netopia.pro

КОНТРОЛЬ СОСТОЯНИЯ СЕТИ

С ПЛАТФОРМОЙ NETOPIA FIREWALL COMPLIANCE



+7 (495) 255-35-82 / INFO@NETOPIA.PRO / МОСКВА-СКОЛКОВО, РОССИЯ

ЕДИНАЯ ПЛАТФОРМА ДЛЯ КОНТРОЛЯ СОСТОЯНИЯ БЕЗОПАСНОСТИ СЕТИ

netopia.pro

Модульность и гибкость

УПРАВЛЕНИЕ УЯЗВИМОСТЯМИ И УГРОЗАМИ (VULNERABILITY AND THREAT MANAGEMENT)

- Интеграция с системами управления уязвимостями и сканерами уязвимостей.
- Маркировка критичных активов.
- Оценка опасности угроз.

- Анализ векторов атак.
- Сверхприоритизация устранения уязвимостей.

УПРАВЛЕНИЕ ПОЛИТИКОЙ БЕЗОПАСНОСТИ (SECURITY POLICY MANAGEMENT)

- Анализ и контроль политик доступа и сегментации сети.
- Контроль конфигураций.
- Анализ и контроль правил доступа и их изменений.
- Визуализация сети.

МОДУЛЬНАЯ ПЛАТФОРМА NETOPIA FIREWALL COMPLIANCE

netopia.pro

Возможные сценарии

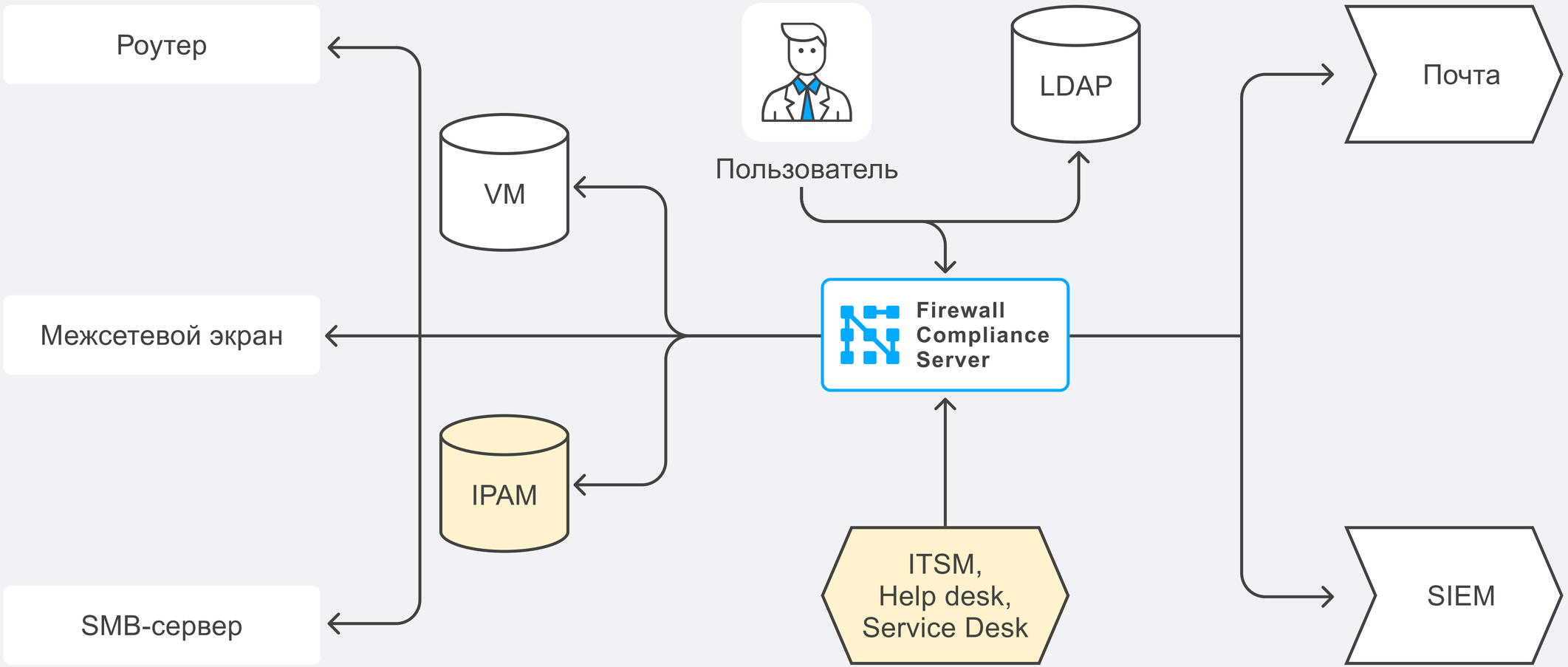
- АНАЛИЗ И ОПТИМИЗАЦИЯ ПРАВИЛ ДОСТУПА
- КОНТРОЛЬ СЕГМЕНТАЦИИ СЕТИ
- АВТОМАТИЗАЦИЯ УПРАВЛЕНИЯ ЖИЗНЕННЫМ ЦИКЛОМ ДОСТУПОВ
- НЕПРЕРЫВНЫЙ АУДИТ И РЕСЕРТИФИКАЦИЯ ПРАВИЛ
- АНАЛИЗ ВЕКТОРОВ АТАК И УПРАВЛЕНИЕ УЯЗВИМОСТЯМИ
- ПРИОРИТИЗАЦИЯ УЯЗВИМОСТЕЙ

Netopia Firewall Compliance

- АУДИТ ПОЛИТИК (FIREWALL ASSURANCE)
- УПРАВЛЕНИЕ ПОЛИТИКАМИ (CHANGE MANAGEMENT)
- АУДИТ СЕТИ (NETWORK ASSURANCE)
- ПРИОРИТИЗАЦИЯ УЯЗВИМОСТЕЙ (VULNERABILITY CONTROL)

ТИПОВАЯ СТРУКТУРА ВЗАИМОДЕЙСТВИЯ

netopia.pro



ПОДДЕРЖИВАЕМЫЕ СИСТЕМЫ

Почта

BPM-системы

SIEM

AD/LDAP



Vulnerability Management

IPAM

Security Scanner

ITSM

netopia.pro

ИНТЕГРИРУЕМЫЕ СИСТЕМЫ

NAUMEN SERVICE DESK

BPM SOFT

SECURITY VISION VM

positive technologies

POSITIVE TECHNOLOGIES VM / POSITIVE TECHNOLOGIES MAXPATROL 8

Microsoft Active Directory

MICROSOFT ACTIVE DIRECTORY / LDAP



IPAM



SIEM

ДОБАВЛЕНИЕ СИСТЕМ ВОЗМОЖНО ПО ЗАПРОСУ

netopia.pro

СПИСОК ПОДДЕРЖИВАЕМОГО ОБОРУДОВАНИЯ И ПО



IOS

ASA Firewall











Континент





positive technologies

















ЗАДАЧИ МОДУЛЯ «АУДИТ СЕТИ» (NETWORK ASSURANCE)

netopia.pro

МОДУЛЬ «АУДИТ СЕТИ» (NETWORK ASSURANCE) ПОМОГАЕТ ПОНЯТЬ

- КАК ВЫГЛЯДИТ ВАША СЕТЬ?
- КАК СКОНФИГУРИРОВАНО СЕТЕВОЕ ОБОРУДОВАНИЕ?
- КАК СЕГМЕНТИРОВАНА ВАША СЕТЬ?

