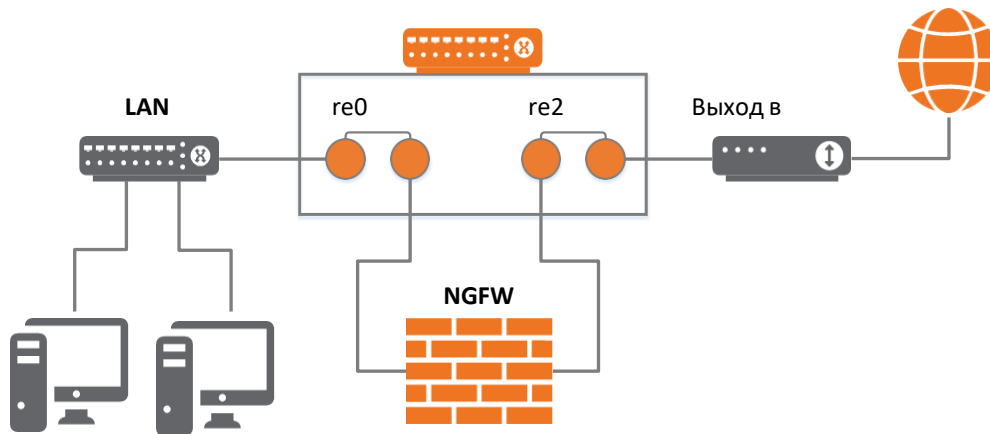
1. Необходимо подключить кабель питания, консольный кабель VGA или COM кабель.
2. Далее необходимо подключить кабели Ethernet к устройству в соответствии с их назначением по таблице 3 и схемой подключения портов на рисунке 1.

Таблица 3. Конфигурация сетевых портов

№ п/п	Порт	Назначение
1.	WAN (LAN1)	Выход в сеть Интернет
2.	NGFW1 (LAN2)	Оборот в кольцо NGFW (WAN)
3.	NGFW2 (LAN3)	Оборот в кольцо NGFW (LAN)
4.	LAN (LAN4)	Выход в локальную сеть

