ARBOR NETWORKS

Решения Arbor Networks

Михаил Родионов

+7.916.934.61.99

mrodionov@arbor.net

Enterprise sales manager, CIS

Темы презентации

- **О компании Arbor Networks**
  - История компании
  - Уникальная система мониторинга мирового трафика – **система ATLAS**
  - Исследовательская деятельность компании – **команда ASERT**
  - Наши заказчики
- **Анатомия DDOS атаки**
  - Типы DDOS атак
  - Почему не помогают обычные средства защиты?
- **Решения Arbor Networks:**
  - Решение Peakflow SP для обеспечения доступности и визуализации сетей крупных компаний
  - Решение Pravail APS для обеспечения доступности крупных и средних компаний
  - Решение Arbor Cloud, облачный сервис для обеспечения доступности для заказчиков имеющих оборудование Arbor Networks
  - Решение Pravail NSI для детектирования сетевых аномалий и визуализации сети
  - Решения Pravail SA для анализа сетевой безопасности компании, обнаружению атак и расследованию инцидентов
- **Краткий обзор решений**

ARBOR NETWORKS

Arbor Networks – кто это?

Производитель, которому доверяют защиту своих сетей самые крупные и требовательные бизнесы мира

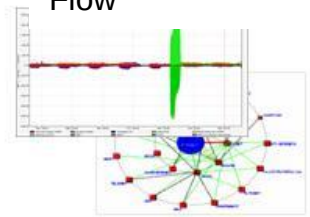
100%	Процент Tier 1 операторов, являющихся клиентами Arbor 
#1	Защищает крупнейший сети компании и наиболее значимые мировые события. Последнее событие мирового масштаба под защитой Arbor Networks – Олимпийский игры в Сочи 2014.
80 Тб/с	Трафик, отслеживаемый системой ATLAS в данный момент – ***Это почти 45% всего Интернет трафика.***
#1	Позиция Arbor на рынке оборудования защиты от DDoS в сегментах Carrier, Enterprise, Mobile – 65% всего рынка [Infonetics Research декабрь 2013]
12 лет	Arbor Networks поставляет инновационные продукты и технологии по обеспечению безопасности и мониторинга сетей
$16 Млрд	Выручка компании Danaher в 2011 году - головной компании, обеспечивающей финансовую стабильность Arbor

ARBOR NETWORKS

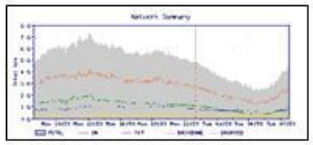
Краткая история компании Arbor Networks

2000 — **Arbor Networks** основан на базе университета Мичиган (США)

2002 — **Peakflow DOS and Trafic** Первая в индустрии система обнаружения DOS и аналитика Flow



2004 — **Peakflow SP** Визуализация, анализ пиринга, обнаружение DOS атак



2006 — **Peakflow SP TMS** Arbor представил TMS 2700 3Gbps

2008 — **ATLAS** – Первая в мире система анализа угроз

Первый ежегодичный отчёт **Worldwide Infrastructure Security Report**

Fingerprint Sharing Alliance (FSA) & Active Threat Feed (ATF)

2010 — **Peakflow SP TMS** Arbor представил первое распределённое решение 40Gbps TMS

2012 — **Pravail APS**

Infonetics назвал Arbor лидером рынка DDOS, более чем 65% всего рынка

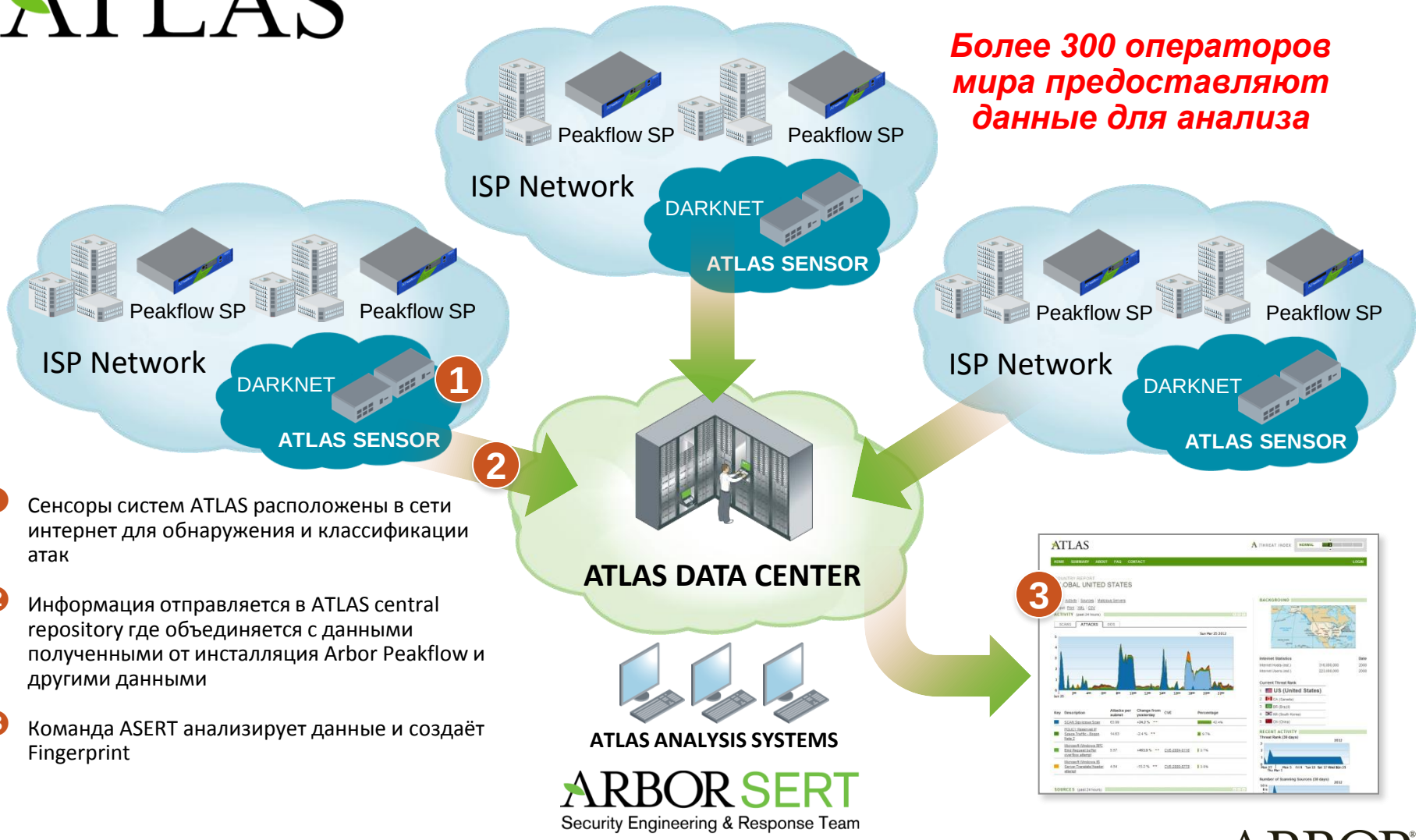
Peakflow SP TMS первая распределённая система 10G очистки трафика в индустрии

Active Threat Level Analysis System (ATLAS)

ATLAS®

Первая в мире система анализа угроз

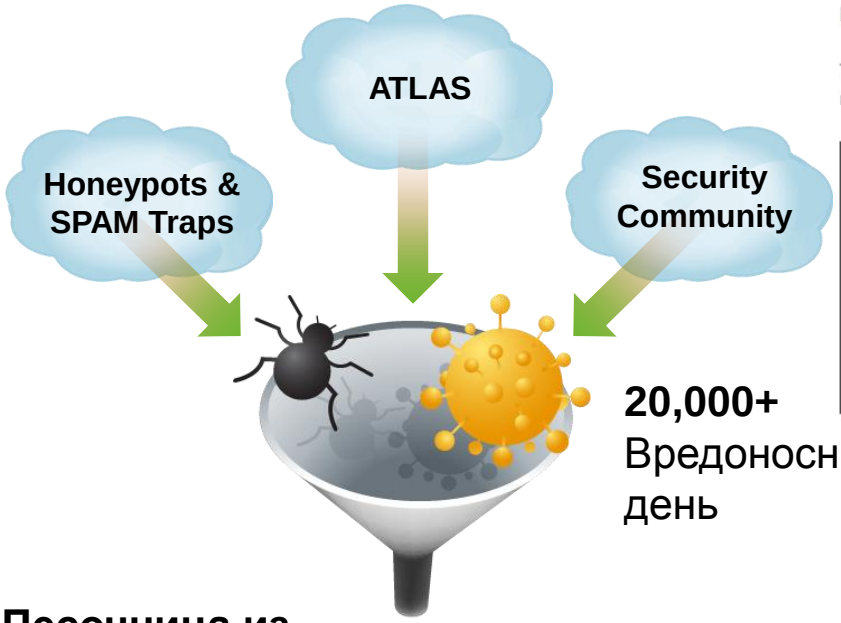
Более 300 операторов мира предоставляют данные для анализа

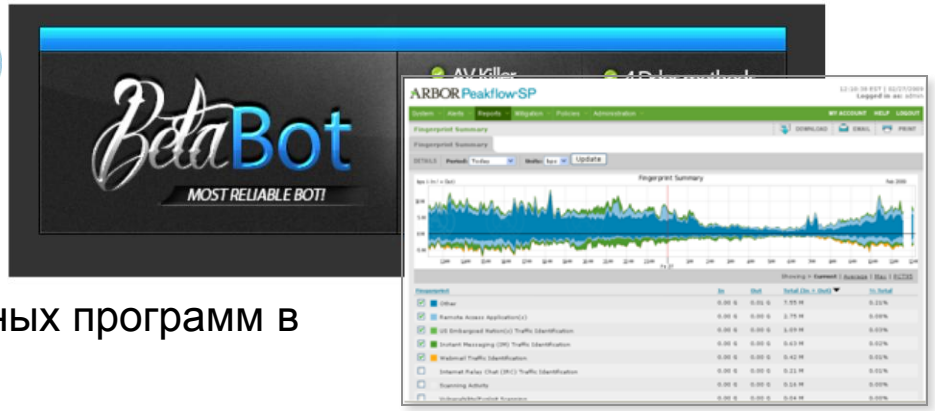


1. Сенсоры систем ATLAS расположены в сети интернет для обнаружения и классификации атак
2. Информация отправляется в ATLAS central repository где объединяется с данными полученными от инсталляция Arbor Peakflow и другими данными
3. Команда ASERT анализирует данные и создаёт Fingerprint

ARBOR NETWORKS

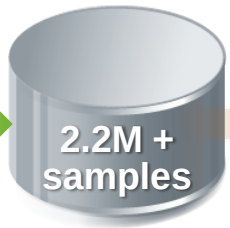
Команда ASERT – исследовательская деятельность компании





20,000+
Вредоносных программ в день

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



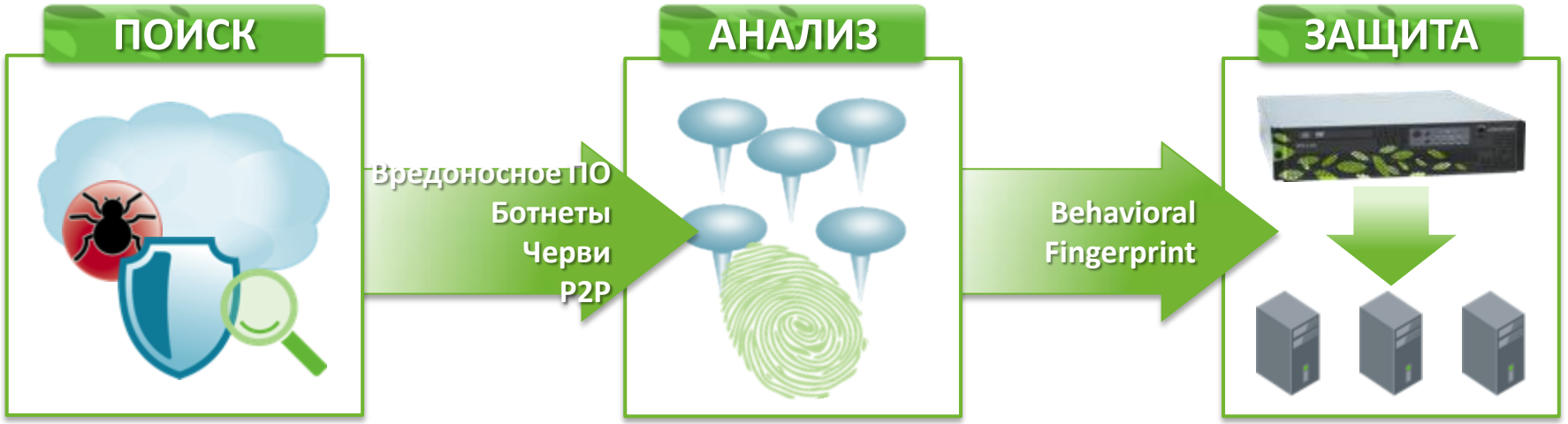
Отчёт и PCAP файлы сохраняются в базе

Постоянная аналитика 24 часа в сутки для создания базы данных сигнатур

“Fingerprint”

ARBOR NETWORKS

ATLAS + ASERT: Беспрецедентная экспертиза об атаках



Arbor Networks анализирует 75Tbps

Команда ASERT находит и анализирует угрозы

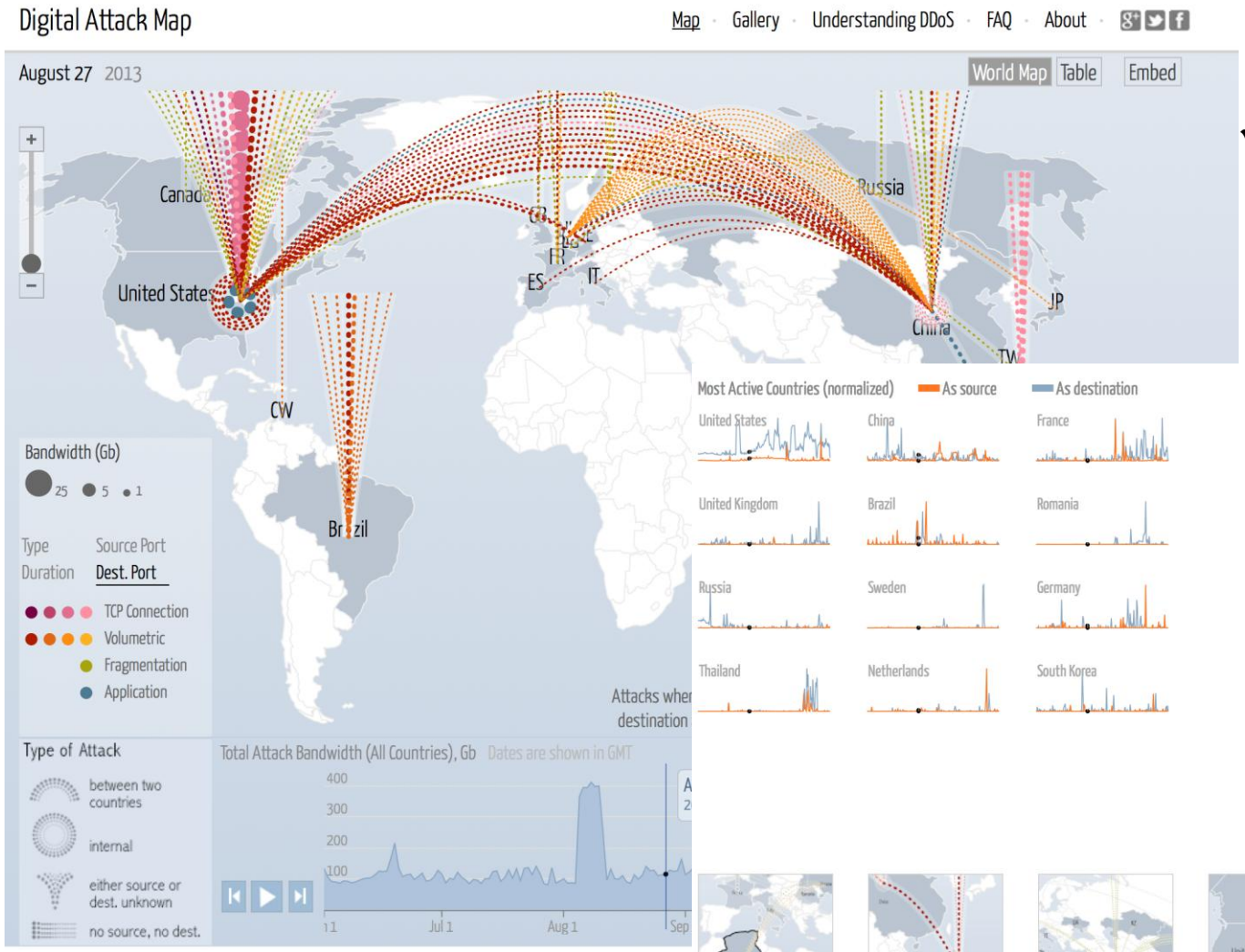
Продукты Arbor Pravail и Peakflow автоматически получают последнюю информацию о интернет угрозах используя **Atlas Intelligence Feed (AIF)**

75Tbps, около 1/3 глобального интернет трафика

ARBOR NETWORKS

ATLAS and Google

Digital attack map http://www.digitalattackmap.com/



News Results (Aug 27 - 29)

China hit by massive DDoS attack causing the Internet ...
thehackernews.com - Aug 27, 2013
China hit by massive DDoS attack causing the Internet inaccessibility for hours : The Hacker News.

Cloud Hosting Company DigitalOcean Hit by DDOS Attack
news.softpedia.com - Aug 28, 2013
TRENDING TODAY. · Download ... Cloud Hosting Company DigitalOcean Hit by DDOS Attack ... DDOS attack launched against DigitalOcean.

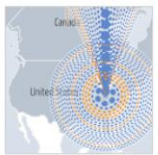
China hit by DDoS attack. The Internet inaccessible for hours
securityaffairs.co - Aug 27, 2013
China hit by DDoS attack. The CINIC confirmed that the country suffered a DDoS attack over the weekend causing the Internet inaccessibility ...

China hit by DDoS attack. The Internet inaccessible for hours ...
www.reddit.com - Aug 27, 2013
Hacktivism, Crypto-anarchy, Darknets, Free Culture. Tools and Data for Revolution. Against All Oppression - Proudly Feminist, Anarchist, Anti- ...

Nov. 6, 2013

Oct. 2, 2013

Sept. 11, 2013


Aug. 31, 2013

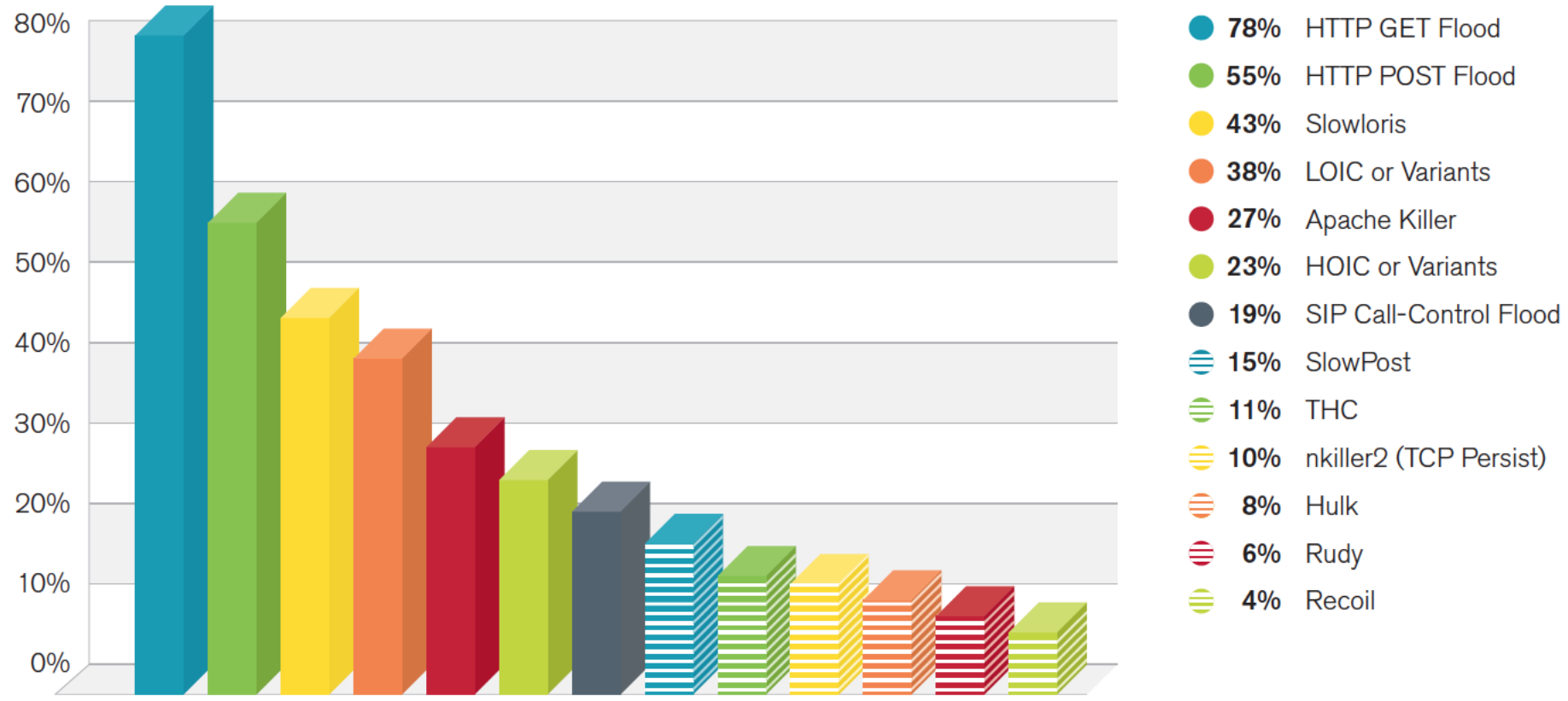

Aug. 27, 2013


Aug. 19, 2013

- ✓ ***Визуализация атак и привязка к новостной ленте***

ARBOR NETWORKS

Наиболее популярные атаки уровня приложений

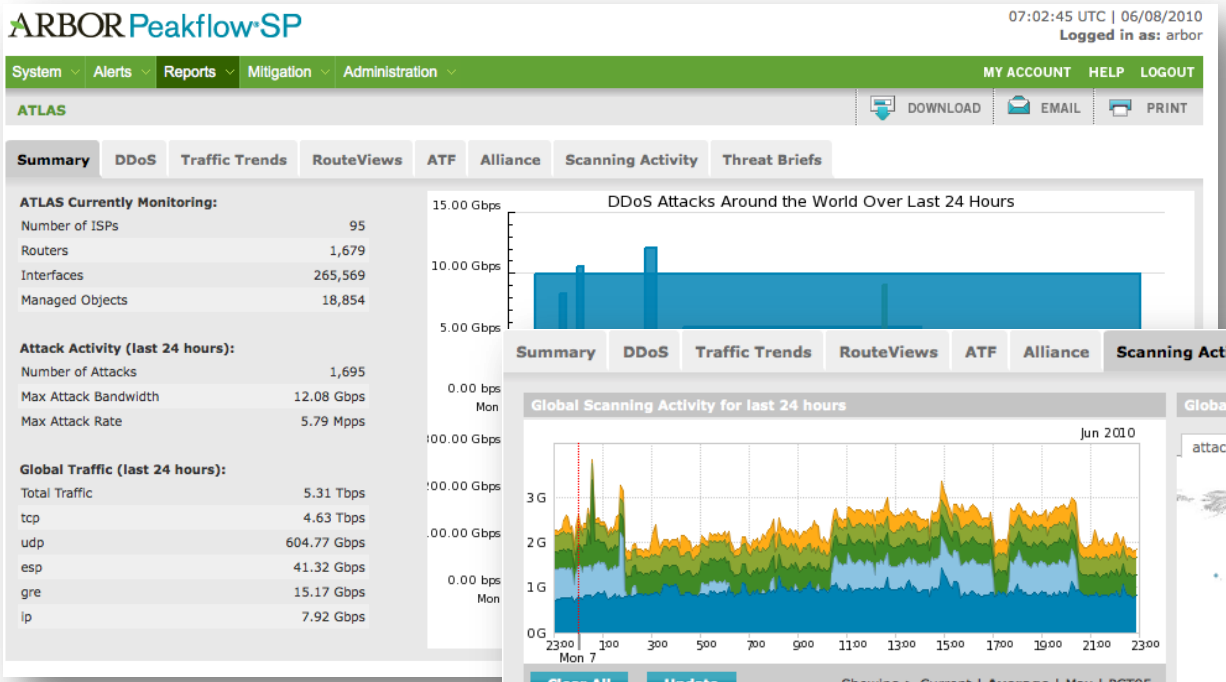


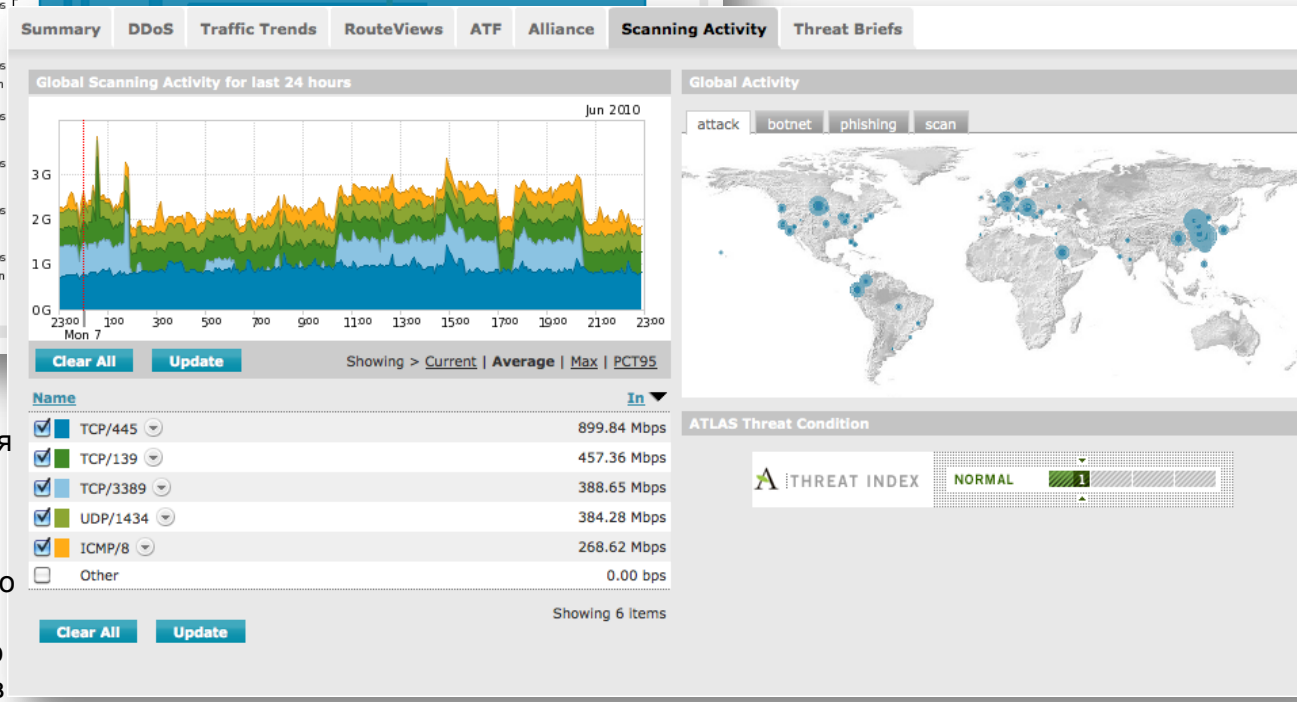
Данные использованы из отчёта Arbor Networks:

Worldwide Infrastructure Security Report IX

ARBOR NETWORKS

ATLAS – глобальный мониторинг





Global View from your Peakflow SP Console

«Благодаря глобальному анализу потенциальных угроз в реальном времени мы может принимать более точные решения по сетевому управлению и сетевой безопасности. Так как ATLAS собирает данные с большого количества операторов связи по всему миру, мы получаем не только информацию для оптимизации нашей маркетинговой стратегии, но и информацию для борьбы с ботнетами, атаками на отказ в обслуживание и другой активностью злоумышленников», -
Ken Haertling, Chief Security Officer в TELUS Business Transformation Technology Operations

ARBOR NETWORKS

ATLAS для всех решений Arbor Networks

- ✓ Получение уникальной экспертизы с помощью апдейтов от системы ATLAS – оборудование моментально начинает блокировать нелегитимный трафик сетей Botnet, Malware и т.п.
- ✓ Обнаружение и детектирование различных атак, обнаруженных экспертами Arbor Networks с помощью данных полученных от системы ATLAS и других источников
- ✓ Знание сетевого поведения вредоносного кода делает решения Arbor уникальными для детектирования сетевых аномалий и правильной борьбы с ними
- ✓ В отчётах системы Arbor будут указаны самые полные детали о произошедших событиях в сети
- ✓ Благодаря ATLAS, решения Arbor Networks обладают наивысшей компетенций для защиты вашей сети

WIRED

“Arbor Networks знает о работе Internet больше чем кто-либо еще (за исключением Агентства Национальной Безопасности). Если Вы хотите узнать, как выглядит актуальный профиль трафика и угроз в Интернете, взгляните на сервис ATLAS.»

ARBOR NETWORKS

Наша экспертиза и исследовательская деятельность = это ваша защита!

ATLAS® + ARBOR SERT Security Engineering & Response Team

Мониторинг около 45% всего глобального трафика
Более 300 крупнейших операторов мира предоставляют данные для анализа

Команда лучших профессионалов мира в области сетевой безопасности на страже вашей сети

=

Возможно лучшие сигнатуры для вашей защиты.
Автоматическое обновление сигнатур трафика для всех наших решений.

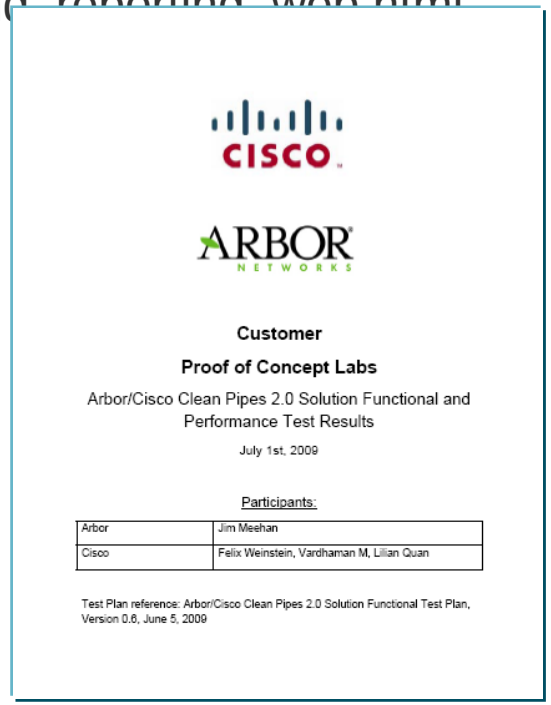
ARBOR Peakflow® ARBOR Pravail™

Безопасность это прежде всего **экспертиза,** откуда экспертиза у вашего поставщика решений?

ARBOR NETWORKS

Cisco выбирает решения Peakflow SP для решения 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

ARBOR NETWORKS

Наши заказчики*

- Крупнейшие заказчики мира из различных сфер – финансы, промышленность, государственные предприятия, университеты, операторы связи, социальные сети, сети профессиональных контактов, интернет магазины, мировые службы доставки и т.п.
- Интернет ресурсы, **которые вы используете каждый день**, защищены оборудованием Arbor Networks
- Arbor Networks **защищает** многие события мирового уровня, например Олимпийский игры в Сочи 2014:

http://www.arbornetworks.com/news-and-events/press-releases/recent-press-releases/5152-arbor-networks-successfully-protects-2014-sochi-olympics-web-properties

* - информация по заказчикам предоставляется по запросу

ARBOR NETWORKS

Некоторые публичные референсные заказчики

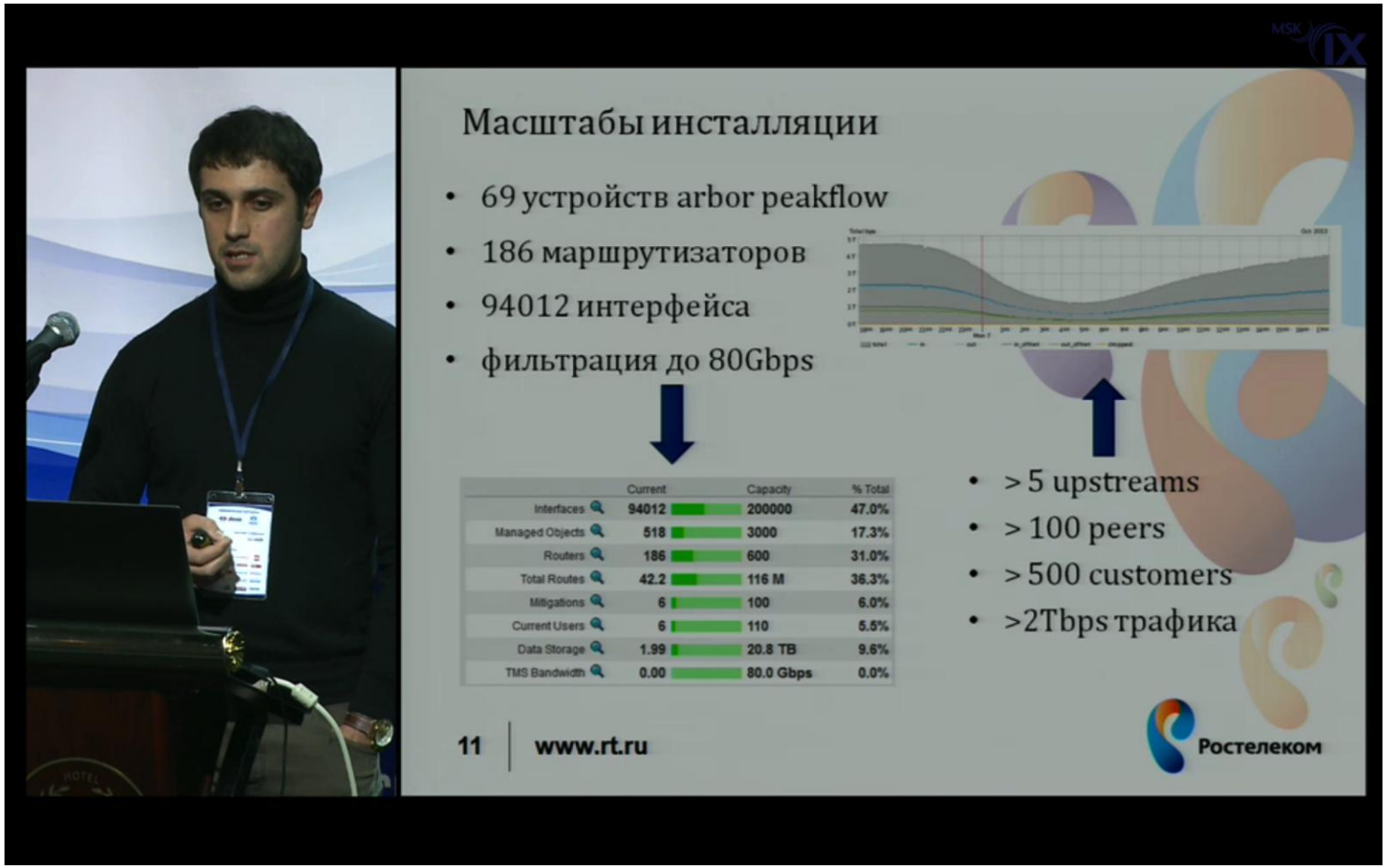
ARBOR NETWORKS

Последние события в России:

- Атаковали сайт Межпарламентской ассамблеи СНГ http://ria.ru/world/20140314/999548434.html
- Атаковали сайт ЦБ РФ: http://news.yandex.ru/yandsearch?cl4url=ria.ru%2Feconomy%2F20140314%2F999514759.html&lr=213&rpt=story
- Атаковали сайт первого канала: http://www.novayagazeta-ug.ru/news/u2802/2014/03/13/46335
- Атаковали сайт ВГТРК: http://www.novayagazeta-ug.ru/news/u2802/2014/03/13/46343
- Атаковали сайт Кремля: http://www.novayagazeta-ug.ru/news/u1542/2014/03/14/46543
- Атака на ВТБ24: http://www.gazeta.ru/tech/news/2014/03/17/n_6017749.shtml
- Атаковали сайт РИА: http://ria.ru/society/20140314/999538110.html
- Атаковали сайт Ленты: http://www.rbcdaily.ru/society/562949990831824
- Атаковали сайт газеты ведомости http://top.rbc.ru/society/30/01/2014/902338.shtml

События в России. Взгляд Ростелекома.

