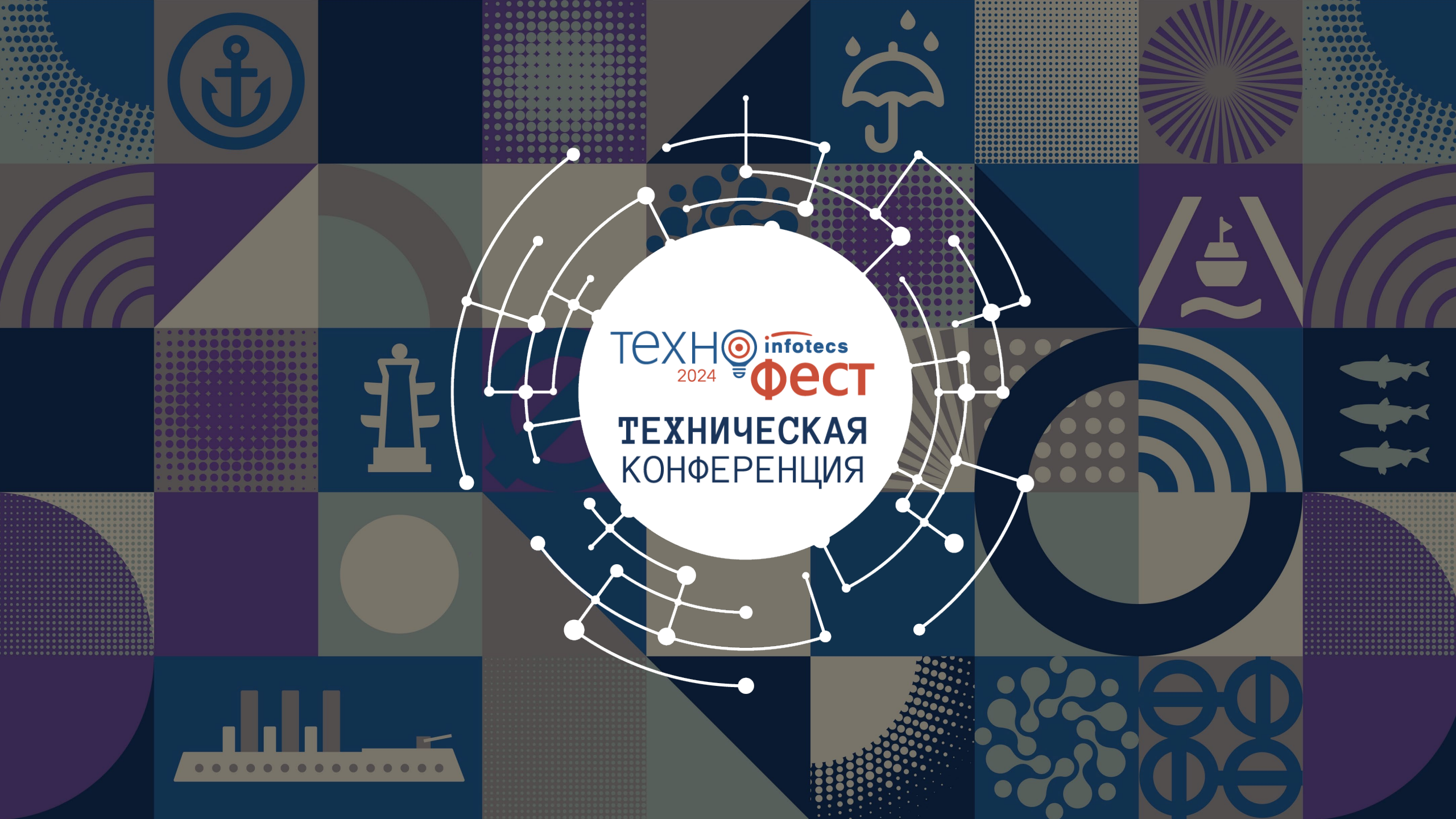

ТЕХНО
2024
infotecs
ФЕСТ
ТЕХНИЧЕСКАЯ
КОНФЕРЕНЦИЯ

ГАЗИНФОРМ СЕРВИС 20 лет вместе x datagile

Май 2024

Модуль управления правилами МЭ

Efros DO: Change Manager

www.gaz-is.ru

В чем суть Change Manager

GIS
ГАЗИНФОРМ СЕРВИС
20 лет вместе

Change Manager – это модуль Efros Defence Operations, для управления конфигурациями устройств с упором на изменения правил межсетевых экранов, через систему заявок и ведения жизненного цикла этих правил

