INFOWATCH

Sk Участник

INFOWATCH ARMA СТЕНА (NGFW) — ТЕХНИЧЕСКОЕ ОПИСАНИЕ

общие сведения | программные возможности | аппаратные спецификации | производительность и масштабируемость | сертификации | соответствие нормативным требованиям

infowatch.ru/ngfw

ОБЩИЕ СВЕДЕНИЯ

InfoWatch ARMA Стена (NGFW) — межсетевой экран нового поколения для защиты корпоративных и промышленных сетей. Объединяет в одном устройстве традиционный межсетевой экран, VPN, систему обнаружения и предотвращения вторжений (IPS / IDS), антивирус, управление пропускной способностью, фильтрацию URL и контроль поведения пользователей в сети.

КЛЮЧЕВЫЕ ВОЗМОЖНОСТИ

Система обнаружения и предотвращения вторжений (СОВ), IPS / IDS

Обнаруживает и блокирует вредоносное ПО, атаки и попытки эксплуатации уязвимостей ПЛК на сетевом и прикладном уровнях. Сигнатурные базы обновляются регулярно

Журналирование событий

Собирает логи и отправляет события во внешние источники

Контроль приложений

Фильтрует приложения по категориями, спискам, доменам и с помощью регулярных выражений

URL-фильтрация

Контролирует доступ к веб-ресурсам с расшифровкой SSL / TLS и подменой сертификата

VPN

Защищает информацию при объединении в единую сеть филиалов предприятия или при удалённом подключении

Антивирусная защита

Dr.Web обнаруживает вирусы, вредоносное ПО и нежелательные ресурсы в сетевом трафике

Управление приоритизацией трафика

Позволяет настроить различным классам трафика разные приоритеты

Межсетевое экранирование

Позволяет блокировать неавторизованные действия пользователей и запрещать недопустимые операции

Глубокая инспекция промышленных протоколов

Обнаруживает вторжения по специализированным промышленным протоколам благодаря глубокому разбору трафика до уровня команд

ПРОГРАММНЫЕ ВОЗМОЖНОСТИ

Межсетевой экран

- фильтрация сетевого трафика с учётом параметров пакета на сетевом и транспортном уровнях
- глубокая инспекция промышленных протоколов до уровня команд
- Stateful Firewall
- DMZ (демилитаризованная зона)
- адрес-листы (именованные списки адресов)
- сокрытие архитектуры и конфигурации защищаемой системы и трансляция адресов (NAT и PAT): DNAT, SNAT, статический NAT и реверс-NAT
- задание расписания срабатывания правил (только UTC)
- фильтрация по GeoIP
- блокировка редиректов и транзитного трафика
- конфигурирование Ethertype в правилах межсетевого экрана

Система обнаружения вторжений

- обнаружение и предотвращение компьютерных атак на сетевом и прикладном уровнях:
  - использование эксплойтов и уязвимостей сетевых приложений
  - предотвращение эксплуатации уязвимостей в протоколах
  - предотвращение сетевого сканирования
  - фильтрация трафика от скомпрометированных хостов и хостов, заражённых ВПО
- L7-фильтрация протоколов через регулярные выражения
- конфигуратор приложений App Control
- разработка пользовательских правил СОВ
- блокирование запрещённых информационных потоков*
- блокирование действий вредоносного ПО*
- предустановленная конфигурация СОВ
- блокировка протокола QUIC

Сетевые функции

- поддержка IPv4 и IPv6
- работа в режиме прозрачного моста
- поддержка протоколов динамической маршрутизации: RIP, OSPFv2, OSPFv3 и BGPv4
- Virtual Routing & Forwarding (VRF)
- прокси-сервер: кеширующий, реверс-, прозрачный (с подменой сертификата), ActiveSync
- расшифровка HTTPS-запросов с помощью SSL / TLS Bump
- безопасные зашифрованные соединения (Stunnel)
- реверс-прокси Nginx (только для ActiveSync) и Haproxy
- поддержка VLAN IEEE 802.1q
- DHCP-сервер и DHCP Relay
- функции QoS (Traffic Shaping)
- балансировка нагрузки на WAN-интерфейсах
- зеркалирование трафика на отдельный порт
- DNS-клиент, кеширующий DNS-сервер
- протоколы туннелирования GIF, GRE и ERSPAN

