

# КОНТРОЛЬ СОСТОЯНИЯ СЕТИ

С ПЛАТФОРМОЙ  
NETOPIA FIREWALL COMPLIANCE

## Модульность и гибкость

### VULNERABILITY AND TREAT MANAGEMENT

- Интеграция с Vulnerability Management системами и сканерами уязвимостей.
- Маркировка критичных активов.
- Оценка опасности угроз.

- Анализ векторов атак.
- Сверхприоритизация устранения уязвимостей.

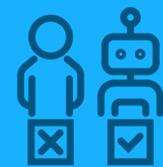
### SECURITY POLICY MANAGEMENT

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

## 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



FIREWALL ASSURANCE



CHANGE MANAGEMENT

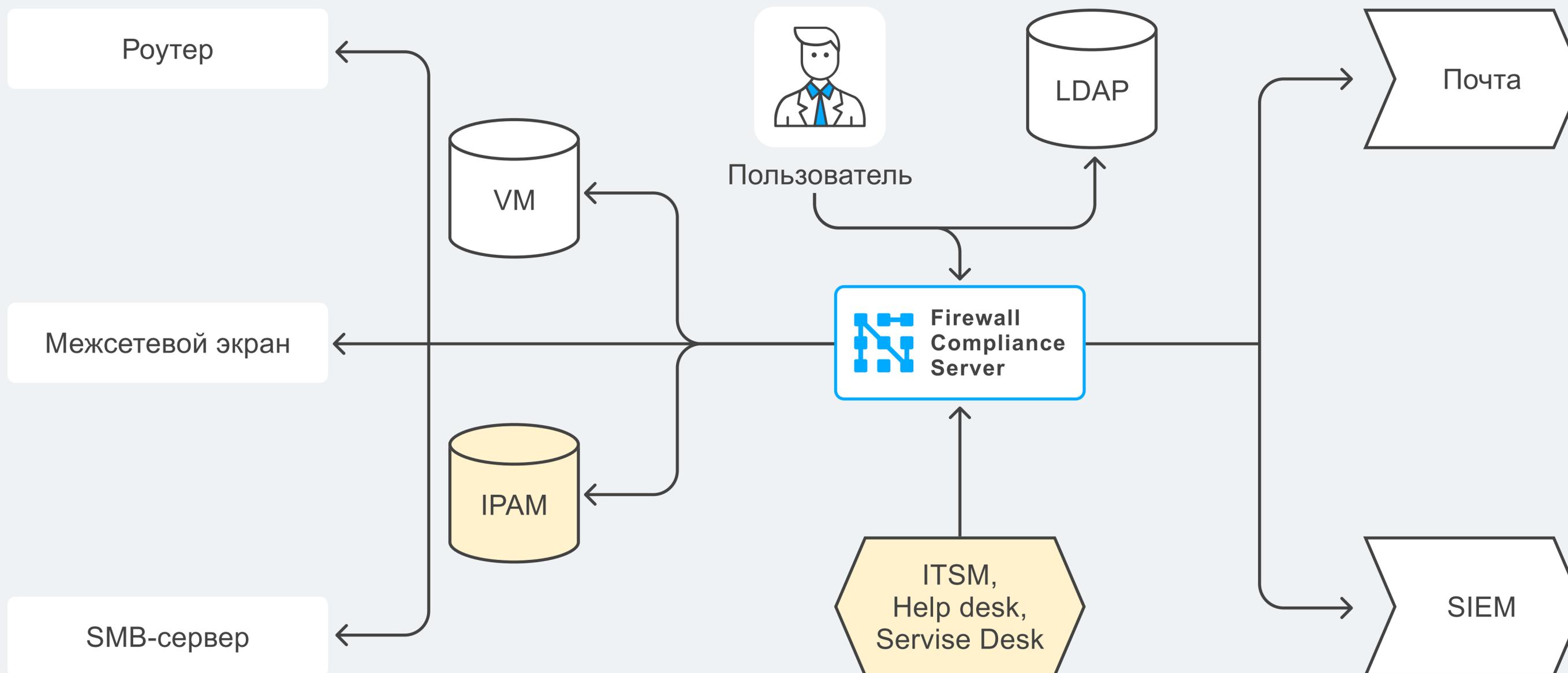


NETWORK ASSURANCE



VULNERABILITY CONTROL

# ТИПОВАЯ СТРУКТУРА ВЗАИМОДЕЙСТВИЯ



# ПОДДЕРЖИВАЕМЫЕ СИСТЕМЫ

Email

BPM-системы

SIEM

AD/LDAP



Vulnerability Management

IPAM

Security Scanner

ITSM

# ИНТЕГРИРУЕМЫЕ СИСТЕМЫ

**NAUMEN**

NAUMEN SERVICE DESK

**BPM**SOFT

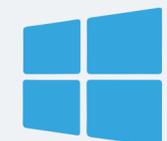
BPM SOFT

**S** Security  
Vision

SECURITY VISION VM

 **positive technologies**

POSITIVE TECHNOLOGIES VM / POSITIVE TECHNOLOGIES MAXPATROI 8

 Microsoft  
**Active Directory**

MICROSOFT ACTIVE DIRECTORY / LDAP



IPAM



SIEM

ДОБАВЛЕНИЕ СИСТЕМ ВОЗМОЖНО ПО ЗАПРОСУ

# СПИСОК ПОДДЕРЖИВАЕМОГО ОБОРУДОВАНИЯ И ПО



**IOS**

ASA Firewall



UserGate

**FORTINET**



**HUAWEI**



**CHECK POINT**

*Контигент*

**с•терра**



**positive technologies**



**В БЛИЖАЙШЕЕ ВРЕМЯ:**



## NETWORK ASSURANCE ПОМОГАЕТ ПОНЯТЬ

**КАК ВЫГЛЯДИТ НАША СЕТЬ?**

**КАК СКОНФИГУРИРОВАНО СЕТЕВОЕ  
ОБОРУДОВАНИЕ?**

**КАК СЕГМЕНТИРОВАНА НАША СЕТЬ?**

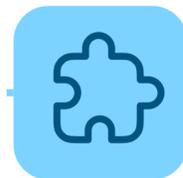
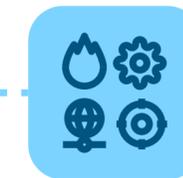
## Полная видимость сети