- Контроль изменения правил МЭ
- Управление правилами МЭ через систему заявок
- Имплементация правил МЭ на цепочке устройств
- Создание временных правил МЭ
- Оценка рисков безопасности при изменении правил МЭ
- Автоматизация управления правилами МЭ
- Уменьшение количества правил МЭ за счет анализа
- Работа с правилами МЭ нескольких вендоров из единой консоли

Из чего состоит Change Manager

GIS
ГАЗИНФОРМ
СЕРВИС
20 лет вместе

1

Система заявок

Формирование типов заявок, создание маршрутов и групп пользователей, аудит

2

Карта сети

Устройства, подсети, связи, виртуализация. Запуск моделирования с отображением пути прохождения

3

Моделирование трафика

Процесс построения маршрута из точки А в точку Б с использованием интерфейсов, маршрутов и правил МЭ

4

Управление правилами МЭ

Генерация скриптов изменения правил МЭ с последующим выполнением через заявки

Система заявок

GIS ГАЗИНФОРМ СЕРВИС 20 лет вместе

Типы заявок

Возможность настраивать свои типы заявок от заказа воды до запроса доступа

Маршруты

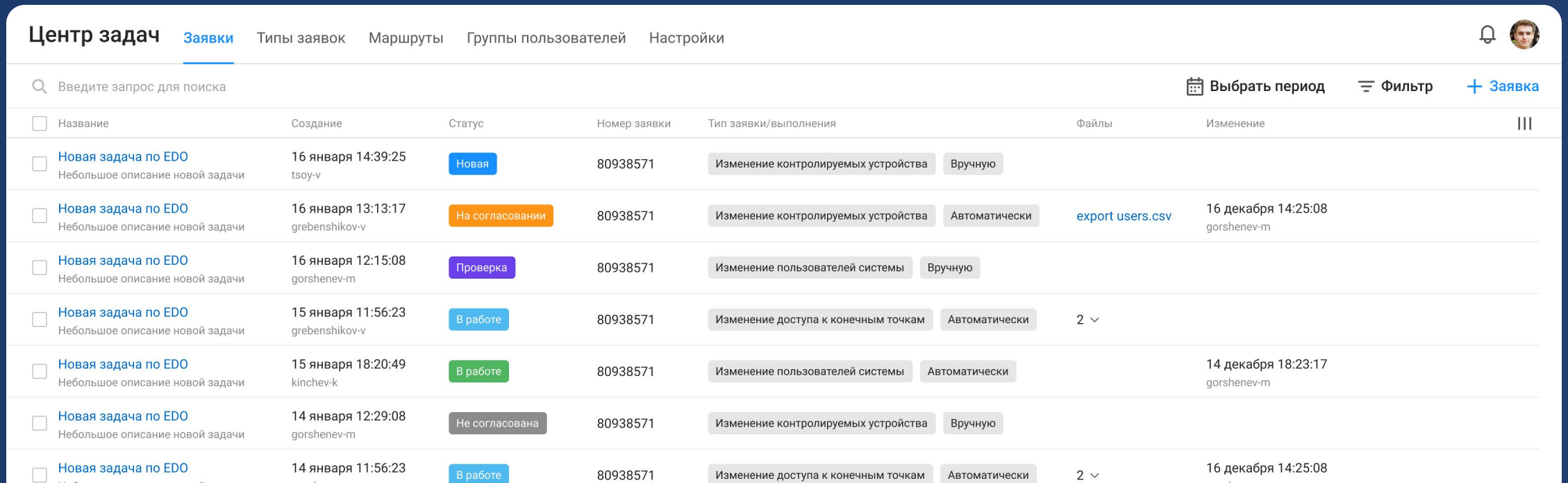
Формирование шагов заявки с настройкой условий и ответственных

