INFOWATCH ARMA NGFW

Межсетевой экран нового поколения для защиты корпоративных сетей

Рады сообщить о выходе ранней версии ARMA NGFW и приглашаем принять участие в пилотном тестировании продукта. Это возможность оценить функциональность и внести вклад в её развитие.

возможности ранней версии

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)
- Сокрытие архитектуры и конфигурации защищаемой системы и трансляция адресов (NAT и PAT)
- Задание расписания срабатывания правил — *только UTC*

Система обнаружения вторжений

- Обнаружение и предотвращение компьютерных атак на сетевом и прикладном уровнях
- L7-фильтрация протоколов через регулярные выражения
- Возможность разработки пользовательских правил СОВ
- Блокирование запрещённых информационных потоков
- Блокирование действий вредоносного ПО

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 (Haproxy)
- Реверс-прокси (Nginx) — *только для ActiveSync*
- Поддержка VLAN IEEE 802.1q
- DHCP-сервер и DHCP Relay
- Функции QoS (Traffic shaping)
- Зеркалирование трафика с выбранного порта на отдельный
- DNS-клиент
- Кеширующий DNS-сервер
- Поддержка протоколов 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 протоколу SYSLOG (интеграция с SIEM)
- Сбор и экспорт статистики NetFlow
- Мониторинг загрузки и состояния сетевых интерфейсов, CPU, памяти и программных модулей
- Журналы МЭ
- Журналы VPN
- Журналы системных событий
- Журналы действий пользователей
- Журналы событий безопасности
- Журналы событий NAT
- Журналы сервисных событий

Управление

- Передача событий в ARMA Management Console — *Syslog*
- Задание и синхронизация времени по протоколу NTP
- Экспорт и импорт конфигурации
- Планировщик задач (на основе сервиса Cron)
- Офлайн-обновление ARMA Industrial Firewall через загрузку и установку файла
- Офлайн-обновление правил Suricata и сигнатур 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 — *без ролевого доступа*
- 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 пяти попыток неудачного входа

VPN

- Возможность построения криптографического тоннеля
- Site-to-site VPN
- Wireguard VPN
- Ikev2
- VPN IPsec
- OpenVPN