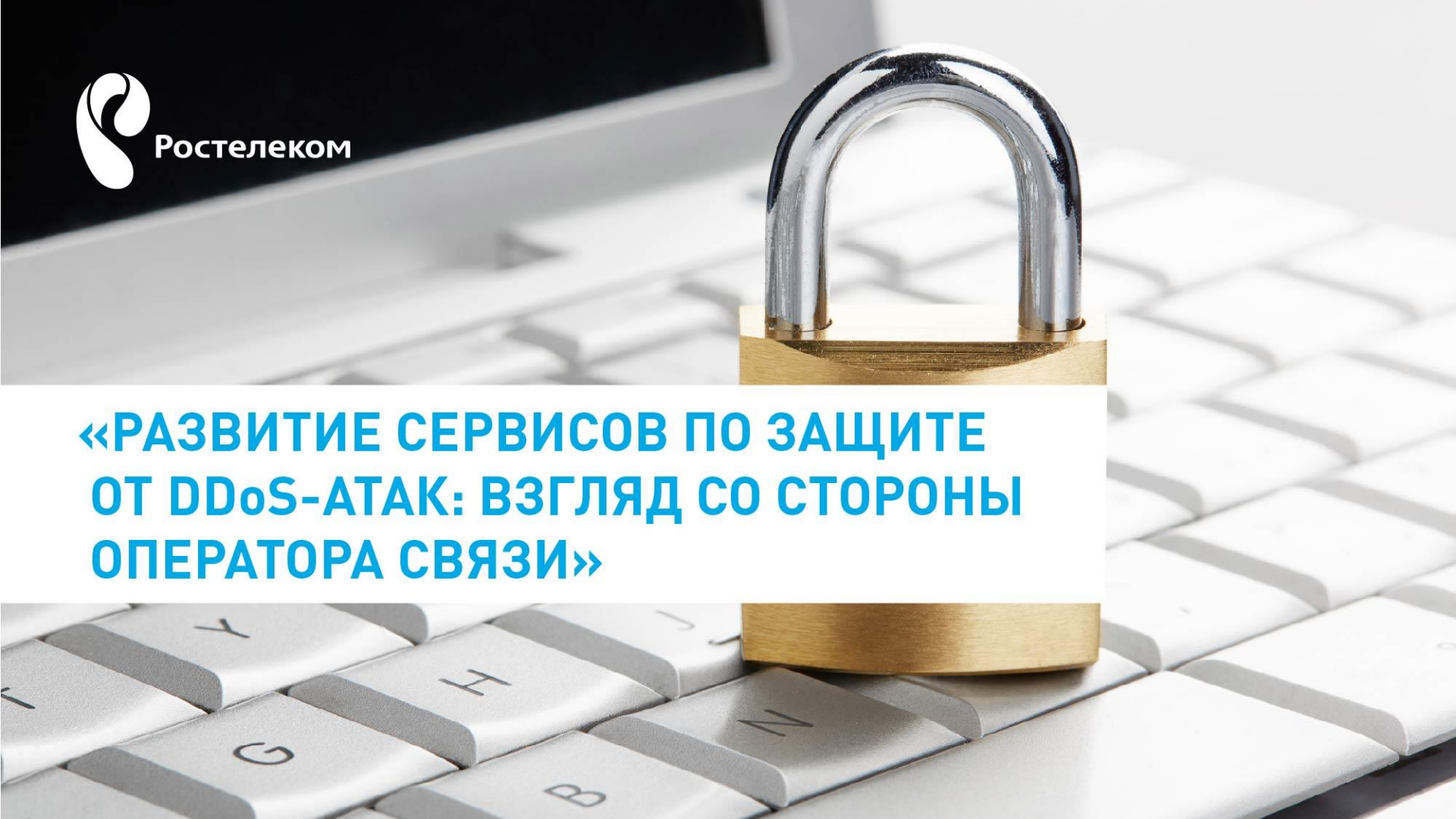
Ростелеком



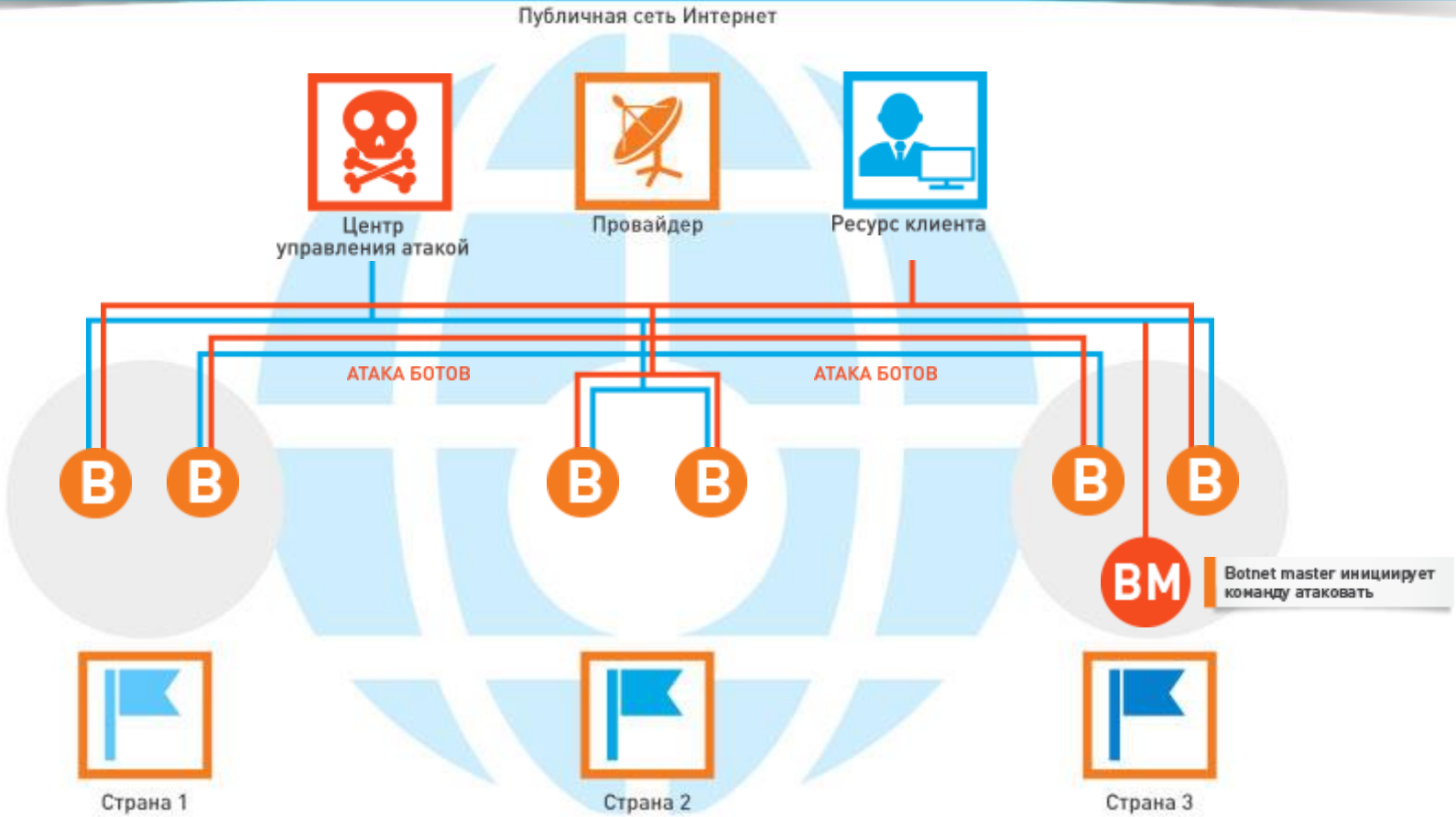
«РАЗВИТИЕ СЕРВИСОВ ПО ЗАЩИТЕ ОТ DDoS-АТАК: ВЗГЛЯД СО СТОРОНЫ ОПЕРАТОРА СВЯЗИ»

РОСТЕЛЕКОМ В ЦИФРАХ

РОСТЕЛЕКОМ В ЦИФРАХ

28 000 000	АБОНЕНТОВ ФИКСИРОВАННОЙ ГОЛОСОВОЙ СВЯЗИ
11 200 000	АБОНЕНТОВ ШИРОКОПОЛОСНОГО ДОСТУПА В ИНТЕРНЕТ
8 200 000	АБОНЕНТОВ ПЛАТНОГО ТЕЛЕВИДЕНИЯ
80	РЕГИОНАЛЬНЫХ ФИЛИАЛОВ
2 500	ТОЧЕК ПРОДАЖ И ОБСЛУЖИВАНИЯ
160 000	СОТРУДНИКОВ
БОЛЬШЕ 50%	АКЦИЙ КОМПАНИИ КОНТРОЛИРУЕТ ГОСУДАРСТВО

КАК ПРОИСХОДЯТ DDoS-АТАКИ?



Ростелеком

САМЫЕ ПОПУЛЯРНЫЕ АТАКИ?
– REFLECTION / AMPLIFICATION

КАК УСТРОЕНА AMPLIFICATION/REFLECTION АТАКА?

