ФАКТОР·ТС

DIONIS-SMP

ЕДИНЫЙ ЦЕНТР УПРАВЛЕНИЯ И МОНИТОРИНГА СЕТЬЮ УСТРОЙСТВ DIONIS DPS

МОСКВА 2021

Портал управления Dionis-SMP предназначен для централизованного управления межсетевыми экранами (криптомаршрутизаторами) Dionis DPS.

Dionis DPS – линейка криптомаршрутизаторов, обладающих функциями МСЭ, СОВ, VPN.

Основные возможности Dionis-SMP

- Мониторинг состояния и настройка интерфейсов
- Настройка маршрутизации (в т.ч. динамической, на основе политик и доступности узлов сети)
- Управление фильтрацией пакетов на основе различных критериев
- Настройка трансляции адресов (в т.ч. с контролем состояния сессий)
- Настройка защищенных криптографических соединений
- Мониторинг системы обнаружения вторжений
- Управление другими параметрами работы Dionis DPS

Кроме того, портал управления Dionis-SMP предоставляет возможность наглядного графического представления текущего состояния событий в сети Dionis DPS, позволяя администратору оперативно реагировать на возникающие проблемы и проводить детальный анализ текущей ситуации. Также имеется возможность получения и анализа событий в сети, полученных и от других сетевых устройств по протоколам syslog, SNMP, Netflow, что позволяет использовать портал управления Dionis-SMP как централизованную систему мониторинга состояния сети и управления событиями информационной безопасности.

Централизованное управление и мониторинг большой сети устройств Dionis DPS значительно упрощает процедуры конфигурирования и обнаружения проблем в работе сети.

Использование Dionis-SMP значительно снижает временные затраты в управлении инфраструктурой сетевой безопасности, и как следствие — совокупную стоимость владения системы, увеличивает скорость реагирования и устранения последствий инцидентов, позволяет контролировать административный доступ и упрощать внедрение политик, используя ролевое администрирование. Ролевое администрирование позволяет устанавливать определенные пользовательские привилегии для управляемых доменов путем объединения устройств и агентов Dionis DPS в независимые управляемые домены.

Благодаря локальному хранению контента обновлений безопасности минимизируется время обработки запросов и увеличивается общая защита сети.

Dionis-SMP объединяет в себе 3 подсистемы:

1. подсистема управления сетью (настройка и управление сетевого оборудования (как Dionis DPS, так и сторонними), управление конфигурациями устройств, отображение топологии сети, устранение неисправностей, получение и обработка логов);
2. подсистема мониторинга (мониторинг сетевого оборудования (SNMP) и сетевого трафика(Netflow), мониторинг самого Dionis-SMP (ресурсы хоста, сервисы, БД), уведомления о неисправностях, отчеты);
3. SIEM (мониторинг ИБ, отображение событий ИБ, аналитика, отчеты, уведомления о критичных событиях, корреляция событий).

Функциональные возможности Dionis-SMP

Мониторинг (SNMP, Netflow, событий ИБ)

— Отображение доступности сетевых устройств в реальном времени и статистика за предыдущие периоды.
— Отображение статуса узлов на топологии сети.
— Получение и отображение SNMP traps.
— Отображение загрузки интерфейсов узлов.
— Отображение загрузки памяти, процессора, дисковой подсистемы узлов и самого Dionis-SMP.
— Отображение статистики по трафику в сети.
— Отображение атак в виде списка с возможностью фильтрации.
— Отображение атак в виде графика с возможностью фильтрации.
— Вывод детальной информации по атаке (атакующий узел, атакуемый узел, CVE, pcap).
— Формирование уведомление администратора об атаках с заданными критериями.
— Формирование сводного дашборда мониторинга, его настройка.
— Возможность построения собственных дашбордов.
— Формирование оповещений по пороговым значениям на графиках.
— Формирование оповещений о недоступности узлов.
— Формирование оповещений о DoS-атаках.
— Отображение возможных реакций на задание различных реакций на различные типы событий и срабатывание правил корреляции.
— Отображение и редактирование списка правил корреляции.

Мониторинг (SNMP, Netflow, событий ИБ)

— Формирование отчета о доступности сетевого устройства за период, график и проценты.
— Формирование отчета со списком и графиком атак за период.
— Формирование отчета со статистикой атак за период с различными критериями.
— Формирование отчета с наиболее популярными категориями угроз.
— Формирование отчета с типами инцидентов.
— Формирование отчета с наиболее популярными целями атак.
— Формирование отчета с наиболее популярными категориями угроз.
— Поиск событий с помощью фильтров и группировка событий в журнале средства обнаружения вторжений на различные типы событий и срабатывание правил корреляции.

Управление устройствами Dionis DPS

Общие функции

— Добавление/изменение/удаление узла, настройки доступа и получаемых логов с узла.
— Отображение списка узлов, группировка узлов.
— Экспорт/импорт списка узлов.
— Включение и выключение СОВ(IPS/IDS) на Dionis DPS
— Загрузка правил СОВ и выгрузка (получение информации о загруженных на узел правилах).
— Настройка правил СОВ, ввод пользовательских правил СОВ.
— Настройки приоритетов правил СОВ.
— Доступ к журналам работы СОВ.
— Возможность подключиться к любому узлу по SSH.
— Ролевое управление доступом к функциям системы.

Управление списками доступа (ACL, NAT)

— Отображение для каждого узла созданных списков ACL, NAT.
— Создание и редактирование списков, контроль синтаксиса.
— Отображение всех интерфейсов узла.
— Сканирование/проверка открытых адресов/портов.
— Управление сетевыми объектами и группами сетевых объектов.
— Управление ACL при помощи политик с использованием сетевых объектов или групп сетевых объектов.

Туннели

— Отображение туннеля или туннельных интерфейсов парой (парой узлов) + связанные маршруты.
— Создание туннелей типа Ditun.
— Анализ и добавление конфигурации туннелей на основе полученной информации из конфигурации с возможностью редактирования.
— Отображения счетчика пакетов, объема переданного трафика.
— Изменение настроек (и ключей) в паре и индивидуально.
— Включение и выключение туннелей индивидуально.
— Отображение всех интерфейсов и маршрутов узла.
— Отображение состояния туннелей (keepalive).
— Замена номера серии для всех туннелей узлов.