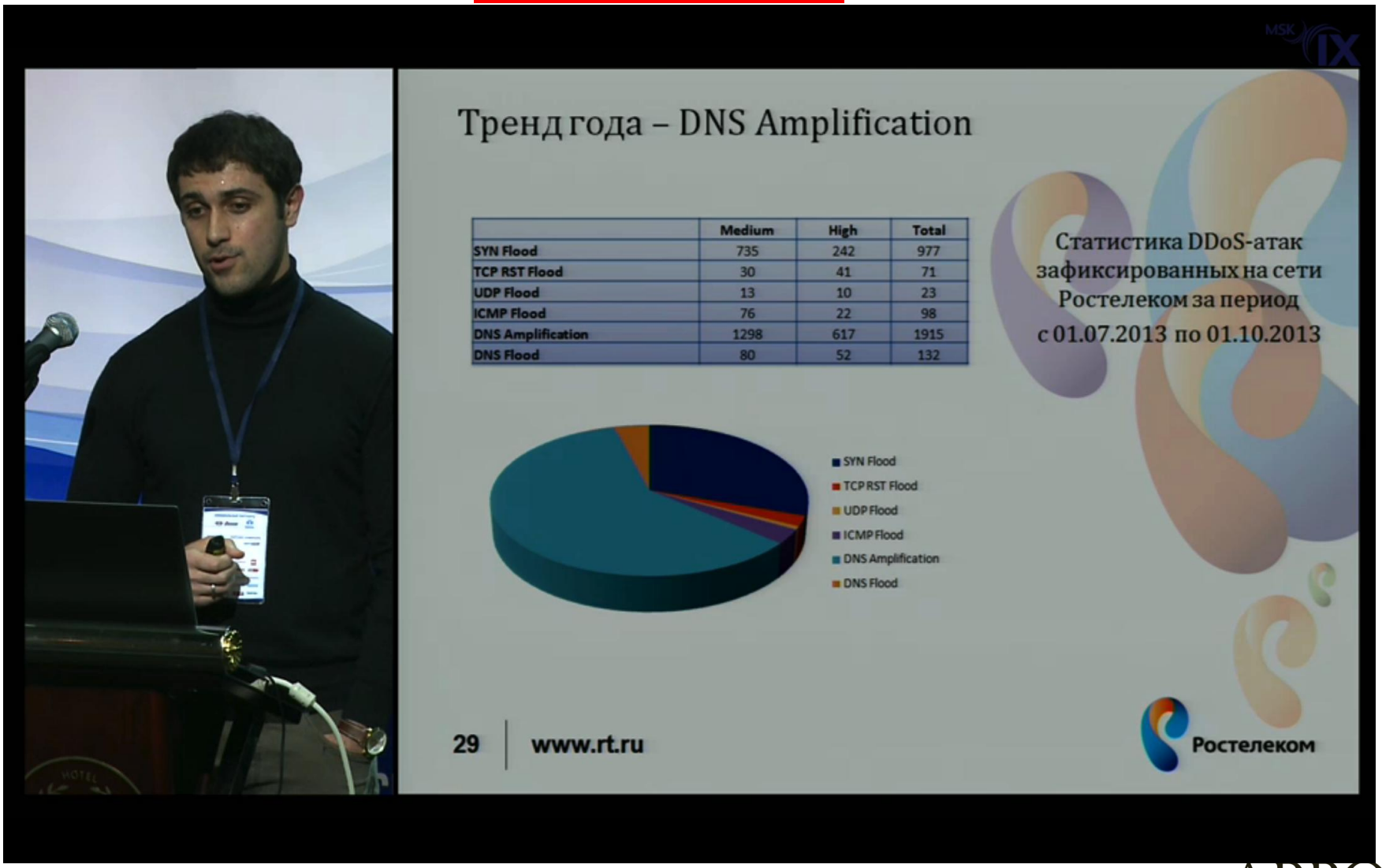
- Фильтрация расширена до 160G
- Применение flow-spec позволяет отбивать атаки больше фильтрационной ёмкости



ARBOR NETWORKS

Только Ростелеком зафиксировал более 3000 атак

За 3 месяца!



	Medium	High	Total
SYN Flood	735	242	977
TCP RST Flood	30	41	71
UDP Flood	13	10	23
ICMP Flood	76	22	98
DNS Amplification	1298	617	1915
DNS Flood	80	52	132

Решения компании Arbor Networks

Компания предлагает комплексный подход для решения следующих задач:

- Обеспечение бесперебойной работы/доступности сетевых сервисов (решения по защите от атак DDOS)
- Визуализация сетей компании
- Детектирование сетевых аномалий
- Решение для расследования и обнаружения атак

ARBOR NETWORKS

Где можно посмотреть наши решения?

- **О DDOS атаках**
  - The Evolution of DDoS Attacks http://www.youtube.com/watch?v=Q7deVOUXPFk
  - Различные материалы о DDOS http://www.arbornetworks.com/resources/media-library
  - Записанные вебинары, в том числе о решениях: http://www.arbornetworks.com/resources/media-library/enterprise-webinars
- **Система Atlas**
  - DDoS Attack Protection: Arbor Network's ATLAS http://www.youtube.com/watch?v=0U68W6gTkP8
  - Atlas Dashboard http://atlas.arbor.net
- **О нашей команде Asert**
  - Arbor Networks: Researching DDoS and Advanced Threats http://www.youtube.com/watch?v=T3oBpvcBxD4
  - Worldwide Infrastructure Security report http://www.youtube.com/watch?v=-83m82sEpNI
  - DDoS and the Evolving Advanced Threat Landscape http://www.youtube.com/watch?v=92p_MbPbewk
  - Asert blog http://www.arbornetworks.com/asert/
- **Решения Arbor Networks (Peakflow, Pravail APS, Pravail NSI, Pravail SA, Arbor Cloud)**
  - Comprehensive DDoS Protection Solutions http://www.youtube.com/watch?v=JP299b-IG6g
  - Video about Pravail family solutions:http://www.youtube.com/watch?v=Qznv913qVzw&list=PLu8eXm-IEjEC-kbMOSsQKPJGoc1V75fnw
  - Pravail NSI Product Tour http://www.youtube.com/watch?v=2Fn_b4g1Tqw
  - Cloud-Based DDoS Protection from Arbor Networks http://www.youtube.com/watch?v=kPJ-wjyhyoM
  - Pravail SA (Packetloop) http://vimeo.com/user6890858/videos

ARBOR NETWORKS

ARBOR®
NETWORKS

Защита от DDOS

Анатомия DDoS-атак. Что такое DDOS?

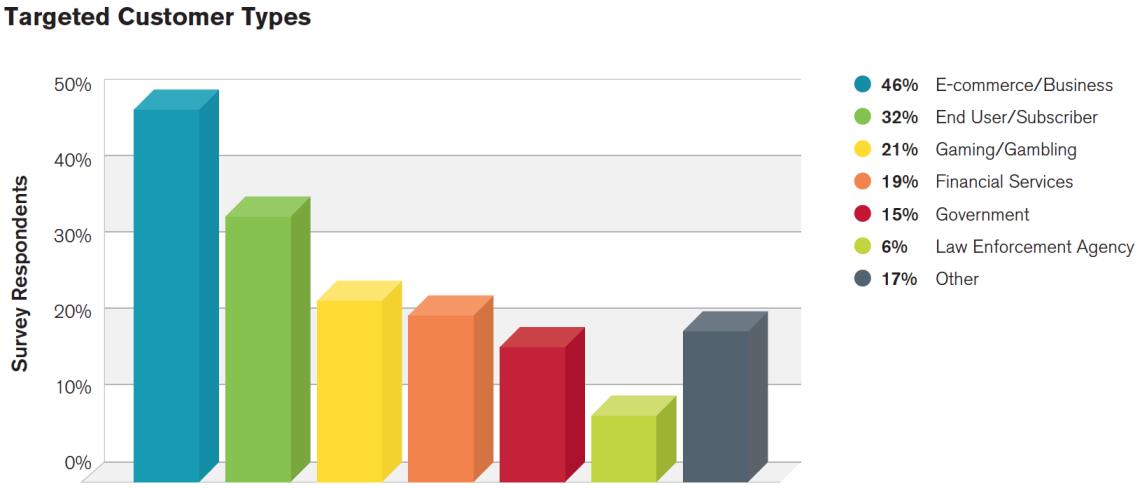
- **Тип атак на приложения или сетевую инфраструктуру компании с целью затруднения доступа к ресурсам/приложения или полного предотвращения доступа к ним**

- **Типичными жертвами данных атак являются:**
  - Финансовая индустрия
  - СМИ
  - Государственные учреждения
  - Интернет-магазины
  - Страховые компании

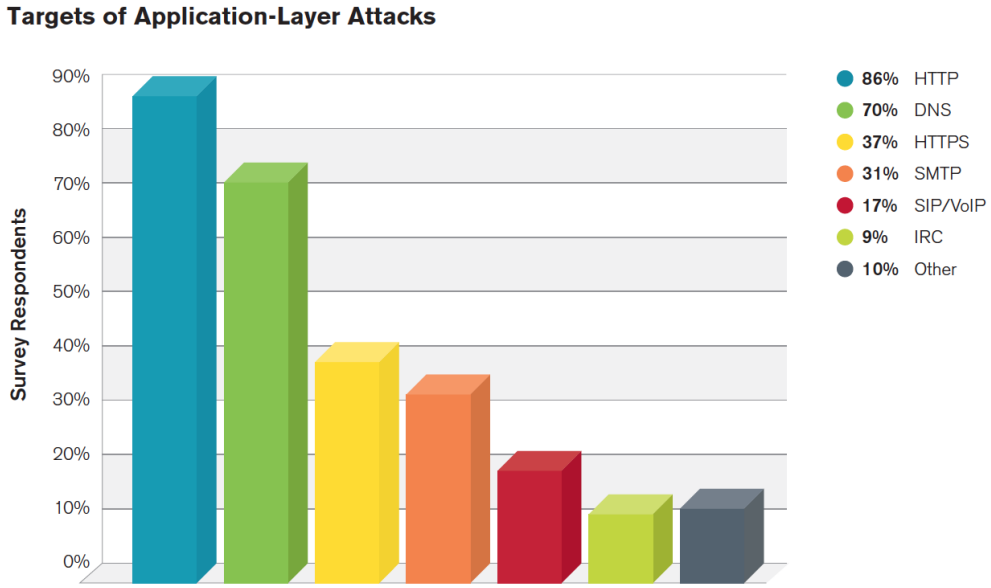
ARBOR NETWORKS

Анатомия DDoS-атак. Что такое DDOS?

Кого атакуют?



Какие сервисы наиболее часто атакуют?



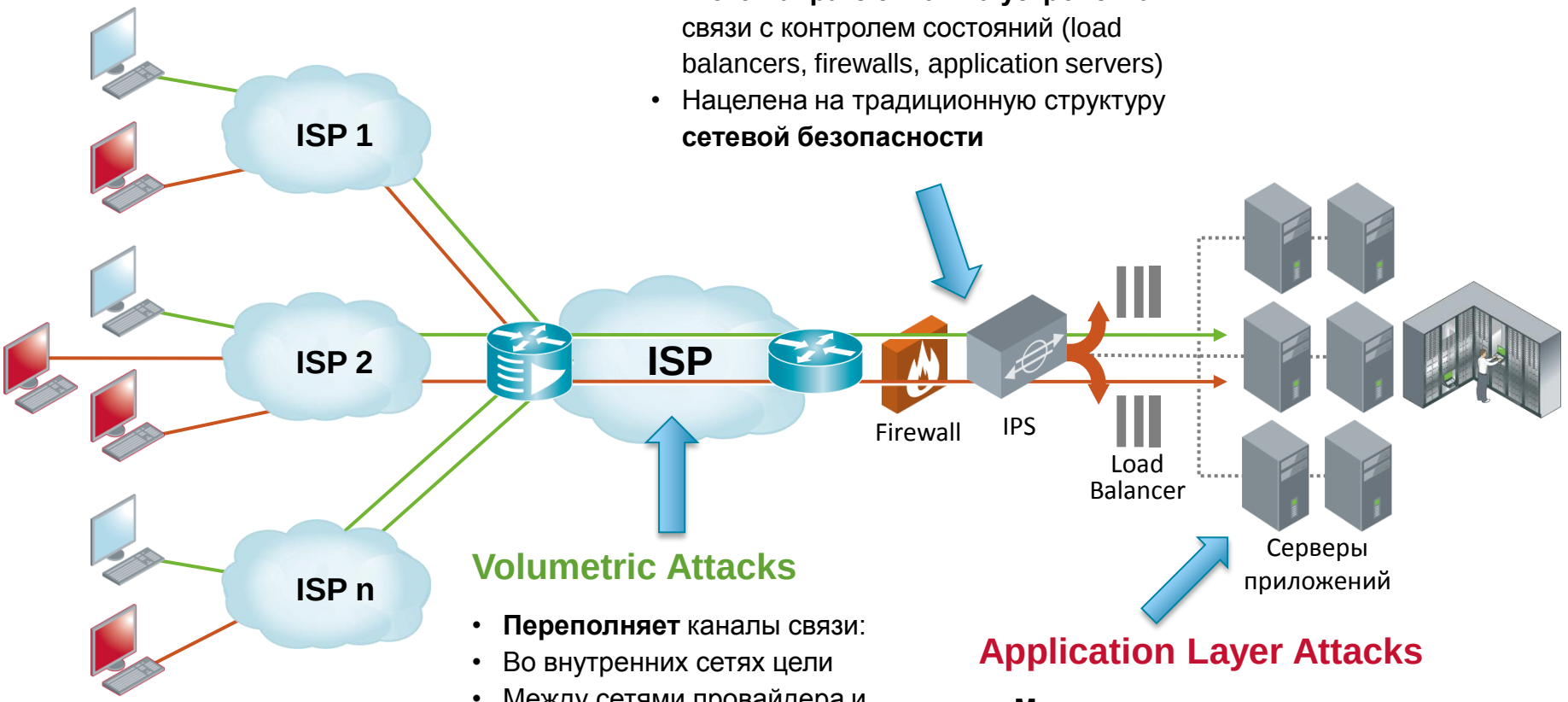
ARBOR NETWORKS

Анатомия DDoS-атак. Что такое DDOS?

Как и какие части сетевой инфраструктуры атакуют?

TCP State-Exhausting Attacks

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



Volumetric Attacks

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

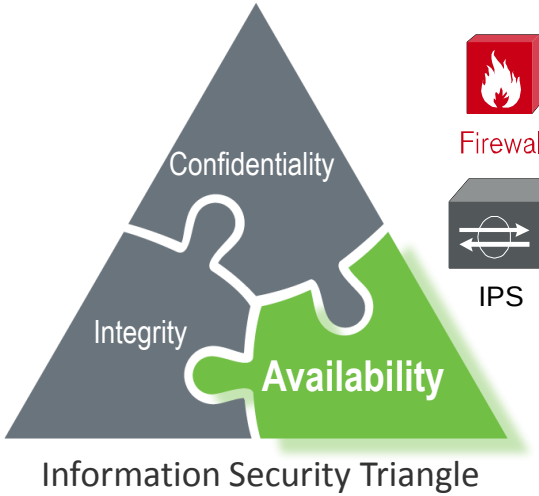
Application Layer Attacks

- **Малозаметные** атаки на приложения
- Нацелены на определённые уязвимости приложений

ARBOR NETWORKS

Почему обычные средства защиты не защищают от DDoS?

Существующие системы защиты периметра не нацелены на обеспечение ***доступности*** данных

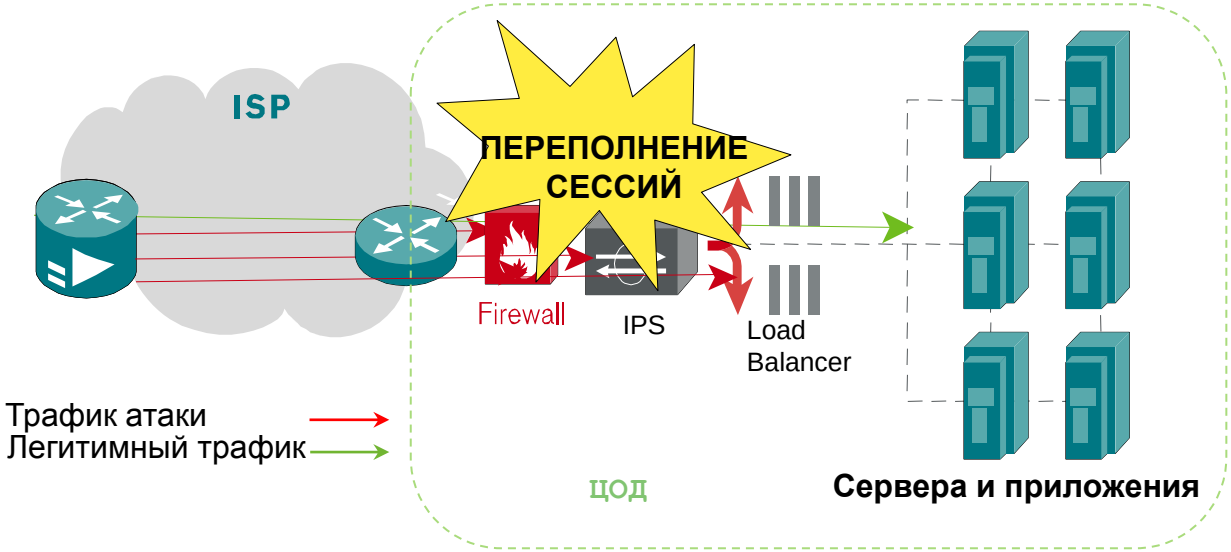


Information Security Triangle

Межсетевые экраны (МСЭ/FW) обеспечивают **целостность** данных или процедур, которое могут быть доступны только авторизованным сторонам

Intrusion Prevention Systems (IPS) обеспечивают **целостность** данных, обеспечивая возможность изменять информацию авторизованными методами

Все МСЭ и IPS являются устройствами с контролем сессий (stateful), поэтому сами по себе могут быть целью атак



ARBOR NETWORKS

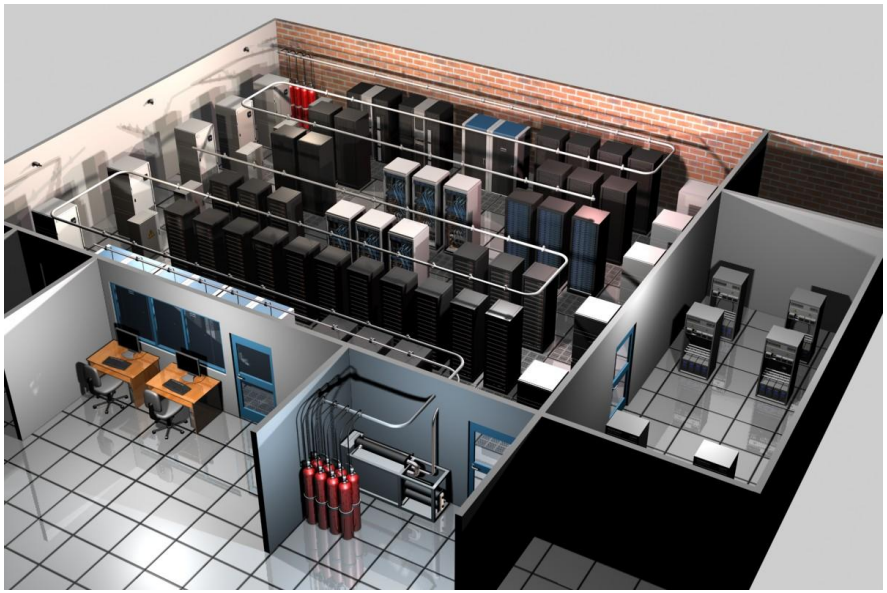
Современная инфраструктура

Многие компании создают узлы связи:

- Бесперебойное электропитание
- Автоматическая система пожаротушения
- Высоклассные и отказоустойчивые системы охлаждения
- Современная высокопроизводительная сетевая инфраструктура
- Превосходное серверное оборудование
- Получение сертификаций на обеспечение доступности, например Uptime Institute Tier III/Tier II/Tier I

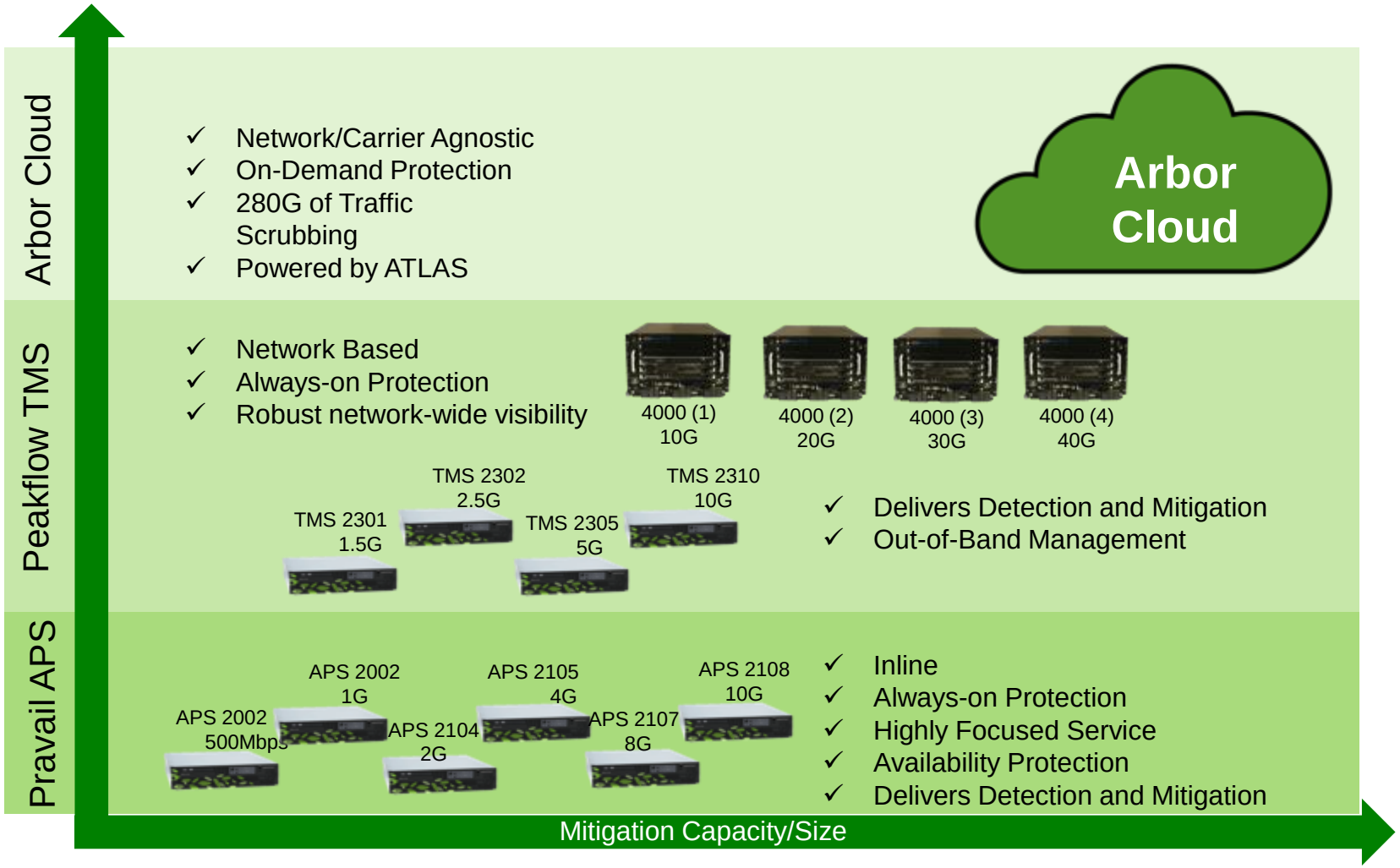
Но поможет ли это при:

- **Малозаметных** атаках на приложения (Application attack)?
- Атаках на **инфраструктуру сетевой безопасности**?
- При атака типа **переполнения канала** связи?
- Сможете ли вы понять **кто вас атаковал** и когда были атаки на протяжении времени?
- Можете ли вы точно сказать - **взламывали** ли вас или нет?

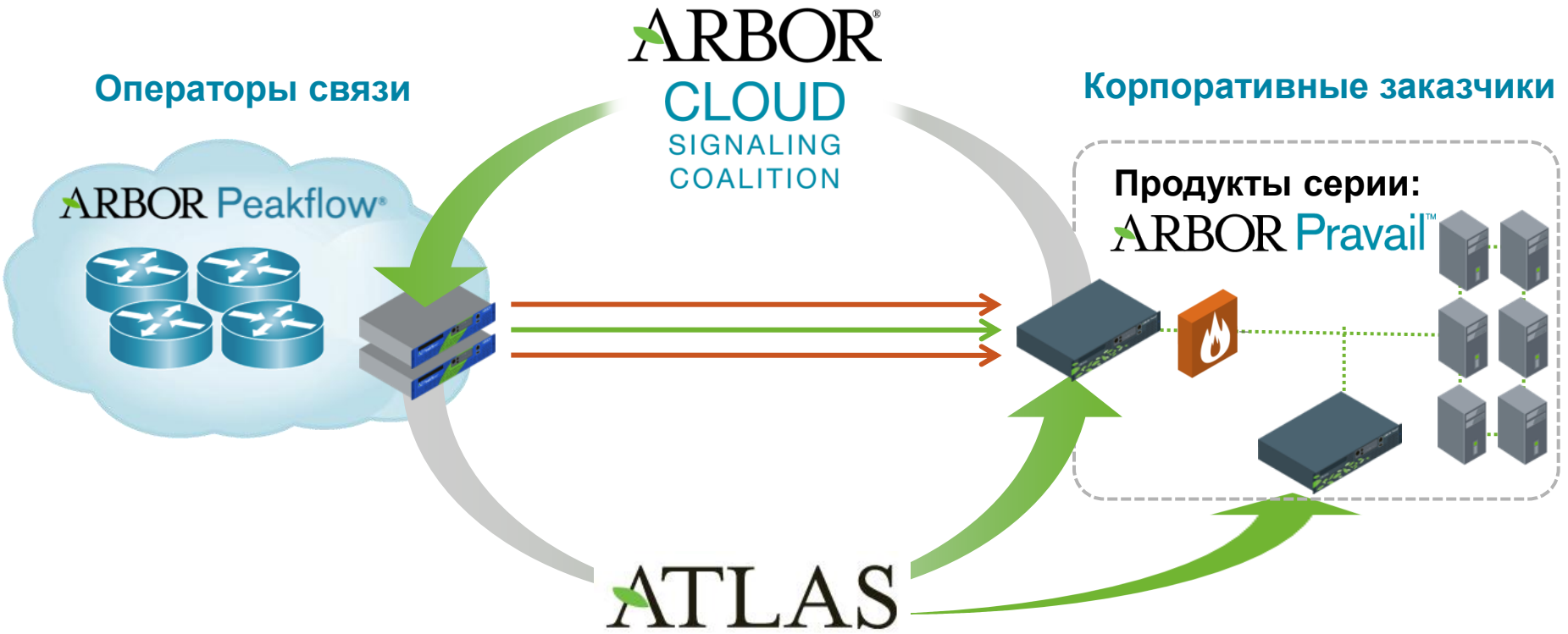


ARBOR NETWORKS

Комплекс решений Arbor Networks по борьбе с DDOS



Комплекс решений Arbor Networks по борьбе с DDOS



Решения:

- ✓ Arbor Peakflow SP
- ✓ Arbor Pravail APS
- ✓ Arbor Pravail NSI
- ✓ Arbor Pravail SA
- ✓ Arbor Cloud

Большие корпорации также используют решения

ARBOR NETWORKS

Pravail APS

Обеспечение доступности сервисов – защита от атак

ARBOR NETWORKS

Решение для защиты - Pravail APS

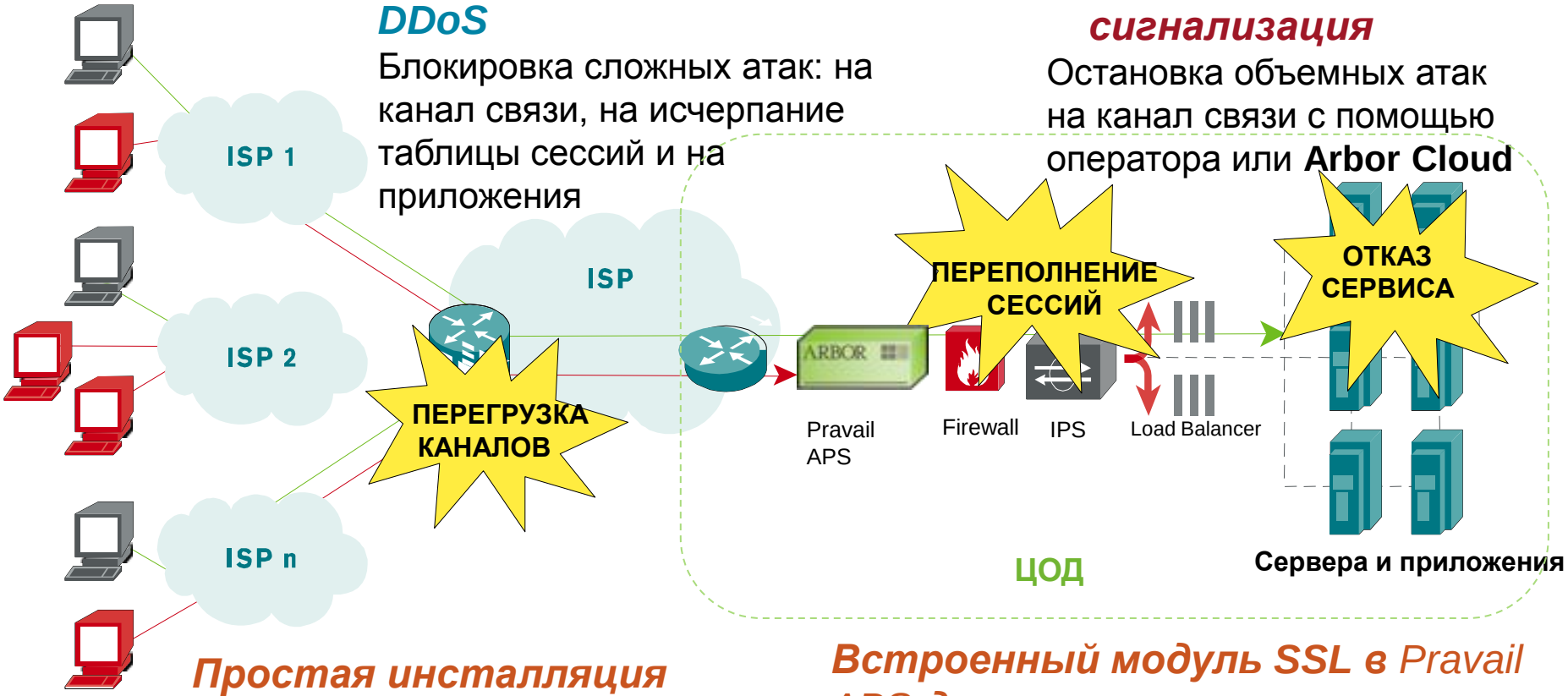
Проверенная защита от DDoS атак на площадке клиента

Блокировка сложных DDoS

Блокировка сложных атак: на канал связи, на исчерпание таблицы сессий и на приложения

