



ПРОБЛЕМАТИКА УПРАВЛЕНИЯ И КОНТРОЛЯ БОЛЬШОЙ РАСПРЕДЕЛЁННОЙ СЕТИ

Миляр Александр Валерьевич

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



Отсутствие единообразия и комплаенса конфигураций стандартам

Большая инфраструктура: в одной голове невозможно держать все правила настройки

Человеческий фактор: ошибки случаются – это нормально и ожидаемо

Нет возможности сверки изменений ретроспективно для анализа проблемы



Устройство: br-rostov-st-1

Конфигурация

Таблица маршрутизации

Интерфейсы

NAT

Политика

Каталог объектов

Различия версий конфигурации устройства

config

80 80 crypto map MAP_PSK

81 81 !

82 82 interface GigabitEthernet0/2

83 - description LA

83 + description LAN

84 84 ip address 172.16.4.1 255.255.255.0

85 85 !

86 86 interface GigabitEthernet0/3

История версий

Дата	Действия
2025.02.18, 12:03:53	✓ 🔍 📄¹
2025.02.18, 12:02:20	✓ 🔍 📄
2025.02.18, 11:56:44	✓ 🔍 📄²
2025.02.17, 17:59:22	✓ 🔍 📄

- Централизованный сбор конфигурации сетевых устройств.
- Ретроспективный анализ изменений конфигурации и контроль изменений.

Контроль конфигураций устройств

Устройства

Переменные

Проверки

Поиск по названию

11 шт.

Перезапустить все проверки

Устройства

Проверки

fw-ispdn-xfw-cl

Фаервол

1 / 5 >

cp-gw-1-cl

Фаервол

2 / 32 >

NL_BGP-AS-02

Роутер

5 / 27 >

rt-ispdn-vesr-1

Фаервол

2 / 26 >

fw-ispdn-ug7-1

Фаервол

1 / 7 >

Выделенные элементы: 0 шт.

