netopia.pro
NETWORK SECURITY PLATFORM

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
NETWORK SECURITY PLATFORM

Модульность и гибкость

МОДУЛЬНАЯ ПЛАТФОРМА NETOPIA FIREWALL COMPLIANCE

netopia.pro
NETWORK SECURITY PLATFORM

Возможные сценарии

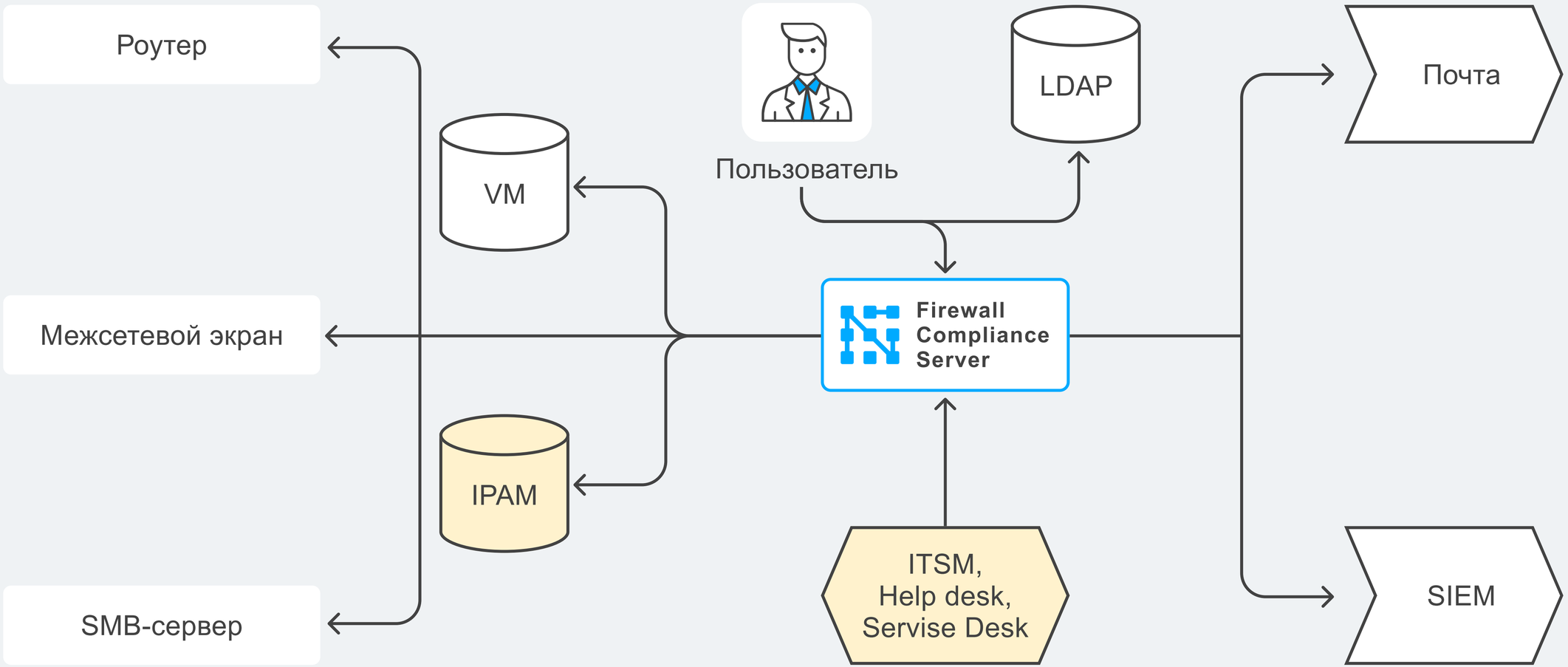
- АНАЛИЗ И ОПТИМИЗАЦИЯ ПРАВИЛ ДОСТУПА
- КОНТРОЛЬ СЕГМЕНТАЦИИ СЕТИ
- АВТОМАТИЗАЦИЯ УПРАВЛЕНИЯ ЖИЗНЕННЫМ ЦИКЛОМ ДОСТУПОВ
- НЕПРЕРЫВНЫЙ АУДИТ И РЕСЕРТИФИКАЦИЯ ПРАВИЛ
- АНАЛИЗ ВЕКТОРОВ АТАК И УПРАВЛЕНИЕ УЯЗВИМОСТЯМИ
- ПРИОРИТИЗАЦИЯ УЯЗВИМОСТЕЙ

Netopia Firewall Compliance

- FIREWAII ASSURANCE
- CHANGE MANAGEMENT
- NETWORK ASSURANCE
- VULNERABILITY CONTROI

ТИПОВАЯ СТРУКТУРА ВЗАИМОДЕЙСТВИЯ

netopia.pro
NETWORK SECURITY PLATFORM



ПОДДЕРЖИВАЕМЫЕ СИСТЕМЫ

Email

BPM-системы

SIEM

AD/LDAP

Vulnerability Management

IPAM

Security Scanner

ITSM

netopia.pro
NETWORK SECURITY PLATFORM

ИНТЕГРИРУЕМЫЕ СИСТЕМЫ

NAUMEN

NAUMEN SERVICE DESK

BPM SOFT

BPM SOFT

Security Vision

SECURITY VISION VM

positive technologies

POSITIVE TECHNOLOGIES VM / POSITIVE TECHOIOGIES MAXPATROI 8

Microsoft Active Directory

MICROSOFT ACTIVE DIRECTORY / LDAP

IPAM

SIEM

ДОБАВЛЕНИЕ СИСТЕМ ВОЗМОЖНО ПО ЗАПРОСУ

netopia.pro
NETWORK SECURITY PLATFORM

СПИСОК ПОДДЕРЖИВАЕМОГО ОБОРУДОВАНИЯ И ПО

CISCO IOS ASA Firewall ViPNet Virtual Private Network UserGate

FORTINET HUAWEI CHECK POINT Континент

с•терра ELTEX positive technologies

ideco

В БЛИЖАЙШЕЕ ВРЕМЯ:

BI TECH QTECH МИР ДОСТУПНЕЕ vmware NSX

netopia.pro NETWORK SECURITY PLATFORM

ЗАДАЧИ NETWORK ASSURANCE

netopia.pro
NETWORK SECURITY PLATFORM

NETWORK ASSURANCE ПОМОГАЕТ ПОНЯТЬ

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

ПРИНЦИП РАБОТЫ NETWORK ASSURANCE

netopia.pro
NETWORK SECURITY PLATFORM

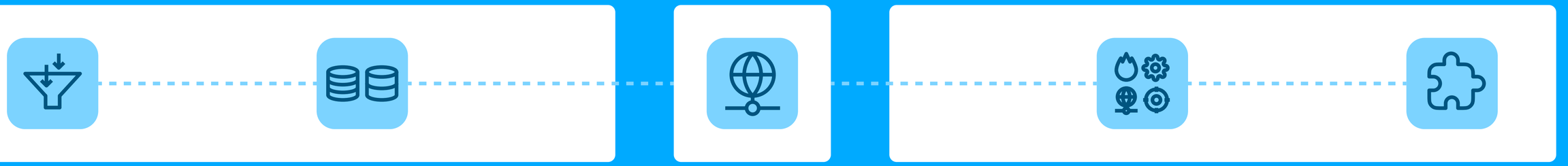
Полная видимость сети

ИНТЕРАКТИВНАЯ КАРТА СЕТИ

КОНТРОЛЬ КОНФИГУРАЦИЙ

КОНТРОЛЬ ПОЛИТИКИ СЕГМЕНТИРОВАНИЯ

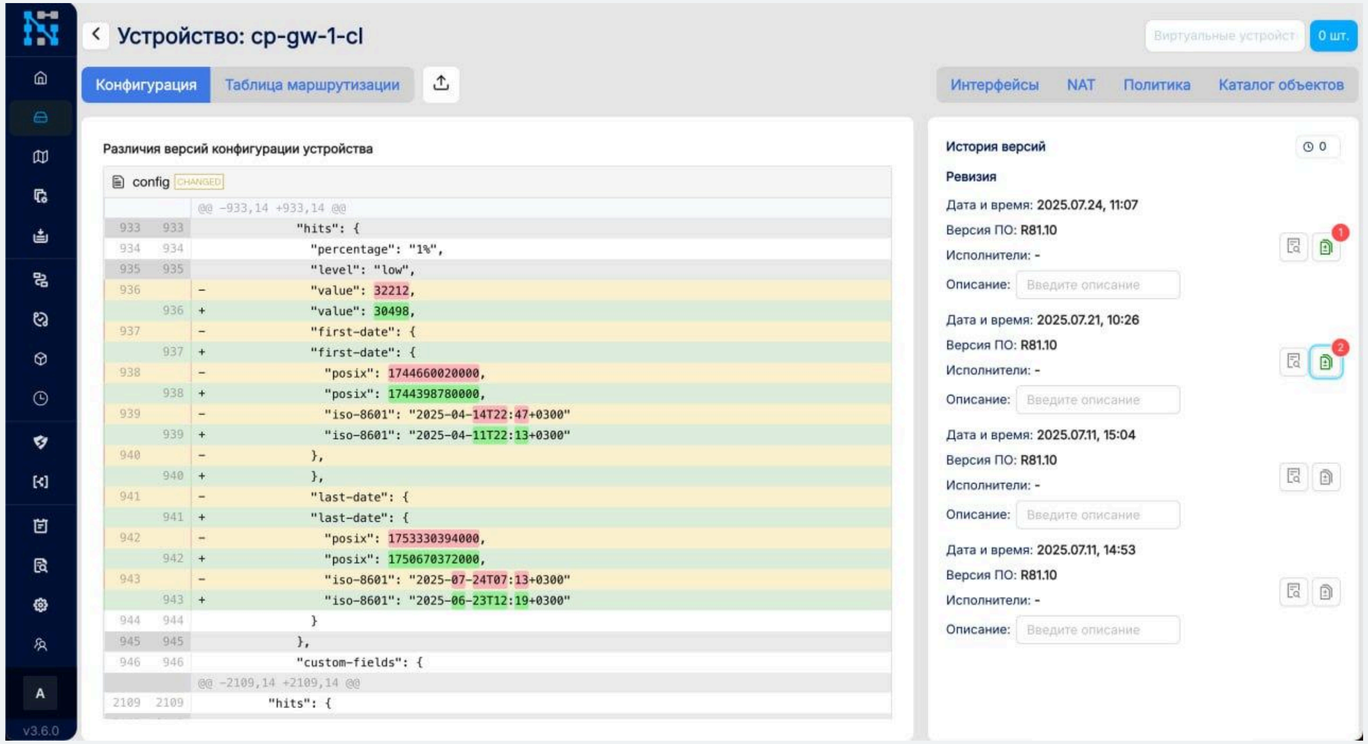
КАК ЭТО РАБОТАЕТ?



