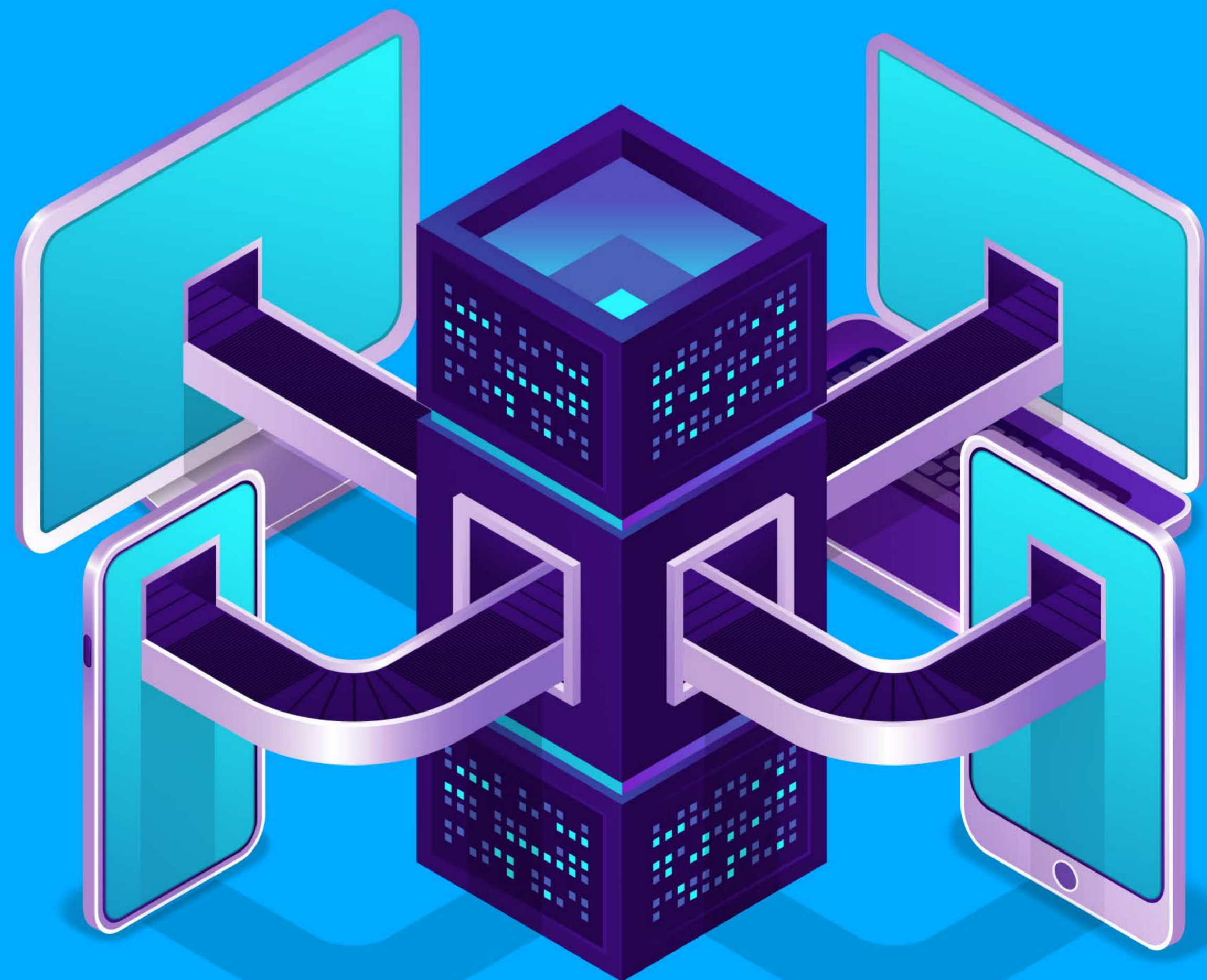


NETOPIA FIREWALL COMPLIANCE





РЕЗИДЕНТЫ
СКОЛКОВО

СЕРТИФИЦИ-
РОВАННЫЕ
СПЕЦИАЛИСТЫ
CCIE

x2 в команде.