**в соответствии с сигнатурами*

- просмотр таблицы активных соединений
- поддержка объединения физических интерфейсов в логические — Ethernet channel и 802.3ad
- агрегирование каналов (LACP): 802.3ad, active-backup, broadcast, round-robin, transmit-load-balance, adaptive-load-balance и xor-hash
- ограничение скорости для подсети (CIDR)
- идентификация по LLDP

Мониторинг и события

- экспорт событий по SYSLOG (интеграция с SIEM)
- сбор и экспорт статистики NetFlow — в том числе sFlow (версии 5, 9 и 10 / IPFIX)
- детализированный просмотр событий межсетевого экрана
- журналирование событий: МЭ, VPN, системные и сервисные события, NAT, действия пользователей, контроль целостности, кеширующий прокси*
- сервис для отправки данных во внешние системы мониторинга, совместимый с форматом Zabbix

Диагностика

- мониторинг загрузки и состояния сетевых интерфейсов, CPU, памяти и программных модулей
- мониторинг параметров аппаратной платформы и блоков питания
- мониторинг трафика на физических интерфейсах
- сервис проверки состояния интерфейсов (резервных каналов связи)
- отображение системных и пользовательских процессов

Управление

- передача событий в InfoWatch ARMA Management Console (SYSLOG)
- отображение статуса кластера в веб-интерфейсе
- задание и синхронизация времени по протоколу NTP
- система управления конфигурациями — сравнение, восстановление, импорт и экспорт
- планировщик задач (на основе сервиса Cron)
- возможность офлайн-обновления образа системы и сигнатур IDS / IPS
- Loop Protection — технологии STP, RSTP и MSTP

Отказоустойчивость

- функции отказоустойчивости, повышения надёжности и резервирования — Active Backup и Active-Passive
- синхронизация учётных записей в кластере
- поддержка протокола VRRP (V2 и V3)

Защита доступа и безопасность

- антивирусная защита — Dr. Web
- обеспечение защищённого канала администрирования системы за счёт управления по протоколу SSH
- аутентификация с использованием RADIUS-сервера, basic, ntlm-v2 и kerberos
- авторизация пользователей ActiveSync в домене по сертификату
- маршрутизация трафика на сервер MS Exchange
- блокировка после нескольких неудачных попыток входа
- шифрование конфигурационного файла с поддержкой протокола SCP
- контроль целостности конфигурации МСЭ, контроль пользовательских сессий

VPN

- Site-to-Site VPN

**в виде логов служб*

АППАРАТНЫЕ СПЕЦИФИКАЦИИ

InfoWatch ARMA Стена K10000

intel 2 × Xeon Silver 4310 | 12 ядер | 24 потока | порты до 10 Гбит/с

64 GB RAM DDR4 ECC Reg

2 × 512 GB M.2 SSD SATA / NVMe

в стойке | 19” 1U

резервируемый RPSU 1 + 1 800 W

22 порта | 12 × RJ45 | 8 × SFP

2 × SFP+ | 2 × USB | microHDMI

RJ-45 (COM) | 2 × 220В

кнопки

включение | перезапуск

индикаторы

активность сетевых портов

активность накопителей

состояние системы

POST-коды

производительность

- EMIX + МЭ + IPS: 6,3 Гбит/сек
  10 000 правил IPS + 1000 правил МЭ
- общая пропускная способность UDP на кадрах 64В: 14 735 632 PPS
  без IPS + 1 правило МЭ
- макс. число новых соединений в секунду: 212 500 CPS
- макс. число конкурентных соединений: 10 625 000 CC
- пропускная способность HTTP 64KB: 7,4 Гбит/сек
  10 000 правил IPS + 1000 правил МЭ