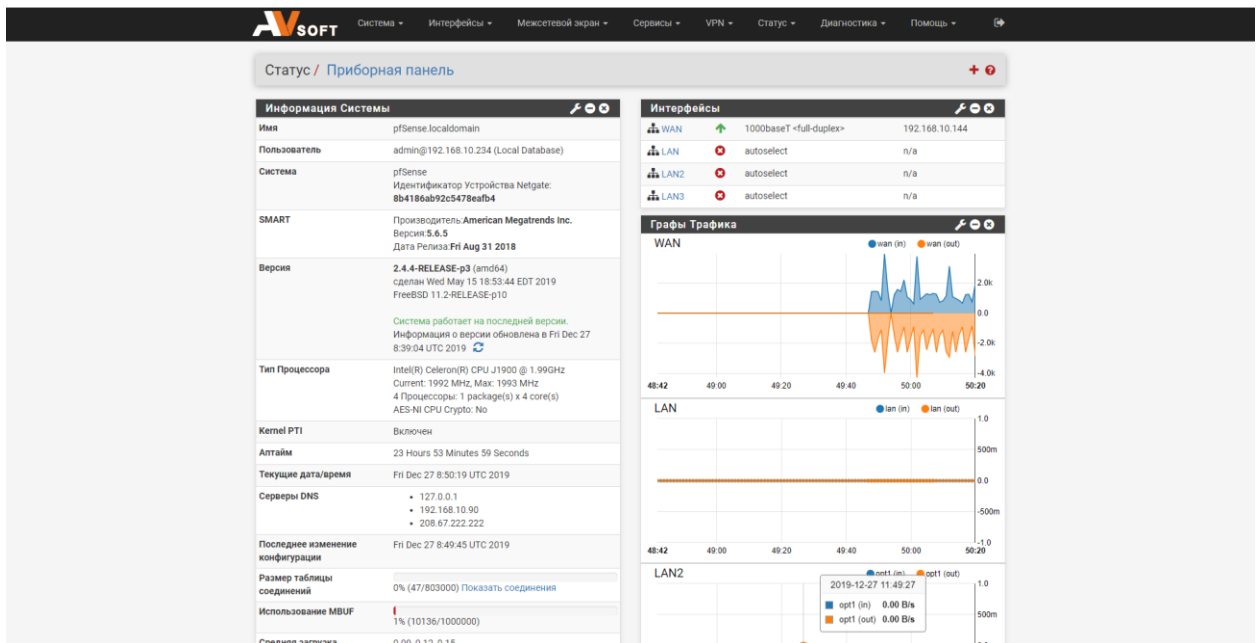
Интерфейсы NFI





**Рисунок 1. Схема подключения портов NFI**

3. Включить NFI. На экране загрузки получить IP адрес, выделенный NFI на интерфейсе WAN.
4. Выполнить авторизацию в веб-интерфейсе NFI по полученному IP адресу из предыдущего пункта из компьютера, подключенного к локальной сети (LAN4) (Рисунок 2).



**Рисунок 2. Авторизация в NFI**



5. Перейти во вкладку «Межсетевой экран» (Рисунок 3).

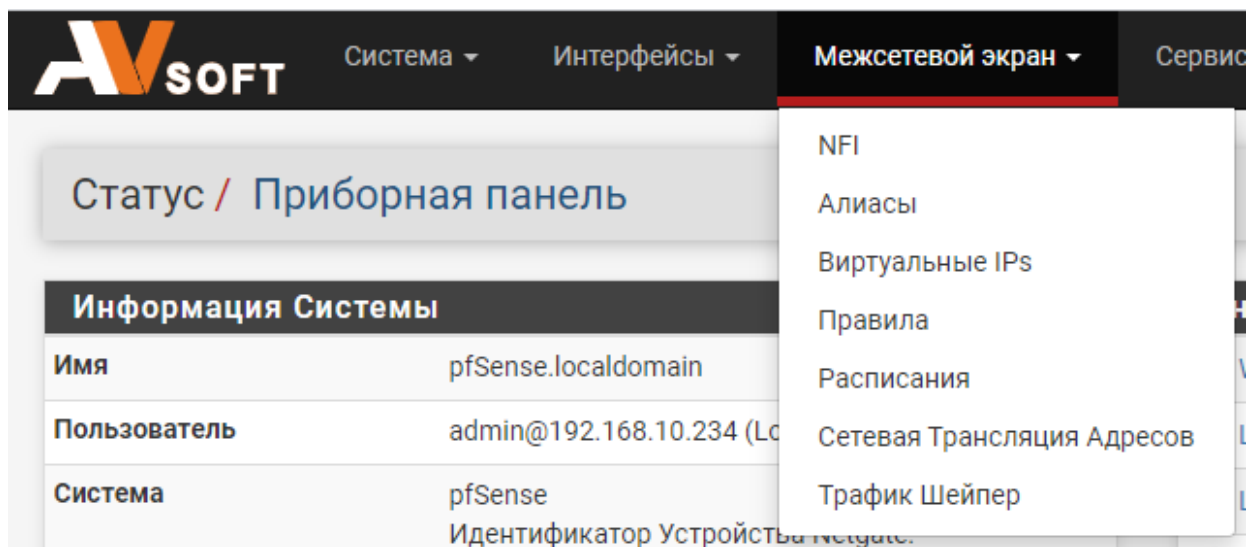


Рисунок 3. Переход в NFI

6. Далее выбрать «NFI» (Рисунок 4).