Изменить связи с тегами

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

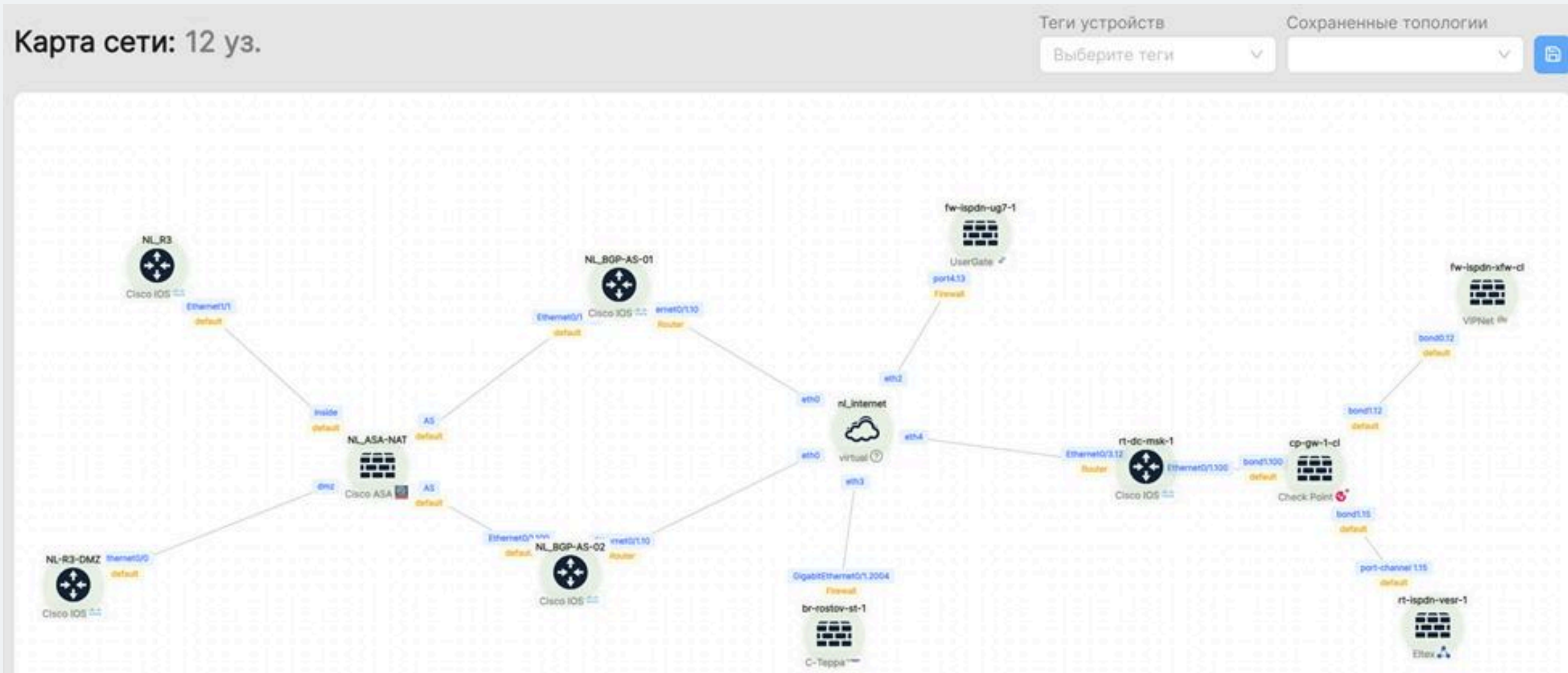
107 Включение SSHv2 >

✗ Не пройдена

108 Защита от пакетов с недействительным

✓ Пройдена

- Приведение настроек в соответствии с корпоративным стандартом (шифрование паролей, установка banner login, настройка NTP/DNS и тд).
- Автоматический анализ конфигурации на best practice и hardening гайды.



Построение карты сети.

Большое количество межсетевых экранов, разные сотрудники управляют правилами доступа, растёт количество правил

Сложность и долгая диагностика отсутствия или наличия доступа

Недостаточный контроль на межсегментный доступ приводит к появлению скрытых доступов



