ARBOR NETWORKS

Arbor Networks

Опыт по защите от DDOS атак: теория и практика

Михаил Родионов

+7.916.934.61.99

mrodionov@arbor.net

Enterprise sales manager, CIS

Arbor Networks – кто это?

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

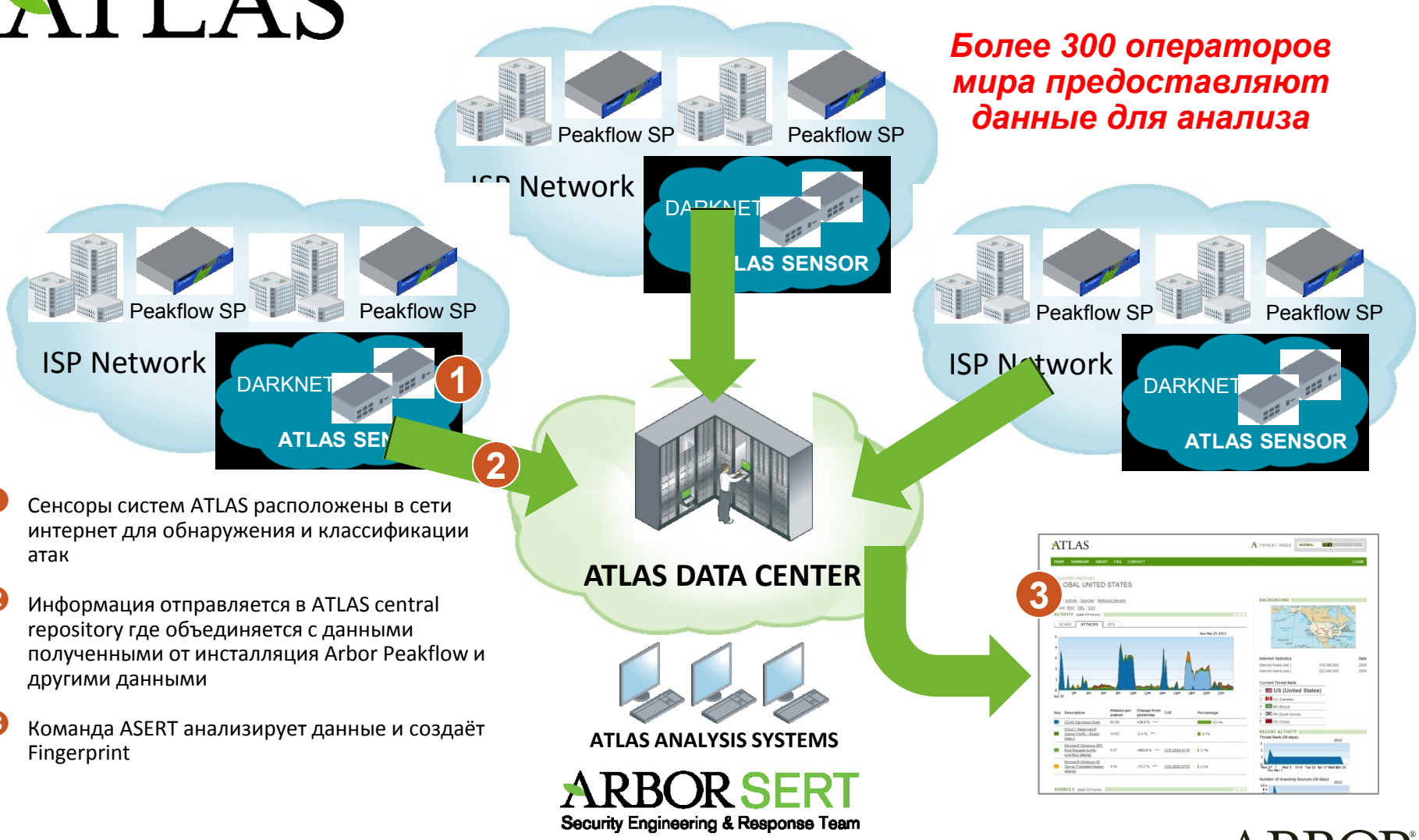
100%	Процент Tier 1 операторов, являющихся клиентами Arbor
70 Тб/с	Трафик, отслеживаемый системой ATLAS в данный момент – ***Это почти 45% всего Интернет трафика.***
#1	Позиция Arbor на рынке оборудования защиты от DDoS в сегментах Carrier, Enterprise, Mobile – 61% всего рынка [Infonetics Research Январь 2013]
14 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

Active Threat Level Analysis System (ATLAS)

ATLAS®

Первая в мире система анализа угроз

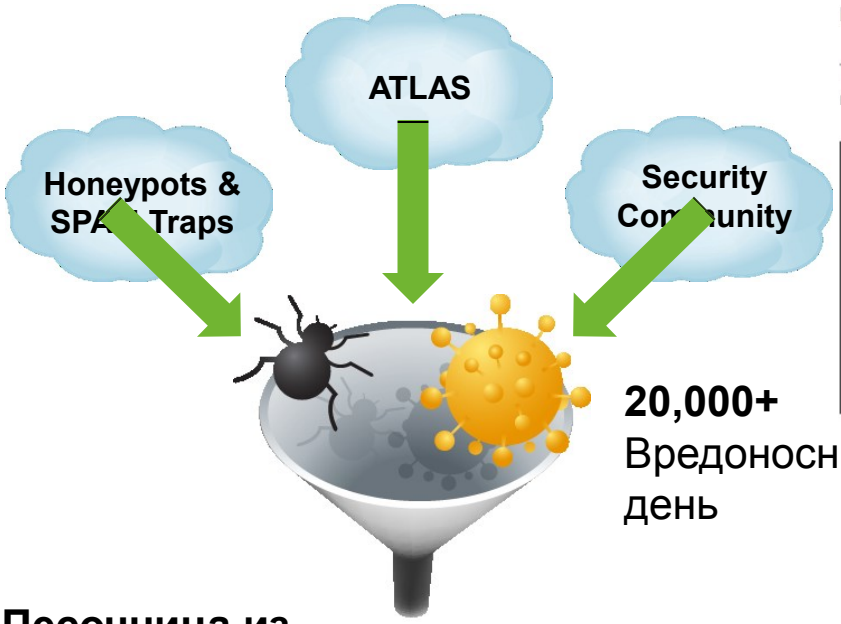
Более 300 операторов мира предоставляют данные для анализа

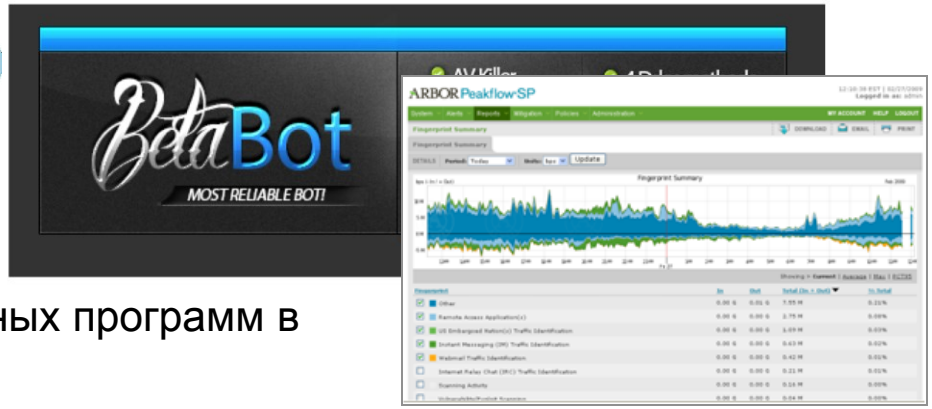


1. Сенсоры систем ATLAS расположены в сети интернет для обнаружения и классификации атак
2. Информация отправляется в ATLAS central repository где объединяется с данными полученными от инсталляция Arbor Peakflow и другими данными
3. Команда ASERT анализирует данные и создаёт Fingerprint

ARBOR NETWORKS

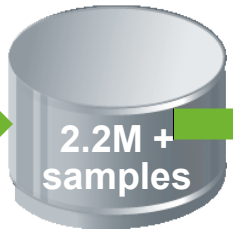
ASERT – исследовательская деятельность Arbor



