NETWELL

Netopia Firewall Compliance
Контроль конфигураций без спешки при ограниченных бюджетах

Подход «целевого инструмента», релевантный для отечественных решений

Традиции, шаблоны и ключевые установки при сокращенных бюджетах

Подход «целевого инструмента»:

- Определение своих ключевых задач, соотносимых с классом решений;
- Выбор приоритетных (первоочередных) задач для закрытия при тестировании и возможном дальнейшем приобретении;
- Тестирование (PoC – prove of concept) нескольких решений от разных производителей;
- Выбор финального варианта, опираясь на близость соответствия;
- По итогам эксплуатации с вендором согласуется возможное исполнение дополнительных задач;

Главный вопрос: КАКИЕ ЗАДАЧИ РЕШИМ?

netopia.pro
NETWORK SECURITY PLATFORM

NETWELL

Практическая польза от решения контроля конфигураций Netopia FC

Польза на основе базовых функций:

- Сокращение объема действующих правил, оптимизация ACLs
- Создание «матриц доступа» и контроль межсегментного доступа
- Оценка конфигураций по Best Practice вендоров и по собственным требованиям
- Топология и картография сетевых сегментов (маршруты + ACL)
- Оперативная оценка блокировки приложений и сервисов по цепочкам доступов
- Насыщение данными по уязвимостям (scanners) и построение «векторов атак»
- Разграничение представляемых данных между службами IT и ИБ (RBAC, заявки)

Пилот из сложной «гонки за всем и сразу» превращается во взвешенную оценку понятной и практической пользы от решения.

Отличительные свойства решения Netopia FC

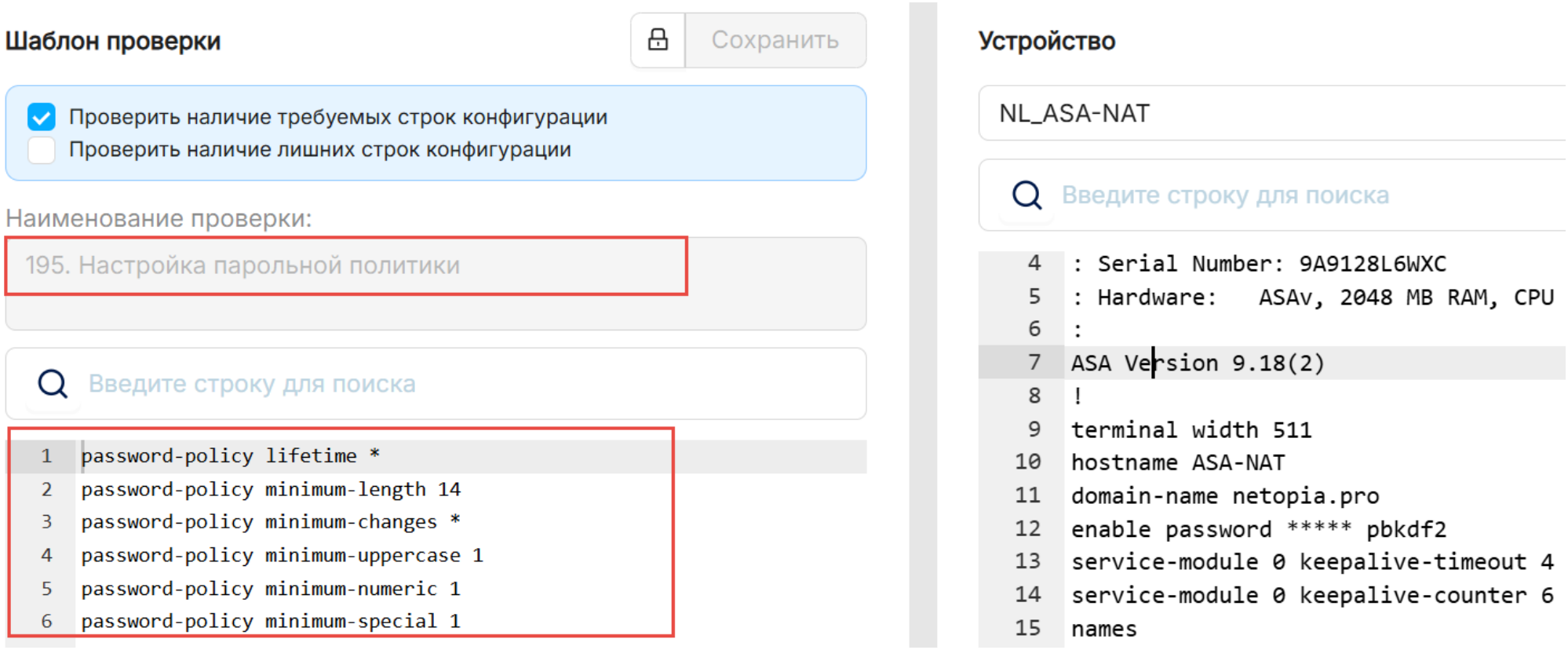
- Fortigate
- Check Point
- Cisco IOS
- Generic
- Cisco ASA
- Cisco Nexus
- UserGate
- Континент
- Huawei NE
- Huawei USG
- ViPNet
- PT NGFW
- Eltex
- C-Teppa
- Ideco