ПРИНЦИП РАБОТЫ МОДУЛЯ «АУДИТ СЕТИ» (NETWORK ASSURANCE)

netopia.pro

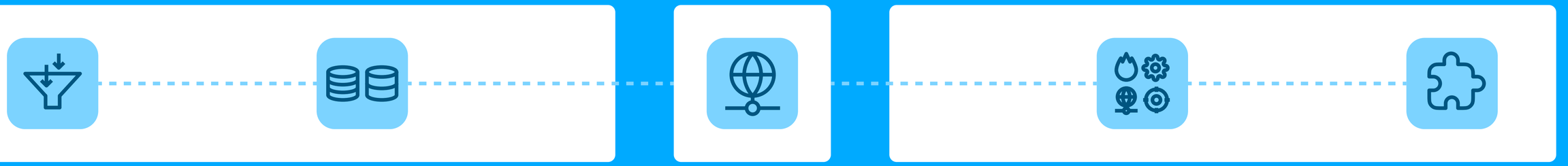
Полная видимость сети

ИНТЕРАКТИВНАЯ КАРТА СЕТИ

КОНТРОЛЬ КОНФИГУРАЦИЙ

КОНТРОЛЬ ПОЛИТИКИ СЕГМЕНТИРОВАНИЯ

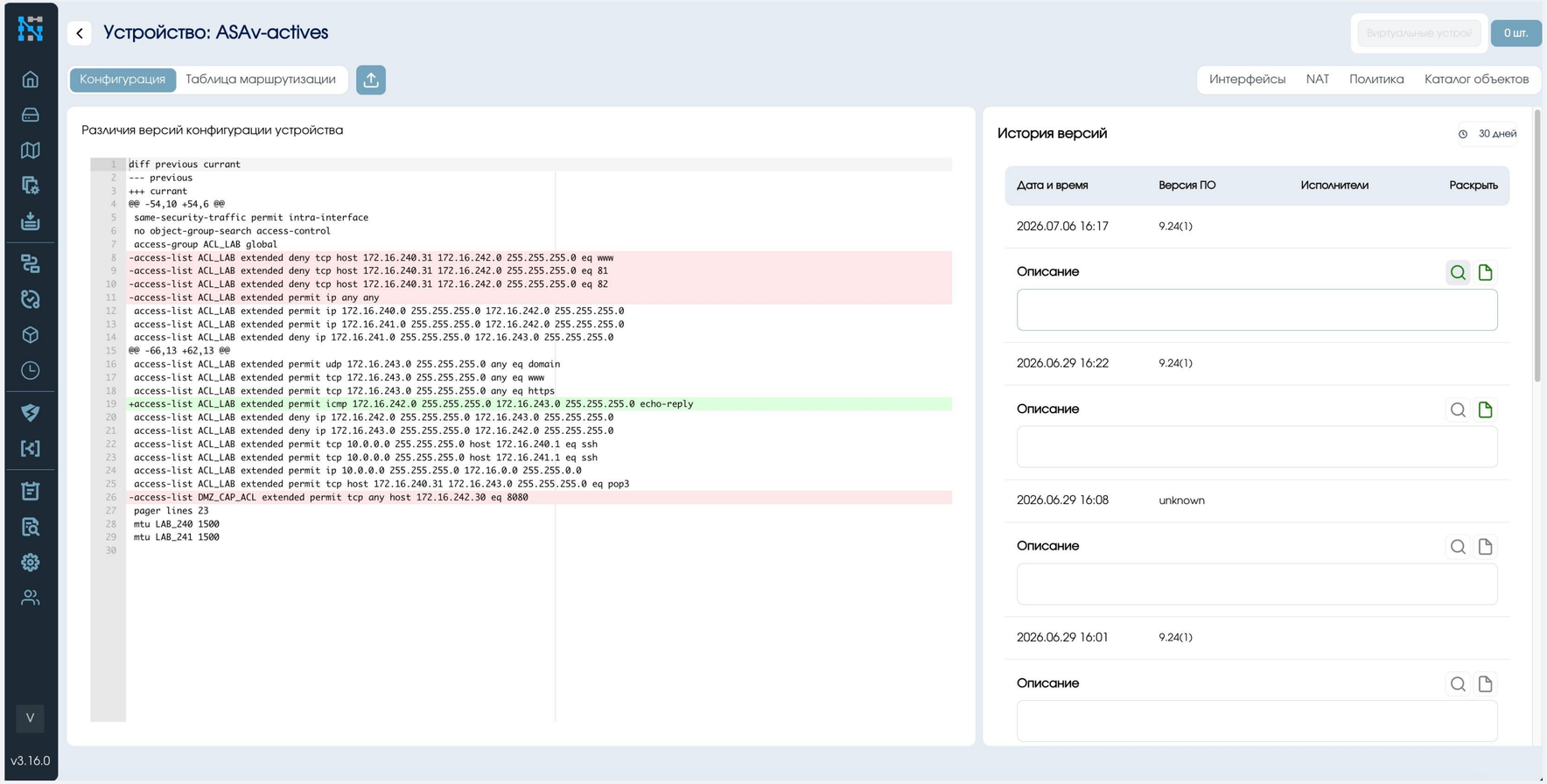
КАК ЭТО РАБОТАЕТ?



1. Сбор и нормализация
2. Моделирование
3. Детальный анализ

СБОР КОНФИГУРАЦИЙ

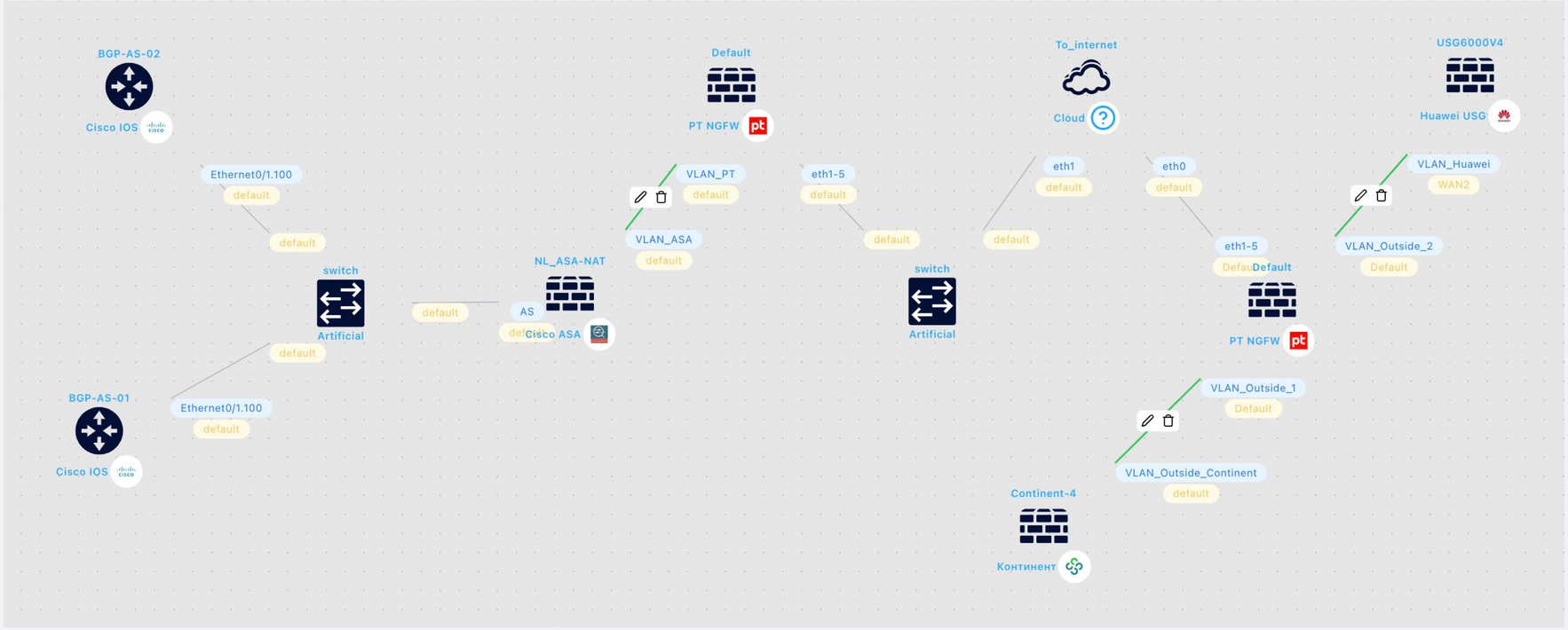
netopia.pro



- Сбор конфигураций по событию или по времени.
- Ретроспективный анализ изменений.

