Купол

Купол.Управление

Единый мультивендорный центр аналитики
и управления сетевыми устройствами, имеющий
функции создания и применения политик
безопасности

Купол

Основные проблемы систем централизованного управления

Оптимизация политик

Как эффективно анализировать и оптимизировать политики безопасности?

Управление политиками

Как централизованно управлять правилами на МЭ разных вендоров?

Мониторинг

Как контролировать состояние подключенных устройств?

Контроль

Как контролировать изменения конфигураций устройств?

Мультивендорная реализация

Как интегрировать решения разных вендоров МЭ в систему управления?

Безопасность

Как обеспечить необходимые уровень Idоступов и сетевой безопасности компании?

Совместимость

Как интегрировать продукт в существующую инфраструктуру?

Ограничение прав

Как ограничить права доступа пользователей к устройствам?

Купол

Купол.Управление

Единый мультивендорный центр контроля, управления и оптимизации работы межсетевых экранов, UTM, NGFW

Ценность для клиента

+ Ускорение и унификация настройки из единого интерфейса политик МЭ всех вендоров устройств, установленных в инфраструктуре компании
+ Видимость всех устройств МЭ в сети компании и своевременное нахождение неисправных
+ Быстрый ввод в эксплуатацию новых сегментов сети с помощью клонирования конфигураций на одно или несколько устройств
+ Полная видимость изменений политик на устройствах и возможность быстро найти устройство, политики которого нарушили какие-либо бизнес-процессы компании
+ Оптимально настроенные политики безопасности во всей инфраструктуре компании и отсутствие политик, снижающих пропускную способность сети компании и ее защищенность

Функции

Мониторинг состояния всех установленных МЭ

Подключение и мониторинг состояния доступности подключенных устройств МЭ: UserGate, CheckPoint, Cisco ASA, Fortigate и др.

Управление конфигурациями

Автобэкапирование конфигураций подключенных устройств, их клонирование на другие устройства, сравнение версий между собой и анализ

Интеграция с SIEM / SOAR

Отправка журналов событий продукта Купол.Управление в сторонние системы по протоколу Syslog

Управление политиками безопасности

Централизованный контроль и управление политиками / правилами МЭ вендоров: UserGate, CheckPoint, Cisco ASA и др.

Оптимизация правил на всех устройствах

Выявление аномалий в правилах МЭ: избыточных, дублирующихся, теневых и других. Рекомендации по их оптимизации

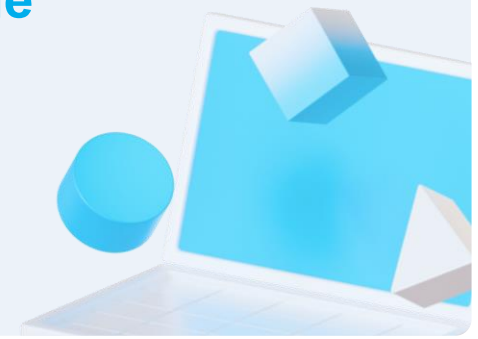
Администрирование

Предоставление прав доступа в систему локальным пользователям и из Active Directory / Astra Linux Directory. Управление парольной политикой. Журнал событий

