

INFOWATCH ARMA INDUSTRIAL FIREWALL 3.16



what's new

В новой версии InfoWatch ARMA Industrial Firewall добавлены инструменты, которые помогают соответствовать требованиям регуляторов и организовать безопасное VPN-соединение между объектами. Управление защитой стало более точечным и удобным.

В релизе 3.16 появилась возможность использовать отечественные криптографические алгоритмы ГОСТ VPN. Для контроля всего трафика был добавлен «неразборчивый» режим в настройках Ethernet-интерфейса. Логи службы обнаружения устройств стали доступны прямо в веб-интерфейсе, а экспорт данных из этой службы стал удобнее. Очистка журнала теперь фиксируется, ротация лог-файлов OpenVPN была обновлена.

Новые возможности

ГОСТ-алгоритмы шифрования

VPN: IPsec: База данных безопасных ассоциаций (SAD)						
Отправитель	Получатель	Протокол	SPI	Алгоритм шифрования	Алгоритм аутентификации	Данные
172.16.	172.16.	ESP	c7 44	magma-mgm		432 B
172.16.	172.16.	ESP	c1 f3	magma-mgm		240 B

VPN: IPsec: База данных безопасных ассоциаций (SAD)						
Отправитель	Получатель	Протокол	SPI	Алгоритм шифрования	Алгоритм аутентификации	Данные
172.16.	172.16.	ESP	c7 44	gost341215k	streobog-512	432 B
172.16.	172.16.	ESP	c1 f3	gost341215k	streobog-512	240 B

Используйте защищённый канал связи по стандартам ГОСТ. Для VPN-соединений на базе IPsec и IKEv2 добавлены отечественные алгоритмы шифрования ГОСТ Р 34.12-2015 («Кузнечик» и «Магма») для создания безопасных подключений в объектах критической информационной инфраструктуры. Решение имеет необходимые сертификаты соответствия.

«Неразборчивый» режим в настройках Ethernet-интерфейса

Общая конфигурация

Смешанный режим

Включает неразборчивый режим на интерфейсе.

Контролируйте весь трафик. «Неразборчивый» режим сетевого интерфейса (romiscuous mode) позволяет межсетевому экрану «видеть» весь трафик сети, включая не предназначенный для него.

Это особенно полезно на SPAN-интерфейсе: вы можете копировать трафик из других портов или сегментов, анализировать его и на основе этого писать точные правила фильтрации, не меняя основной трафик.

Журнал службы обнаружения устройств

Сеть: обнаружение устройств. Журналирование

Дата	Сообщение
16 октября 2025, 12:47:02	arpwatch: new station 99.8.77.6 00:50:56:bd:fd:9a
16 октября 2025, 12:47:02	arpwatch: new station 99.8.77.66 00:50:56:bd:63:30
16 октября 2025, 12:43:13	arpwatch: new station 999.888.777.66 00:50:56:bd:41:a8
16 октября 2025, 12:43:13	arpwatch: new station 999.888.777.666 00:50:56:bd:49:f7
16 октября 2025, 12:33:01	arpwatch: listening on vmtx3
16 октября 2025, 12:33:01	arpwatch: listening on vmtx1

Сеть: обнаружение устройств. Хосты

Записи не могут быть удалены, пока сервис работает

Имя	Интерфейс	MAC	IP	Дата	Статус	Комментарий
vmtx1	LAN	00:50:56:80:19:f7	999.888.777.666	16 октября 2025 г., 12:43	<input type="checkbox"/>	Не определено VMware, Inc.
vmtx1	LAN	00:50:56:80:41:a8	999.888.777.666	16 октября 2025 г., 12:43	<input type="checkbox"/>	Не определено VMware, Inc.
vmtx3	OPT1	00:50:56:80:63:30	99.8.77.66	16 октября 2025 г., 12:47	<input type="checkbox"/>	Не определено VMware, Inc.
vmtx3	OPT1	00:50:56:80:fd:9a	99.8.77.6	16 октября 2025 г., 12:47	<input type="checkbox"/>	Не определено VMware, Inc.

Контролируйте работу службы обнаружения устройств и упростите интеграцию данных в отчёты.
Логи службы теперь доступны прямо в веб-интерфейсе, а обнаруженные устройства можно экспортировать в .csv и .pdf для импорта в документы организации.

Уведомление об очистке журналов

Система: журналы. Журнал Syslog	
Дата	Сообщение
5 февраля 2026, 14:55:00	armaif: Пользователь "root" получил доступ к журналу "/var/log/core/system" (Система: Журналы: Журнал Syslog)
5 февраля 2026, 14:55:00	armaif: Пользователь "root" очистил журнал "/var/log/core/system" (Система: Журналы: Журнал Syslog)

Контролируйте попытки скрыть действия.
Теперь при очистке журнала действий пользователем автоматически создаётся запись с именем исполнителя, фиксируя само событие в том же журнале.

Ротация лог-файлов OpenVPN

Оптимизируйте загрузку жёстких дисков. Механизм ротации журнала OpenVPN был обновлён и позволяет эффективнее использовать хранилища аппаратных платформ.