Облачная сигнализация

Остановка объемных атак на канал связи с помощью оператора или **Arbor Cloud**



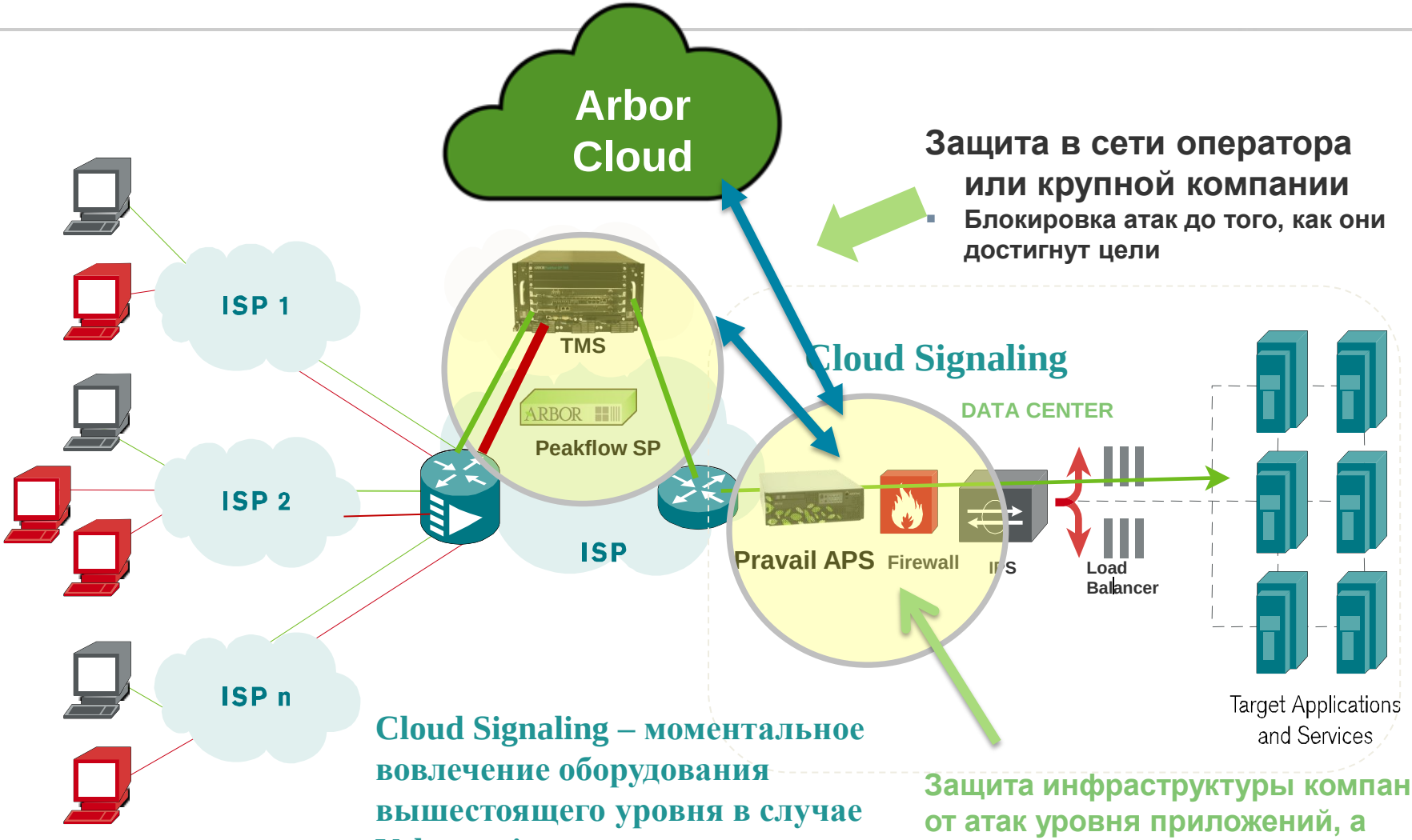
Простая инсталляция

Автообновление сигнатур останавливает актуальные угрозы

Встроенный модуль SSL в Pravail APS для остановки атак на сервисы с использованием шифрования

ARBOR NETWORKS

Эшелонированная защита от Arbor Networks



Защита в сети оператора или крупной компании

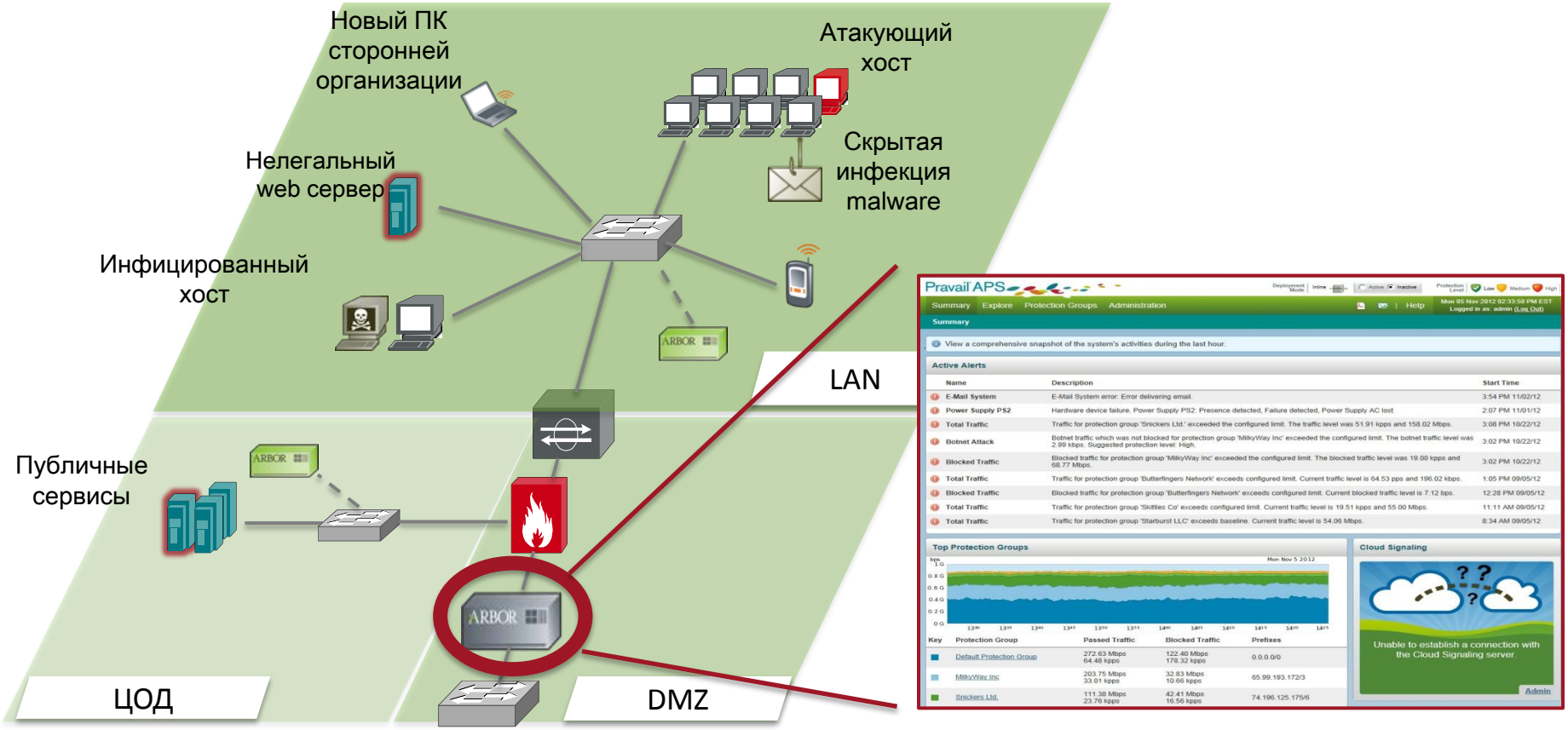
- **Блокировка атак до того, как они достигнут цели**

Cloud Signaling – моментальное вовлечение оборудования вышестоящего уровня в случае Volumetric атаки

Защита инфраструктуры компании от атак уровня приложений, а также от Volumetric до установленного порога, в том числе и для митигации атак с использованием SSL

ARBOR NETWORKS

Как работает APS?



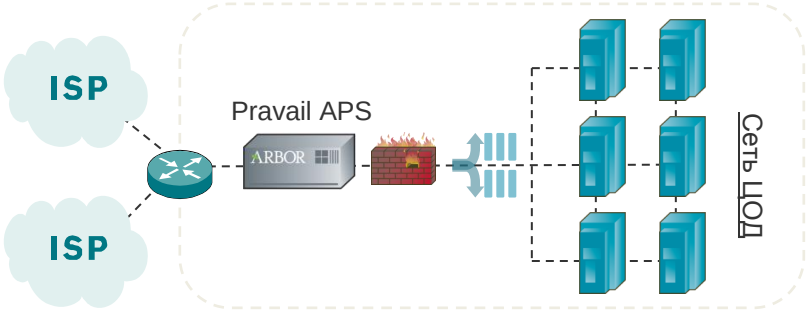
Фаза 1: Установка на периметре → Фаза 2: Обнаружение угрозы → Фаза 3: Подавление угрозы → Фаза 4: Извещение администратора

Защита от актуальных угроз доступности

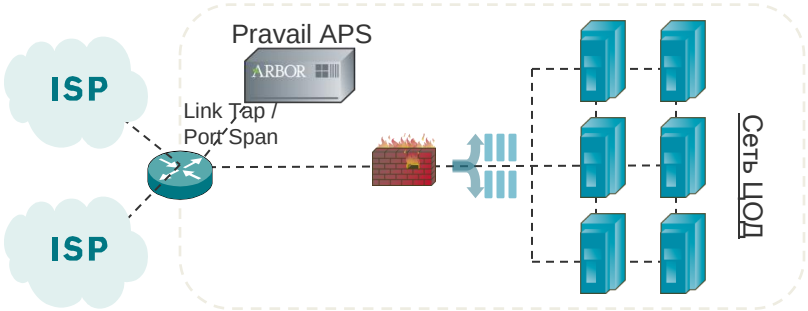
Специализация на защите от DDoS

- APS реализует специфические требования для защиты от DDoS
  - Блокировка трафика по странам (геофильтры)
  - Идентификация CDN и proxy – трафик легитимных пользователей не блокируется
  - Возможность ассиметричного внедрения
- А также стандартные требования для режима «в разрыв»
  - Варианты: блокировка, предупреждение без блокировки, мониторинг на SPAN/TAP интерфейсах
  - Встроенный bypass для всех типов интерфейсов
  - Программный bypass для прохода трафика без инспекции

В разрыв: активный/пассивный



Мониторинг на Span/Tap

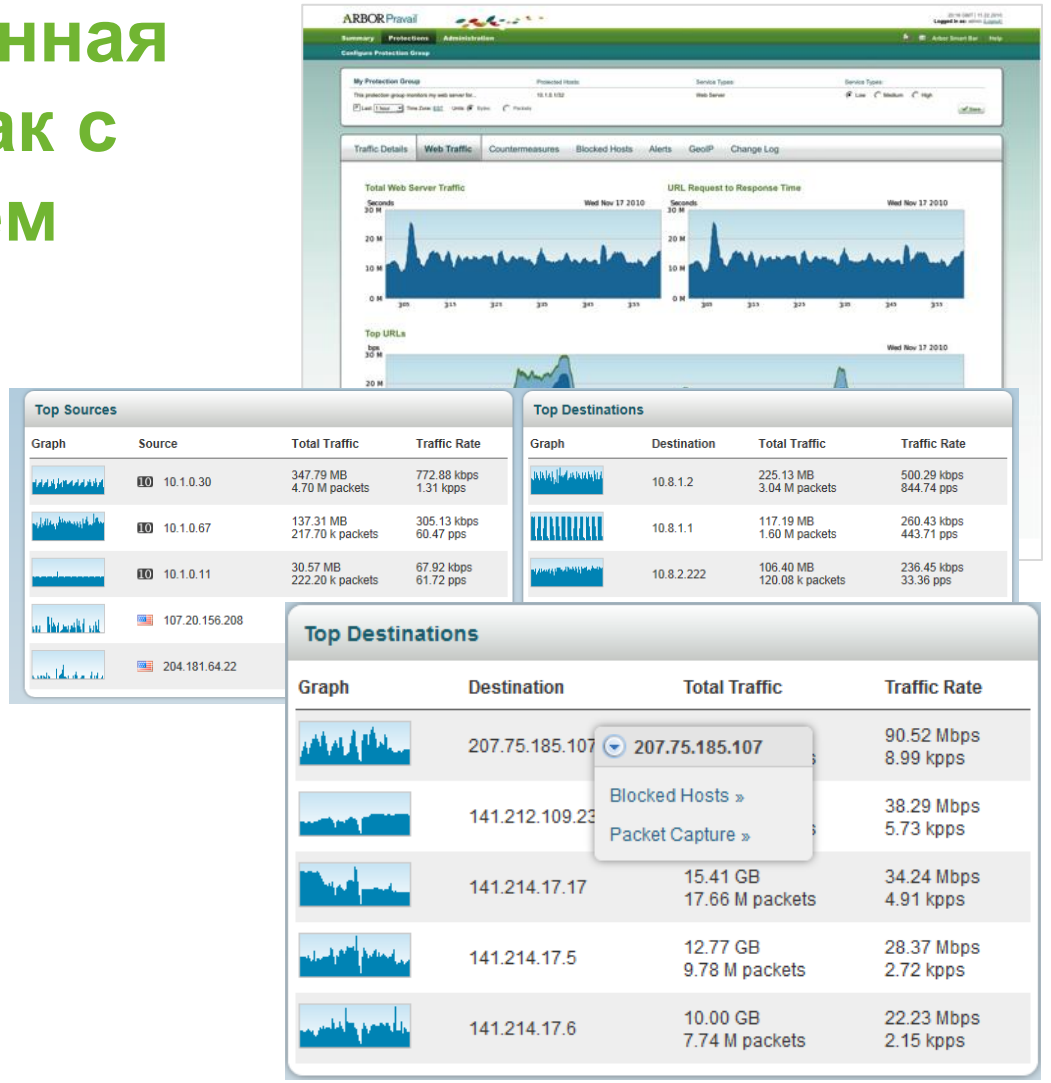


ARBOR NETWORKS

Простая установка и мгновенная защита

Цель APS – немедленная защита от DDoS-атак с полным контролем

- ***Простая и быстрая*** установка
- ***Защита от DDoS-атак*** на HTTP/DNS/VoIP сразу после установки
- ***Разные варианты*** установки – «в разрыв», в режиме мониторинга



ARBOR NETWORKS

Остановка сложных DDoS атак

Блокируются все виды DDoS, включая прикладные атаки и атаки на TCP

- Остановка сложных атак за счет инспекции всех пакетов
- Остановка сложных атак с помощью разных противомер
- Использование данных ATLAS для блокировки ботнетов

DDoS атаки
Из одного источника
Распределенный DoS
С/без подделки IP адресов
TCP атаки
TCP SYN атаки
Нелегитимные комбинации TCP флагов
Атаки на размер окна (Sockstress)
Атаки на сессии (TCP Idle, slow TCP и т.п.)
HTTP атаки
Медленные HTTP сессии (Slowloris, Pyloris)
Атаки на SSL сигнализацию (Pushdo, THC-SSL)
HTTP GET / POST URL флуды
DNS атаки
DNS флуд
DNS Cache Poisoning
Другие атаки
UDP / ICMP флуды
Атаки IP / TCP / UDP фрагментами
Атаки на VoIP/SIP

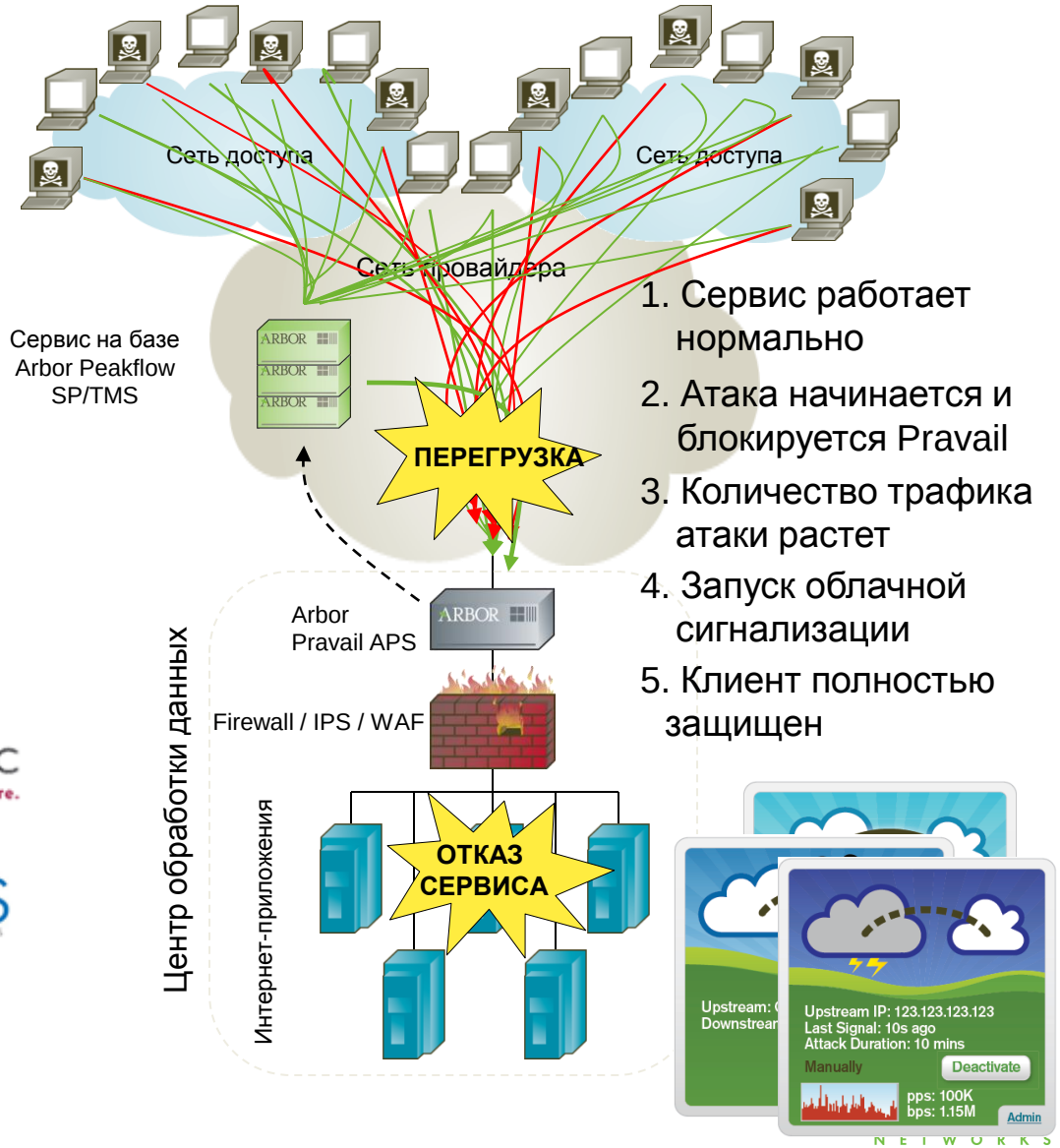
ARBOR NETWORKS

Альянс Cloud Signaling

CLOUD SIGNALING COALITION

Сотрудничество ISP и их клиентов с помощью протокола облачной сигнализации.

adversor DDoS Protection That Works™ · Axtel Comunícate mejor. · aixit · circular · colt smarter / faster / further · du وتحيا بها الحياة add life to life · Embratel · TATA · PROLEXIC DDoS Attacks End Here. · Telefónica · TelstraClear · VOCUS communications · swisscom · neustar



Модели Pravail APS

Серия 2000

Только для модернизации

Варианты интерфейсов защиты:

8 x 10/100/1000 (медь GE)

8 x GE Fiber (SX, LX)

Серия 2100

Варианты интерфейсов защиты:

12 x 10/100/1000 (медьGE)

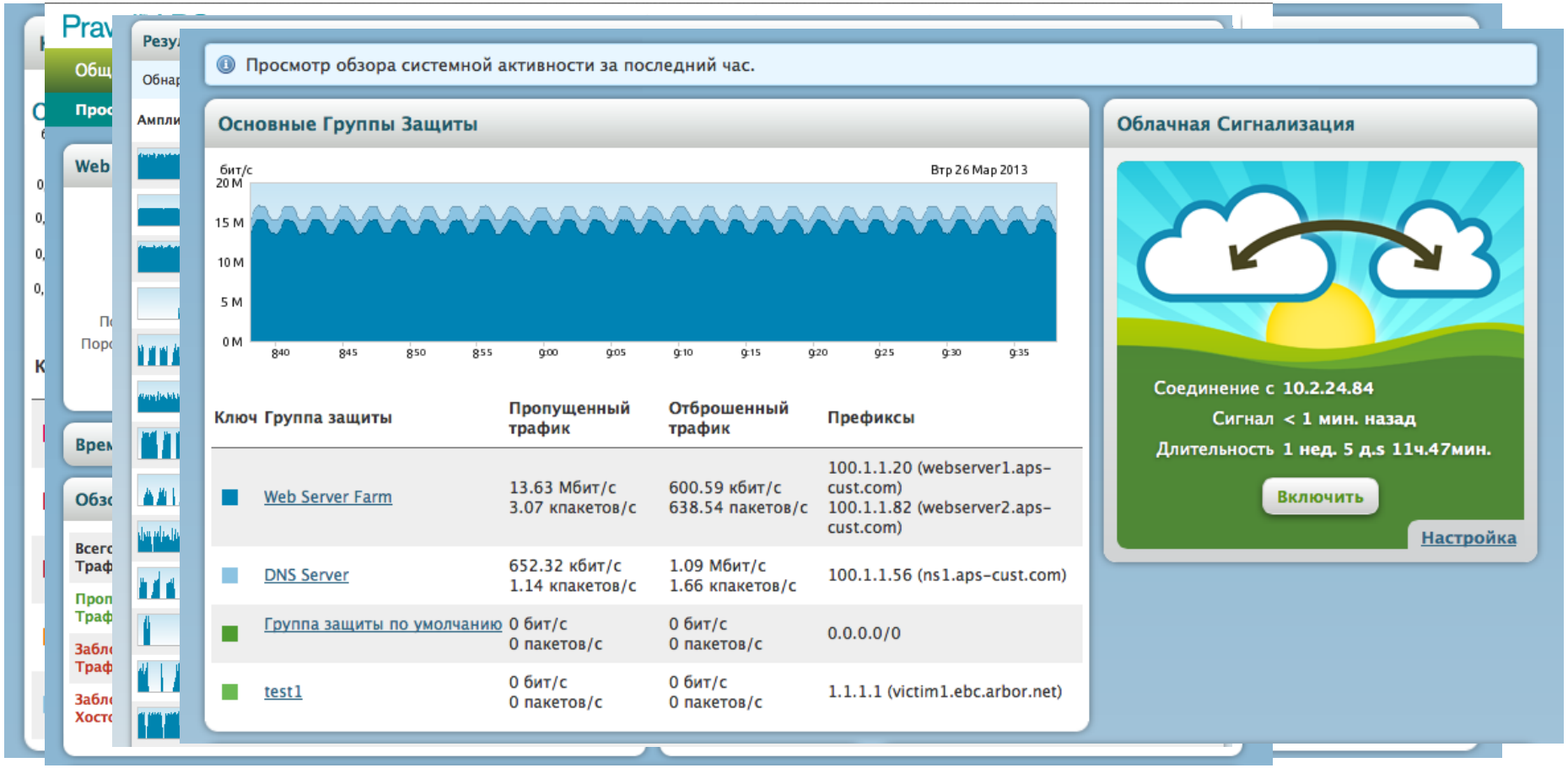
12 x GE Fiber (SX, LX)

4 x 10/100/1000 4 x GE SX + 4x GE LR

4 x 10G Interfaces (SR, LR)

Приятные мелочи

- Интерфейс и документация на русском языке



Pravail APS это эффективно и очень удобно!

- Защита Out of the Box (используя данные системы **ATLAS**)
- Предотвращение атак на приложения
- Защита от атак сетей Botnet
- Возможность общения с вышестоящим оборудованием по Cloud Signalling
- Продвинутая система отчётов, возможность видеть в реальном времени заблокированные хосты и причину их блокировки
- Возможность генерации сигнатур администраторами
- Интеграция с решением по детектированию аномалий и визуализации корпоративных сетей
- Возможность блокировки трафика по месторасположению (GeoIP)
- И при этом простой и удобный интерфейс, понятный пользователю!

ARBOR NETWORKS

Pravail NSI

Визуализация и анализ угроз

ARBOR NETWORKS

Обзор Pravail NSI

Анализ всего трафика для выявления сложных угроз

Глобальная визуализация

- Постоянный мониторинг без помех для трафика
- Учет каждого устройства и выявление аномалий

Выявление сложных угроз

- Профилирование трафика важных систем для определения аномалий
- Выявление трафика приложений

Расследование инцидентов

- Детальная информация по каждой сессии
- Помощь в ретроспективном анализе

ARBOR NETWORKS

Решение Pravail NSI

Pravail NSI обеспечивает визуализацию сетевого трафика и анализ угроз, которые не обнаруживаются пограничными устройствами безопасности

Визуализация корпоративного уровня

- Знайте вашу сеть

Анализ приложений

- Классификация приложений и трафика для обнаружения угроз

Отслеживание пользователей (Active Directory, Radius)

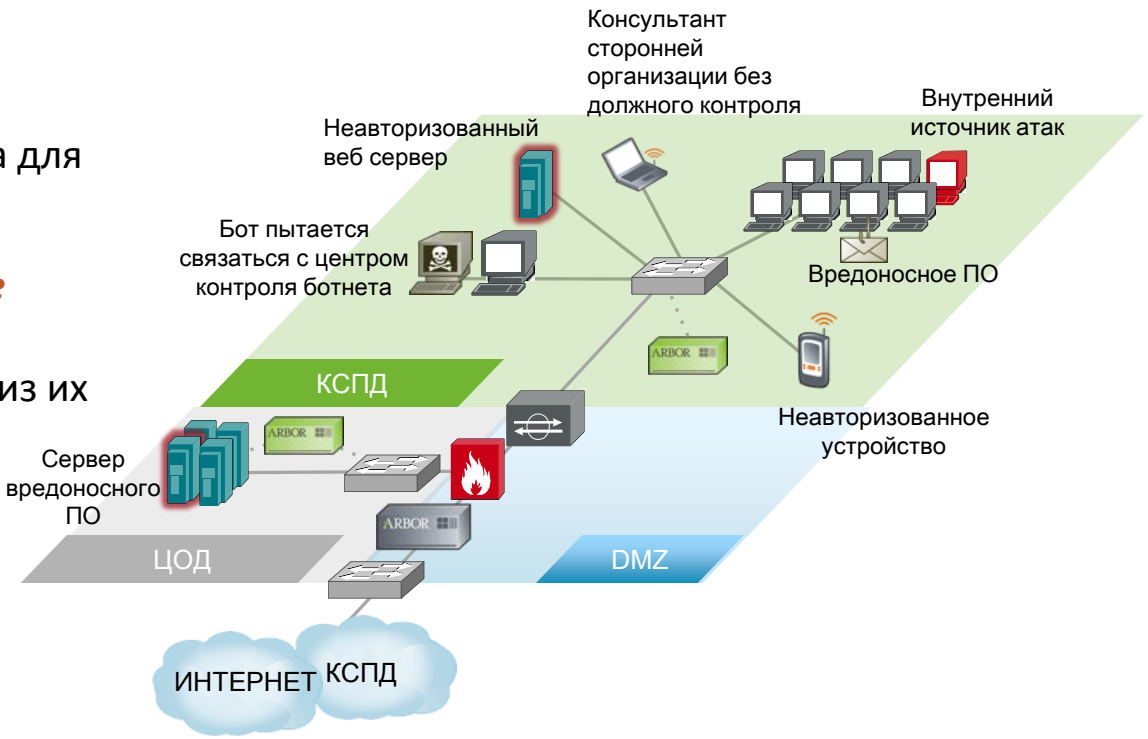
- Контроль и аудит пользователей, анализ их действий

Детектирование сложных угроз

- Профилирование важных систем и обнаружение аномалий

Простой механизм отчетов

- Мощный и легкий в использовании механизм построения отчетов



Глобальный анализ угроз

Использование глобального операторского мониторинга Arbor Networks для выявления угроз

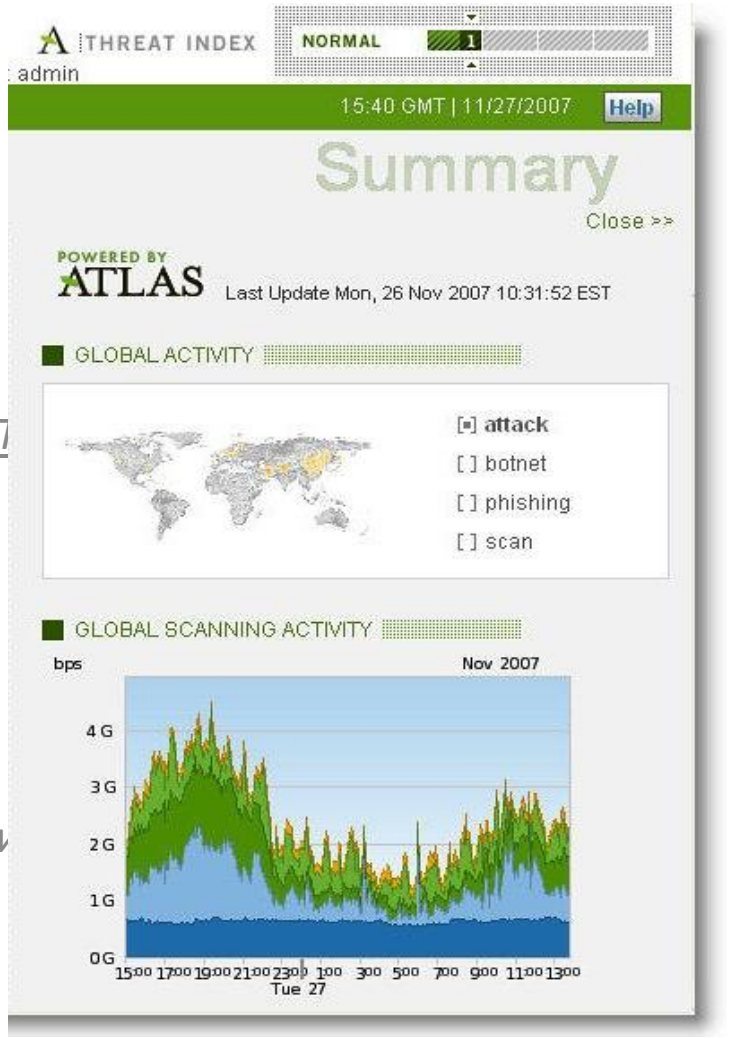
С помощью глобального мониторинга Arbor команда ASERT создает «сигнатуры поведения»

- Подробная информация о поведении известных или новых угроз.
- Выявление сложного вредоносного ПО, сканирования портов, фишинга, центров контроля ботнетов и проч.

Поведенческие сигнатуры доступны пользователям Pravail NSI через подписку ATF (Active Threat Feed)

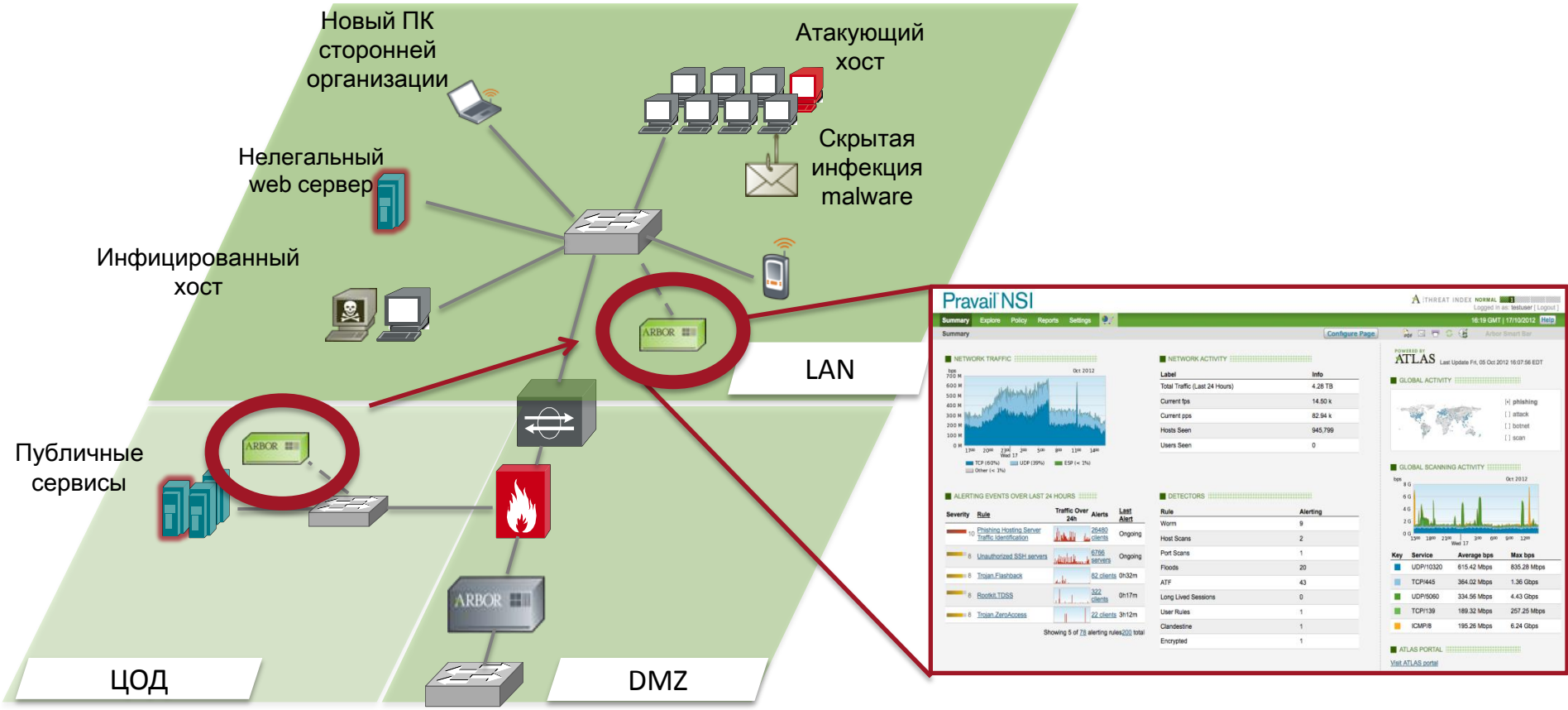
С помощью поведенческих сигнатур администраторы могут:

- Выявить атаку, определить источник, проанализировать особенности поведения и подавить атаку.