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

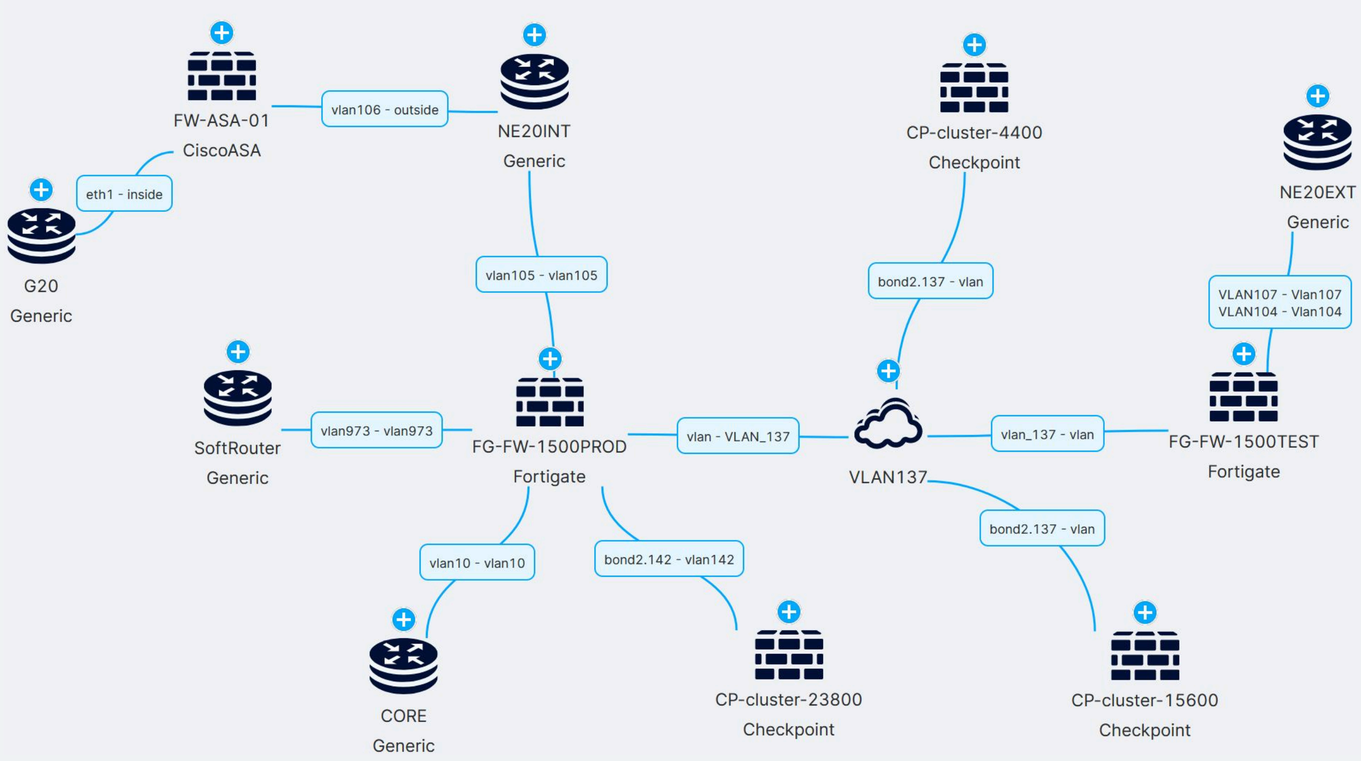
СБОР КОНФИГУРАЦИЙ

netopia.pro
NETWORK SECURITY PLATFORM



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

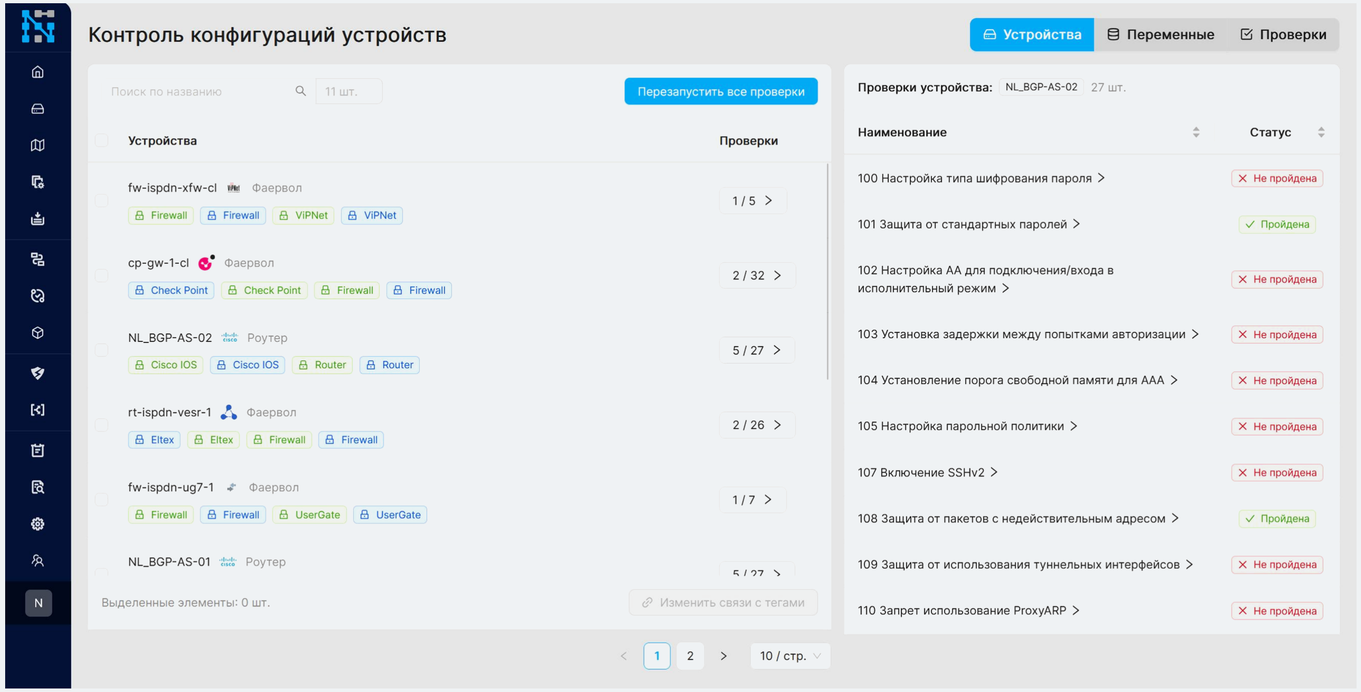
ПОСТРОЕНИЕ КАРТЫ СЕТИ



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

ДЕТАЛЬНЫЙ АНАЛИЗ

netopia.pro
NETWORK SECURITY PLATFORM



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