На текущее время эксклюзивно:

- Поддержка Positive Technologies NGFW
- Поддержка Max Patrol и Max Patrol VM «из коробки»

Отличительные свойства решения Netopia FC

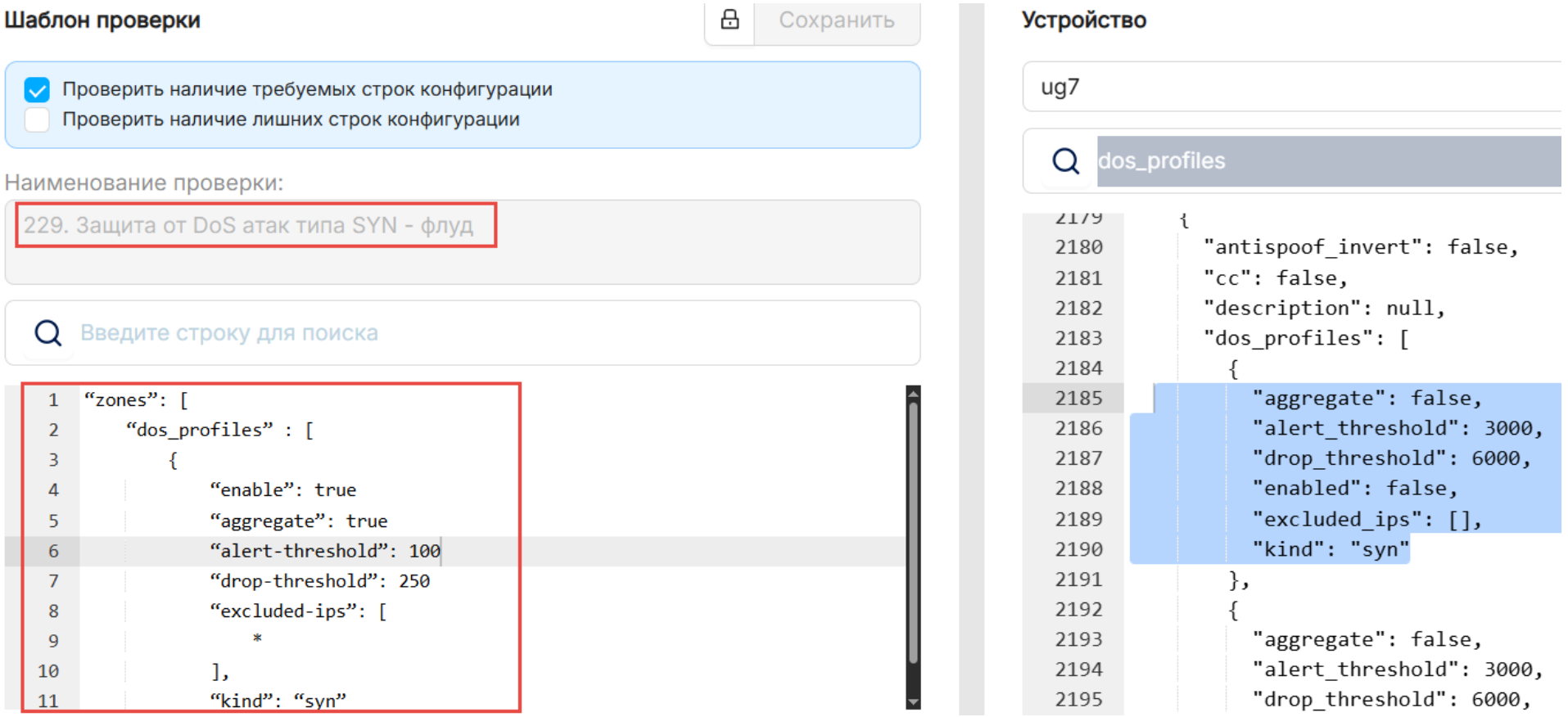
Прозрачность и управляемость параметрами ИБ-проверок конфигураций