ARBOR NETWORKS

Как работает NSI?



Фаза 1: Сбор данных → Фаза 2: Анализ данных → Фаза 3: Генерация отчетов → Фаза 4: Извещение администратора

Единый интерфейс для всех сетевых «вопросов»

Визуализация трафика корпоративного уровня

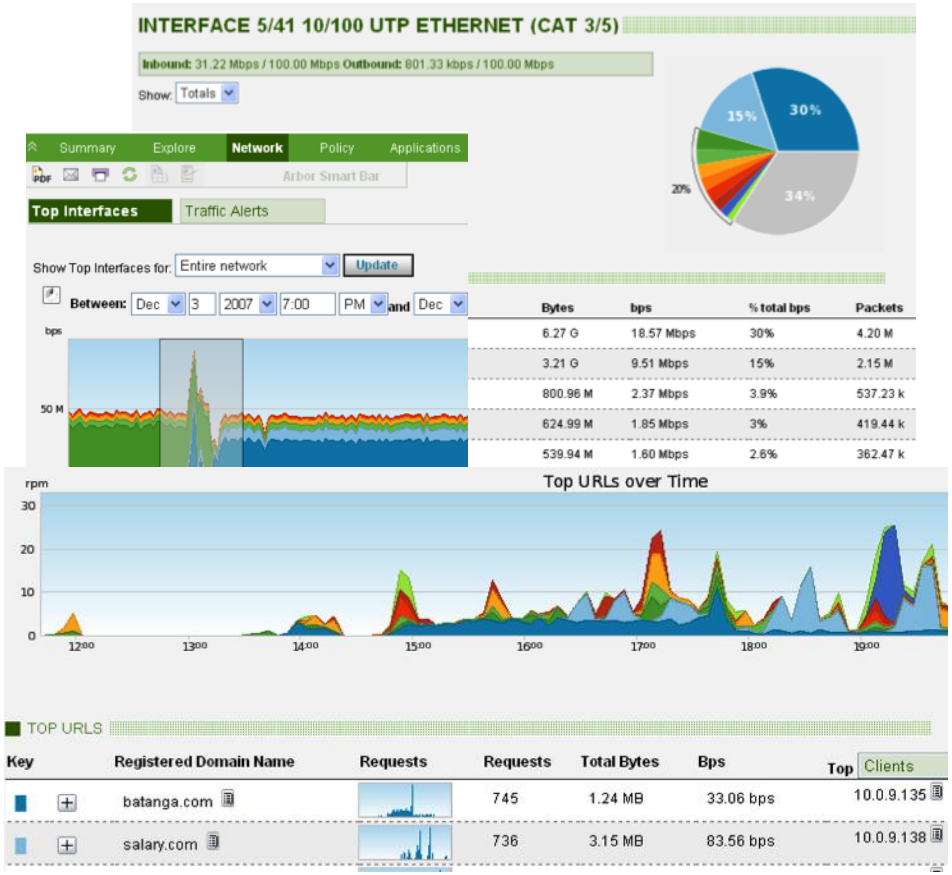
Визуализация трафика – необходимая основа безопасности
«Вы не можете обезопаситься от того, чего не видите»

Использование технологий IP Flow:

•Эффективная визуализация трафика всей компании

Обеспечение безопасности всей сети, а не только периметра:

•Анализ трафика по всей сети без границ



Мониторинг всей корпоративной сети

Визуализация трафика – необходимая основа безопасности

«Вы не можете обезопаситься от того, что не видите»

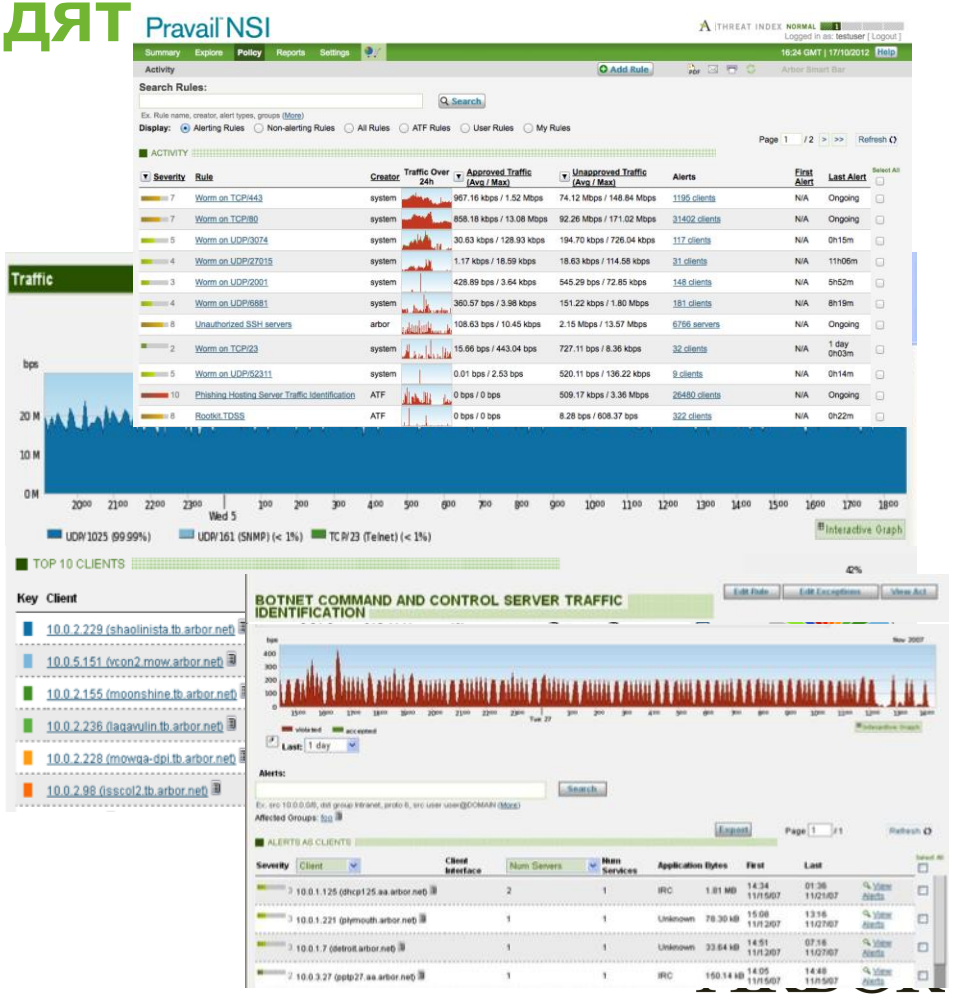
- *Знайте,* какой трафик передается в сети, от кого, куда и когда он идет
- *Идентифицируйте* аномалии в работе важных сервисов
- *Решайте проблемы ИБ*, владея контекстной информацией

ARBOR NETWORKS

Обнаружение сложных угроз

Идентифицируйте сложные угрозы, которые традиционные системы защиты периметра не видят

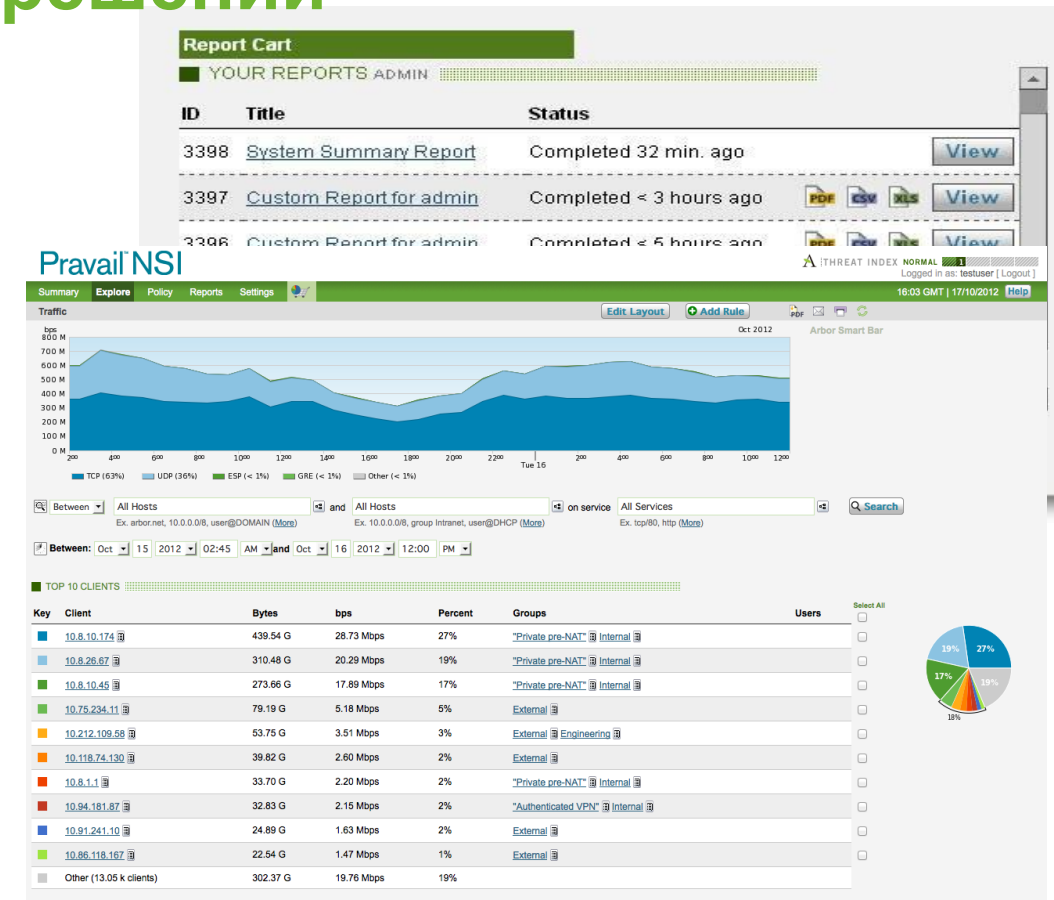
- *Обнаруживайте актуальные угрозы*, направленные на Вас и Ваши сервисы
- Используйте *поведенческий анализ и анализ на основе активности* для обнаружения malware



Отчетность и расследование инцидентов

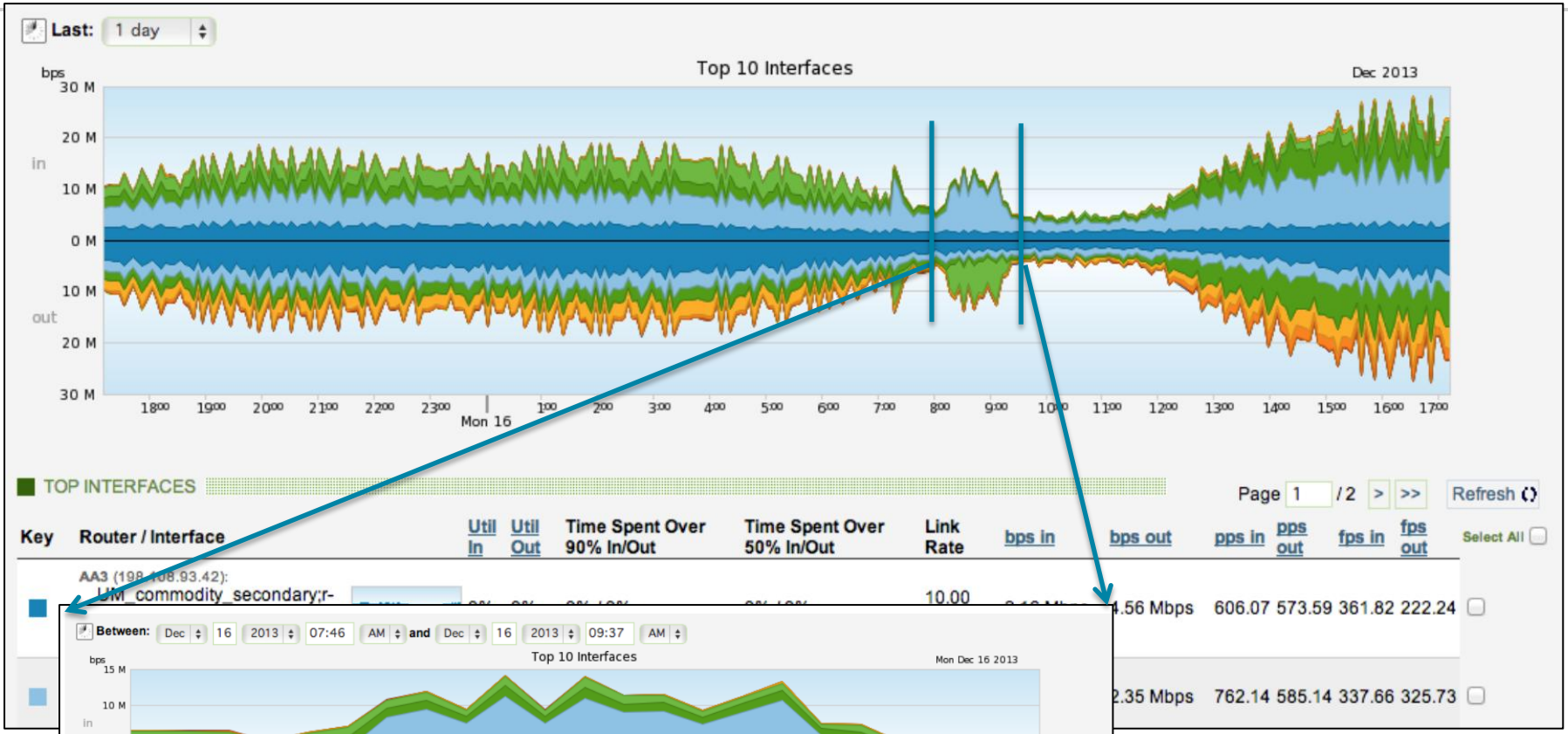
Широкий набор отчетов для упрощения эксплуатации сети и поддержки управленческих решений

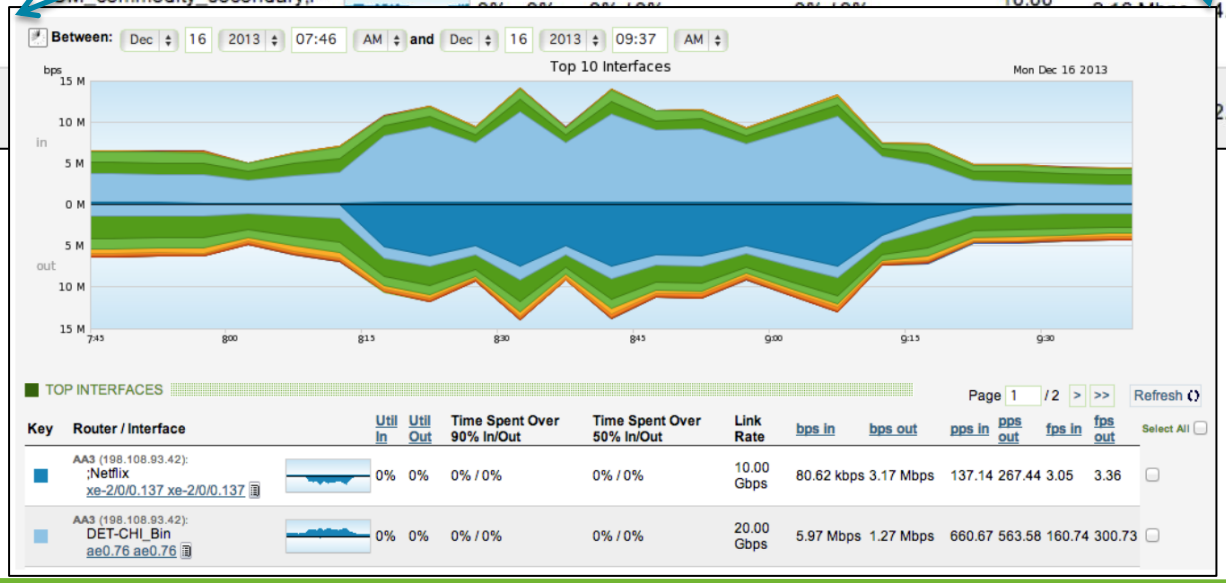
- *Настраиваемые отчеты* для технического и управленческого персонала
- *Информация об инцидентах* - вся активность любого устройства и пользователя
- *Соответствие* требованиям регуляторов HIPAA, PCI, EU Data Protection Directive, ITIL и ISO 17799.



ARBOR NETWORKS

Пример: обнаружение узких мест в сети

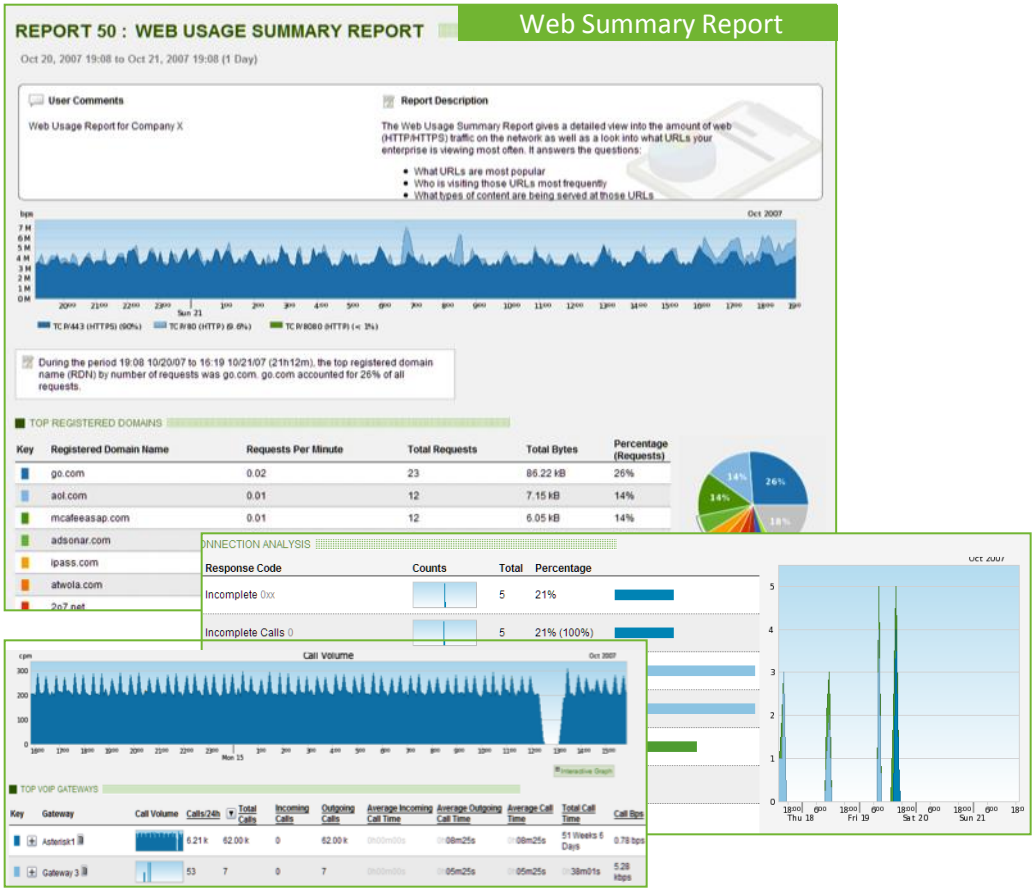




ARBOR NETWORKS

Анализ приложений

Глубокий анализ трафика и приложений для предотвращения утечек данных и выявления сложных угроз

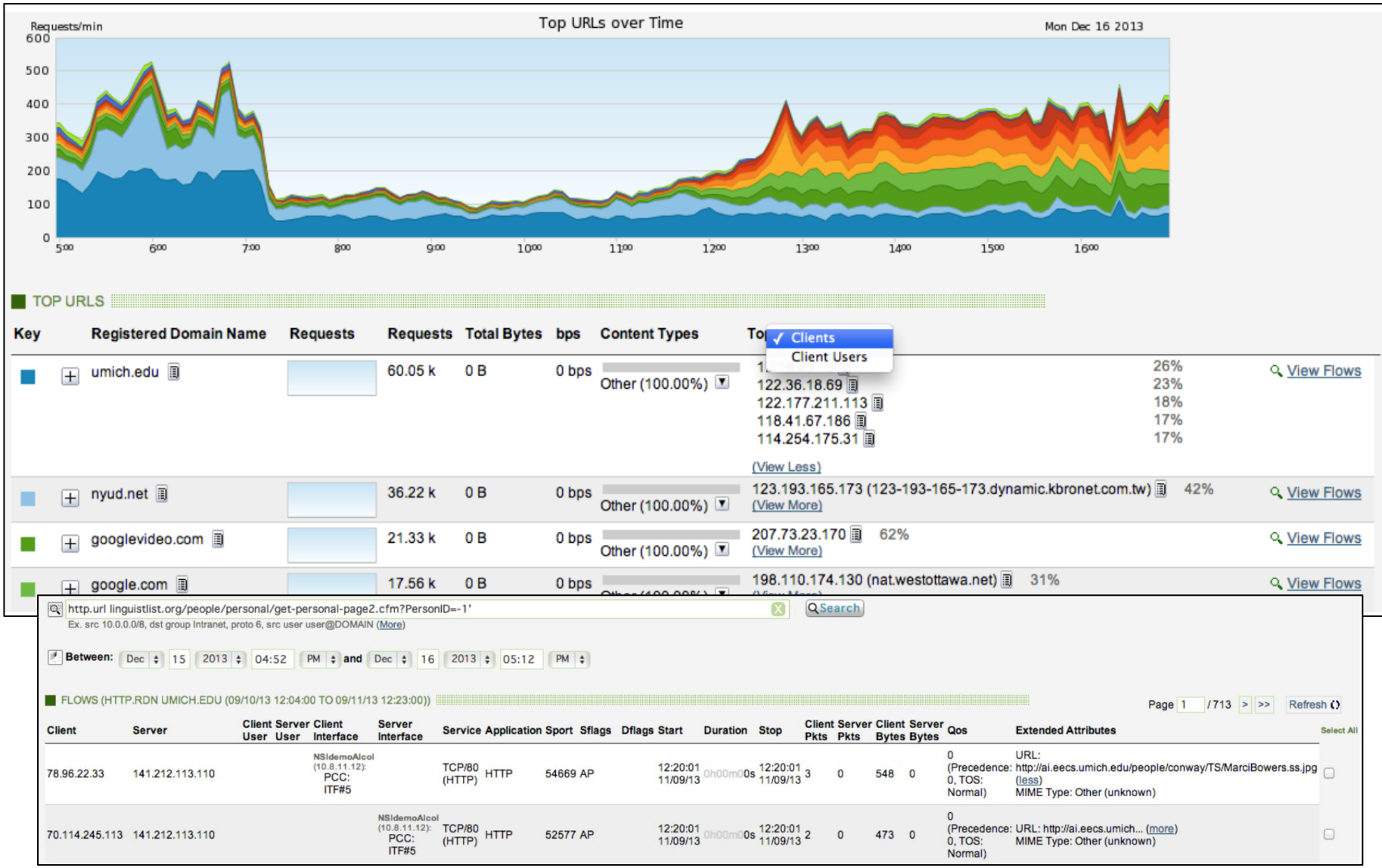


Предотвращение утечек данных за счет информации об открываемых ресурсах, трафике на некорректных портах и типе передаваемых данных

Аудит использования сайтов и приложений – полная информация об использовании приложений и доступе к ресурсам

ARBOR NETWORKS

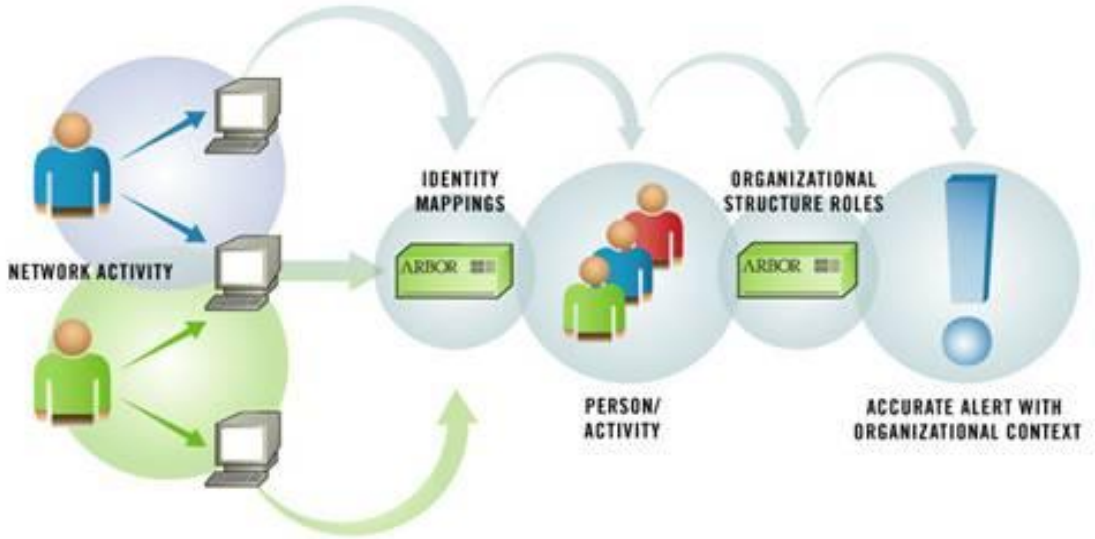
Пример: аналитика по URL



ARBOR NETWORKS

Контроль действий пользователей

Аудит и обеспечение безопасности не только с точки зрения IP адресации, но и с применением имен пользователей



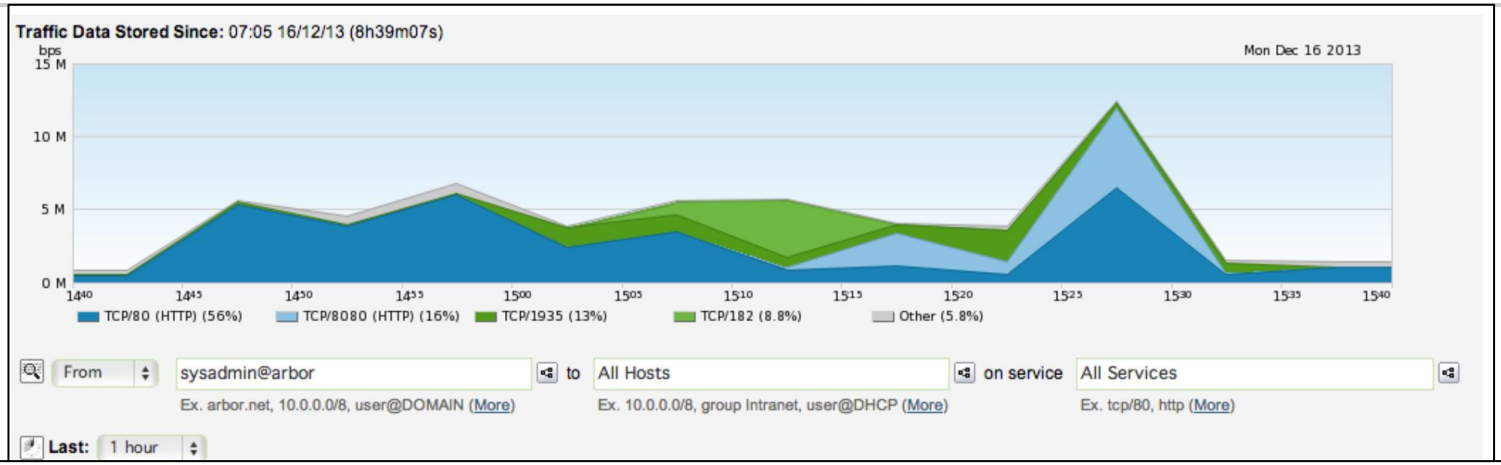
Выявляйте пользователей вредоносного ПО, а не только IP адреса

Выполняйте глубокий аудит всех соединений, сервисов и устройств связанных с пользователем.

Интегрируйте NSI с SAN для длительного хранения данных

ARBOR NETWORKS

Пример: трафик пользователя с правами администратора



TOP 10 SERVICES

Key	Applications
TCP/80	
TCP/8080	
TCP/1935	
TCP/182	
TCP/443	84% SSL
TCP/22	99% SSH
TCP/5103	85% HTTP
TCP/8006	
TCP/4070	
UDP/19305	
Other (31 services)	

TOP 10 SERVERS

Key	Server	Bytes	bps	Percent	Groups
	8.27.81.254	317.82 M	706.27 kbps	15%	External
	192.96.204.199	232.84 M	517.41 kbps	11%	External
	199.101.135.167	220.95 M	490.99 kbps	11%	External
	4.27.1.252	179.39 M	398.65 kbps	9%	External
	204.160.108.254	179.27 M	398.38 kbps	9%	External
	192.96.205.169	115.62 M	256.93 kbps	6%	External
	192.96.204.198	95.01 M	211.13 kbps	5%	External
	173.223.6.237	93.78 M	208.40 kbps	5%	External
	8.26.213.253	84.30 M	187.34 kbps	4%	External
	192.96.205.168	63.46 M	141.01 kbps	3%	External
	Other (1.83 k servers)	481.40 M	1.07 Mbps	23%	

ARBOR NETWORKS

Архитектура Pravail NSI

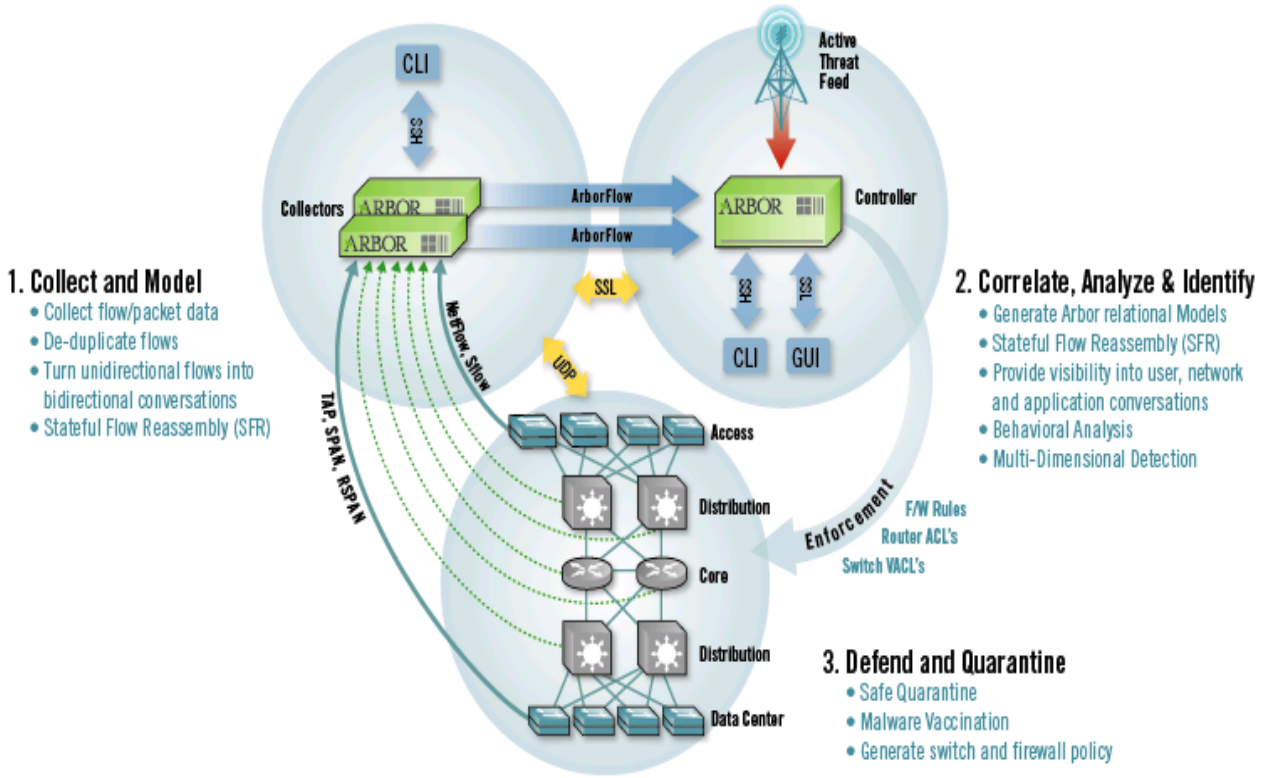
Двухуровневая архитектура для максимальной масштабируемости

Контроллер

- Устройство, содержащее БД и flow log, а также предоставляющее GUI для централизованного управления и построения отчетов

Коллектор

- Устройство, собирающее NetFlow и SNMP с сетевых устройств, выполняющее первоначальный анализ трафика
- Устройство, получающее копию трафика со SPAN порта и выполняющее L7 анализ



ARBOR NETWORKS

Устройства Pravail NSI

Контроллеры серии 5100

Замена лицензии

Замена лицензии

Контроллеры серии 5200

Замена лицензии

Контроллеры NSI 5200 поддерживают модуль *DHM* для длительного хранения информации для аудита на SAN