ПОСТРОЕНИЕ КАРТЫ СЕТИ

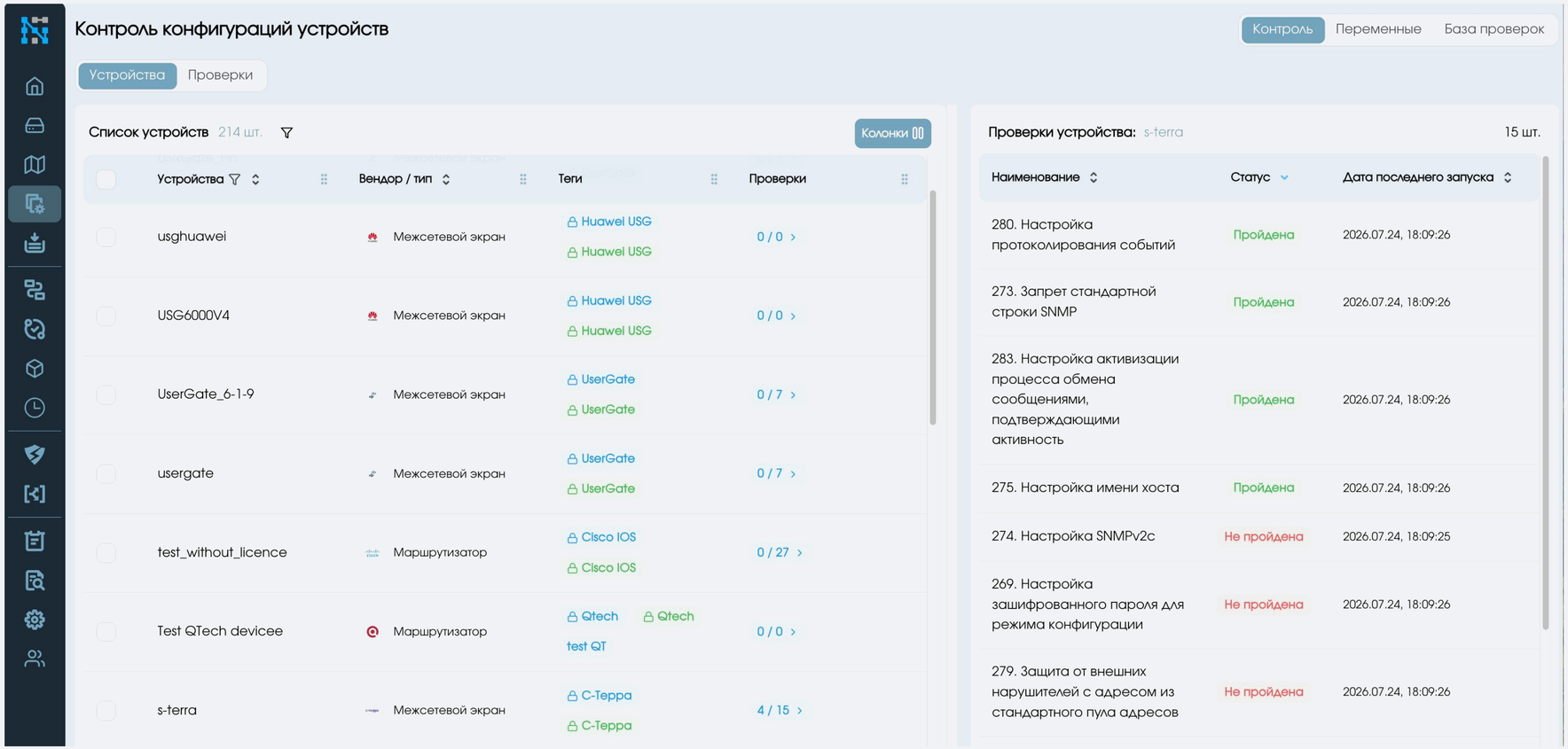
netopia.pro



Построение карты сети (уровня L3) и визуализация сетевой инфраструктуры.

ДЕТАЛЬНЫЙ АНАЛИЗ

netopia.pro



Анализ соответствия конфигураций сетевых устройств заданным стандартам (Анализ настроек на Hardening и Best Practices, нормативные документы (ГОСТ 57580, ПДН, ГИС, КИИ)).

ЗАДАЧИ МОДУЛЯ «АУДИТ ПОЛИТИК» (FIREWALL ASSURANCE)

netopia.pro

МОДУЛЬ «АУДИТ ПОЛИТИК» (FIREWALL ASSURANCE) ПОМОГАЕТ ПОНЯТЬ

- ОПТИМАЛЬНЫ ЛИ ВАШИ ПРАВИЛА?
- СООТВЕТСТВУЮТ ЛИ ПРАВИЛА ЗОНАМ БЕЗОПАСНОСТИ?
- КАК МЕНЯЮТСЯ ПРАВИЛА ДОСТУПА?

ПРИНЦИП РАБОТЫ МОДУЛЯ «АУДИТ ПОЛИТИК» (FIREWALL ASSURANCE)

netopia.pro

АНАЛИЗ ПРАВИЛ ДОСТУПА
И ИХ ОПТИМИЗАЦИЯ

КОНТРОЛЬ
ЗОН БЕЗОПАСНОСТИ

КОНТРОЛЬ ИЗМЕНЕНИЙ
ПРАВИЛ ДОСТУПА

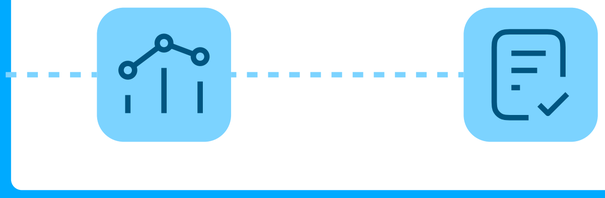
КАК ЭТО РАБОТАЕТ?



1. Сбор и нормализация



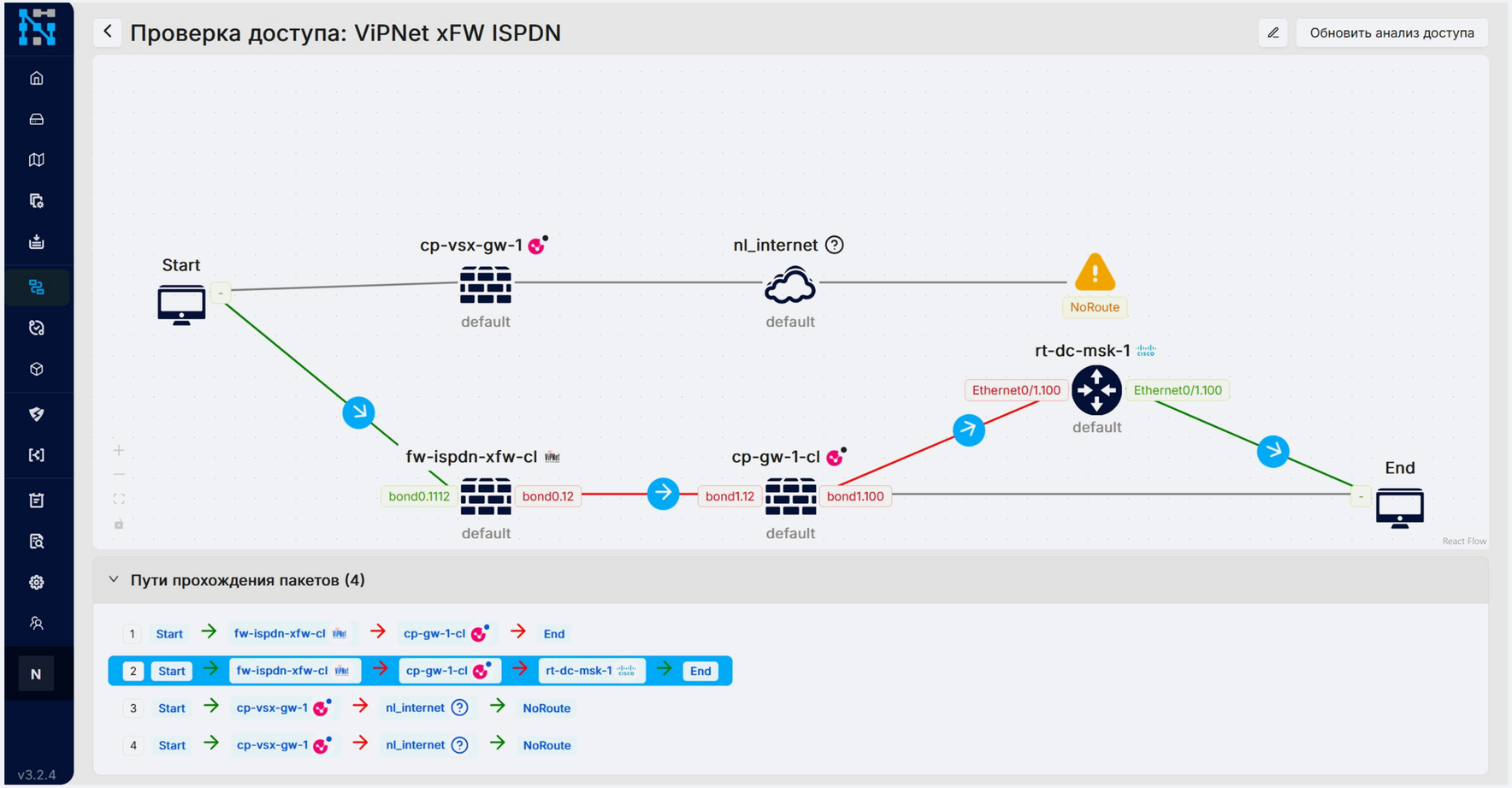
2. Анализ. Настраиваемые задачи и проверки