РОССИЙСКАЯ
РАЗРАБОТКА

Порядковый номер
в реестре отечественного
ПО — 17109.

https://reestr.digital.gov.ru/reestr/1393430/?sphrase_id=4213163



ЛАБОРАТОРИЯ
В МГУ ИМ. Н.Э.
БАУМАНА

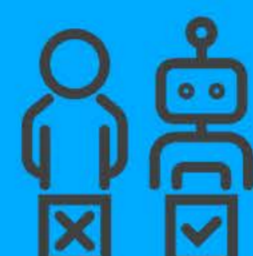
Открытие летом
2025 года.



ВОЗМОЖНОСТИ ПЛАТФОРМЫ КОНТРОЛЯ СЕТЕВОЙ БЕЗОПАСНОСТИ



АНАЛИЗ И ОПТИМИЗАЦИЯ
ПРАВИЛ СЕТЕВОГО ДОСТУПА



АНАЛИЗ СООТВЕТСТВИЯ
КОНФИГУРАЦИЙ СЕТЕВЫХ
УСТРОЙСТВ ЗАДАНЫМ
СТАНДАРТАМ



РАСЧЁТ ВОЗМОЖНЫХ ВЕКТОРОВ
АТАК С УЧЁТОМ НАСТРОЕК
СЕТЕВОГО ОБОРУДОВАНИЯ

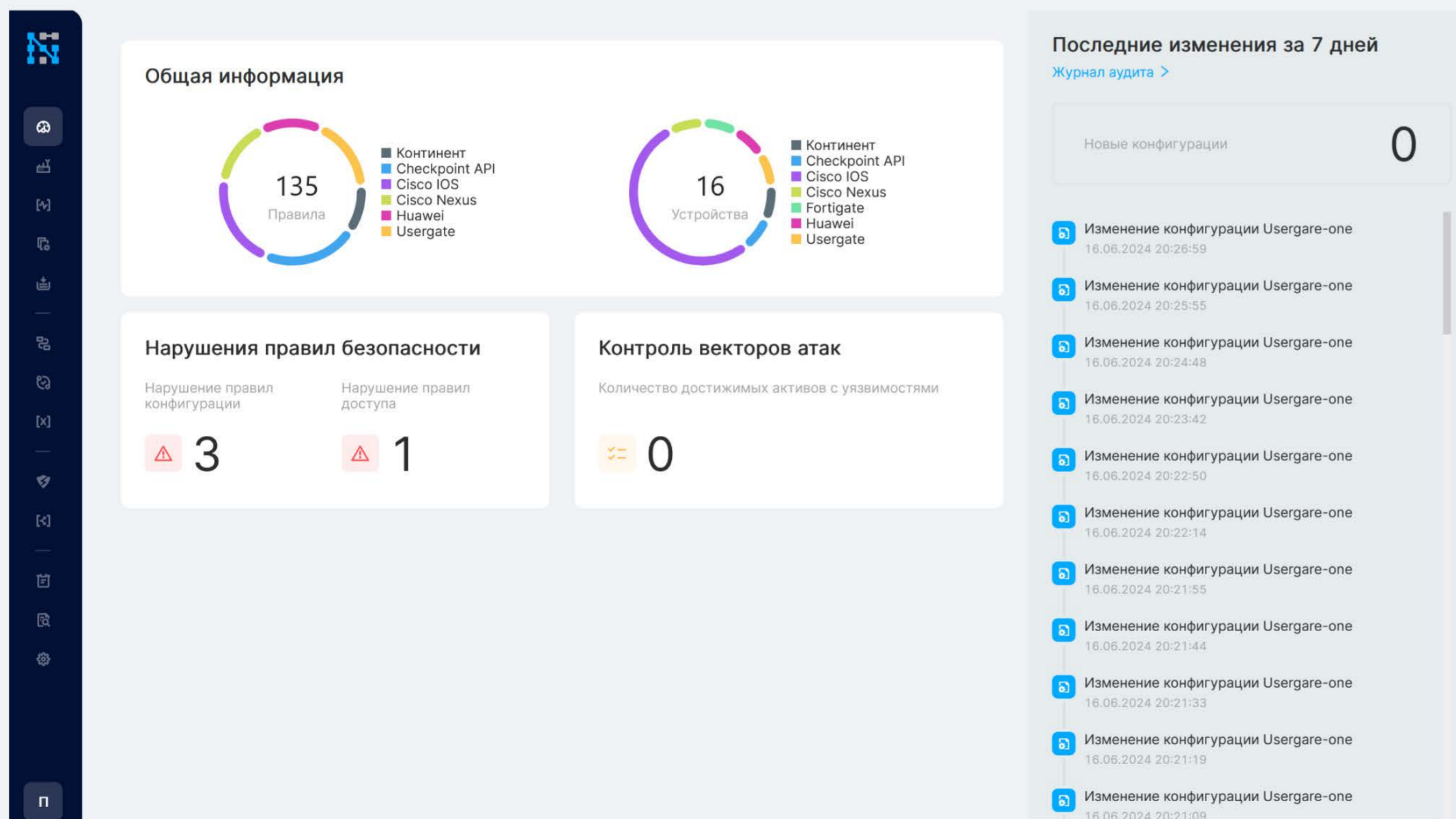


ВИЗУАЛИЗАЦИЯ СЕТЕВОЙ