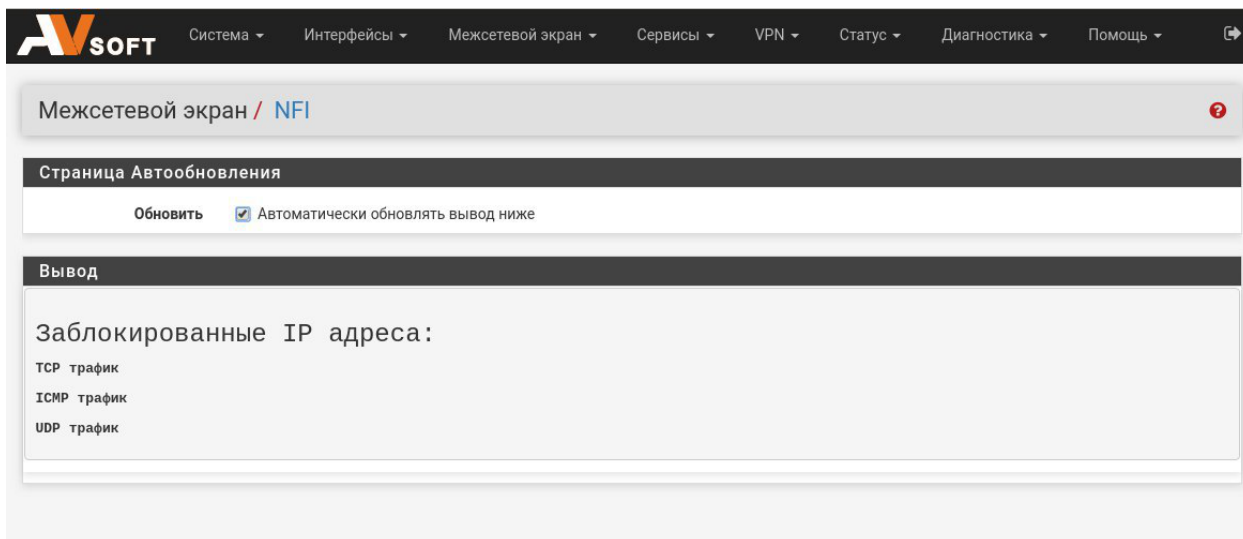
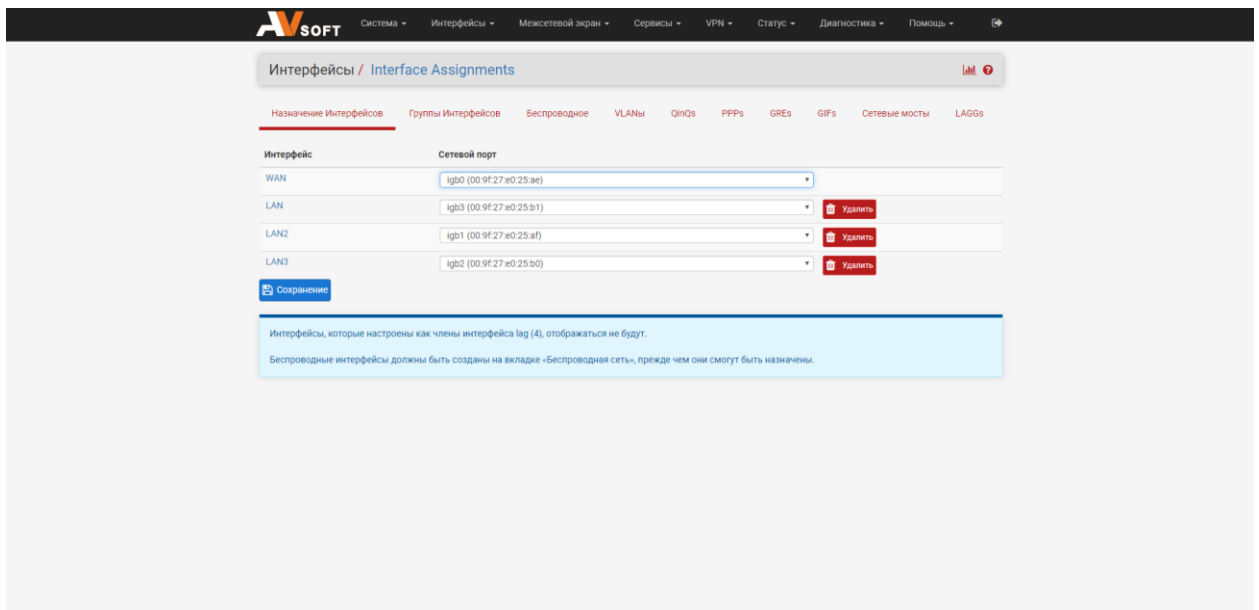


Рисунок 4. Вкладка «Межсетевой экран/NFI»



**Рисунок 5. Настройка сетевых портов**

7. Проверить наличие доступа в Интернет на машине, которая подключена к NGFW со стороны локальной сети (Интерфейс LAN).

## 4 Описание операций

Описание интерфейсов по порядку прохождения сетевых пакетов представлено в таблице 4.