3. Отчёты и реагирование

АНАЛИЗ ПУТИ ПРОХОЖДЕНИЯ ТРАФИКА

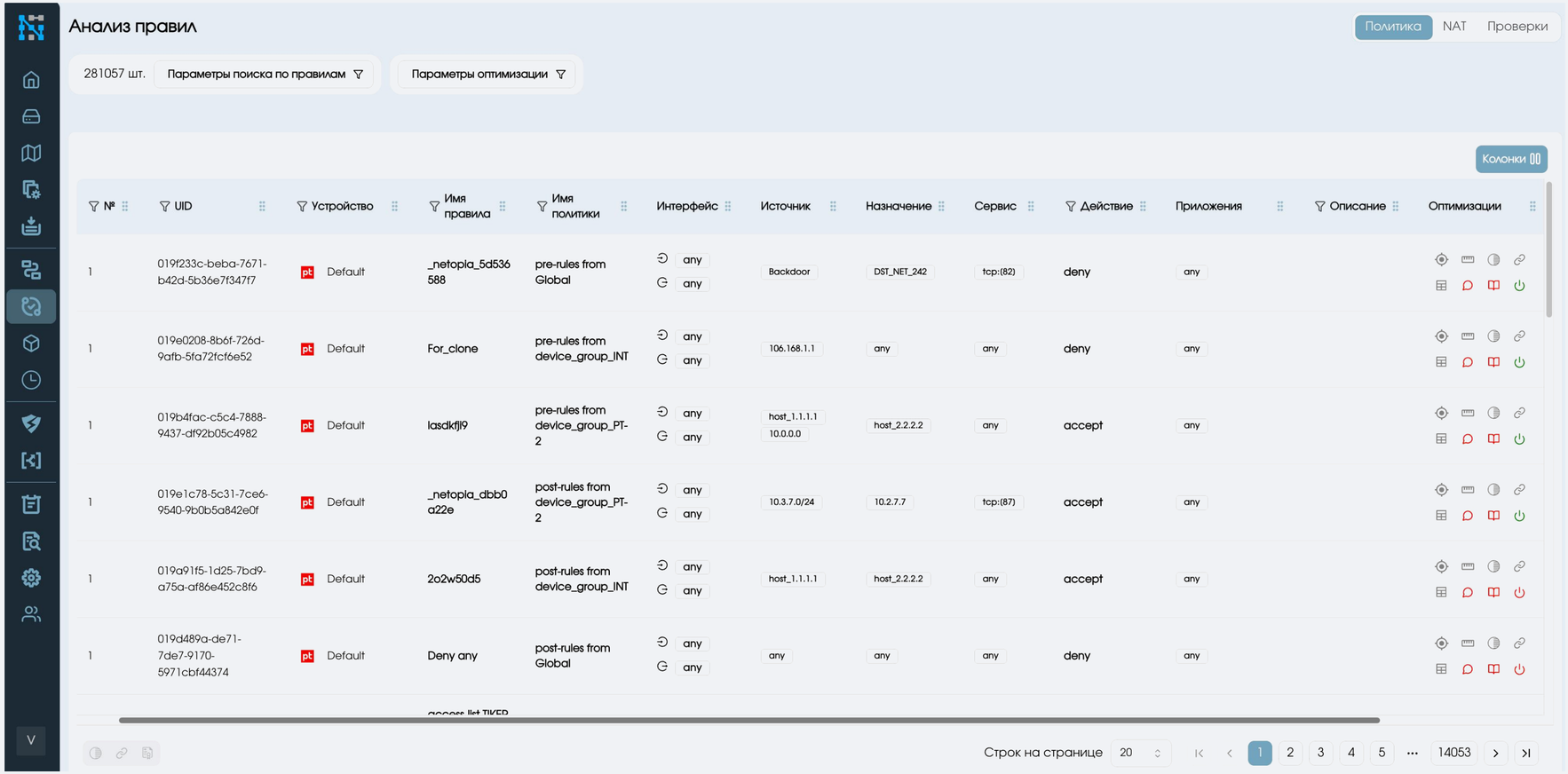
netopia.pro



- Анализ пути прохождения трафика по сети.
- Контроль наличия или отсутствия доступа в правилах межсетевых экранов по всему пути прохождения трафика.

