

# INFOWATCH ARMA СТЕНА (NGFW)

отечественный межсетевой экран нового поколения для защиты корпоративных сетей



InfoWatch ARMA Стена K10000 ↑

InfoWatch ARMA Стена K1000 →



## импортозамещение

### Выбор в пользу InfoWatch ARMA Стена (NGFW)

- ☒ Отечественное ПО
- ☒ ПАК российского производства
- ☒ Соответствие требованиям производительности для корпоративного сегмента

## Успешный опыт в импортозамещении

Импортозамещение — не только про поиск технического аналога, но и про опыт взаимодействия с вендором. Мы понимаем важность сопровождения как на этапе внедрения, так и на протяжении жизненного цикла продукта. Команда InfoWatch ARMA готова обеспечить профессиональную поддержку и быстрое развитие продукта.



2/3 из 50 крупнейших компаний России — наши клиенты



4 000 клиентов из 20 отраслей в 26 странах



С 2003 года на рынке информационной безопасности

## InfoWatch ARMA Стена (NGFW): все основные возможности межсетевого экрана нового поколения, необходимые заказчикам

### ● Система обнаружения и предотвращения вторжений (COB), IPS / IDS

Собственная база сигнатур постоянно пополняется командой экспертов InfoWatch ARMA — позволяет обнаруживать попытки эксплуатации как классических, так и специфических уязвимостей. Возможно самостоятельно дополнять базу COB пользовательскими правилами для максимальной защиты компании

### ● Контроль приложений

Фильтрация протоколов на уровне L7 через регулярные выражения

### ● URL-фильтрация

Контроль доступа пользователей к веб-ресурсам

### ● Авторизация и аутентификация пользователей

Авторизация пользователей ActiveSync в домене по сертификату

Маршрутизация трафика на сервер MS Exchange

### ● Журналирование событий

Механизм логирования и отправки событий во внешние источники

### ● Управление приоритизацией трафика

Предоставление различным классам трафика разные приоритеты

### ● Шифрование TCP / IP

Поддержка механизмов Stunnel позволяет шифровать соединения посредством SSL и TLS

#### другие возможности

- VPN-подключения
- Совместимость с отечественными ОС
- Фильтрация по GeolP
- Совместимость с отечественным ПО
- Веб-прокси
- Объединение сетевых интерфейсов в виртуальный
- Интеграция с Active Directory
- Объединение сегментов (подсетей) в единую сеть

<sup>1</sup>NGFW — Next-generation firewall, англ. «межсетевой экран нового поколения»

# Полный перечень возможностей

## Межсетевой экран

- Фильтрация сетевого трафика с учётом параметров пакета на сетевом и транспортном уровнях
- Функции Stateful Firewall
- DMZ (демилитаризованная зона)
- Адрес-листы (именованные списки адресов)
- Соккрытие архитектуры и конфигурации защищаемой системы и трансляция адресов (NAT и PAT)
- Задание расписания срабатывания правил (*только UTC*)
- Фильтрация по GeoIP

## Система обнаружения вторжений

- Обнаружение и предотвращение компьютерных атак на сетевом и прикладном уровнях
- L7-фильтрация протоколов через рег. выражения
- Разработка пользовательских правил COV
- Блокирование запрещённых информационных потоков<sup>1</sup>
- Блокирование действий вредоносного ПО<sup>1</sup>

## Сетевые функции

- Работа в режиме прозрачного моста
- Поддержка статической маршрутизации
- Поддержка протоколов динамической маршрутизации: RIP, OSPFv2, OSPFv3 и BGPv4
- Virtual routing and forwarding (VRF)
- Маршрутизация на основе политик
- Прокси-сервер
- Безопасные зашифрованные соединения (Stunnel)
- Реверс-прокси Nginx (*только для ActiveSync*) и Noproxy
- Поддержка VLAN IEEE 802.1q
- DHCP-сервер и DHCP Relay
- Функции QoS (Traffic shaping)
- Зеркалирование трафика на отдельный порт
- DNS-клиент
- Кеширующий DNS-сервер
- Протоколы туннелирования GIF, GRE и ERSPAN
- Поддержка IPv4 и IPv6
- Поддержка объединения физических интерфейсов в логические — Ethernet channel и 802.3ad
- Просмотр таблицы активных соединений