< Затенение

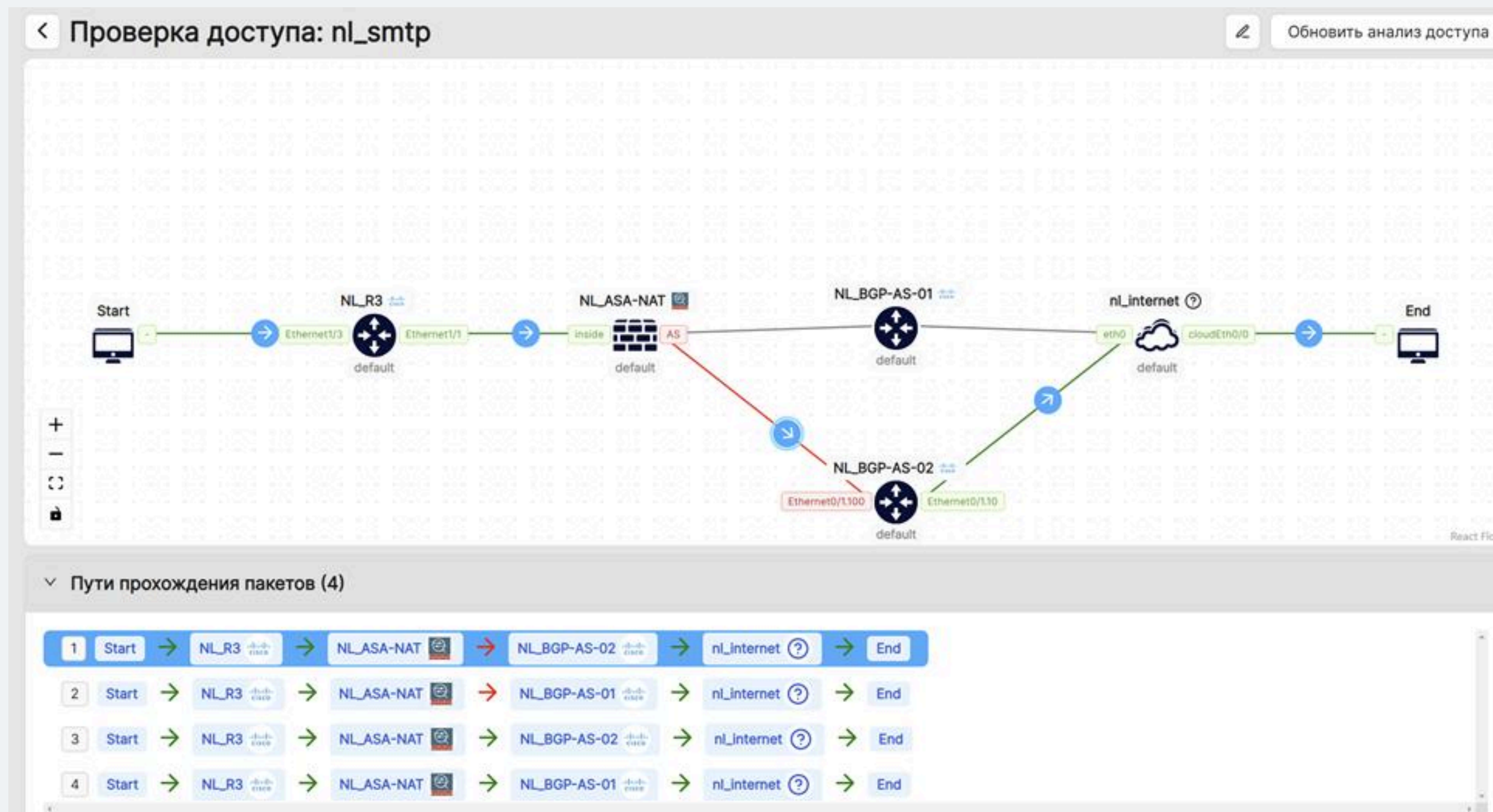
Правило

№	Имя	Входящий интерфейс	Исходящий интерфейс	Источник	Назначение	Сервис	Действие
3	inside_access_in line 3	any	any	obj_10.1.35.0_24	any	[tcp:[25]]	deny

Часть правила с затенением

№	Имя	Входящий интерфейс	Исходящий интерфейс	Источник	Назначение	Сервис	Действие
2	inside_access_in line 2	any	any	obj_10.1.35.10	any	[tcp:[25]]	accept

- Оптимизация правил:
- Выявление перекрытий правил.
 - Выявление частичных перекрытий правил.
 - Выявление давно не срабатывавших правил.



Проверка доступа по всей цепочке межсетевых экранов:

- Анализ прохождения трафика по 5tuple.
- Моментальный пока пути прохождения трафика, межсетевых экранов в цепочке, разрешающих или запрещающих правил.
- Учитывается multipath, VRF, NAT.

Анализ доступов

Отслеживаемые

Неотслеживаемые

Создать анализ доступа

Наименование	Откуда	Куда	Сервис	Отслеживание	Статус	Дата создания / обновления	Действия
nl_smtp	10.1.35.0/24	94.100.180.201/32	tcp/25		Нарушено	2025.02.17, 18:23:24 2025.03.05, 18:25:06	
vipnet-dns	192.168.12.123/32	8.8.8.8/32	tcp/53		Не нарушено	2025.02.18, 11:45:48 2025.03.05, 18:23:04	
dmz-to-nl-http	31.228.181.0/24	10.1.35.0/24	tcp/80		Не нарушено	2025.02.17, 18:22:41 2025.02.28, 15:56:55	
ns-dns-deny	10.1.35.0/24	66.254.114.42/32	tcp/53		Не нарушено	2025.02.17, 18:21:50 2025.02.28, 15:56:55	

- Создание правил межсегментного взаимодействия.
- Контроль соответствия правилами: уведомление при появлении или исчезновении доступа.

ПРОБЛЕМАТИКА РОСТА КОЛИЧЕСТВА ПРАВИЛ, ДОЛГОГО ОТКРЫТИЯ ДОСТУПОВ

С ростом количества правил на межсетевых экранах появляется ощущение хаоса с доступами

