Руководство по эксплуатации

программного обеспечения «Программное средство автоматизированного контроля и мониторинга веб-приложений NF Web Application Firewall (NF WAF)»

ООО «Сивиэй Технолоджиес»

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

«Программное средство автоматизированного контроля и мониторинга веб-приложений NF Web Application Firewall (NF WAF)»

РУКОВОДСТВО ПО ЭКСПЛУАТАЦИИ

На 12 листах

Ростов-на-Дону

2023

Все упомянутые в этом документе названия продуктов, логотипы, торговые марки товарные знаки принадлежат их владельцам.

Товарные знаки «NeuroFortress», «NF WAF», «NF Web Application Firewall», принадлежат ООО «Сивиэй Технолоджиес», «CVA Technologies».

Ни при каких обстоятельствах нельзя истолковывать любое содержимое настоящего документа как прямое или косвенное предоставление лицензии или права на использование товарных знаков, логотипов или знаков обслуживания, приведенных в нем. Любое несанкционированное использование этих товарных знаков, логотипов или знаков обслуживания без письменного разрешения их правообладателя строго запрещено.

Содержание

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

Сокращения, которые используются в настоящем документе, приведены в таблице 1.

Таблица 1 – Сокращения и расшифровки

Сокращение	Расшифровка
ОС	Операционная система
ПК	Персональный компьютер
ПО	Программное обеспечение
ИМ	Информационная модель
ПО NF Web Application Firewall	«Программное средство автоматизированного контроля и мониторинга веб-приложений NF Web Application Firewall (NF WAF)»

1. Общие сведения. Назначение

Программный продукт «Программное средство автоматизированного контроля и мониторинга веб-приложений NF Web Application Firewall (NF WAF)» - это совокупность программных мониторов и фильтров, предназначенных для обнаружения и блокирования сетевых атак на веб-приложение. NF Web Application Firewall (NF WAF) устанавливается перед защищаемым веб ресурсом и анализирует все передаваемые HTTP запросы на наличие вредоносного кода и потенциально опасную активность злоумышленников. При проведении анализа NF Web Application Firewall (NF WAF) основывается на различных механизмах сигнатурного анализа, правилах, средствах анализа аномалий. Также в своей работе NF Web Application Firewall (NF WAF)могут использовать нейросети и различные индикаторы атак.

В случае обнаружения вредоносных запросов NF Web Application Firewall (NF WAF) может выполнить следующие действия: удалить из запроса опасные данные по аналогии с тем, как антивирус пытается лечить зараженные файлы, также запрос может быть заблокирован целиком. Также возможна блокировка источника атаки на сетевом уровне, то есть, блокировка всех обращений с данного IP-адреса.

2. Системные требования

Операционная система Windows

Операционная система	Windows 10,11
Процессор	CPU 2 ядра и более
Оперативная память	Минимально – 2 ГБ Рекомендуется – 4 ГБ
Жесткий диск (свободное пространство)	SSD или HDD размером от 10 Гб

Операционная система Linux

Операционная система	Linux Ubuntu, Linux Ubuntu Server, Astra Linux, ALT Linux, OS Atlant
Процессор	CPU 2 ядра и более
Оперативная память	Минимально – 2 ГБ Рекомендуется – 4 ГБ
Жесткий диск (свободное пространство)	SSD или HDD размером от 10 Гб

–

3. Проверка работоспособности ПО NF Web Application Firewall (NF WAF)

Для начала работы с программным продуктом «Программное средство автоматизированного контроля и мониторинга веб-приложений NF Web Application Firewall (NF WAF)» необходимо запустить приложение, подключиться к системе и авторизоваться в соответствии с данными, полученными от сотрудников ООО «Сивиэй Технолоджиес», после чего информационная модель перейдёт на главный экран ПО NF Web Application Firewall (NF WAF).