Независимое тестирование от «Инфосистем Джет»

55 000 правил IPS + 200 правил МЭ: 6,2 Гбит/сек

InfoWatch ARMA Стена K1000

intel Xeon D-1537 | 8 ядер | 16 потоков | порты до 1 Гбит/с

32 GB RAM DDR4

512 GB M.2 SSD SATA

в стойке | 19” 1U

резервируемый RPSU 1 + 1 300 W

16 портов | 8 × RJ45 | 8 × SFP

2 × USB | RJ-45 (COM)

VGA | 2 × 220В

кнопки

включение | перезапуск

индикаторы

активность сетевых портов

питание

состояние системы

производительность

- EMIX + МЭ + IPS: 495 Мбит/сек
  10 000 правил IPS + 1000 правил МЭ
- общая пропускная способность UDP на кадрах 64В: 326 247 PPS
  без IPS + 1 правило МЭ
- макс. число новых соединений в секунду: 41 500 CPS
- макс. число конкурентных соединений: 495 000 CC
- пропускная способность HTTP 64KB: 578 Мбит/сек
  10 000 правил IPS + 1000 правил МЭ

InfoWatch ARMA Стена K100

intel Atom X6425E | 4 ядра | 4 потока | порты до 1 Гбит/с

16 GB RAM DDR4

256 GB M.2 SSD SATA

настольный

19” (крепление в комплекте)

внешний резервируемый БП

8 портов | 8 × RJ45 | 2 × HDMI

2 × USB | RJ-45 (COM) | 2 × 12В

кнопки

включение | перезапуск

индикаторы

активность сетевых портов

активность накопителей

питание

производительность

- EMIX + МЭ + IPS: 388 Мбит/сек
  10 000 правил IPS + 1000 правил МЭ
- общая пропускная способность UDP на кадрах 64В: 454 857 PPS
  без IPS + 1 правило МЭ
- макс. число новых соединений в секунду: 50 250 CPS
- макс. число конкурентных соединений: 480 000 CC
- пропускная способность HTTP 64KB: 541 Мбит/сек
  10 000 правил IPS + 1000 правил МЭ

СЕРТИФИКАЦИИ

1 Сертификат ФСТЭК России №4953:

Профиль защиты межсетевых экранов типа Б четвёртого класса защиты

ИТ.МЭ.Б4.ПЗ

Профиль защиты межсетевых экранов типа Д четвёртого класса защиты

ИТ.МЭ.Д4.ПЗ

Профиль защиты систем обнаружения вторжений уровня сети четвёртого класса защиты

ИТ.СОВ.С4.ПЗ

2 Реестр ПО и ПАК Минцифры России № 23568

3 Реестр отечественной продукции Минпромторга России:

Аппаратная платформа InfoWatch ARMA K10000

на базе «Рубеж-Т»

Запись в реестре «Сетевое устройство «Рубеж-Т», КРПЕ.466539.009»

Аппаратная платформа InfoWatch ARMA K1000

на базе «Рубеж-С»

Запись в реестре «Сетевое устройство «Рубеж-С», КРПЕ.466539.008»

Аппаратная платформа InfoWatch ARMA K100

на базе «Рубеж-Н1»

Запись в реестре «Сетевое устройство «Рубеж-Н1», КРПЕ.466539.014-01»

СООТВЕТСТВИЕ НОРМАТИВАМ

Сертификаты соответствия требованиям технического регламента ЕАЭС (технического регламента Таможенного союза) на аппаратные платформы:

ТР ТС 004/2011 «О безопасности низковольтного оборудования»

ТР ТС 020/2011 «Электромагнитная совместимость технических средств»

Попробуйте InfoWatch ARMA Стена (NGFW) в деле

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

sales@infowatch.ru
+7 495 22 900 22

infowatch.ru/ngfw

/InfoWatchOut

/InfoWatch