УЦСБ
Интегратор Сильных Решений

Уральский центр систем безопасности
Технологии защиты бизнеса
Аудит. Проектирование. Внедрение. Сопровождение.

ARBOR NETWORKS

Защита от DDoS-атак. Сегодня. В России

Илья Яблонко, CISSP
менеджер по развитию решений
сетевой безопасности
ООО «УЦСБ»

Алексей Холмов
Systems Engineer, RCIS
Arbor Networks EMEA

Содержание

1. DDoS: статистика и основные тенденции
2. Защита. Исторически и сегодня
3. Решения Arbor Networks
4. Операторы связи. Ростелеком

УЦСБ
Интегратор Сильных Решений

Уральский центр систем безопасности
Технологии защиты бизнеса
Аудит. Проектирование. Внедрение. Сопровождение.

ARBOR NETWORKS

Worldwide Infrastructure Security Report

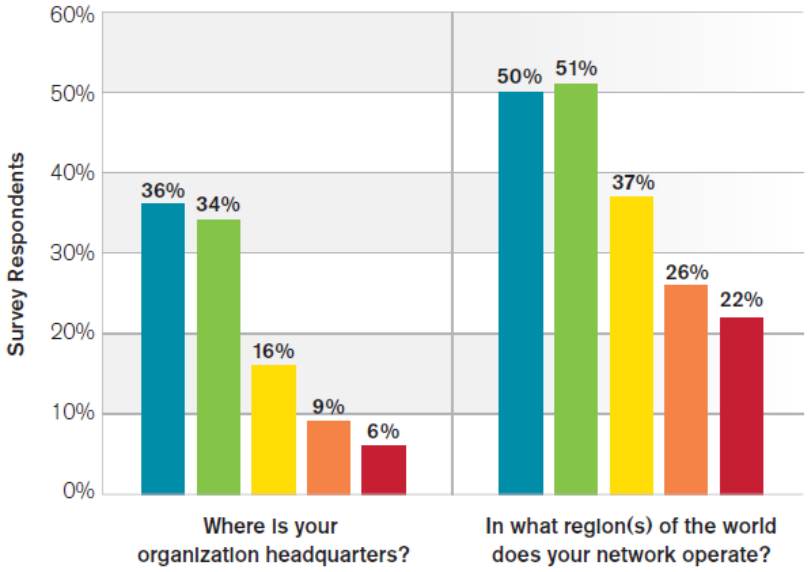
Volume X

www.USSC.ru
www.arbornetworks.com

VII Уральский форум
Информационная безопасность банков

Башкортостан
17 февраля 2015 г

Organization's Geographic Information

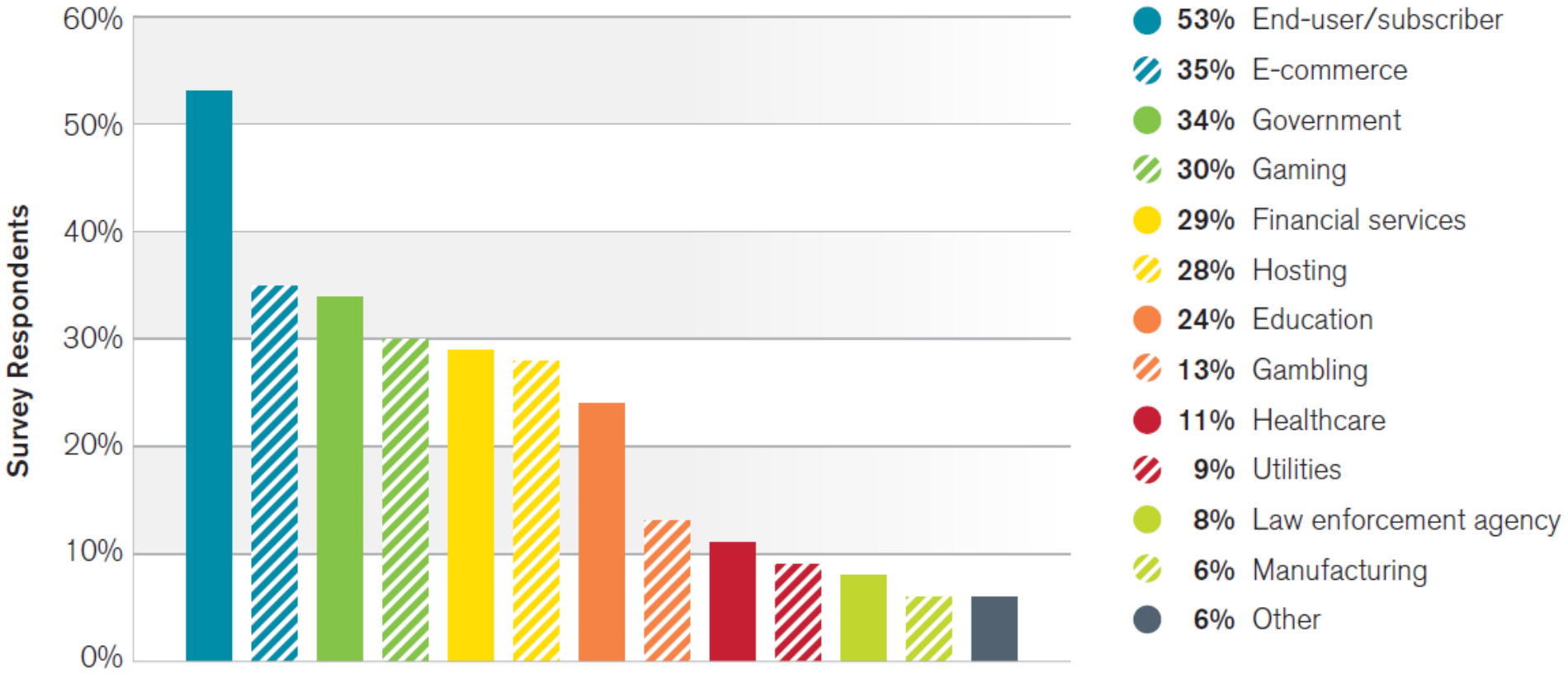


- US and Canada
- Western, Central and Eastern Europe (including Russia and Iceland)
- Asia Pacific and Oceana
- Middle East and Africa
- Latin America

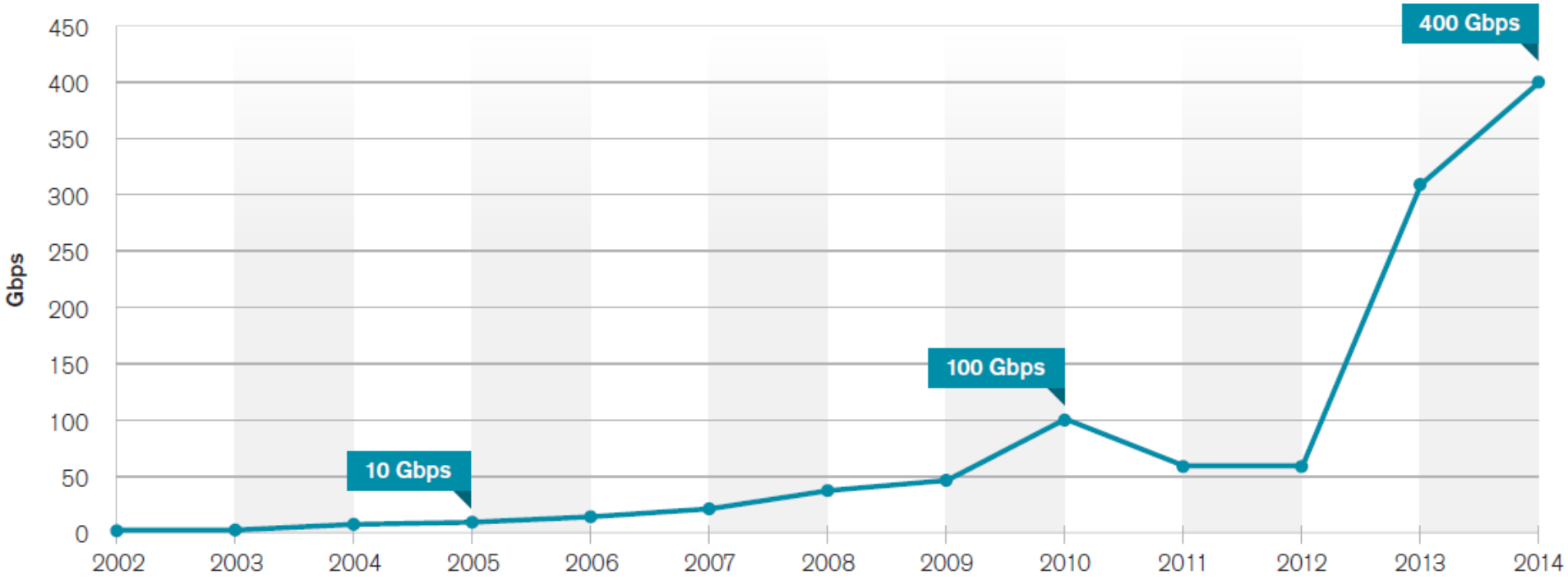
Respondent Organization's Primary Business Function