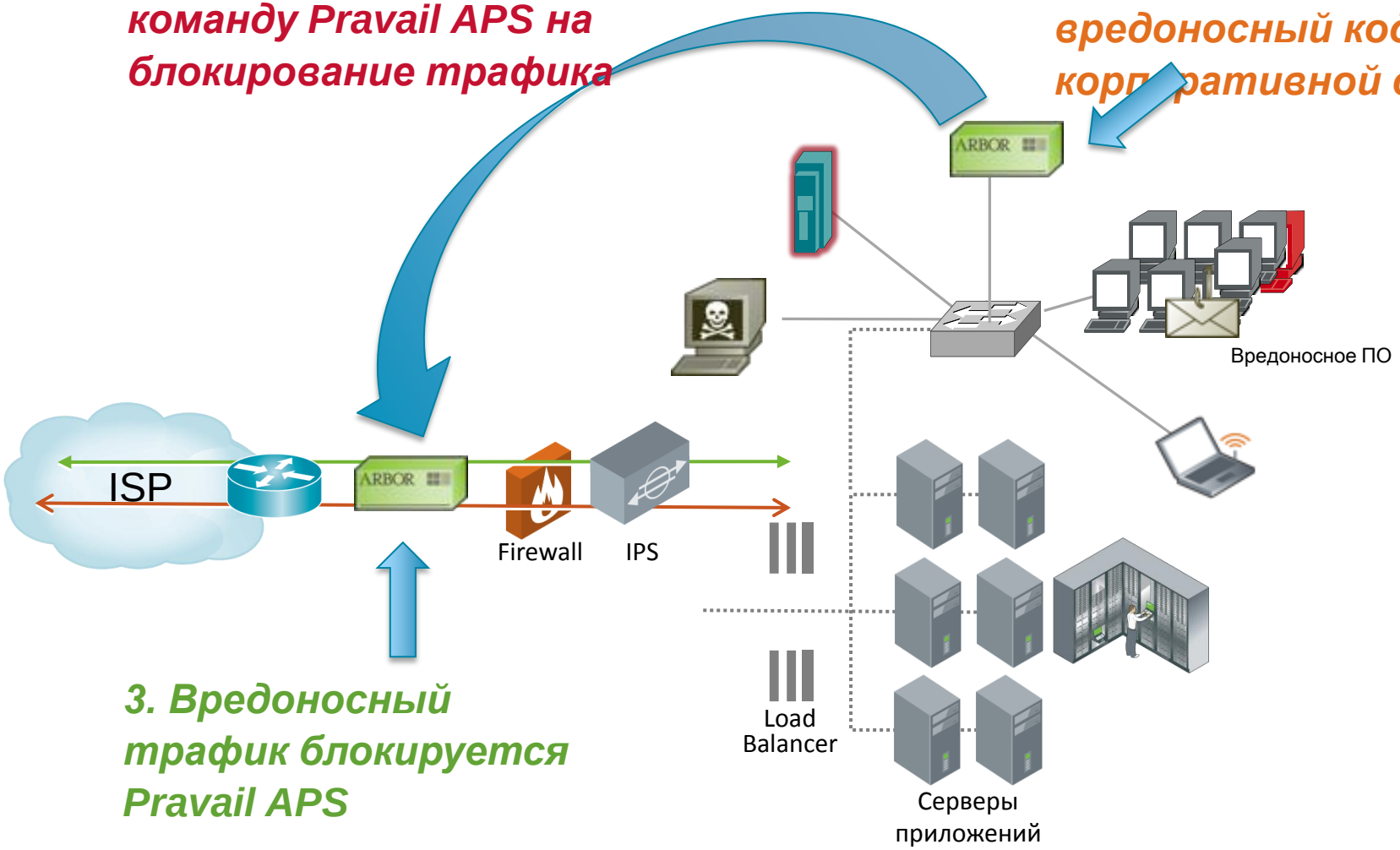
Коллекторы серии 5000

ARBOR NETWORKS

Интеграция Pravail APS и Pravail NSI

1. Pravail NSI детектирует вредоносный код в корпоративной сети

2. Pravail NSI отдаёт команду Pravail APS на блокирование трафика



3. Вредоносный трафик блокируется Pravail APS

ARBOR NETWORKS

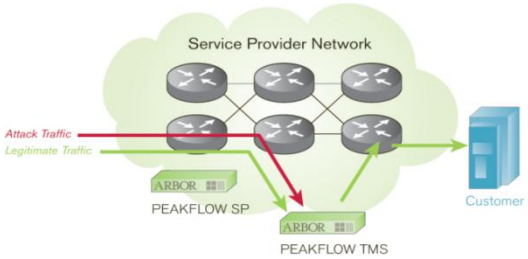
Peakflow SP

Обеспечение доступности сервисов и визуализация сети

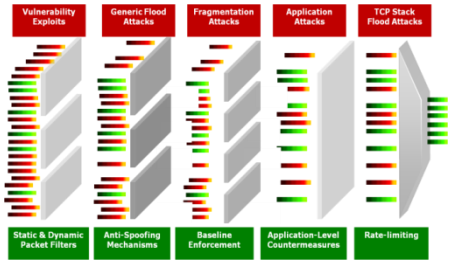
ARBOR®
NETWORKS

Peakflow SP, в качестве решения защиты от DDoS

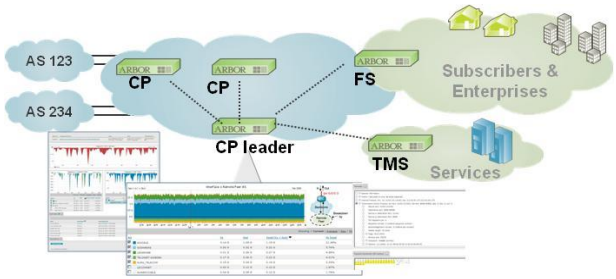
Хирургическая очистка



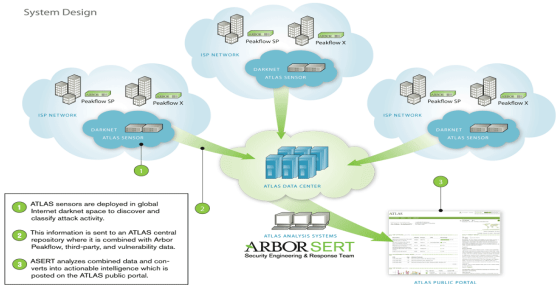
Многочисленные противомеры



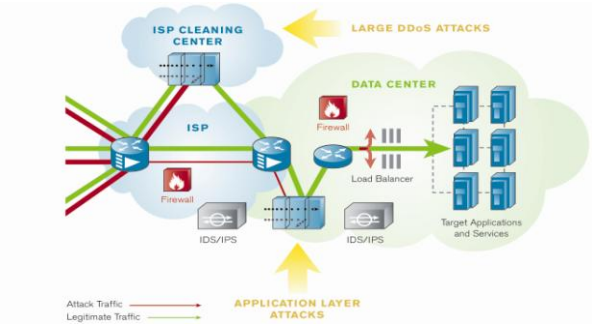
Распределенное детектирование



Глобальный анализ



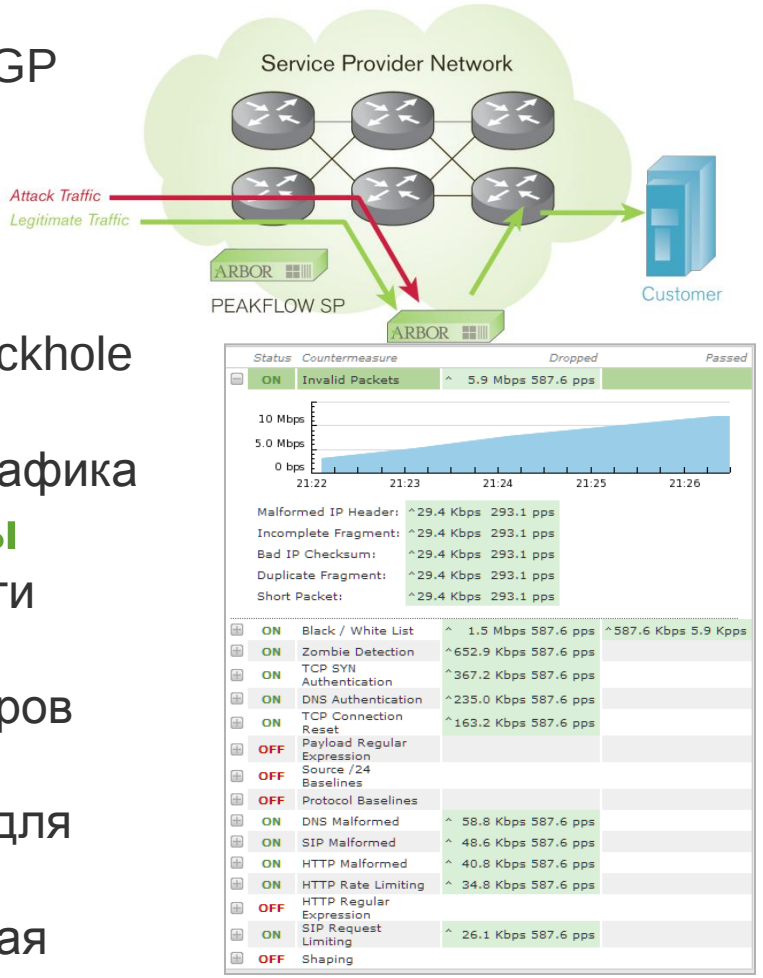
Оптимальное внедрение решения



ARBOR NETWORKS

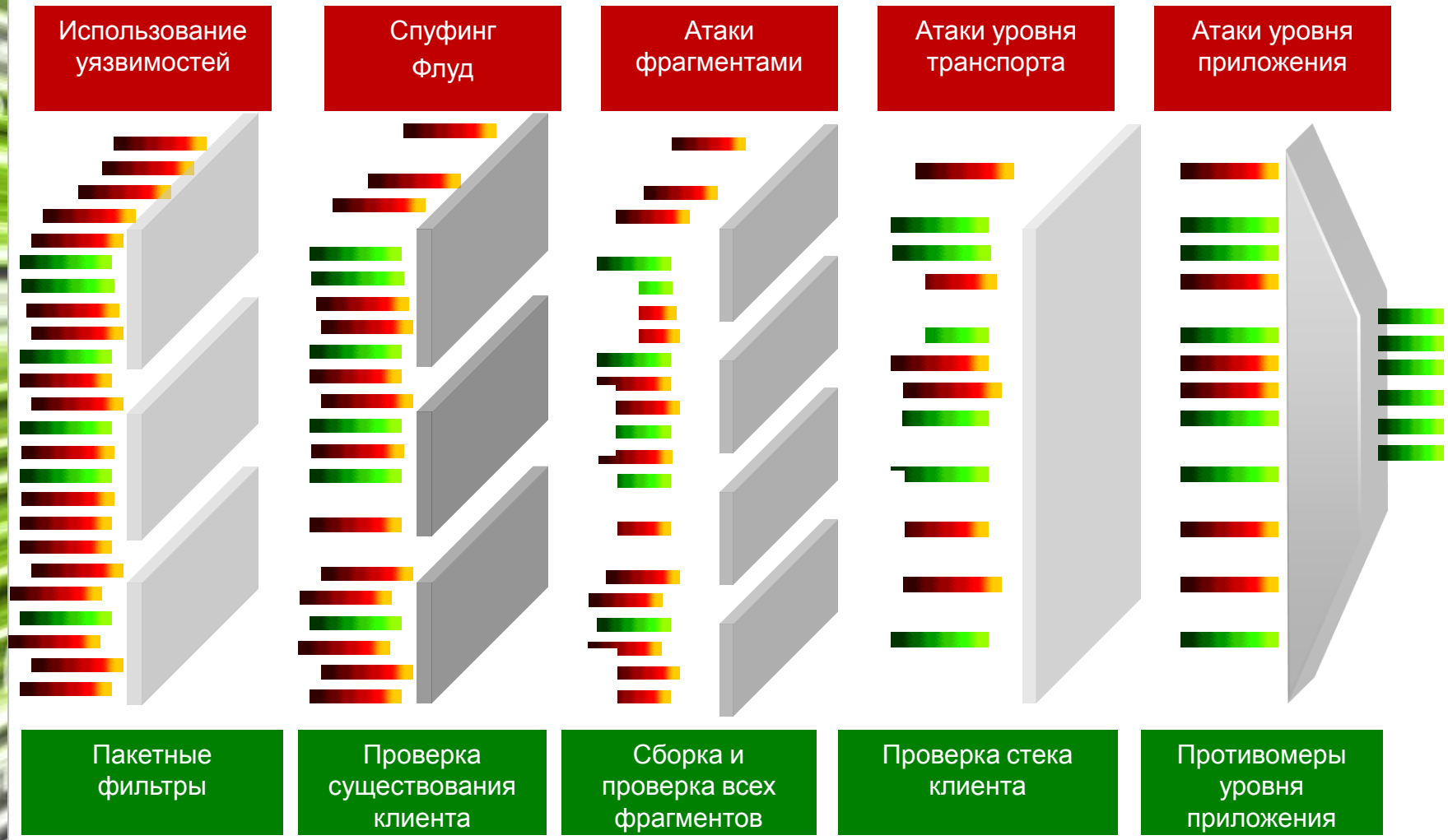
Гибкие и хирургические механизмы очистки трафика

- **Гибкость очистки**
  - Установка TMS в режиме BGP Off Ramp
  - Установка TMS в режиме In-Line
  - Генерация списков доступа
  - Поддержка механизмов Blackhole (RTBH, S/RTBH, Flowspec)
  - Механизмы ограничения трафика
- **Хирургические механизмы**
  - Контроль производительности сервисов
  - Черные белые списки фильтров
  - Сложные пакетные фильтры
  - Специальные противомеры для HTTP, DNS, SIP
  - Сигнатурная и географическая очистка
  - Поддержка режима обучения



ARBOR NETWORKS

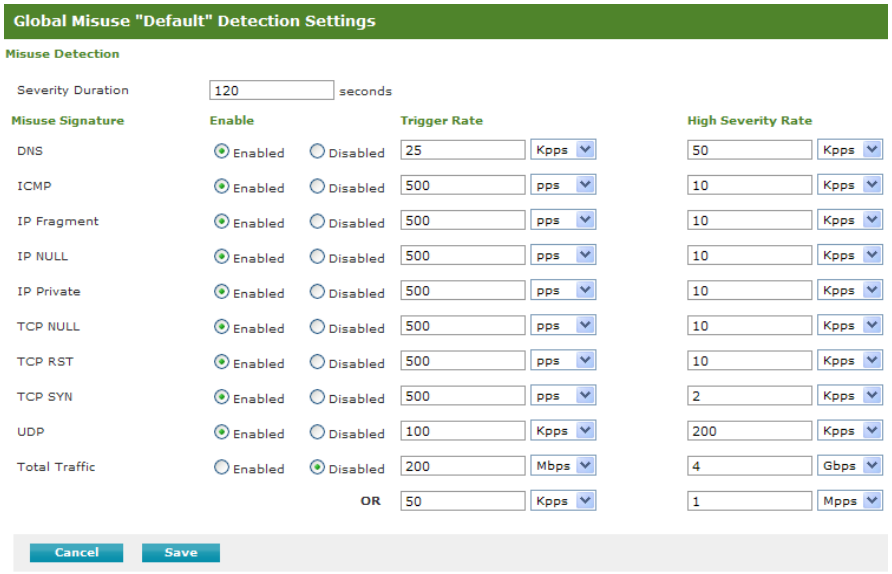
Многочисленные противомеры для атак всех видов

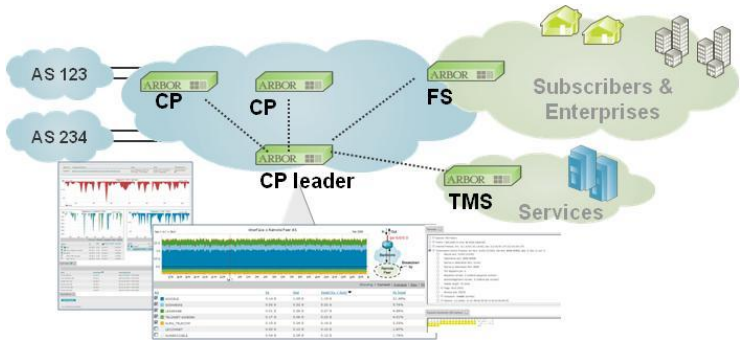


ARBOR NETWORKS

Распределенное адаптивное детектирование

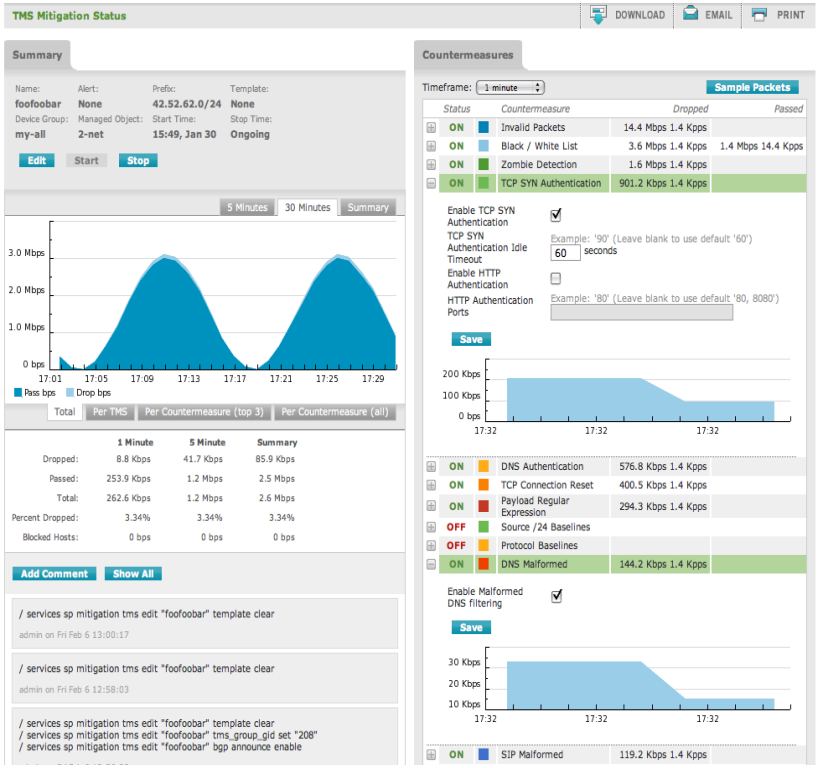
- **Аномалии Misuse**
  - Уровни срабатывания для потенциального подозрительного трафика (TCP SYN, фрагменты IP, DNS и т.п.)
- **Аномалии Profiled**
  - Аномальное увеличение уровней трафика
- **Сигнатурные аномалии**
  - Известные сигнатуры атак
  - Авто обновления – ATF, FSA
  - Собственные сигнатуры
- **Аномалии GeoIP**
  - Поиск аномалий на основе географической информации





Защита сервисов

- Защита приложений HTTP/Web2.0
  - Блокировка некорректных пакетов
  - Ограничения запросов HTTP
  - Очистка по регулярным выражениям
  - Контексты для защиты HTTP
  - Списки фильтров URL
  - Проверка стека клиентов
- Защита сервисов VoIP
  - Блокировка некорректных пакетов
  - Ограничение запросов SIP
- Защита DNS
  - Очистка по регулярным выражениям
  - Проверка стека клиентов
  - Ограничение запросов DNS
  - Защита от Cache Poisoning
  - Пакетное детектирование DNS атак
  - Списки фильтров DNS
  - Контексты для защиты DNS
- Защита на уровне IP
  - Проверка пакетов (TCP / UDP / ICMP)
  - Сброс сессий TCP
  - Черные и белые загружаемые списки
  - Блокировка зомби

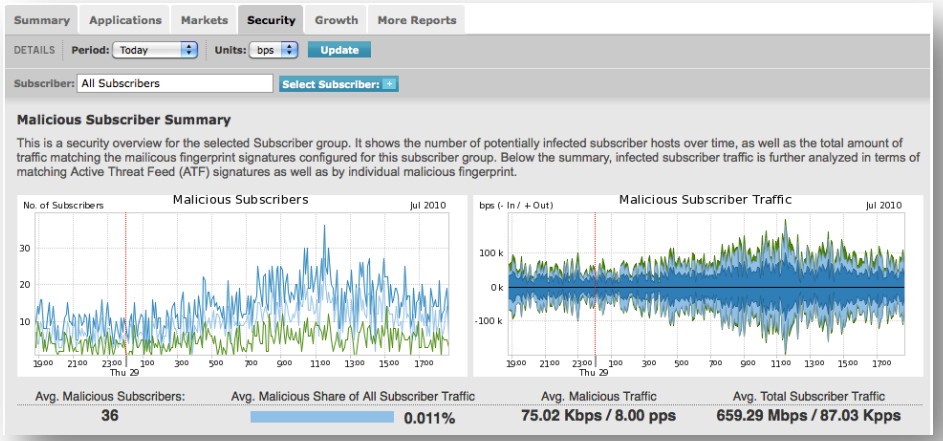


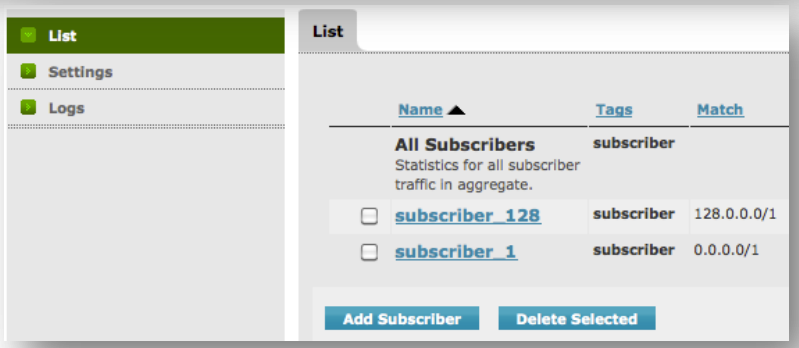
Преимущество

Защита важной инфраструктуры и приложений от спектра атак

Отчеты по абонентам и выявление инфицированных абонентов

- Отслеживание инфицированных абонентов и их трафика
- Общие отчеты по абонентскому трафику
- Прогноз роста трафика
- Определение ключевых рынков (городов IP Location)
- Определение ключевых приложений
- Защита и отчетность для сетей мобильного и фиксированного доступа





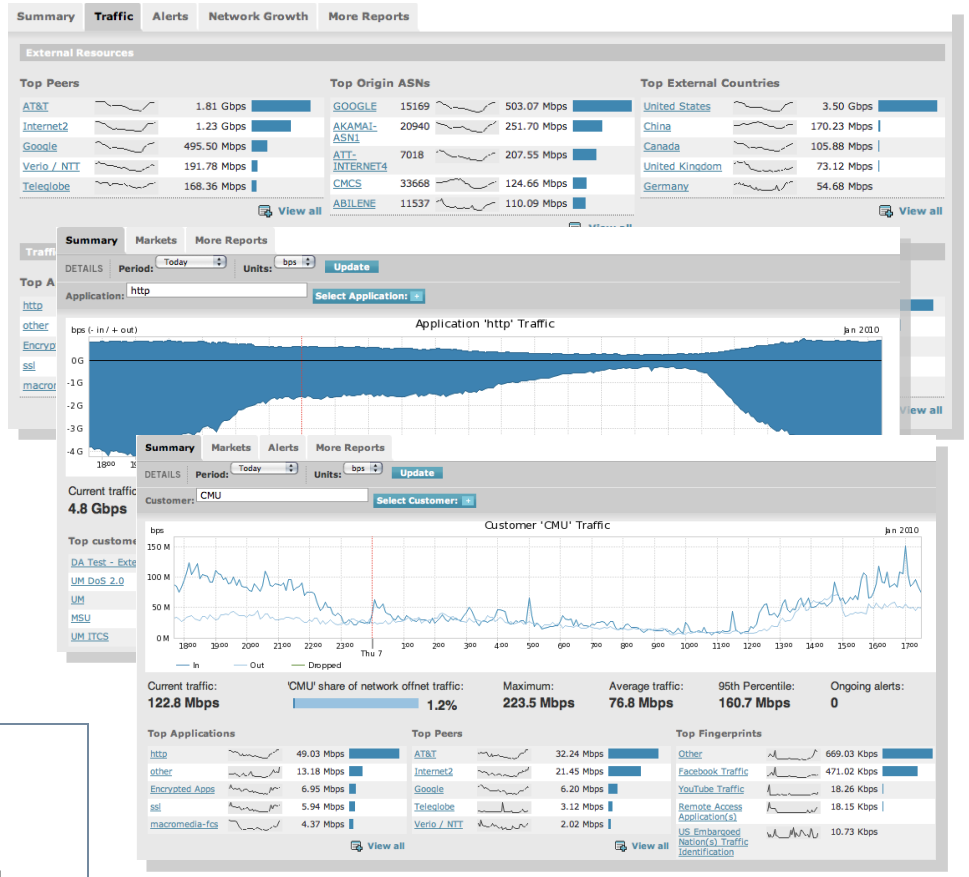
Преимущества

Идентификация зараженных абонентов
Защита абонентов и сетей доступа
Отчеты для планирования развития

ARBOR NETWORKS

Интегрированные отчеты

- **Сеть:** Основные пиры, автономные системы, страны, регионы, города, приложения, сигнатуры, анализ роста
- **Приложения:** Клиенты, порты, пиры, рынки
- **Клиенты:** приложения, пиры, сигнатуры, рынки, события
- **Маршрутизаторы:** Статистика, интерфейсы, приложения, клиенты



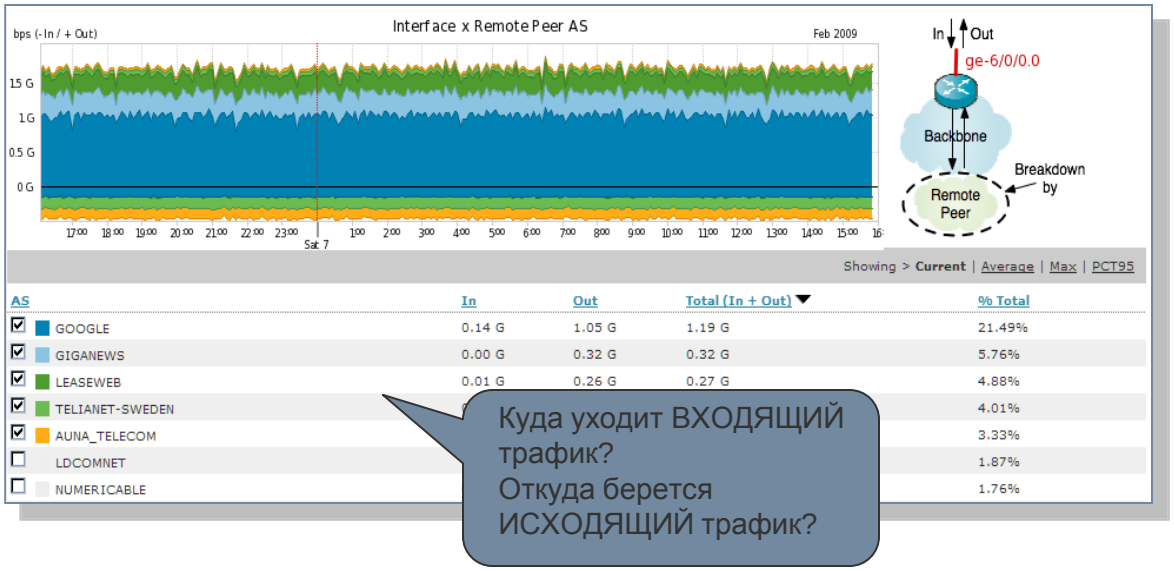
Преимущества

Полная картина сети
Источник информации для принятия взвешенных решений

Широкий спектр пиринговых и транзитных отчетов

Функционал

- Отчеты по клиентам
- Отчеты по пирам
- Отчеты по интерфейсам
- Анализ источников и получателей трафика
- Графическое представление



- **Получение информации об истинном назначении трафика**
- **Данные для принятия взвешенных решений по изменению пиринговой политики**
- **Реализация максимального потенциала из существующих пиринговых соглашений**
- **Контроль выполнения пиринговых контрактов и клиентских обязательств**

Преимущества

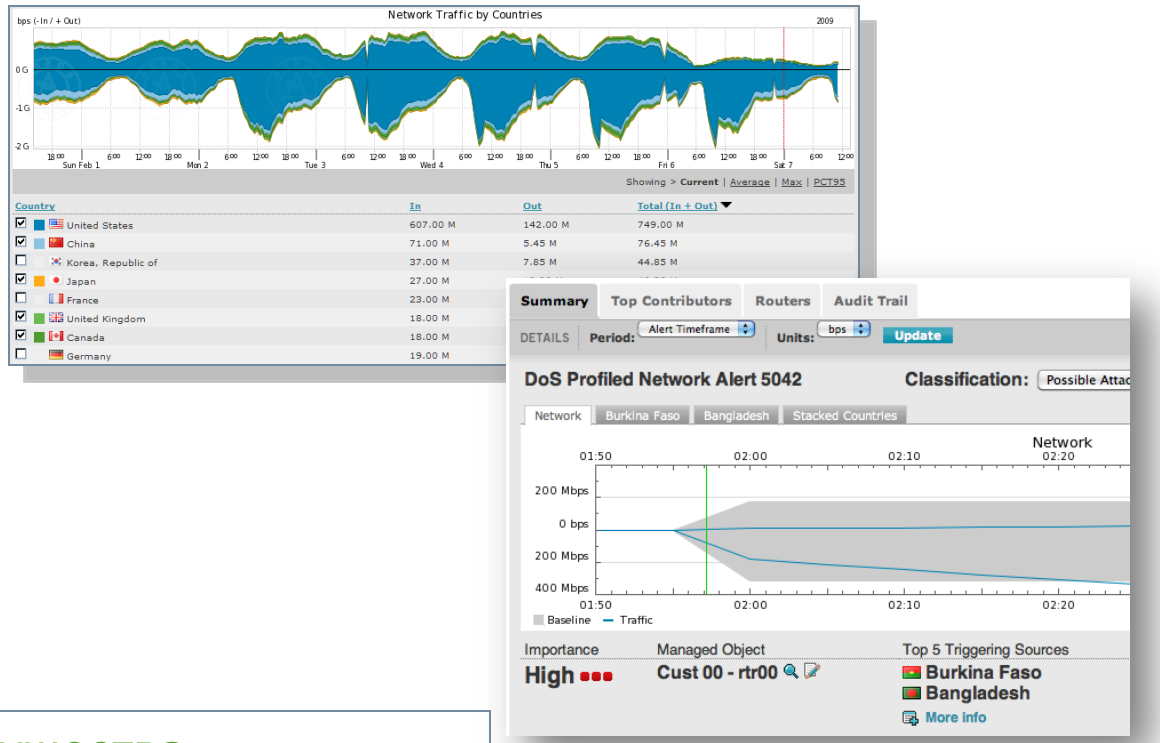
Оптимизация издержек на пиринг
Улучшение качества сервиса

ARBOR NETWORKS

Глобальная географическая отчетность – IP Location

- Отчеты по странам, регионам и городам
- Географическое проецирование источников атак
- Выявление и анализ аномалий с учетом географии
- Использование географии при очистке трафика
- Анализ рынков

Новое измерение сетевого анализа



Преимущества

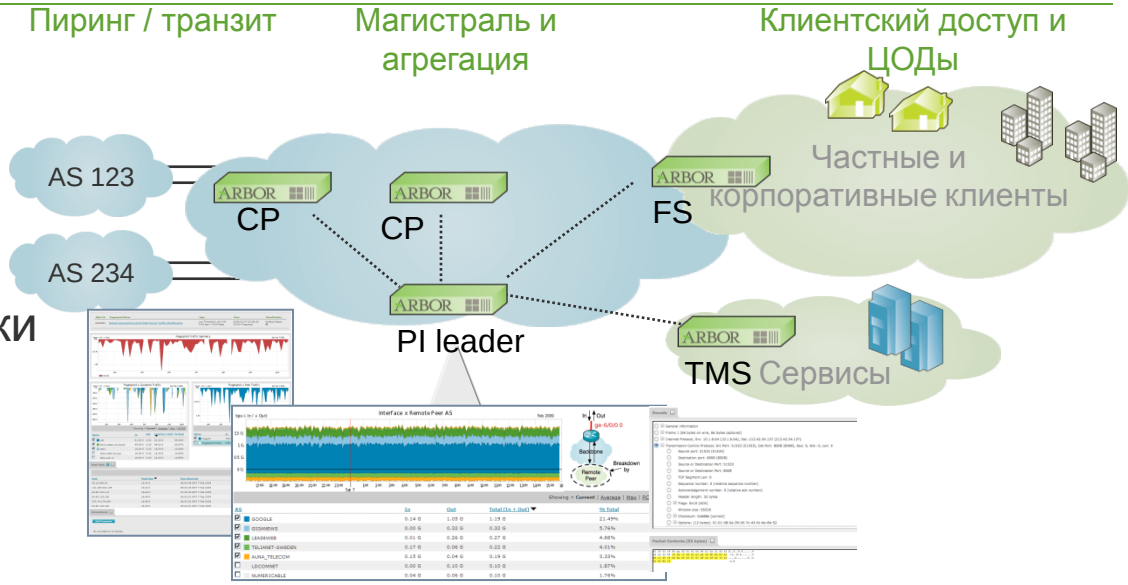
Улучшение поиска и анализа аномалий

Глубокий анализ рынка

Уникальные возможности планирования

Мониторинг сервисов

- Измерение потребления приложений
- Отслеживание ключевых параметров производительности:
  - Вариация задержки
  - Задержка
  - Потеря пакетов
- Глубокий анализ 90 приложений
- Возможность определения собственных приложений
- Отчеты по основным URL
- Отчеты по VoIP звонкам
- Отчеты по DNS запросам
- Отладка сервисов с помощью анализа пакетов в реальном времени
- Выявление аномалий по изменению параметров сервисов
- Анализ изменения параметров сервисов



Преимущества

Выявление и устранение проблем до возникновения жалоб

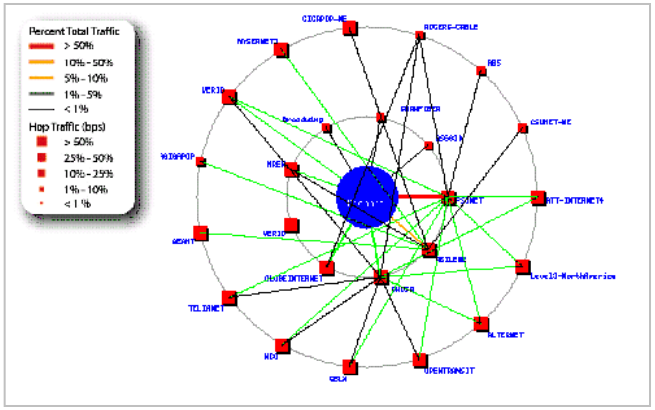
Уменьшение нагрузки на колл-центр

Улучшение планирования сети и сервисов

ARBOR NETWORKS

Анализ маршрутных таблиц

- Поддержка BGP
  - Анализ маршрутных таблиц
  - Отчеты для оптимизации пиринговых и транзитных взаимоотношений
  - Выявлений атак на таблицы маршрутизации
  - Анализ нестабильностей
- Анализ трафика MPLS VPN

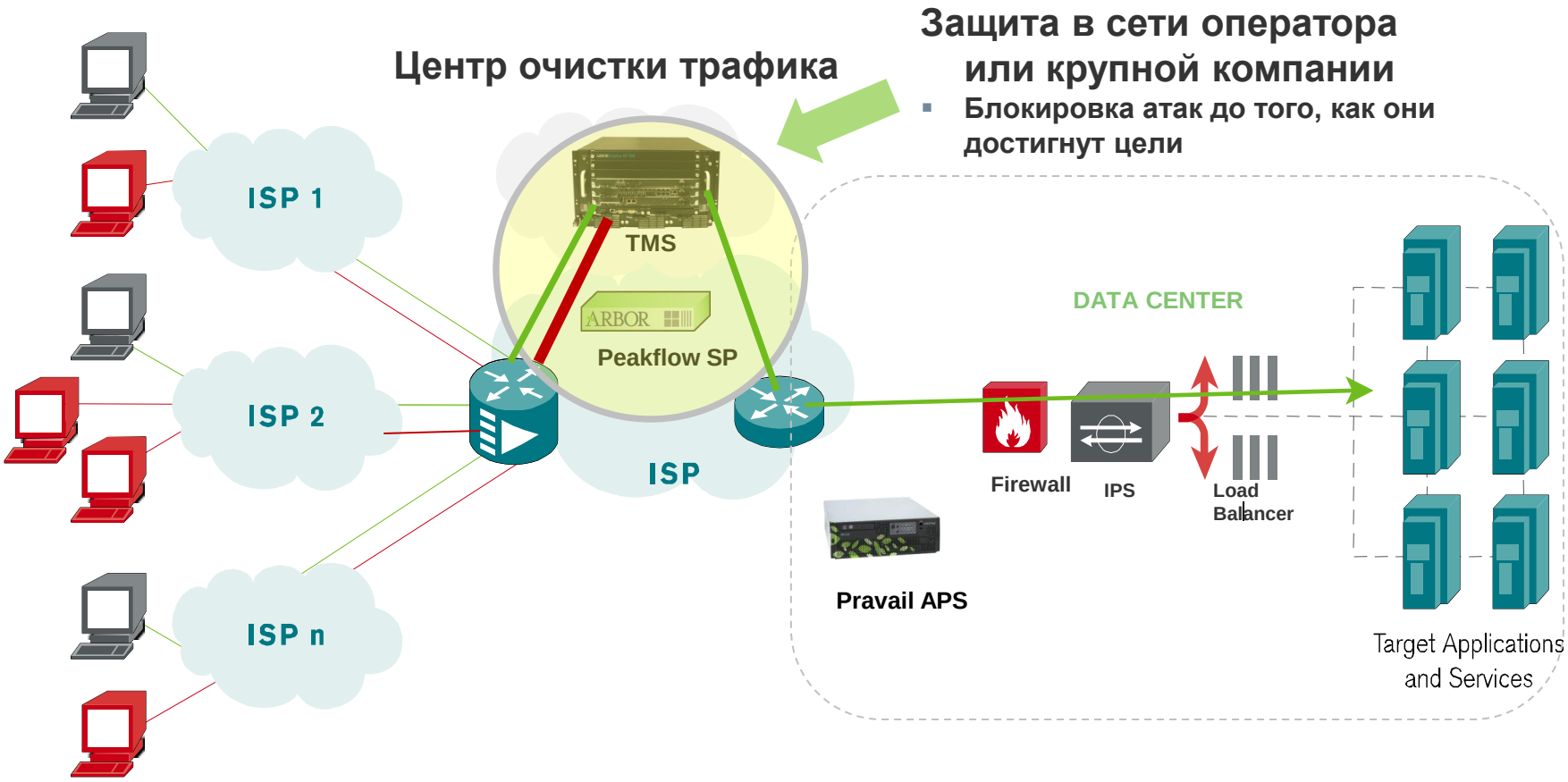


Преимущества

Уменьшение расходов на пиринг и транзит
Проверка выполнения договорных обязательств
Упрощение миграции на IPv6 / 4x байтные ASN
Выявление новых сервисов и возможностей заработка
Оптимизация инвестиций в сетевую инфраструктуру

ARBOR NETWORKS

Многоуровневая защита от Arbor Networks
Защита в сети оператора/крупной компании



Как работает Peakflow?