Таблица 4. Описание интерфейсов

№ п/п	Интерфейс	Описание
1.	Интерфейс LAN (LAN4)	К данному интерфейсу подключается локальная сеть, локальный маршрутизатор. Те IP адреса, на которые поступает запрос из этого интерфейса, заносятся в специальный список с разрешёнными IP адресами. Данный список включает в себя счётчик пакетов для данного IP адреса, а также время (в секундах), когда пакет был обработан.
2.	Интерфейс NGFW2 (LAN3)	К данному интерфейсу подключается NGFW. Пакеты пришедшие с интерфейса LAN попадают на NGFW не претерпевая никаких изменений.
3.	Интерфейс NGFW1 (LAN2)	К данному интерфейсу подключается выход NGFW. Пакеты, проходящие из этого интерфейса, должны фильтроваться на случай НСД со стороны межсетевого экрана. Для тех IP адресов, которые были найдены в ранее заведённом списке, прохождение пакета будет заблокировано.
4.	Интерфейс WAN (LAN1)	К данному интерфейсу подключается выход в сеть Интернет. Пакеты на данном этапе уже отфильтрованы от НСД со стороны NGFW.

Минимальные требования к техническим средствам представлены в таблице 5.

**Таблица 5. Минимальные требования к техническим средствам**

<b>№ п/п</b>	<b>Характеристики оборудования</b>	<b>Требования</b>
1.	Процессор	Intel Celeron J1000 или похожий. 2 ядра, от 1 GHz
2.	Оперативная память	4 GB
3.	Жесткий диск	HDD 30 Гб
4.	Сетевая карта	4 порта 10/100BASE-T(X)

Для работы в диалоговом режиме используется экран дисплея, клавиатура и манипулятор типа «мышь».

Для поддержки графического режима необходимо наличие адаптер SVGA.

Входные данные хранятся на гибком и/или жестком дисках. Программа работает под управлением ОС FreeBSD.

## 5 Нештатные ситуации

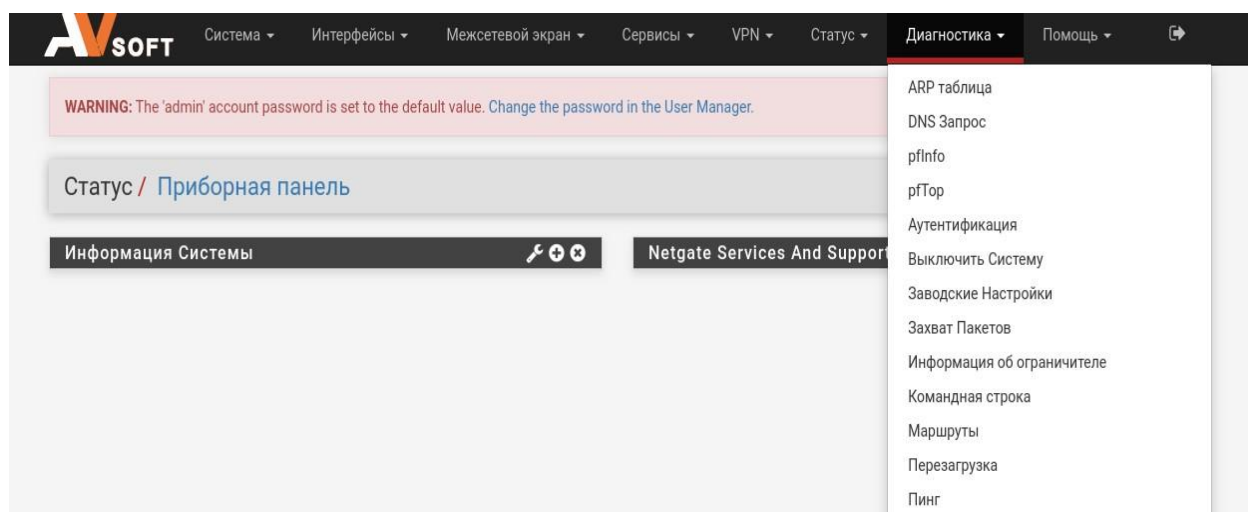
Примеры возможных нештатных ситуаций, связанных с программным и аппаратным сбоем, а также порядок действий, приведены в таблице .