Ростелеком

NTP(для примера)

СЕРВЕРЫ, МАРШРУТИЗАТОРЫ, CPE

172.19.234.6

КАК УСТРОЕНА AMPLIFICATION/REFLECTION АТАКА?

Ростелеком

NTP серверы

UDP/80 – UDP/123, ~50 БАЙТ/ПАКЕТ
ИСТОЧНИК (СПУФИНГ): 172.19.234.6
НАЗНАЧЕНИЕ: РЯД СЕРВЕРОВ NTP
NTP ЗАПРОС: MONLIST

172.19.234.6

КАК УСТРОЕНА AMPLIFICATION/REFLECTION АТАКА?

Ростелеком

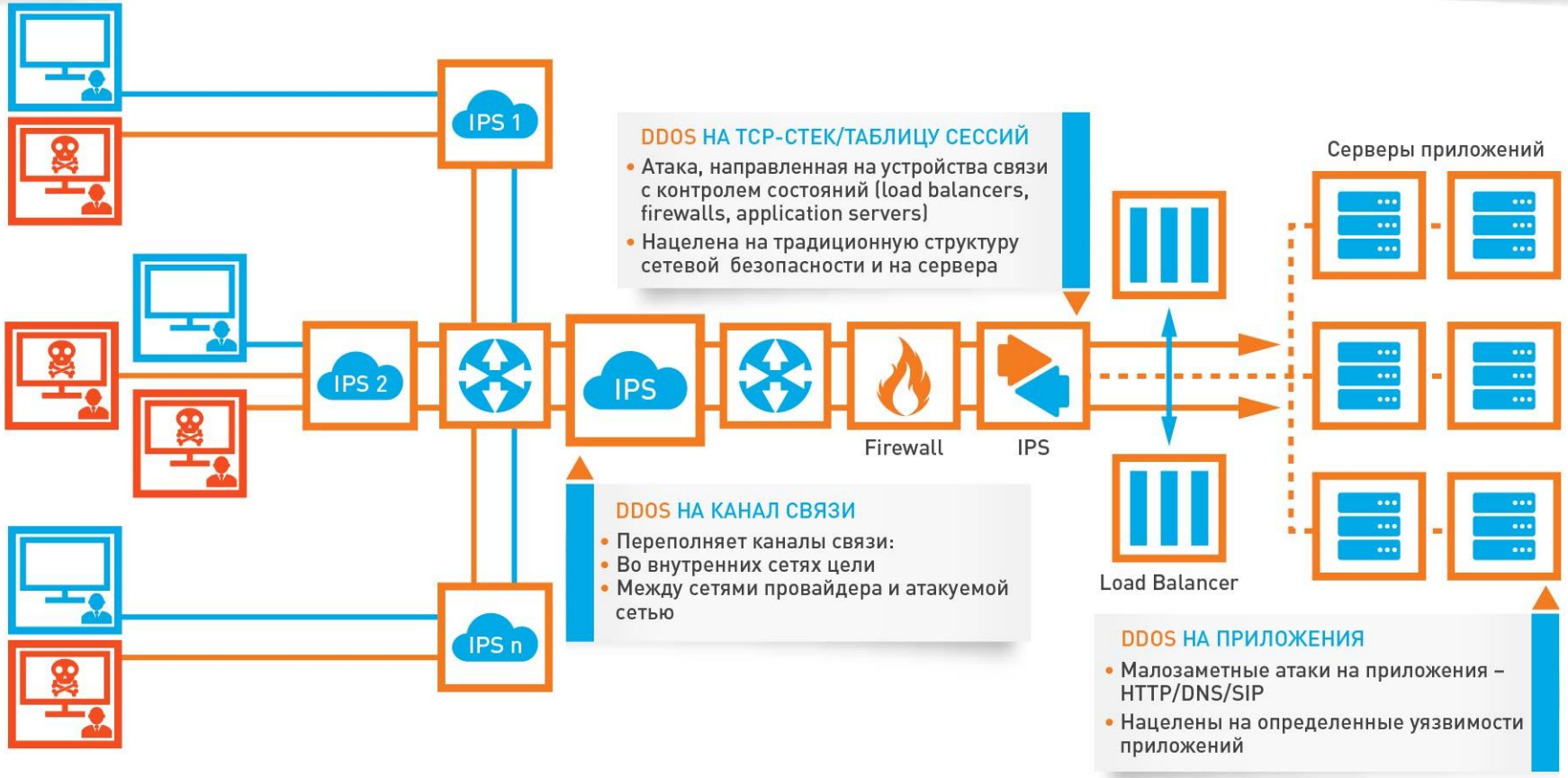
NTP серверы

UDP/123 – UDP/80, ~468 БАЙТ
ИСТОЧНИК: NTP СЕРВЕР
ПОЛУЧАТЕЛЬ: 172.19.234.6
ОТВЕТ: ДАННЫЕ О 600 ХОСТАХ

172.19.234.6

ВИДЫ DDoS-АТАК

Ростелеком



DDOS НА TCP-СТЕК/ТАБЛИЦУ СЕССИЙ

- Атака, направленная на устройства связи с контролем состояний (load balancers, firewalls, application servers)
- Нацелена на традиционную структуру сетевой безопасности и на сервера