ИНТЕРАКТИВНАЯ КАРТА СЕТИ

КОНТРОЛЬ КОНФИГУРАЦИЙ

КОНТРОЛЬ ПОЛИТИКИ СЕГМЕНТИРОВАНИЯ

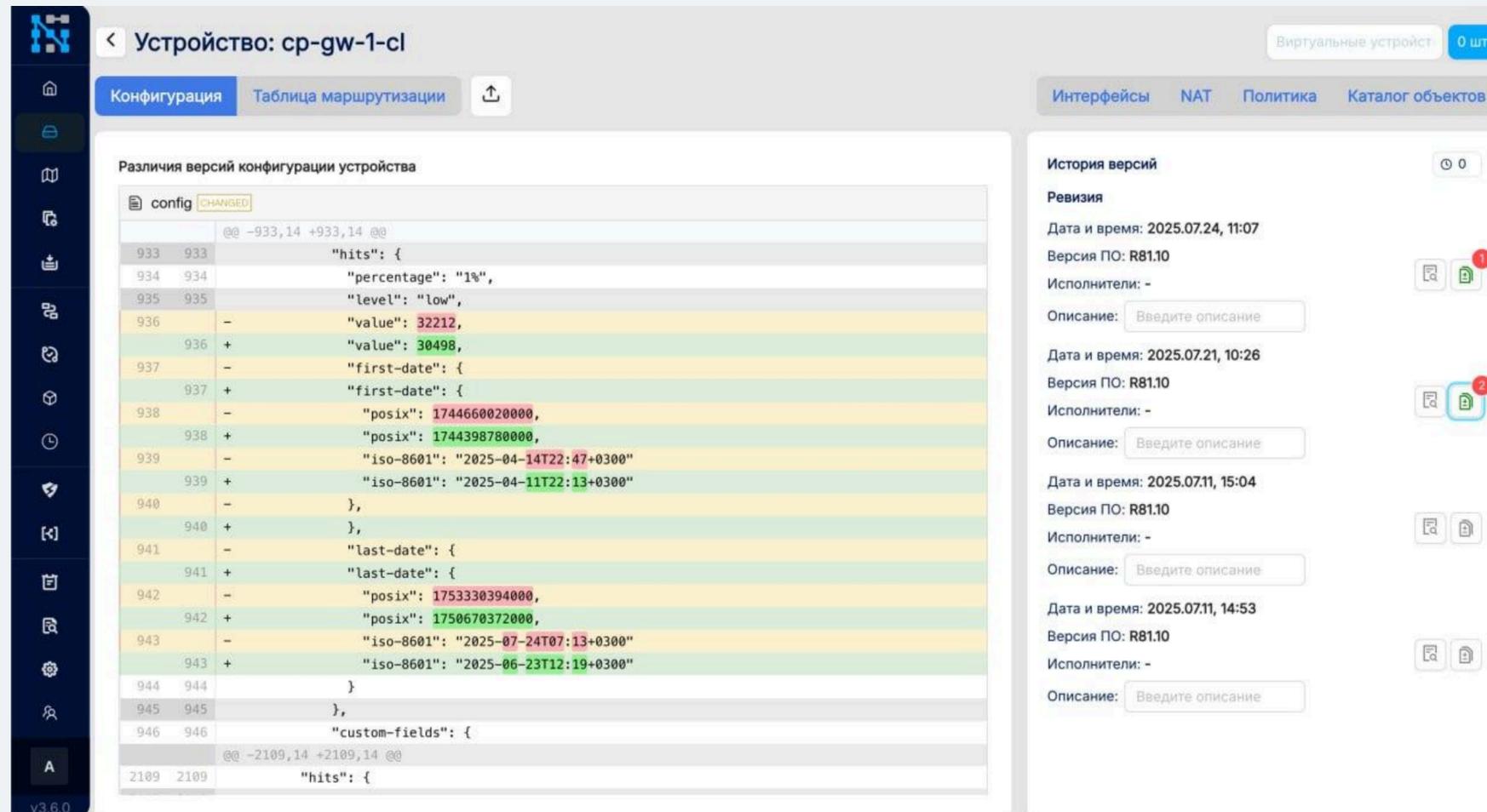
# КАК ЭТО РАБОТАЕТ?



1. Сбор и нормализация

2. Моделирование

3. Детальный анализ



Устройство: sr-gw-1-cl

Виртуальные устройства: 0 шт.

Конфигурация | Таблица маршрутизации

Интерфейсы | NAT | Политика | Каталог объектов

### Различия версий конфигурации устройства

```
config CHANGED
@@ -933,14 +933,14 @@
933 933      "hits": {
934 934      "percentage": "1%",
935 935      "level": "low",
936 -      "value": 32212,
936 +      "value": 30498,
937 -      "first-date": {
937 +      "first-date": {
938 -      "posix": 1744660020000,
938 +      "posix": 1744398780000,
939 -      "iso-8601": "2025-04-14T22:47+0300"
939 +      "iso-8601": "2025-04-11T22:13+0300"
940 -      },
940 +      },
941 -      "last-date": {
941 +      "last-date": {
942 -      "posix": 1753330394000,
942 +      "posix": 1750670372000,
943 -      "iso-8601": "2025-07-24T07:13+0300"
943 +      "iso-8601": "2025-06-23T12:19+0300"
944 944      }
945 945      },
946 946      "custom-fields": {
@@ -2109,14 +2109,14 @@
2109 2109      "hits": {
```

### История версий

Ревизия

Дата и время: 2025.07.24, 11:07  
Версия ПО: R81.10  
Исполнители: -  
Описание:

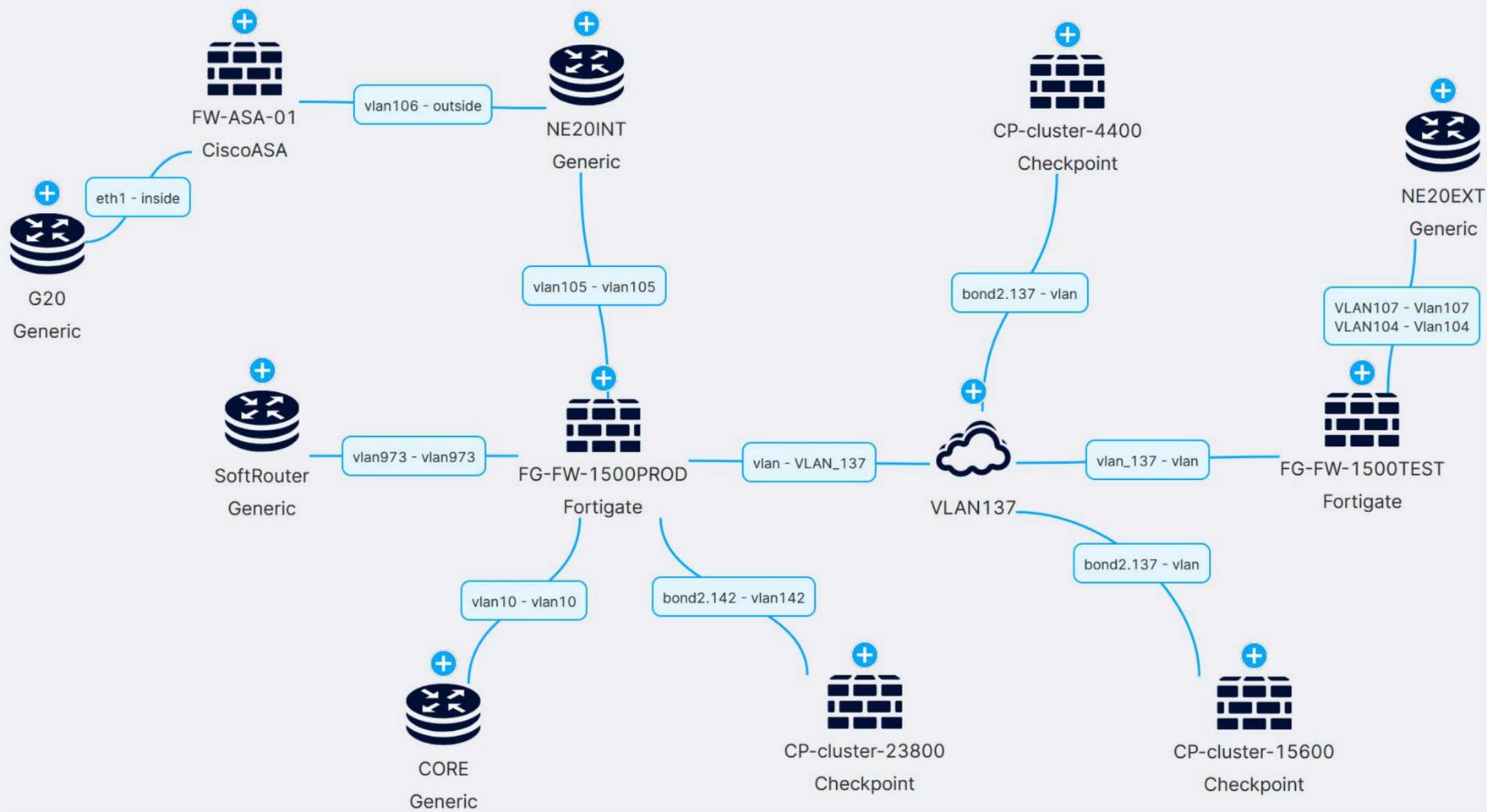
Дата и время: 2025.07.21, 10:26  
Версия ПО: R81.10  
Исполнители: -  
Описание:

Дата и время: 2025.07.11, 15:04  
Версия ПО: R81.10  
Исполнители: -  
Описание:

Дата и время: 2025.07.11, 14:53  
Версия ПО: R81.10  
Исполнители: -  
Описание:

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

# ПОСТРОЕНИЕ КАРТЫ СЕТИ



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

# ДЕТАЛЬНЫЙ АНАЛИЗ

Контроль конфигураций устройств

Поиск по названию Перезапустить все проверки

Устройства Переменные Проверки

Устройства	Проверки
fw-ispdn-xfw-cl  Фаервол  Firewall  Firewall  VIPNet  VIPNet	1 / 5 >
ср-gw-1-cl  Фаервол  Check Point  Check Point  Firewall  Firewall	2 / 32 >
NL_BGP-AS-02  Роутер  Cisco IOS  Cisco IOS  Router  Router	5 / 27 >
rt-ispdn-vesr-1  Фаервол  Eltex  Eltex  Firewall  Firewall	2 / 26 >
fw-ispdn-ug7-1  Фаервол  Firewall  Firewall  UserGate  UserGate	1 / 7 >
NL_BGP-AS-01  Роутер  Cisco IOS  Cisco IOS	5 / 27 >

Выделенные элементы: 0 шт. Изменить связи с тегами

1 2 > 10 / стр. v

Проверки устройства: NL\_BGP-AS-02 27 шт.