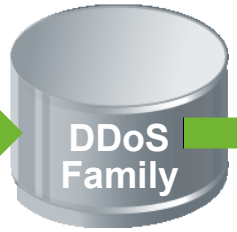


20,000+
Вредоносных программ в день

“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

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

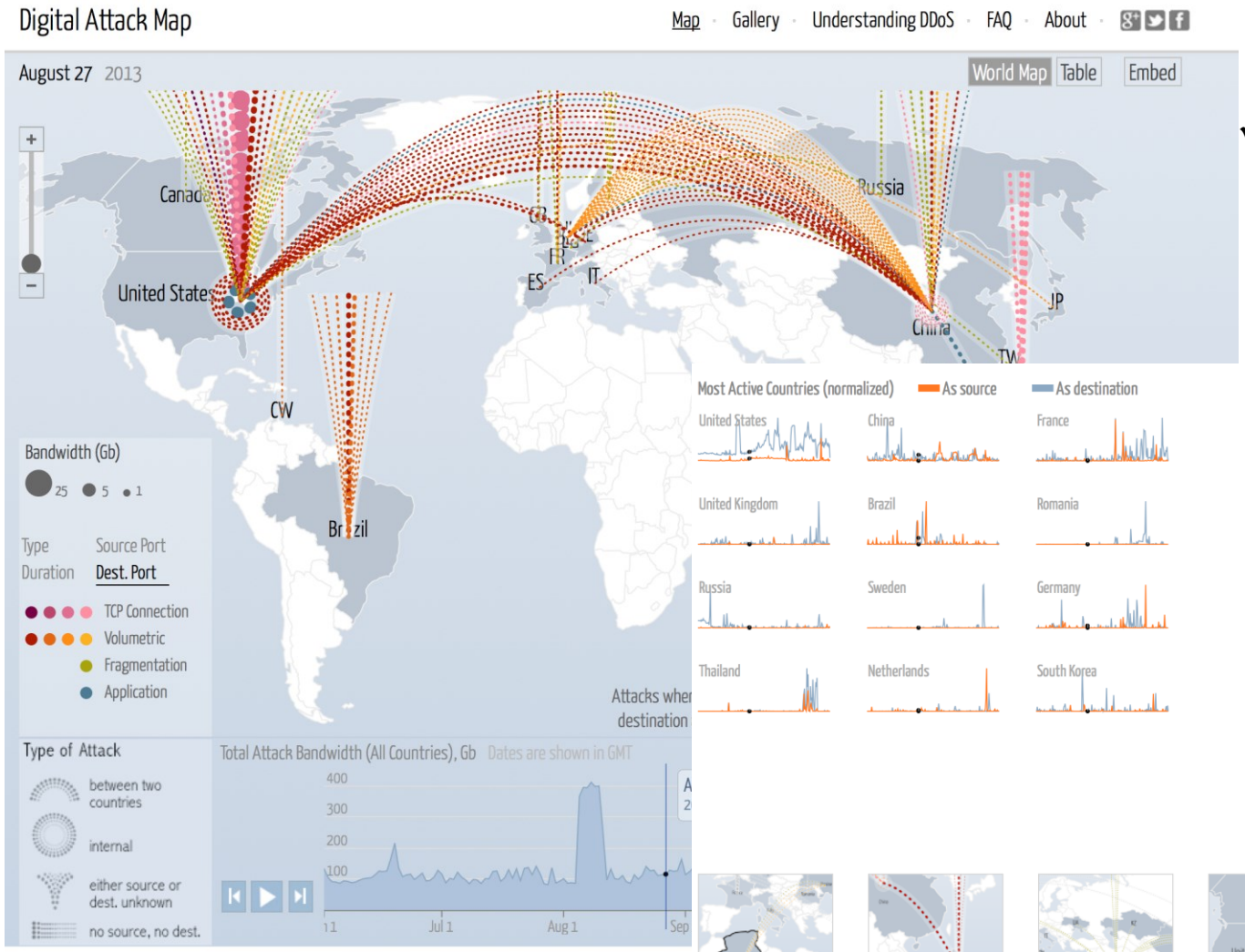
ARBOR Pravail™

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

ARBOR NETWORKS

ATLAS and Google

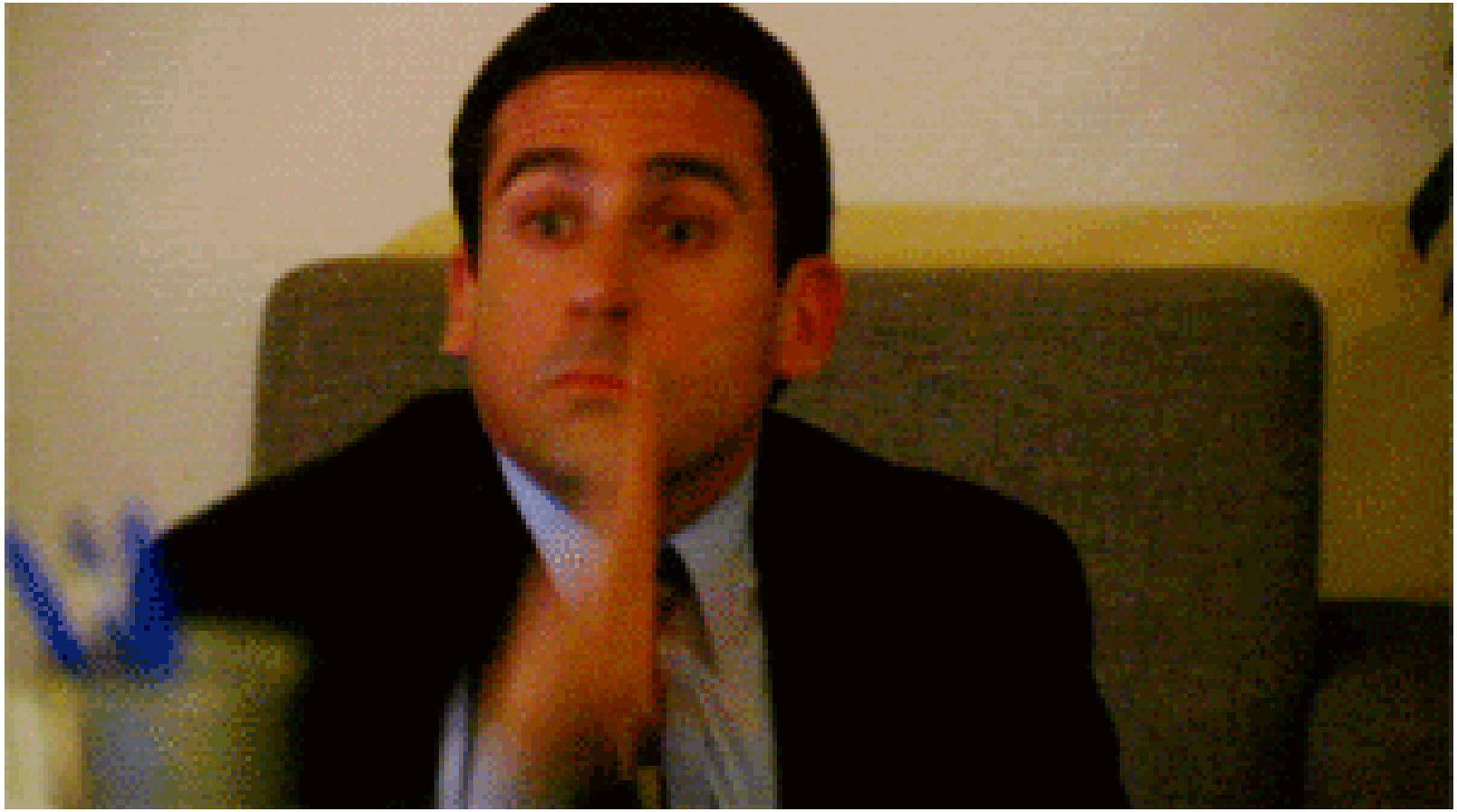
Digital attack map http://www.digitalattackmap.com/



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

ARBOR NETWORKS

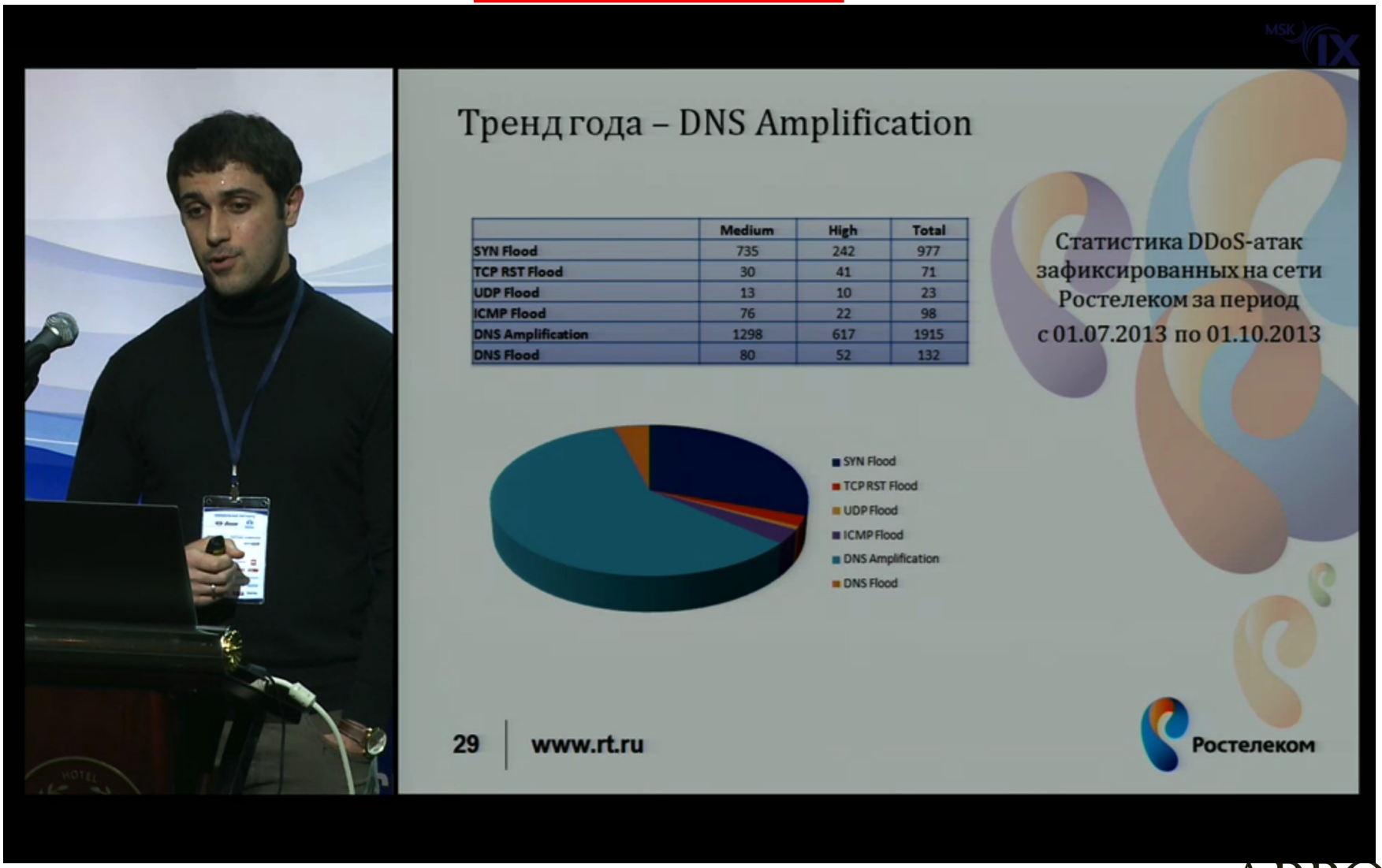
Бывали ли у вас DDOS атаки?



ARBOR NETWORKS

Только Ростелеком зафиксировал более 3000 атак

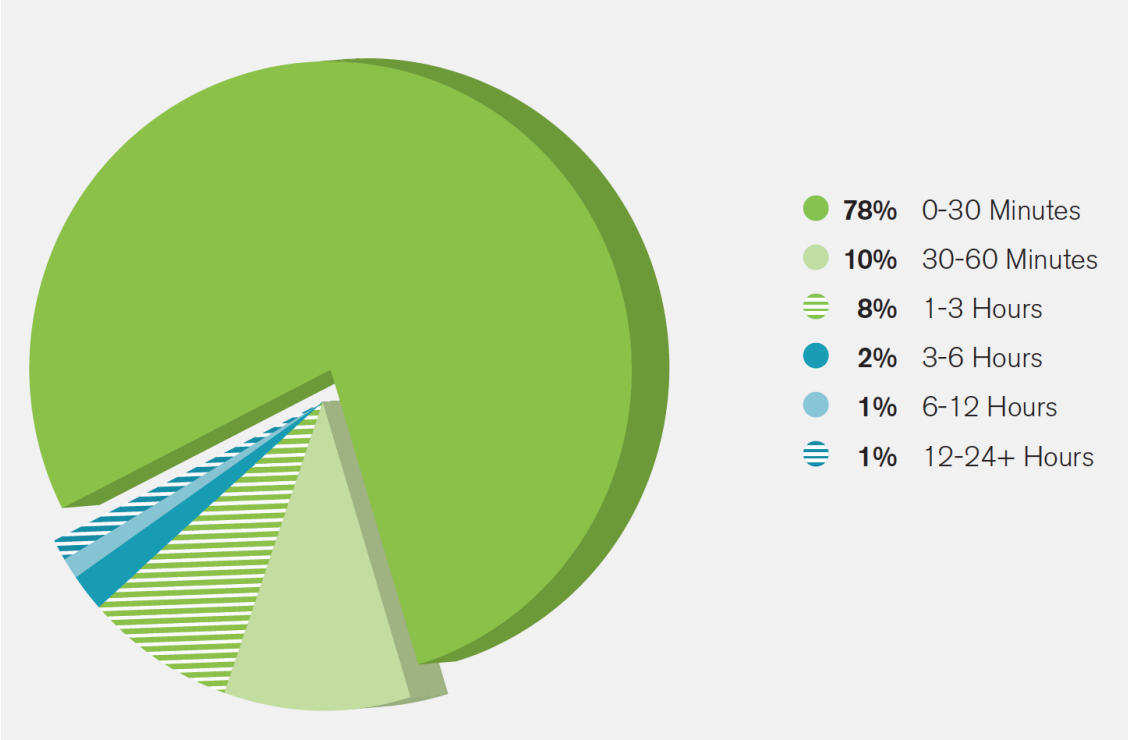
За 3 месяца!