Купол

Интеграция средства защиты информации

Купол.Управление



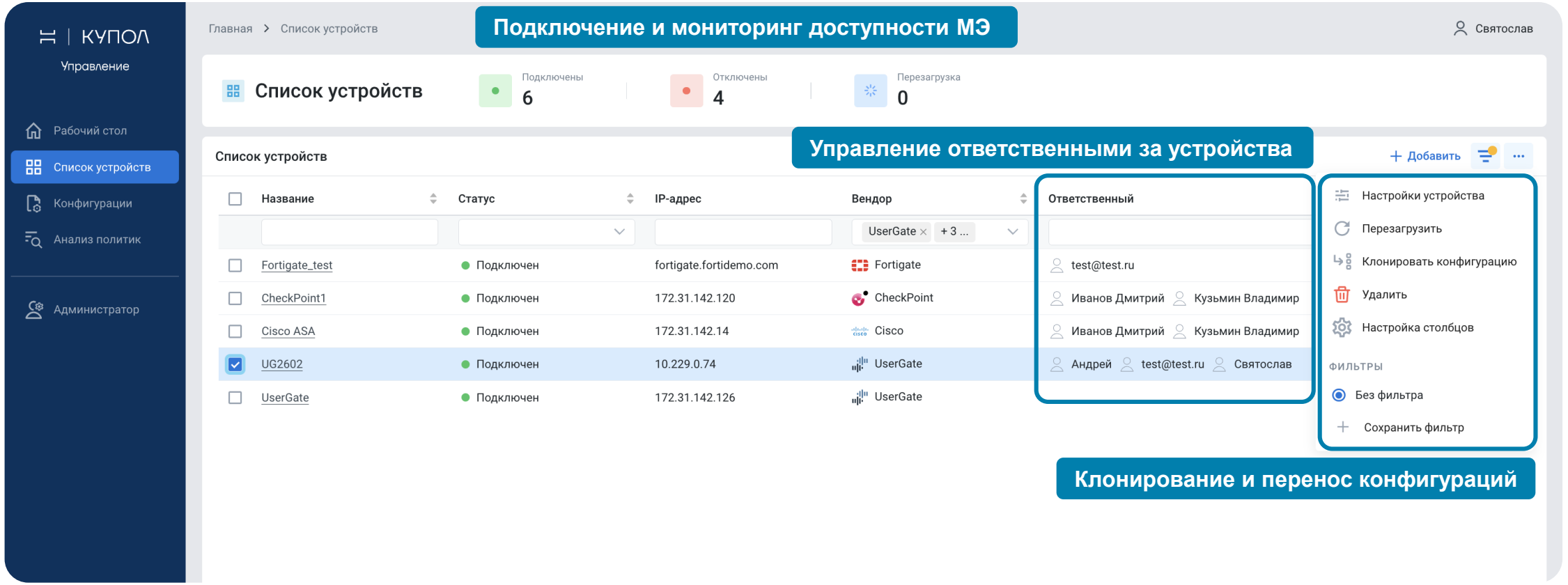
- Межсетевой экран
- Межсетевой экран
- Межсетевой экран

Единая система для контроля, анализа и управления

- UserGate
- Cisco
- Код безопасности
- Eltex
- ideco
- Fortinet
- infotecs
- Check Point
- Фактор-ТС
- Другие вендора МЭ, UTM, NGFW и сетевых устройств