Управление устройствами Dionis DPS

Менеджер конфигураций

— Отображение списка конфигураций по списку узлов с группировкой узлов.
— Отображение последней загруженной конфигурации узла.
— Хранение конфигураций узлов (истории изменений конфигураций).
— Редактирование конфигурации узлов.
— Получение конфигураций по расписанию для каждого узла.
— Сравнение двух конфигураций в истории одного узла и между двумя узлами.
— Отображение изменений при сравнении конфигураций узлов.
— Формирование уведомления о нахождении различий полученной конфигурации с эталонной конфигурацией.
— Отправка, применение конфигурации startup-config на узле с перезагрузкой.
— Безопасное применение конфигурации с автоматическим откатом при проблемах.

Скрипты

— Отображение и редактирование переменных и шаблонов переменных по списку узлов.
— Отображение списка скриптов.
— Выполнение скриптов на устройстве или группе устройств.

Политики

— Задание сетевых объектов, группы сетевых объектов, сервисов.
— Формирование политик с использованием переменных, шаблонов переменных, сетевых объектов, группы сетевых объектов, сервисов.
— Применение созданных политик на узлах.

Топология сети

— Отображение результатов сканирования сети на схеме сети.
— Отображение статуса устройства на схеме сети.
— Возможность выполнить скрипт на устройстве на схеме сети.
— Редактирование схемы сети.
— Объединение нескольких схем сети в одну.

Управление устройствами Dionis DPS

Журналы

— Централизованный сбор журналов (syslog) с узлов.
— Долговременное хранение журналов.
— Список журналов для получения.
— Задание периода хранения журналов.
— Поиск и фильтрация по журналам.
— Создание правил корреляции по ключевым словам, найденным в журналах.

Dionis SMP функционирует под управлением ОС Astra Linux 1.5, 1.6 и Debian Linux 9.8.

Имеется возможность развертывания и функционирования в системе виртуализации как virtual appliance, а также возможность развертывания и функционирования в виде Docker-контейнеров.

Минимальной областью действия является локальная сеть, развернутая на Dionis DPS (рис. 1). Dionis DPS подключаются к Dionis-SMP, далее с помощью него проводится мониторинг и управление всеми параметрами работы Dionis DPS, обнаружение вторжений и сбор информации по работе сети. В системе Dionis-SMP есть возможность горизонтального масштабирования и объединения комплексов в иерархию с передачей определенных событий на вышестоящие уровни иерархии и передачей конфигураций и правил обнаружения вторжений на нижележащие правила иерархии, что позволяет строить системы управления информационной безопасностью произвольного масштаба.