	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

ATLAS –продолжительность атак

88% заканчиваются в течении **1 часа**
78% атак продолжаются лишь **30 минут**



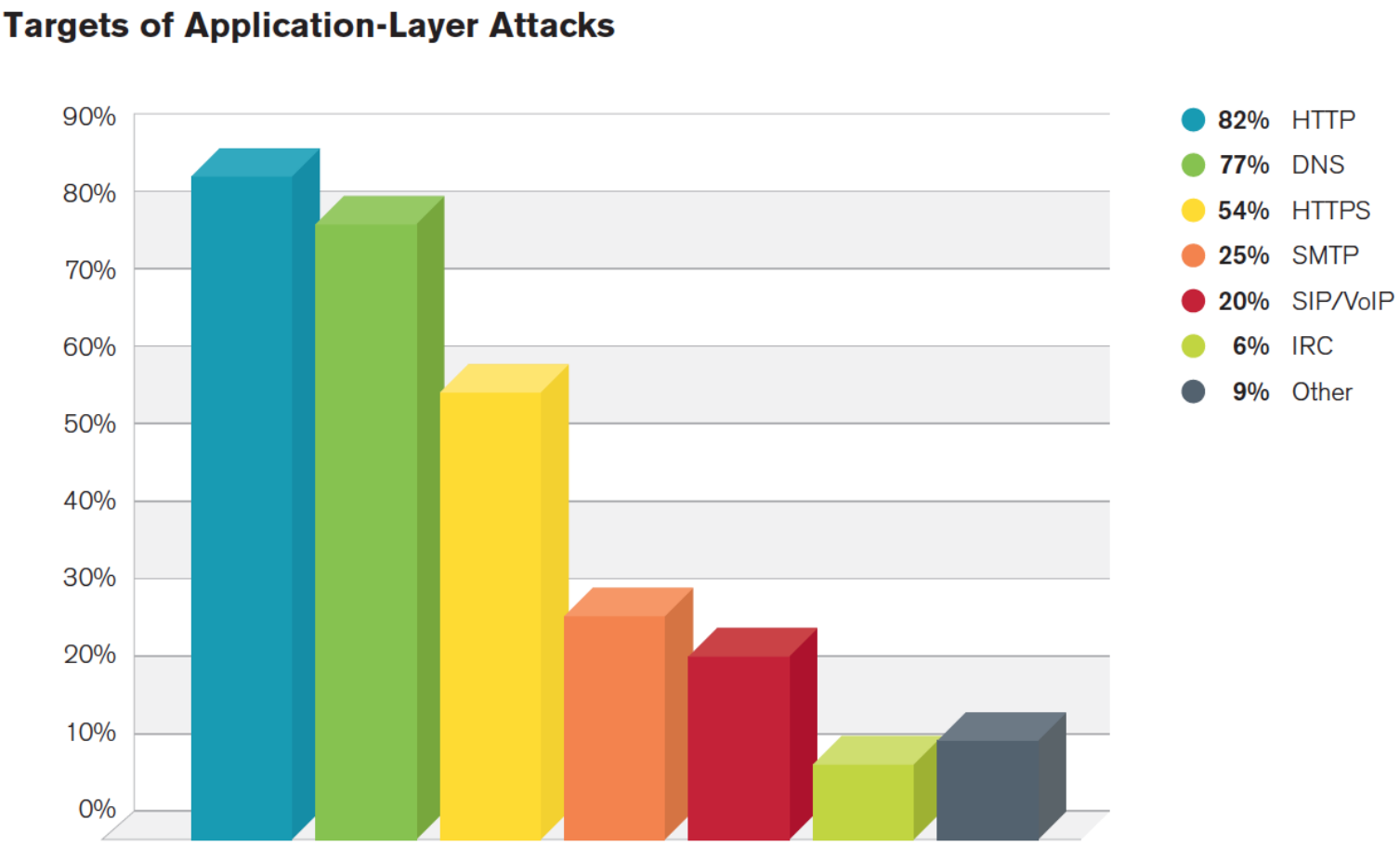
Данные использованы из отчёта Arbor Networks:

Worldwide Infrastructure Security Report IX

ARBOR NETWORKS

Наиболее атакуемые сервисы (Application layer)

До **54%** атак идёт на зашифрованные сервисы

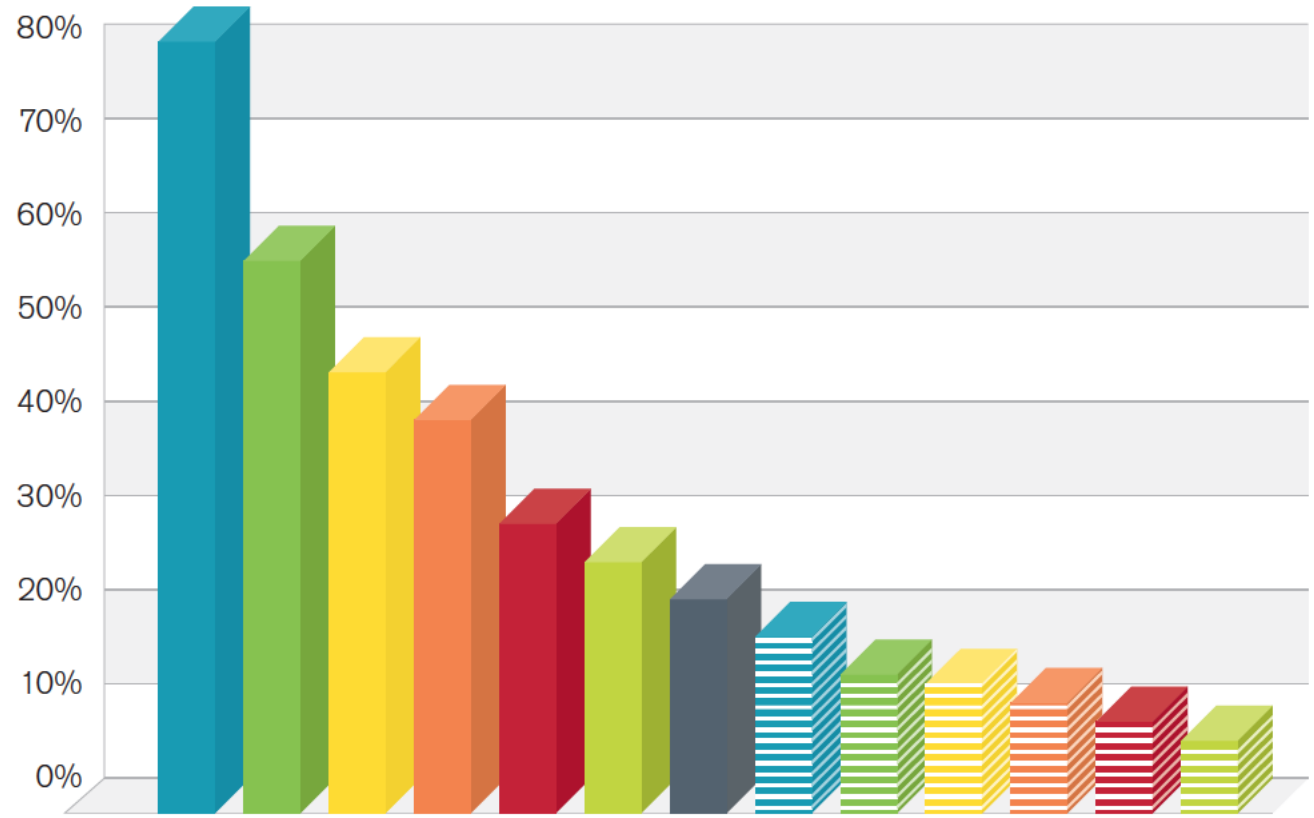


Данные использованы из отчёта Arbor Networks:

Worldwide Infrastructure Security Report IX

ARBOR NETWORKS

Наиболее популярные атаки уровня приложений



- 78% HTTP GET Flood
- 55% HTTP POST Flood
- 43% Slowloris
- 38% LOIC or Variants
- 27% Apache Killer
- 23% HOIC or Variants
- 19% SIP Call-Control Flood
- 15% SlowPost
- 11% THC
- 10% nkiller2 (TCP Persist)
- 8% Hulk
- 6% Rudy
- 4% Recoil

Данные использованы из отчёта Arbor Networks:

Worldwide Infrastructure Security Report IX

ARBOR NETWORKS

Опыт иностранных банков

В 2013 году ряд банков заявил о проблеме DDOS после атак, эти данные отображены в отчётах 10-K для Citigroup, JPMorgan Chase, Bank of America и многих других

Goldman Sachs
usbancorp
citigroup
JPMorganChase
Bank of America
CapitalOne
HSBC

Bank of America: "Our websites have been subject to a series of distributed denial of service cybersecurity incidents. Although these incidents have not had a material impact on Bank of America, nor have they resulted in unauthorized access to our or our customers…"

Атаки с использованием HTTPS в 2013 году составили около 54% всех атак на приложения.