Пример для Cisco ASA, параметры парольной политики

Отличительные свойства решения Netopia FC

Прозрачность и управляемость параметрами ИБ-проверок конфигураций



Пример для UserGate, защита от SYN –flood пакетов

Отличительные свойства решения Netopia FC

Для дубликатов и перекрывающихся объектов есть отметка о присутствии в конфигурации

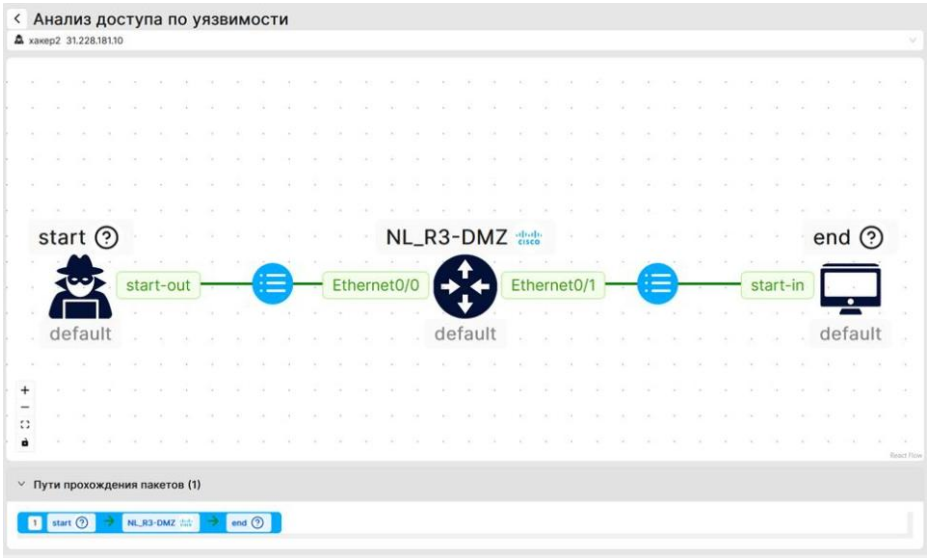
	Наименование	Тип объект			Связанные правила		Устройство	Вендор
					NAT	SECURITY		
group_obj_fbfef5b3-35da-4375-a1c1-5f8a8939036a IPRangeGroup	group_obj_fbfef5b3-35da-4375-a1c1-5f8a8939036a	IPRangeGroup		3	Нет связанных правил	Нет связанных правил	NL_ASA-NAT	Cisco ASA

