



INFOWATCH ARMA INDUSTRIAL FIREWALL 3.7.2

What's new

Новые возможности

[Обновлён функционал VPN](#)

[Улучшена работа протоколов](#)

[Расширены функции журналов](#)

[Иные улучшения](#)

Обновлён функционал VPN

- Добавлена поддержка OpenVPN-ГОСТ, что позволяет пользователю включить шифрование каналов связи на базе сертифицированного ФСБ России СКЗИ
 - В настройки VPN добавлена возможность выбора типа OpenVPN или OpenVPN-ГОСТ, которая позволяет пользователю самостоятельно выбирать и настраивать предпочитаемый тип шифрования каналов связи
 - В журнал VPN добавлена фильтрация логов по конкретному типу VPN
- Реализована возможность экспорта настроек выбранного типа VPN
- В раздел «Статус соединения» добавлено отображение выбранного типа VPN, что позволяет пользователю отслеживать статус соединения настроенного у него типа VPN
- Добавлено оповещение пользователя об окончании срока действия лицензии OpenVPN-ГОСТ и необходимости её продления для корректной работы сертифицированного шифрования каналов связи
-

Улучшена работа протоколов

- Добавлена поддержка промышленного протокола KRUG, используемого в контроллерах и СКАДА производства компании «НПФ „КРУГ“», что позволяет пользователям создавать правила и фильтровать трафик по данному типу протокола
- В интерфейс создания правила для протоколов KRUG и GOOSE добавлены подсказки к заполняемым полям, позволяющие пользователю корректно задать параметры правилам для этих протоколов
- Для протокола GOOSE добавлена возможность настройки правила фильтрации по времени
- Для протокола S7Comm_Plus улучшен парсер, добавлена возможность работы на уровне приложений
- Для протокола OPC UA реализована настройка детектирования по значениям идентификатора пространства имён: числовой тип, строковый тип, GUID-тип

The image shows a configuration interface with four sections, each with a dropdown menu:

- Тип сообщения:** MESSAGE
- Тип запроса:** BROWSE
- Идентификатор пространства имен:** A dropdown menu is open, showing options: Отсутствует, Числовой тип, Строковый тип, GUID тип. A mouse cursor is pointing at 'Строковый тип'.
- Тип идентификатора узла:** Отсутствует

Below the dropdowns, there are labels: 'Выберите опцию' under the first two, and 'Выберите тип идентификатора узла' under the last one.

Расширены функции журналов

- В журнал Syslog добавлена возможность выгрузки всего журнала / лога, позволяющая пользователю одним нажатием выгрузить сразу весь журнал
- В «Журнал событий безопасности» добавлено отображение логов антивируса, содержащих информацию о заблокированных вирусах и вирусных файлах
- В журнал раздела «Обнаружение вторжений» добавлена возможность фильтрации логов по типу «Журнал СОВ» или «Журнал загрузки правил», а также по уровню сообщения «Все», «Ошибка», «Предупреждение», «Примечание», «Информация», что позволяет пользователю в более удобном формате работать с зафиксированными событиями

Обнаружение вторжений: Администрирование

Настройки Сохранение Правила **Журналирование** Расписание

Поиск Журнал COB Все

Дата	Сообщение	Классификация
4 мая 2022, 10:34:25	suricata[33822]: [Alert] [1:2210046:2] SURICATA STREAM SHUTDOWN RST invalid ack [Classification: Generic Protocol Command Decode] [Priority: 3] [TCP] 192.168.56.1:9003 -> 192.168.73.146:38651	92.168.73.146:38651
4 мая 2022, 10:34:25	suricata[33822]: [Alert] [1:2210045:2] SURICATA STREAM SHUTDOWN RST invalid ack [Classification: Generic Protocol Command Decode] [Priority: 3] [TCP] 192.168.56.1:9003 -> 192.168.73.146:38651	92.168.73.146:38651
4 мая 2022, 10:29:45	suricata[33822]: [Alert] [1:2210046:2] SURICATA STREAM SHUTDOWN RST invalid ack [Classification: Generic Protocol Command Decode] [Priority: 3] [TCP] 192.168.56.1:9003 -> 192.168.73.146:35775	92.168.73.146:35775

Иные улучшения

- Добавлена возможность полного восстановления конфигурации InfoWatch ARMA Industrial Firewall, включая настройки сетевых интерфейсов
- В расширенные настройки раздела «Обнаружение вторжений: администрирование» добавлена возможность задать размер сохраняемых журналов в диапазоне от 8 до 512 Мбайт

Обнаружение вторжений: Администрирование

Настройки Сохранение Правила **Журналирование**

расширенный режим справка

Размер сохраняемых журналов 256

- Исправлена ошибка, из-за которой в кластере не синхронизировались правила COB
- В настройки «Netflow» добавлено поле «Время ротации flowd.log»: 10–120 сек.

Захват Кэш

расширенный режим

Прослушиваемые интерфейсы LAN, WAN

Интерфейсы WAN WAN

Захватывать внутренний трафик

Версия v9

Получатели 127.0.0.1:2056

Тайм-аут активности 1800

Тайм-аут неактивности 15

Время ротации flowd.log 9 Должно быть числом в диапазоне от 10 до 120