Банки в штатах рапортовали о худшей статистике – весь HTTP трафик атаки был зашифрован SSL

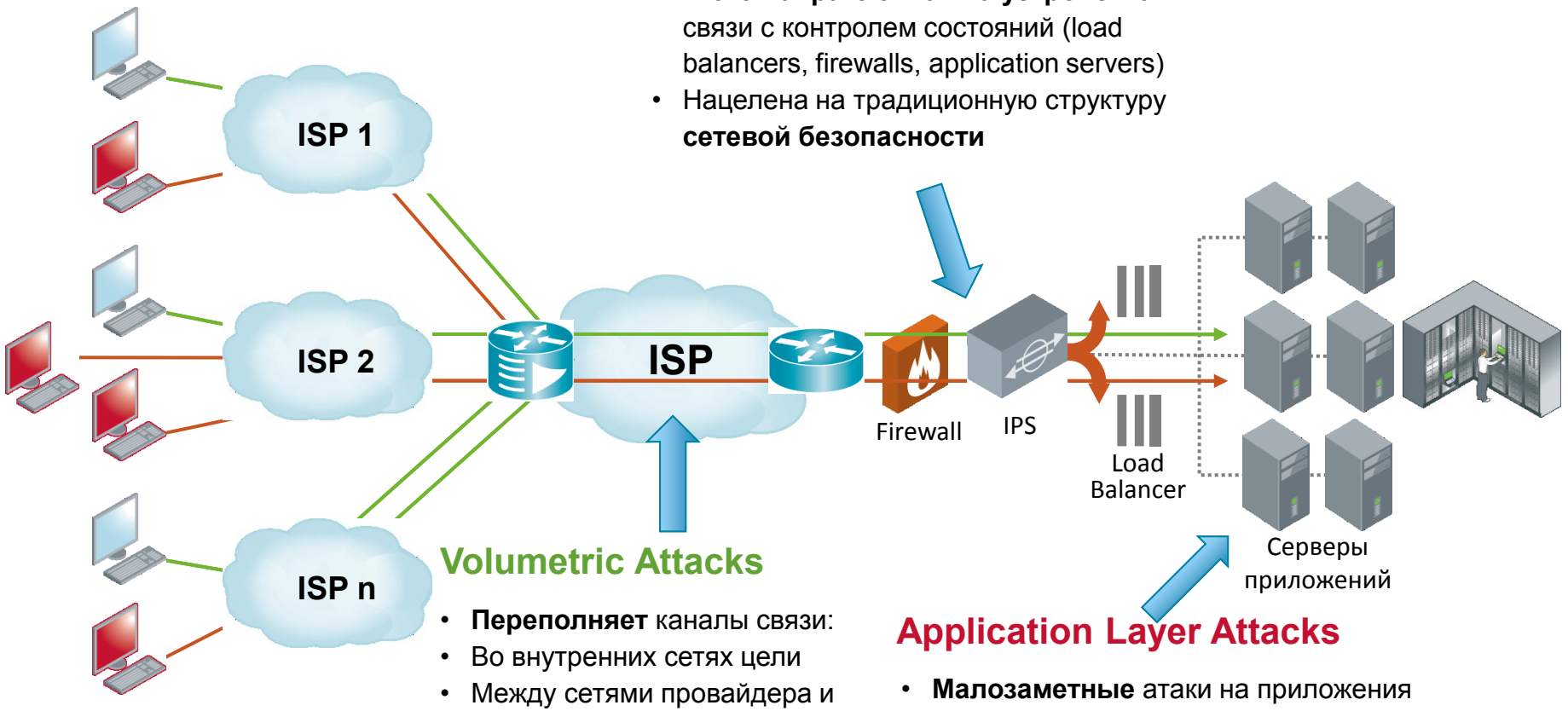
ARBOR NETWORKS

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

Решение для защиты - Pravail APS

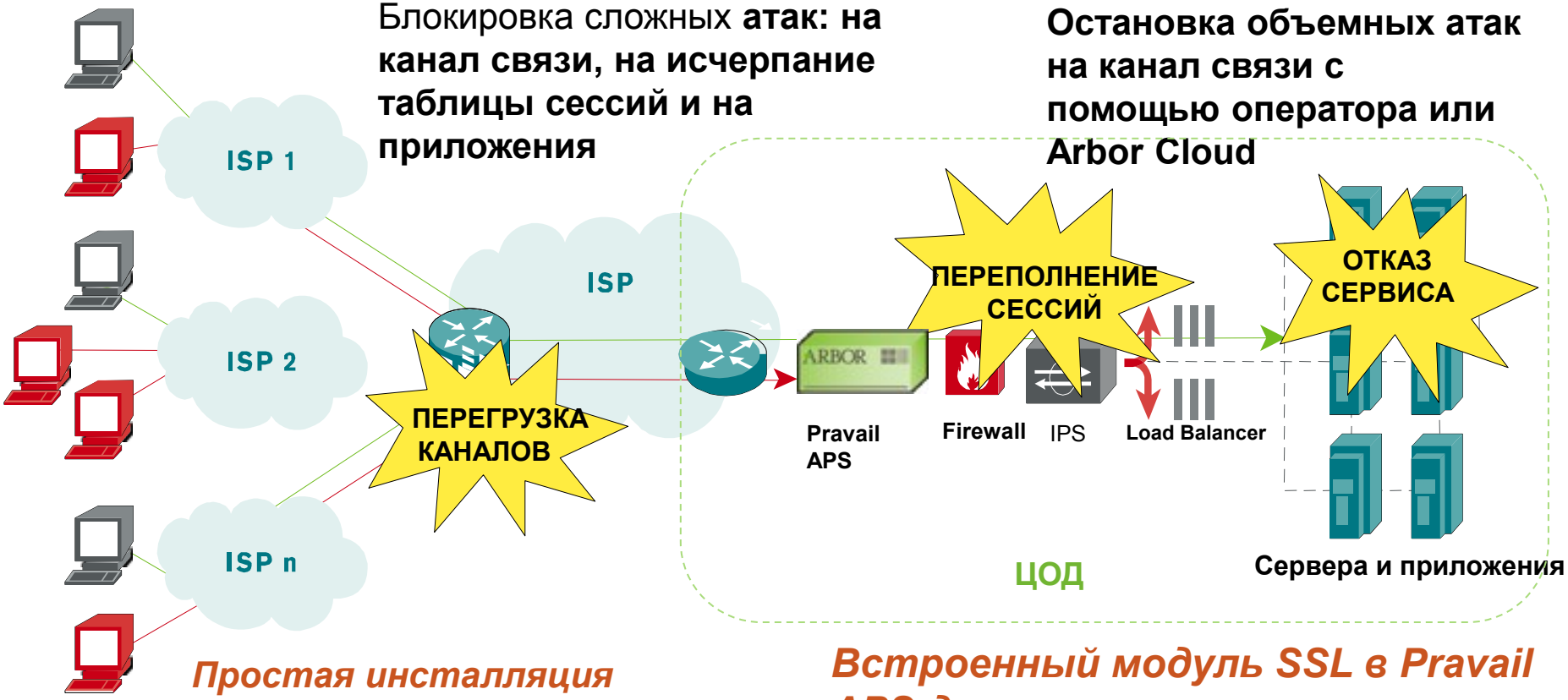
Проверенная защита от DDoS атак на площадке клиента

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

ARBOR NETWORKS

Альянс Cloud Signaling

CLOUD SIGNALING COALITION

Сотрудничество ISP и их клиентов с помощью протокола облачной сигнализации.

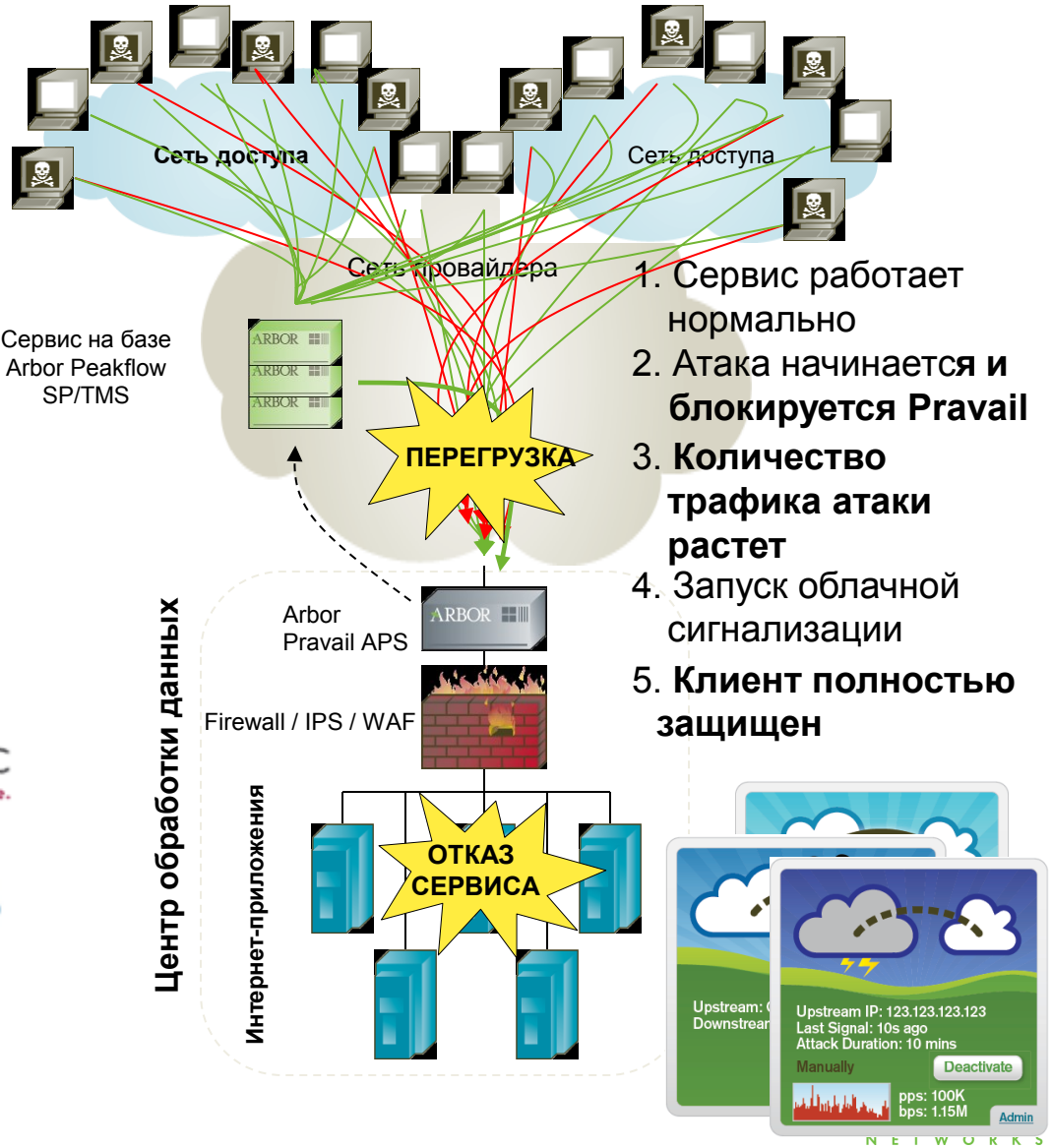
Ростелеком

circular colt smarter / faster / further du وتحيا بها الحياة add life to life

Embratel TATA PROLEXIC DDoS Attacks End Here.