## Мониторинг и события

- Экспорт событий по SYSLOG (интеграция с SIEM)
- Сбор и экспорт статистики NetFlow
- Мониторинг загрузки и состояния сетевых интерфейсов, CPU, памяти и программных модулей
- Журналирование событий: МЭ, VPN, системные, сервисные и события NAT, действия пользователей<sup>2</sup>
- Сервис для отправки данных во внешние системы мониторинга, совместимый с форматом Zabbix

## Управление

- Передача событий в Management Console (SYSLOG)
- Задание и синхронизация времени по протоколу NTP
- Экспорт и импорт конфигурации
- Планировщик задач (на основе сервиса Cron)
- Возможность офлайн-обновления образа системы
- Возможность офлайн-обновления сигнатур IDS / IPS
- Loop protection. Технологии STP
- Возможность сброса настроек

## Отказоустойчивость

- Функции отказоустойчивости, повышения надёжности и резервирования. Active backup, Active-Passive
- Поддержка протокола VRRP

## Защита доступа

- Обеспечение защищённого канала администрирования системы за счёт управления по протоколу SSH
- Аутентификация по различным базам: RADIUS-сервер, basic, ntlm-v2, kerberos
- Авторизация пользователей ActiveSync в домене по сертификату и маршрутизация трафика на сервер MS Exchange
- Блокировка после нескольких неудачных попыток входа

## VPN

- Возможность построения криптографического туннеля
- Site-to-site VPN
- Wireguard VPN
- IPsec / IKEv2
- VPN IPsec
- OpenVPN

<sup>1</sup>в соответствии с сигнатурами

<sup>2</sup>в виде логов служб

## Сертифицированные аппаратные платформы

### технические характеристики

	InfoWatch ARMA Стена K10000	InfoWatch ARMA Стена K1000
пропускная способность	до 10 Гбит/с	до 1 Гбит/с
корпус	19" 1U	19" 1U
процессор	2 × Intel Xeon Silver 4310 (12C / 24T)	Intel Xeon D-1537 (8C / 16T)
оперативная память	64 GB RAM DDR4 ECC Reg	32 GB RAM DDR4
накопители SSD	2 × 512 GB M.2 SSD NVMe / SATA	512 GB M.2 SSD SATA
сетевые порты	22 порта: 12 × RJ45, 8 × SFP и 2 × SFP+	16 портов: 8 × RJ45 и 8 × SFP
питание	RPSU резервируемый 1 + 1 800 W	RPSU резервируемый 1 + 1 300 W
разъёмы на панели	USB 3.0, USB 2.0, RJ-45 (COM), microHDMI	USB 3.0, USB 2.0, RJ-45 (COM), VGA
индикаторы на панели	кнопки — включение и перезапуск, индикаторы — активность сетевых портов, активность накопителей, состояние системы, POST-коды	кнопки — включение и перезапуск, индикаторы — активность сетевых портов, питание, состояние системы

## реальные показатели производительности

	InfoWatch ARMA Стена K10000	InfoWatch ARMA Стена K1000
Нагрузочное тестирование от InfoWatch ARMA	<p>Режим UTM. 1000 правил МЭ, 7200 правил IPS:</p> <ul style="list-style-type: none"><li>● EMIX-трафик = 7,6 Гбит/с</li><li>● SFR-трафик = 9 Гбит/с</li></ul> <p>Режим МЭ. 1000 правил МЭ:</p> <ul style="list-style-type: none"><li>● EMIX-трафик = 8,8 Гбит/с</li><li>● SFR-трафик = 9,54 Гбит/с</li></ul>	<p>Режим UTM. 1000 правил МЭ, 78000 правил IPS:</p> <ul style="list-style-type: none"><li>● EMIX-трафик = 297 Мбит/с</li><li>● SFR-трафик = 321 Мбит/с</li></ul> <p>Режим МЭ. 1000 правил МЭ:</p> <ul style="list-style-type: none"><li>● EMIX-трафик = 840 Мбит/с</li><li>● SFR-трафик = 972 Мбит/с</li></ul>
Независимое тестирование от «Инфосистемы Джет»	<p>Режим UTM. 200 правил МЭ, 55000 правил IPS:</p> <ul style="list-style-type: none"><li>● EMIX-трафик = 6,2 Гбит/с</li></ul>	

[ngfw.infowatch.ru](https://ngfw.infowatch.ru)

## Попробуйте InfoWatch ARMA Стена (NGFW) в деле

InfoWatch ARMA Стена (NGFW) — принципиально новая аппаратная платформа и архитектура, разработанные для корпоративных заказчиков с учётом необходимой функциональности, особенностей корпоративных протоколов и требований к производительности.