ИНФРАСТРУКТУРЫ



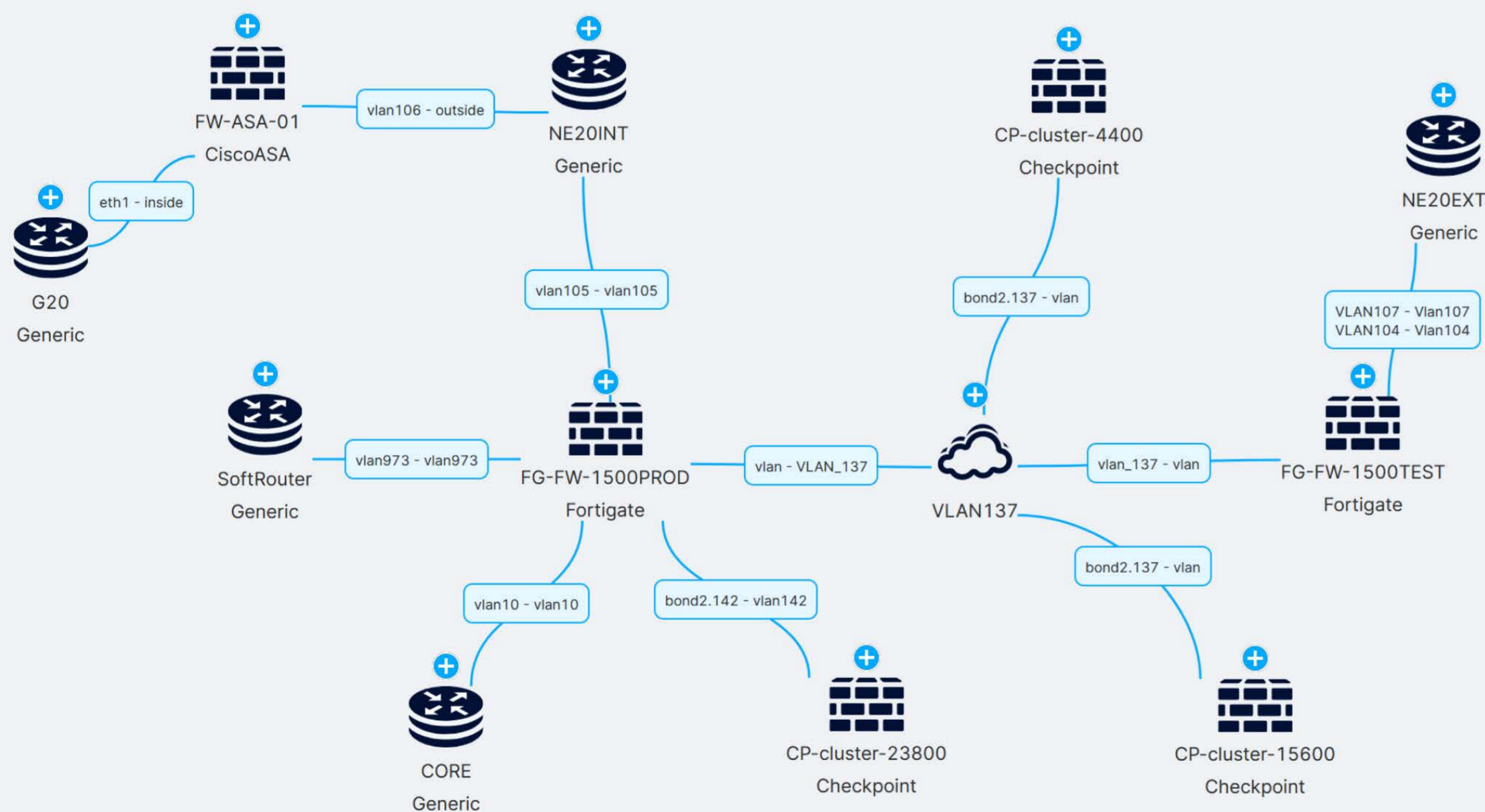
ПРИОРИТИЗАЦИЯ
УЯЗВИМОСТЕЙ





ПРИ ПЕРВИЧНОЙ НАСТРОЙКЕ СИСТЕМЫ ПОЛУЧАЕМ ИНФОРМАЦИЮ ОБ УЯЗВИМОСТИ ИНФРАСТРУКТУРЫ:

- Доступность уязвимых активов.
- Слабые места в access-листах.
- Статистика по сетевой инфраструктуре.