DDOS НА КАНАЛ СВЯЗИ

- Переполняет каналы связи:
- Во внутренних сетях цели
- Между сетями провайдера и атакуемой сетью

DDOS НА ПРИЛОЖЕНИЯ

- Малозаметные атаки на приложения – HTTP/DNS/SIP
- Нацелены на определенные уязвимости приложений

МАКСИМАЛЬНЫЙ ОБЪЕМ DDoS-АТАКИ В 2014 ГОДУ (ОТРАЖЕНИЕ КОМПЛЕКСОМ КОМПАНИИ «РОСТЕЛЕКОМА»

Ростелеком

Alert Summary

DoS Alert 2825751 Classification: Possible Attack Mar 17 10:49 - Ongoing (0:17)

Severity Level	Severity Percent	Impact	Type	Affected	Direction	Mitigations
High ●●●	19,452.5% of 71.6 Mbps	124.9 Gbps 33.4 Mpps	Profiled Bandwidth	cm_MSK [redacted]	Incoming	None

Alert Characterization

Sources	Source Ports	Destinations	Destination Ports	Protocols	TCP Flags
0.0.0.0/0 ? 195.0.0.0/8 ?	123 (ntp) 0	[redacted]/32 ? 0.0.0.0/0 ?	80 (www-http) 64 - 127	udp (17) tcp (6)	SAFRP (0x1F)

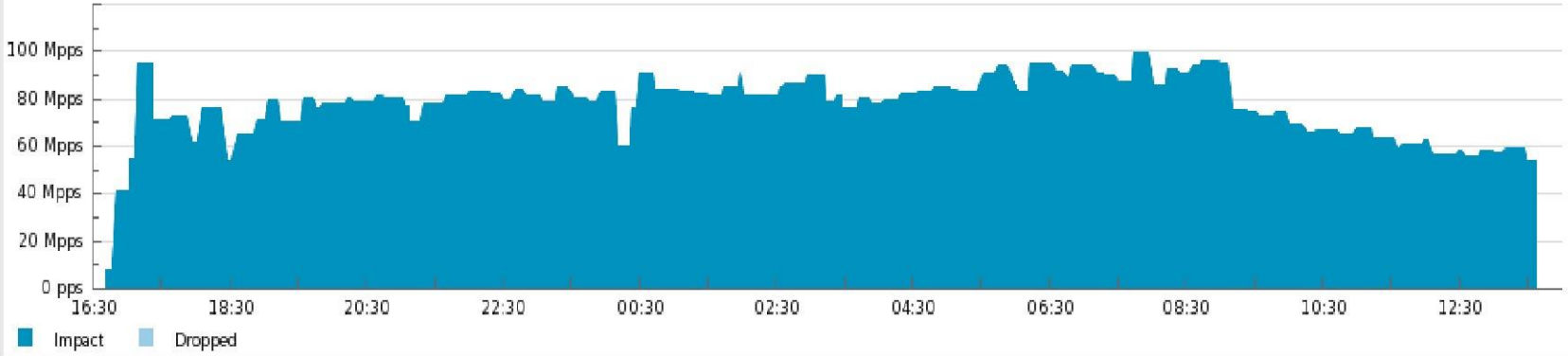
Generate Raw Flows Report View Raw Flows Report

МАКСИМАЛЬНЫЙ ОБЪЕМ DDoS-АТАКИ В 2015 ГОДУ (ОТРАЖЕНИЕ КОМПЛЕКСОМ КОМПАНИИ «РОСТЕЛЕКОМА»