- 24% Tier 2/3 provider or regional ISP
- 17% Enterprise
- 12% Other (not service provider)
- 10% Tier 1 service provider
- 6% Educational/research
- 6% Managed service provider
- 5% Hosting/data center/co-location services
- 5% Government
- 5% Mobile service provider
- 5% Cloud service provider
- 2% Other (service provider)
- 1% Wireline broadband (MSO, DSL, etc.)
- 1% CDN/content delivery
- 1% DNS registrar/DNS service provider

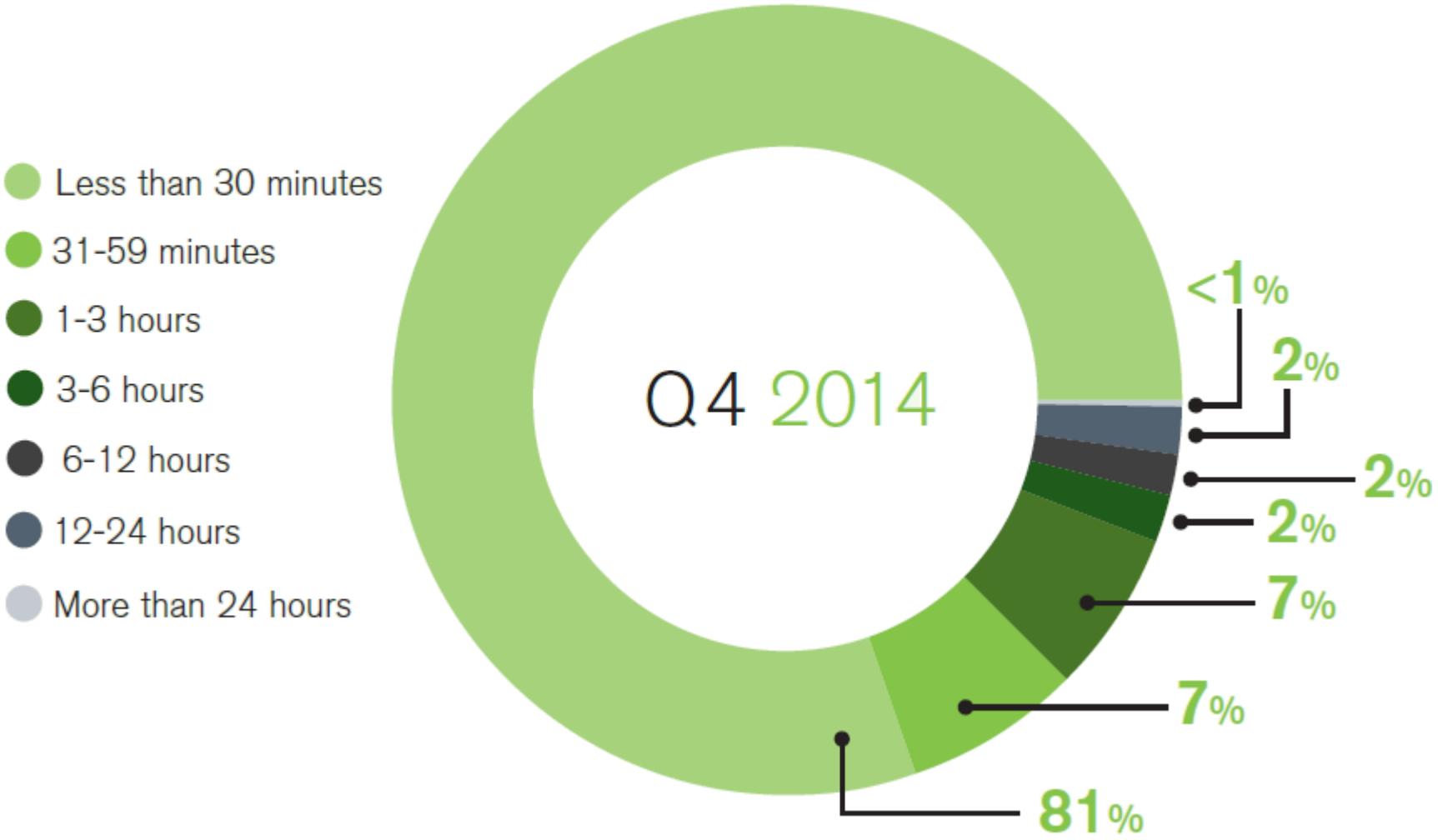
Attack Target Customer Vertical



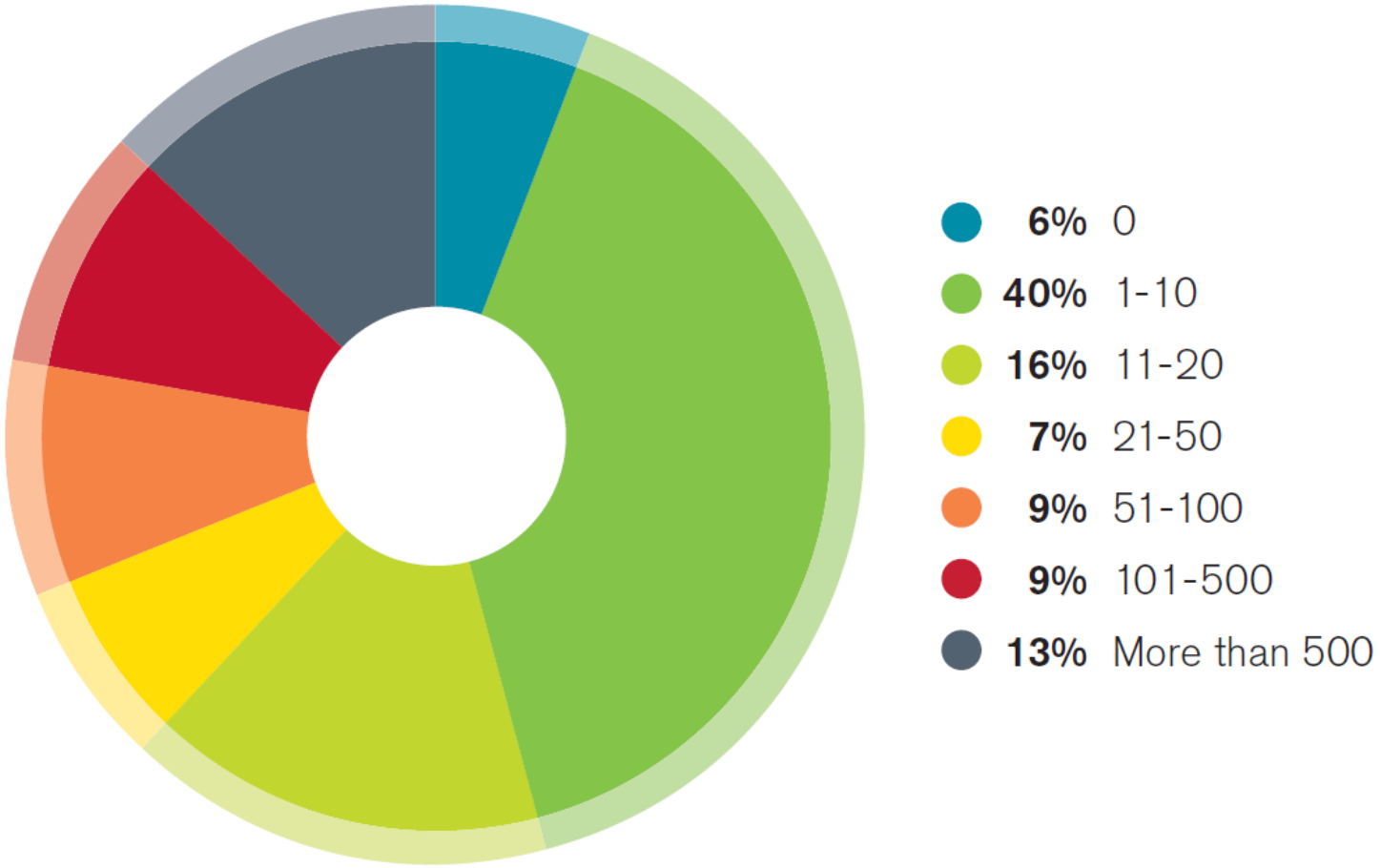
Survey Peak Attack Size Year Over Year