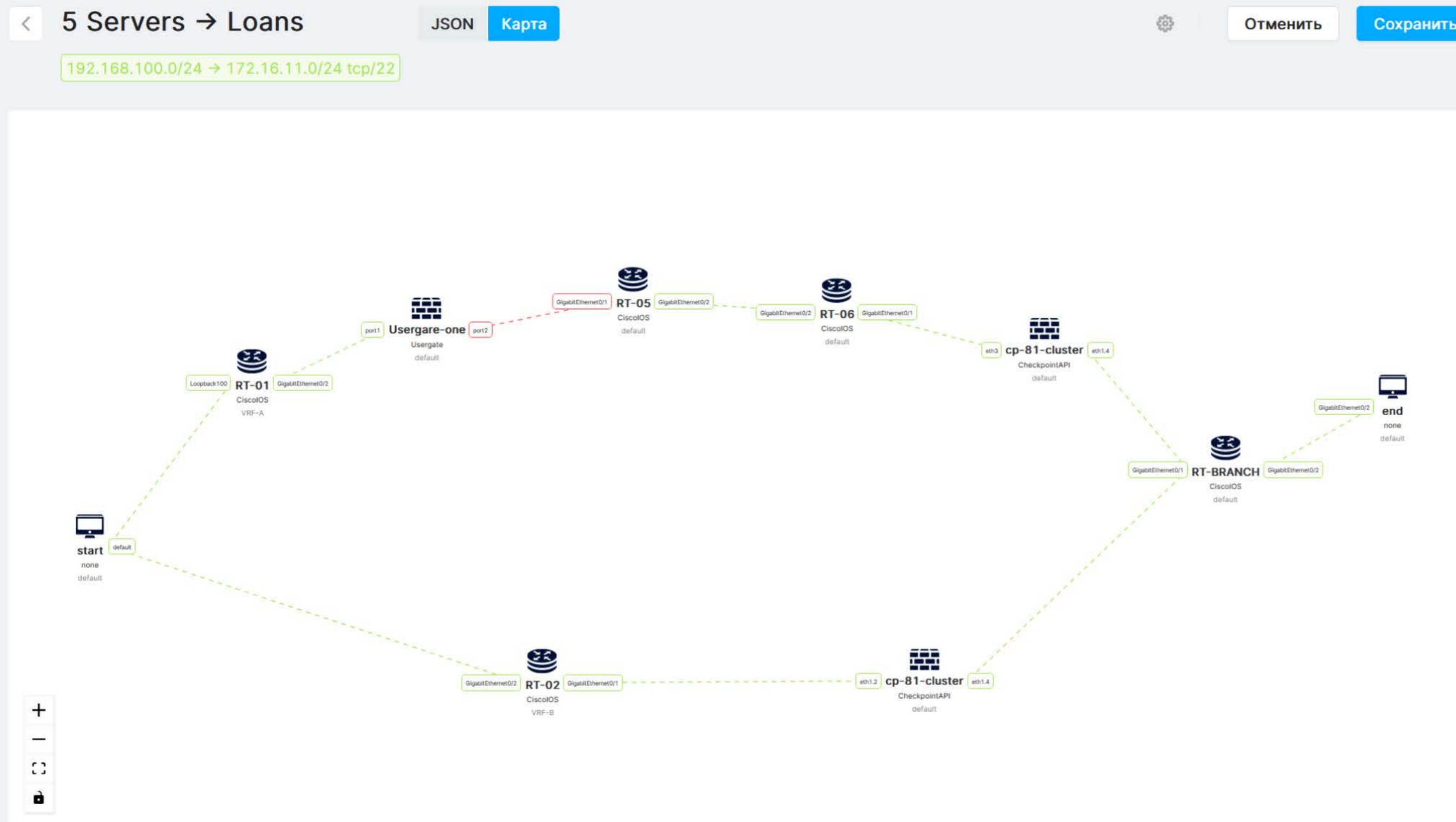
ПОСТРОЕНИЕ КАРТЫ СЕТИ

- Сбор конфигураций сетевого оборудования и построение карты сети.
- Поддерживаются Generic-роутеры для скрытия / упрощения части сети.
- Поддерживаются multi-path маршруты.

АНАЛИЗ СООТВЕТСТВИЯ КОНФИГУРАЦИЙ СЕТЕВЫХ УСТРОЙСТВ ЗАДАННЫМ СТАНДАРТАМ

КОНТРОЛЬ КОНФИГУРАЦИЙ СЕТЕВЫХ УСТРОЙСТВ ПО ЗАДАННЫМ ТРЕБОВАНИЯМ:

- Лучшие практики по настройке и безопасности, предлагаемые производителями межсетевых экранов.
- Корпоративные стандарты настройки оборудования (AAA, NTP, Syslog и т.д.).
- Нормативные требования (PCI DSS, ГОСТ 57580, Приказы ФСТЭК и ФСБ России).



АНАЛИЗ ПРОХОЖДЕНИЯ ТРАФИКА ПО СЕТИ

1. На основании source (откуда), destination (куда) и сервиса строится граф прохождения трафика по сети.
2. Указываются правила, срабатывающие на межсетевых экранах.
3. Проверяются зоны на соответствие корпоративным стандартам по сетевой безопасности:
 - Добавление ключевых сервисов, согласно корпоративным стандартам.
 - Мониторинг соответствия корпоративным стандартам.

