CAPIF 2 2023

Вызовы для IXP по безопасности и стабильности

Александр Ильин
Технический директор MSK-IX

Ключевые аспекты безопасности

Предотвращение

Аутентификация, контроль доступа

Обнаружение и анализ

Выбор ключевых показателей

Сдерживание

Изоляция повреждённых участков

Реагирование

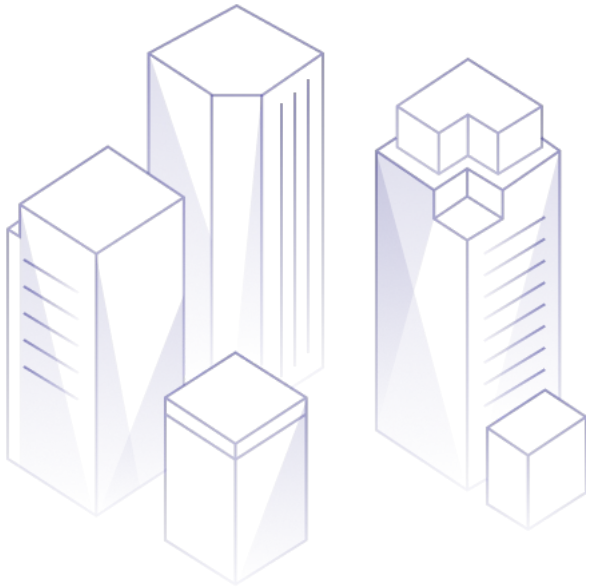
Ключевые события, начало проблем

Восстановление

резервная копия данных

1. Наши подходы: Защита

- Изолированная сеть управления
- Ограничение доступа
- Разграничение прав/стабильность персонала
- Двойной контроль критичных изменений
- Постоянный поиск и анализ уязвимостей
- Двухфакторная аутентификация
- Контроль авторизации, надежные средства оповещения
- Автоматизация процессов



2. Отказоустойчивость и резервирование

- «Двойное ядро», кольцевые топологии, Anycast для сервисов
- ЗИП на ключевых узлах
- Учет оптических модулей с быстрой заменой
- 24/7 «удалённые руки» и персонал для оперативного выезда
- Резервирование на всех уровнях (порты, оборудование, ЛС)
- Размещение систем мониторинга/управления в разных ЦОД
- Комплекс мероприятий по митигации на случай выхода из строя

4. Пропускная способность

- Регулярный анализ загрузки линий связи
  Внутренних, междугородних
- Математический анализ изменений трафика клиентов
- Контроль и учёт свободных ресурсов
  Минимум двухкратный резерв
- Заблаговременный план по апгрейду оборудования
  Планирование от года и далее
- Моделирование нагрузки в лаборатории

Защита участников MSK-IX

- ТУ обязательные к исполнению

- **Контроль доступа по SRC MAC**

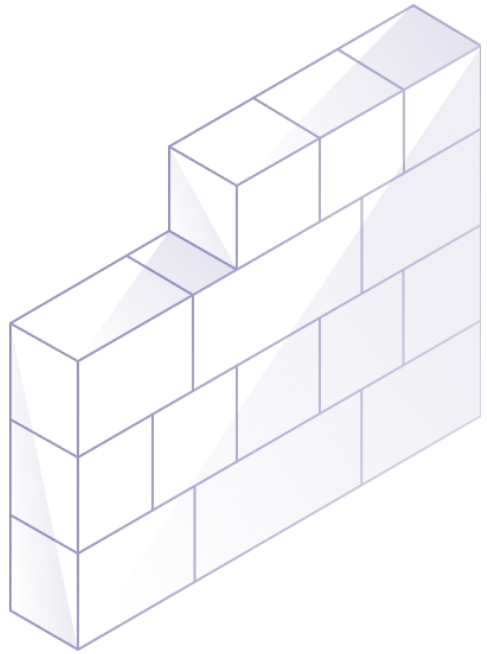
  — Возможность самостоятельной смены в КК New

- **Route Server**

  — BGP фильтрация
  — RPKI валидация
  — Блокировка приватных AS/сетей/default
  — Контроль соответствию IRR