Наименование	Статус
100 Настройка типа шифрования пароля >	✗ Не пройдена
101 Защита от стандартных паролей >	✓ Пройдена
102 Настройка AA для подключения/входа в исполнительный режим >	✗ Не пройдена
103 Установка задержки между попытками авторизации >	✗ Не пройдена
104 Установление порога свободной памяти для AAA >	✗ Не пройдена
105 Настройка парольной политики >	✗ Не пройдена
107 Включение SSHv2 >	✗ Не пройдена
108 Защита от пакетов с недействительным адресом >	✓ Пройдена
109 Защита от использования туннельных интерфейсов >	✗ Не пройдена
110 Запрет использование ProxуARP >	✗ Не пройдена

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

## FIREWALL ASSURANCE ПОМОГАЕТ ПОНЯТЬ

**ОПТИМАЛЬНЫ ЛИ ВАШИ ПРАВИЛА?**

**СООТВЕТСТВУЮТ ЛИ ПРАВИЛА ЗОНАМ  
БЕЗОПАСНОСТИ?**

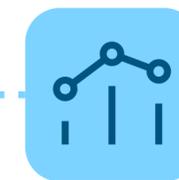
**КАК МЕНЯЮТСЯ ПРАВИЛА ДОСТУПА?**

АНАЛИЗ ПРАВИЛ ДОСТУПА  
И ИХ ОПТИМИЗАЦИЯ

КОНТРОЛЬ  
ЗОН БЕЗОПАСНОСТИ

КОНТРОЛЬ ИЗМЕНЕНИЙ  
ПРАВИЛ ДОСТУПА

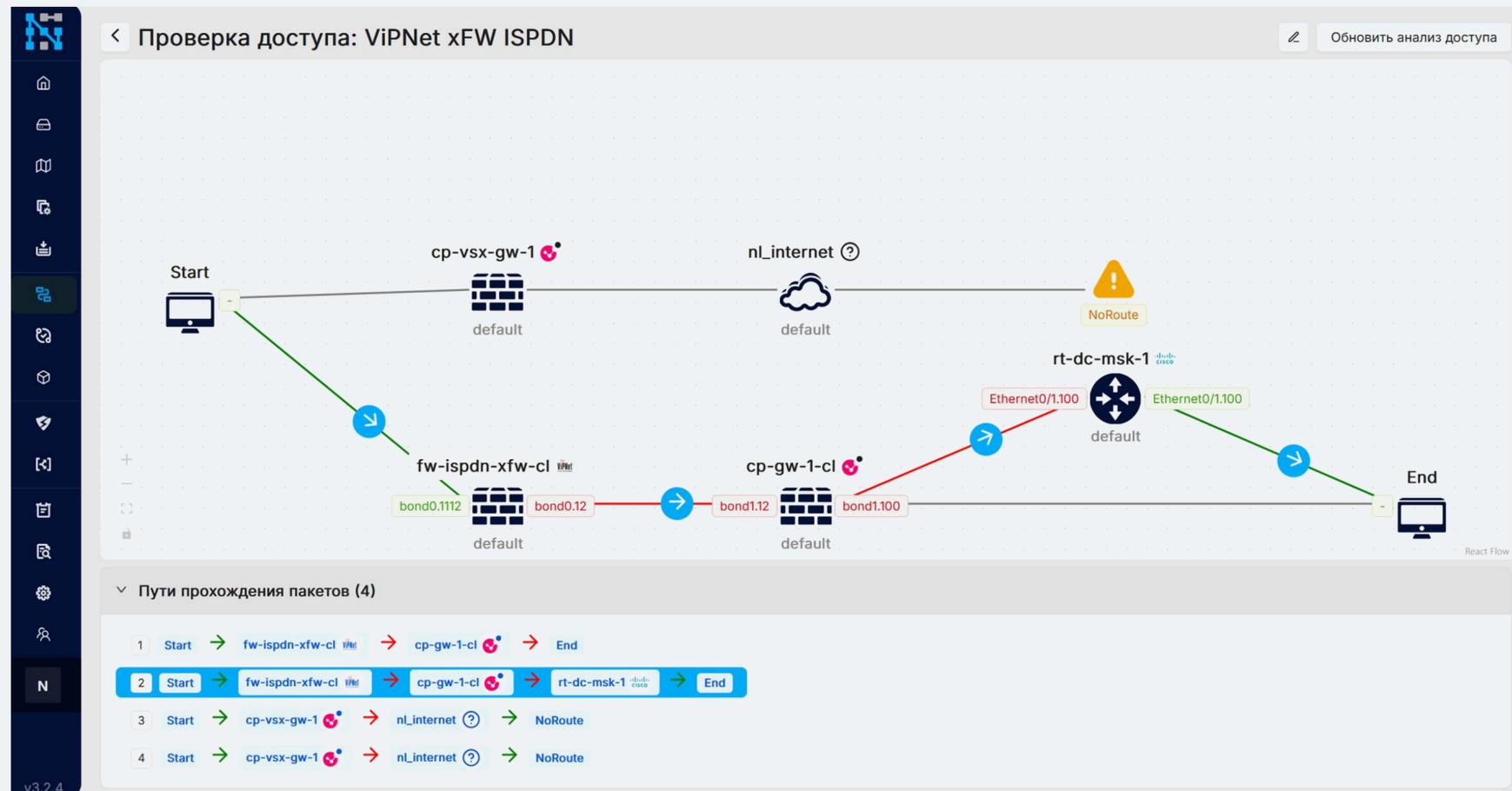
## КАК ЭТО РАБОТАЕТ?



1. Сбор и нормализация

2. Анализ. Настраиваемые  
задачи и проверки

3. Отчёты и реагирование



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

# ОПТИМИЗАЦИЯ СЕТЕВЫХ ПРАВИЛ

Анализ правил

Фильтрация по наименованию/вендору  
Введите подстроку

Параметры поиска по правилам  
Параметры поиска не применены

Параметры оптимизации  
Параметры фильтрации не применены

№	Вендор/Устройство	Имя правила	Имя политики	Действие	Интерфейс	Источник/Назначение	Сервис	Описание	Оптимизации
1	ideco	input_1	input	deny	any	obj_host_192.168.22.100/32 obj_host_192.168.19.110/32	icmp		<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
2	ideco	input_5	input	deny	any	any	tcp:[0-65535]		<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
3	ideco	input_8	input	deny	any	obj_host_172.16.254.100/32 obj_host_192.168.19.110/32	test		<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
4	ideco	input_2	input	deny	any	any	tcp:[0-65535]		<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
5	ideco	input_3	input	accept	any	any	gre		<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
6	ideco	input_10	input	accept	any	any	gre		<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
1	ideco	forward_8	forward	accept	any	Servers net LAN	test		<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
2	ideco	forward_9	forward	accept	any	obj_host_172.16.254.100/32 any	test		<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
3	ideco	forward_1	forward	accept	any	Servers range any	tcp:[0-65535]		<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>

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

# ОПТИМИЗАЦИЯ ОБЪЕКТОВ ПОЛИТИК

Анализ объектов

599 шт.