Наименование	Тип объекта			Связанные правила		Устройство	Вендор
				NAT	SECURITY		
obj_66.6.16.242_66.6.16.242	IPRange			Нет связанных правил	dmz_access_in	- // -	- // -
obj_10.1.35.31_10.1.35.31	IPRange			Нет связанных правил	dmz_access_in	- // -	- // -

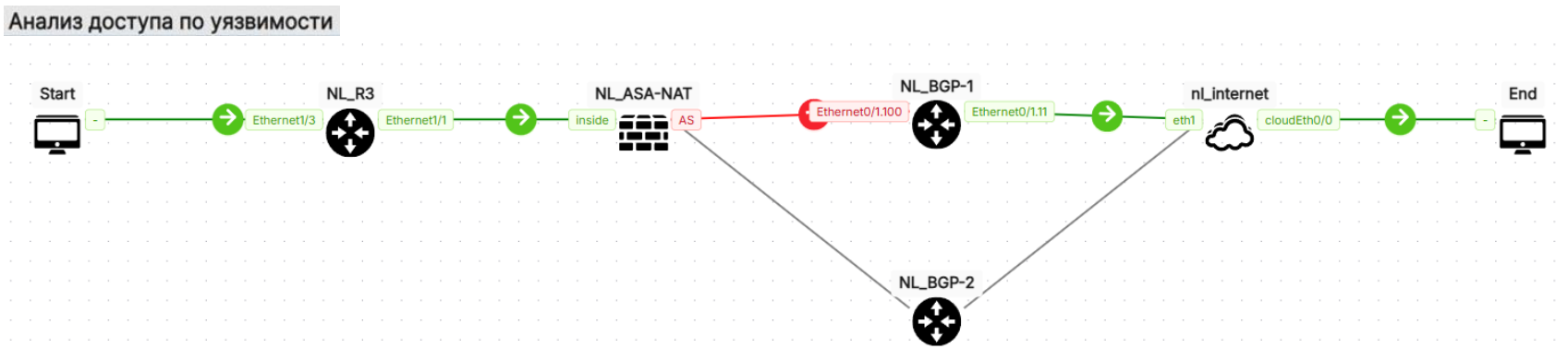
Моментально проверяется присутствие объекта во всех NAT и ACL-списках!