- **Route Server:**

  — Roles (RFC 9234) New



Защита участников: Enhanced Blackhole

- Отдельное оборудование для фильтрации трафика
- Полная блокировка DDoS во время атаки
- Участник отдаёт агрегат с BGP community
- Блокируемый маршрут (/25-/32) с BGP community
- Трафик агрегата попадает на систему очистки и очищенный возвращается к участнику

Защита участников: DDoS Protection

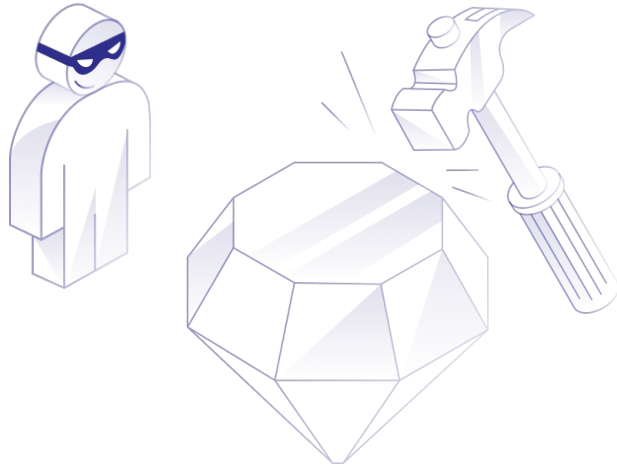
BGP FlowSpec

— Отдельная сессия для обмена FlowSpec data

— Гибкие фильтры под любые условия

— Очистка на аппаратном уровне

— Быстрая блокировка изменяемых векторов атаки



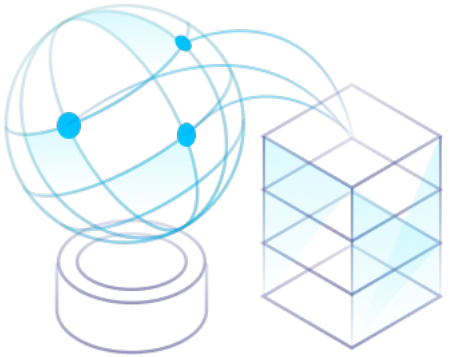
Защищённые пиринговые группы

- Защита от атак за счет изоляции от Public Internet
- Выделенный приватный VLAN, не пересекающийся с другими
- Возможность использования любых диапазонов IP и приватных AS
- Выделенный Route Server для упрощения обмена
- Свои «правила» обмена и приёма новых участников
- **Насыщение дополнительным контентом – своя экосистема**
- Контроль и предотвращение нарушений 24x7x365

Anycast сервисы

Anycast DNS

- Ультра быстрый ответ на запросы
- Надежность: не зависит от работоспособности отдельных узлов
- Доступность 100%
- Поддержка DNSSec
- Редактор DNS-зон и white-label: своё имя для сервиса



Публичный DNS резолвер

- Фильтрация с использованием XDP (eBPF)
- Распределенный сервис Anycast DNS
- Зеркало корневой зоны
- Многоуровневая защита от DNS атак

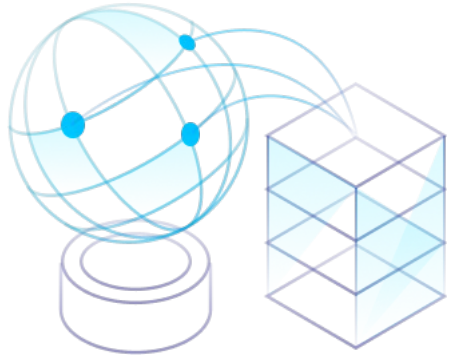
  RRL на уровне ядра, на уровне фильтров, на уровне приложения

Anycast сервисы

Публичный NTP сервис

- Новая модель frontend-backend Stratum 1
- Приоритет GLONASS над всеми другими
- Поддержка NTPd и Chrony
- Защита от атак за счет Anycast

In progress



Итоги

- Сетевая безопасность
  - Регулярный процесс гигиены
  - Постоянное совершенствование
  - Требует постоянно денег
- MSK-IX помогает:
  - Улучшать связанность
  - Снижать негативное воздействие внешнего мира
  - Связаться с контрагентами и сервисами
  - Поддерживать основу безопасного интернета

Спасибо за внимание
Ваши вопросы?

Александр Ильин
Технический директор MSK-IX