ЗАДАЧИ FIREWALL ASSURANCE

netopia.pro
NETWORK SECURITY PLATFORM

FIREWALL ASSURANCE ПОМОГАЕТ ПОНЯТЬ

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

ПРИНЦИП РАБОТЫ FIREWALL ASSURANCE

netopia.pro
NETWORK SECURITY PLATFORM

АНАЛИЗ ПРАВИЛ ДОСТУПА
И ИХ ОПТИМИЗАЦИЯ

КОНТРОЛЬ
ЗОН БЕЗОПАСНОСТИ

КОНТРОЛЬ ИЗМЕНЕНИЙ
ПРАВИЛ ДОСТУПА

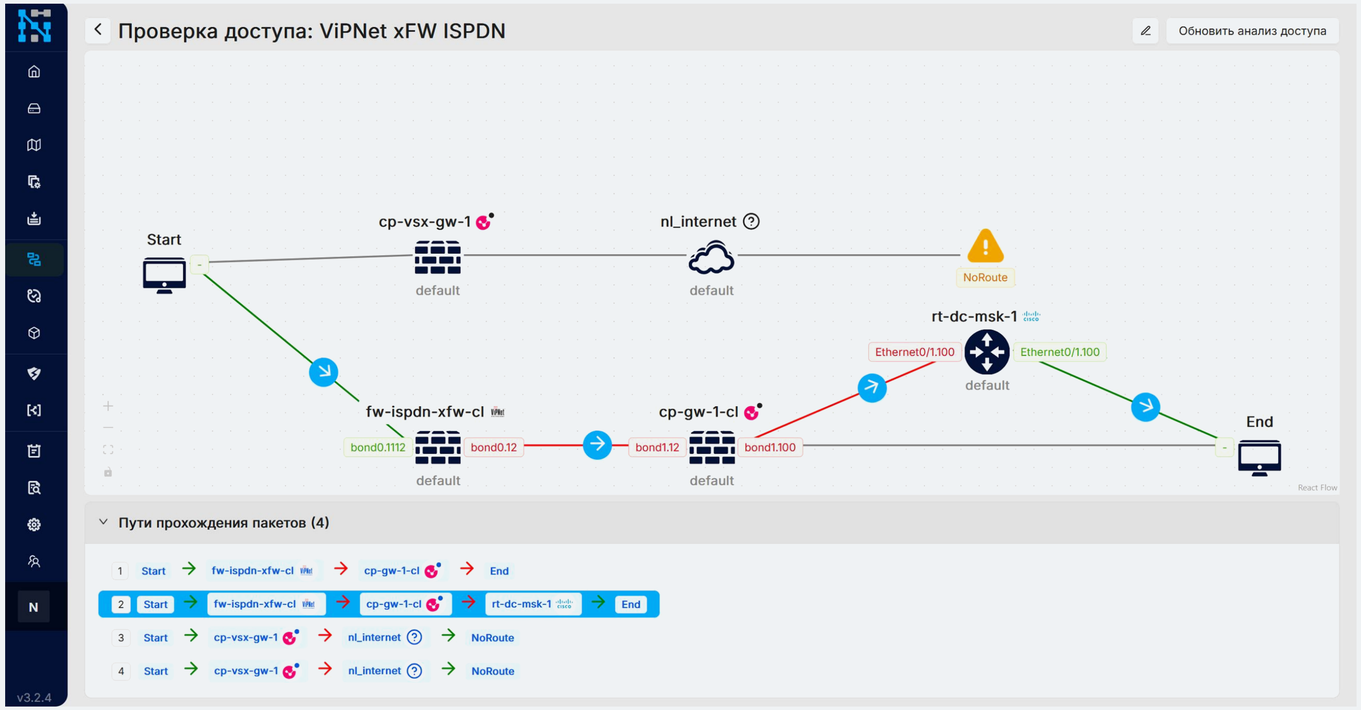
КАК ЭТО РАБОТАЕТ?