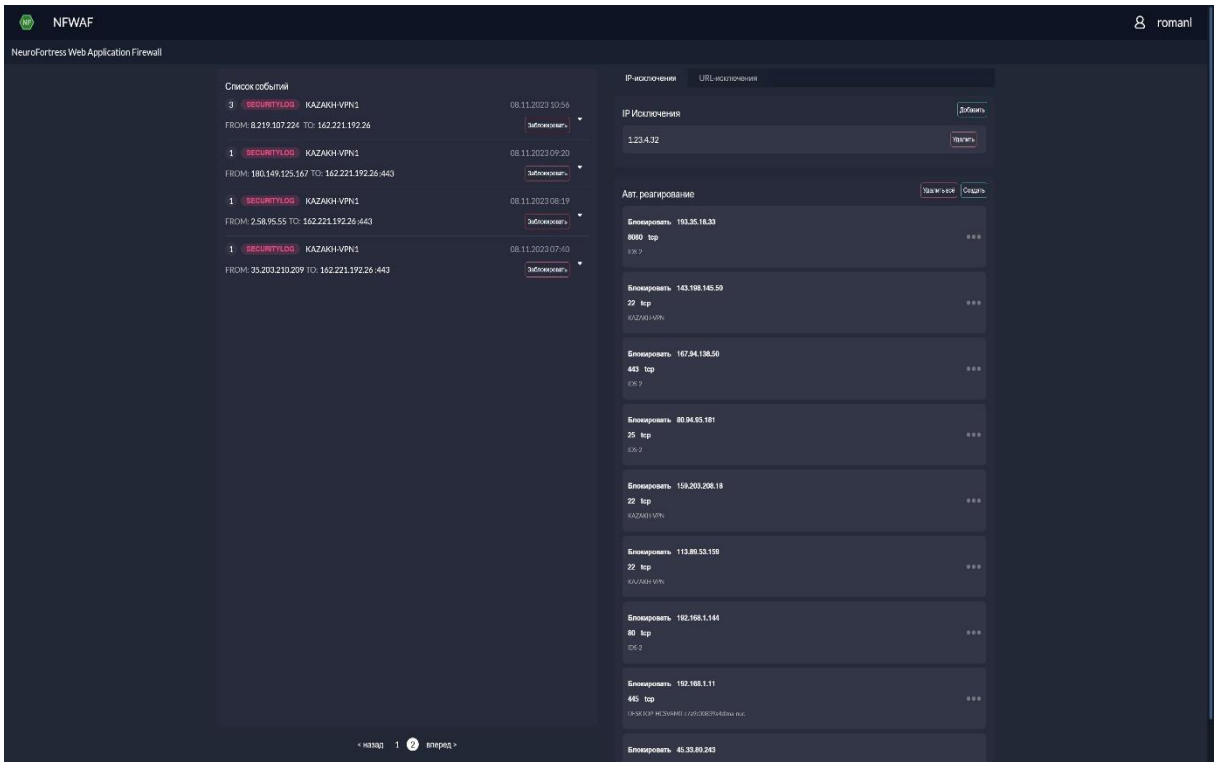

Рисунок 4 – Главный экран NF Web Application Firewall (NF WAF)

Путем контроля информационной модели «Список события» проверяют наличие как минимум одного поля событий брандмауэра.

Положительных результат контроля данных информационных систем говорит о выполнении требований к качественным и количественным характеристикам функционала « NF Web Application Firewall (NF WAF)».

4. Работа в ПО NF Web Application Firewall (NF WAF)

На главном экране приложения программного продукта «Программное средство автоматизированного контроля и мониторинга веб-приложений NF Web Application Firewall (NF WAF)» слева расположена вертикальная информационная модель, представляющая собой список событий.

Чтобы отобразить информацию о событии проводится нажатие щелчком левой кнопки мыши на нужное событие в информационной модели «События». После чего отобразятся все атаки, принадлежащие выбранному событию. Для просмотра информации об атаке левым щелчком мыши проводится нажатие на кнопку Подробнее. После чего на информационной модели отобразится подробная информация о выбранной атаке – Рисунок 5. Чтобы добавить URL-исключение, в отобразившемся окне щелчком левой кнопки мыши проводится нажатие на кнопку Добавить в исключения.

