НОРСИ-ТРАНС

Закрытое Акционерное Общество

Решения для противодействия DDoS-атакам магистрального уровня

Докладчик: Волков Алексей

Дата: 19 сентября 2017 года

Классификация DDoS атак

Атаки на канал

- UDP/ICMP Based, Amplification и др.

Атаки на уровень протоколов

- TCP Syn Flood, ICMP и др.

Атаки на уровень приложений

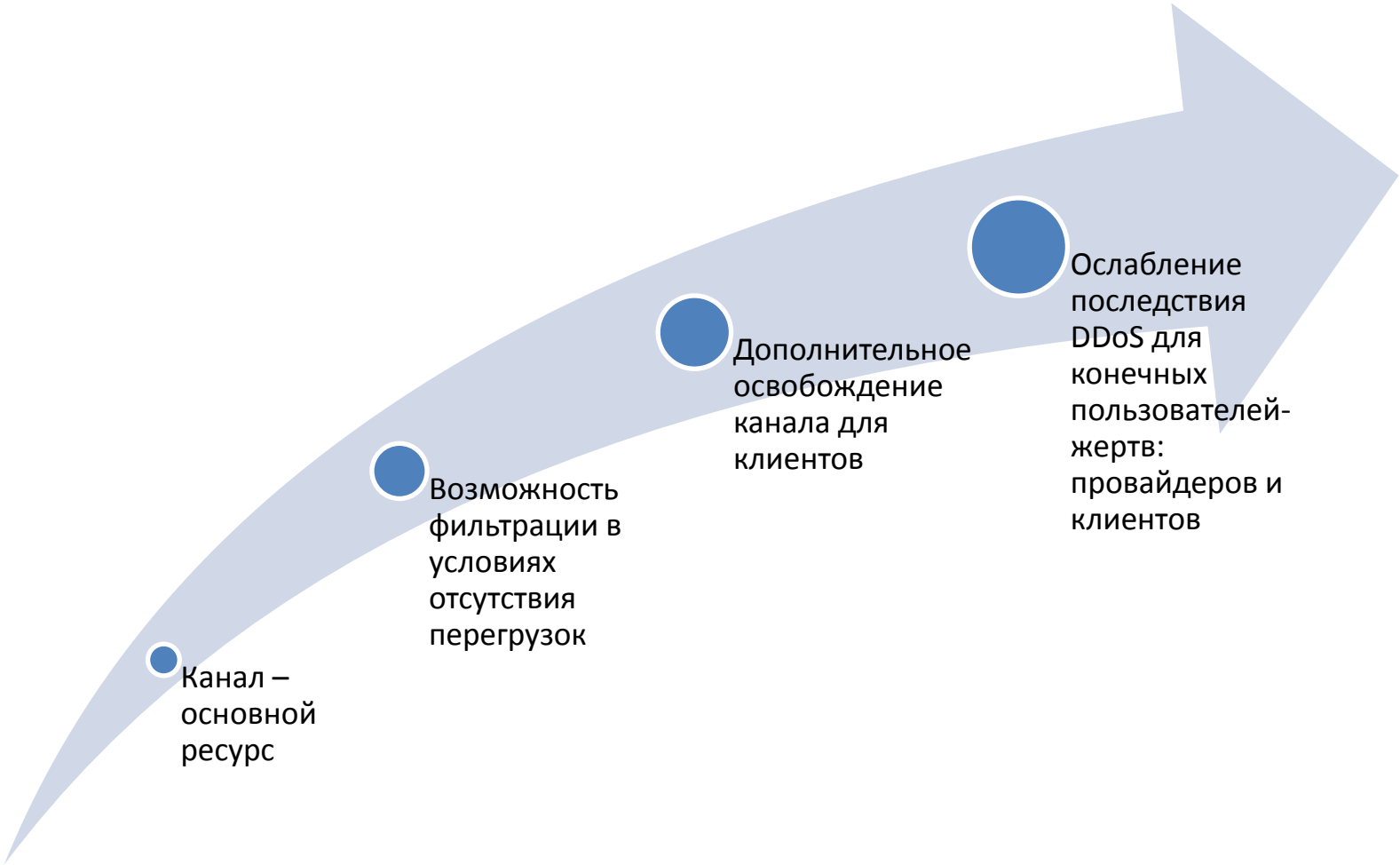
- HTTP Get Flood, HTTP Pingback, Slowloris и др.