1. Сбор и нормализация


2. Анализ. Настраиваемые задачи и проверки


3. Отчёты и реагирование

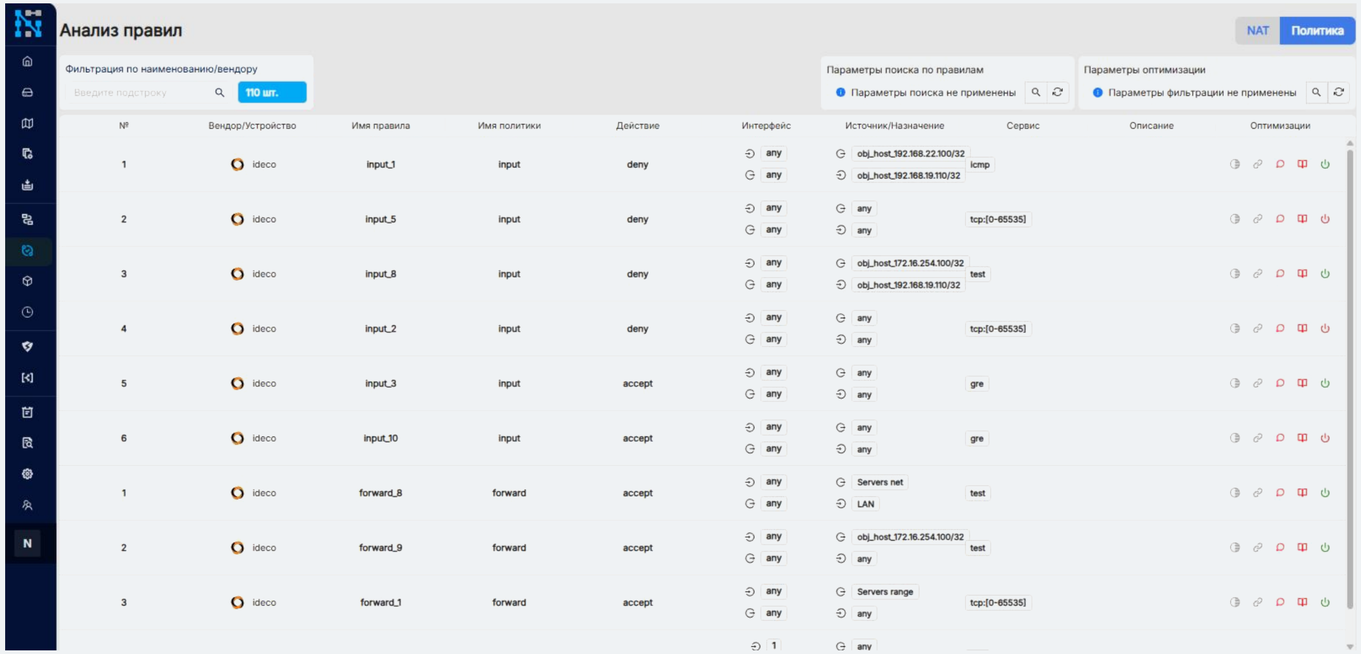
АНАЛИЗ ПУТИ ПРОХОЖДЕНИЯ ТРАФИКА



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

ОПТИМИЗАЦИЯ СЕТЕВЫХ ПРАВИЛ

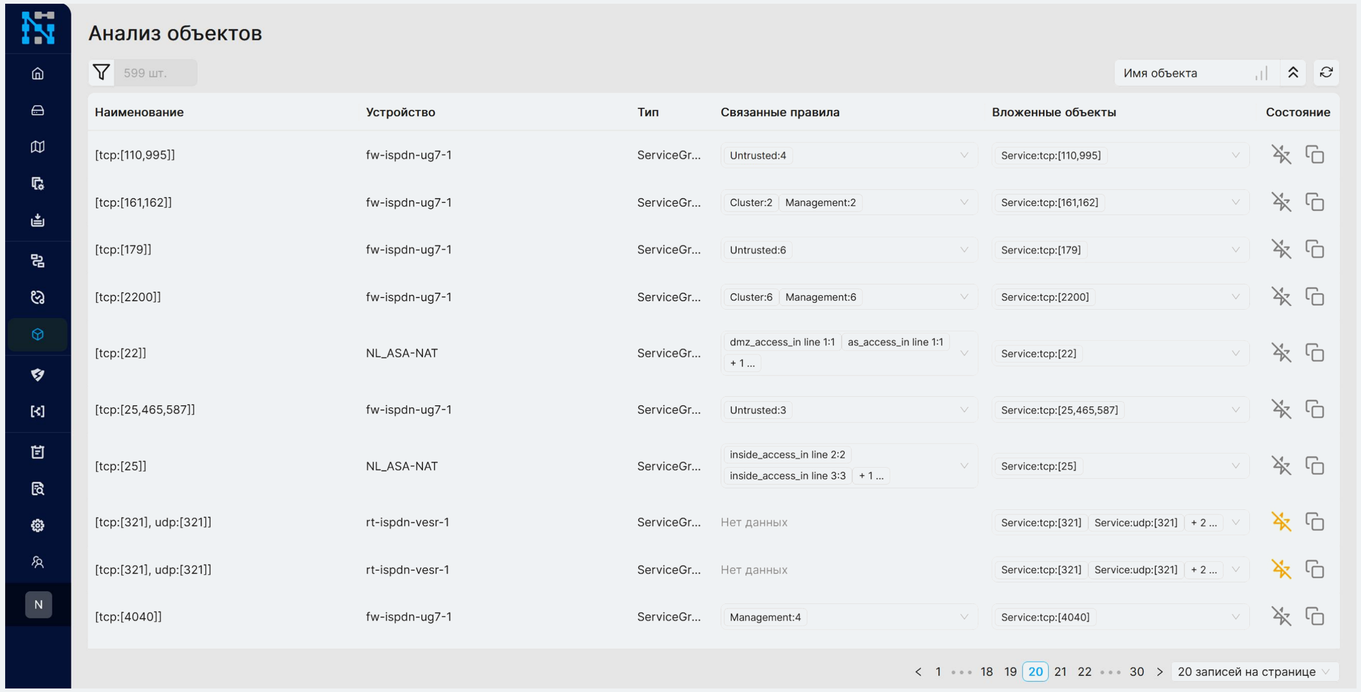
netopia.pro
NETWORK SECURITY PLATFORM



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

ОПТИМИЗАЦИЯ ОБЪЕКТОВ ПОЛИТИК

netopia.pro
NETWORK SECURITY PLATFORM



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

CHANGE MANAGEMENT РЕШАЕТ ЗАДАЧИ

netopia.pro
NETWORK SECURITY PLATFORM

СОЗДАНИЯ ПРАВИЛ

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

ПЕРЕСМОТРА ПРАВИЛ (РЕСЕРТИФИКАЦИИ)