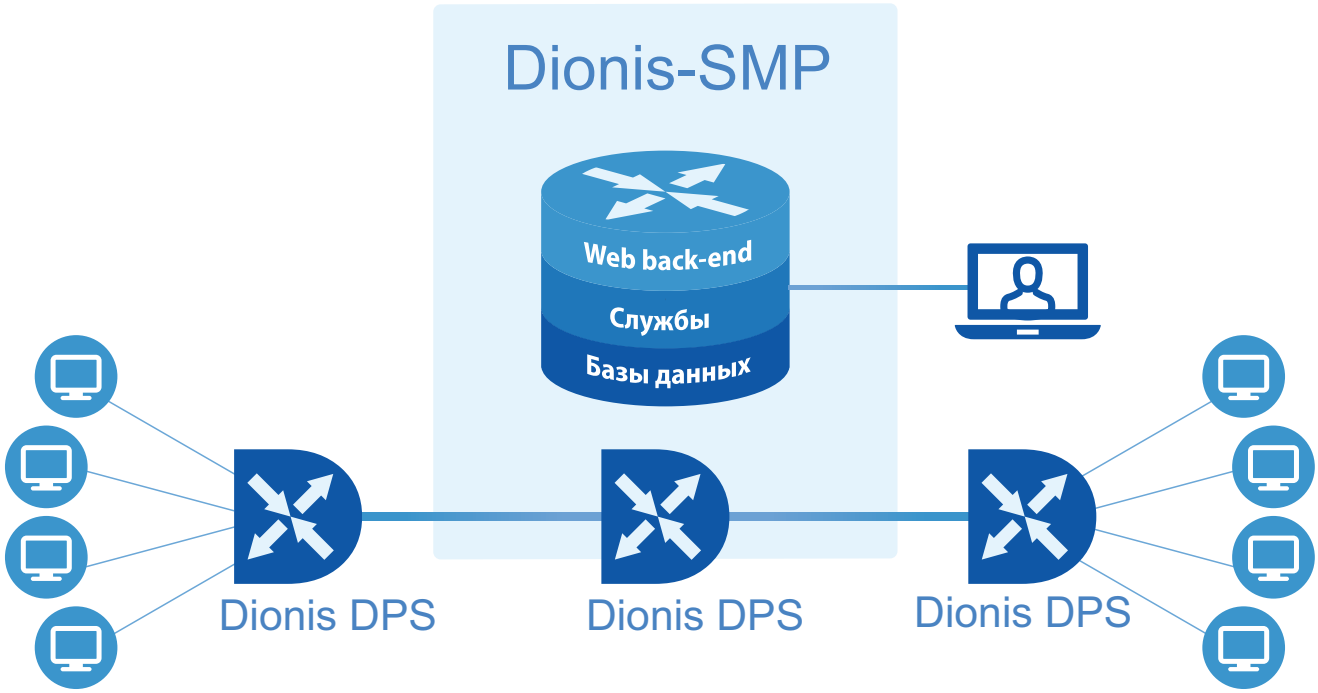

Рисунок 1. Пример развертывания Dionis-SMP

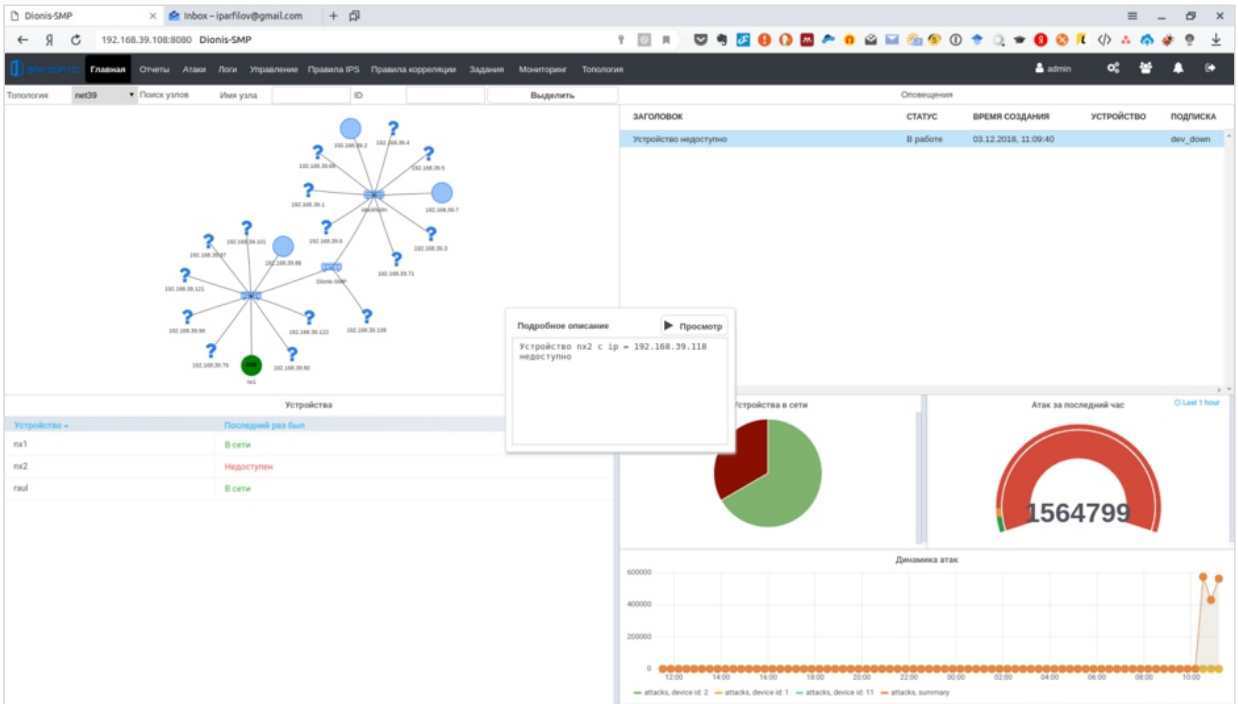

Рисунок 2. Главное окно Dionis-SMP

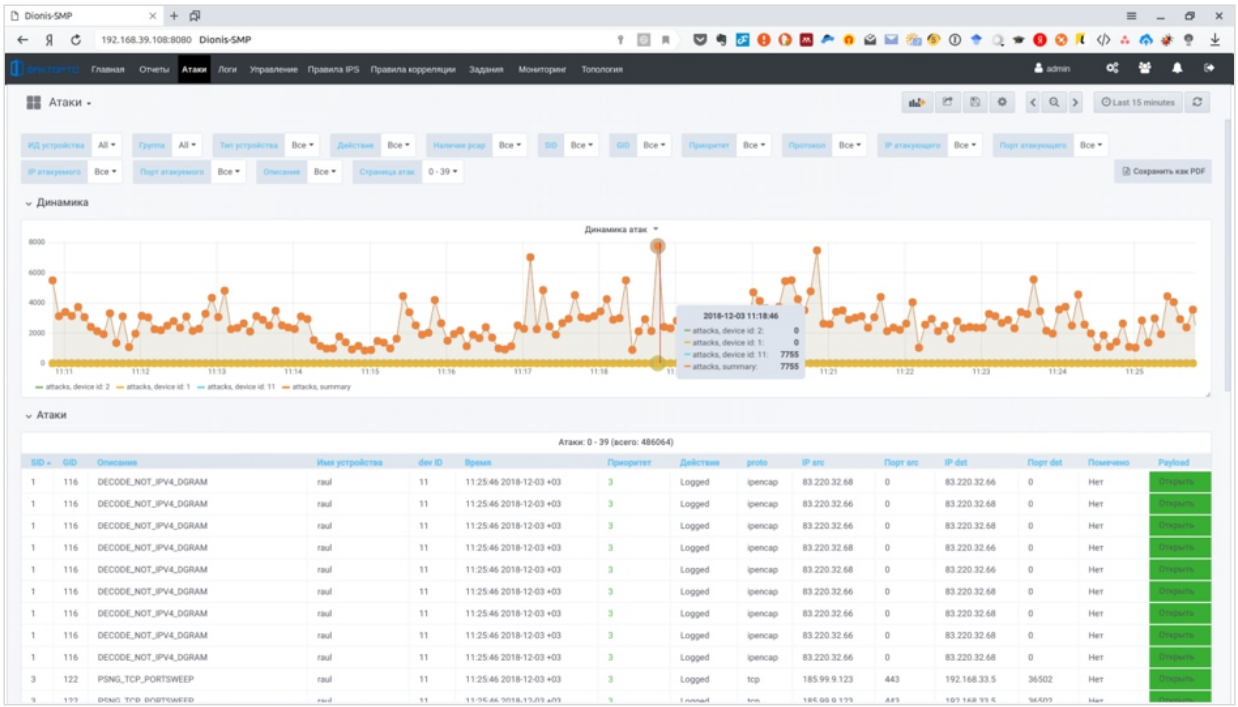

Рисунок 3. Главное окно Dionis-SMP
(статистика по событиям информационной безопасности)