Имя объекта

Наименование	Устройство	Тип	Связанные правила	Вложенные объекты	Состояние
[tcp:[110,995]]	fw-ispdn-ug7-1	ServiceGr...	Untrusted:4	Service:tcp:[110,995]	✖ 📄
[tcp:[161,162]]	fw-ispdn-ug7-1	ServiceGr...	Cluster:2 Management:2	Service:tcp:[161,162]	✖ 📄
[tcp:[179]]	fw-ispdn-ug7-1	ServiceGr...	Untrusted:6	Service:tcp:[179]	✖ 📄
[tcp:[2200]]	fw-ispdn-ug7-1	ServiceGr...	Cluster:6 Management:6	Service:tcp:[2200]	✖ 📄
[tcp:[22]]	NL_ASA-NAT	ServiceGr...	dmz_access_in line 1:1 as_access_in line 1:1 + 1 ...	Service:tcp:[22]	✖ 📄
[tcp:[25,465,587]]	fw-ispdn-ug7-1	ServiceGr...	Untrusted:3	Service:tcp:[25,465,587]	✖ 📄
[tcp:[25]]	NL_ASA-NAT	ServiceGr...	inside_access_in line 2:2 inside_access_in line 3:3 + 1 ...	Service:tcp:[25]	✖ 📄
[tcp:[321], udp:[321]]	rt-ispdn-vesr-1	ServiceGr...	Нет данных	Service:tcp:[321] Service:udp:[321] + 2 ...	⚠ 📄
[tcp:[321], udp:[321]]	rt-ispdn-vesr-1	ServiceGr...	Нет данных	Service:tcp:[321] Service:udp:[321] + 2 ...	⚠ 📄
[tcp:[4040]]	fw-ispdn-ug7-1	ServiceGr...	Management:4	Service:tcp:[4040]	✖ 📄

< 1 ... 18 19 20 21 22 ... 30 > 20 записей на странице

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

## СОЗДАНИЯ ПРАВИЛ

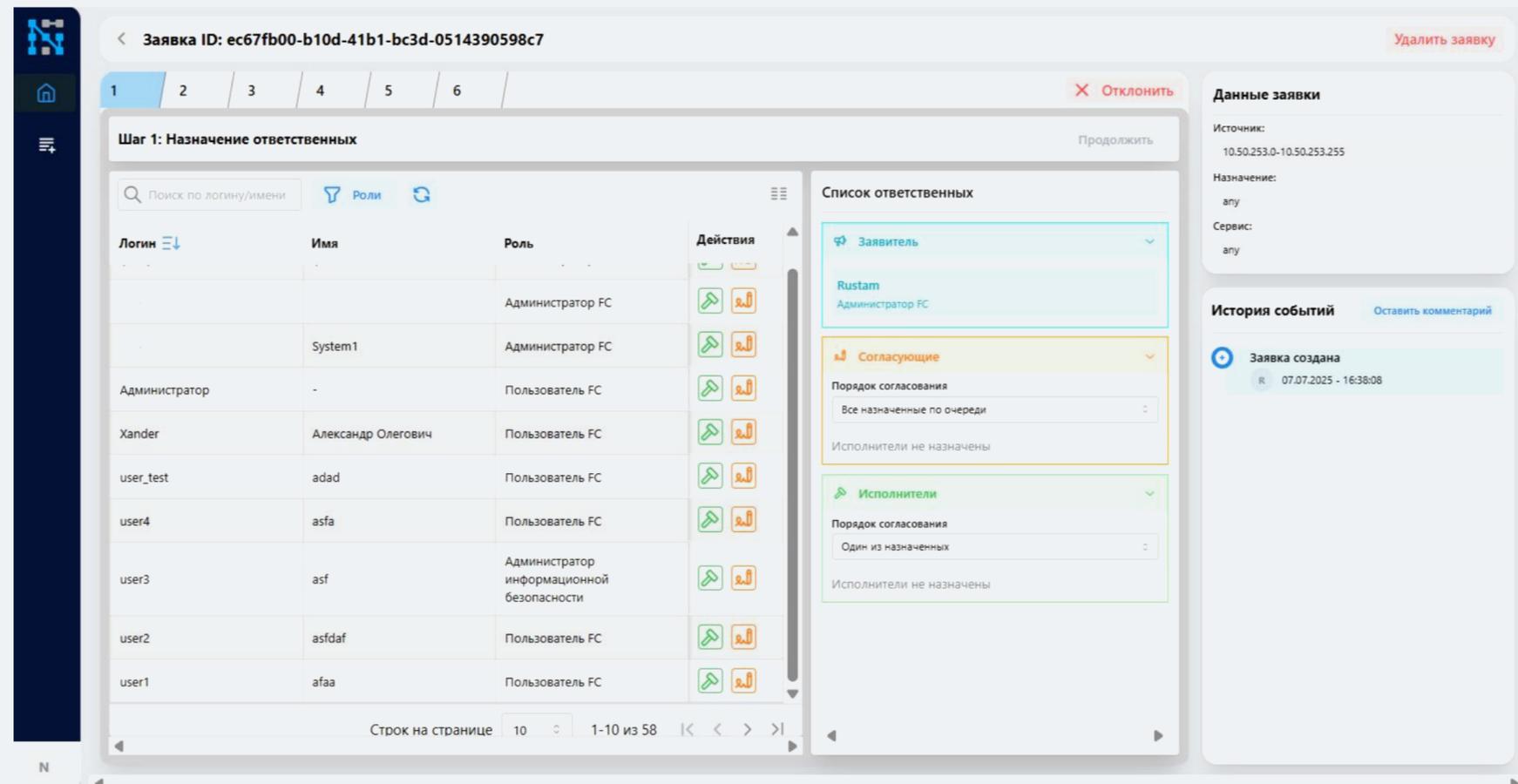
- Анализ маршрута.
- Определение задействованных устройств.
- Оценка влияния планируемых изменений.