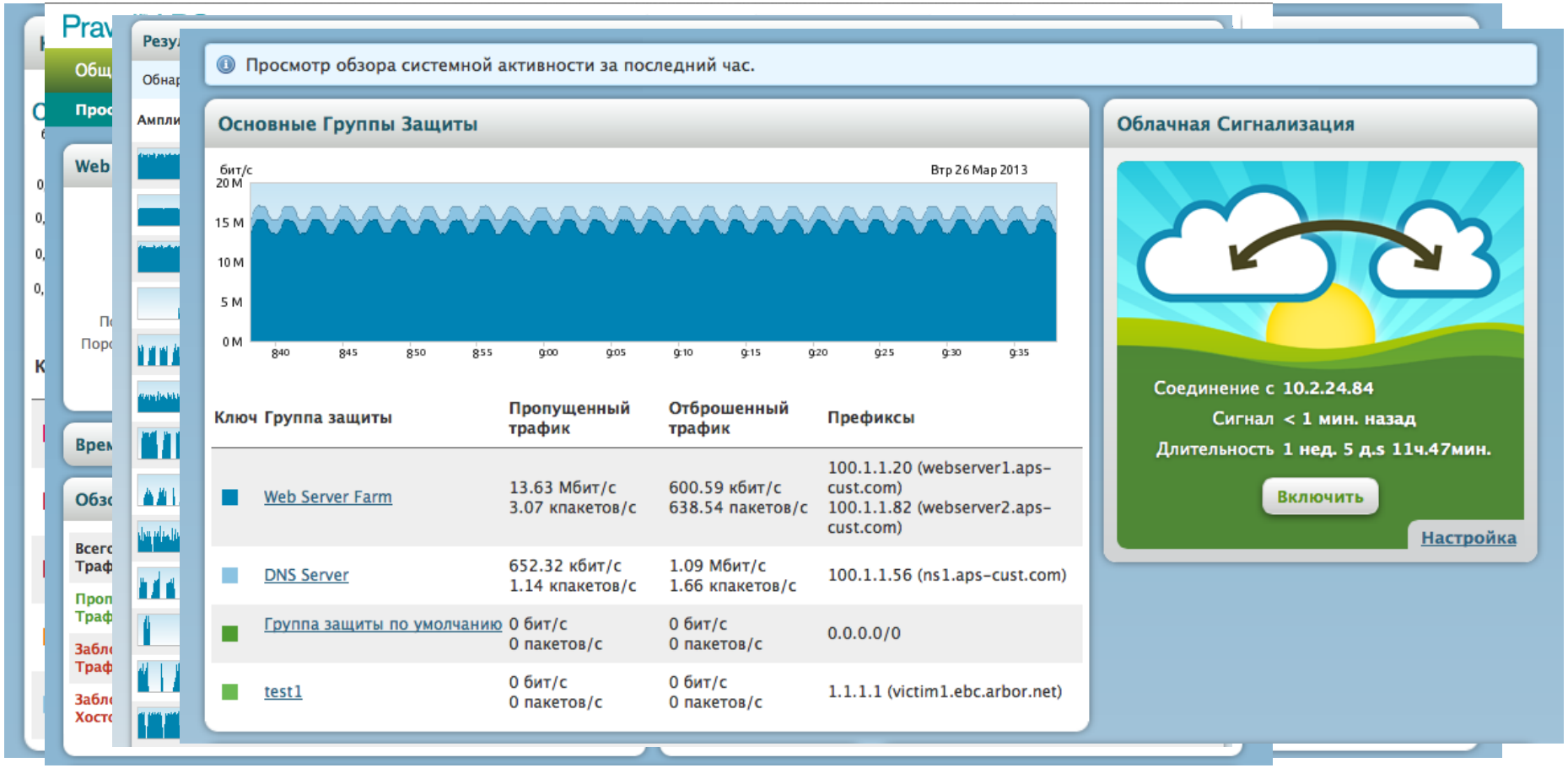
Telefonica TelstraClear VOCUS communications

swisscom neustar



Приятные мелочи

Интуитивно понятный интерфейс и документация на русском языке



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)

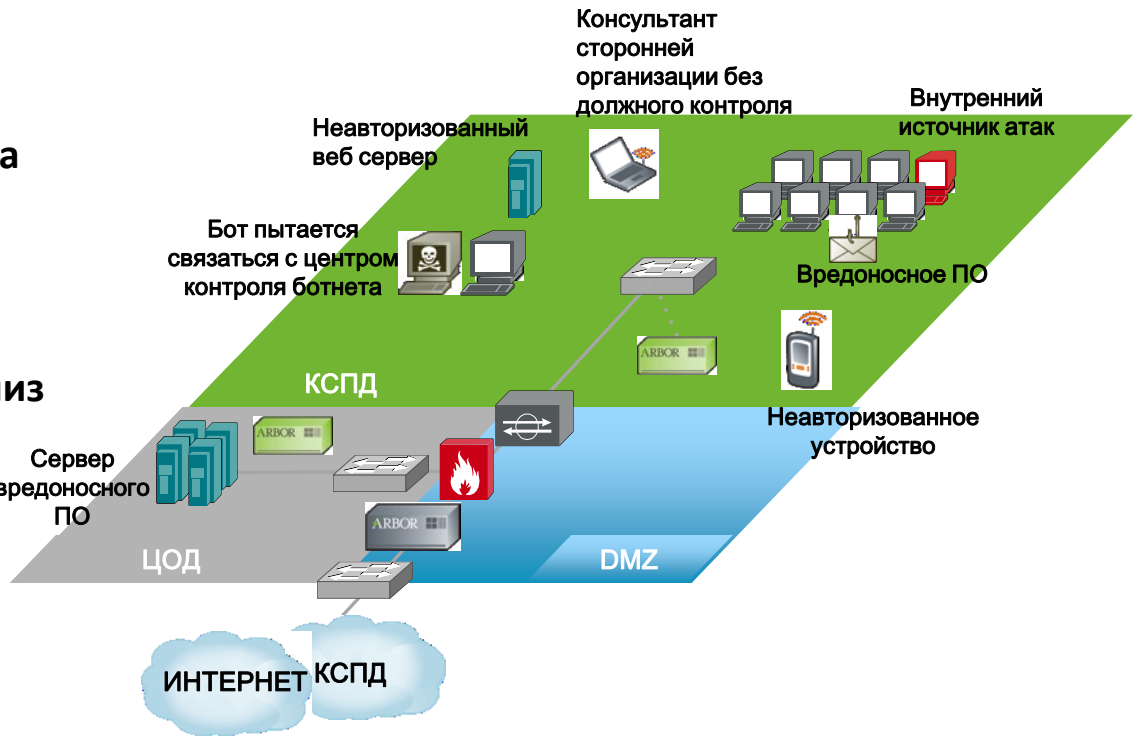
- Контроль и аудит пользователей, анализ их действий

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

Визуализация трафика корпоративного уровня

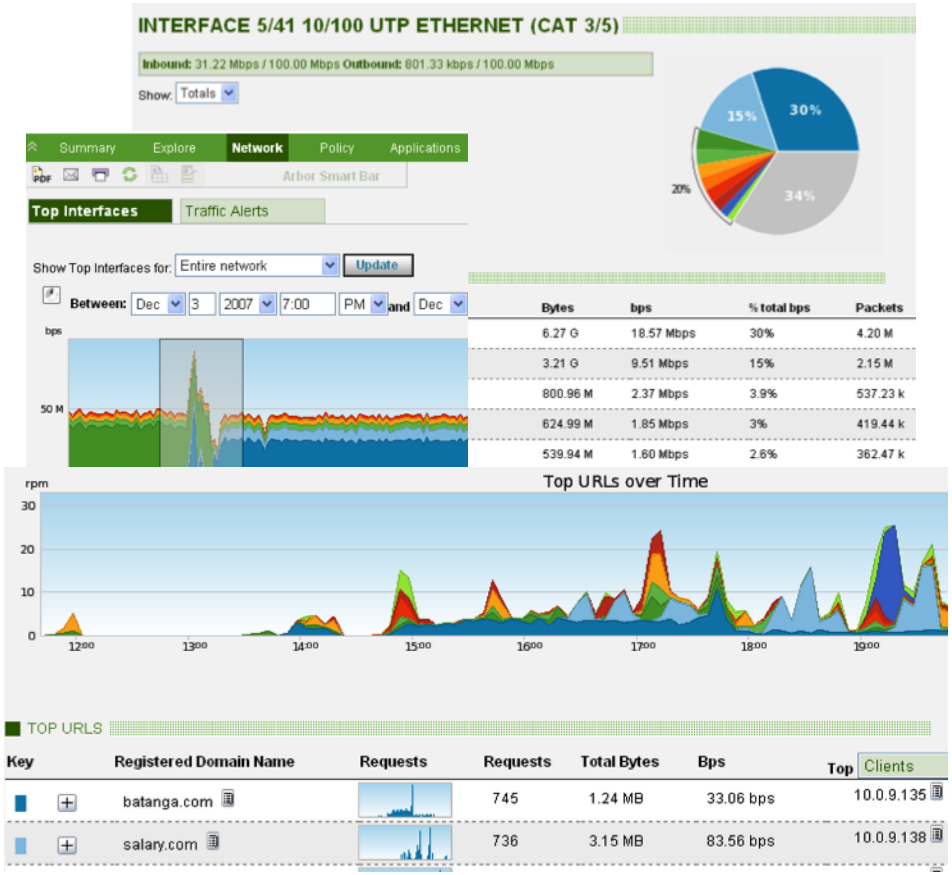
Визуализация трафика – необходимая основа безопасности
«Вы не можете обезопаситься от того, чего не видите»

Использование технологий IP Flow:

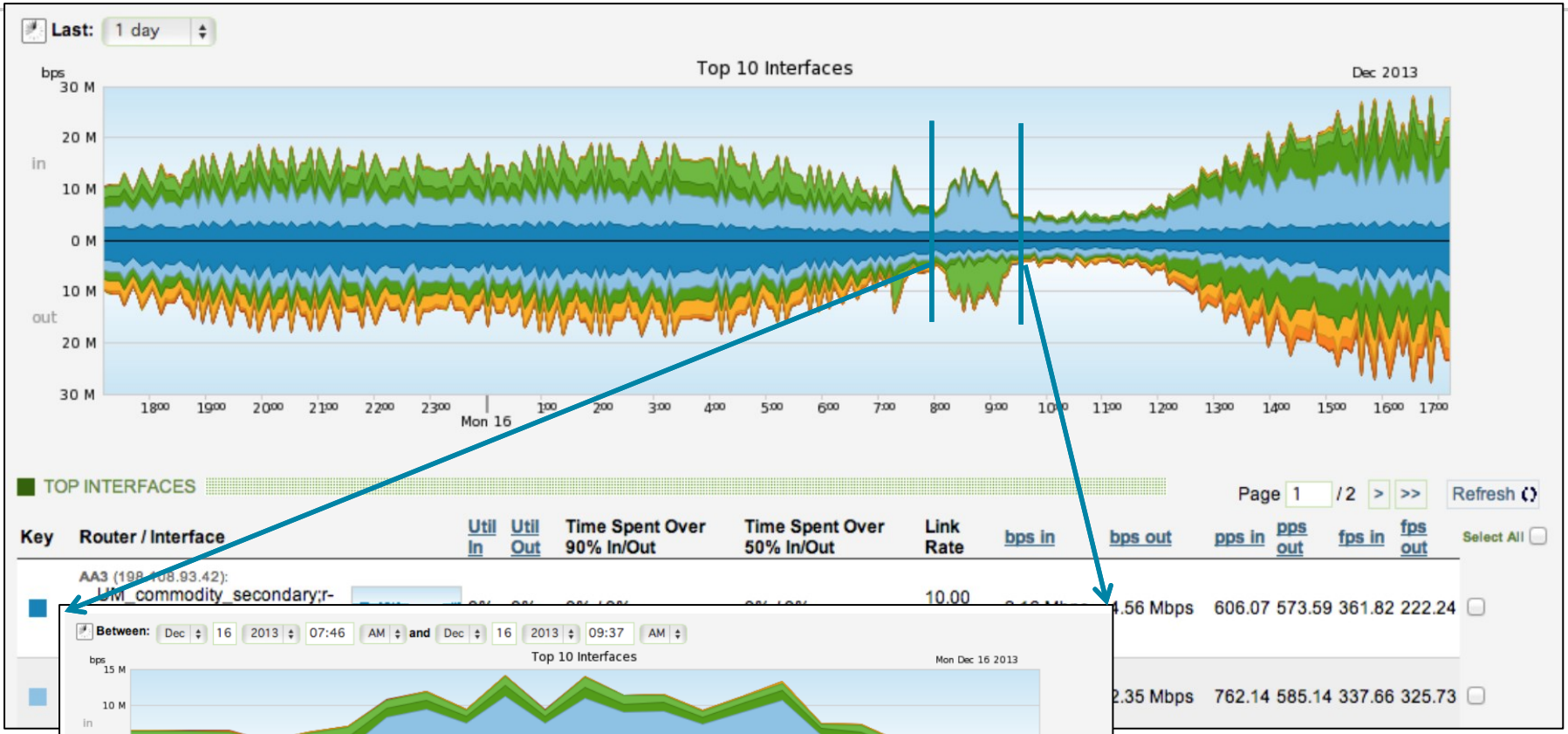
•**Эффективная визуализация трафика всей компании**

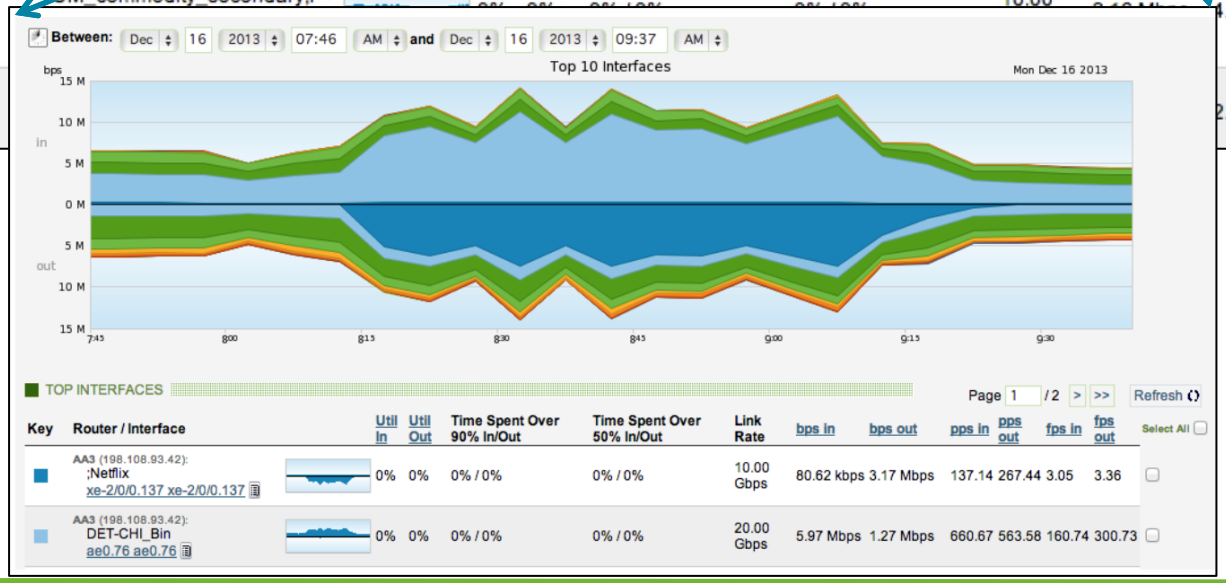
Обеспечение безопасности всей сети, а не только периметра:

•**Анализ трафика по всей сети без границ**



Пример: обнаружение узких мест в сети

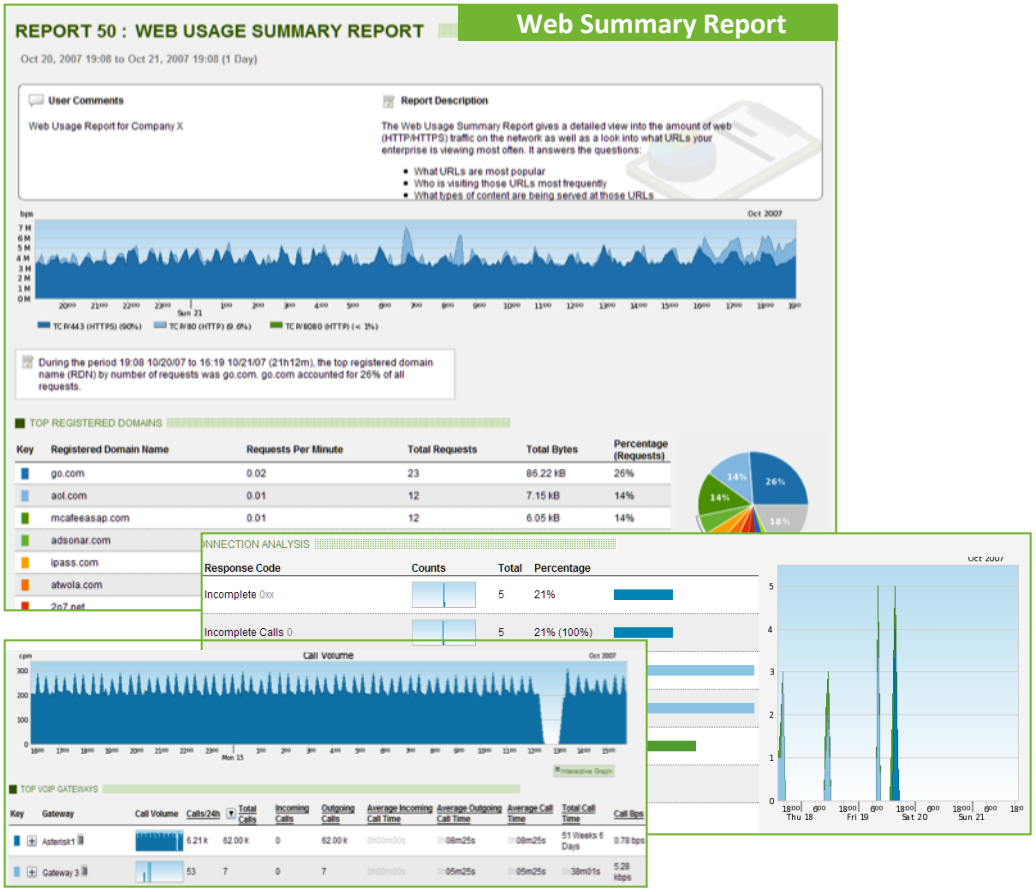




ARBOR NETWORKS

Анализ приложений

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

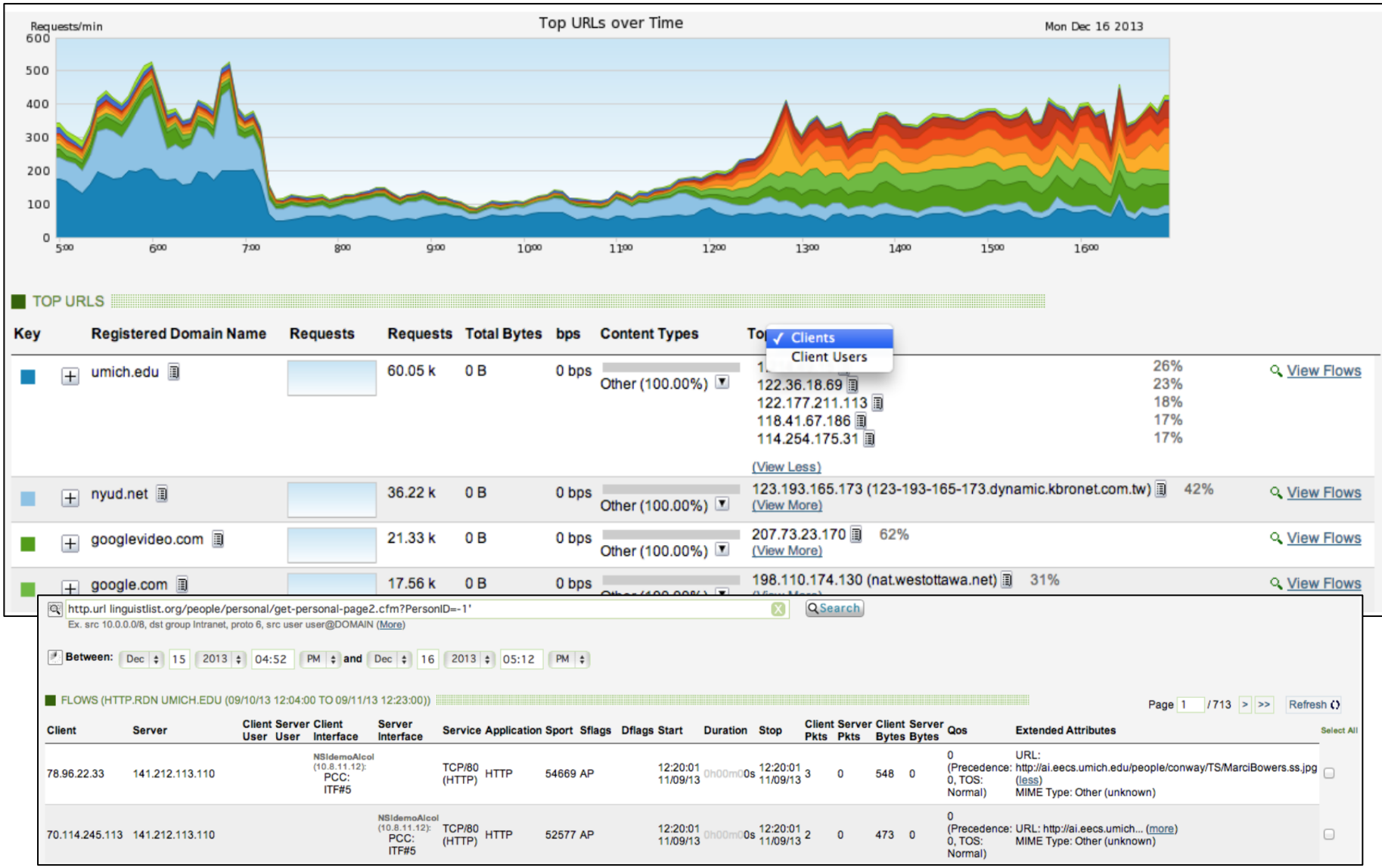


Предотвращение утечек данных **за счет информации об открываемых ресурсах, трафике на некорректных портах и типе передаваемых данных**