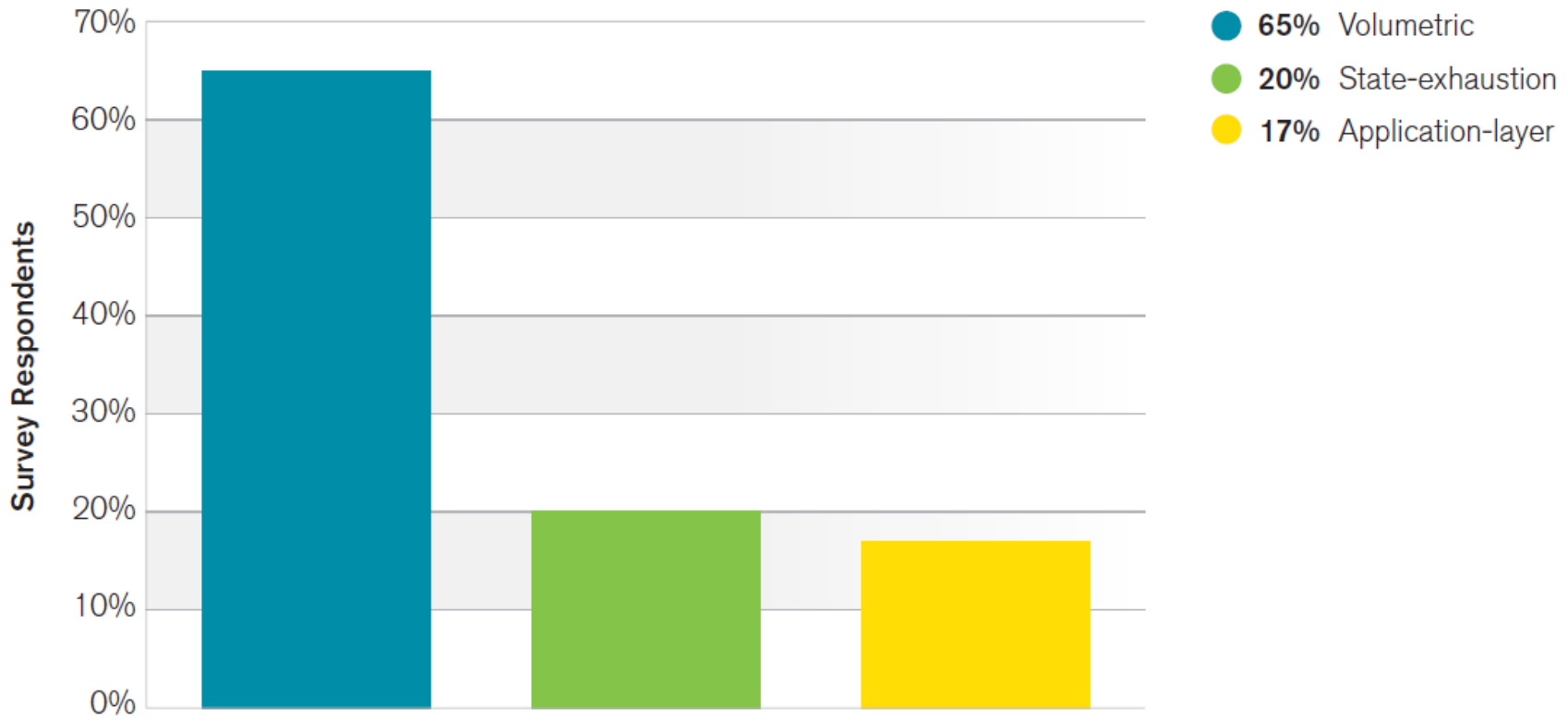
DDoS Attack Duration Breakout



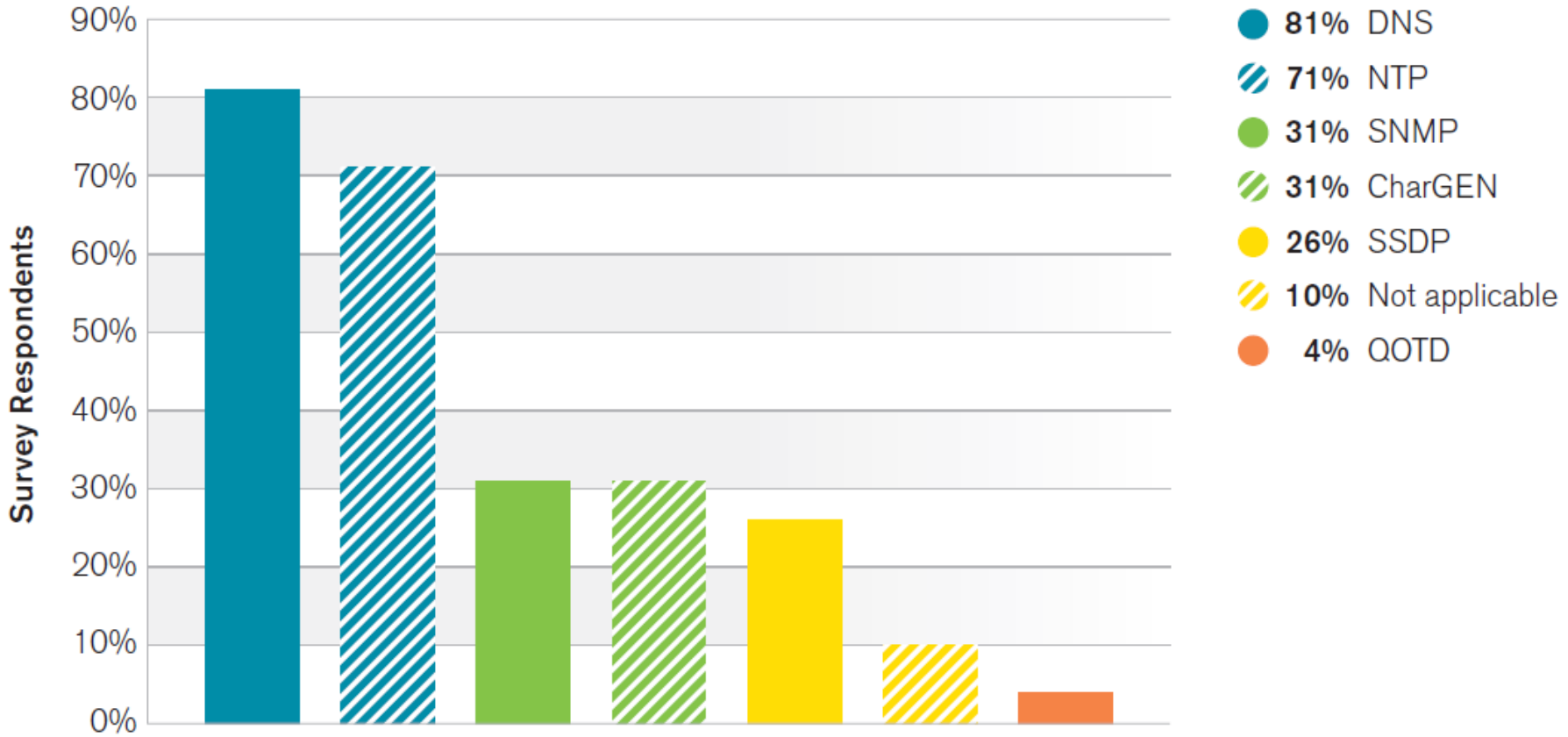
Attack Frequency, Per Month



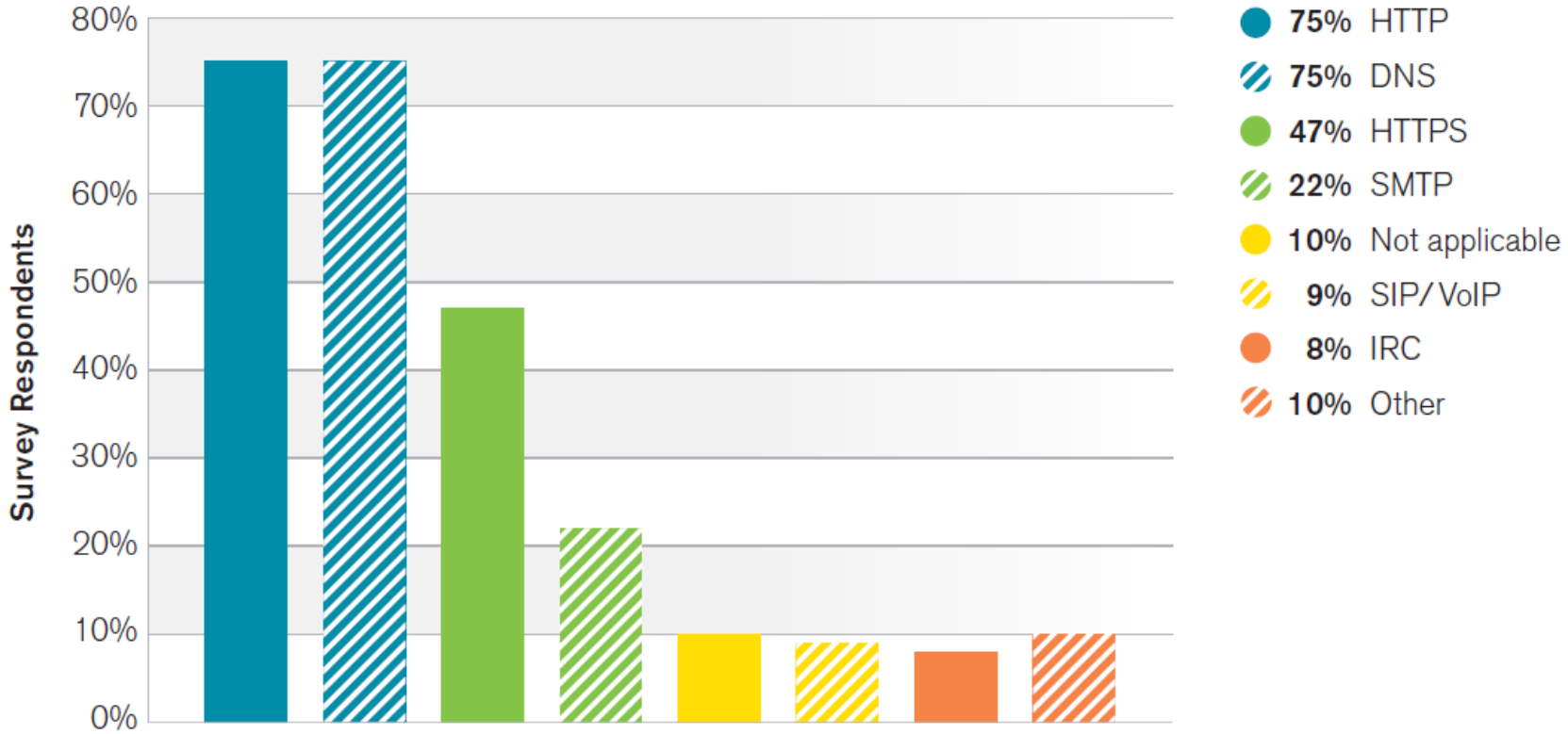
DDoS Attack Types



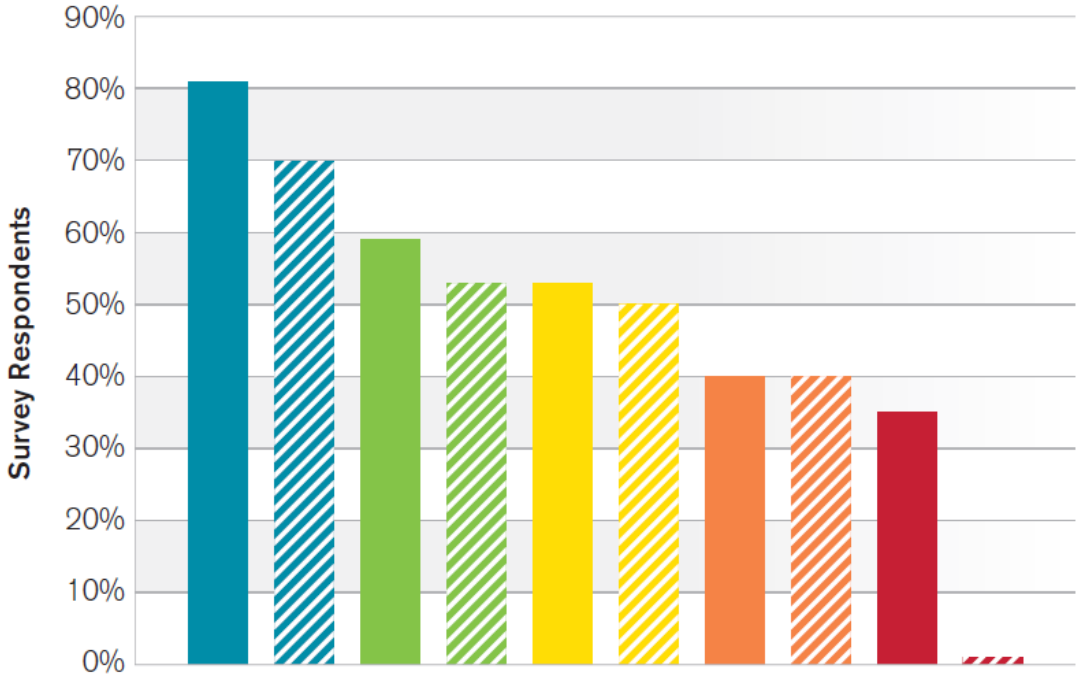
Protocols Used for Reflection/Amplification