CUSTOMER PORTAL

(web based Portal-Service)

Для управляемых услуг по предоставлению отчетов и подавлению атак

COLLECTOR PLATFORM (CP)

- **Безопасность**
- Обнаружение угроз инфраструктуре и клиентам
- Обнаружение DDoS атак
- Анализ, traceback, отчетность

- **Управление трафиком**
- Анализ и видимость трафика
- Отчеты по приложениям, BGP, географии, пирингу, клиентам, интерфейсам

THREAT MANAGEMENT (TMS)

- **Подавление атак**
- Решение операторского уровня
- 1.5-40 Гбит/с на устройство
- Постоянно расширяющийся набор противомер по очистке трафика
- Отчетность и подстройка системы в реальном времени
- Несколько вариантов интеграции для любого дизайна сети

- **DPI-анализ трафика**
- HTTP/DNS/VOIP - отчетность

- **SLA- отчетность**

PORTAL INTERFACE (PI)

- HA для графического интерфейса
- Масштабирование системы для управляемых услуг

FLOW SENSOR (FS)

- Масштабирование системы для мониторинга агрегации/PE/BRAS
- Похоже на CP, нет отчетов по внешнему BGP-пирингу

BUSINESS INTELLIGENCE (BI)

- HA для данных клиентов
- Расширение системы по объектам мониторинга

PEAKFLOW SP/TMS

В реальном времени: Измерение, Корреляция, Отчеты по трафику; Обнаружение и Подавление угроз

FLOW данные

SRC, DST, PORT, PROTOCOL, ...

ROUTING данные

BGP, SNMP, TOPOLOGY, CONNECTIVITY

Пакеты

OFF/ON-RAMPING, PORT-MIRROR, INLINE

Компоненты решения Peakflow SP

Arbor Peakflow SP CP

Модели: CP-5500-5, CP5500-2, CP5500-0

Collector Platform (CP) используется для получения информации от пиринговых и магистральных маршрутизаторов, а так же для подключения TMS и FS

Arbor Peakflow SP TMS

Модели: TMS-1200/2500/3000/4000

Threat Management System (TMS) – операторское решение для очистки трафика и визуализации сервисов

Arbor Peakflow SP FS

Модели: FS-5500-15, FS-5500-32

Flow Sensor (FS) предназначен для сбора информации с абонентских маршрутизаторов и используется для масштабирования решения

Arbor Peakflow SP BI

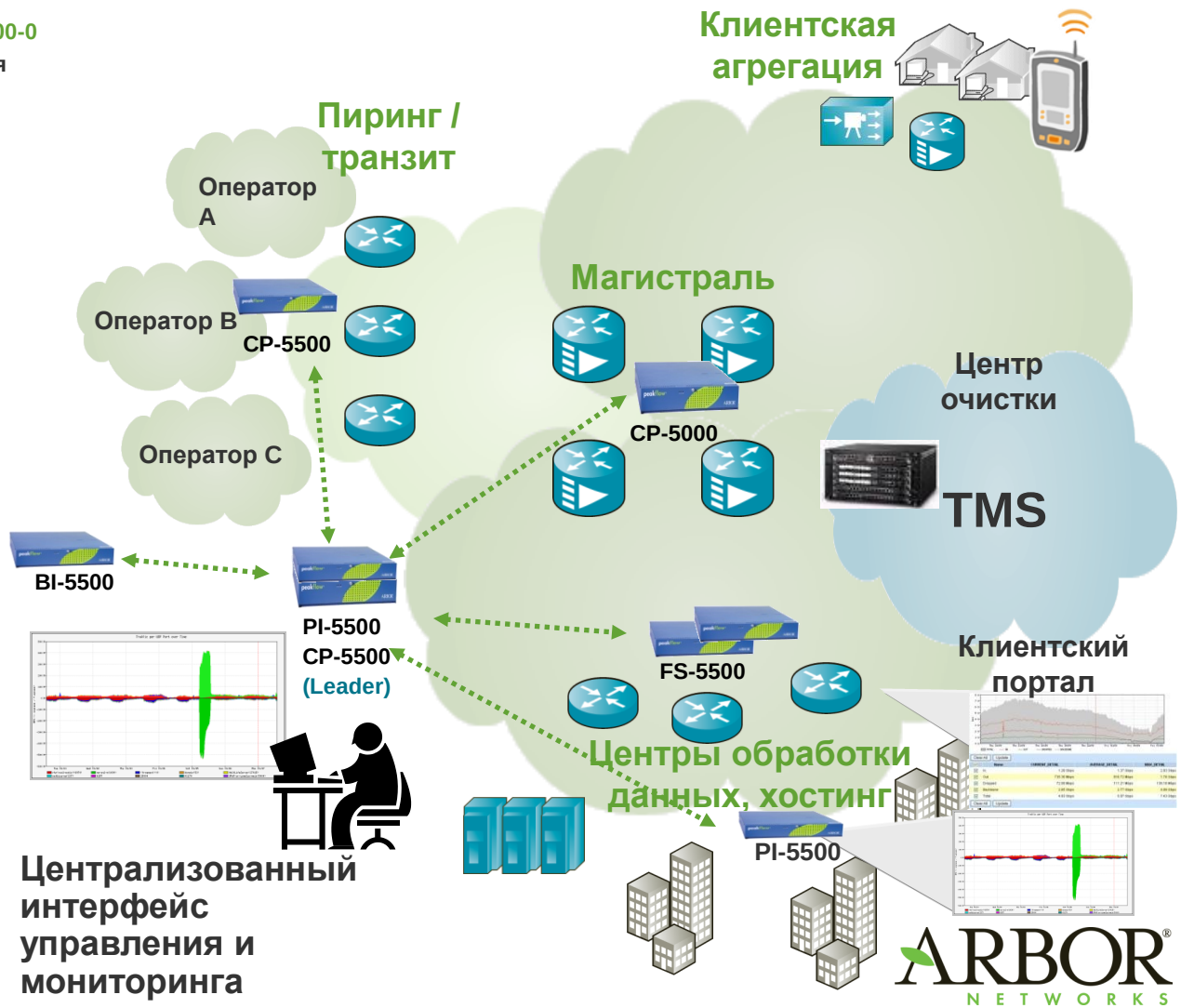
Модель: BI-5500-500

Business Intelligence (BI) увеличивает количество объектов мониторинга и обеспечивает отказоустойчивость хранения данных

Arbor Peakflow SP PI

Модель: PI-5500-25

Portal Interface (PI) увеличивает количество одновременных пользовательских сессий, а так же обеспечивает отказоустойчивость управления



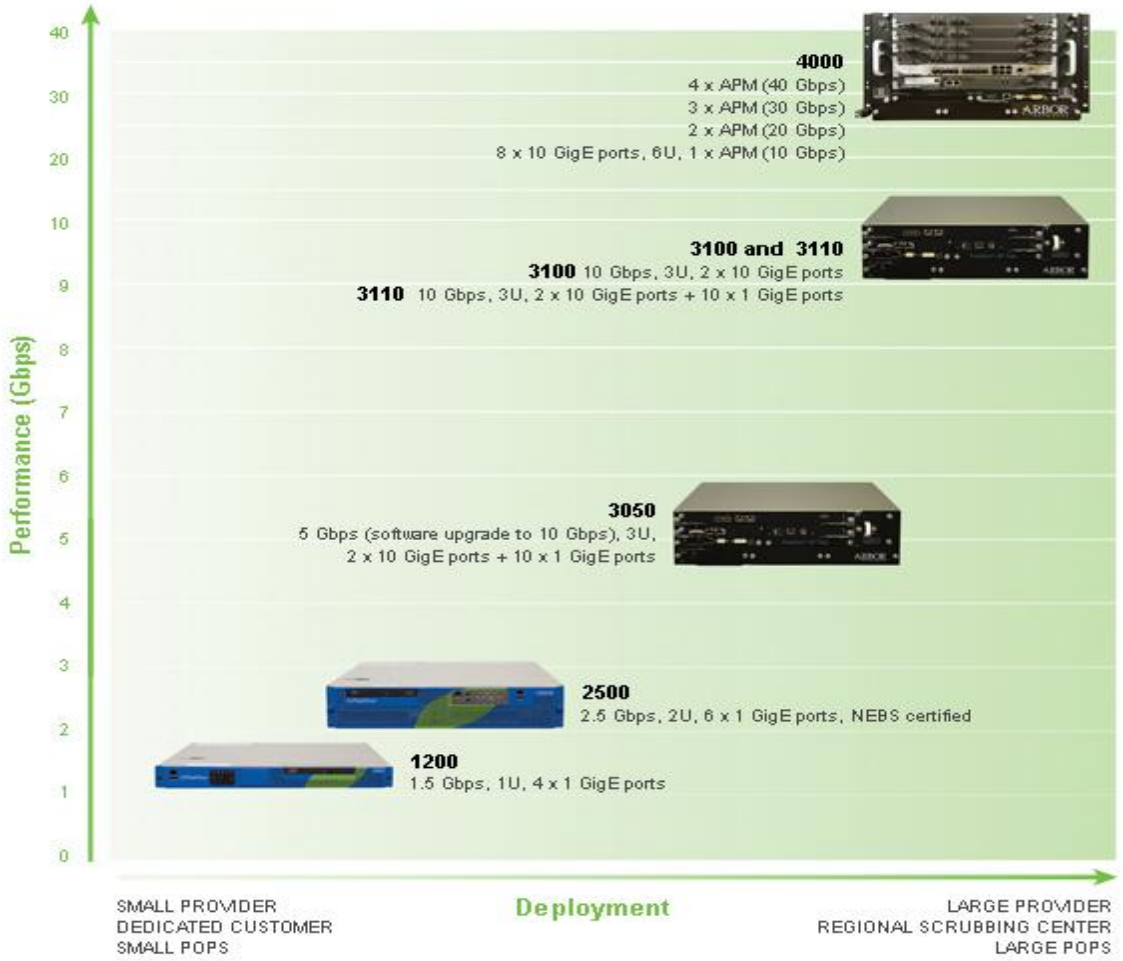
Широкая линейка устройств подавления атак

Peakflow TMS можно модернизировать при росте трафика

- Модельный ряд от 1.5 до 40 Гбит/с
- Наличие акций для замены

Все TMS управляются из единого интерфейса

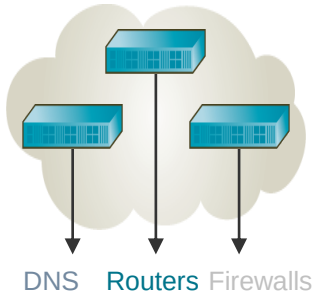
Единственное в отрасли решение с таким количеством опций



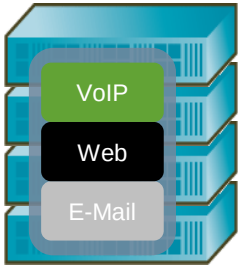
Arbor Peakflow SP: обеспечение доступности

Обеспечение доступности

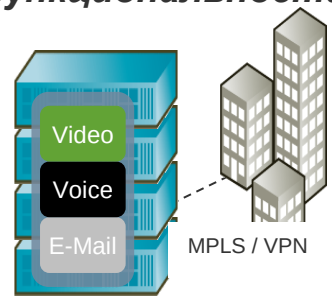
Защита инфраструктуры



Защита сервисов



Защита функциональности



Защита ресурсов

Визуализация инфраструктуры

Выявление и защита от атак на каналы связи и инфраструктуру. Блокировка плохих пакетов

Визуализация сервисов

Выявление и защита от атак направленных на важные приложения

Визуализация производительности

Отслеживание ключевых индикаторов производительности

Визуализация ресурсов

Оптимизация маршрутов трафика, транзитных и пиринговых взаимоотношений

Визуализация сети и сервисов

Основа обеспечения доступности

ARBOR NETWORKS

Pravail Security Analytics

Обнаружение и расследование атак

ARBOR® NETWORKS

Обзор решения Pravail SA

Решения Pravail SA используют наиболее полный источник информации – пакет со всеми заголовками и содержимым

- Уникальный интерфейс
  - Очень удобная визуализация событий
  - Анализ данных в режиме реального времени или исторических данных
- Масштабируемость
  - Легко работает с годами данных или терабайтами информации
  - Расследуйте инциденты на временной шкале от годов до минут

Это CCTV для вашей сети – проигрывайте, ставьте на паузу или делайте перемотку назад ваших данных

Мы видим то, что не видят другие

ARBOR NETWORKS

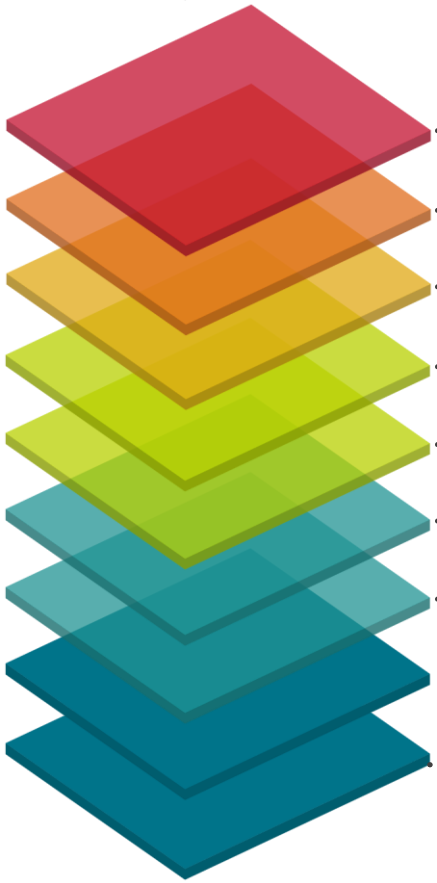
Pravail SA отвечает на ваши вопросы!

- *“Как я могу проверить насколько насколько совершенны наши системы безопасности и как убедить в этом CIO или президента компании?”*
- *“Меня тревожит - нас могли атаковать и мы об этом не знаем”*
- *“Я хотел бы знать, если нас начнут слишком часто атаковать”*
- *“Хороших аналитиков по сетевой безопасности тяжело найти и ещё сложнее удержать”*
- *“Все эти средства безопасности сложны и трудно внедряемы. Работа системы зависит от конфигурации оборудования и от уровня специалистов, настраивающих её”*
- *“Мы потратили уйму времени на внедрение различных решений по безопасности и нас до сих взламывают. Как можно быстро понять ситуацию?”*
- *“Возможно нас и атаковали, но мы незнаем этого точно, у нас нет достаточной информации, чтобы проверить это”*

ARBOR NETWORKS

Полнейшая видимость атак

10 Full view of attack



Machine Learning

Files

Sessions

Packets

Flow

9 Frame by frame

8 Protocol attributes

7 Use attack intelligence sources

6 Packet capture

5 Once alert is triggered

4 ArborFlow Detection

3 Who is coming in

2 Shows who and what to where

1 Raw Netflow

UNDERSTAND

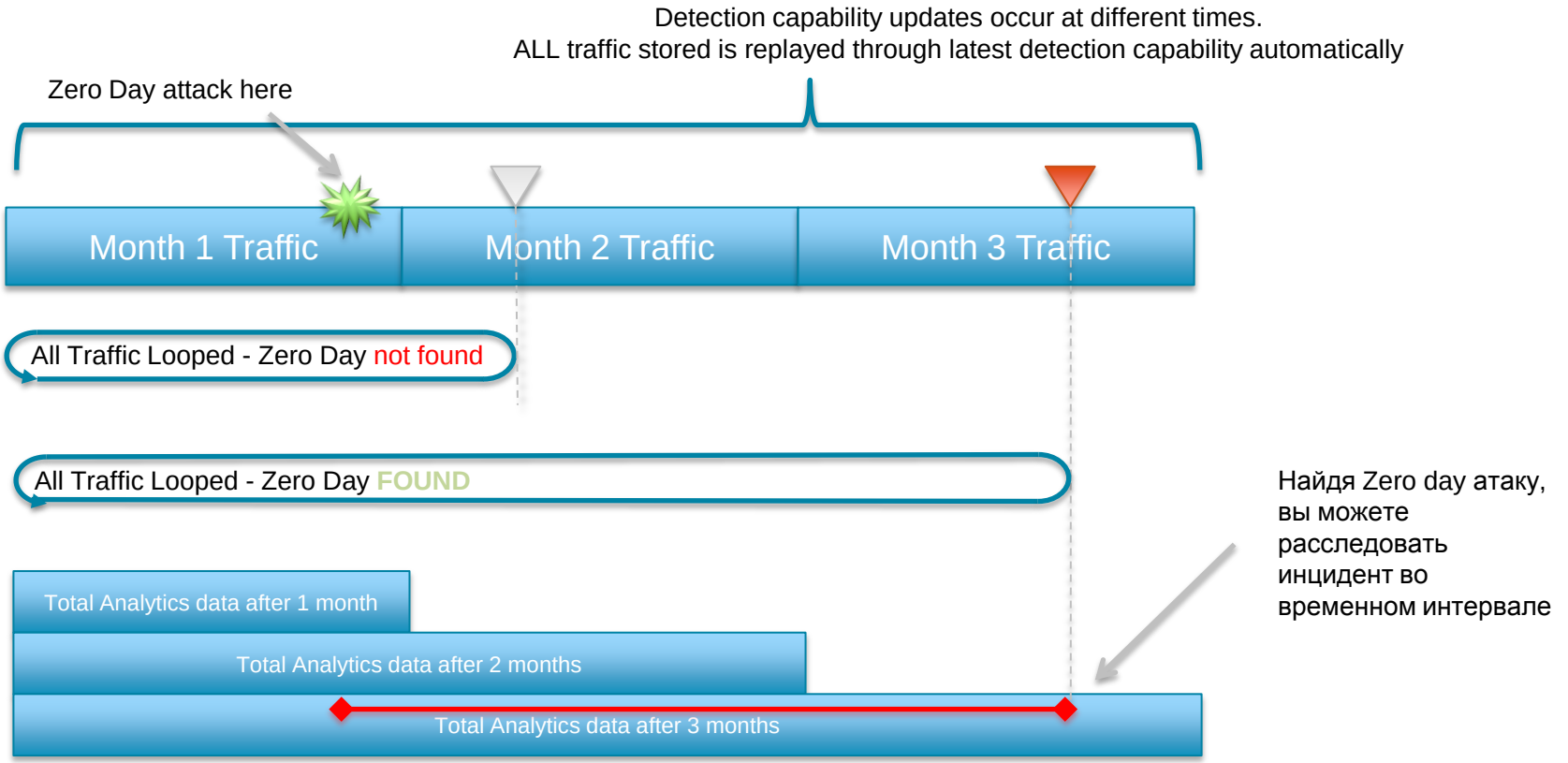
IDENTIFY

ARBOR NETWORKS

Алгоритм работы - Обнаружение Zero Day Attacks

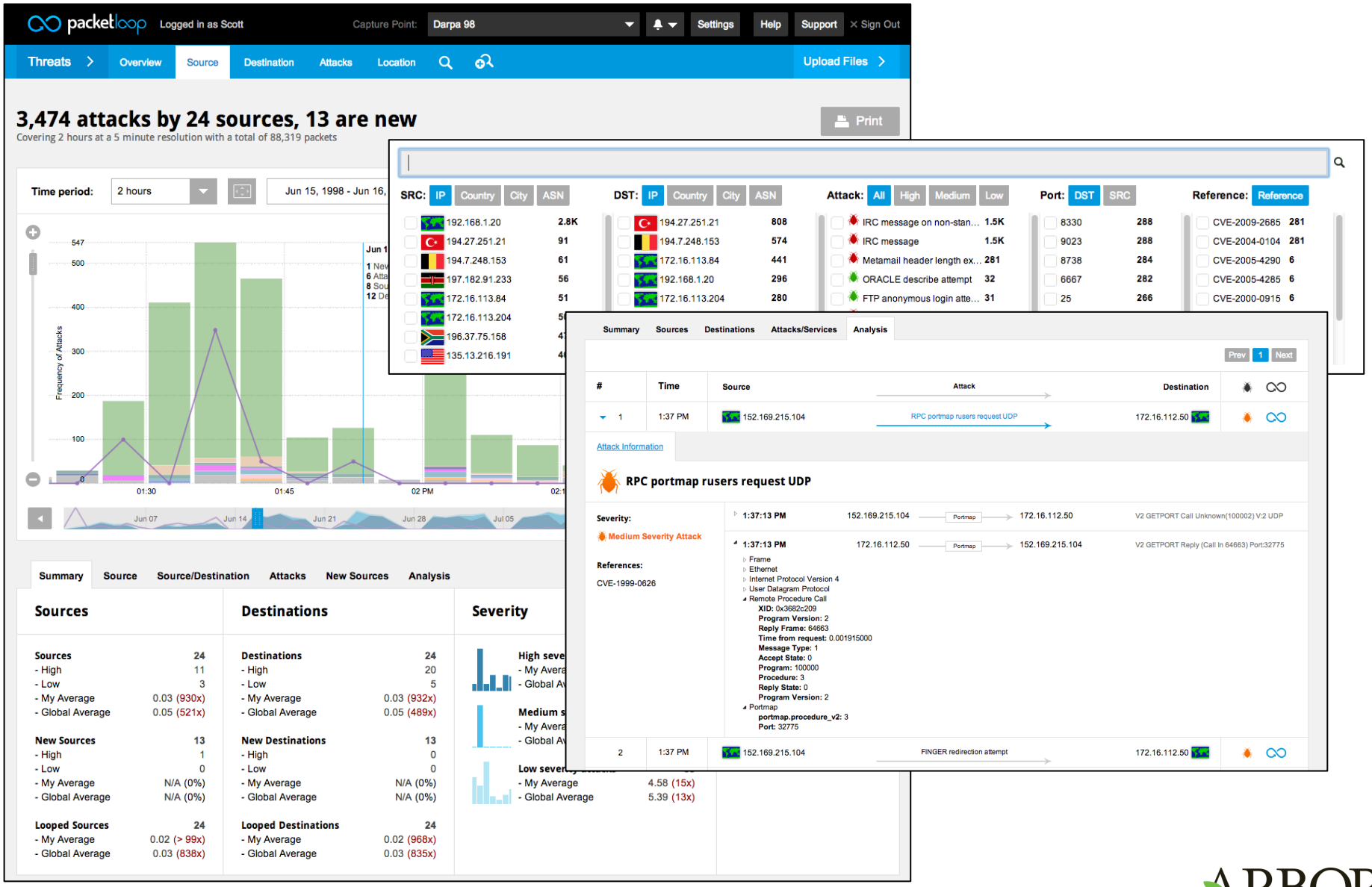
Сигнатуры детектирования атак без искомой Zero Day атаки