## ПЕРЕСМОТРА ПРАВИЛ (РЕСЕРТИФИКАЦИИ)

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

## УДАЛЕНИЯ ПРАВИЛ

Автоматическое применение изменений

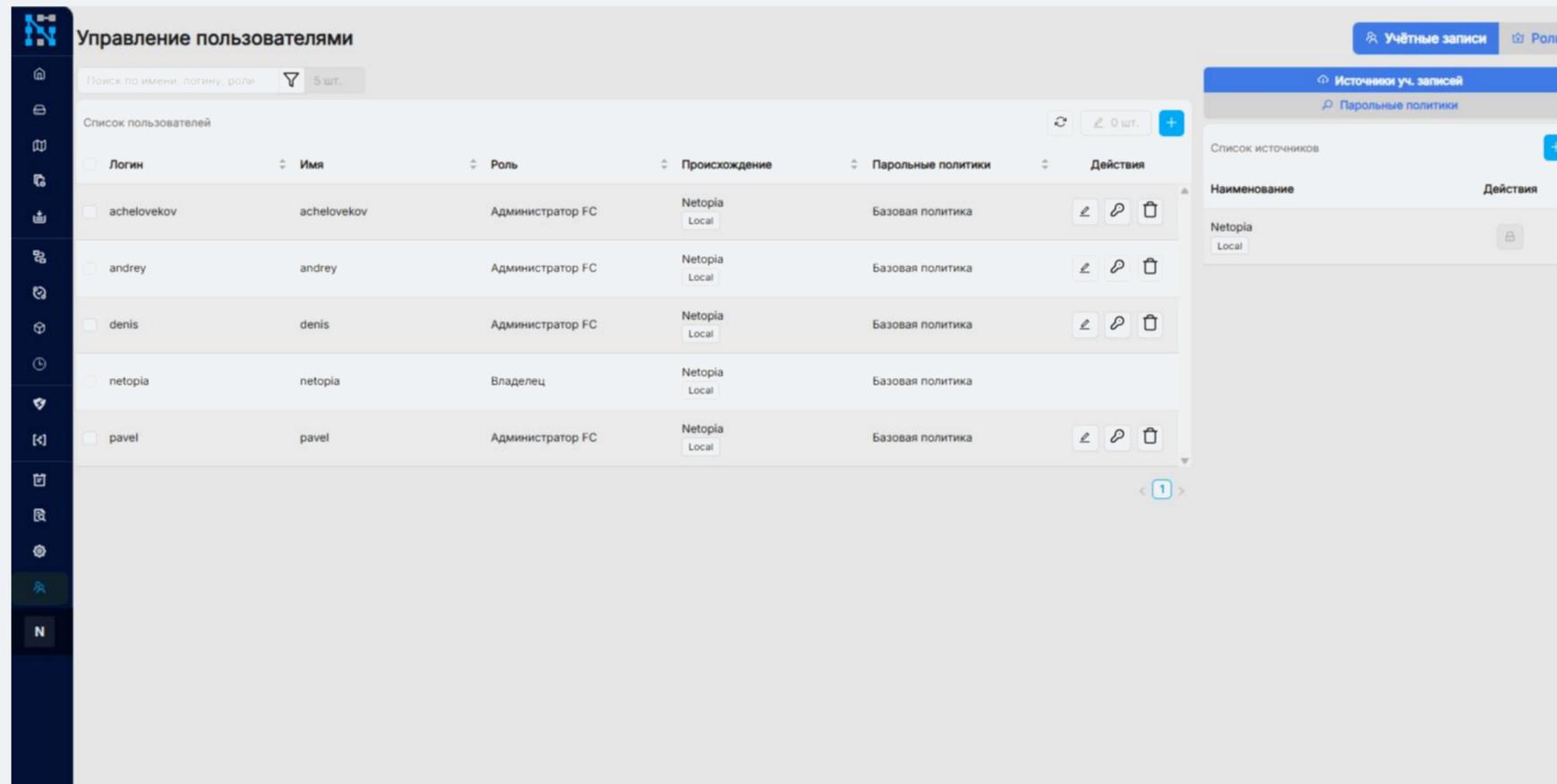


The screenshot displays the Netopia Pro Change Management interface. At the top, a request ID is shown: "Заявка ID: ec67fb00-b10d-41b1-bc3d-0514390598c7". The interface is divided into several sections:

- Шаг 1: Назначение ответственных** (Step 1: Assigning responsible parties): A table with columns for "Логин" (Login), "Имя" (Name), "Роль" (Role), and "Действия" (Actions). The table lists several users and their roles, including "Администратор FC" and "Пользователь FC".
- Список ответственных** (List of responsible parties): A section for assigning roles to specific users. It includes a dropdown for "Заявитель" (Requester) with "Rustam" selected, and two sections for "Согласующие" (Approver) and "Исполнители" (Executor), each with a dropdown for "Порядок согласования" (Approval order) and a note "Исполнители не назначены" (Executors not assigned).
- Данные заявки** (Request details): A section with fields for "Источник" (Source), "Назначение" (Assignment), and "Сервис" (Service).
- История событий** (Event history): A section showing a log of events, including "Заявка создана" (Request created) on 07.07.2025 at 16:38:08.

- 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



Управление пользователями

Поиск по имени, логину, роли 5 шт.