НОРСИ-ТРАНС
Закрытое Акционерное Общество

Схемы включения решений противодействию DDoS

1. Противодействие в сети провайдера услуг.
   - Анализ на основе NetFlow, SPAN
   - Фильтрация в inline, либо в ассиметричной схеме BGP маршрутизации
   - Поиндицентное включение
   - Необходимы человеческие ресурсы и канальные мощности.
2. Противодействие в сети провайдера облачной защиты от DDoS
   - Постоянная фильтрация, либо гибридная схема – анализ трафика с помощью сенсоров, переключение по инциденту
   - Экономически обоснованные траты на человеческие ресурсы и канальные мощности
   - Необходимость перенаправления своего трафика в сеть сервиса
   - Возможное увеличение сетевых задержек
3. **Предложение:** Противодействие в сети магистрального провайдера
   - Невозможность стандартных подходов противодействия - нет явных ресурсов, которые защищаем
   - Постоянная фильтрация
   - Большая ответственность перед клиентами

Зачем фильтровать в магистралях и кто от этого выиграет



Требования к решениям фильтрации в магистральных сетях

НОРСИ-ТРАНС
Закрытое Акционерное Общество

Околонулевой процент «False Positive» срабатываний

Постоянная фильтрация – поинцидентная не подходит в связи с отсутствие защищаемых ресурсов как класса

Прозрачные, хорошо документированные методы фильтрации без эффекта черного ящика

Сверхвысокий уровень отказоустойчивости с возможностью горячего резервирования и поддержкой bypass

Система отчетов по каждому заблокированному пакету

НОРСИ-ТРАНС
Закрытое Акционерное Общество

Методы фильтрации в магистральных сетях

- *Фильтрация «серого» и нераспределенного адресного пространства*
  https://tools.ietf.org/html/bcp38
  http://www.team-cymru.org/bogon-bit-notation.html
  - ✓ **0.0.0.0/8**
  - ✓ **10.0.0.0/8**
  - ✓ **100.64.0.0/10**
  - ✓ **127.0.0.0/8**
  - ✓ **169.254.0.0/16**
  - ✓ **172.16.0.0/12**
  - ✓ **192.0.0.0/24**
  - ✓ **192.0.2.0/24**
  - ✓ **192.168.0.0/16**
  - ✓ **198.18.0.0/15**
  - ✓ **198.51.100.0/24**
  - ✓ **203.0.113.0/24**
  - ✓ **224.0.0.0/3**

Методы фильтрации в магистральных сетях

- Фильтрация «серого» и нераспределенного адресного пространства
- *Запрет уязвимых, устаревших протоколов, а так же протоколов, применение которых оправданно только в локальных сетях*
  - ✓ **CharGEN**
  - ✓ **NetBIOS**
  - ✓ **UDP-based Portmap**
  - ✓ **SSDP**
  - ✓ **и т.д.**

НОРСИ-ТРАНС
Закрытое Акционерное Общество

Методы фильтрации в магистральных сетях

- Фильтрация «серого» и нераспределенного адресного пространства
- Запрет уязвимых, устаревших, сервисных и протоколов, применение которых оправданно только в локальных сетях
- *Черные списки с коротким окном (до 5 секунд) и простыми условиями добавления на основании анализа трафика в коротком окне*
  - ✓ **Количество повторов пакетов с одним SEQ+ACK_SEQ в TCP сессии**
  - ✓ **Количество повторов пакетов в UDP сессии**
  - ✓ **Количество повторов пакетов ICMP**

НОРСИ-ТРАНС
Закрытое Акционерное Общество

Методы фильтрации в магистральных сетях

- Фильтрация «серого» и нераспределенного адресного пространства
- Запрет уязвимых, устаревших, сервисных и протоколов, применение которых оправданно только в локальных сетях
- Черные списки с коротким окном (до 5 секунд) и простыми условиями добавления на основании анализа трафика в коротком окне
- *Алгоритмы проверки сборки IP фрагментов в заданном окне*