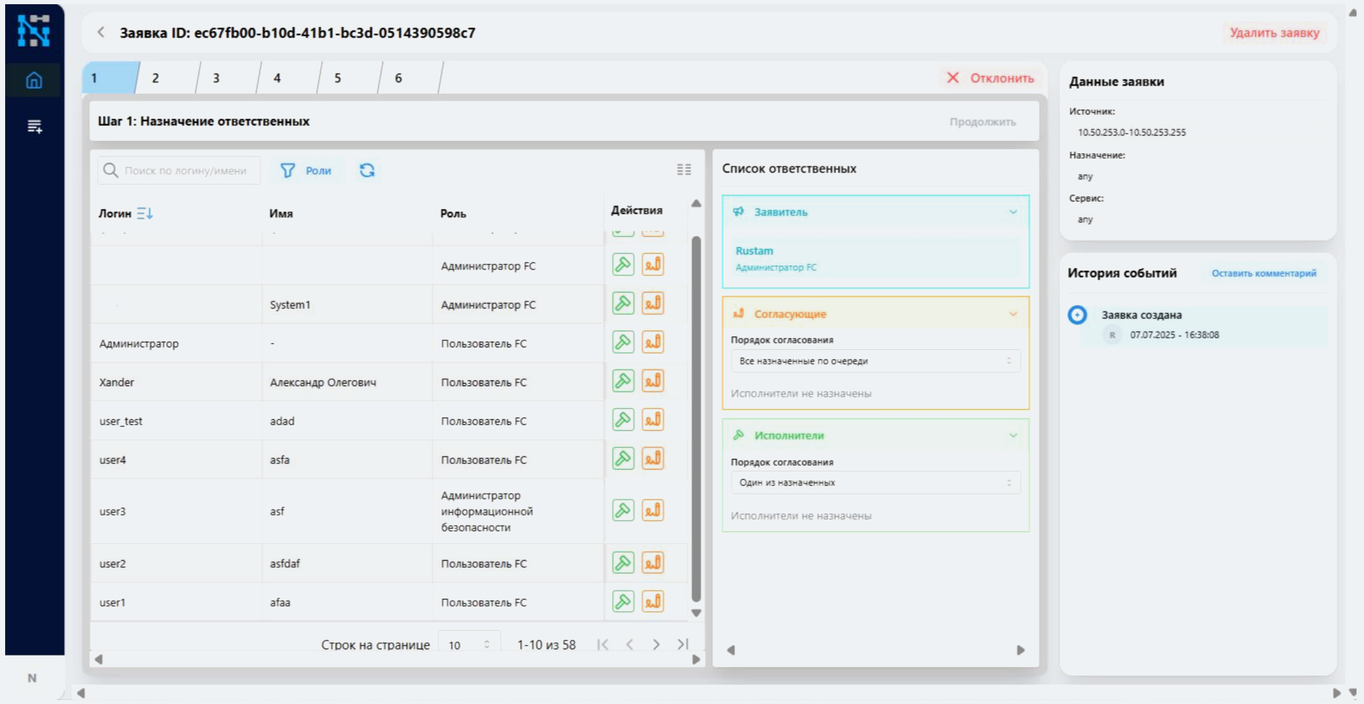
- Напоминание о сроках пересмотра правил.
- Управление доступом.
- Верификация изменений.