Список пользователей

Логин	Имя	Роль	Происхождение	Парольные политики	Действия
achelovekov	achelovekov	Администратор FC	Netopia Local	Базовая политика	✎ ✎ 🗑
andrey	andrey	Администратор FC	Netopia Local	Базовая политика	✎ ✎ 🗑
denis	denis	Администратор FC	Netopia Local	Базовая политика	✎ ✎ 🗑
netopia	netopia	Владелец	Netopia Local	Базовая политика	
pavel	pavel	Администратор FC	Netopia Local	Базовая политика	✎ ✎ 🗑

Учётные записи Роли

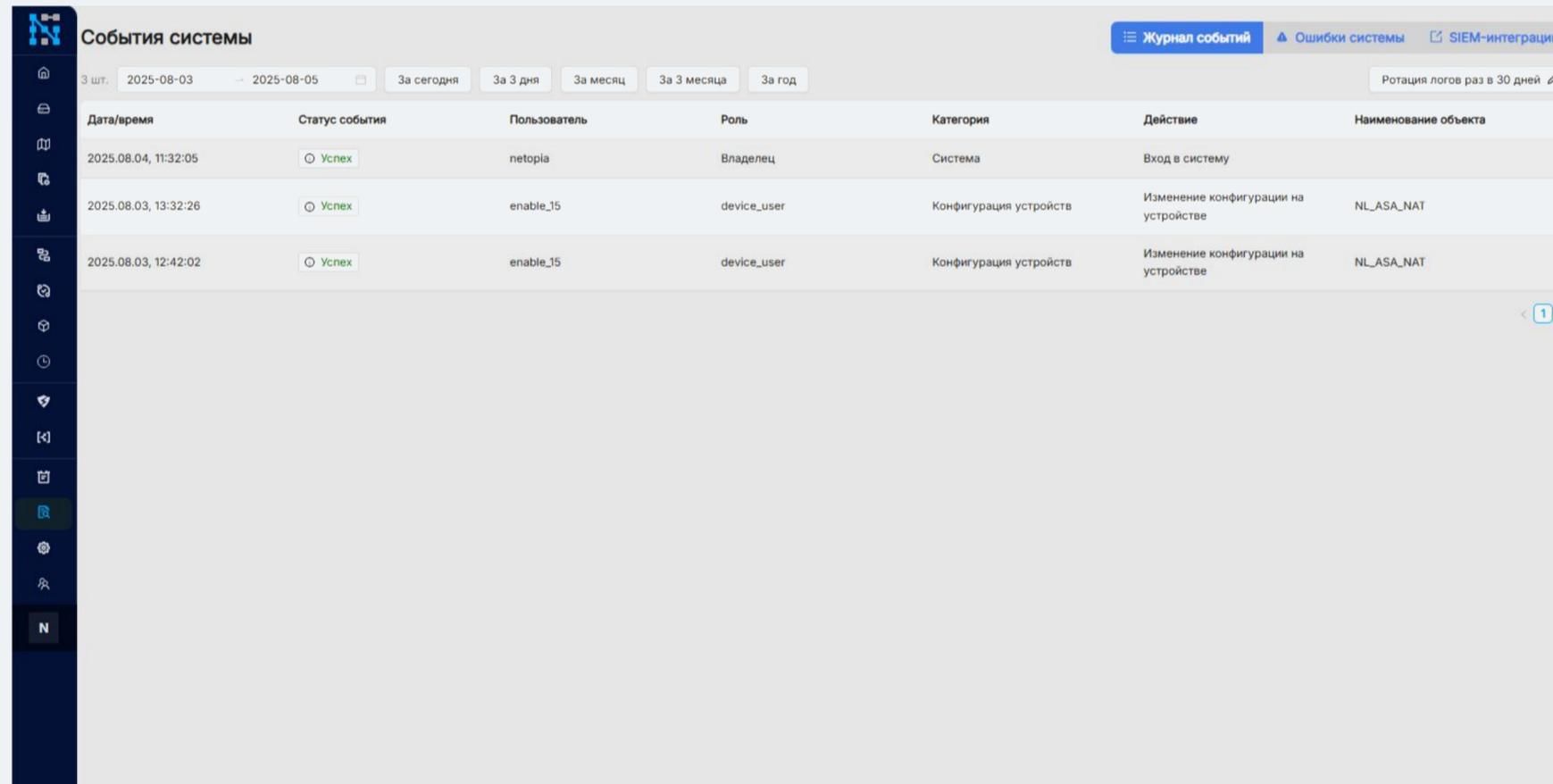
Источники уч. записей Парольные политики

Список источников

Наименование	Действия
Netopia Local	🔒

- 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



The screenshot shows the 'События системы' (System Events) interface. It features a top navigation bar with tabs for 'Журнал событий' (Event Log), 'Ошибки системы' (System Errors), and 'SIEM-интеграции' (SIEM Integrations). Below the navigation bar, there are filters for the number of items (3 шт.), a date range (2025-08-03 to 2025-08-05), and time-based filters (За сегодня, За 3 дня, За месяц, За 3 месяца, За год). A 'Ротация логов раз в 30 дней' (Log rotation every 30 days) option is also visible. The main content area is a table with the following columns: 'Дата/время' (Date/Time), 'Статус события' (Event Status), 'Пользователь' (User), 'Роль' (Role), 'Категория' (Category), 'Действие' (Action), and 'Наименование объекта' (Object Name). The table contains three entries, all with a status of 'Успех' (Success).

Дата/время	Статус события	Пользователь	Роль	Категория	Действие	Наименование объекта
2025.08.04, 11:32:05	Успех	netopia	Владелец	Система	Вход в систему	
2025.08.03, 13:32:26	Успех	enable_15	device_user	Конфигурация устройств	Изменение конфигурации на устройстве	NL_ASA_NAT
2025.08.03, 12:42:02	Успех	enable_15	device_user	Конфигурация устройств	Изменение конфигурации на устройстве	NL_ASA_NAT

Возможность отслеживать все произошедшие события в системе.

## 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?**

## Автоматическая оценка опасности уязвимостей

ВЫЯВЛЕНИЕ УЯЗВИМОСТЕЙ

РАСЧЁТ ВЕКТОРОВ АТАК В КОНТЕКСТЕ СЕТИ

РАСЧЁТ ПРИОРИТЕТОВ И РЕАГИРОВАНИЕ

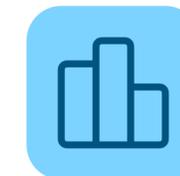
# КАК ЭТО РАБОТАЕТ?