НОРСИ-ТРАНС
Закрытое Акционерное Общество

Методы фильтрации в магистральных сетях

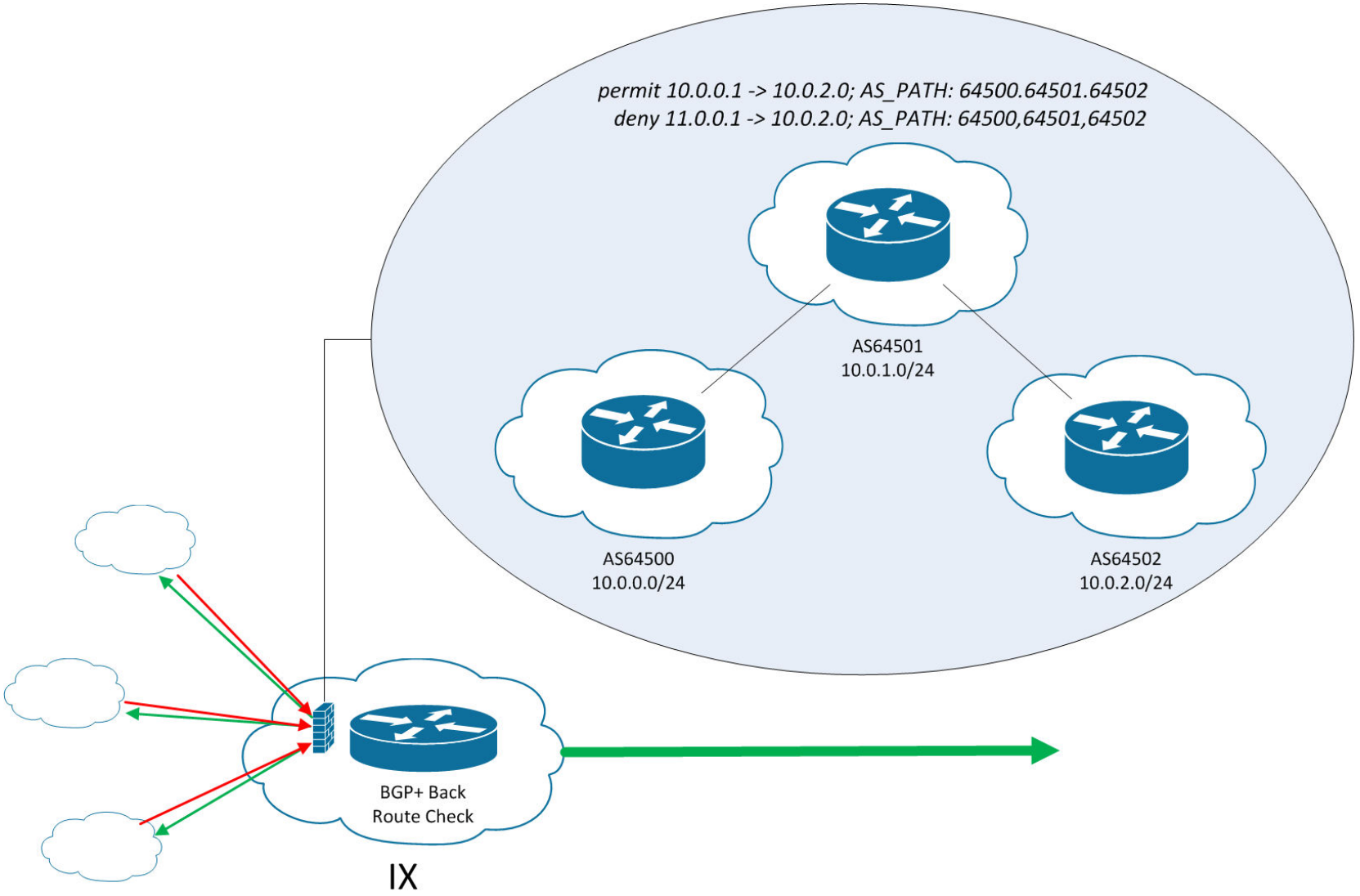
- Фильтрация «серого» и нераспределенного адресного пространства
- Запрет уязвимых, устаревших, сервисных и протоколов, применение которых оправданно только в локальных сетях
- Черные списки с коротким окном (до 5 секунд) и простыми условиями добавления на основании анализа трафика в коротком окне
- Алгоритмы проверки сборки IP фрагментов в заданном окне
- *Фильтрация L3-L4 malformed пакетов*
  - ✓ **Структура пакетов согласно RFC**
  - ✓ **Проверка контрольных сумм L3, L4**

НОРСИ-ТРАНС
Закрытое Акционерное Общество

Методы фильтрации в магистральных сетях

- Фильтрация «серого» и нераспределенного адресного пространства
- Запрет уязвимых, устаревших, сервисных и протоколов, применение которых оправданно только в локальных сетях
- Черные списки с коротким окном (до 5 секунд) и простыми условиями добавления на основании анализа трафика в коротком окне
- Алгоритмы проверки сборки IP фрагментов в заданном окне
- Фильтрация L3-L4 malformed пакетов
- *Концепт. Частичное противодействие возможности спуфинга на основе BGP маршрутной информации*

Частичное противодействие спуфингу. Концепт



Что можем предложить мы. АПК «КРОЗ»

- Большое число рабочих методов фильтрации и противодействия, в том числе описанные выше.
- Сбор и хранение статистической информации по метрикам и атрибутам все уровней модели OSI, получаемой по NetFlow или SPAN без агрегации и прореживания
- Инструменты анализа BGP маршрутной информации, в том числе утечки маршрутов. Возможность сопоставления этой информации со статистикой по трафику.
- Возможность простого наращивания пропускной способности, до 160Gbps в 1U
- Возможность построения кластеров с собственными решениями bypass, а так же аппаратным решением балансировки/агрегации и фильтрации трафика **NanoSwitch**

НОРСИ-ТРАНС
Закрытое Акционерное Общество

Спасибо за внимание!

Волков Алексей,
ЗАО «НОРСИ-ТРАНС»
email: avolkov@norsi-trans.ru