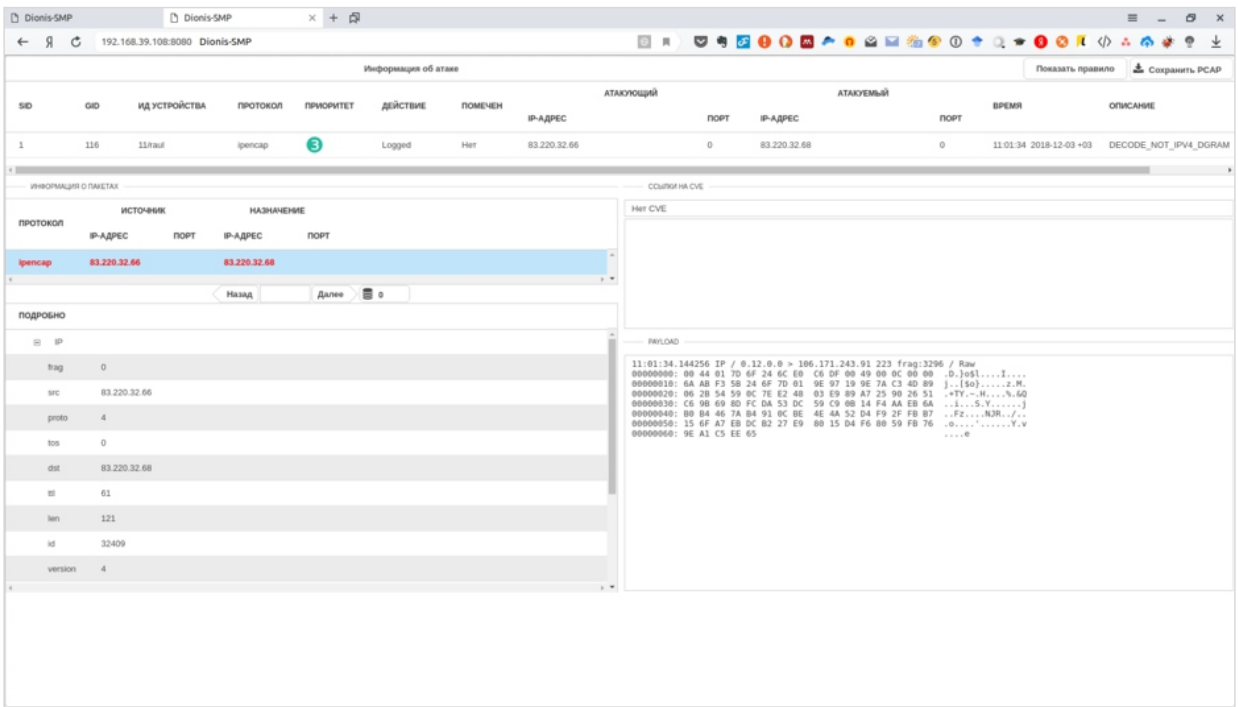

Рисунок 4. Подробная информация по компьютерным атакам

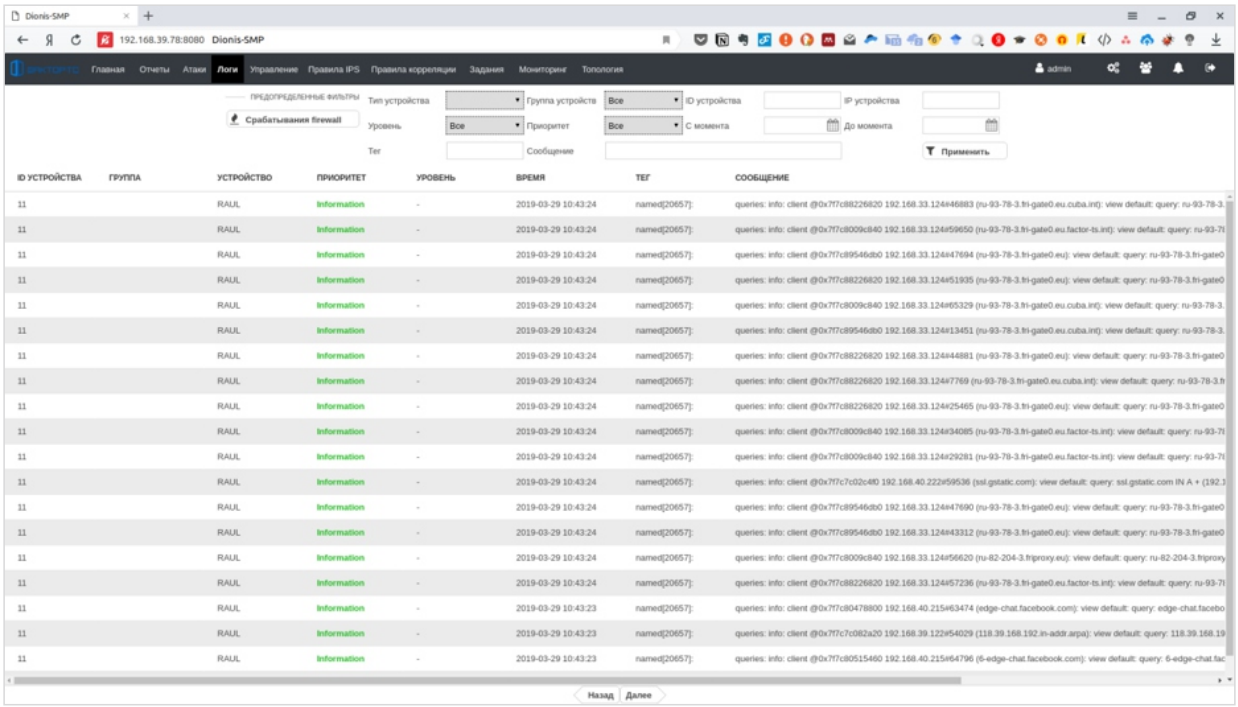

Рисунок 5. Централизованное управление журналами событий различных систем защиты информации