1. Выявление



2. Анализ



3. Приоритизация



4. Реагирование

# АНАЛИЗ И ПРИОРИТИЗАЦИЯ УЯЗВИМОСТЕЙ

Управление уязвимостями

Активы | Источники | Уязвимости | Злоумышленники | База уязвимостей

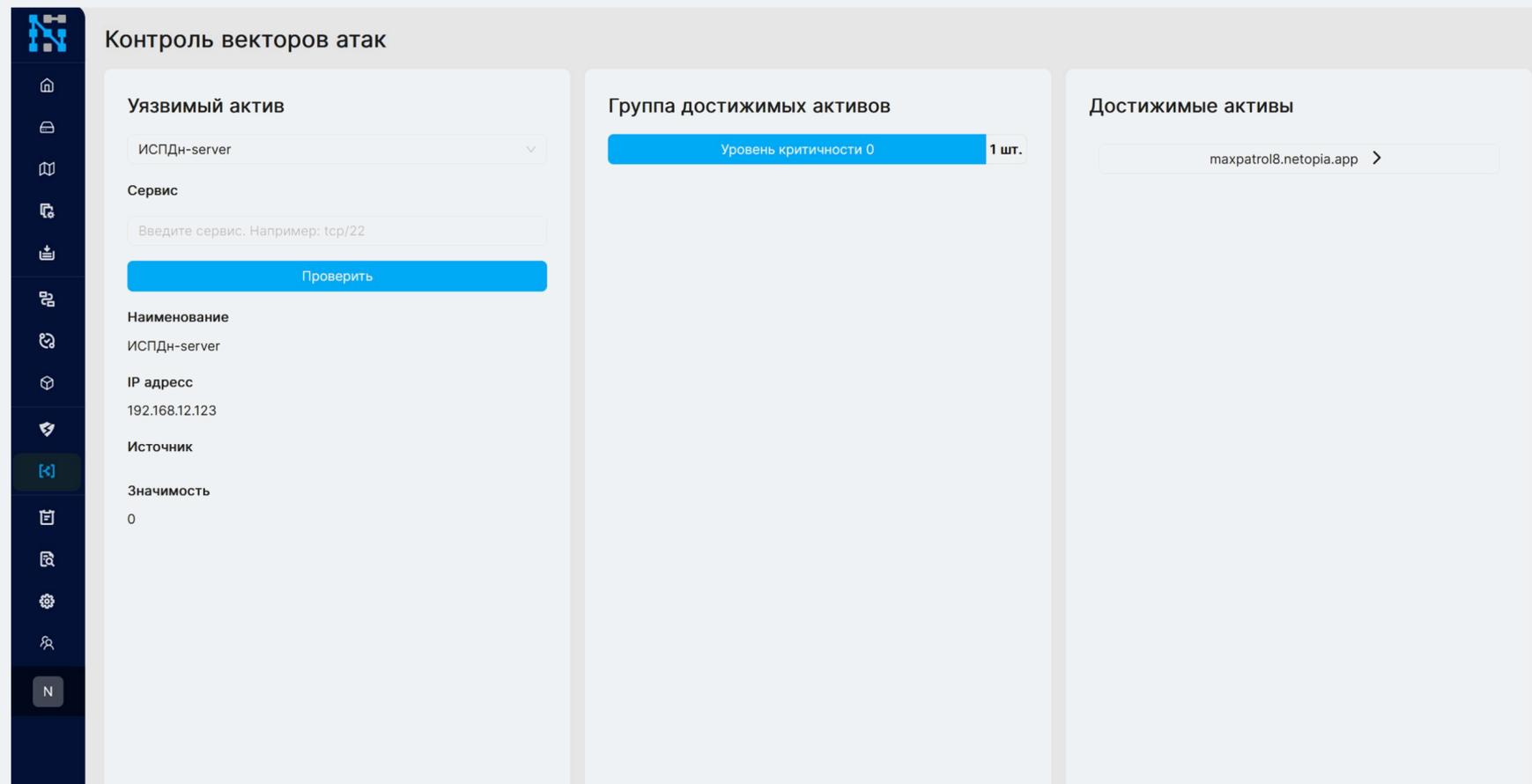
Поиск по имени, IP, источнику 4 шт.

Наименование	IP	Количество уязвимостей	Оценка риска	Источник	Срок актуальности, дни		
<input type="checkbox"/> 10.0.0.35	10.0.0.35	5	90.5	test5host	Осталось: 11	<input type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/> 10.0.0.36	10.0.0.36	7	88.4	test5host	Осталось: 11	<input type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/> maxpatrol8.netopia.app	10.0.1.9	0	-	test5host	Осталось: 11	<input type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/> 10.0.0.2	10.0.0.2	0	-	test5host	Осталось: 11	<input type="checkbox"/>	<input checked="" type="checkbox"/>

Выделенные элементы: 0 шт.

- **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



**Контроль векторов атак**

**Уязвимый актив**

ИСПДн-server

Сервис

Введите сервис. Например: tcp/22

Проверить

Наименование  
ИСПДн-server

IP адресс  
192.168.12.123

Источник

Значимость  
0

**Группа достижимых активов**

Уровень критичности 0 1 шт.

**Достижимые активы**

maxpatrol8.netopia.app >

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

Модуль	Описание	Лицензирование
<b>Network Assurance</b>	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.
<b>Firewall Assurance</b>	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. <b>FA NA</b>
<b>Change Management</b>	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». <b>ЛИЦЕНЗИОННЫЕ ТРЕБОВАНИЯ:</b> <b>CM FA</b>
<b>Vulnerability Control</b>	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». <b>ЛИЦЕНЗИОННЫЕ ТРЕБОВАНИЯ:</b> <b>VC FA NA</b>

**NA** — Network Assurance

**FA** — Firewall Assurance

**CM** — Change Management

**VM** — Vulnerability Control

# ОЦЕНИТЕ ПРЕИМУЩЕСТВА ИСПОЛЬЗОВАНИЯ РЕШЕНИЯ NETOPIA FIREWALL COMPLIANCE!



## 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 отечествен-  
ного ПО — 17109

Резиденты  
Сколково



ПРЕМИЯ  
ЦИФРОВЫЕ  
ВЕРШИНЫ 2025

+7 (495) 255-35-82 / [info@netopia.pro](mailto:info@netopia.pro)