АНАЛИЗ И ОПТИМИЗАЦИЯ ПРАВИЛ СЕТЕВОГО ДОСТУПА

АНАЛИЗ ПРАВИЛ ДОСТУПА (ACL):

- Выявление правил, содержащих "any" в полях.
- Выявление правил без комментариев, отключенных, не логируемых, без имени.

ОПТИМИЗАЦИЯ ПРАВИЛ ДОСТУПА (ACL) МЕЖСЕТЕВЫХ ЭКРАНОВ:

- Выявление затененных правил.
- Выявление редко используемых правил и объектов.
- Формирование рекомендаций по оптимизации правил.

ПРИОРИТЕЗАЦИЯ УЯЗВИМОСТЕЙ

Уровни уязвимостей

Активы Уязвимости Злоумышленники Уровни злоумышленников



Наименование	IP	Значимость	Источник	Дата создания	Дата обновления	Контроль
Сервер финансы	192.168.20.2	4	pt_vrn	21.03.2024 18:05:40	21.03.2024 18:05:40	<input type="checkbox"/>
10.10.0.1	10.10.0.1	4	pt_vrn	21.03.2024 18:05:40	21.03.2024 18:05:40	<input type="checkbox"/>
Сервер разработка	192.168.168.2	2	pt_vrn	21.03.2024 18:05:40	21.03.2024 18:05:40	<input type="checkbox"/>
192.168.10.1	192.168.10.1	4	pt_vrn	21.03.2024 18:05:40	21.03.2024 18:05:40	<input type="checkbox"/>
192.168.168.1	192.168.168.1	4	pt_vrn	21.03.2024 18:05:40	21.03.2024 18:05:40	<input type="checkbox"/>
sonarqube.netopia.app (10.0.0.35)	10.0.0.35	1	pt_vrn	21.03.2024 18:05:40	21.03.2024 18:05:40	<input type="checkbox"/>
10.0.0.3	10.0.0.3	4	pt_vrn	21.03.2024 18:05:40	21.03.2024 18:05:40	<input type="checkbox"/>
192.168.111.1	192.168.111.1	4	pt_vrn	21.03.2024 18:05:40	21.03.2024 18:05:40	<input type="checkbox"/>
openvpn (10.0.0.7)	10.0.0.7	4	pt_vrn	21.03.2024 18:05:40	21.03.2024 18:05:40	<input type="checkbox"/>
demo.netopia.app (10.0.0.31)	10.0.0.31	1	pt_vrn	21.03.2024 18:05:40	21.03.2024 18:05:40	<input type="checkbox"/>

< 1 2 3 > 10 записей на странице

- Сбор активов из Asset Management систем.
- Сбор уязвимостей из Vulnerability Management систем.
- Расстановка приоритетов согласно доступности активов со стороны злоумышленников.
- Гибкая система формирования злоумышленников.

РАСЧЁТ ВОЗМОЖНЫХ ВЕКТОРОВ АТАК С УЧЁТОМ НАСТРОЕК СЕТЕВОГО ОБОРУДОВАНИЯ

Контроль векторов атак

Уязвимый актив	Группа достижимых активов	Достижимые активы
<input type="text" value="10.0.0.24"/>		
Наименование 10.0.0.24	Уровень критичности 1 5	10.0.0.8 10.0.0.8
IP адрес 10.0.0.24	Уровень критичности 2 1	192.168.111.1 192.168.111.1
Источник MP VM	Уровень критичности 3 1	10.10.0.1 10.10.0.1
Значимость 4	Уровень критичности 4 13	192.168.168.1 192.168.168.1
		орелврл (10.0.0.7) 10.0.0.7
		Сервер финансы 192.168.20.2
		10.0.0.3 10.0.0.3
		192.168.10.1 192.168.10.1
		Сервер DMZ 192.168.10.2
		Сервер КИИ 192.168.111.2
		10.0.0.9 10.0.0.9
		192.168.20.1 192.168.20.1
		license-manager.netopia.app (10.0.0.36) 10.0.0.36

- Выбор скомпрометированного хоста.
- Создание искусственных активов.
- Просчёт плоскости атаки в рамках сети организации.