Таблица 6. Порядок действий в нештатных ситуациях

№ п/п	Нештатная ситуация	Порядок действий
1.	Отсутствует проверка сетевого трафика	<ul style="list-style-type: none"><li>– Проверить корректность настройки сетевых портов.</li><li>– Необходимо перейти в веб-интерфейс NFI и удостовериться, что отсутствует сообщение об ошибках.</li><li>– Необходимо проверить работоспособность NGFW.</li></ul>
2.	Потеря питания	При потере питания система NFI, то все сетевые порты автоматически переходит в режим Vurass (но в данном режиме контроля сетевого трафика не осуществляется).
3.	Потеря данных	Для восстановления данных в системе необходимо инициировать процедуру восстановления данных из резервной копии, которая осуществляется после каждого изменения в системе NFI.
4.	Потеря работоспособности	Использовать функцию пробуждения по сети.

№ п/п	Нештатная ситуация	Порядок действий
5.	Отключение NGFW	При отключении можно использовать NFI в качестве межсетевого экрана (требуется дополнительная настройка) с ограниченным функционалом.
6.	Несанкционированное вмешательство в данные	Отключить доступ во внешнюю сеть Интернет.

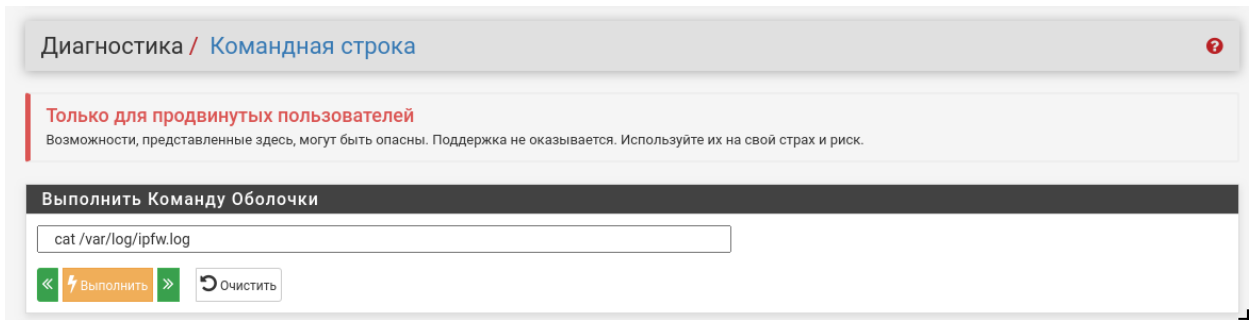
Для просмотра полной информации о заблокированных пакетах необходимо перейти во вкладку «Диагностика» далее «Командная строка» (Рисунок 6).



**Рисунок 6. Открытие командной строки**

В открытой вкладке в поле «Command» необходимо вписать следующую команду:

```
cat /var/log/ipfw.log
```