УДАЛЕНИЯ ПРАВИЛ

Автоматическое применение изменений

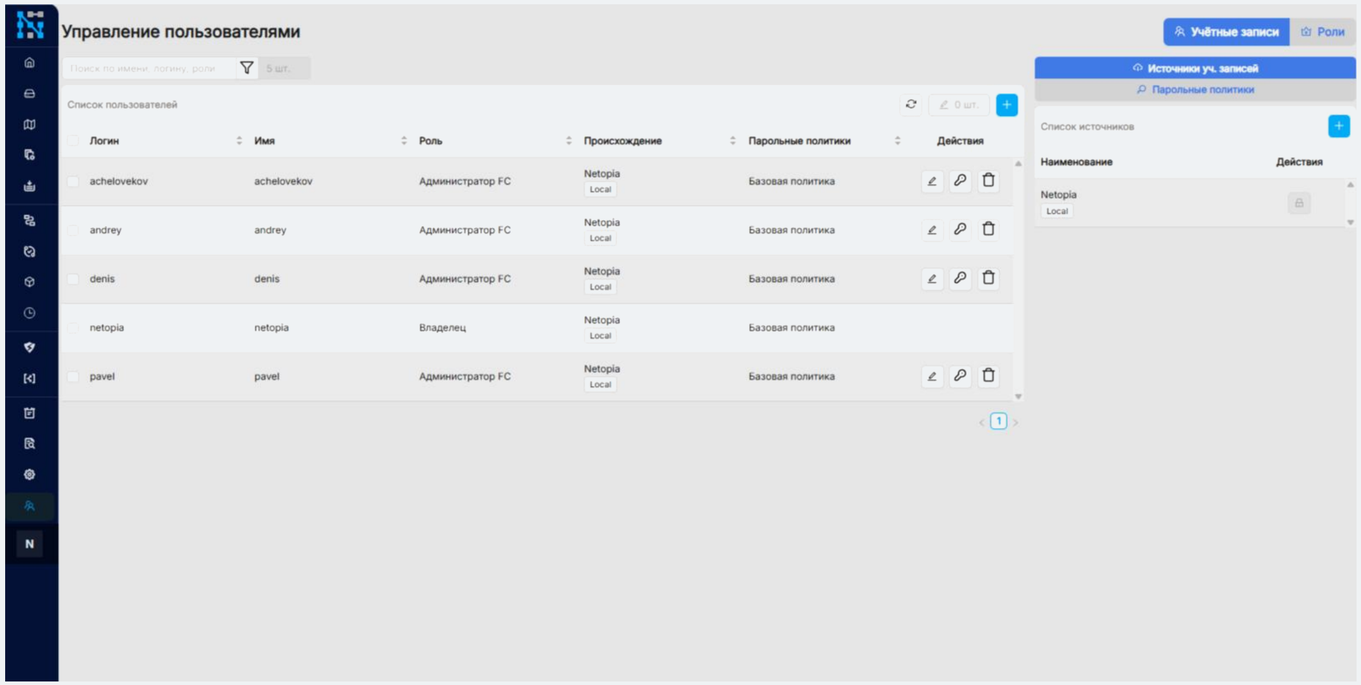
CHANGE MANAGEMENT

netopia.pro
NETWORK SECURITY PLATFORM



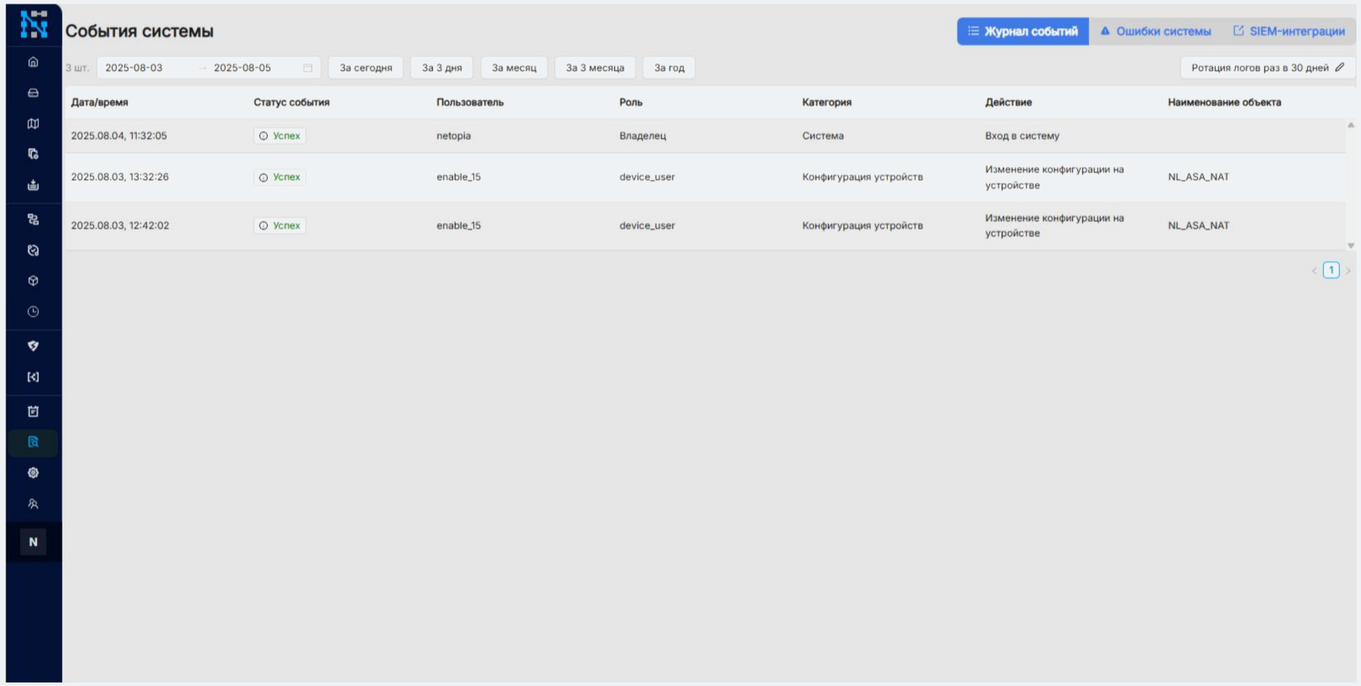
- Управление изменениями политик / конфигураций межсетевых экранов в автоматизированном режиме.
- Внесение и валидация изменений на межсетевых экранах.
- Интеграция с существующими системами управления изменениями в организации (ITSM, PAM, BPM и др.) посредством API.

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 VULNERABILITY CONTROL

netopia.pro
NETWORK SECURITY PLATFORM

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 VULNERABILITY CONTROL

netopia.pro
NETWORK SECURITY PLATFORM

Автоматическая оценка опасности уязвимостей

ВЫЯВЛЕНИЕ УЯЗВИМОСТЕЙ

РАСЧЁТ ВЕКТОРОВ АТАК В КОНТЕКСТЕ СЕТИ

РАСЧЁТ ПРИОРИТЕТОВ И РЕАГИРОВАНИЕ

КАК ЭТО РАБОТАЕТ?