СРАВНЕНИЕ С КОНКУРЕНТАМИ



	netopia.pro	SKYBOX SECURITY	tufin	algosec	Нетхаб	EFROS ACCESS CONTROL SERVER
Network Assurance Сбор конфигураций Контроль конфигураций Карта сети	✓	✓	✓	✓	✓	✓
Firewall Assurance Анализ сетевой доступности Оптимизация правил Матрица сетевой доступности	✓	✓	✓	✓	✓	✓
Vulnerability Control Приоритезация уязвимостей Построение векторов атак	✓	✓	✗	✗	✗	✗
Change Management Workflow по изменению сетевой политики Изменение сетевых политик на устройстве	✗	✓	✓	✓	✓	✓ ✗
В реестре российского ПО	✓	✗	✗	✗	✓	✓

ПОДДЕРЖИВАЕМОЕ ОБОРУДОВАНИЕ И ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ



IOS

ASA Firewall



UserGate

FORTINET



Контиент

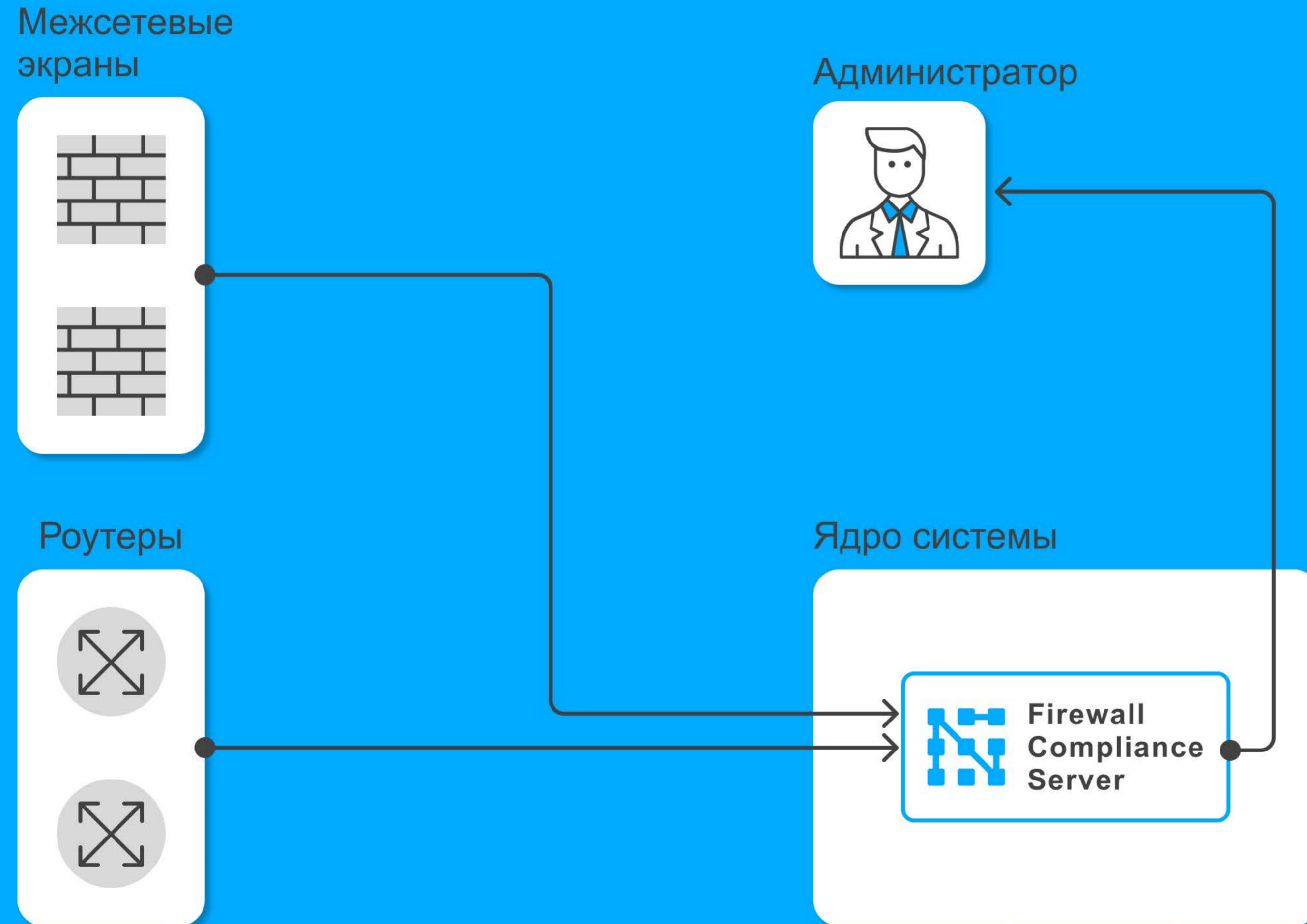
с•терра



В БЛИЖАЙШЕЕ ВРЕМЯ:



АРХИТЕКТУРА РЕШЕНИЯ



Netopia Firewall Compliance

является аналитической системой и состоит из одного сервера из-за отсутствия большой нагрузки.

FIREWALL COMPLIANCE SERVER

Это ядро системы — модуль управления, позволяющий регулировать конфигурацию и настройку системы.

Все настройки и управление производится в одном месте.

ПРЕИМУЩЕСТВА



Высокий уровень экспертизы*

* Сотрудники с высшими сертификациями по производителям сетевого оборудования.



Многочисленная поддержка систем



Кастомизация решения



Российская разработка



ЛИЦЕНЗИРОВАНИЕ

- ЛИЦЕНЗИЯ БЕССРОЧНА