Targets of Application-Layer Attacks

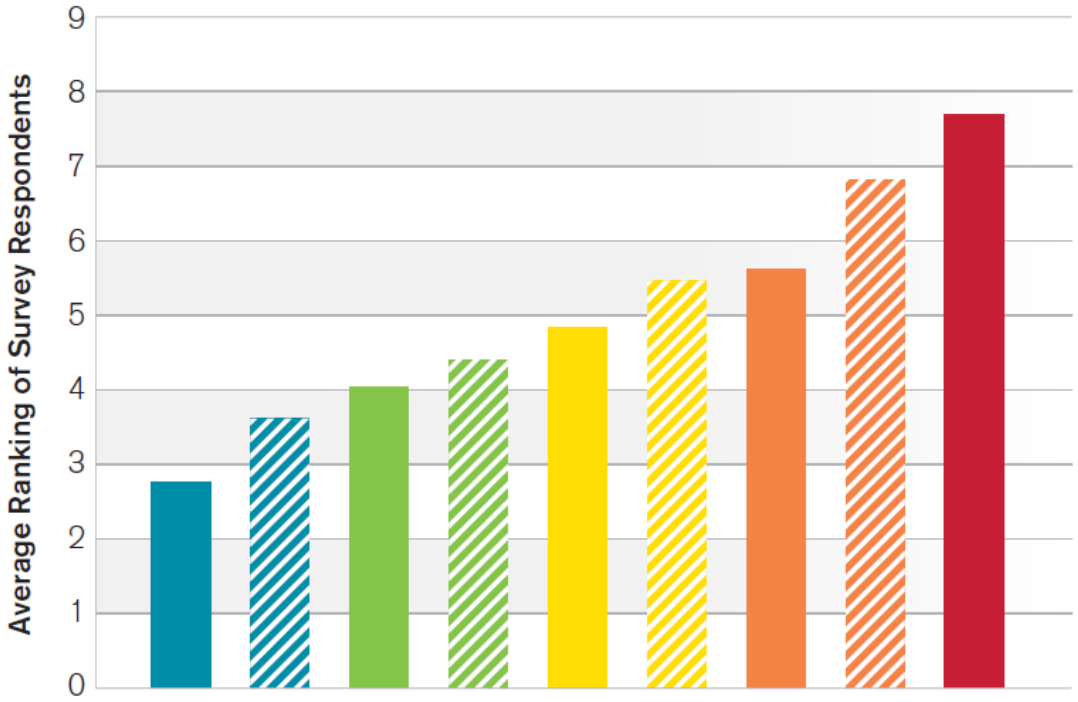


Threat Detection Tools



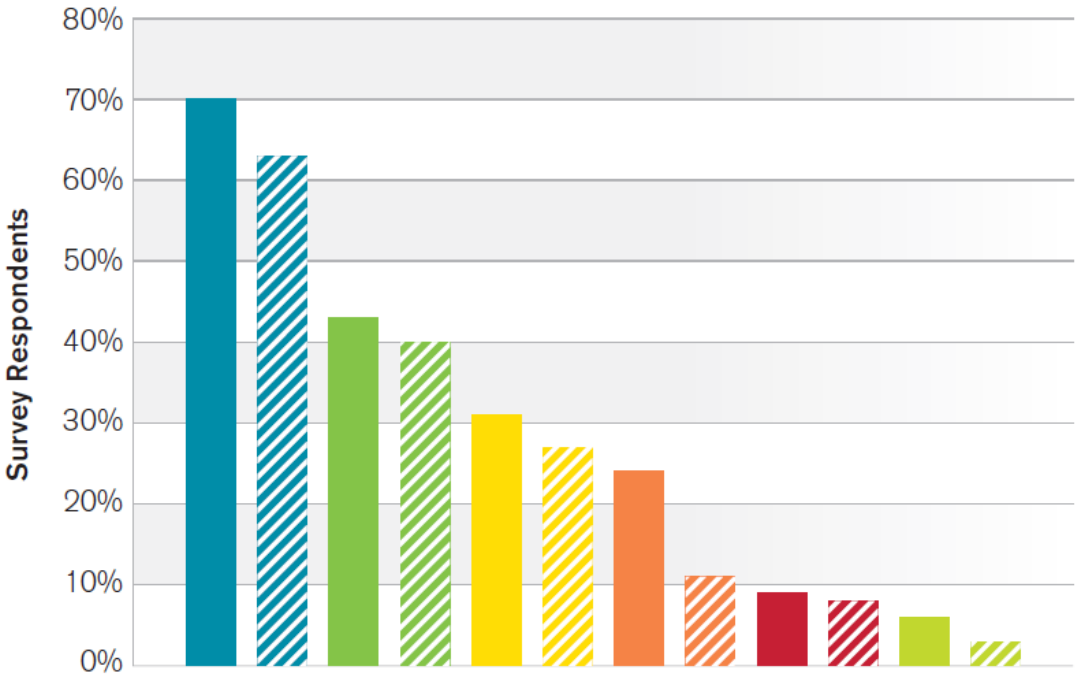
- **81%** NetFlow-based analyzers (e.g. Peakflow SP)
- **70%** Firewall logs
- **59%** IDS/IPS
- **53%** SNMP-based tools
- **53%** Performance management/monitoring solutions
- **50%** Customer call/help desk ticket
- **40%** Security Information and Event Management (SIEM) platforms
- **40%** In-house developed scripts/tools
- **35%** Inline DDoS detection/mitigation system (e.g. Pravail APS)
- **1%** Other

Effectiveness of Threat Detection Tools



- **2.75** Customer call/help desk ticket
- **3.59** SIEM
- **4.02** Performance management/monitoring solutions
- **4.38** Firewall logs
- **4.80** In-house developed scripts/tools
- **5.43** IDS/IPS
- **5.59** SNMP-based tools
- **6.78** Inline DDoS detection/mitigation system
- **7.65** NetFlow-based analyzers

Attack Mitigation Techniques



- **70%** Intelligent DDoS mitigation systems (IDMS) such as Arbor Peakflow or Pravail APS
- **63%** Access Control Lists (ACLs)
- **43%** Destination-based remote triggered blackhole (D/RTBH)
- **40%** Firewall (including WAF, Next Gen)
- **31%** IPS
- **27%** Source-based remote triggerd blackhold (S/RTBH)
- **24%** Load balancer
- **11%** FlowSpec
- **9%** Managed security service provider
- **8%** Content Delivery Network (CDN)
- **6%** DPI systems
- **3%** None

Time to Mitigate

- **16%** Automatically through scripts/tools
- **23%** Less than 10 minutes
- **29%** More than 10 minutes but less than 20 minutes
- **14%** More than 20 minutes but less than 30 minutes
- **11%** More than 30 minutes
- **7%** We do not mitigate attacks

Ключевые выводы

- ✓ Частота наблюдения атак выросла по сравнению с прошлым годом
- ✓ **Атаки против клиентов (Customers)** являются основной угрозой для операторов связи
- ✓ **Reflection/Amplification технологии** продолжают использоваться для запуска больших атак. Размер атак достиг 400 Гбит/с, в 2014 г. наблюдалось около 10 атак > 100 Гбит/с
- ✓ Около 65% атак - **Volumetric**, но почти все респонденты наблюдали **Application атаки**
- ✓ **Application** атаки составляют 29% по наблюдениям Customers, и всего 17% по общей статистике; это означает что операторы связи не выявляют многие Application атаки
- ✓ 42% респондентов наблюдали **атаки на сервисы, использующие шифрование**
- ✓ Свыше трети ЦОД сталкивались с DDoS-атаками, переполняющими каналы связи
- ✓ Firewall, Application Firewall и IPS остаются наиболее популярными средствами защиты ЦОД, однако наблюдается рост использования IDMS (Intelligent DDoS Mitigation System)

(C) Worldwide Infrastructure Security Report. Arbor Networks, 2015

Ключевые выводы

- ✓ Наиболее эффективными и распространенными средствами обнаружения остаются Netflow анализаторы, Firewall logs вторые по популярности, но шестые по эффективности
- ✓ Впервые системы IDMS (Intelligent DDoS Mitigation System) заняли первое место по распространенности среди средств фильтрации DDoS, обойдя межсетевые экраны
- ✓ Количество организаций, использующих технологии антиспуфинга на границе сети, уменьшилось с 50% до 33% - это облегчает запуск DDoS-атак
- ✓ Относительно небольшое число организаций уделяют внимание защищенности DNS, и их доля не меняется
- ✓ Растет количество респондентов, способных оперативно (за 20 минут) подавить DDoS-атаки: в 2013 году это 60%, в 2014 – 68%

(C) Worldwide Infrastructure Security Report. Arbor Networks, 2015

УЦСБ
Интегратор Сильных Решений

Уральский центр систем безопасности
Технологии защиты бизнеса
Аудит. Проектирование. Внедрение. Сопровождение.

ARBOR NETWORKS

Специализированные решения

ARBOR NETWORKS

radware

ИНФИСОФТ

Check Point SOFTWARE TECHNOLOGIES LTD.

Специализированные сервисы

KASPERSKY lab

QRATOR

BIFIT
Банковские и финансовые Интернет Технологии

ARBOR NETWORKS

GROUP IB

Операторы связи

Rostelecom
More possibilities

orange Business Services

МегаФон

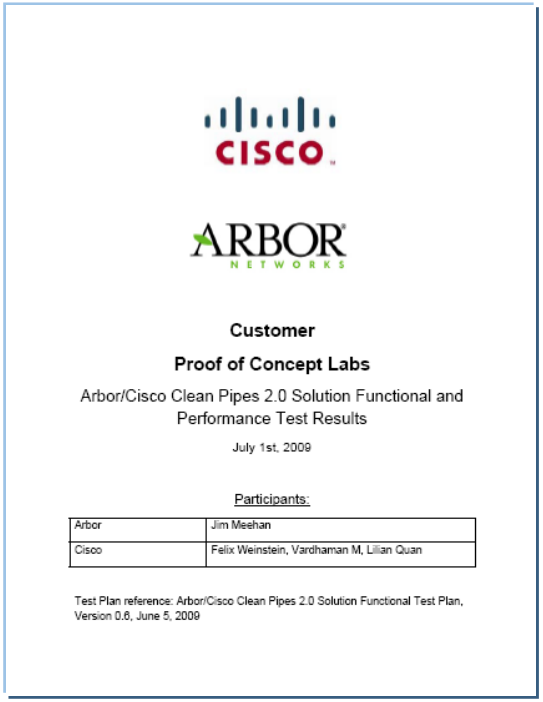
Билайн

акадо телеком

TTK

Cisco Clean Pipes

- В 2010 Cisco анонсировала закрытие линеек Cisco Guard и Anomaly Detector.
- Cisco предложила своим заказчикам использовать решения Arbor Networks Peakflow SP
- Clean Pipes 2.0 – Cisco оттестировала и проверила решения Arbor.
- Компания Cisco также использует решения Arbor Networks для защиты своих сетей: http://www.cisco.com/web/about/ciscoitatwork/network_systems/network_data_monitoring_and_reporting_web.html


CISCO

ARBOR NETWORKS

Customer

Proof of Concept Labs

Arbor/Cisco Clean Pipes 2.0 Solution Functional and Performance Test Results

July 1st, 2009

Participants:

Arbor	Jim Meehan
Cisco	Felix Weinstein, Vardhaman M, Lilian Quan

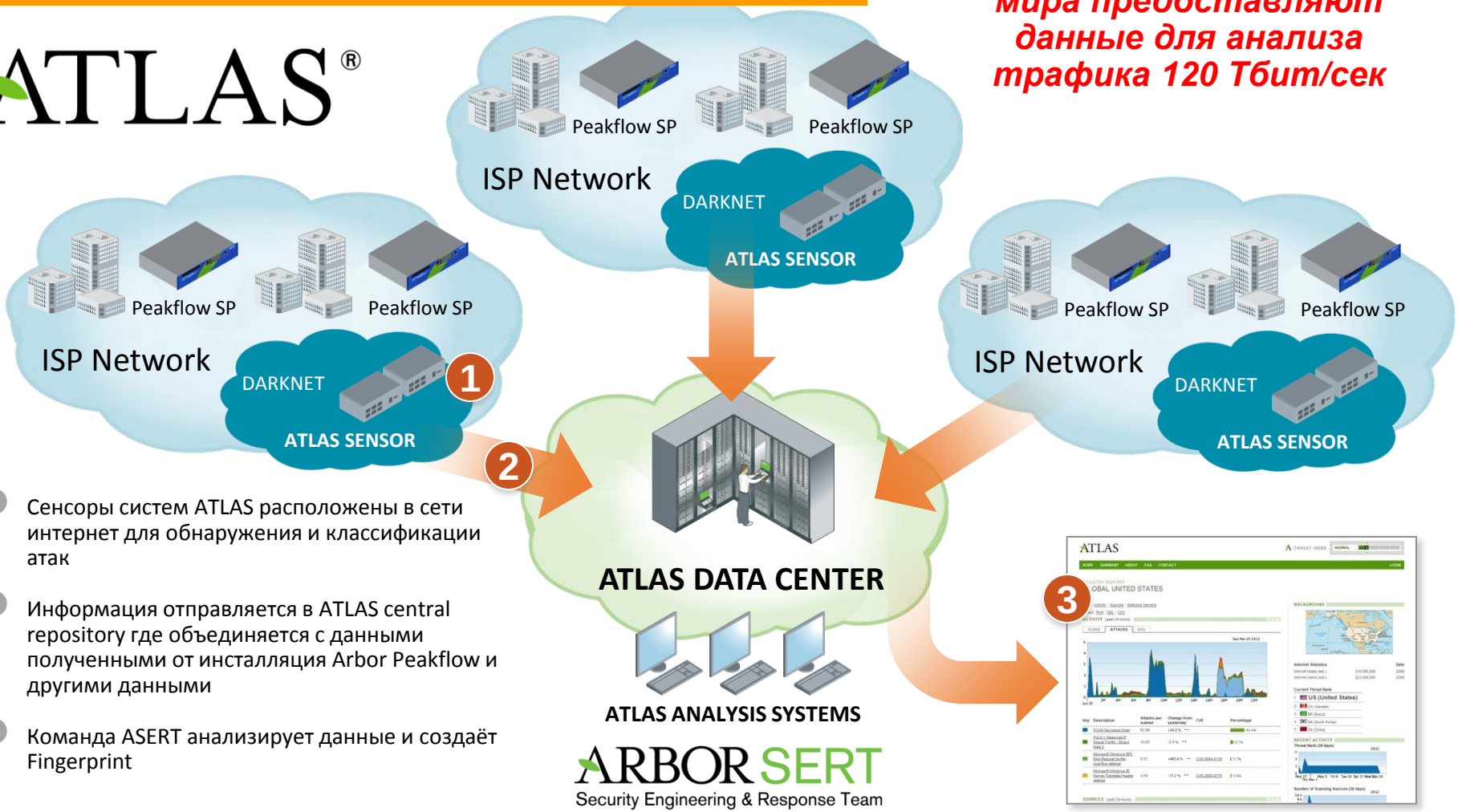
Test Plan reference: Arbor/Cisco Clean Pipes 2.0 Solution Functional Test Plan, Version 0.6, June 5, 2009

http://www.arbornetworks.com/cleanpipes

Active Threat Level Analysis System

ATLAS®

Более 300 операторов мира предоставляют данные для анализа трафика 120 Тбит/сек



1. Сенсоры систем ATLAS расположены в сети интернет для обнаружения и классификации атак
2. Информация отправляется в ATLAS central repository где объединяется с данными полученными от инсталляция Arbor Peakflow и другими данными
3. Команда ASERT анализирует данные и создаёт Fingerprint

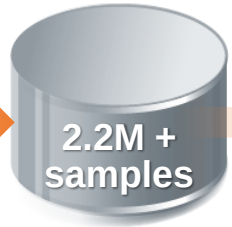
DDoS атаки в России

- 1-ый квартал 2014:
  - Количество атак – 10622
  - Самые мощные атаки – 124,9 Гбит/сек и 33,4 Мпакетов/сек
- 2-й квартал 2014
  - Количество атак – 9296
  - Самые мощные атаки – 83,025 Гбит/сек и 25,3 Мпакетов/сек
- 3-й квартал 2014
  - Количество атак – 8093
  - Самые мощные атаки – 121,3 Гбит/сек и 50,0 Мпакетов/сек
- 4-й квартал 2014
  - Количество атак – 14600
  - Самые мощные атаки – 64,045 Гбит/сек и 92,91 Мпакетов/сек

Active Threat Level Analysis System

“Песочница из виртуальных машин” запускает вредоносный код (ищет командный центр сети ботнет, отслеживает отклонения и закономерности сетевого поведения кода)

100,000+
Вредоносных программ в день



Отчёт и PCAP файлы сохраняются в базе

Постоянная аналитика 24 часа в сутки для создания базы данных сигнатур

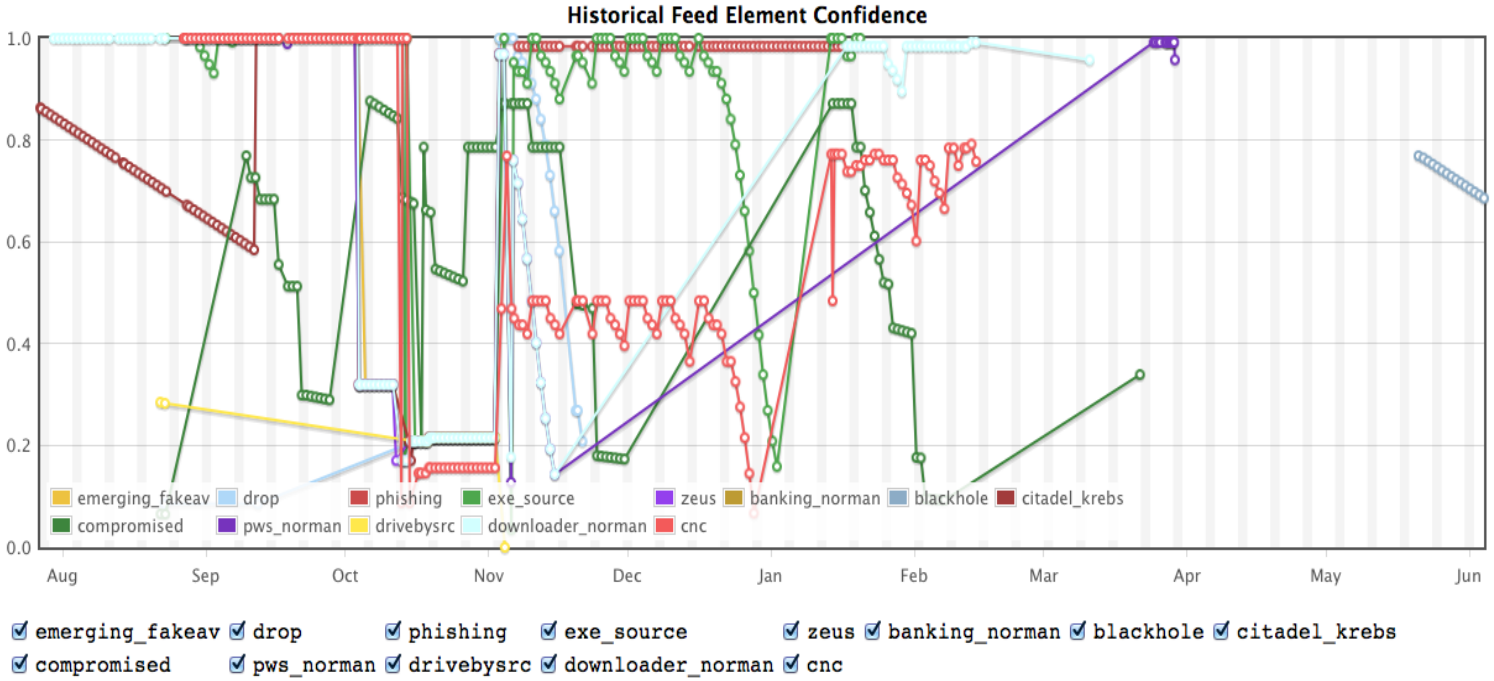
“Fingerprint”