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

ARBOR NETWORKS

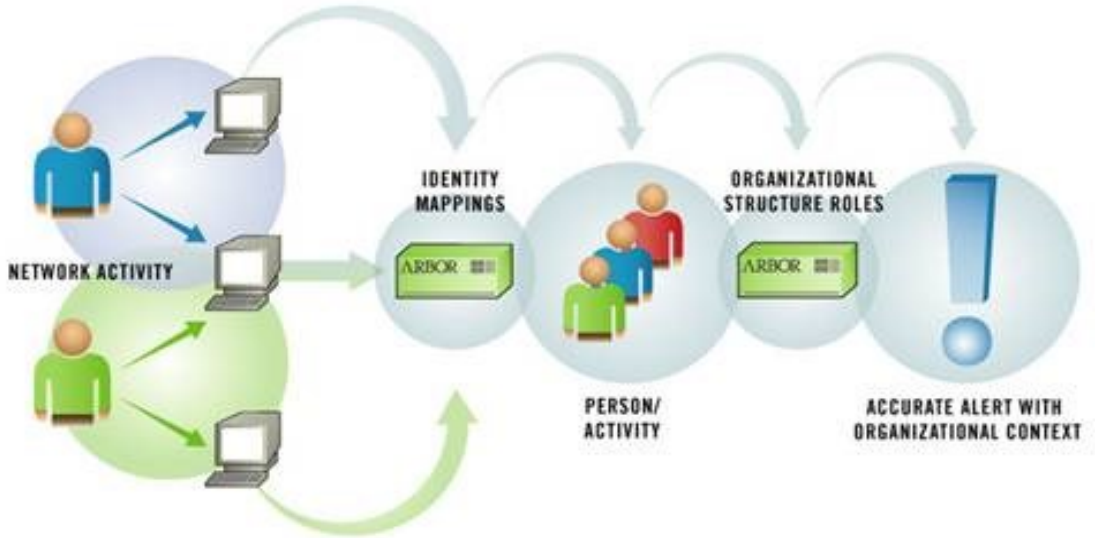
Пример: аналитика по URL



ARBOR NETWORKS

Контроль действий пользователей

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



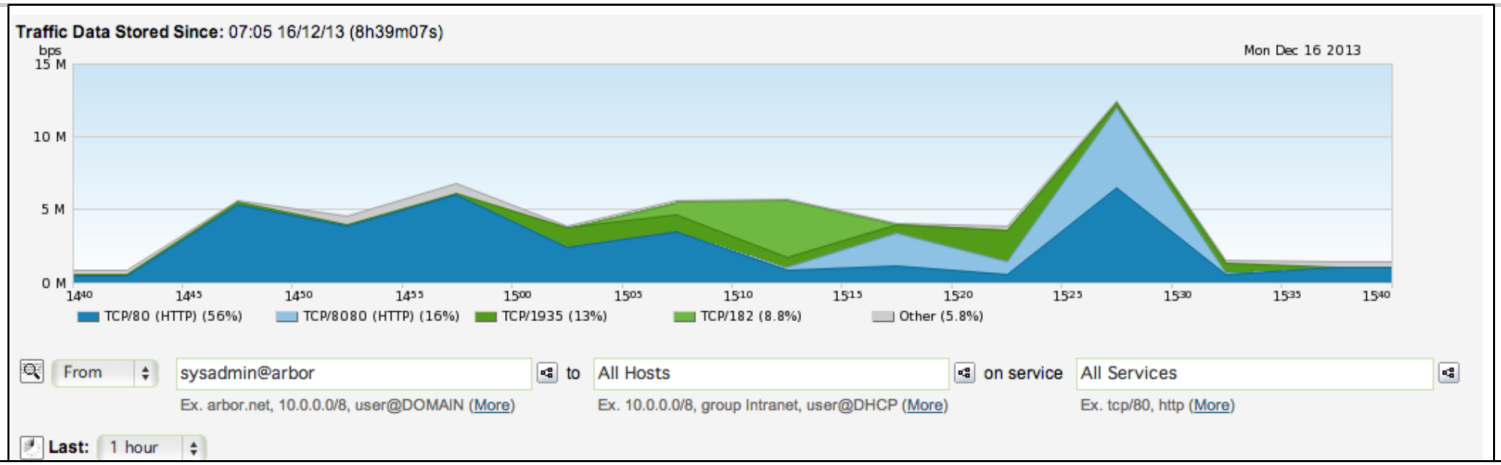
Выявляйте пользователей **вредоносного ПО, а не только IP адреса**

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

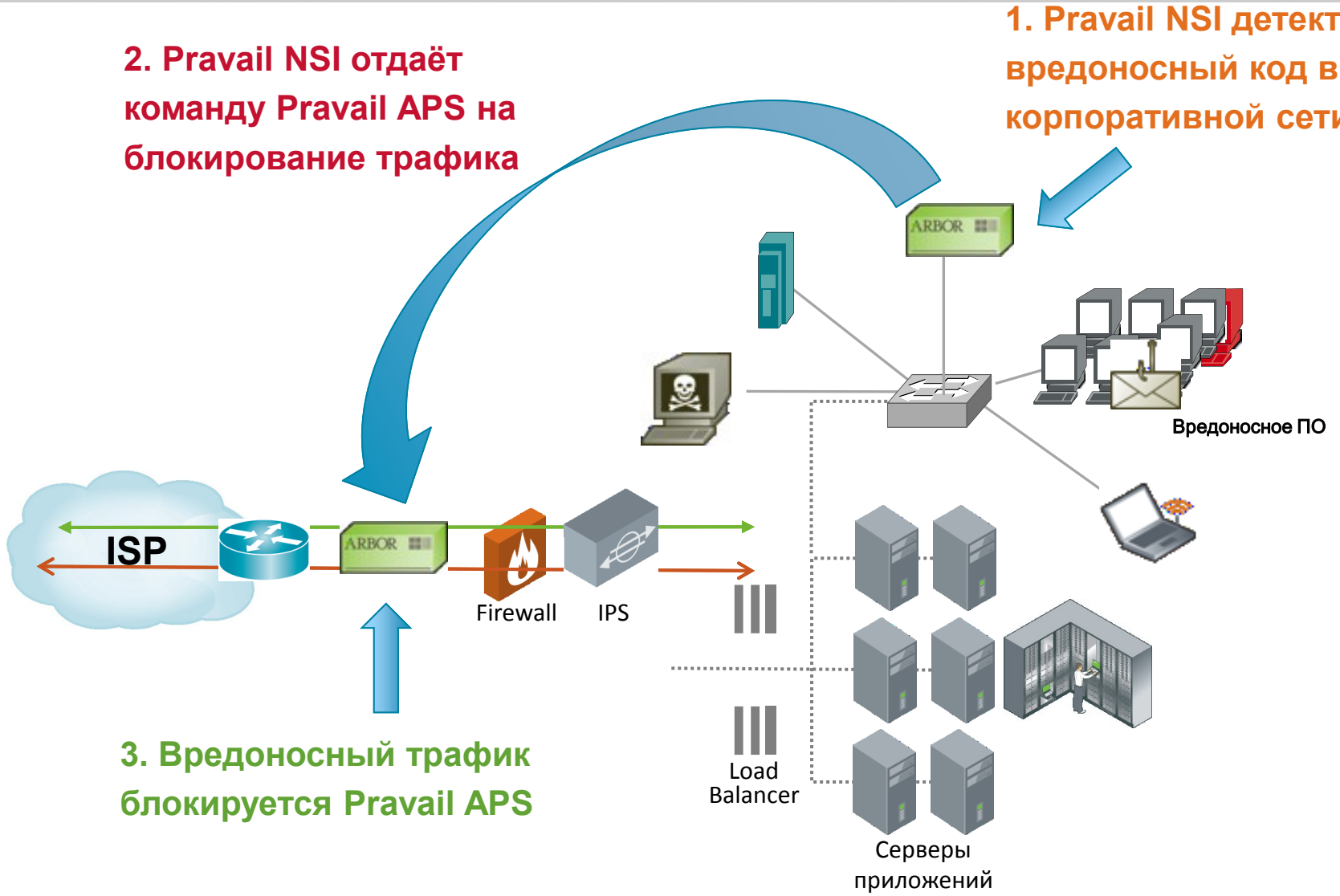
Key	Applications
TCP/80	
TCP/8080	
TCP/1935	
TCP/182	
TCP/443	84% SSL
TCP/22	99% SSH
TCP/5103	85% HTTP
TCP/8006	
TCP/4070	
UDP/19305	
Other (31 services)	