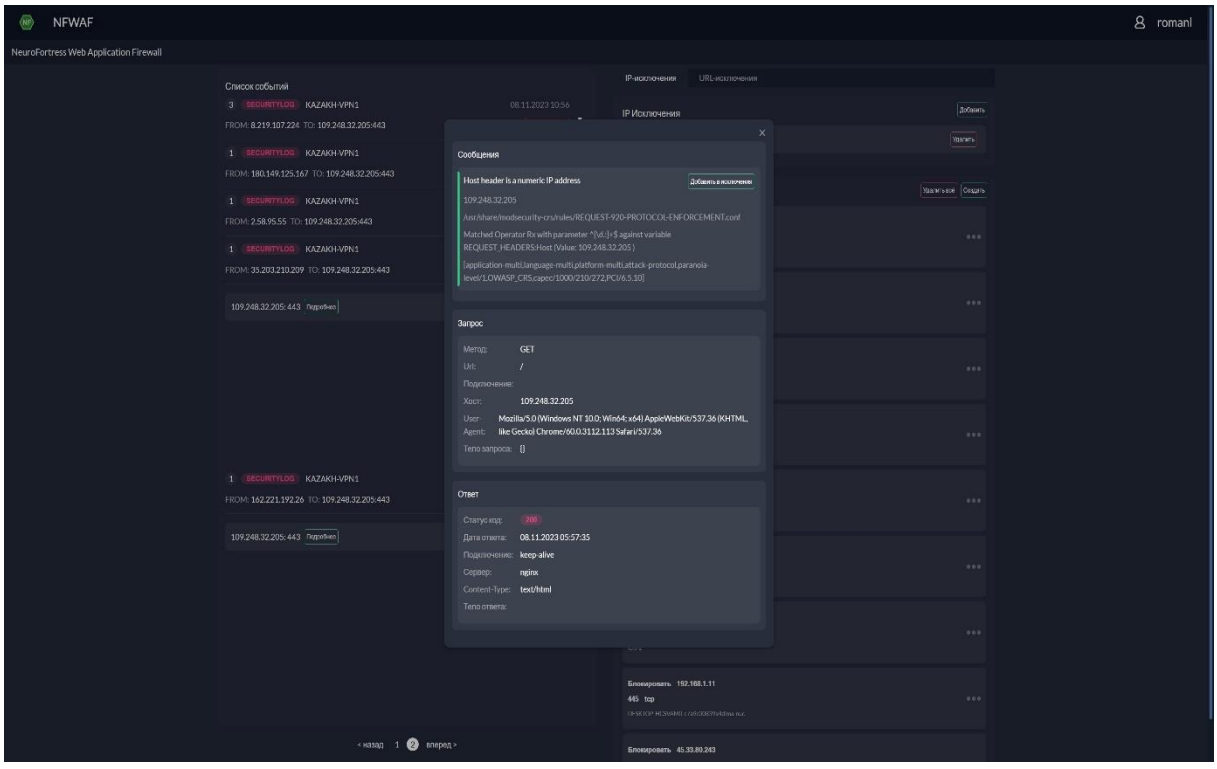

Рисунок 5 – Окно с подробной информацией об атаке

Информационная модель веб приложений позволяет контролировать события блокировки и устанавливать исключения для сервисов, каталогов.

Чтобы создать исключения для IP адресов, левым щелчком мыши проводится нажатие на кнопку **Добавить** на информационной модели «IP-исключения». После чего в отобразившееся поле для ввода вводится IP адрес сети, который требуется добавить в исключения – Рисунок 6.

Затем левым щелчком мыши проводится нажатие на кнопку **Добавить**.