Beta Bot – A Code Review

Introduction

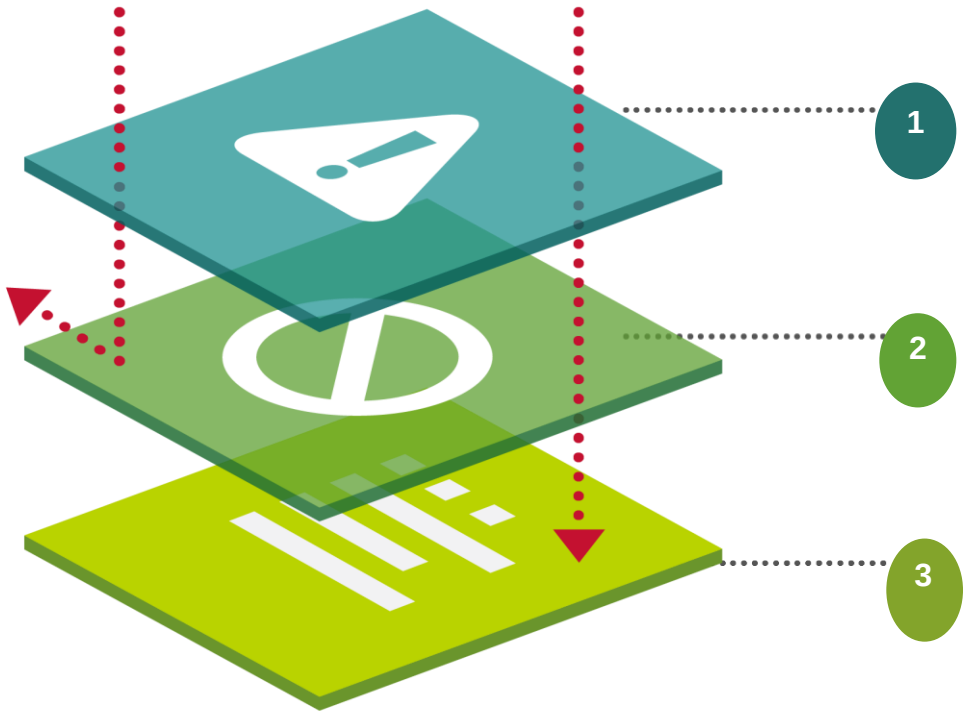
The basics on Beta Bot was covered by Limor Kessem on the RSA blog. As a quick feature summary:

Политики ATLAS Intelligence Feed (AIF)



- **Индекс доверия характеризует участников глобальной сети Интернет в привязке к IP адресам, доменным именам и используется для формирования политик безопасности**
- **Вероятность блокировки различных объектов в Интернет может изменяться со временем**
- **Уровень доверия зависит от зловредной активности хостов**

Комплексный подход к современным угрозам



Pravail APS, NSI, SA -> Идентификация:

Определить аномальный трафик или подозрительную активность.

Pravail APS -> Действие:

Заблокировать атаку на границе сети или в «облаке».

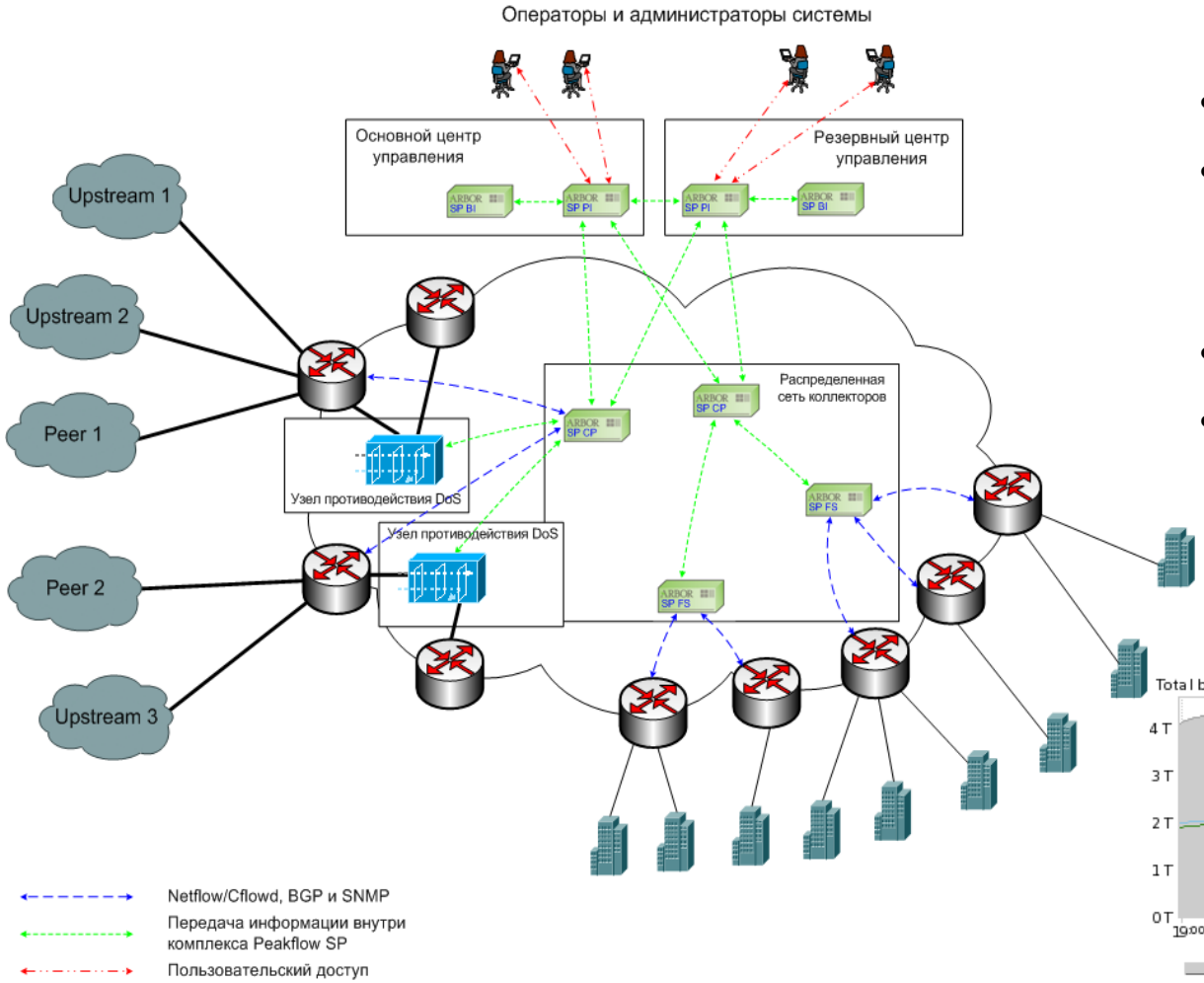
Pravail APS, NSI, SA -> Понимание:

Проведение оперативных расследований и **понимание** в деталях атаки и причинённого ущерба.

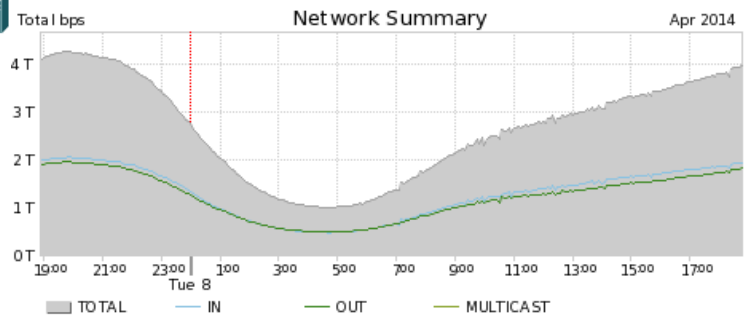
Arbor: ключевые особенности

- ✓ Установлен у 100% Tier-1 и у 60% Tier-2 операторов связи в мире
- ✓ Самая большая база знаний о DDoS-атаках - ATLAS
- ✓ Два решения: Peakflow и Pravail (для ISP и Enterprise), + Cloud Signalling
- ✓ Защита от DDoS атак на **различные протоколы и приложения,** в том числе от атак внутри SSL
- ✓ Аппаратное резервирование (блоки питания, интерфейсы ByPass, диски RAID)
- ✓ Поддержка RFC 5575 (**FlowSpec**)
- ✓ Для работы Peakflow и Pravail симметричность трафика не требуется
- ✓ Arbor Pravail работает на L2 - не требуется изменение топологии сети
- ✓ **Stateless режим** – Pravail неуязвим к State Exhausting атакам
- ✓ Блокировка по GEO IP, анализатор пакетов, анализатор эффективности противомер, русскоязычный интерфейс