Ростелеком

Alert Summary

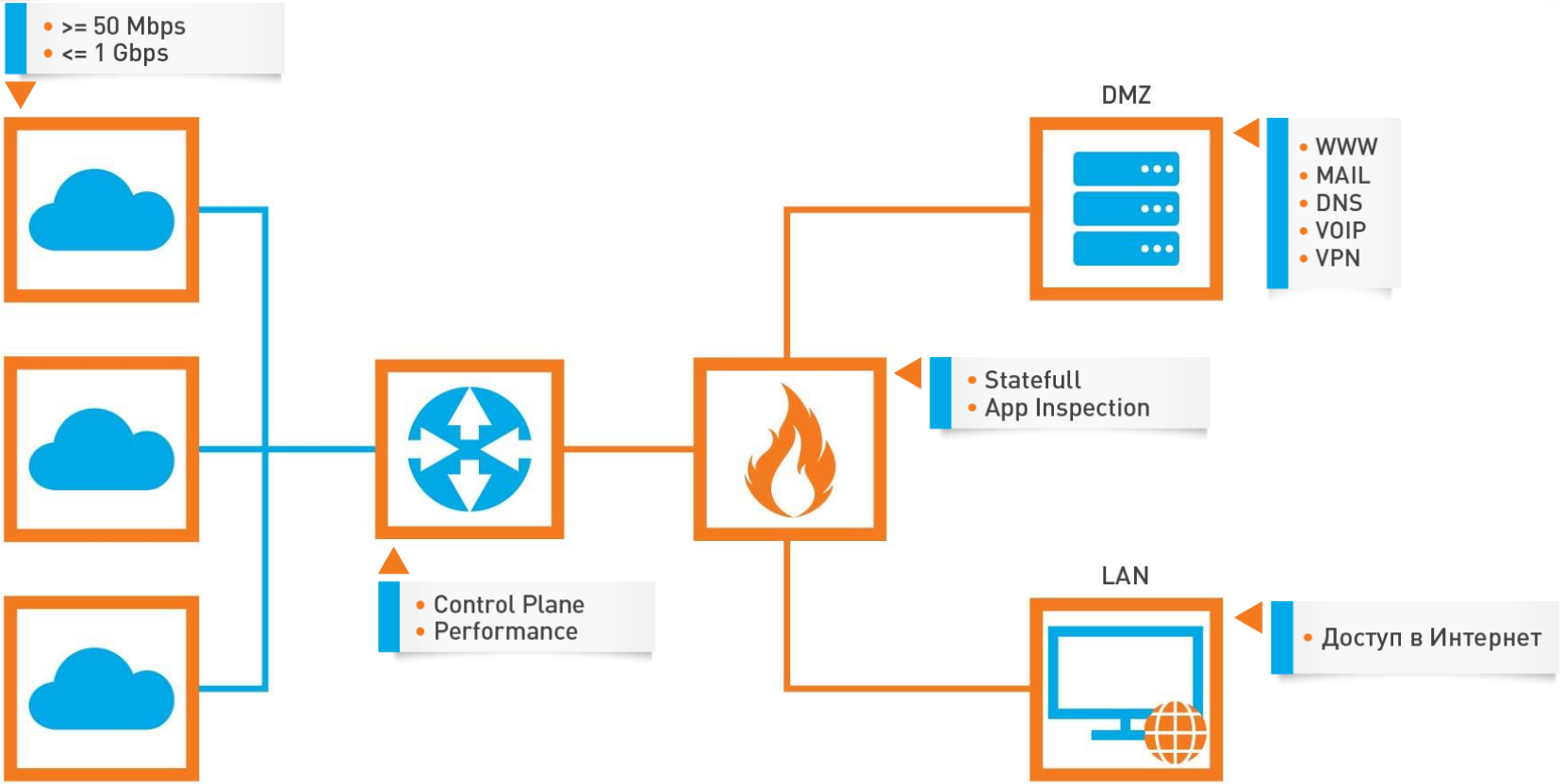
DoS Alert 4019814 **Classification:** Possible Attack **Jan 26 16:29 - Ongoing (21:06)**



Severity Level	Severity Percent	Impact	Type	Affected	Direction	Mitigations
High	388,683.0% of 10 Kpps	32.0 Gbps 99.2 Mpps	TCP SYN Misuse	[redacted]	Incoming	[redacted] tms