Сигнатуры детектирования атак включая сигнатуру для Zero Day атаки



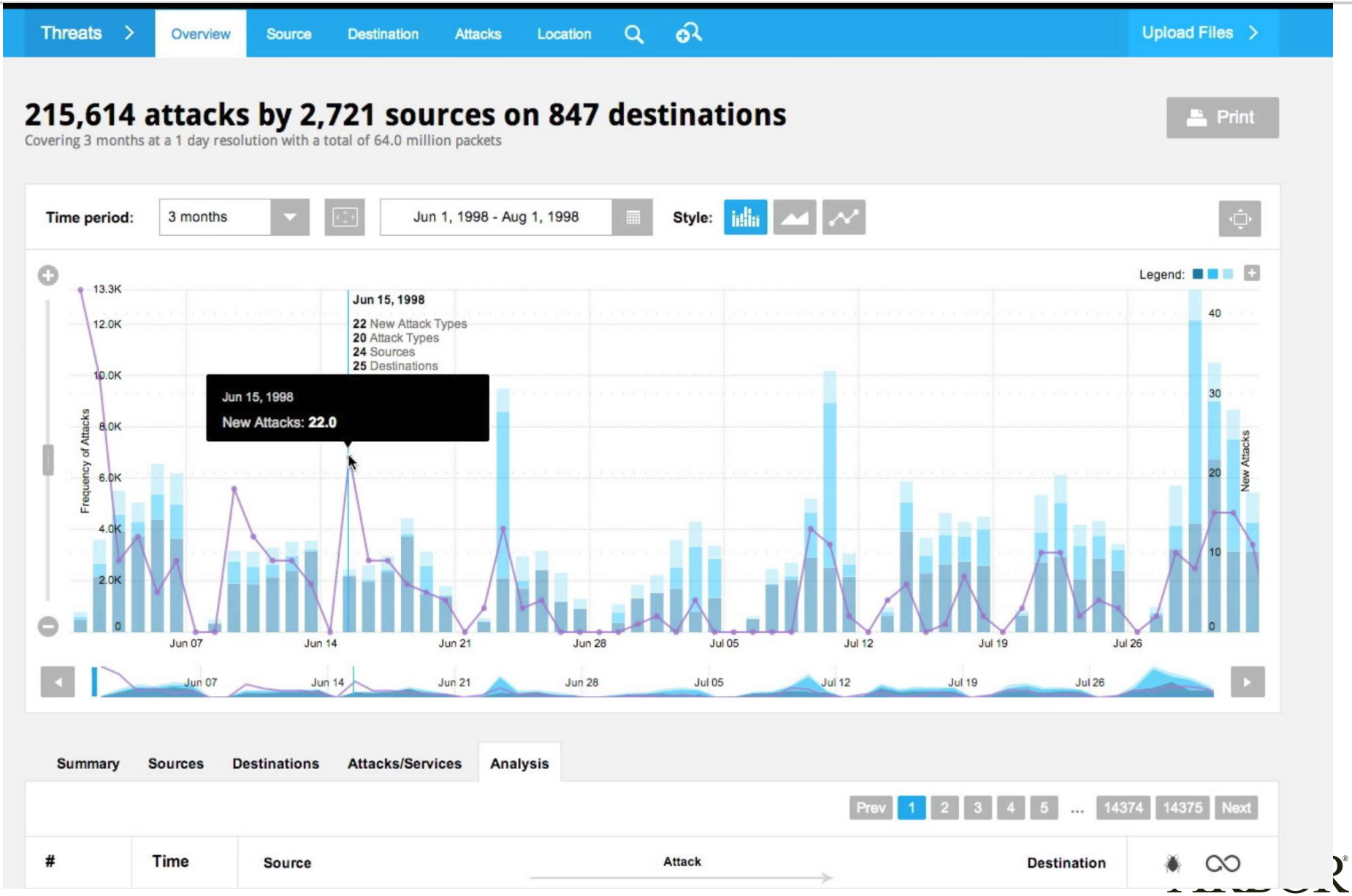
ARBOR NETWORKS

Удобнейшая визуализация данных

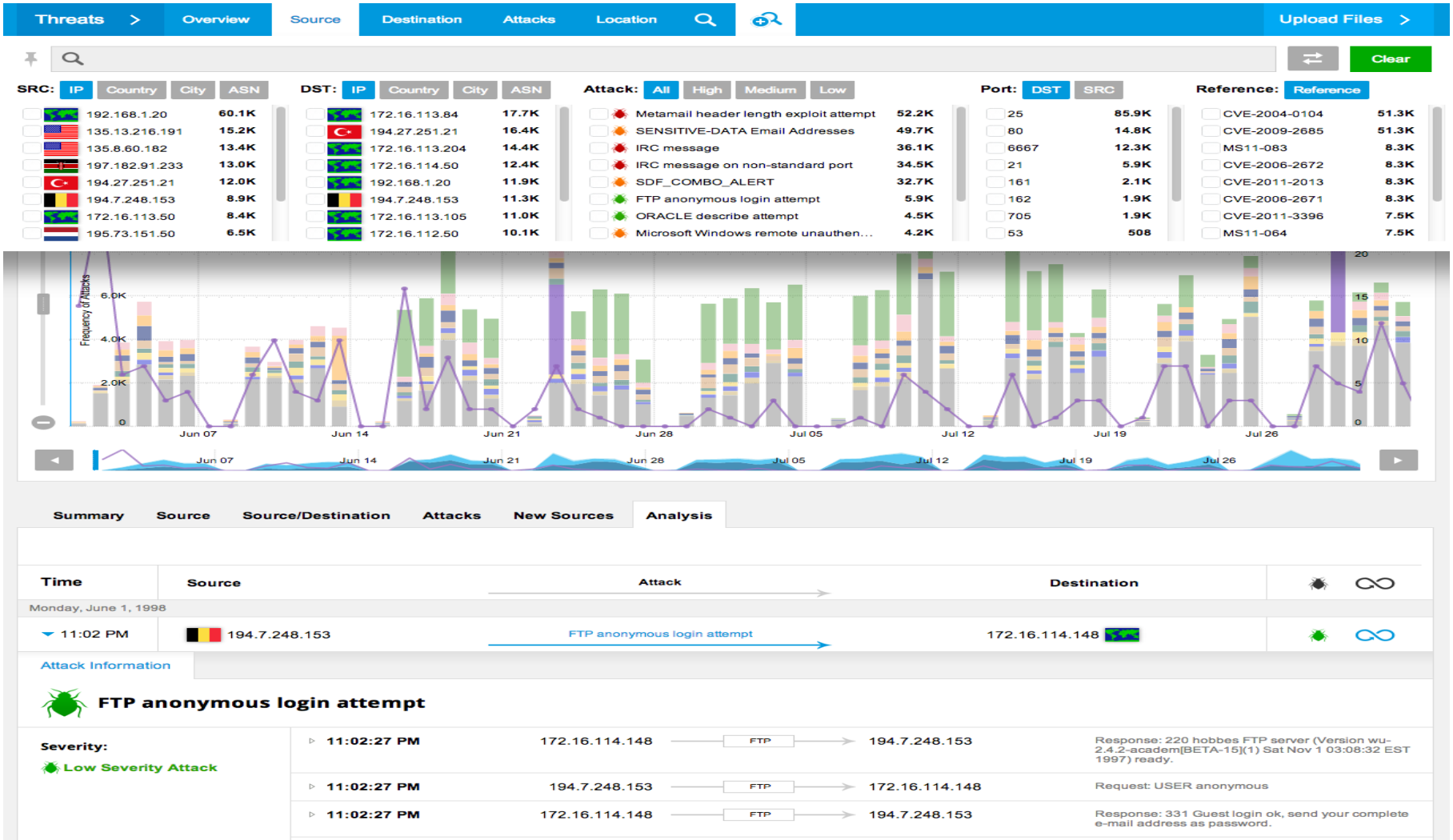


ARBOR NETWORKS

Удобнейшая визуализация данных

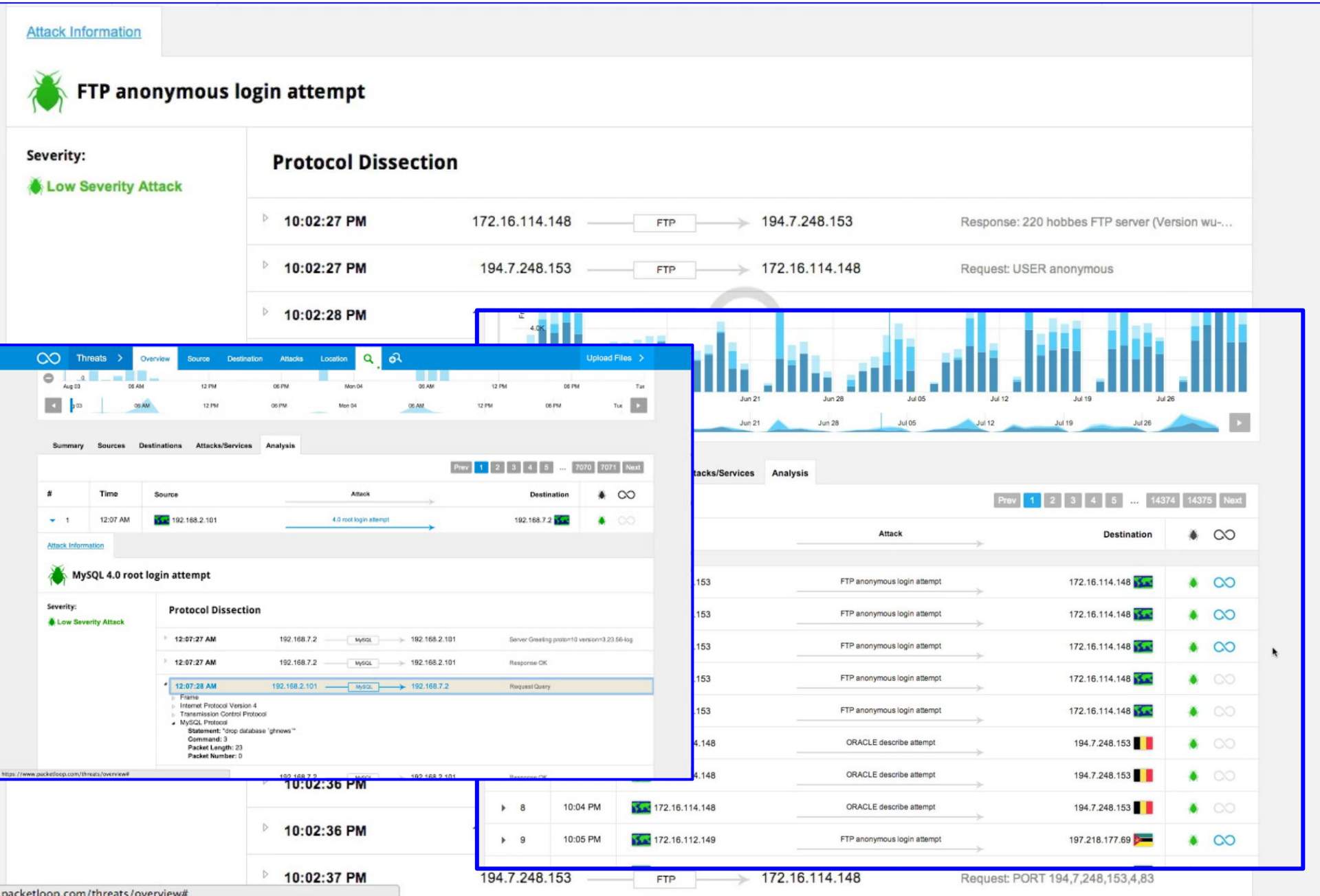


Удобнейшая визуализация данных

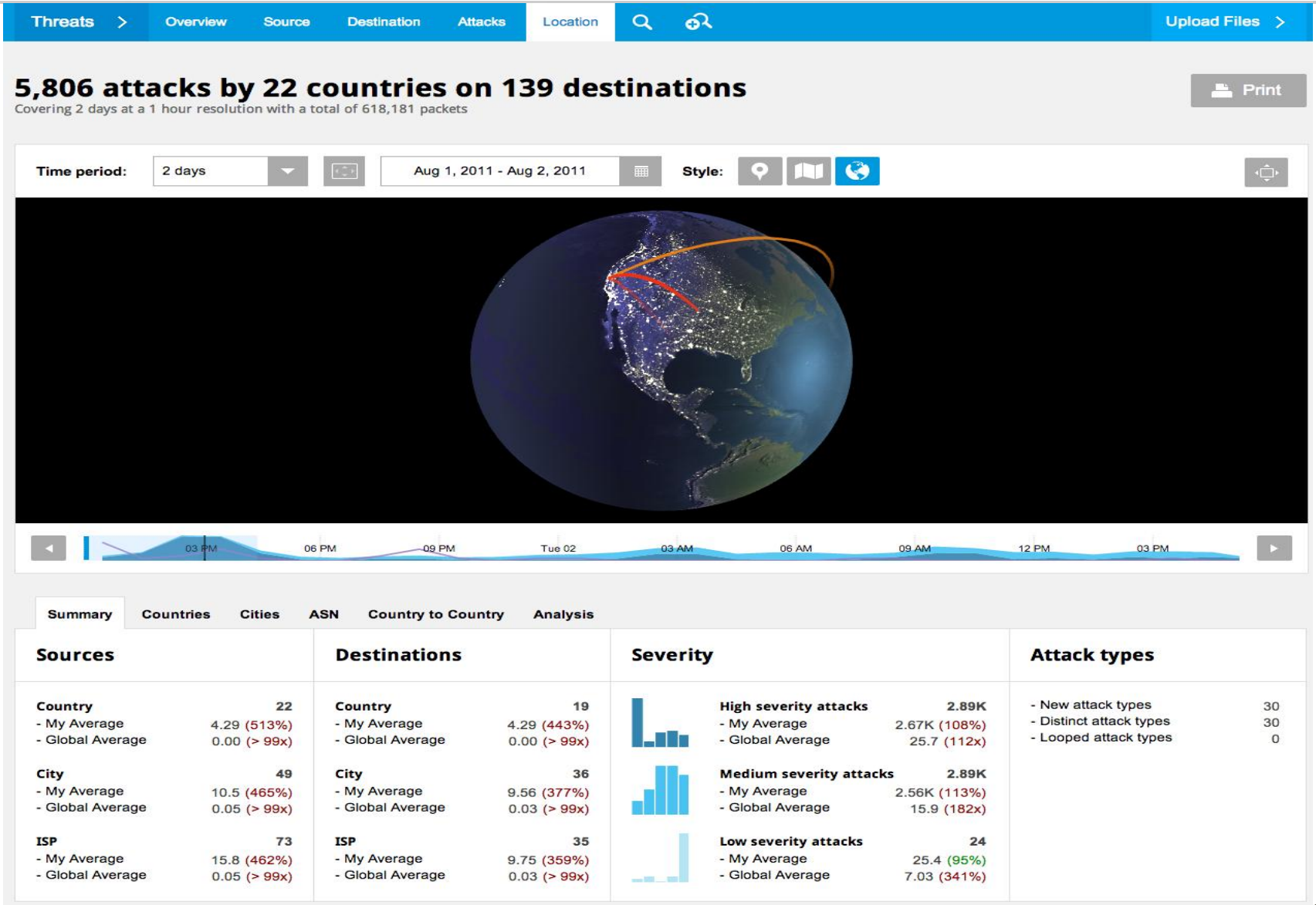


ARBOR NETWORKS

Удобнейшая визуализация данных



Удобнейшая визуализация данных



Обзор решения Pravail SA

- Все данные сохраняются, анализируются и визуализируются локально
- Требуется минимально один контроллер для аналитики и один или более коллектор для захвата трафика в нескольких сетевых точек
- Аналитика и метрики отправляются на контроллер для визуализации и анализа
- Предоставляется отчёт в реальном времени и в историческом разрезе
- Требуется подключение к интернет для получения апдейтов
- Также планируется к выпуску на базе Oracle Big Data Appliance (BDA)

Pravail SA Appliances – Controller

Pravail SA Controller это устройство, хранящее данные после анализа и предоставляющую доступ к ним через интерфейс пользователя. Это первый компонент системы.

Базовые модели	**6115 (2RU)**	6132 (2RU) **(В РАЗРАБОТКЕ)**	6164 (3RU) **(В РАЗРАБОТКЕ)**
Парт-номер	PRA-SA-6115	PRA-SA-6132	PRA-SA-6164
Стоимость (list)	from $95,200	TBE	TBE
Память (Raw)	15TB	32TB	64TB
Интерфейсы	1 (1 or 10Gbps)	1 (1 or 10Gbps)	1 (1 or 10Gbps)

- Базовые модели включают интерфейс 1Gbps медь. Другие доступные интерфейсы:
  FS – 1Gbps Fiber (Short Range) FL– 1Gbps Fiber (Long Range)
  SS – 10Gbps Fiber (Short Range) SL – 10Gbps Fiber (Long Range)
- Поддержка M&S 19% от листовой стоимости. Подписка AIF до 10% от листовой стоимости.

ARBOR NETWORKS

Pravail SA Appliances – Collector

Pravail SA Collector это устройство для сбора, хранения и обработки пакетов. Доступный объём хранения повышается путём добавления устройств в кластер.

Базовые модели	6015 (2RU)	6032 (2RU)	6064 (3RU)
Парт-номер	PRA-SA-6015	PRA-SA-6032	PRA-SA-6064
Цена (list)	от $122,400	TBE	TBE
Память (Raw)	15TB	32TB	64TB
Интерфейсы	1 (1 or 10Gbps)	1 (1 or 10Gbps)	1 (1 or 10Gbps)

- Базовые модели включают интерфейс 1Gbps медь. Другие доступные интерфейсы:
  FS – 1Gbps Fiber (Short Range) FL– 1Gbps Fiber (Long Range)
  SS – 10Gbps Fiber (Short Range) SL – 10Gbps Fiber (Long Range)
- Поддержка M&S 19% от листовой стоимости. Подписка AIF до 10% от листовой стоимости.

ARBOR NETWORKS

Расчёт решения

Storage (Total Required Nodes) = Network Link Size x Avg Utilisation x Retention Period

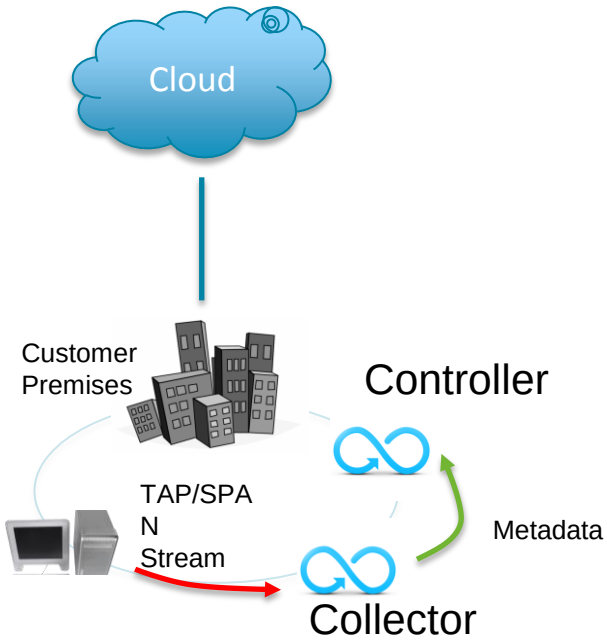
Appliance Sizing Calculator

Network Link Size	1	Gbps
Avg Utilisation (over 24 hrs)	30%	
Daily Capture Req.	3240	GB
Retention Days	15	

ARBOR NETWORKS

Пример решения №1 (небольшая компания)

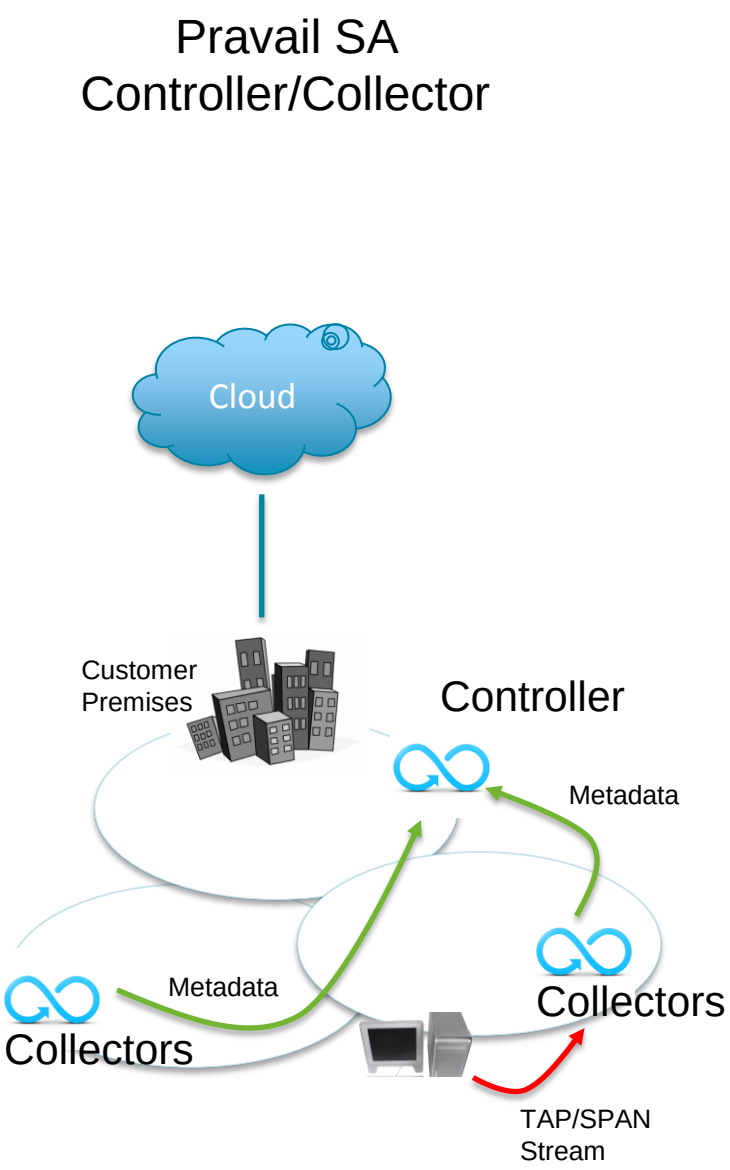
Pravail SA
Controller/Collector



Описание	
Сценарий	Внедряется локальная система из двух компонент –контроллер и коллектор
Компоненты решения	6115 Controller (PRA-SA-6115) 6064 Collector (PRA-SA-6064-FS)
Цена	От 217,800$ по прайс-листу

ARBOR NETWORKS

Пример решения №2 (большая компания)



Описание	
Сценарий	Внедряется решение в 5 основных офисах и 5 дополнительных офисах (3 офиса подключены по 1Gbps и 2 по 500Mbps). Требуется единая отчётность по всей системе безопасности компании.
Компоненты решения	6115 Controller (PRA-SA-6115) 6064 Collector (PRA-SA-6064) 6032 Collector (PRA-SA-6032)
Цена	1 x (PRA-SA-6115-FS) 4 x (PRA-SA-6064) 2 x (PRA-SA-6032) Цена от 1.5M$ по прайс-листу

ARBOR NETWORKS

Кратко о Pravail Security Analytics (SA)

Arbor Pravail SA это уникальное и совершенное решение для анализа безопасности вашей сети, которое позволяет использовать самую полную информацию (полная запись пакетов) о вашей сети с различных точек в режиме реального времени или анализировать историю событий для обеспечения контроля эффективности систем сетевой безопасности. Продвинутая аналитика позволяет анализировать данные во временном разрезе для обнаружения реального времени атаки (в том числе и ранее неизвестных атак), адаптировать систему безопасности и предотвратить атаки в дальнейшем.

ARBOR NETWORKS

Кратко о решении

Arbor Networks Pravail SA (Packetloop)

- ✓ **Решение позволяющее однозначно ответить на ваши вопросы**
- ✓ **Способно обнаруживать атаки в реальном времени и выявлять атаки в историческом разрезе**
- ✓ **Просто настраивается и не требует интеграции с другими устройствами безопасности**
- ✓ **Бесподобная визуализация данных – забудьте о табличках или гистограммах**
- ✓ **Решение работающее с первых же секунд**
- ✓ **Возможность сравнивать свои данные с глобальными атаками**

Видео как работает решение:
http://vimeo.com/user6890858/videos

ARBOR NETWORKS

Arbor Cloud

Обеспечение доступности – облачный сервис для заказчиков имеющих оборудование Arbor Networks

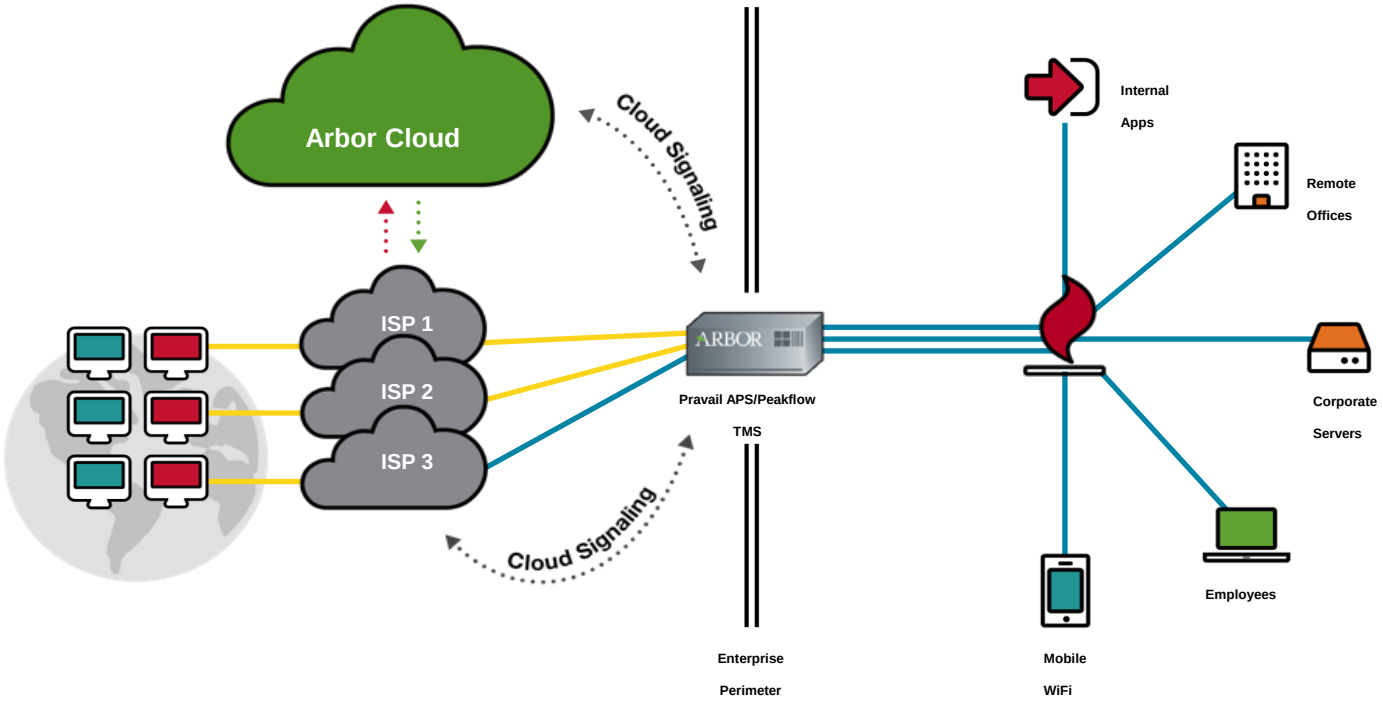
ARBOR® NETWORKS

Arbor Cloud многоуровневая защита от DDoS

Блокирование сложных DDOS атак

Контроль сетевой безопасности

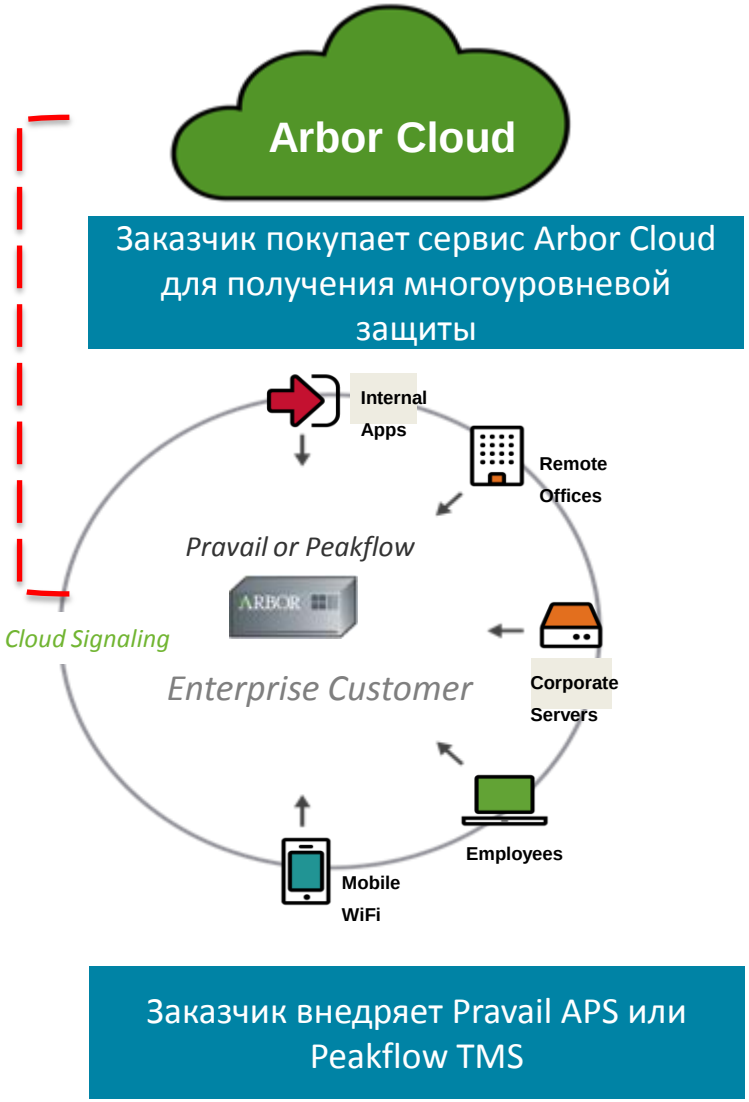
Защита от глобальных угроз



ARBOR NETWORKS

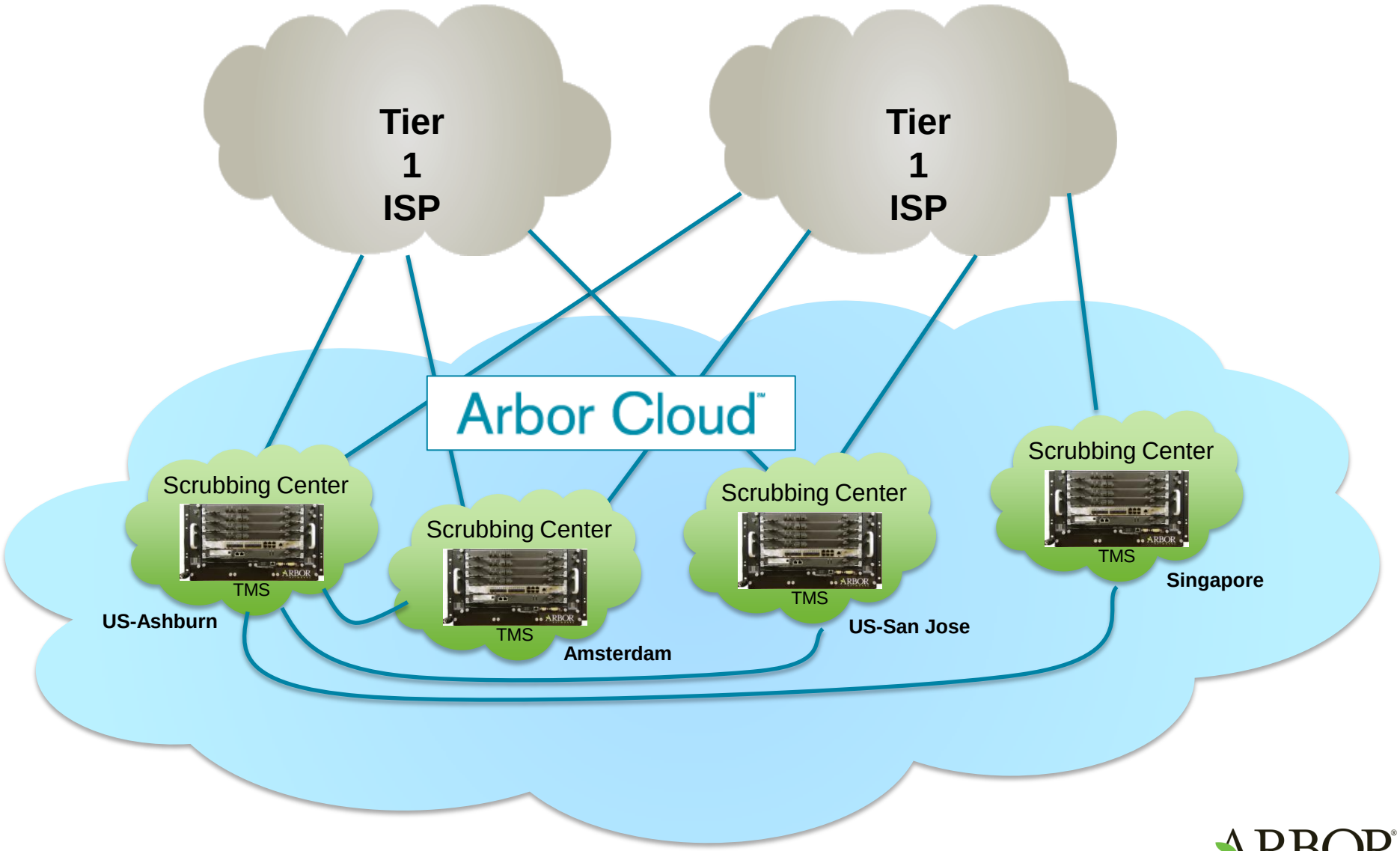
Arbor Cloud: защита от DDoS по требованию

- *280G+* очистной способности
- 4 центра очистки трафика
- BGP или DNS редирект трафика
- Поддержка SSL
- Подписка на сервис исходит из **чистого трафика** компании, а не всего



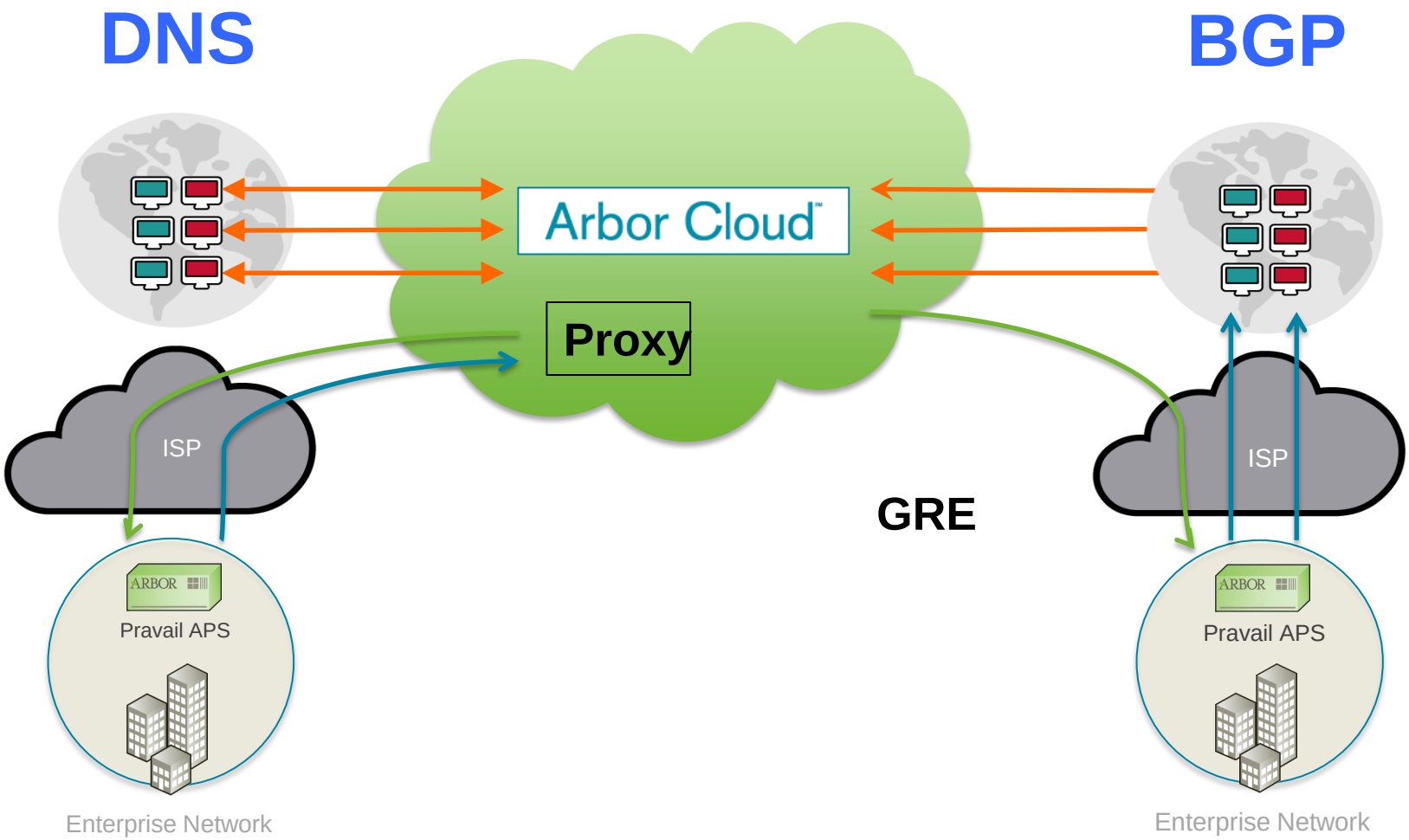
ARBOR NETWORKS

Arbor Cloud глобальная сеть очистки

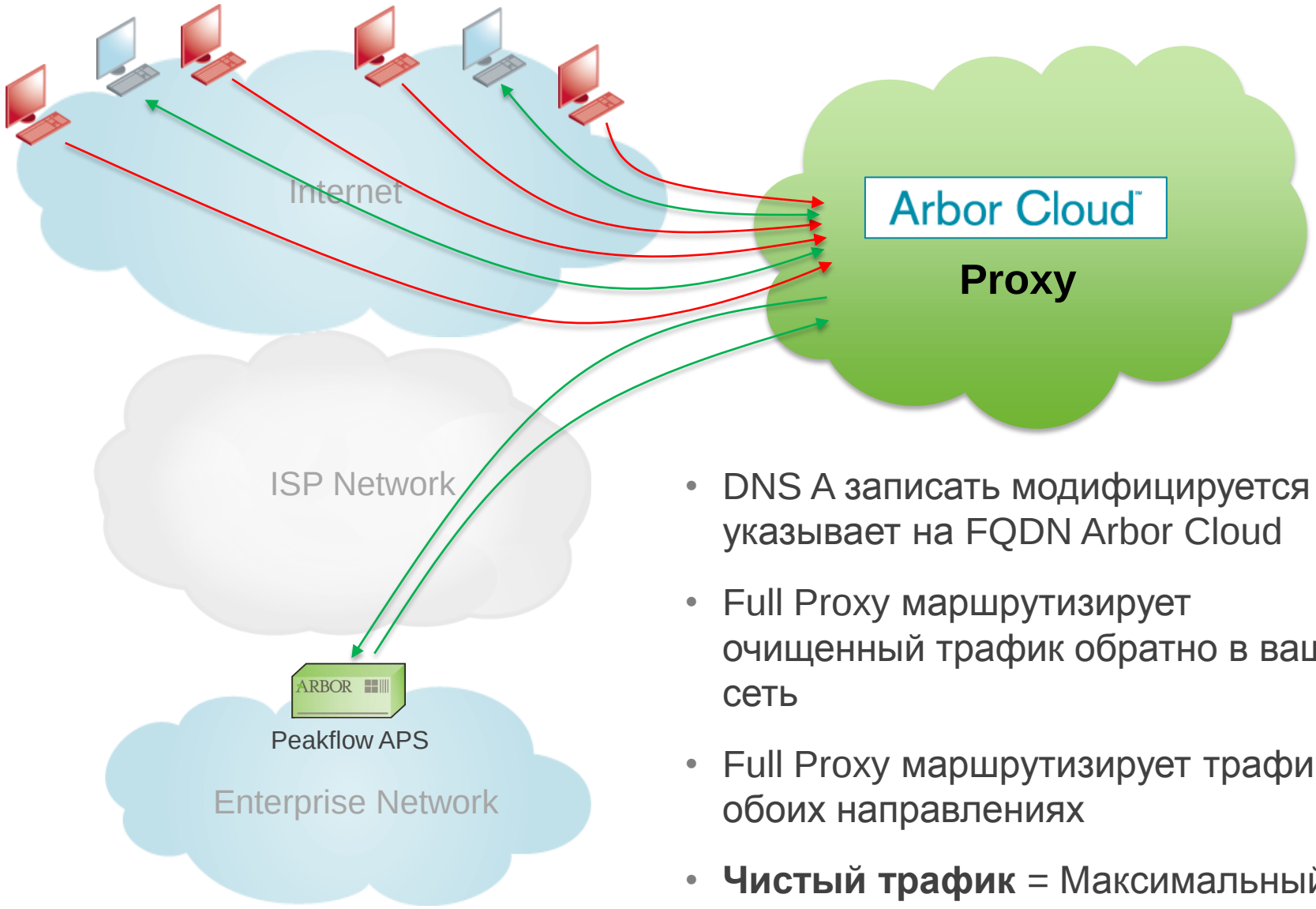


ARBOR NETWORKS

Опции редиректа трафика: BGP или DNS

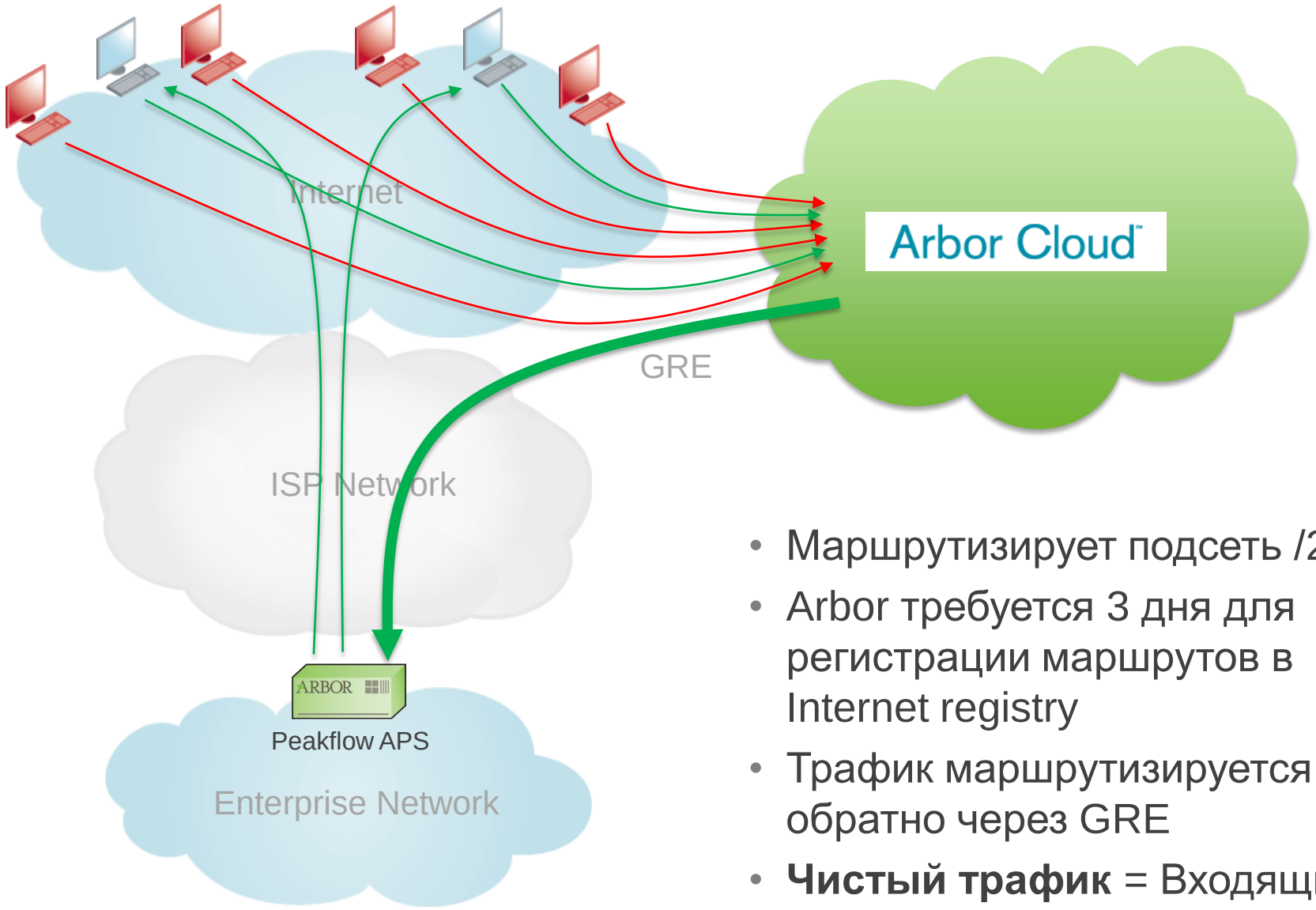


DNS редирект



- DNS A записать модифицируется и указывает на FQDN Arbor Cloud
- Full Proxy маршрутизирует очищенный трафик обратно в вашу сеть
- Full Proxy маршрутизирует трафик в обоих направлениях
- **Чистый трафик** = Максимальный трафик исходящий или входящий