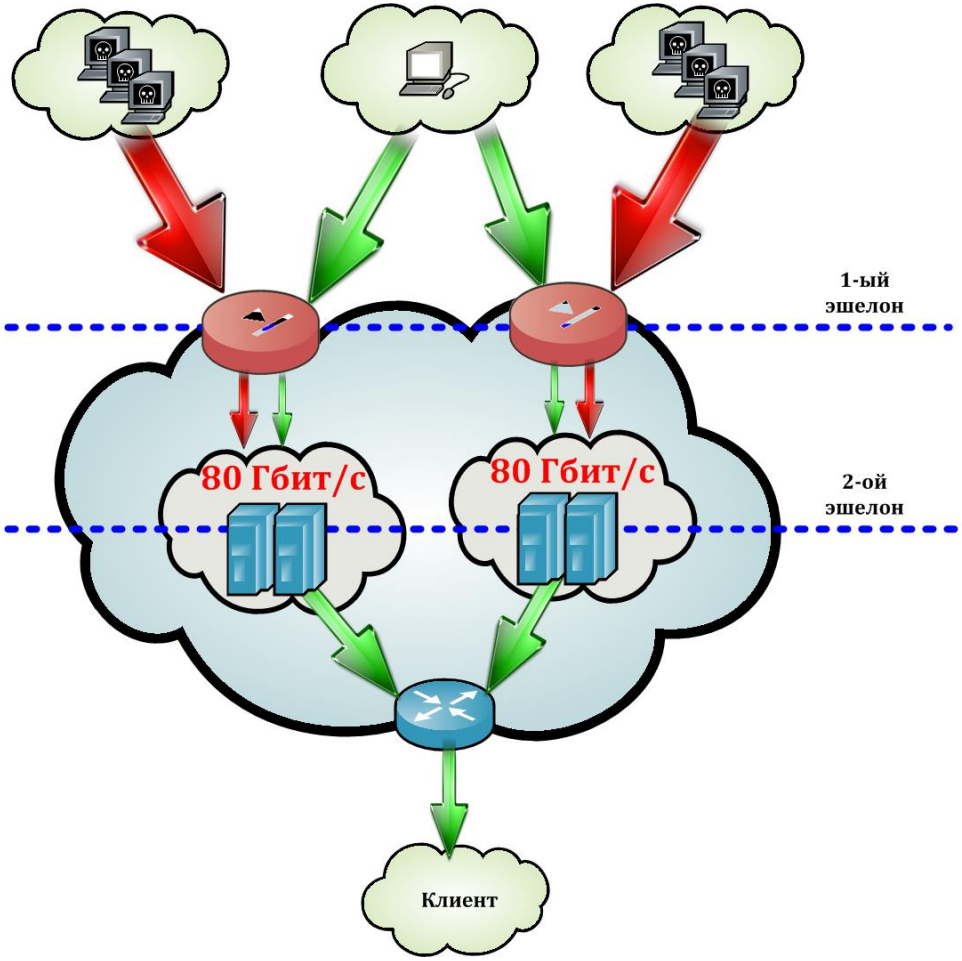
Ростелеком: подсистема анализа трафика



- Анализ >2 Тбит/с трафика
- Анализ трафика >300 магистральных маршрутизаторов
- Анализ IPv6
- Использование Arbor Peakflow

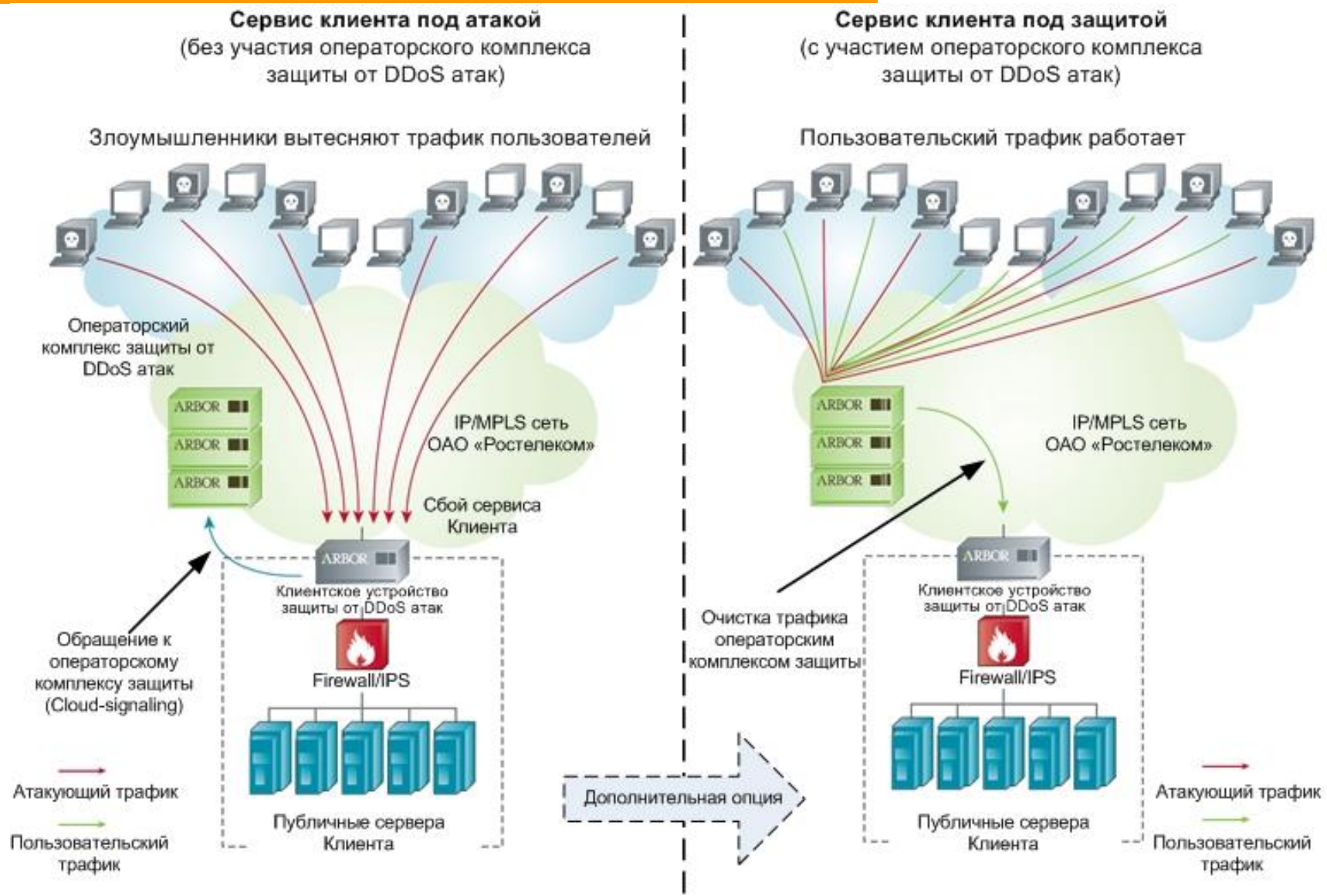


Ростелеком: подсистема очистки трафика



- 2 центра очистки трафика
- Производительность точной фильтрации на Arbor Peakflow TMS 160 Гбит/с
- Эшелонированная фильтрация: взаимодействие Arbor Peakflow по протоколу Flowspec с граничными маршрутизаторами

Ростелеком: Cloud Signalling



Ростелеком без Arbor Pravail

- ✓ **Не детектируются небольшие атаки и Application атаки** (мониторинг семплированного Netflow)
- ✓ **Заказчик не имеет интерфейс управления системой очистки**, только мониторинг (организационные ограничения)

Ростелеком + Arbor Pravail

- ✓ Заказчик **полностью управляет политикой и настройками защиты**
- ✓ **Фильтруются все виды атак:** Application, State-Exhausting, Volumetric
- ✓ **Защита от Volumetric атак любого размера** (ограничивается производительностью подключений Ростелекома)
- ✓ **Защита от атак автоматическая** – нет ручного согласования между заказчиком и провайдером

Спасибо за внимание!

Илья Яблонко, CISSP
менеджер по развитию решений
сетевой безопасности
ООО «УЦСБ»
+7 912 607 55 66
IYablonko@USSC.ru

Алексей Холмов
Системный инженер, RCIS
Arbor Networks EMEA
+7 916 671 78 38
akholmov@arbor.net