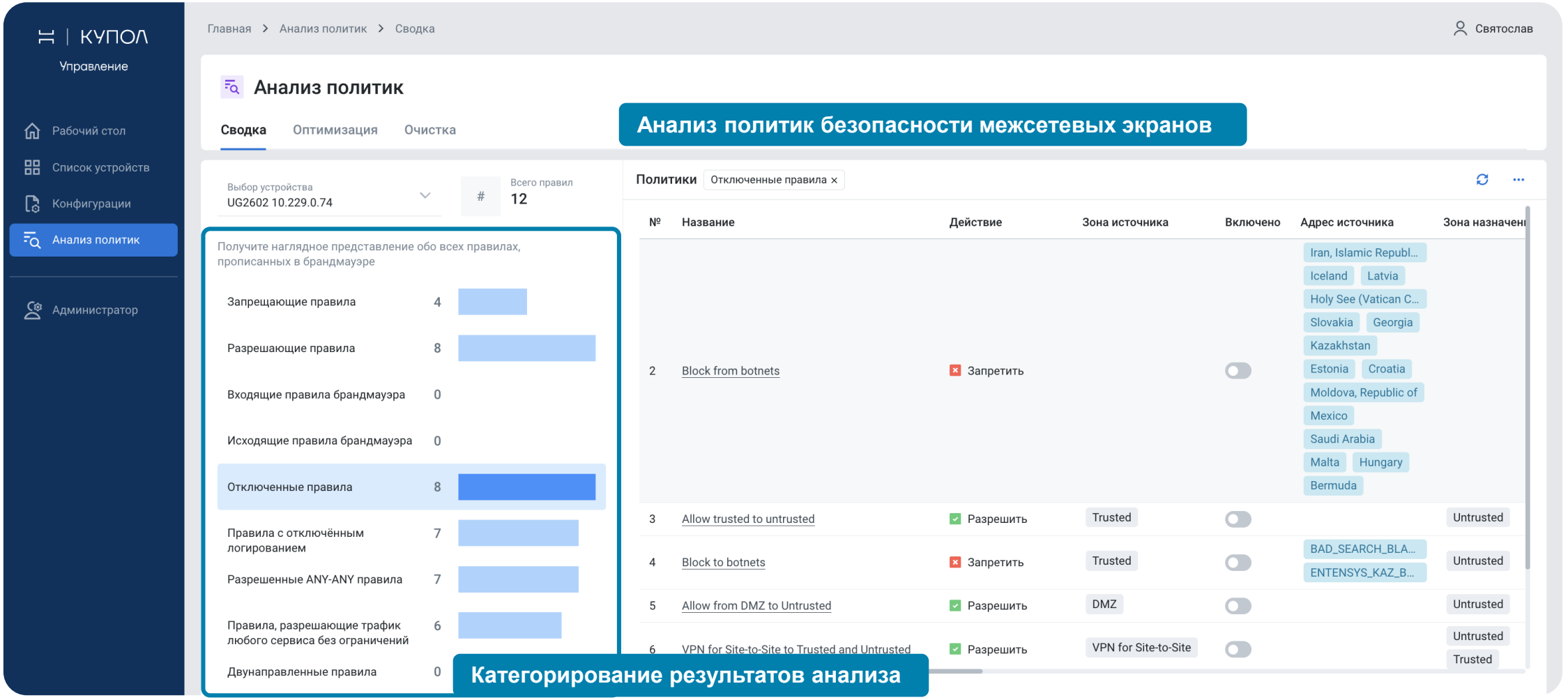
Купол

Интеграция межсетевых экранов различных вендоров



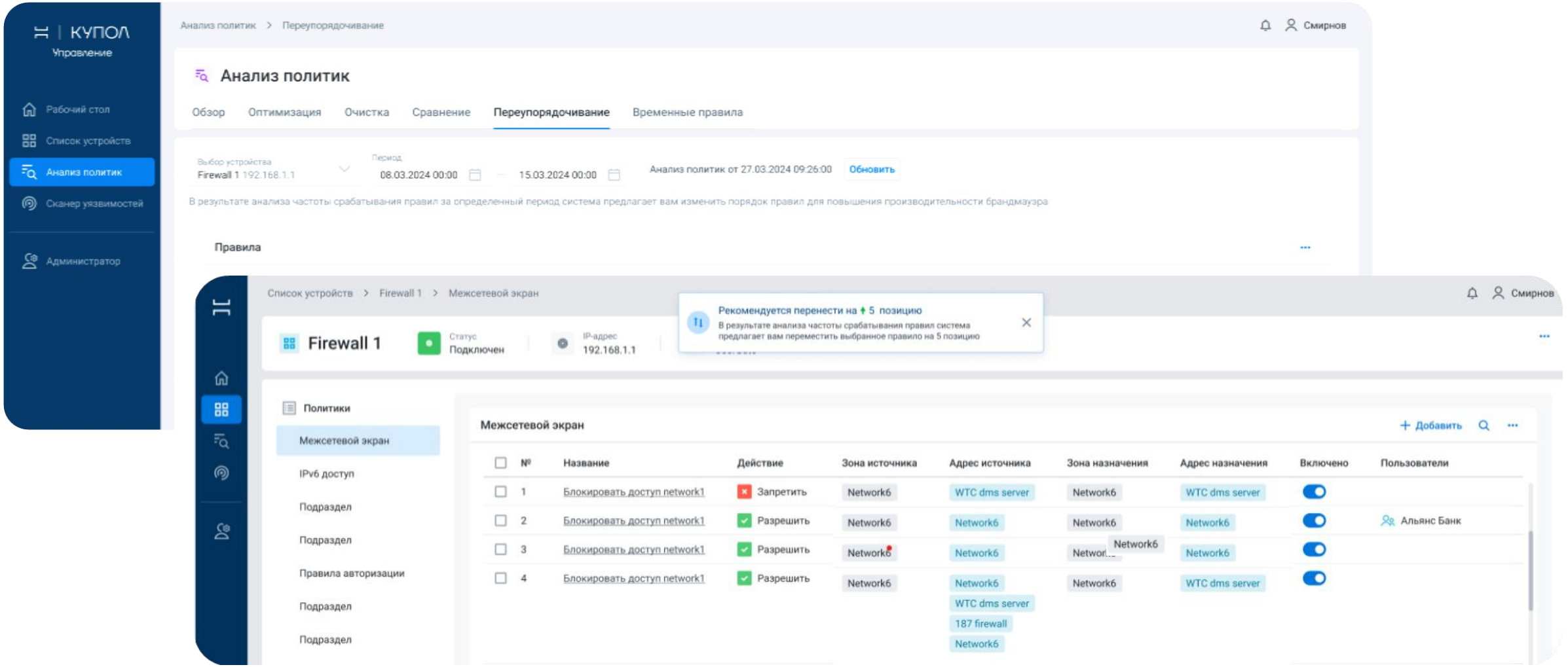
Купол

Анализ политик безопасности



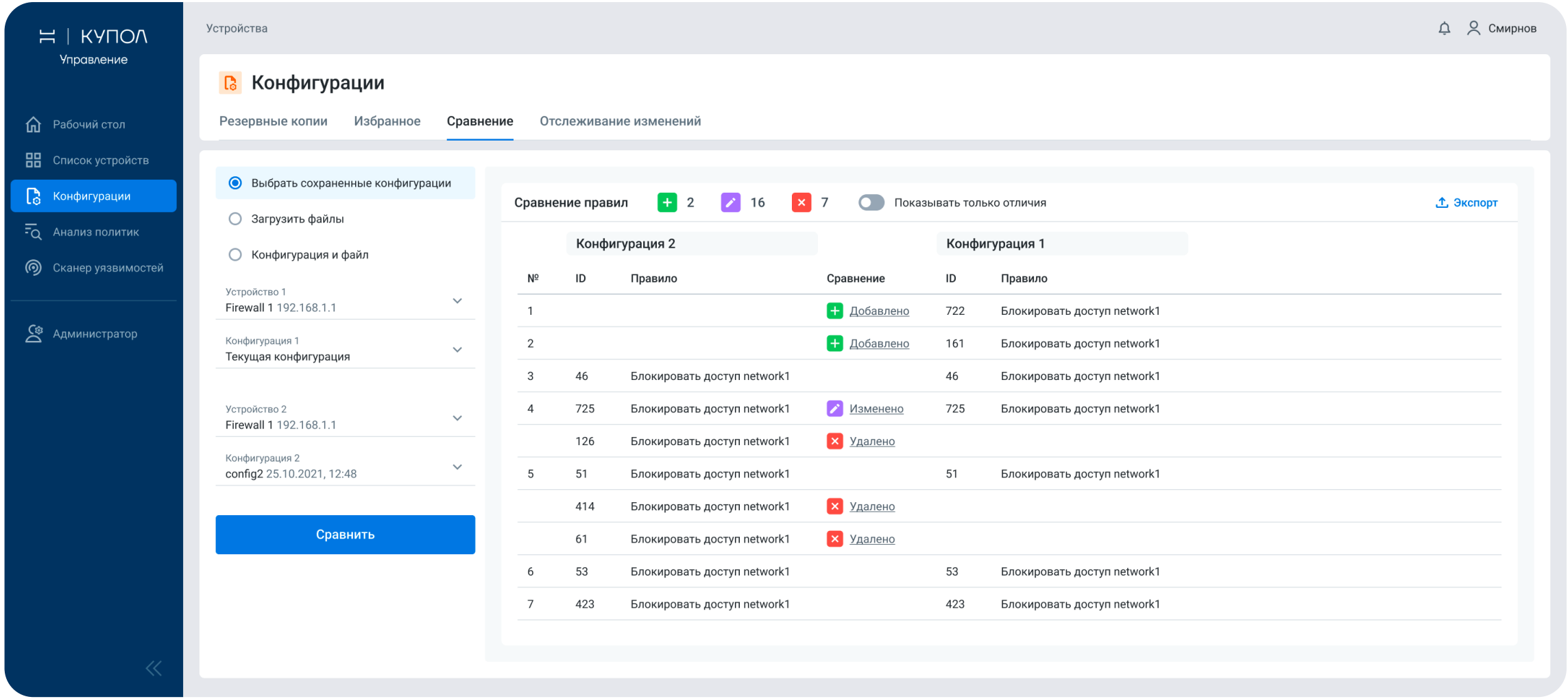
Купол

Рекомендации по оптимизации



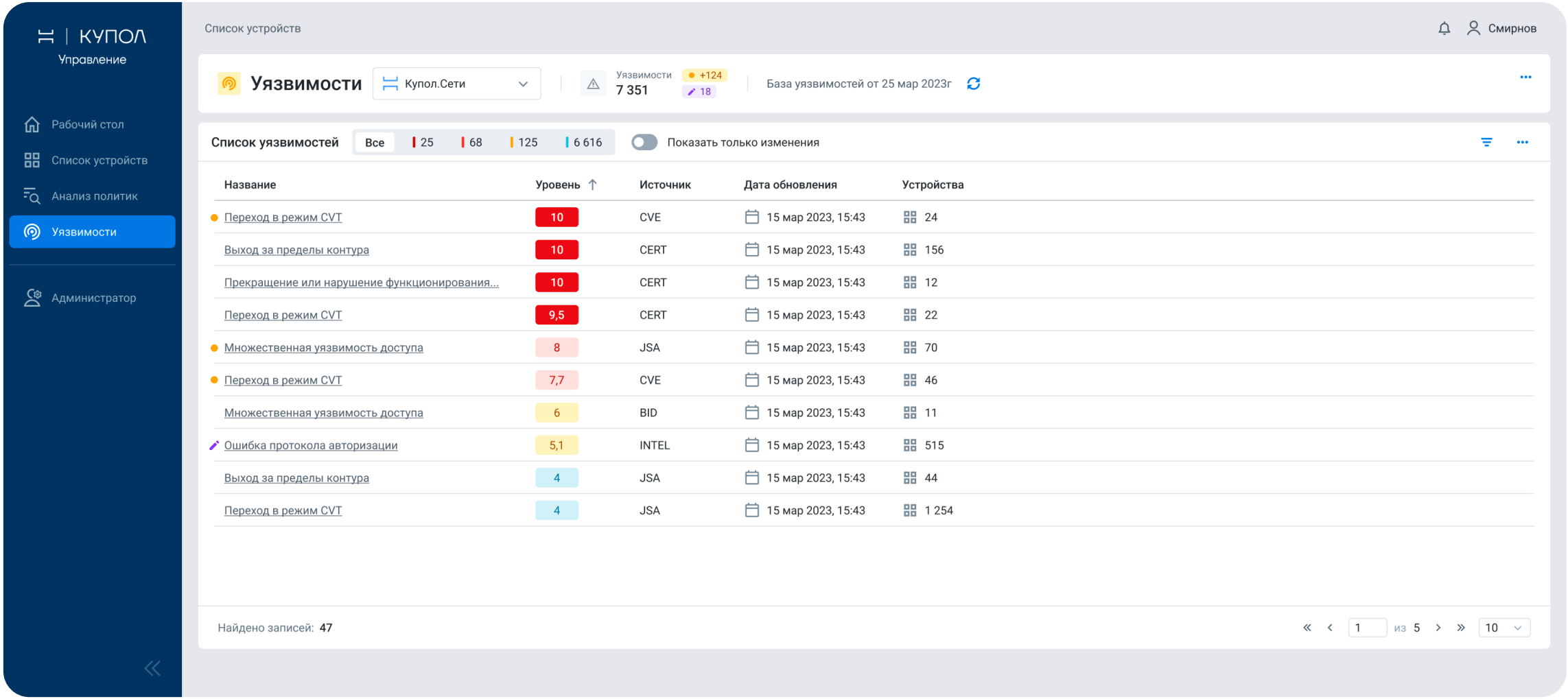
Купол

Сравнение конфигураций



Купол

Проверка уязвимостей МЭ



Купол

Пример решения проблем

Предприятие с ~110 межсетевыми экранами 4 различных производителей

Проблема клиента до внедрения продукта

Обслуживание межсетевых экранов

Обслуживание межсетевых экранов осуществлялось 2 специалистами (блок ИТ), тем не менее, ввиду импортозамещения и наличие у каждого производителя своего центра управления- время на контроль и настройку значительно увеличивалось

Отсутствуют решения, которые работают с российскими межсетевыми экранами

Рынок российских решений, которые будут поддерживать российские МЭ очень скудный. А также требуется поддержка специфичных межсетевых экранов

Сложность в анализе правил МЭ

Наличие на каждом из МЭ по 50–100 тысяч правил, что значительно снижает производительность сетевых средств защиты, на анализ которых у персонала просто нет времени

Результат внедрения продукта

Единый центр управления

У заказчика появилась возможность не только управлять всеми межсетевыми экранами, но и проводить перенос настройки из одной группы МЭ в другую

Поддержка любого производителя

Решение из коробки поддерживала 3 производителя заказчика, в течении пилотного проекта был освоен и подключен 4, финальный производитель, который использовался у заказчика. В дорожную карту также были заложены 2 производителя, которые в перспективе заменят оставшихся западных производителя