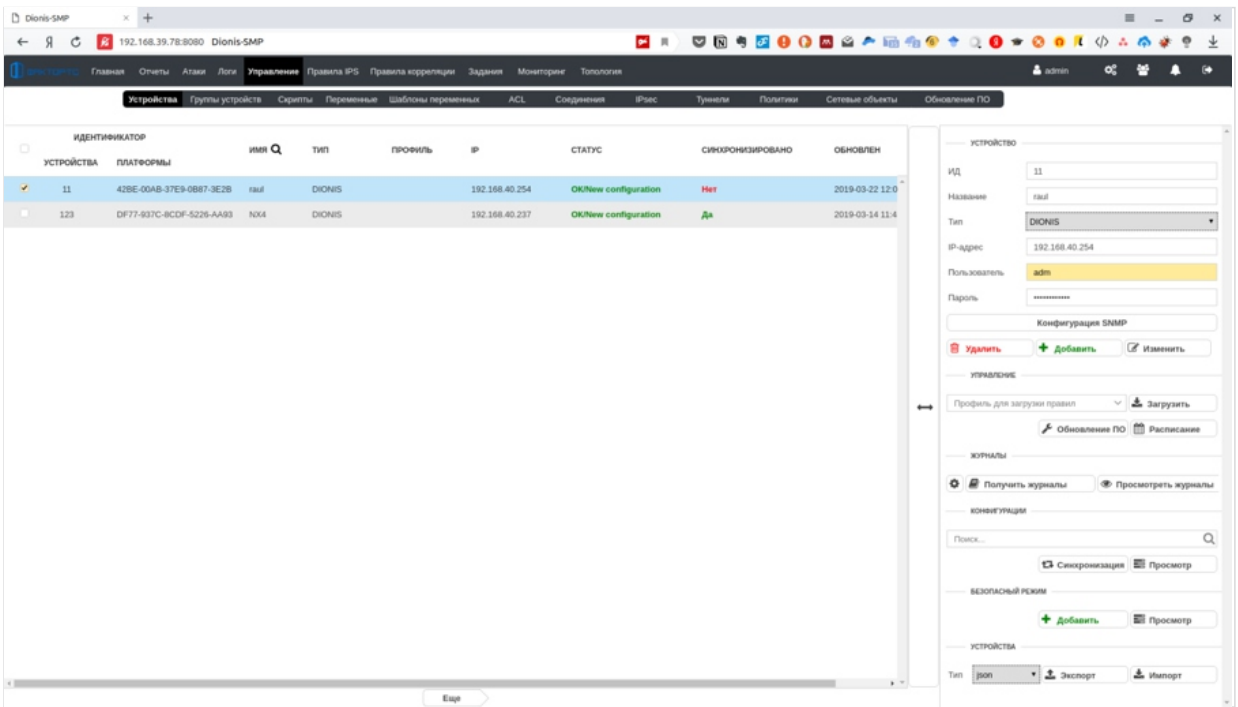

Рисунок 6. Централизованное управление сетью на базе Dionis DPS

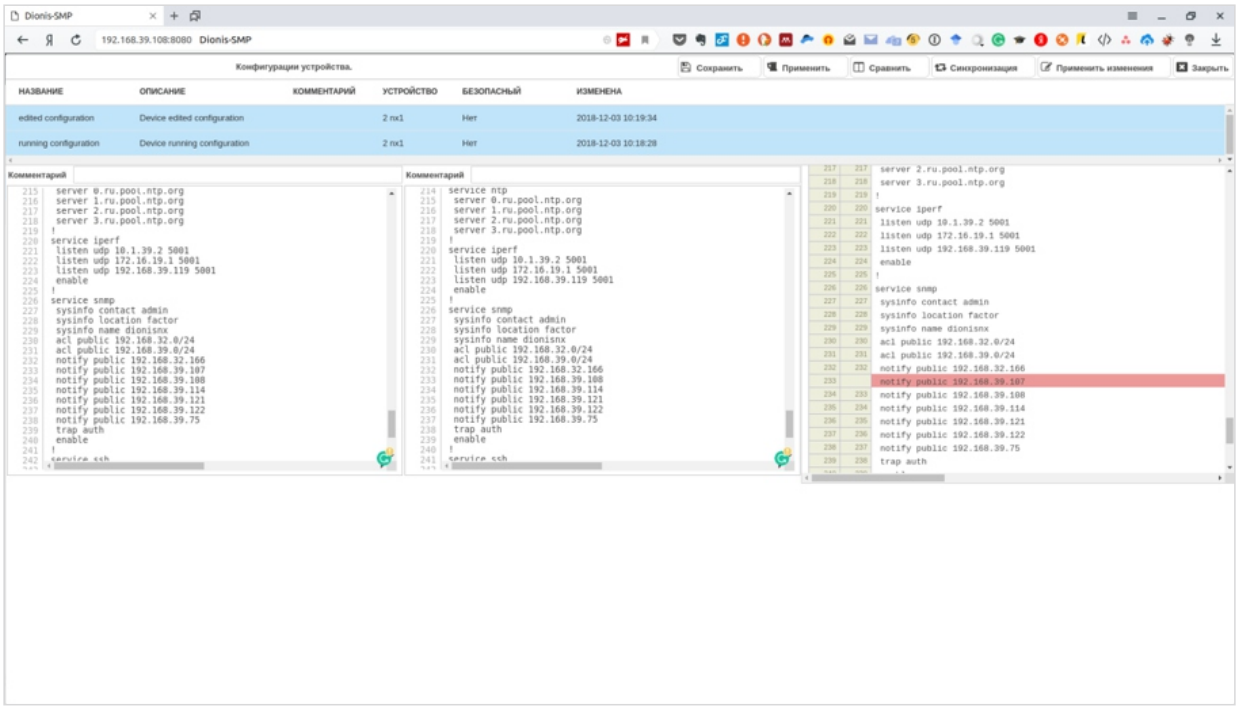

Рисунок 7. Сравнение полученных конфигураций Dionis DPS