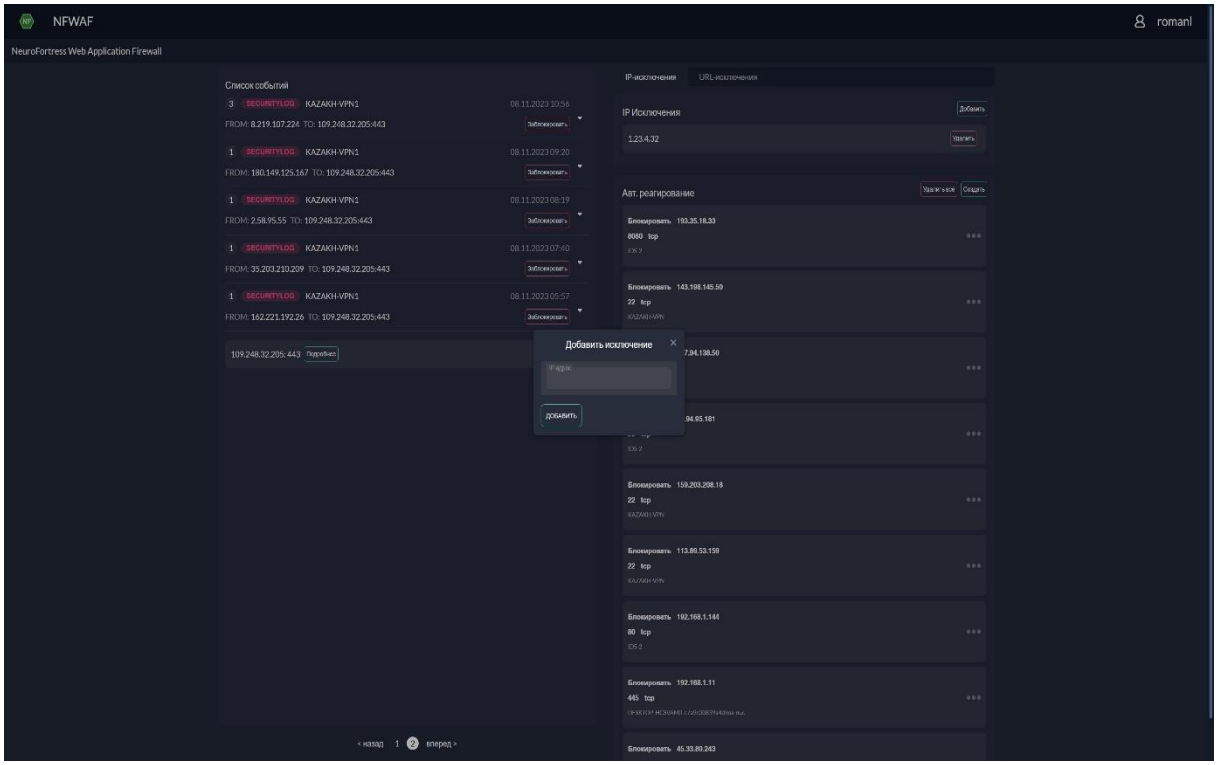

Рисунок 6 - Форма создания IP-исключения

Чтобы отобразить список URL-исключений , щелчком левой кнопки мыши проводится нажатие на кнопку **URL-исключения** на информационной модели «IP-исключения» – Рисунок 7.

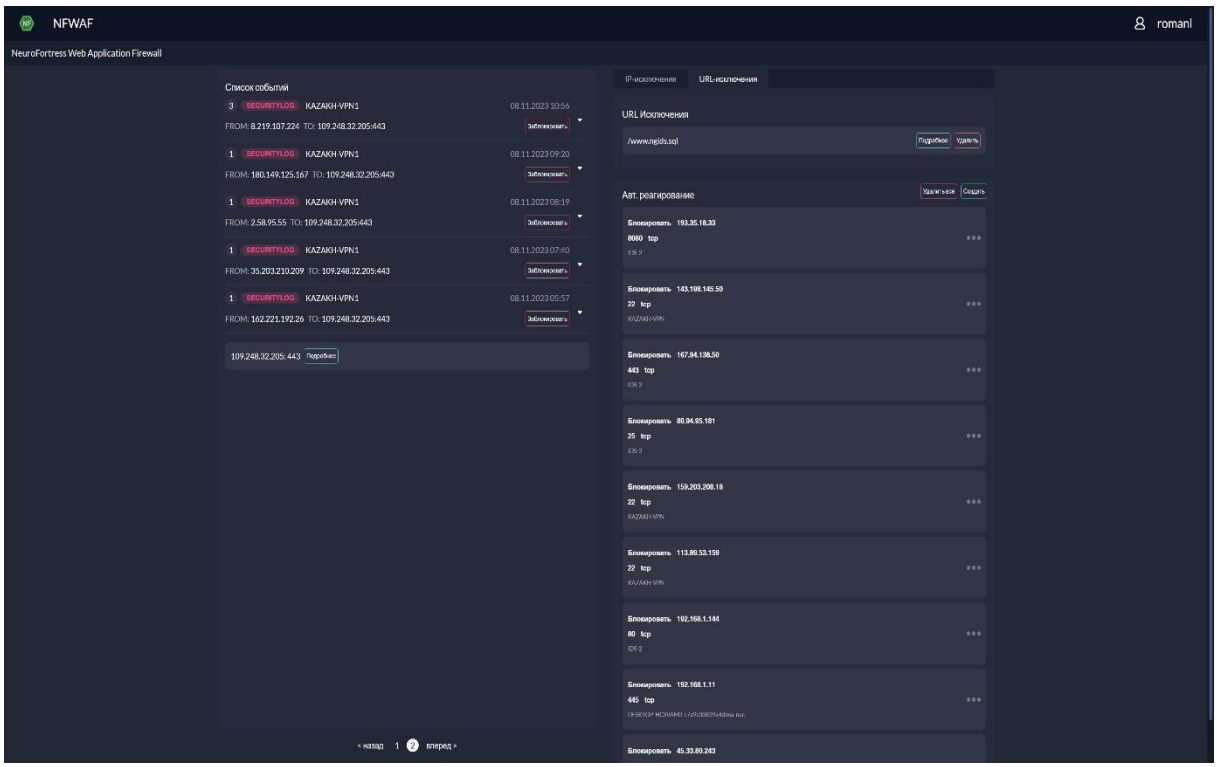

Рисунок 7 – Экран NF Web Application Firewall (NF WAF) с ИМ моделью URL-исключения

По событиям блокировки возможно создание постоянных правил блокирования относительно вектора атакующего воздействия.