ОПТИМИЗАЦИЯ СЕТЕВЫХ ПРАВИЛ

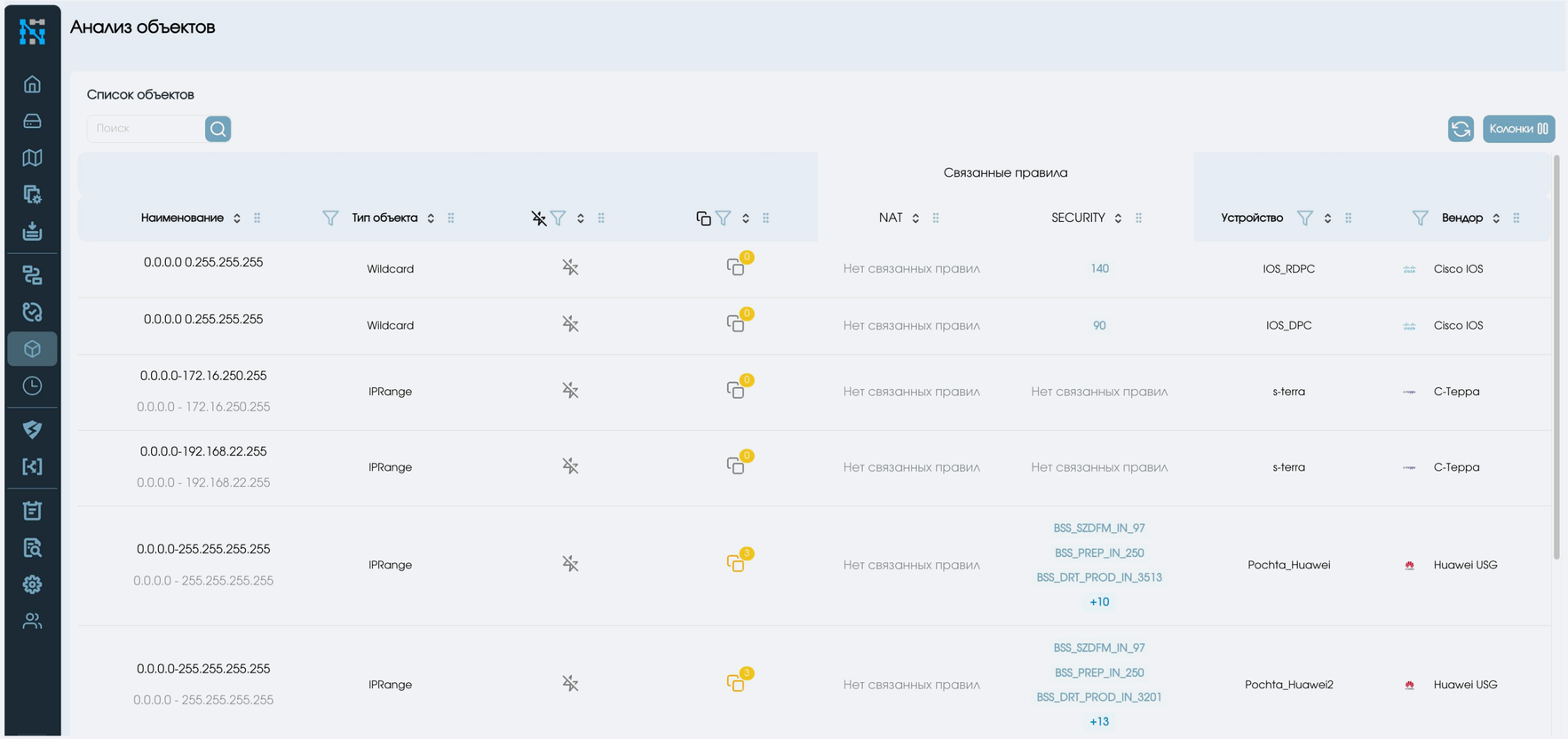
netopia.pro



Оптимизация политик (затенённые правила, давно не работающие правила, правила со слишком большим избыточным доступом и другие оптимизации).

ОПТИМИЗАЦИЯ ОБЪЕКТОВ ПОЛИТИК

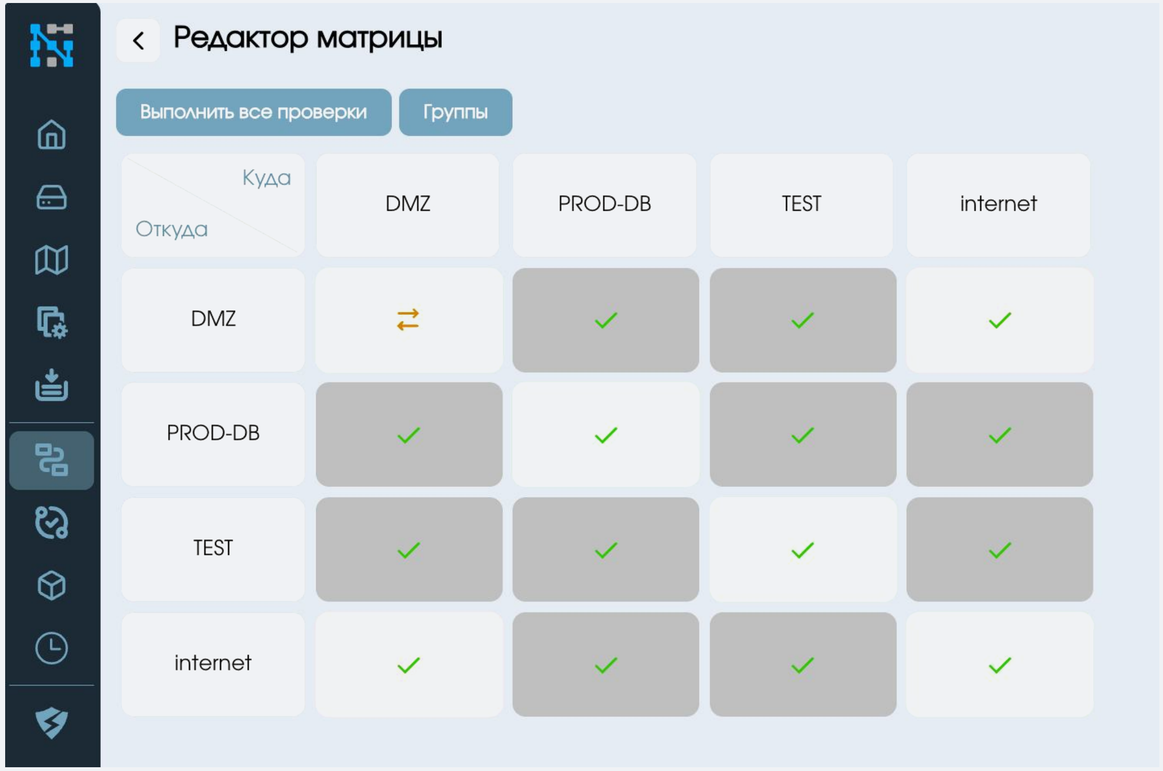
netopia.pro



Оптимизация объектов политик (объекты, не привязанные ни к каким правилам, дублирующиеся объекты).

МАТРИЦА ДОСТУПОВ

netopia.pro



Матрица доступа — визуальная зональная структура на платформе Netopia, задающая и контролирующая соблюдение правил доступа к сети.

Отображает разрешённый / запрещённый трафик между сегментами сети (зонами) для соответствия требованиям безопасности (ГОСТ 57580, ПДН, ГИС, КИИ, HIPAA, PCI DSS и т.д.), снижая риски и предоставляя оповещения о нарушениях в режиме реального времени для упрощения сегментации и управления сетью.

МОДУЛЬ «УПРАВЛЕНИЕ ПОЛИТИКАМИ» (CHANGE MANAGEMENT) РЕШАЕТ ЗАДАЧИ

netopia.pro

СОЗДАНИЯ ПРАВИЛ

- Анализ маршрута.
- Определение задействованных устройств.
- Оценка влияния планируемых изменений.

ПЕРЕСМОТРА ПРАВИЛ (РЕСЕРТИФИКАЦИИ)

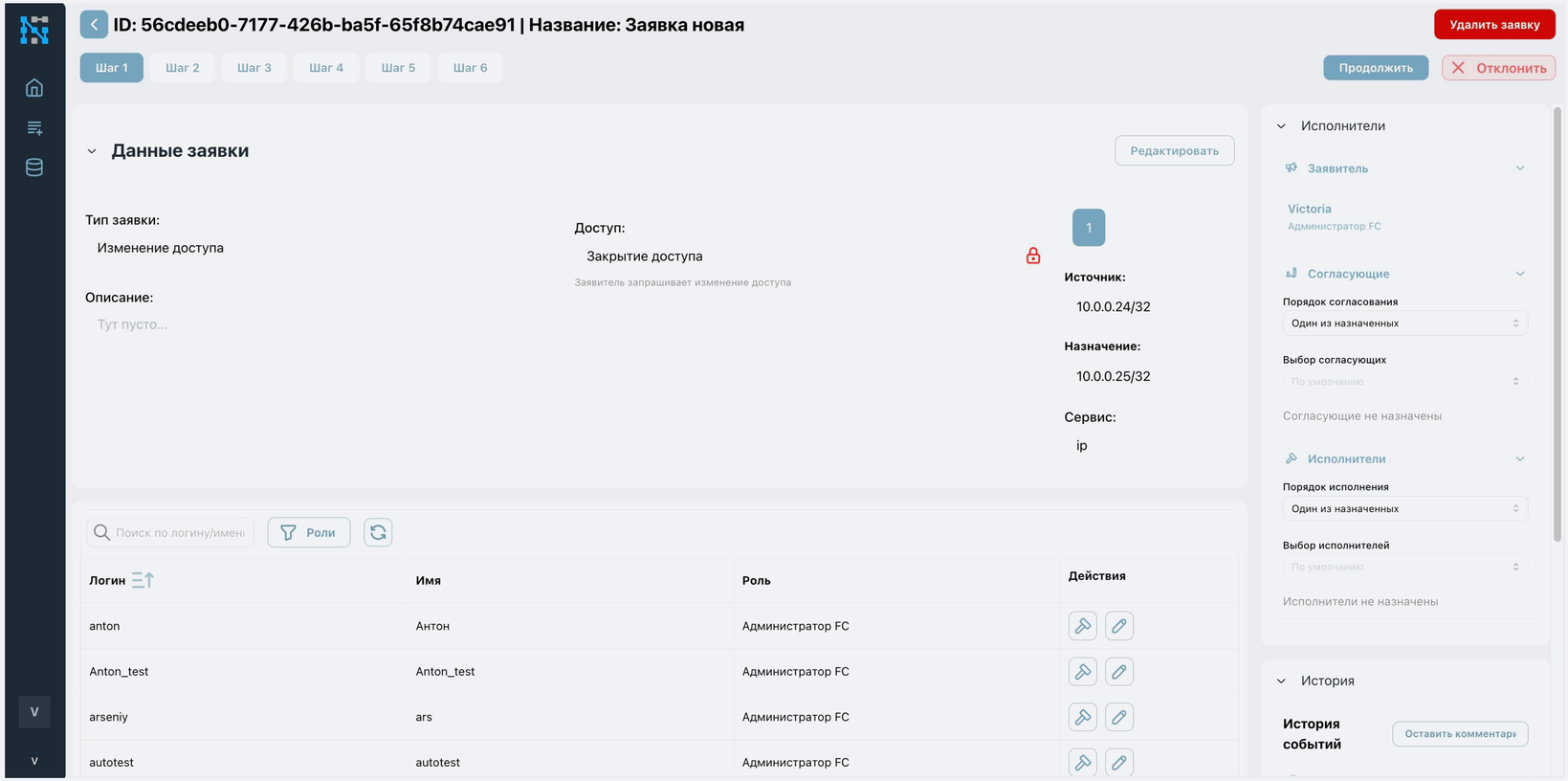
- Напоминание о сроках пересмотра правил.
- Управление доступом.
- Верификация изменений.