Отличительные свойства решения Netopia FC

Вектора атак и построение модели злоумышленника

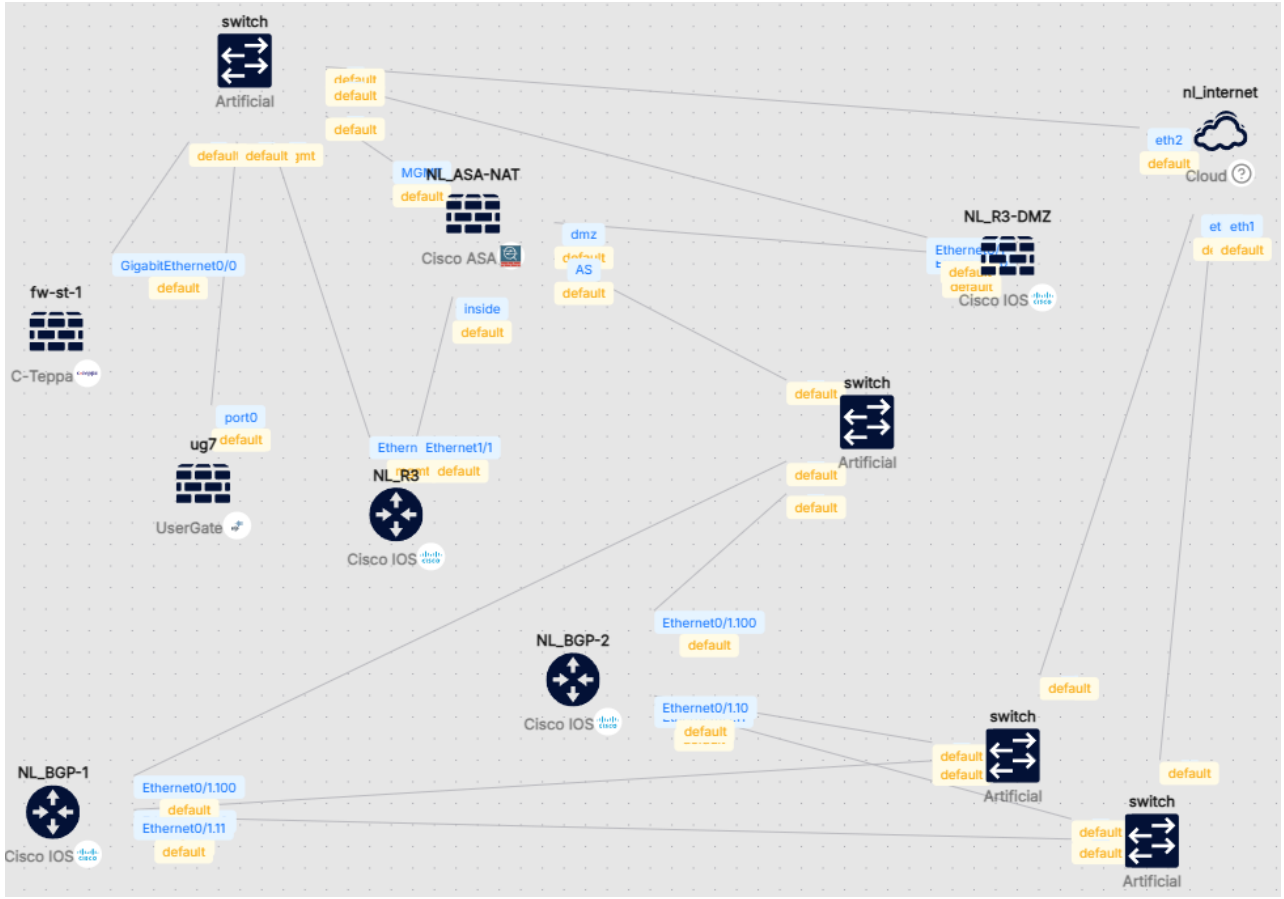


- Выгрузка данных по уязвимостям из Max Patrol / MP VM
- Классификация уязвимостей по BDU FSTEK, CVE/CPE, базам вендоров
- Построение модели злоумышленника (3 уровня хакера)
- Поиск множества связанных путей по топологии сети