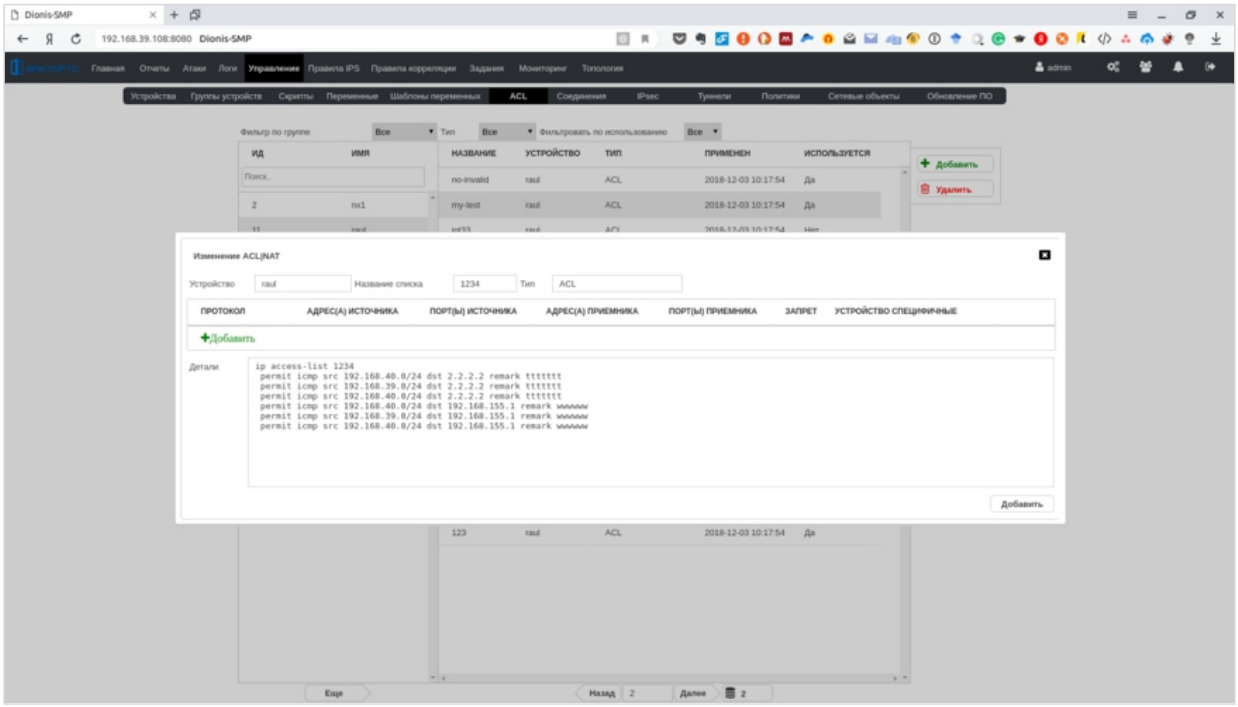

Рисунок 8. Настройка правил межсетевого экрана Dionis DPS

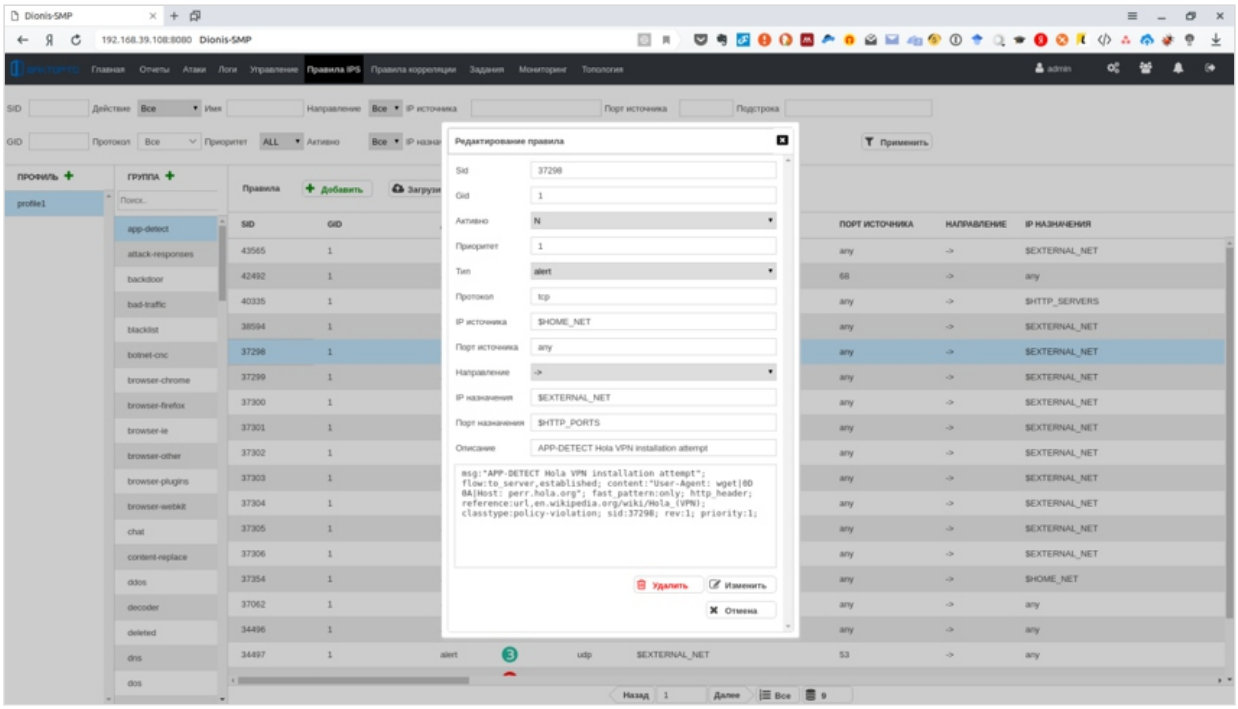

Рисунок 9. Настройка правил системы обнаружения вторжений Dionis DPS

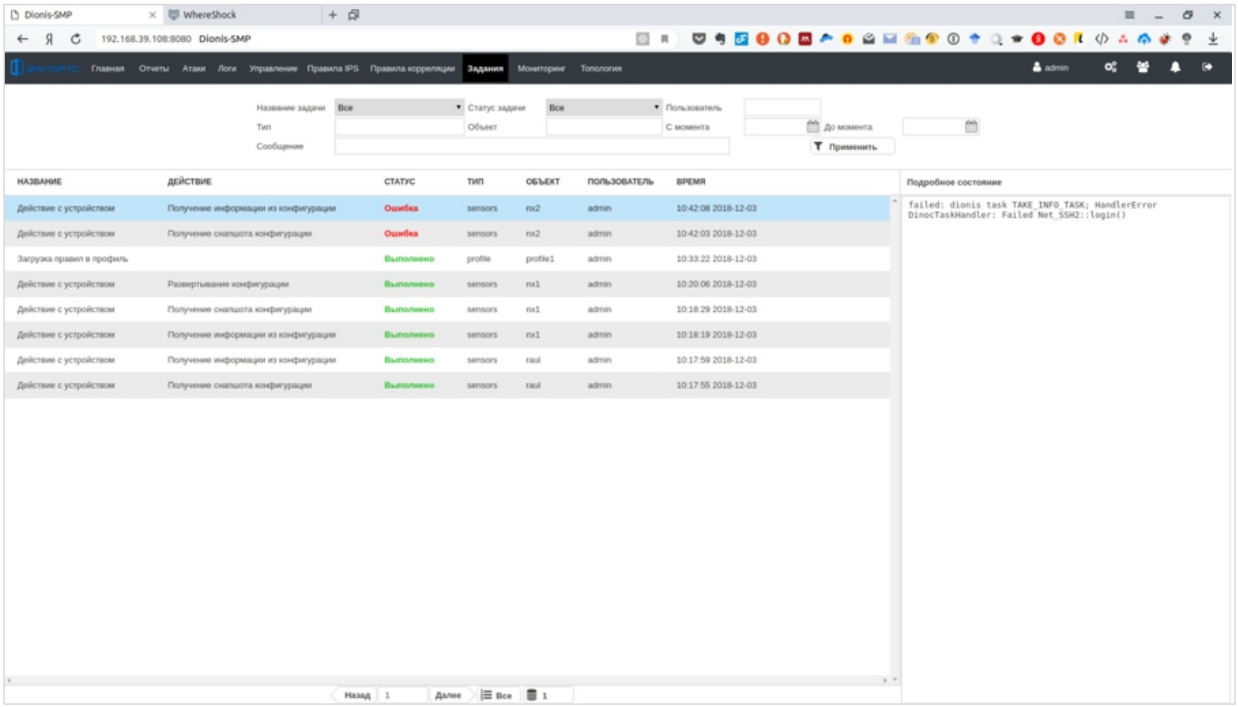