УДАЛЕНИЯ ПРАВИЛ

Автоматическое применение изменений

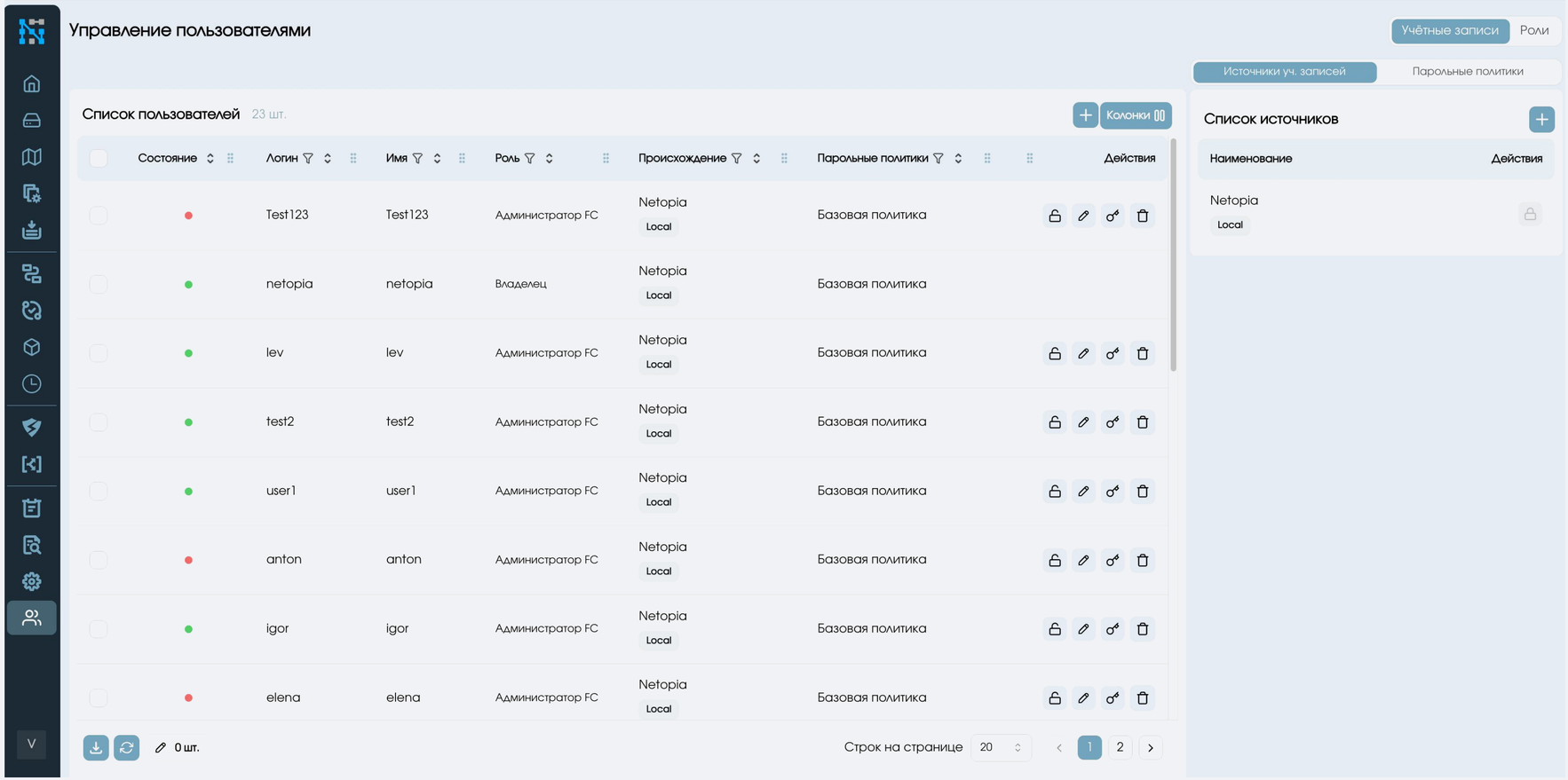
МОДУЛЬ «УПРАВЛЕНИЕ ПОЛИТИКАМИ» (CHANGE MANAGEMENT)

netopia.pro



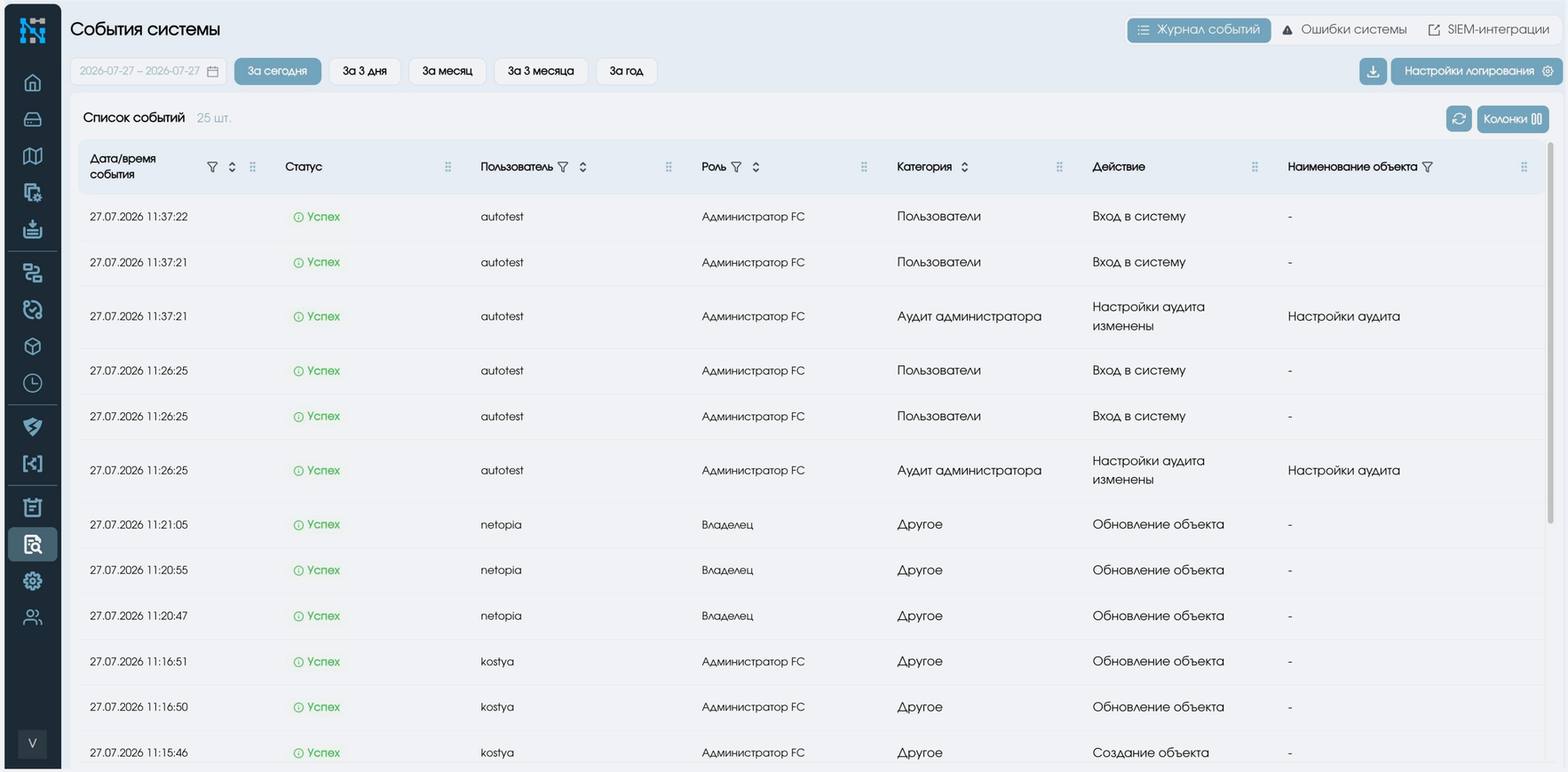
- Управление изменениями политик / конфигураций межсетевых экранов в автоматизированном режиме.
- Внесение и валидация изменений на межсетевых экранах.
- Интеграция с существующими системами управления изменениями в организации (ITSM, PAM, BPM и др.) посредством API.