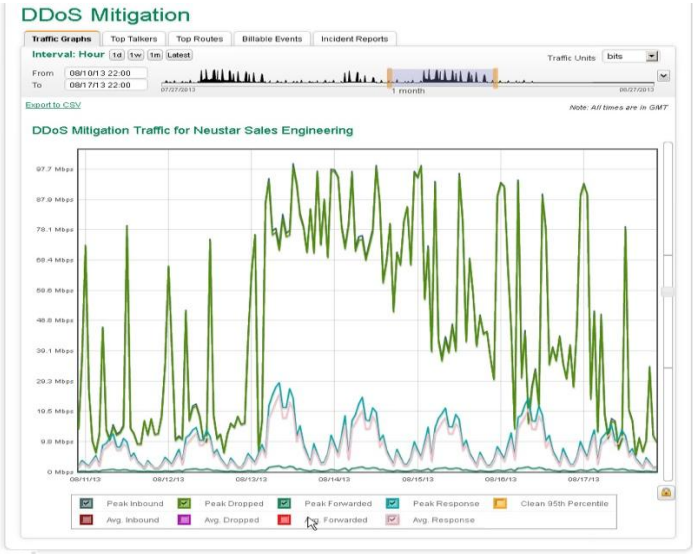
BGP редирект

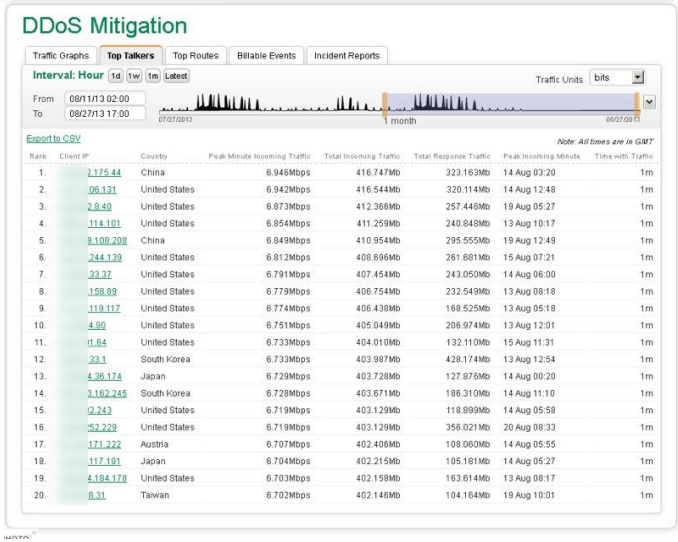


- Маршрутизирует подсеть /24
- Arbor требуется 3 дня для регистрации маршрутов в Internet registry
- Трафик маршрутизируется обратно через GRE
- **Чистый трафик** = Входящий трафик

Отчёт о предоставленном сервисе

- **Подробная информация о:**
  - Traffic Graphs,
  - Top Talkers (IP)
  - Top Routes
  - Billable Events
  - Incident Reports
    - Подготовка отчетов о атаке
- **Статистика о:**
  - Собирается со всех центров очистки
  - Хранится 90 дней





ARBOR NETWORKS

Отчёты о атаке – DNS

- **Во время атаки вы получаете ежечасные отчёты по почте**

Below is a summary of the traffic related to your Neustar DDoS Mitigation service for account Customer XXXXX. The following DDoS Mitigation traffic was seen from 08/19/2013 14:00 to 08/22/2013 14:00 UTC.

Traffic Type	1-Hour Peak Minute	1-Hour Peak Traffic	1-Hour Average Traffic	72-Hour Peak Minute	72-Hour Peak Traffic	72-Hour Average Traffic
Total Inbound	08/22/2013 13:00 UTC	0.000 Kbps	0.000 Kbps	08/19/2013 14:13 UTC	4.199 Mbps	1.919 Mbps
Dirty	08/22/2013 13:00 UTC	0.000 Kbps	0.000 Kbps	08/19/2013 14:09 UTC	214.000 Kbps	36.451 Kbps
Clean Forwarded	08/22/2013 13:00 UTC	0.000 Kbps	0.000 Kbps	08/19/2013 14:13 UTC	4.129 Mbps	1.884 Mbps
Clean Response	08/22/2013 13:00 UTC	0.000 Kbps	0.000 Kbps	08/19/2013 19:55 UTC	17.265 Mbps	6.664 Mbps

Clean Traffic 95th Percentile : 8.562 Mbps (Past 72 Hours)

Отчёты о атаках

- **Отчёты после атаки включают в себя информацию как автоматически сгенерированную так и дополненную нашими специалистами**

Event Summary information	
Event Start:	06/23/2012 – 12:00 am (EST)
Event End:	06/26/2012 – 12:00 pm (EST)
Attack Type:	HTTP GET Flood (Example Attack Vector)
Destination:	www.example.com
Sources:	Multiple sources, though most attack traffic originated from (Country).

Executive Summary

(Company Name) activated Neustar SiteProtect at 12:00 am (EST) on 06/23/2012, in preparation for a credible DDoS attack threat from Anonymous.

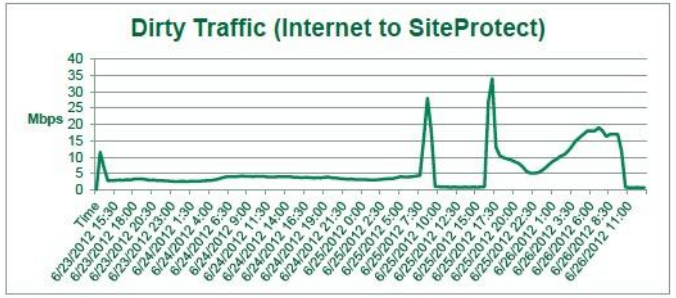
The attack was announced to start at 4:00 am (EST) on 06/23/2012; however, some DDoS activity was already on-going when Neustar SiteProtect was enabled.

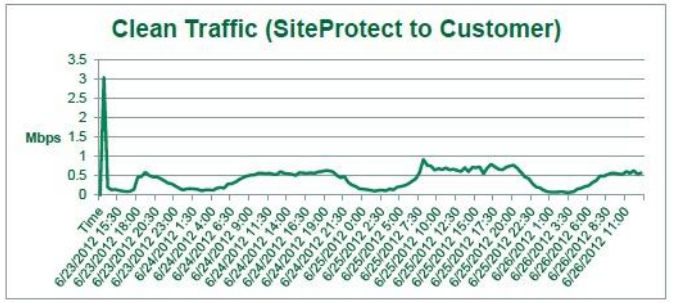
Initially, the Neustar Security Operations Center observed attack traffic of around (#) Mbps, peaking at (#) Mbps on 06/25/2012 between 10 am and 12:00 pm (EST). The HTTP GET Flood was fully mitigated, and the Neustar SiteProtect service was kept enabled until 12:00pm on 06/26/2012 as a precaution.

The Neustar SOC monitored well known cyber gang blogs and chat rooms during the attack.

Mitigation Activities	
Connection Rate Limiting	Rate limit settings (if applicable)
Bandwidth Throttling	None
Blocked Referrers	Sample Referrer Blocks
String Filters	Sample Block Strings
UserAgent Filters	Sample UserAgent Filters

Traffic Graphs





ARBOR NETWORKS

SLA для сервиса Arbor Cloud

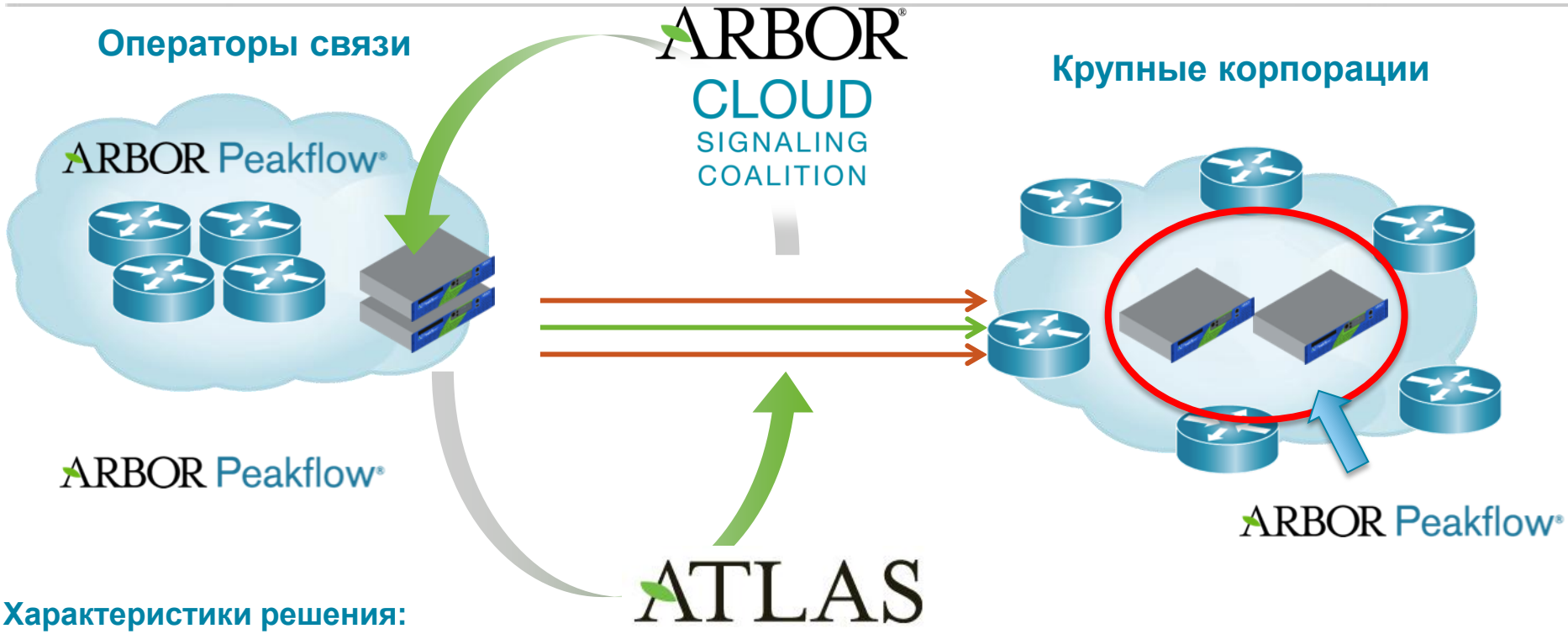
SLA Area	Contracted
Arbor Cloud Platform Availability	100% Monthly Availability (99.999% ≥1 scrubbing centers scrubbing customer traffic)
Standard Setup (Initial) • Completion of Provisioning Call • Final Configuration Submission by Customer • Applies once Final Configuration is provided	≤72hrs (DNS Redirection) ≤72hrs (BGP Redirection)
Standard Setup Updates	≤72hrs (DNS Redirection) ≤72hrs (BGP Redirection)
•Emergency Setup (Initial) • Additional Fees apply • Applies once Final Configuration is provided	≤4hrs (DNS Redirection Only)
•Emergency Setup Updates • Additional Fees apply	≤4hrs (DNS Redirection) ≤4hrs (BGP Redirection)
Time to Mitigate • From Time Customer Redirects Traffic to Neustar • Each Attack Vector Change Starts New Time to Mitigate • Mitigation equals ≤5% dirty traffic passed to customer	≤5min (Layer 3 & 4 Attacks) ≤15min (Layer 7 Attacks)

ARBOR NETWORKS

Краткий обзор решений

ARBOR®
NETWORKS

Решения Arbor – Pravail Peakflow для больших корпораций



Характеристики решения:

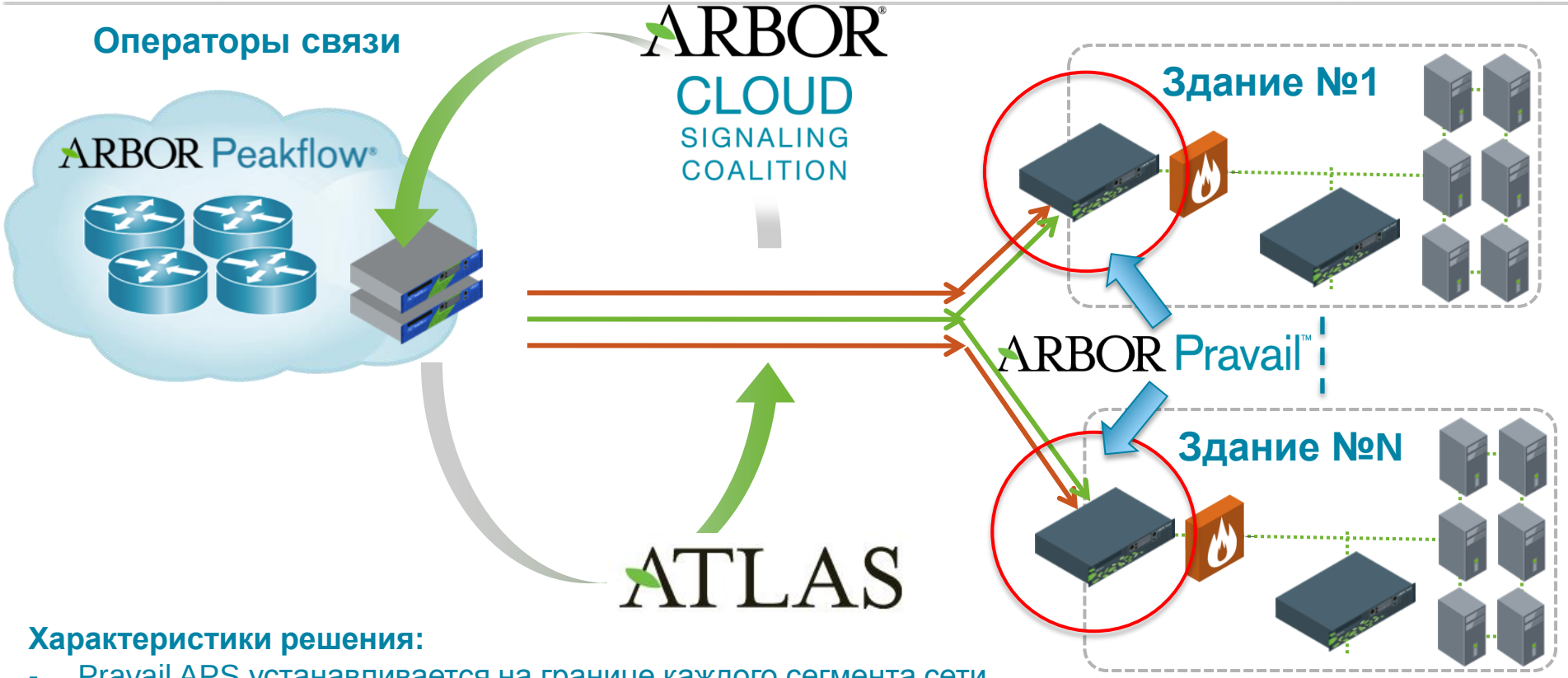
- Peakflow устанавливается во внутреннем периметре сети, внедрение может быть как централизованным, так и распределённым
- Гранулярная очистка **интересующего трафика, до 4Tbps**
- Мониторинг трафика с целью выявления сложных угроз
- Визуализация сети и пиринга компании
- Взаимодействие с системой ATLAS и получение новейших данных об угрозах

Стоимость решения: от 150k$

Кто использует: Крупнейшие мировые заказчики это финансовый сектор, государственные учреждения, нефтедобывающая промышленность, ритейлеры и прочие. Крупнейшие финансовые компании России используют Арбор для защиты своей сети.

ARBOR NETWORKS

Решения Arbor – Pravail APS для корпораций



Характеристики решения:

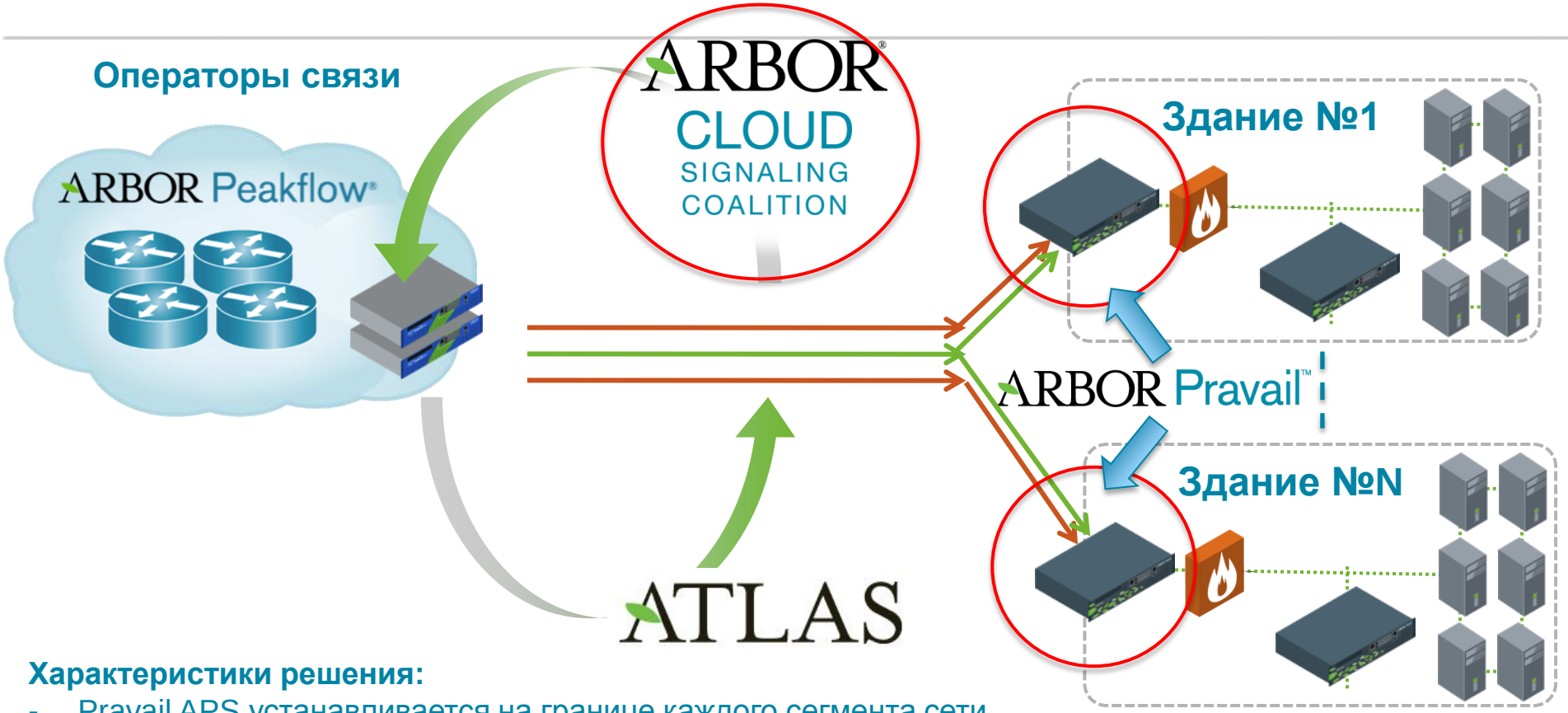
- Pravail APS устанавливается на границе каждого сегмента сети
- Пропускная способность оборудования варьируется от 500Mbps до 10Gbps
- Моментальная защита от атак
- Взаимодействие с системой ATLAS и получение новейших данных об угрозах, возможность использования Cloud Signalling

Стоимость решения: от 56k$

Кто использует в России: Система Pravail APS используется для защиты как крупнейших Российских банков так и для компаний среднего размера

ARBOR NETWORKS

Решения Arbor – Pravail APS + Arbor Cloud



Характеристики решения:

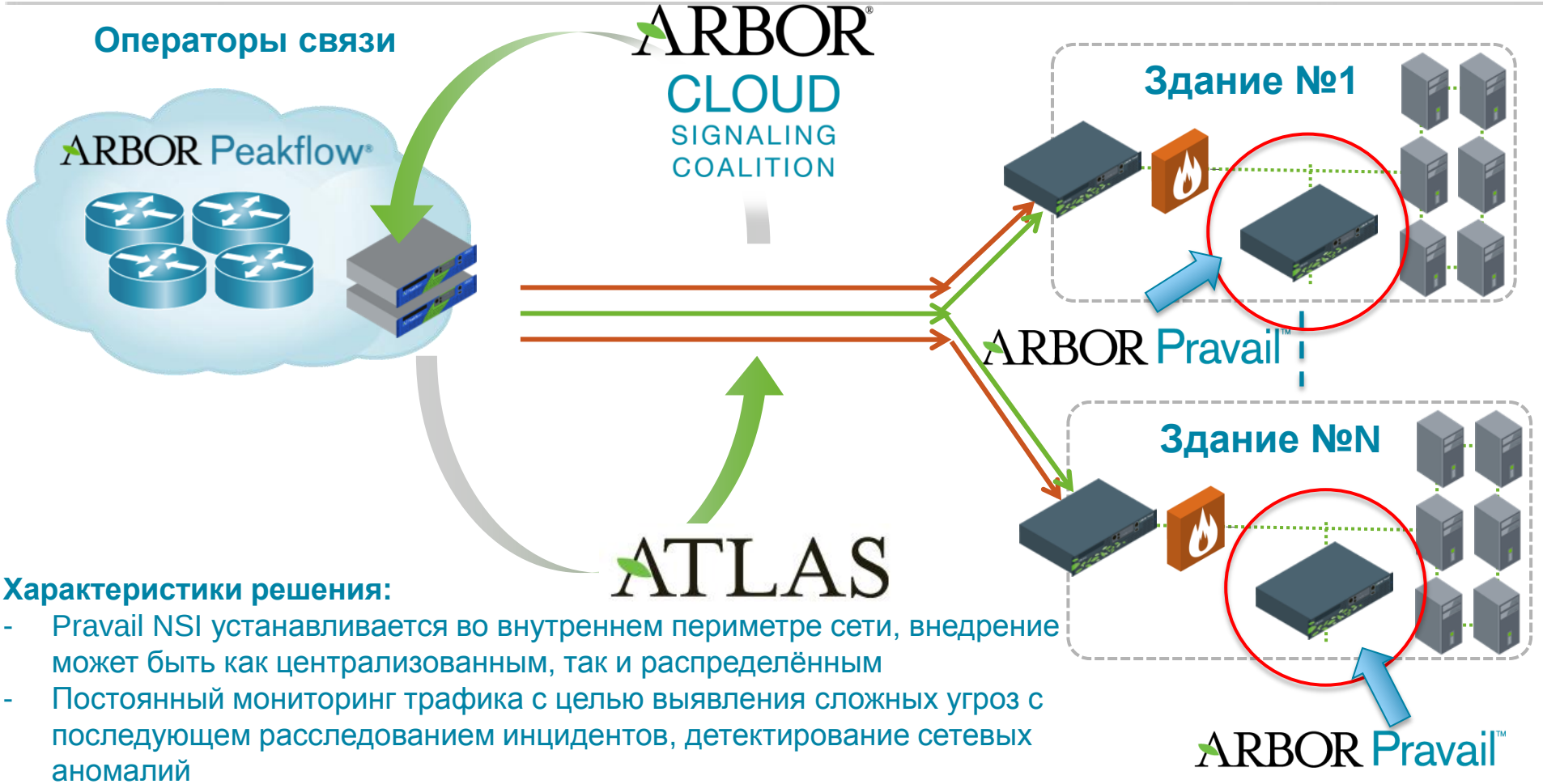
- Pravail APS устанавливается на границе каждого сегмента сети
- Пропускная способность оборудования варьируется от 500Mbps до 10Gbps
- Pravail APS работает в связке с Arbor Cloud для многоступенчатой очистки
- Моментальная защита от атак
- Взаимодействие с системой ATLAS и получение новейших данных об угрозах, возможность использования Cloud Signalling

Стоимость решения: от 77k$

Кто использует в России: Система Pravail APS используется для защиты как крупнейших Российских банков так и для компаний среднего размера

ARBOR NETWORKS

Решения Arbor – Pravail NSI для корпораций



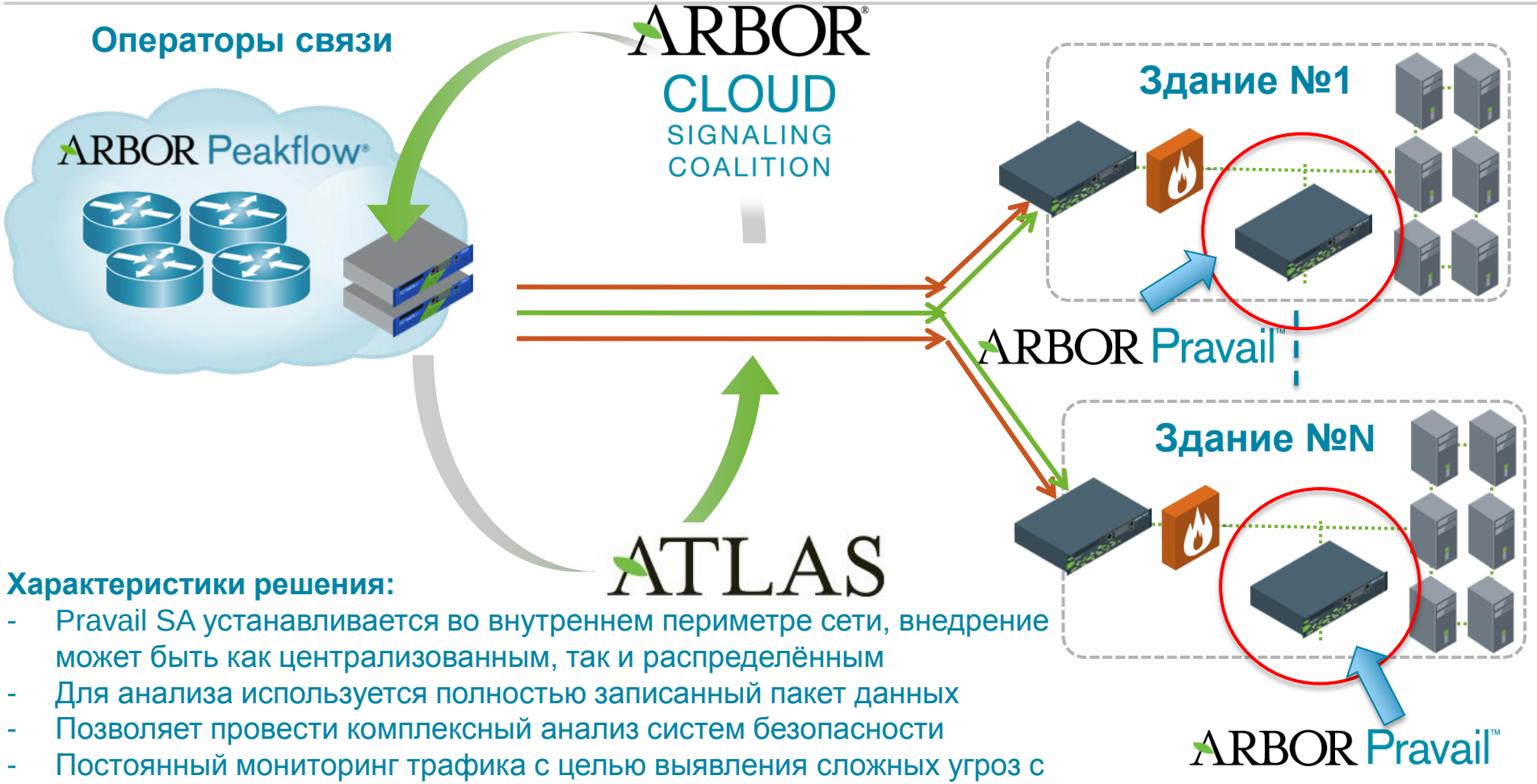
Характеристики решения:

- Pravail NSI устанавливается во внутреннем периметре сети, внедрение может быть как централизованным, так и распределённым
- Постоянный мониторинг трафика с целью выявления сложных угроз с последующем расследованием инцидентов, детектирование сетевых аномалий
- Интеграция с системами Pravail APS - централизованная отчётность и возможность блокирования вредоносного трафика на Pravail APS по команде Pravail NSI
- Взаимодействие с системой ATLAS и получение новейших данных об угрозах

Стоимость решения: от 62k$

ARBOR NETWORKS

Решения Arbor – Pravail SA для корпораций



Характеристики решения:

- Pravail SA устанавливается во внутреннем периметре сети, внедрение может быть как централизованным, так и распределённым
- Для анализа используется полностью записанный пакет данных
- Позволяет провести комплексный анализ систем безопасности
- Постоянный мониторинг трафика с целью выявления сложных угроз с последующем расследованием инцидентов на временном интервале в годы (система легко работает с терабитами информации) или в режиме реального времени
- Взаимодействие с системой ATLAS и получение новейших данных об угрозах

Стоимость решения: от 217k$

ARBOR NETWORKS

Где можно посмотреть наши решения?

- **О DDOS атаках**
  - The Evolution of DDoS Attacks http://www.youtube.com/watch?v=Q7deVOUXPFk
- **Система Atlas**
  - DDoS Attack Protection: Arbor Network's ATLAS http://www.youtube.com/watch?v=0U68W6gTkP8
  - Atlas Dashboard http://atlas.arbor.net
- **О нашей команде Asert**
  - Arbor Networks: Researching DDoS and Advanced Threats http://www.youtube.com/watch?v=T3oBpvcBxD4
  - Worldwide Infrastructure Security report http://www.youtube.com/watch?v=-83m82sEpNI
  - DDoS and the Evolving Advanced Threat Landscape http://www.youtube.com/watch?v=92p_MbPbewk
  - Asert blog http://www.arbornetworks.com/asert/
- **Решения Arbor Networks (Peakflow, Pravail APS, Pravail NSI, Pravail SA, Arbor Cloud)**
  - Comprehensive DDoS Protection Solutions http://www.youtube.com/watch?v=JP299b-IG6g
  - Video about Pravail family solutions:http://www.youtube.com/watch?v=Qznv913qVzw&list=PLu8eXm-IEjEC-kbMOSsQKPJGoc1V75fnw
  - Pravail NSI Product Tour http://www.youtube.com/watch?v=2Fn_b4g1Tqw
  - Cloud-Based DDoS Protection from Arbor Networks http://www.youtube.com/watch?v=kPJ-wjyhyoM
  - Pravail SA (Packetloop) http://vimeo.com/user6890858/videos

ARBOR NETWORKS

Где можно посмотреть наши решения?

- **Лучше всего смотреть решения прямо у вас на сети**
  - Для этого не требуется изменять конфигурацию вашей сети
  - Решения могут работать только в режиме анализа во время пилота
- **Или посмотреть на сети наших заказчиков**
- **Наши решения можно взять на тесты, в том числе и по программе Try&Buy!**
  - Обращайтесь к нашим партнёрам или к представителям Arbor Networks

ARBOR NETWORKS

Спасибо за внимание!

Михаил Родионов

+7.916.934.61.99

mrodionov@arbor.net

Enterprise sales manager, CIS

WIRED

“Arbor Networks знает о работе Internet больше чем кто-либо еще (за исключением Агентства Национальной Безопасности). Если Вы хотите узнать, как выглядит актуальный профиль трафика и угроз в Интернете, взгляните на сервис ATLAS.»

ARBOR NETWORKS