Рисунок 10. Журнал событий в системе Dionis-SMP

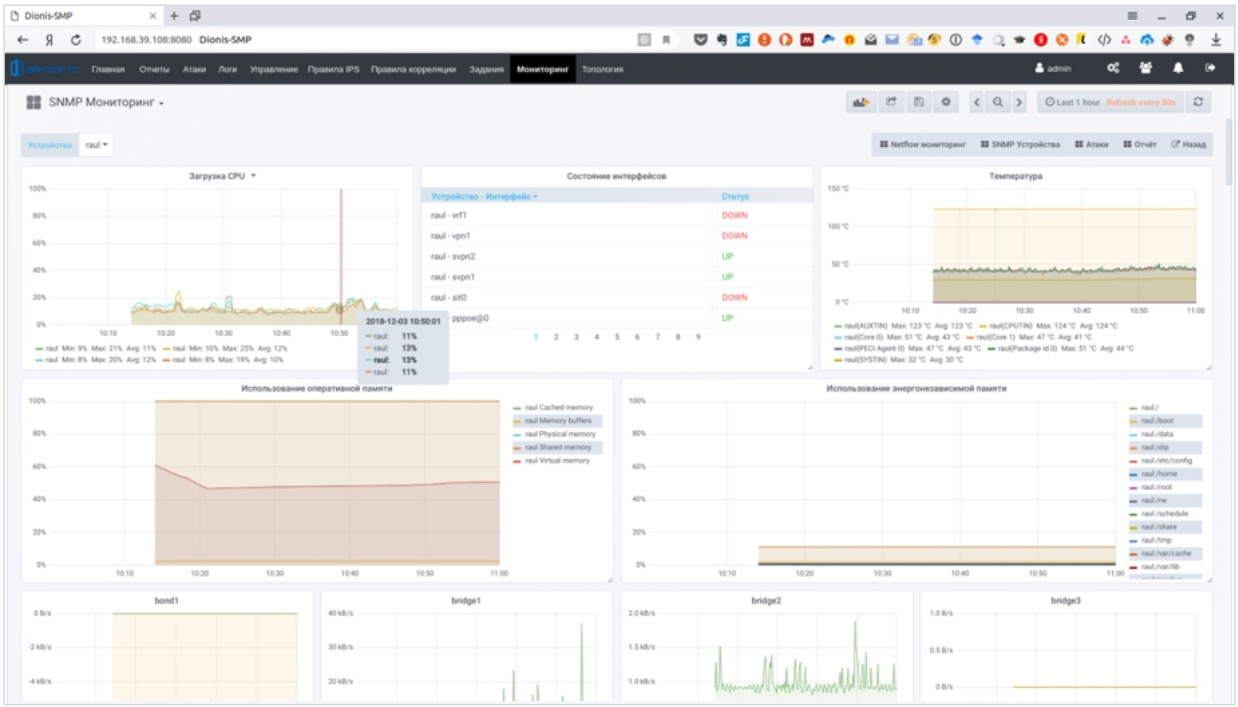

Рисунок 11. Мониторинг состояния устройств в Dionis-SMP

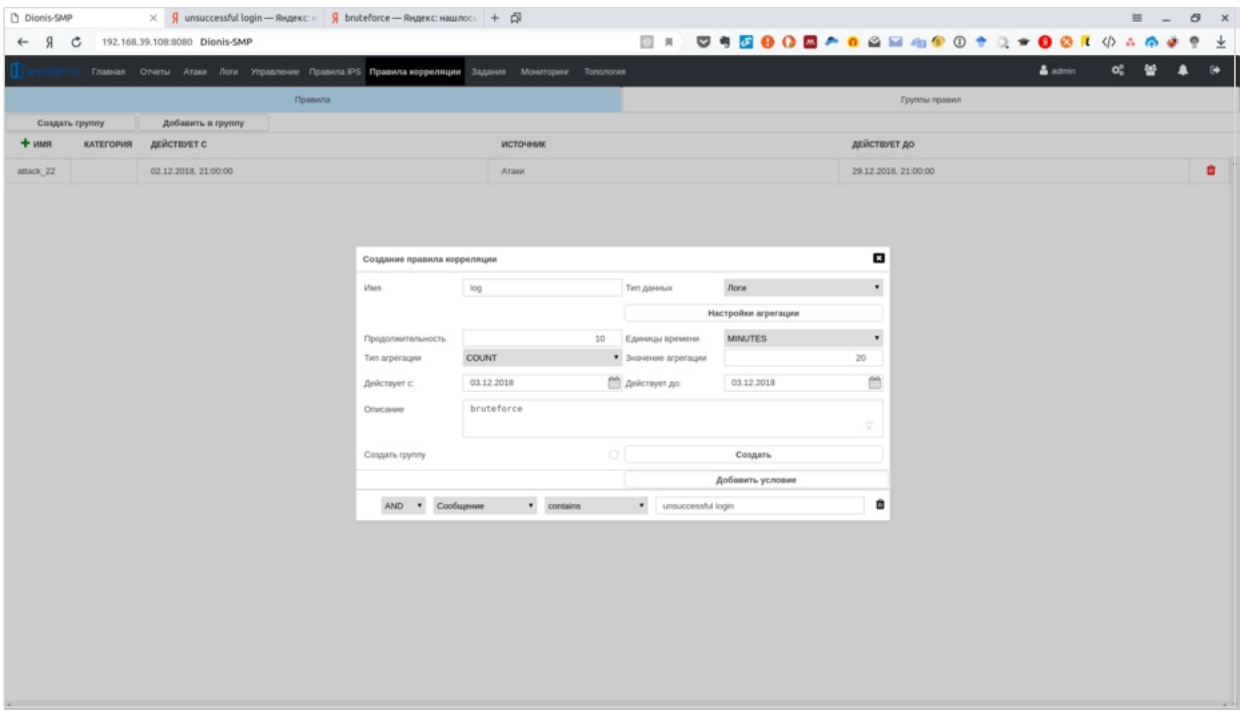