УПРАВЛЕНИЕ ПОЛЬЗОВАТЕЛЯМИ



- Возможность управлять локальными учётными записями пользователей и ролями (создавать, изменять, удалять).
- Управление и создание различных парольных политик.
- Интеграция с AD/ LDAP.
- Гибкая ролевая модель.

СОБЫТИЯ СИСТЕМЫ



Возможность отслеживать все произошедшие события в системе.

ЗАДАЧИ МОДУЛЯ «ПРИОРИТИЗАЦИЯ УЯЗВИМОСТЕЙ» (VULNERABILITY CONTROL)

netopia.pro

МОДУЛЬ «ПРИОРИТИЗАЦИЯ УЯЗВИМОСТЕЙ» (VULNERABILITY CONTROL) ПОМОГАЕТ ПОНЯТЬ

- ОБО ВСЕХ ЛИ УЯЗВИМОСТЯХ ВЫ ЗНАЕТЕ?
- КАКИЕ УЯЗВИМОСТИ ЯВЛЯЮТСЯ РЕАЛЬНО ОПАСНЫМИ ИМЕННО ДЛЯ ВАШЕЙ ИНФРАСТРУКТУРЫ?
- КАК ОПТИМАЛЬНО И БЫСТРО УСТРАНИТЬ ОПАСНЫЕ УЯЗВИМОСТИ?

ПРИНЦИП РАБОТЫ МОДУЛЯ «ПРИОРИТИЗАЦИЯ УЯЗВИМОСТЕЙ» (VULNERABILITY CONTROL)

netopia.pro

Автоматическая оценка опасности уязвимостей

ВЫЯВЛЕНИЕ УЯЗВИМОСТЕЙ

РАСЧЁТ ВЕКТОРОВ АТАК В КОНТЕКСТЕ СЕТИ

РАСЧЁТ ПРИОРИТЕТОВ И РЕАГИРОВАНИЕ

КАК ЭТО РАБОТАЕТ?