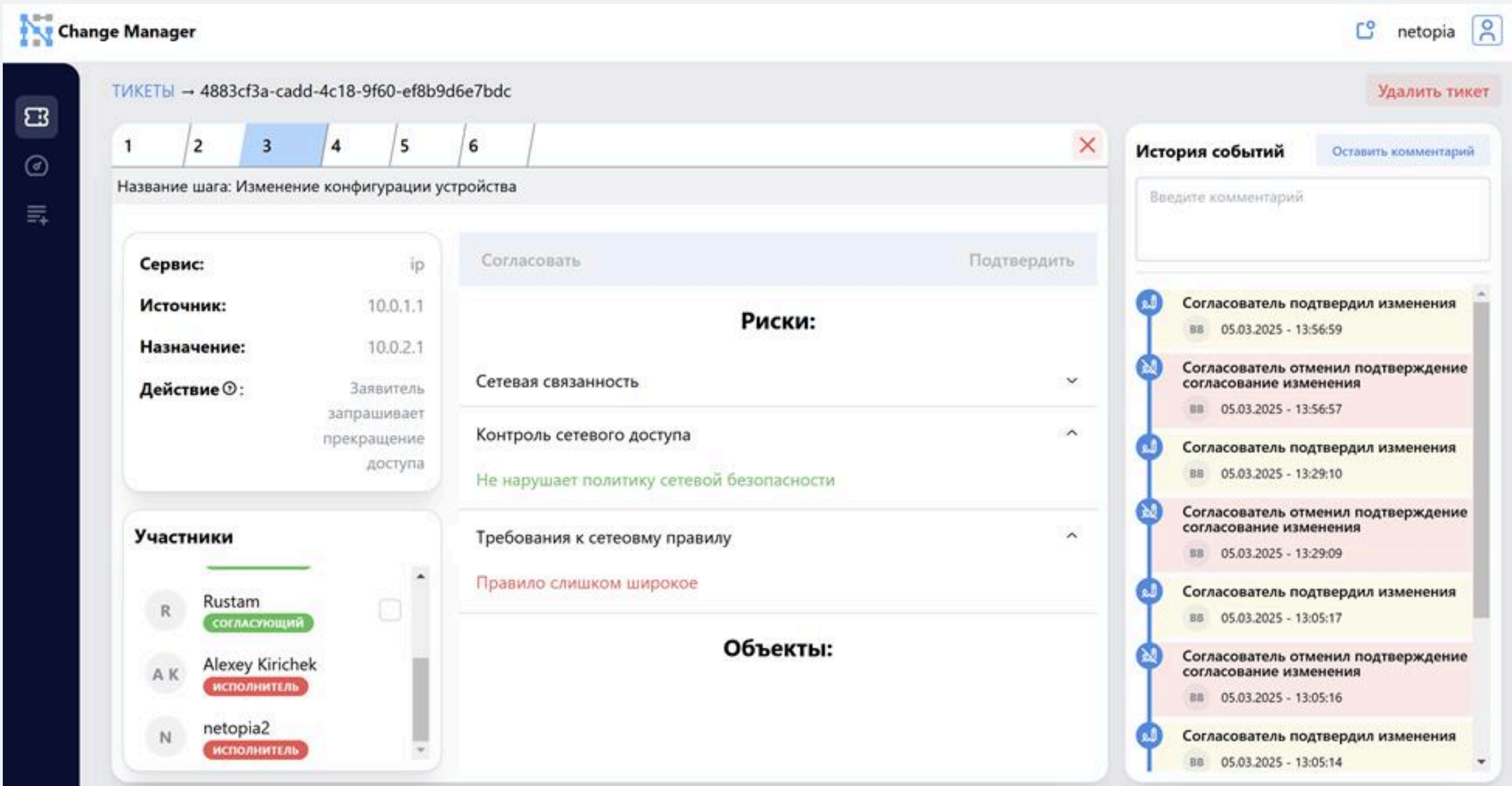
Открытие доступа на множестве сетевых устройств имеет свойство затягиваться по времени

Ошибки и недооткрытые доступы

Отсутствие управления жизненным циклом доступа

Долгое предоставление доступов к системам новым сотрудникам

Сотрудники IT тратят много времени на типизированное открытие доступов (90% изменений правил доступа в больших организациях типизированы)