- ОБНОВЛЕНИЕ ПО - БЕСПЛАТНО В ПЕРВЫЙ ГОД
- ПРОДЛЕНИЕ ЛИЦЕНЗИИ - ЧЕРЕЗ ГОД ЭКСПЛУАТАЦИИ



ЭТАПЫ РЕАЛИЗАЦИИ ПРОЕКТА ПО ВНЕДРЕНИЮ РЕШЕНИЯ NETORIA FIREWALL COMPLIANCE В ИМЕЮЩУЮСЯ ИТ-ИНФРАСТРУКТУРУ



АУДИТ ТЕКУЩЕЙ ИНФРАСТРУКТУРЫ ЗАКАЗЧИКА

Анализ работы текущих межсетевых экранов, выявление ключевых сервисов, выделение правил фильтрации ключевых сервисов.

ТЕХНИЧЕСКАЯ ПОДДЕРЖКА СОГЛАСНО SLA
+
ОБНОВЛЕНИЕ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

ВНЕДРЕНИЕ РЕШЕНИЯ NETORIA FIREWALL COMPLIANCE

Необходимы вычислительные ресурсы под инфраструктуру Netoria Firewall Compliance, доступ к межсетевым экранам для взаимодействия с ПО.

NETORIA FIREWALL COMPLIANCE — ЧАСТЬ ГЛОБАЛЬНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ



ЦИФРОВАЯ ПЛАТФОРМА NETORIA

КОМПОНЕНТ NETWORK MONITOR

Проводит мониторинг сетевого оборудования в потоковом режиме для раннего выявления проблем и ошибок в работе вычислительной сети.

КОМПОНЕНТ NETWORK COMPLIANCE

Обеспечивает контроль конфигурации сетевого оборудования путём анализа оригинальной части конфигурации.

КОМПОНЕНТ FIREWALL COMPLIANCE

Обеспечивает контроль сетевой безопасности, рассчитывает вектора атак, приоритизирует уязвимости сети. Производит сбор и анализ конфигураций сетевых устройств.



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