Рисунок 12. Настройка правил корреляции и оповещений

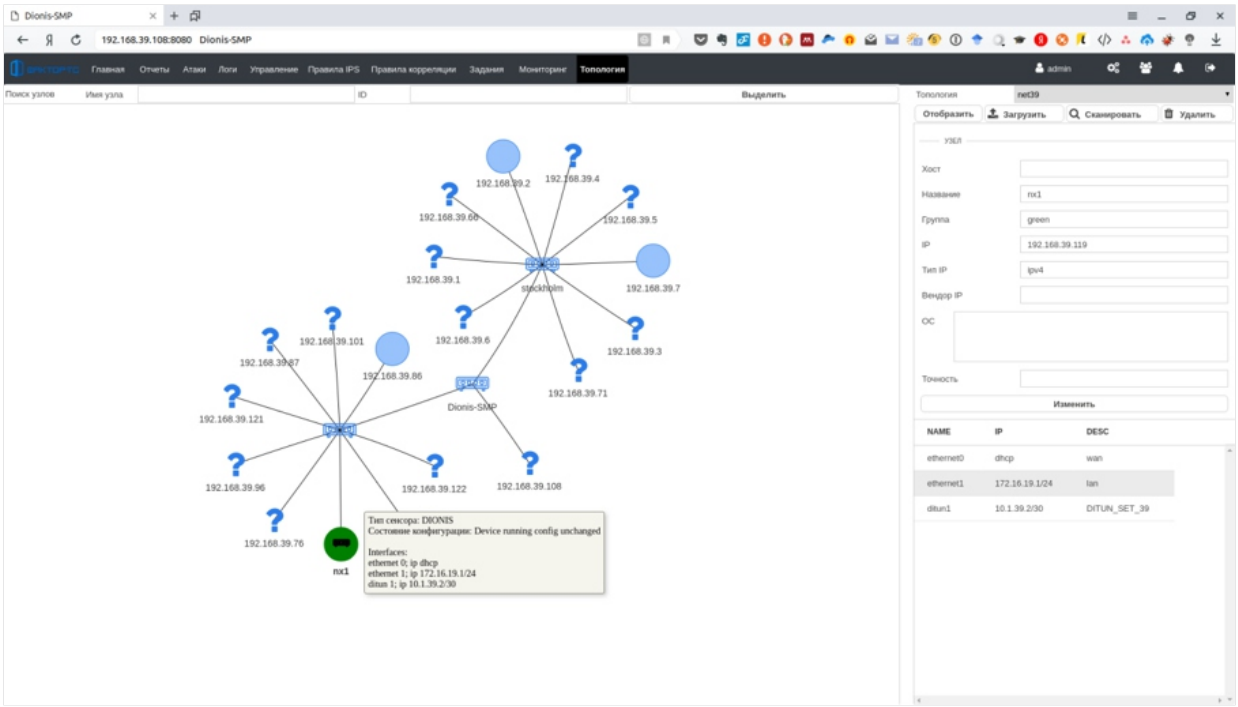

Рисунок 13. Топология сети

Москва, 1-й Магистральный пр-д,
дом 11, строение 1

dps.factor-ts.ru
sales@factor-ts.ru
+7 (495) 644 31 30