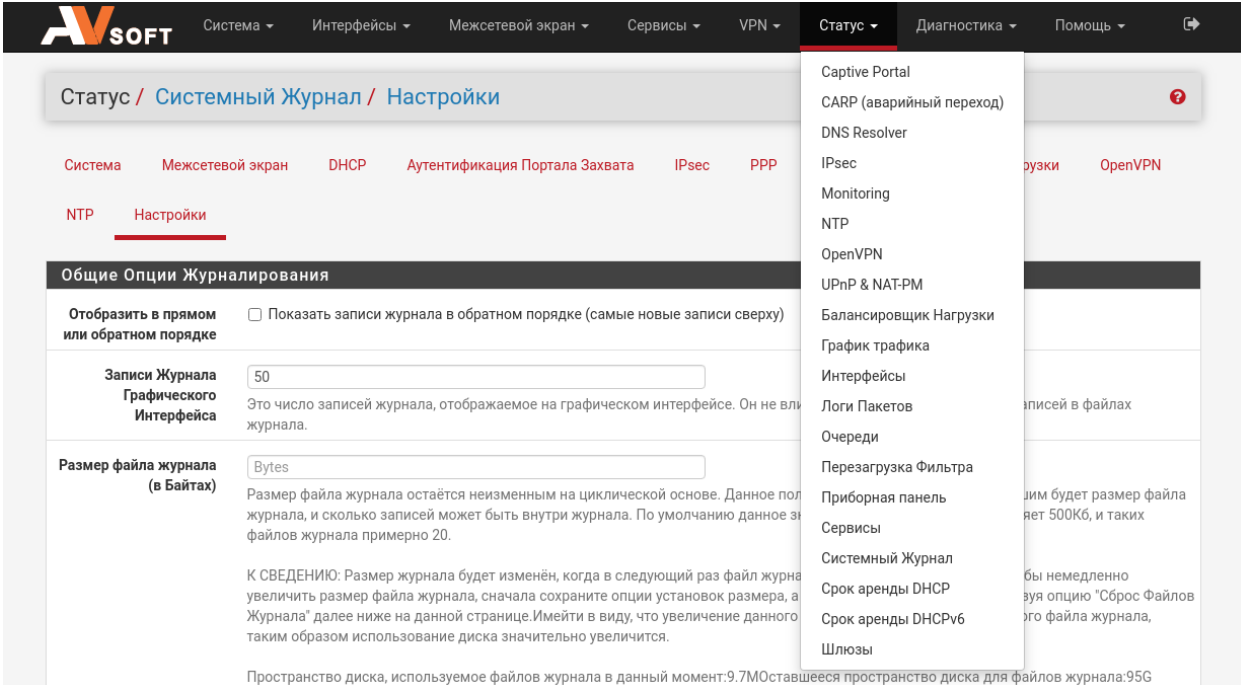


**Рисунок 7. Выполнение команды командной строке**

## 6 Интеграция с внешним SIEM

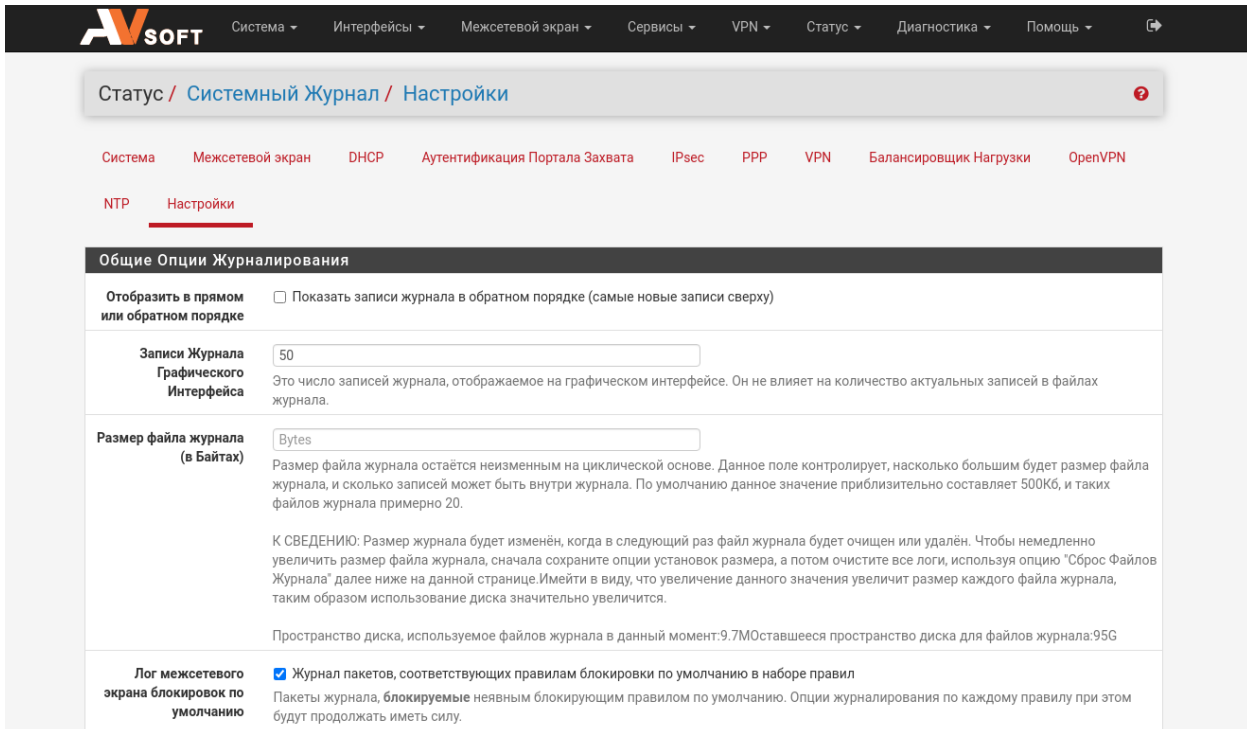
Для подключения к внешнему SIEM необходимо:

### 1. Перейти в графическом интерфейсе NFI во вкладку Статус



The screenshot shows the AVSOFT NFI interface. The top navigation bar includes 'Система', 'Интерфейсы', 'Межсетевой экран', 'Сервисы', 'VPN', 'Статус', 'Диагностика', and 'Помощь'. The 'Статус' menu is open, displaying a list of system components: Captive Portal, CARP (аварийный переход), DNS Resolver, IPsec, Monitoring, NTP, OpenVPN, UPnP & NAT-PM, Балансировщик Нагрузки, График трафика, Интерфейсы, Логи Пакетов, Очереди, Перегрузка Фильтра, Приборная панель, Сервисы, Системный Журнал, Срок аренды DHCP, Срок аренды DHCPv6, and Шлюзы. The main content area shows the 'Системный Журнал / Настройки' page with various configuration options for logging.

### 2. Далее «Системный журнал» (Настройки)



The screenshot shows the 'Системный журнал' settings page in the AVSOFT NFI interface. The top navigation bar is the same as in the previous screenshot. The main content area is titled 'Общие Опции Журналирования' and contains the following settings:

- Отобразить в прямом или обратном порядке:**  Показать записи журнала в обратном порядке (самые новые записи сверху)
- Записи Журнала Графического Интерфейса:** 50. This number represents the number of log entries displayed on the graphical interface. It does not affect the number of actual entries in the log files.
- Размер файла журнала (в Байтах):** Bytes. The log file size remains constant on a cyclic basis. This field controls how large the log file will be, and how many entries can fit inside it. By default, this value is approximately 500KB, and such log files are about 20.
- Лог межсетевого экрана блокировок по умолчанию:**  Журнал пакетов, соответствующих правилам блокировки по умолчанию в наборе правил. Packets from the log, blocked by a default blocking rule. Logging options for each rule will continue to have effect.

Additional information at the bottom of the page: 'Пространство диска, используемое файлами журнала в данный момент: 9.7Мб' and 'Оставшееся пространство диска для файлов журнала: 95G'.



### 3. В нижней части страницы выбрать опцию «Отправлять сообщения журнала на удаленный сервер syslog»

#### Опции Удалённого Журналирования

**Включить Удалённое Журналирование**  Отправлять сообщения журнала на удаленный сервер syslog

**Адрес Источника**

Эта опция позволяет демону журналирования связываться с одним IP адресом, вместо всех IP адресов. Если выбран один IP, все удалённые серверы системного журнала должны быть этого типа IP. Чтобы использовать IPv4 и IPv6 удалённые серверы системного журнала, привяжите их ко всем интерфейсам.

К СВЕДЕНИЮ: Если IP адрес не может быть найден на выбранном интерфейсе, демон будет привязан ко всем адресам.

**IP Протокол**

Данная опция используется только при выборе выше не-дефолтного адреса в качестве источника. Данная опция всего лишь выражает предпочтение; Если IP адрес данного типа не найден на выбранном интерфейсе, будет предпринята попытка использования другого типа.

**Серверы удалённого журнала**

**Содержание Удалённого Сервера Журнала**  Все

- Системные События
- События Межсетевого Экрана
- DNS-события (Резолвер/исходящий, Форвардер/dnsmasq, filterdns)
- События DHCP (DHCP-демон, DHCP-ретрансляция, DHCP-клиент)
- События PPP (клиент WAN PPPoE, клиент WAN L2TP, клиент WAN PPTP)
- События Портала авторизации
- События VPN (IPsec, OpenVPN, L2TP, PPPoE-сервер)
- События монитора шлюза
- События демона маршрутизации (RADVD, UPnP, RIP, OSPF, BGP)
- События Балансировщика Нагрузки Сервера (relayd)
- События Протокола Сетевого Времени (демон NTP, клиент NTP)
- События беспроводной сети (hostapd)

Системный Журнал отправляет датаграммы на порт 514 указанного удалённого сервера системного журнала, если не указан другой порт. Убедитесь в том, что настроен syslogd на удалённом сервере, чтобы принимать сообщения системного журнала от pfSense.

### 4. Ввести адрес сервера и отметить необходимые события