Пользователи

Группы пользователей для выбора участия в шагах маршрута

События

Возможность просмотра всех событий модуля по тематически разделенным категориям



Карта сети

GIS ГАЗИНФОРМ СЕРВИС 20 лет вместе

Устройства

Элементы сети отображаемые на основе конфигурации интерфейсов

Подсети

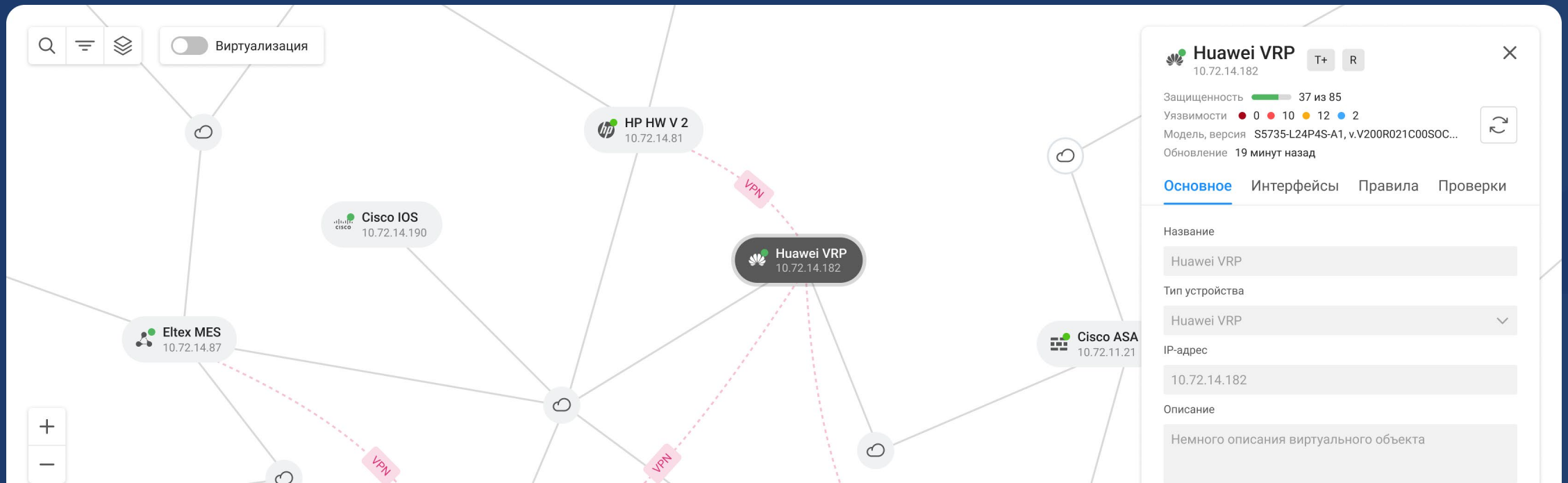
Автоматически генерируемые элементы для демонстрации принадлежности устройств к сети

Связи

Построение связей между устройствами и подсетями с поддержкой отображения VPN туннелей