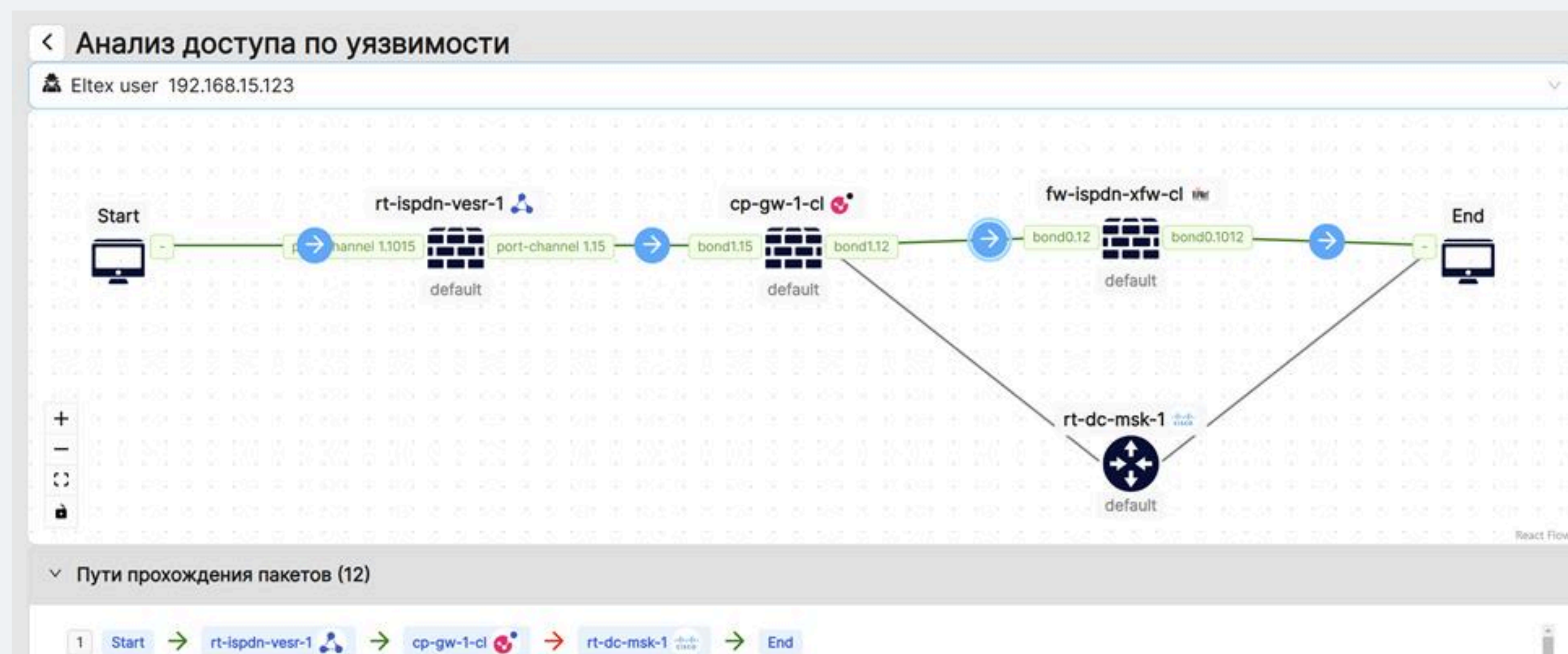
- Интеграция с Business Process Management (BPM) и IT Infrastructure Management (ITSM) системами.
- Автоматизация прописывания правил доступа.
- Управление жизненным циклом доступов: выход нового сотрудника на работу, смена роли сотрудника, увольнение сотрудника.
- Прозрачность согласования доступов.
- Анализ комплаенса на корректность праивла и возможность такого доступа между сегментами.

В больших организациях множество критических уязвимостей

Нет возможности оперативно закрыть их все

Нет возможности дополнительной приоритезации





- Вводим понятие «сверхкритичных» уязвимостей.
- Сверхкритичные уязвимости – это те уязвимости, которые доступны из неконтролируемых или слабоконтролируемых сетей (интернет, VPN подключения с подрядчиками, гостевой wifi и тд).
- Среди, к примеру, 100 критичных уязвимостей выделяем только 5, которые доступны из неконтролируемых сетей и устраняем «здесь и сейчас, сегодня», помечаем их «сверхкритичными».
- Остальные 95 устраняем в рабочем порядке.
- Служба ИБ выполняет свой KPI по закрытию уязвимостей в срок.
- ИТ служба выполняет запрос от ИБ на устранение «сверхкритичных» уязвимостей.

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



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

Порядковый номер в
реестре отечественного
ПО — 17109

Резиденты
Сколково