Чтобы создать постоянное правило блокирования щелчком левой кнопки мыши проводится нажатие на кнопку **Заблокировать** у нужного события, после чего на информационной модели отобразится заполненная форма с данными для блокировки – Рисунок 8.

После чего, в отобразившейся форме левым щелком мыши проводится нажатие на кнопку **Создать правило**. Затем на информационной модели отобразится новая заполненная форма, которая при необходимости редактируется. Для подтверждения создания постоянного правила блокирования щелчком левой кнопки мыши проводится нажатие на кнопку Создать, после чего созданное правило добавится в список информационной модели «**Авт. реагирование**».

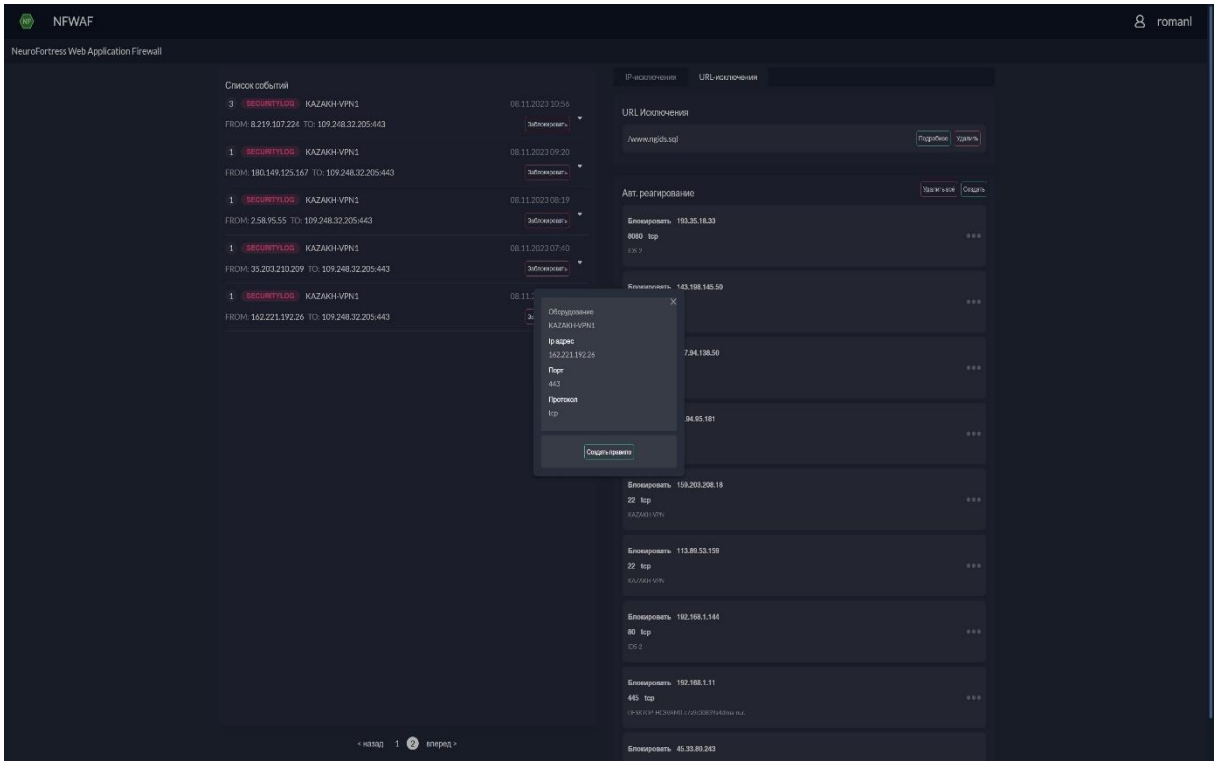

Рисунок 8 – Форма создания правила блокирования

5. Техническая поддержка

Контактная информация службы технической поддержки ООО «СИВИЭЙ Технолоджиес» CVA Technologies в случае возникновения вопросов, неописанных в данном руководстве:

1. Адрес электронной почты: vav@cvatec.com
2. Телефон: 8-900-130-3-666.