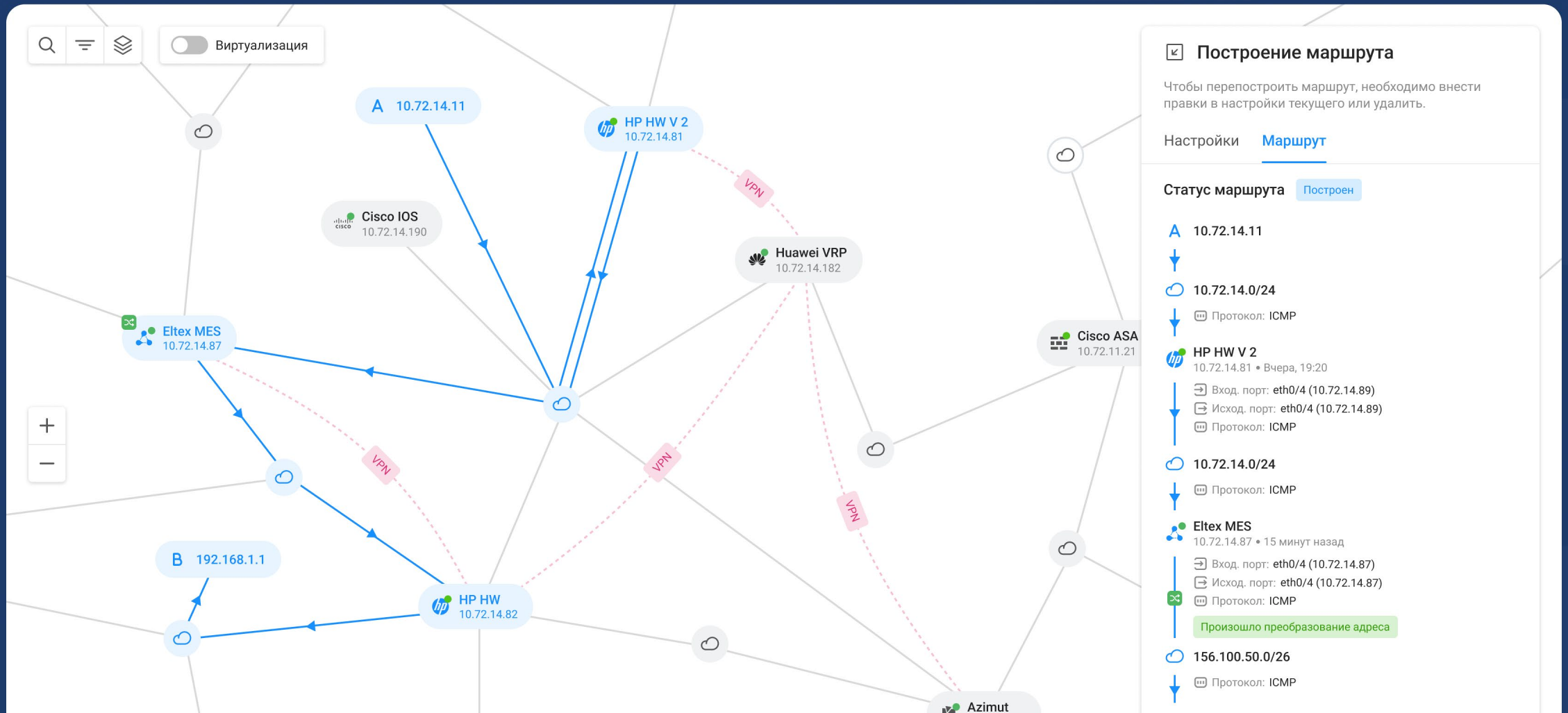
Виртуализация

Возможность дополнять карту виртуальными устройствами с пользовательскими настройками



Моделирование трафика

Процесс построения маршрутов из точки А в точку Б на основе конфигураций по маршрутам, правилам МЭ с учетом NAT, VPN, PBR для демонстрации проходимости трафика



Управление правилами МЭ

GIS ГАЗИНФОРМ СЕРВИС 20 лет вместе

Change Manager реализован через специальные системные заявки с заложенной в них поддержкой Stage-маршрутов, данные заявки зависят от лицензии на Change Manager и появляются только при ее наличии. Текущее оборудование, с которым умеем работать, это Check Point, Cisco ASA, Cisco FMC

Создание заявки

Настройка точки А и Б между которыми необходимо получить доступ с указанием протокола и порта

Запуск

Запуск процесса, то есть создание заявки и перевод ее в стадию моделирования

Моделирование

Выявление блокирующих правил и генерация предложенных изменений для предоставления доступа, генерация скриптов на изменение конфигурации

Согласование

Проверка предложенных данных и оценки их влияния на безопасность через специализированные отчеты. Зонный анализ, стандарты МЭ

Утверждение

Дополнительная стадия проверки (Опционально)

Выполнение

Процесс запуска выполнения скриптов в автоматическом или ручном режиме с последующей проверкой корректности выполнения

Проверка

Статистика заявки, возможность посмотреть запрашиваемый доступ, все промежуточные отчеты по конфигурациям и проверкам, запуск построения моделирования для проверки предоставления доступа

Закрытие

Перевод заявки в стадию «Выполнено»

Сценарий создания заявки на запрос доступа

Текущие ограничения

GIS ГАЗИНФОРМ СЕРВИС 20 лет вместе

В разработке

Возможность добавления правил только поверх блокирующих

На текущий момент правила не могут быть изменены или передвинуты, другими словами переиспользованы

В разработке

Удаление правил только с полным совпадением

Удаление правил только по отношению к полному совпадению запрашиваемого доступа без анализа пересечений

В разработке

Переиспользование объектов только с полным совпадением

Невозможность использовать существующие объекты, модифицировать их и проверять их применимость в других правилах

Планы на 2024

GIS ГАЗИНФОРМ СЕРВИС 20 лет вместе

1

Динамические маршруты

Возможность назначения ответственных на устройства и автоматического использования их в stage маршрутов согласно изменяемым устройствам заявки

2

Новые типы заявок

Запуск процесса, то есть создание заявки и перевод ее в стадию моделирования. Добавление правил, удаление, изменение правил, конфигурирование устройств скриптами

3

Развитие алгоритма

Развитие процессов изменения правил в части учета пересечений, изменения, а так же оптимизации с целью уменьшения их кол-ва

4

Объекты правил

Поддержка работы с объектами как отдельными сущностями для последующего их изменения в рамках текущих заявок и новых типов

5

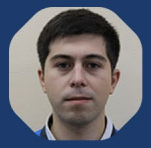
Автоматизация

Автоматизация процессов выполнения заявки без участия пользователя, предоставление метрик для настройки

GIS ГАЗИНФОРМ СЕРВИС 20 лет вместе x datagile

Май 2024

Спасибо за внимание!



Дмитрий Семенов
Ведущий аналитик Datagile