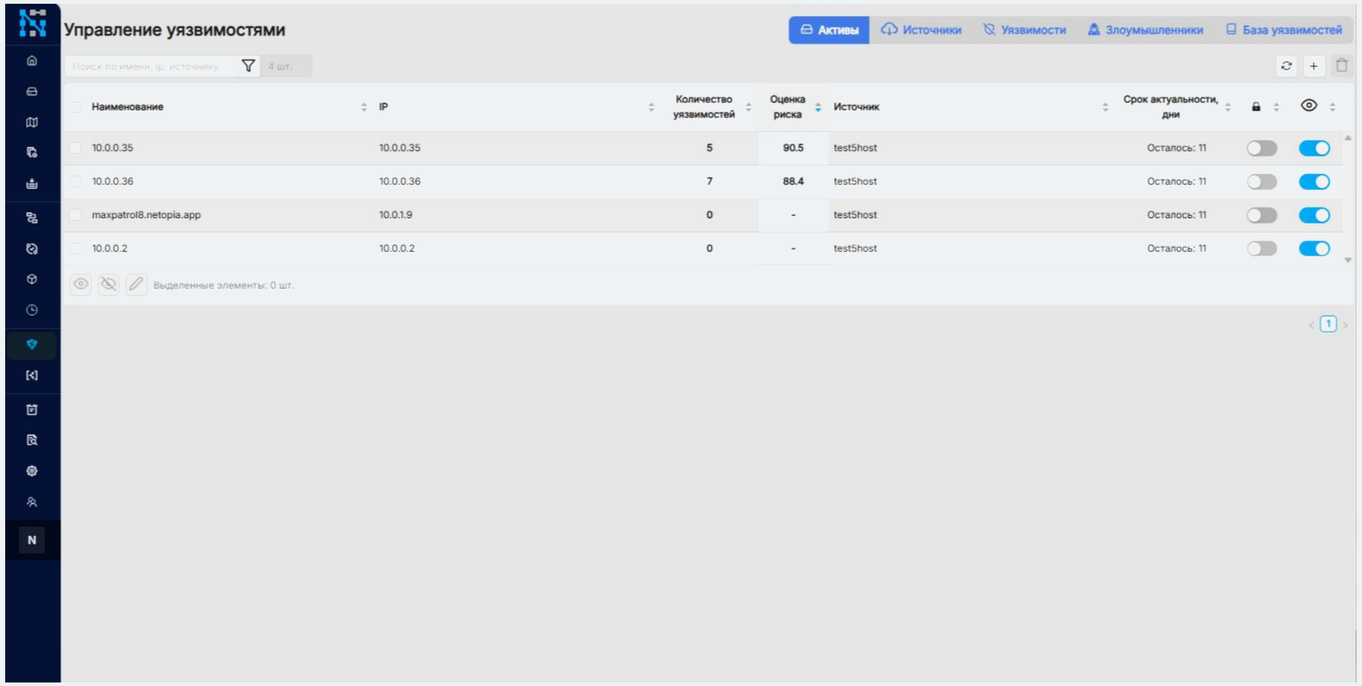
1. Выявление

2. Анализ

3. Приоритизация

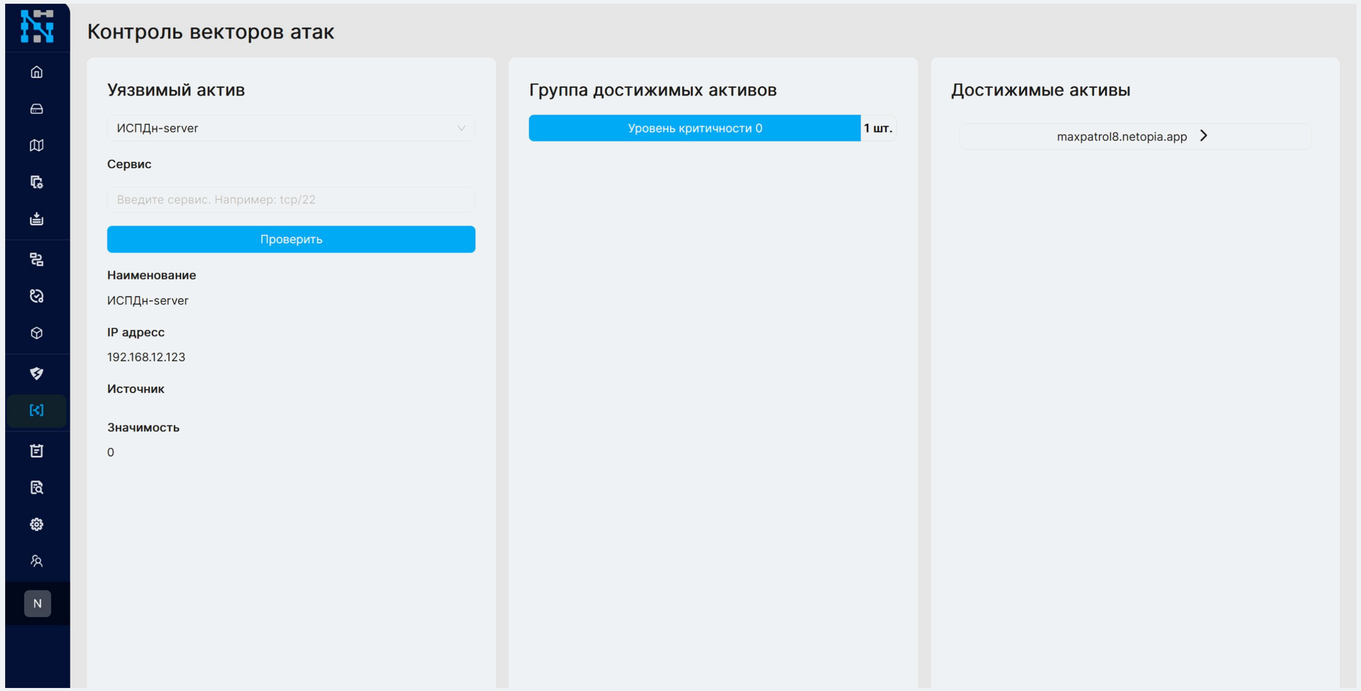
4. Реагирование

АНАЛИЗ И ПРИОРИТИЗАЦИЯ УЯЗВИМОСТЕЙ



- 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
NETWORK SECURITY PLATFORM

Модуль	Описание	Лицензирование
Network Assurance	Анализ соответствия конфигураций сетевых устройств заданным стандартам; ретроспективный анализ изменений конфигураций, анализ настроек на Hardening и Best Practice, построение карты сети и визуализация сетевой инфраструктуры.	По количеству маршрутизирующих устройств.
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. Включает в себя модуль Network Assurance. FA NA
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, на которых будут проводиться изменения политик доступа. Для работы модуля обязательно наличие лицензии «Firewall Assurance». ЛИЦЕНЗИОННЫЕ ТРЕБОВАНИЯ: CM FA
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 «Firewall Assurance» (обязательно) и «Network Assurance». ЛИЦЕНЗИОННЫЕ ТРЕБОВАНИЯ: VC FA NA

NA — Network Assurance

FA — Firewall Assurance

CM — Change Management

VM — Vulnerability Control

ОЦЕНИТЕ ПРЕИМУЩЕСТВА ИСПОЛЬЗОВАНИЯ РЕШЕНИЯ NETOPIA FIREWALL COMPLIANCE!

netopia.pro

NETWORK SECURITY PLATFORM

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