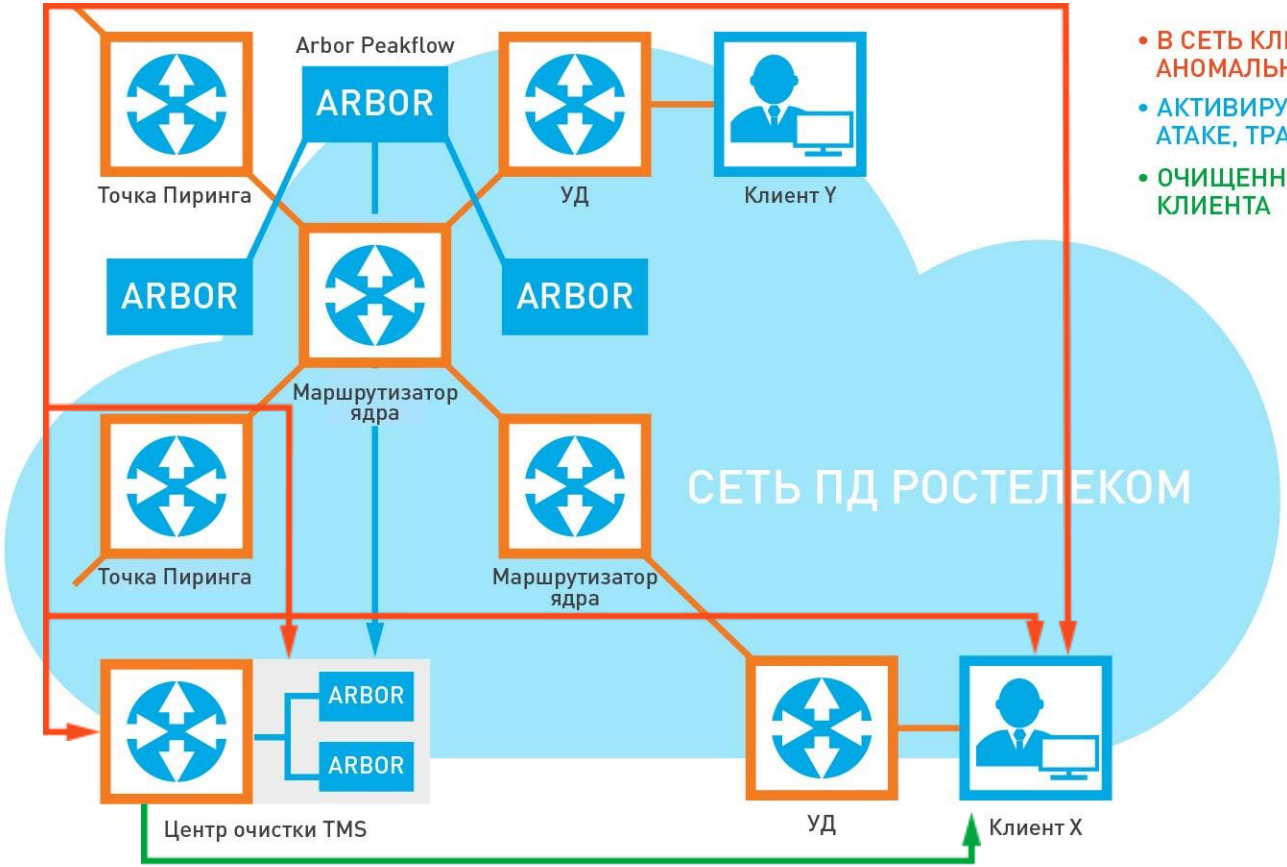
ТИПОВОЕ ПОДКЛЮЧЕНИЕ КОМПАНИЙ К ИНТЕРНЕТУ

Ростелеком



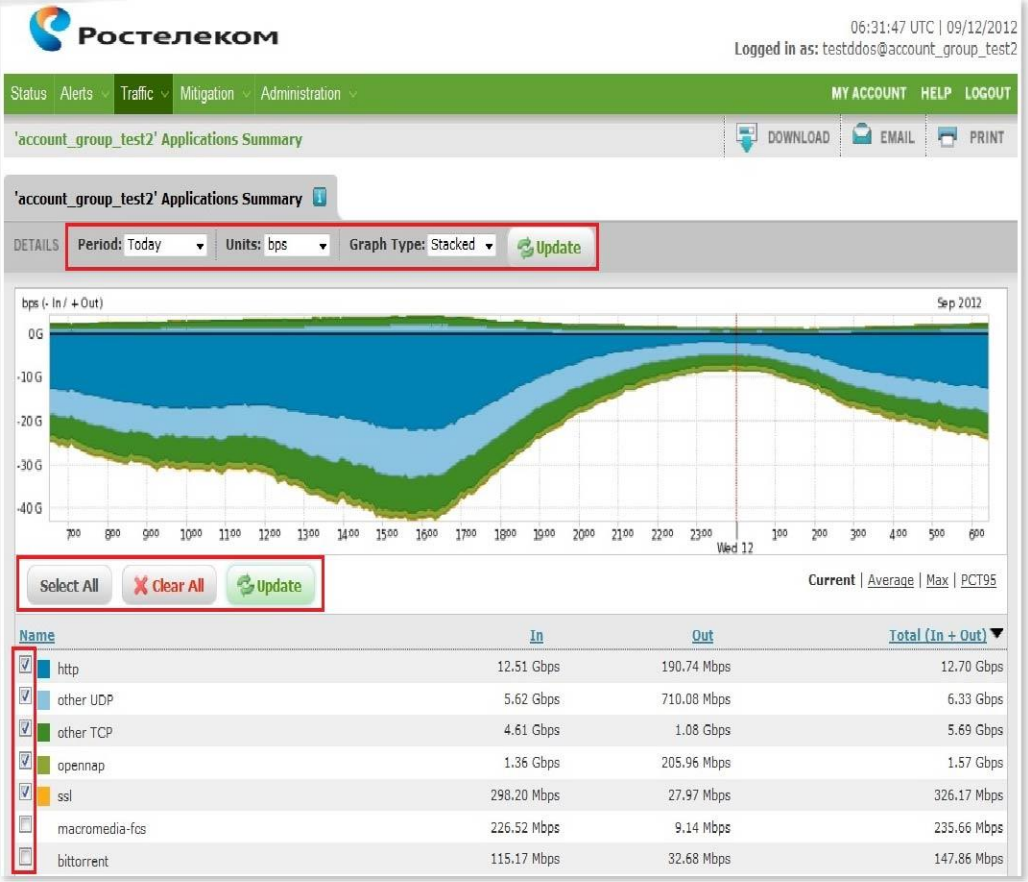
ЗАЩИТА НА СТОРОНЕ КЛИЕНТА (БЕЗ УЧАСТИЯ ОПЕРАТОРА)