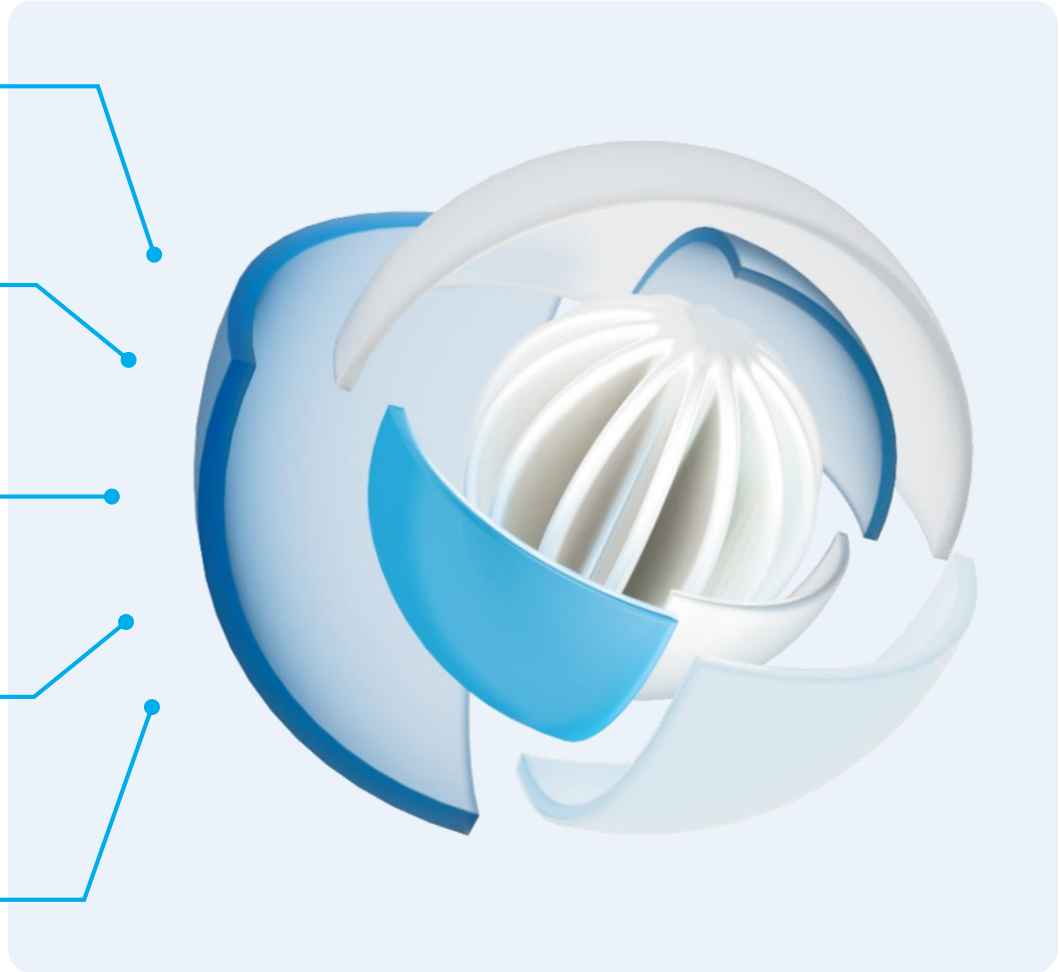
Оптимизация политик МЭ

Были выявлены аномалии в настройках политик подключенных МЭ, что позволило снизить количество правил до 30 000 правил и увеличить производительность сетевых средств защиты

Купол

Конкурентные преимущества Купол.Управление

- Централизованное мультивендорное управление правилами МЭ, подключенных устройств
- Более 15 категорий анализа правил МЭ устройств различных вендоров и формирование рекомендаций по их оптимизации
- Автобэкапирование конфигураций подключенных устройств с возможность их клонирования на другие устройства вендора и сравнения между собой
- Предоставление доступа в систему пользователям каталога Astra Linux Directory
- Возможность назначения пользователей системы ответственными за одно или несколько подключенных устройств



Интеграция средства защиты информации

Доступные вендора в Купол.Управление

UserGate	Межсетевые экраны UserGate	CISCO	Межсетевые экраны Cisco
КОД безопасности	Межсетевые экраны Код безопасности	ELTEX	Межсетевой экраны Eltex
ideco	Межсетевые экраны Ideco	FORTINET	Межсетевые экраны Fortinet
infotecs	Межсетевые экраны Infotecs	CHECK POINT	Межсетевые экраны Check Point
ФАКТОР-ТС	Межсетевые экраны Фактор-ТС		Другие вендора МЭ, UTM, NGFW и сетевых устройств

Купол

Спасибо
за внимание