Отличительные свойства решения Netopia FC

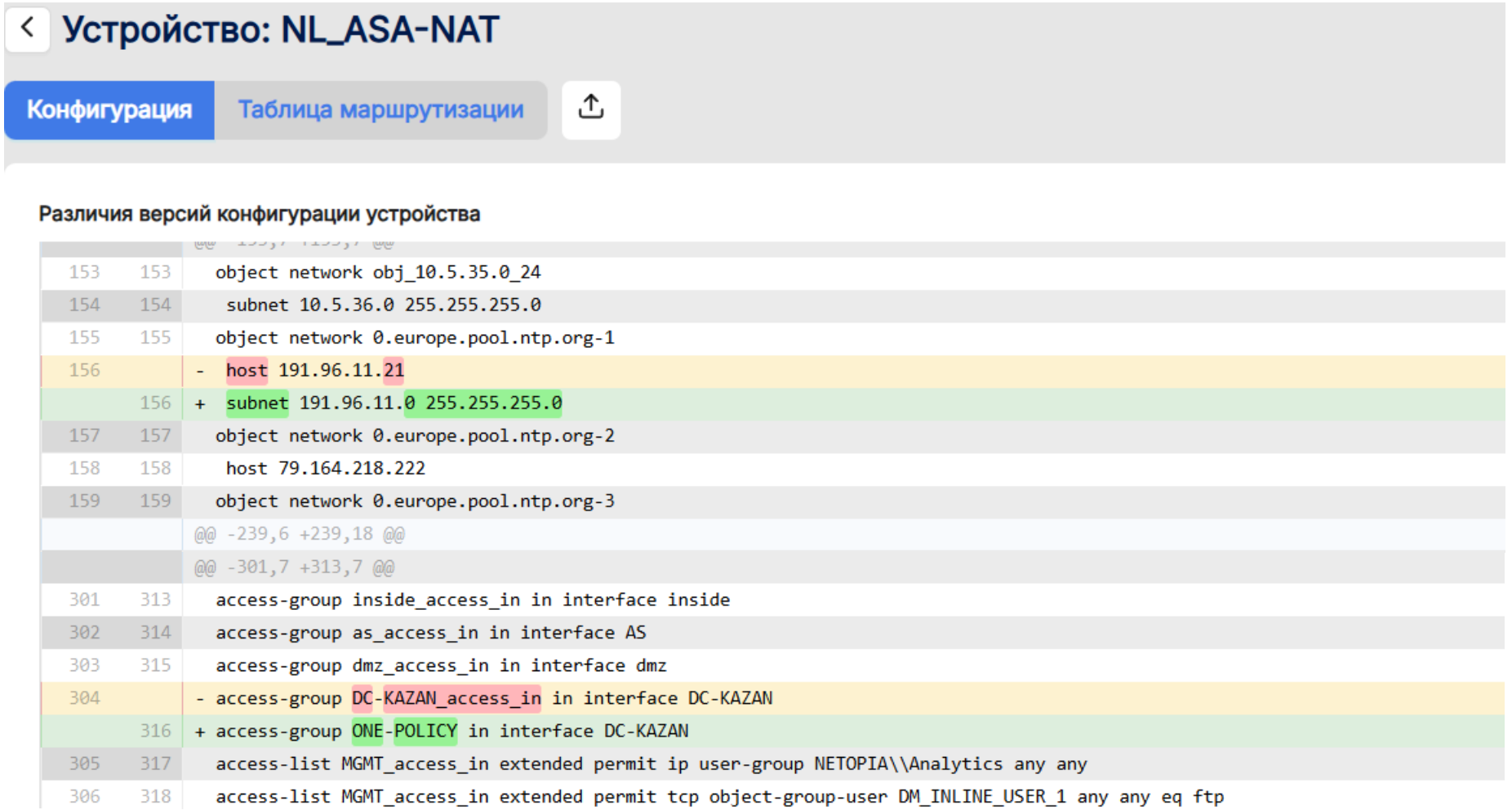
Топология и картография сети



- Для устройств МСЭ: учет маршрутов, NAT и ACLs
- Модель «слепков» текущих конфигураций (статика и динамика)
- Обновление данных по интервалам и syslog
- Формирование отдельных сохраняемых карт (по устройствам)
- Ожидается (2025) – поддержка VPN IPSec

Отличительные свойства решения Netopia FC

Текстовые и графические данные об изменениях доступов



Отличительные свойства решения Netopia FC

Текстовые и графические данные об изменениях доступов

Изменено (до)	3	inside_access_in	inside_access_in	any any	obj_10.1.35.10 any	[tcp:[25]]
Изменено (после)	3	inside_access_in	inside_access_in	any any	obj_10.1.35.2 obj_66.254.114.42	[udp:[53], tcp:[53]]
Изменено (до)	4	inside_access_in	inside_access_in	any any	obj_10.1.35.0_24 any	[tcp:[25]]
Изменено (после)	4	inside_access_in	inside_access_in	any any	obj_10.1.35.2 obj_66.254.114.41	[udp:[53], tcp:[53]]

Контакты

Москва
115114, 1-й Дербеневский пер., 5 БЦ «Дербеневская Плаза»

Санкт-Петербург
190000, Английская набережная, 70

Казань
420107, Спартаковская, 23

+7 (495) 662 39 66
info@netwell.ru
netwell.ru
Telegram-канал