СХЕМА СИСТЕМЫ АНАЛИЗА ТРАФИКА И ЗАЩИТЫ ОТ DDoS АТАК



- В СЕТЬ КЛИЕНТА НАЧИНАЕТ ПОСТУПАТЬ АНОМАЛЬНЫЙ ТРАФИК АТАКИ
- АКТИВИРУЕТСЯ СИСТЕМА ПРОТИВОДЕЙСТВИЯ АТАКЕ, ТРАФИК НАПРАВЛЯЕТСЯ НА ОЧИСТКУ
- ОЧИЩЕННЫЙ ТРАФИК ПЕРЕДАЁТСЯ В СЕТЬ КЛИЕНТА

КЛИЕНТСКИЙ ПОРТАЛ



Ключевыми функциями портала являются оповещение клиента о начале и окончании атак

ПРИ ВОЗНИКНОВЕНИИ АТАКИ ПРЕДУСМОТРЕНЫ ТРИ ТИПА ОПОВЕЩЕНИЙ:

«ЗЕЛЕНОЕ» – небольшое превышение трафика, малая вероятность наличия атаки

«ЖЕЛТОЕ» – умеренное превышение, вероятность наличия атаки средняя

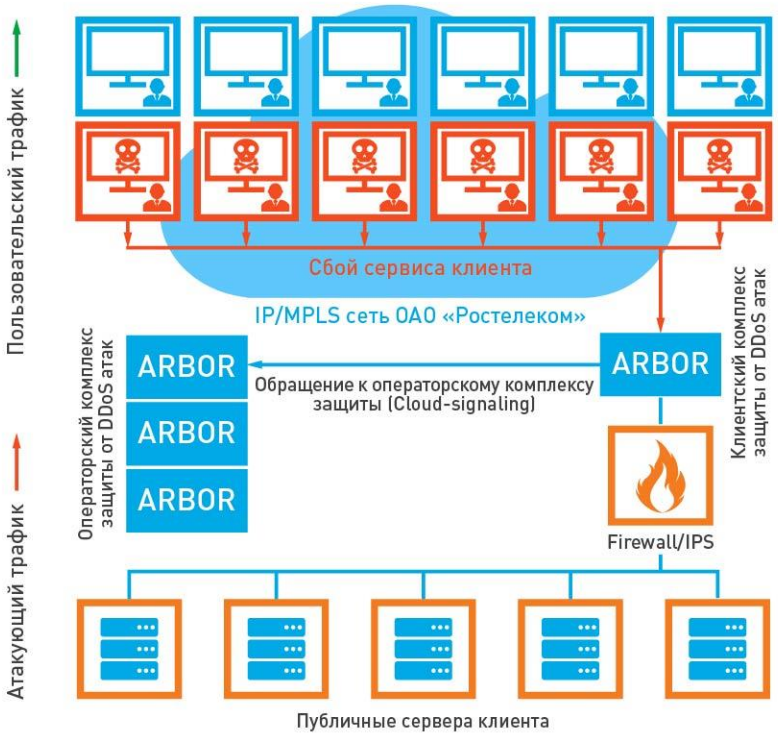
«КРАСНОЕ» – критическое превышение, совершается атака