1. Выявление



2. Анализ

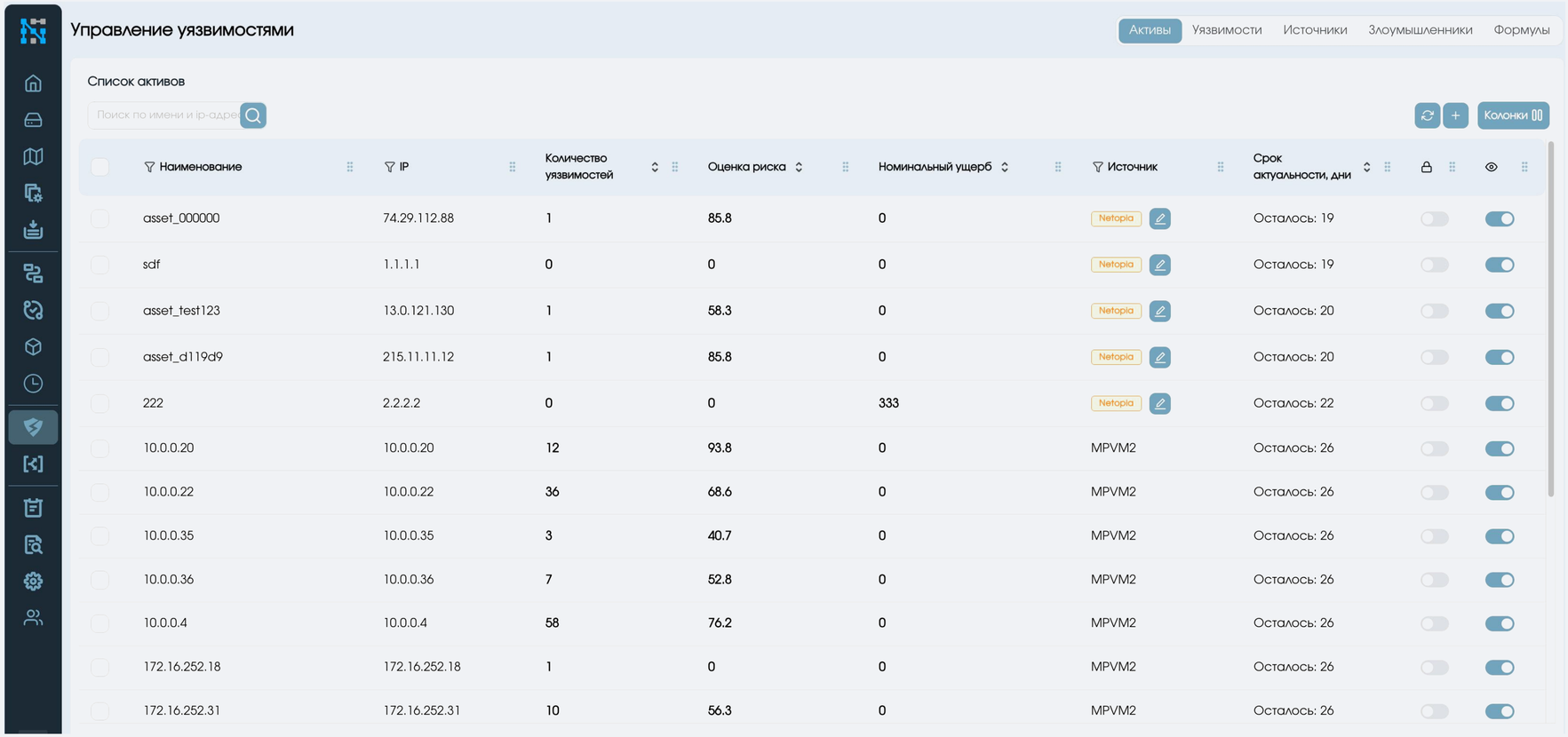


3. Приоритизация



4. Реагирование

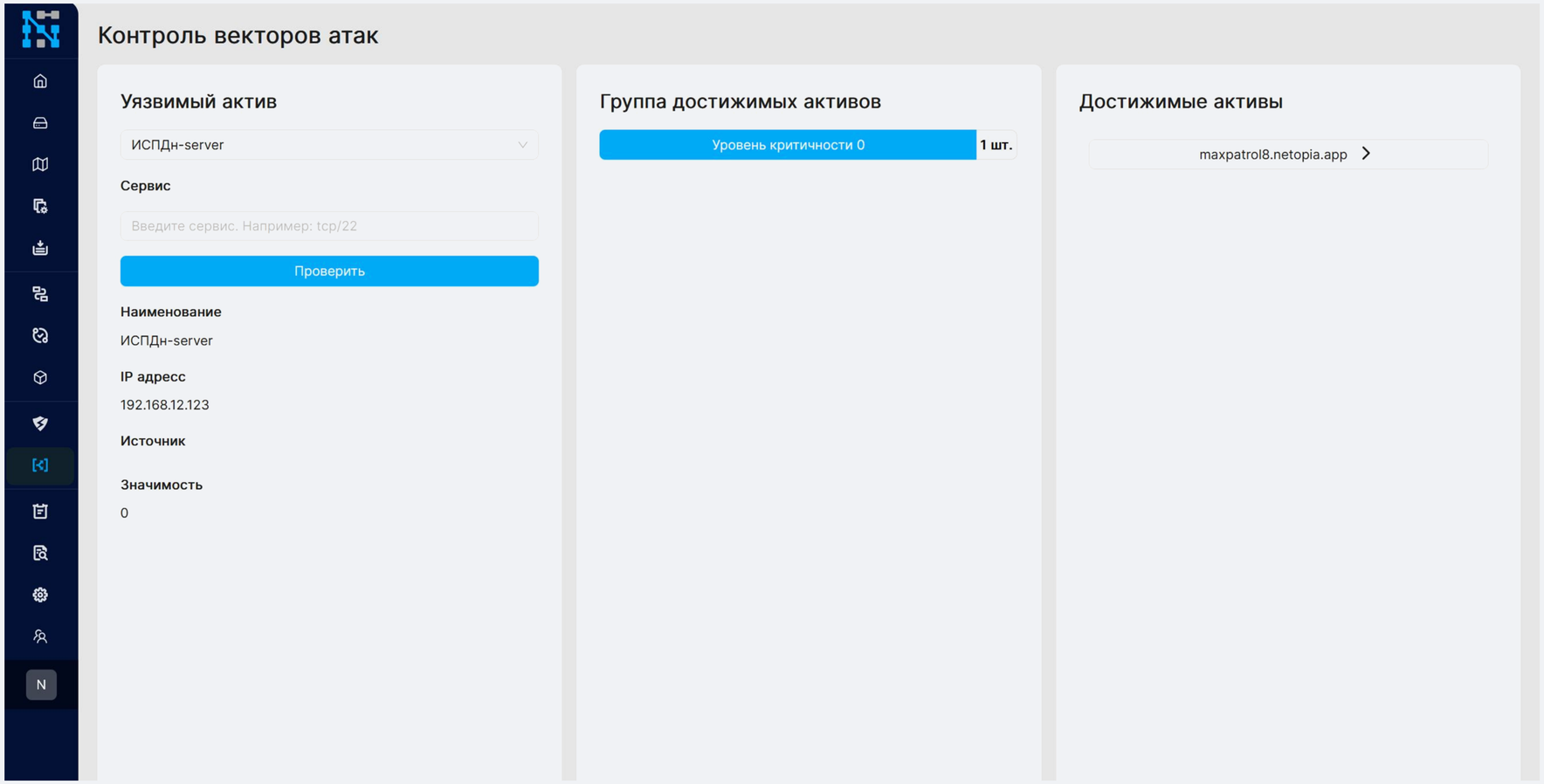
АНАЛИЗ И ПРИОРИТИЗАЦИЯ УЯЗВИМОСТЕЙ



Наименование	IP	Количество уязвимостей	Оценка риска	Номинальный ущерб	Источник	Срок актуальности, дни
asset_000000	74.29.112.88	1	85.8	0	Netopia	Осталось: 19
sdf	1.1.1.1	0	0	0	Netopia	Осталось: 19
asset_test123	13.0.121.130	1	58.3	0	Netopia	Осталось: 20
asset_d119d9	215.11.11.12	1	85.8	0	Netopia	Осталось: 20
222	2.2.2.2	0	0	333	Netopia	Осталось: 22
10.0.0.20	10.0.0.20	12	93.8	0	MPVM2	Осталось: 26
10.0.0.22	10.0.0.22	36	68.6	0	MPVM2	Осталось: 26
10.0.0.35	10.0.0.35	3	40.7	0	MPVM2	Осталось: 26
10.0.0.36	10.0.0.36	7	52.8	0	MPVM2	Осталось: 26
10.0.0.4	10.0.0.4	58	76.2	0	MPVM2	Осталось: 26
172.16.252.18	172.16.252.18	1	0	0	MPVM2	Осталось: 26
172.16.252.31	172.16.252.31	10	56.3	0	MPVM2	Осталось: 26

- **Корреляция текущих уязвимых активов с их доступностью по сети: из интернета, из сетей подрядчиков или иных внешних источников.**
- **Приоритизация устранения уязвимостей исходя из их достижимости.**

ПОСТРОЕНИЕ ВЕКТОРОВ АТАК



Выявление векторов атак и достижимости по сети критических защищаемых данных через существующие уязвимости.

ЛИЦЕНЗИРОВАНИЕ

netopia.pro

Модуль	Описание	Лицензирование
«Аудит сети» (Network Assurance)	Анализ соответствия конфигураций сетевых устройств заданным стандартам; ретроспективный анализ изменений конфигураций, анализ настроек на харденинг и лучшие практики сетевой безопасности, построение карты сети и визуализация сетевой инфраструктуры.	По количеству маршрутизирующих устройств.
«Аудит политик» (Firewall Assurance)	Анализ пути прохождения трафика и контроль доступа. Анализ правил доступа, политик и их оптимизация (затенённые правила, давно не работающие правила, правила со слишком большим избыточным доступом и другие оптимизации). Контроль наличия или отсутствия доступа в правилах межсетевых экранов по всему пути прохождения трафика.	По количеству межсетевых экранов: физических и виртуальных. Включает в себя модуль «Аудит сети» (Network Assurance). FA NA
«Управление политиками» (Change Management)	Управление изменениями политик межсетевых экранов в автоматизированном режиме с поддержкой цепочек согласований, присвоением номера тикетов правилам, интеграцией с существующими системами управления изменениями в организации (ITSM, PAM и др.) посредством API.	По количеству межсетевых экранов: физических и виртуальных, на которых будут проводиться изменения политик доступа. Для работы модуля обязательно наличие лицензии «Аудит политик» (Firewall Assurance). ЛИЦЕНЗИОННЫЕ ТРЕБОВАНИЯ: CM FA
«Приоритизация уязвимостей» (Vulnerability Control)	Корреляция текущих уязвимых активов с их доступностью по сети: из интернета, из сетей подрядчиков или иных внешних источников. Приоритизация устранения уязвимостей исходя из их достижимости. Выявление векторов атак и достижимости по сети критических защищаемых данных через существующие уязвимости (Multi-hop атаки).	По количеству активов в сети. Для эффективной работы модуля требуется как можно более полная информация о сети из модулей «Аудит политик» (Firewall Assurance) — обязательно и «Аудит сети» (Network Assurance). ЛИЦЕНЗИОННЫЕ ТРЕБОВАНИЯ: VC FA NA

NA Аудит сети (Network Assurance)

FA Аудит политик (Firewall Assurance)

CM Управление политиками (Change Management)

VC Приоритизация уязвимостей (Vulnerability Control)

ОЦЕНИТЕ ПРЕИМУЩЕСТВА ИСПОЛЬЗОВАНИЯ РЕШЕНИЯ NETOPIA FIREWALL COMPLIANCE!

netopia.pro

ООО «НЕТОПИЯ»

121205, г. Москва, муниципальный округ Можайский, территория инновационного центра «Сколково», б-р Большой, д. 42, стр. 1, этаж 2, помещение № 162/№ 4

Порядковый номер в реестре отечественного ПО — 17109

Резиденты Сколково

ПРЕМИЯ ЦИФРОВЫЕ ВЕРШИНЫ 2025

+7 (495) 255-35-82 / info@netopia.pro