ОПЦИЯ CLOUD-SIGNALING

Ростелеком

СЕРВИС КЛИЕНТА ПОД АТАКОЙ (БЕЗ УЧАСТИЯ ОПЕРАТОРСКОГО КОМПЛЕКСА ЗАЩИТЫ ОТ DDoS АТАК

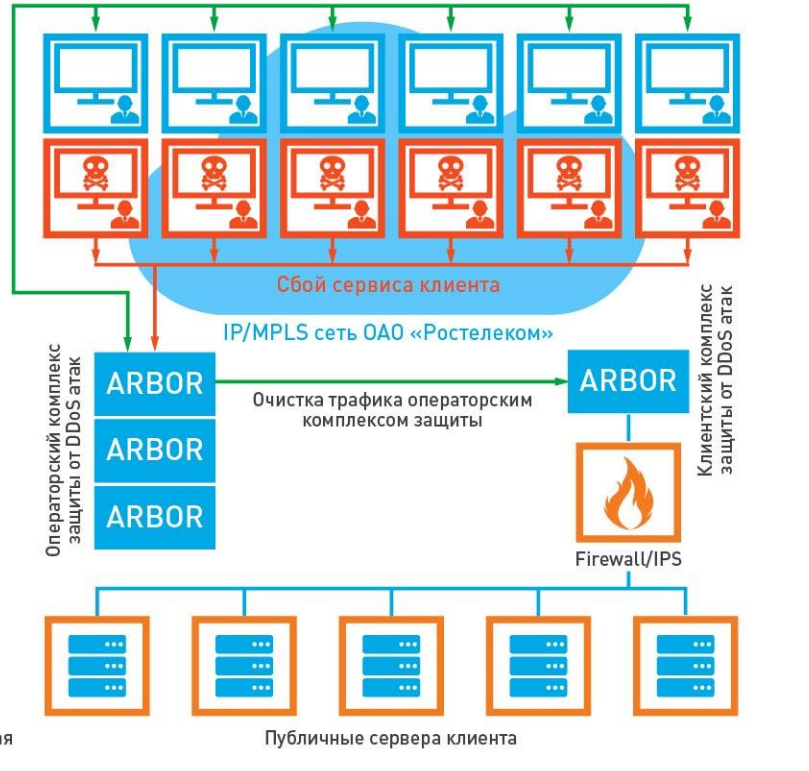
Злоумышленники вытесняют трафик пользователей



Дополнительная опция

СЕРВИС КЛИЕНТА ПОД АТАКОЙ (С УЧАСТИЕМ ОПЕРАТОРСКОГО КОМПЛЕКСА ЗАЩИТЫ ОТ DDoS АТАК

Пользовательский трафик работает



ПРЕИМУЩЕСТВА ПАО «РОСТЕЛЕКОМ»

КРУПНЕЙШАЯ В ЕВРОПЕ ИНСТАЛЛЯЦИЯ ОПЕРАТОРСКОГО КОМПЛЕКСА ЗАЩИТЫ ARBOR PEAKFLOW

- Позволяет отражать атаки емкостью 160 Гбит/с до уровня приложений
- Позволяет отражать атаки емкостью более 2 Тбит/с за счет отражения атаки на пограничных маршрутизаторах

КРУПНЕЙШАЯ КОМАНДА СПЕЦИАЛИСТОВ В СНГ ПО ОТРАЖЕНИЮ DDoS АТАК

- 50 инженеров обученных Arbor Peakflow
- Опыт отражения атак пиковой производительностью 130 Гбит/с
- Ежедневная фильтрация более 15 инцидентов емкостью более 10 Гбит/с
- Опыт успешной защиты информационных ресурсов Олимпийских Игр Сочи 2014

ПРЕИМУЩЕСТВА ПАО «РОСТЕЛЕКОМ»

Ростелеком

- Система Arbor ATLAS отслеживает около половины глобального интернет трафика, что позволяет знать всю текущую информацию по атакам и противодействию им
- Всем клиентам предоставляется доступ в личный кабинет по управлению услугой
- Выделенная круглосуточная смена по отражению DDoS атак
- Стоимость услуги не зависит от мощности и количества DDoS-атак
- Единственный оператор связи, имеющий опыт подключения клиентских устройств защиты от DDoS - Arbor Pravail (опция Cloud-signaling)
- Емкость российских пиринговых стыков составляет более 1,7 Тбит/с, международных пиров более 500 Гбит/с, емкость стыков с МН-апстримами – 700 Гбит/с, что позволяет контролировать существенную долю интернет трафика в РФ и отражать атаки на границе сети

СПАСИБО ЗА ВНИМАНИЕ!

Ростелеком

КАРПУЗИКОВ АЛЕКСАНДР СЕРГЕЕВИЧ

РУКОВОДИТЕЛЬ НАПРАВЛЕНИЯ
ПАО «РОСТЕЛЕКОМ»

ALEKSANDR.KARPUZIKOV@RT.RU
+7 (915) 486-36-15