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

Интеграция Pravail APS и Pravail NSI



ARBOR NETWORKS

Новое решение - 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

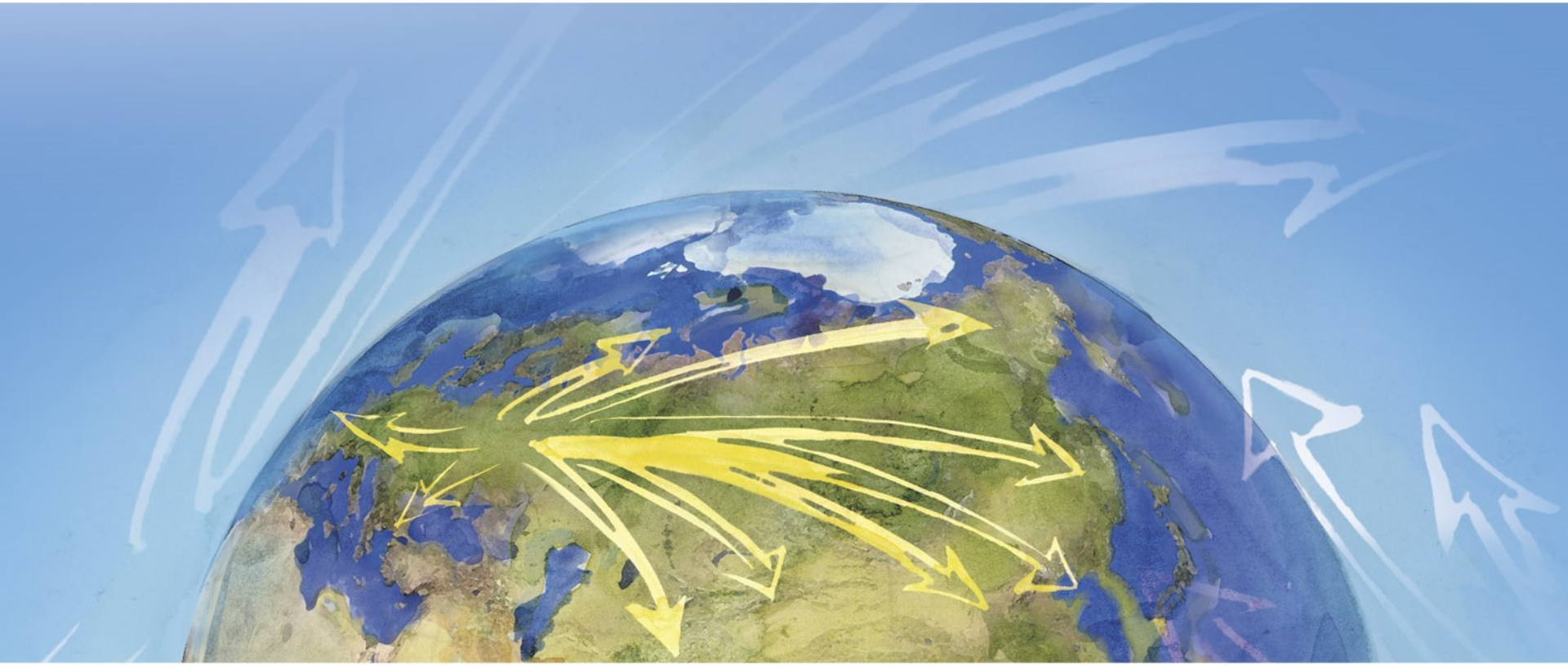
Мы видим то, что не видят другие

ARBOR NETWORKS

микротест®

ОТКРЫТОЕ АКЦИОНЕРНОЕ ОБЩЕСТВО
ХАНТЫ-МАНСИЙСКИЙ БАНК

Ханты-Мансийский Банк: Arbor Pravail APS



Илья Яблонко, CISSP
заместитель руководителя направления ИБ Микротест

План доклада

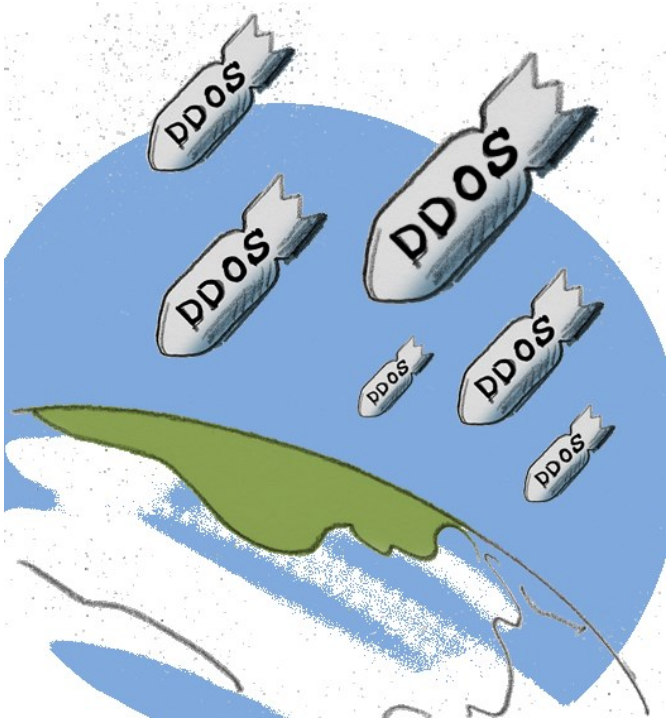
- Как Банк осознал необходимость в защите от DDoS-атак?
- Как Банк выбирал решение?
- Как внедрялось решение?
- Какой Банк имеет результат?

Как возникла задача в защите от DDoS?

- В 2011 – 2012 гг. Банк подвергся нескольким DDoS-атакам, которые привели к нарушению работы сетевого оборудования на Интернет-периметре.
  В результате атаки Банк оказался отрезанным от Интернет

- Тип атаки: Syn Flood

- Слабое звено: корпоративный межсетевой экран



Какие типы решений по защите от DDoS может рассматривать банк?

- решения в виде аппаратно-программных или программных комплексов, устанавливаемых в корпоративной сети заказчика

ARBOR NETWORKS
radware
МГТИ СОФТ

- сервисы по защите от DDoS-атак, предоставляемые провайдерами и поставщиками услуг

KASPERSKY lab
BIFIT Банковские и Финансовые Интернет Технологии
GROUP IB
QRATOR

Arbor имеет следующие преимущества

- Решения Arbor Networks установлены у **100% операторов связи Tier-1** и у **60+% операторов связи Tier-2** во всем мире
- Лаборатория ASERT анализирует угрозы ИБ в Интернет-трафике, разрабатывает противомеры и сигнатуры для защиты от DDoS
- Arbor Pravail APS предоставляет полное аппаратное резервирование во всех моделях оборудования, включая аппаратный и программный ByPass на всех типах интерфейсов, резервные блоки питания, несколько каналов связи
- Arbor Pravail APS предоставляет **более широкий набор функций и более гибкую настройку противомер** для подавления DDoS-атак
- Cloud Signalling: Arbor Pravail APS + Arbor Peakflow SP у вышестоящего оператора связи = **эффективная защита** не только инфраструктуры, но и канала связи
- Наличие у партнеров Arbor **сервисных центров**, предоставляющих качественную техподдержку на русском языке
- Arbor является **технологическим лидером в отрасли**, остальные производители находятся в статусе «догоняющих»

Почему «облачные сервисы» не подходят для банка?

- Облачные провайдеры используют либо собственные разработ (сомнительное качество услуг) либо Arbor, Radware, МФИ-Софт
- У российских облачных операторов небольшая клиентская база по защите от DDoS, соответственно страдает экспертиза, универсальность, гибкость
- Если же число клиентов у облачного провайдера становится большим, теряется индивидуальность подхода и скорость реакции на атаки на банк
- Иностранным облачным сервисам российские заказчики не доверяют
- Максимальная оперативность и гибкость реагирования на атаки достигается только если банк самостоятельно или с помощью выделенных специалистов техподдержки (аутсорсинга) управляет механизмами защиты своих ресурсов
- Arbor Pravail APS предоставляет два режима работы – неактивный и активный, что позволяет обучить систему и минимизировать количество ошибок
- Большая часть облачных провайдеров защищает в основном HTTP и не позволяют защищаться от атак на сигнализацию SSL и на атаки внутри установленной SSL-сессии. Arbor позволяет защититься от атак на HTTPS, DNS, VoIP, SMTP, UDP, ICMP и др.

Простота интеграции Arbor в сеть банка

При внедрении Arbor Pravail APS:

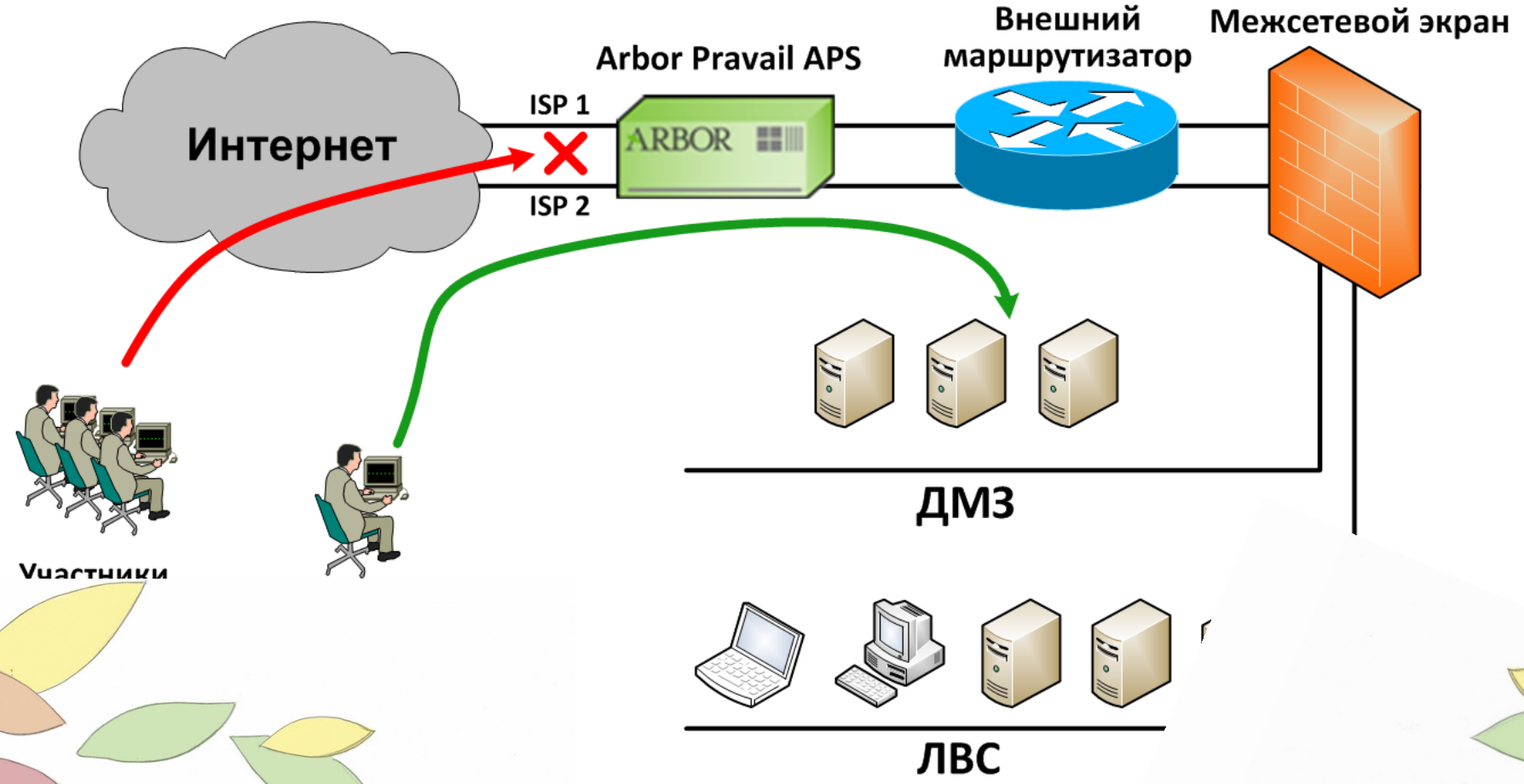
- Не требуется изменение топологии сети
- Не требуется перенаправление трафика в центр очистки оператора связи
- Не требуется изменение IP-адресации (система работает в transparent L2 режиме)
- Не требуется дополнительное резервирование аппаратной части
- Не требуется перенос SSL-сертификата банка на сервер поставщика услуг

Ханты-Мансийский Банк выбрал для защиты от DDoS-атак АПК Arbor Pravail APS 2002

Характеристики платформы Arbor Pravail APS 2002:

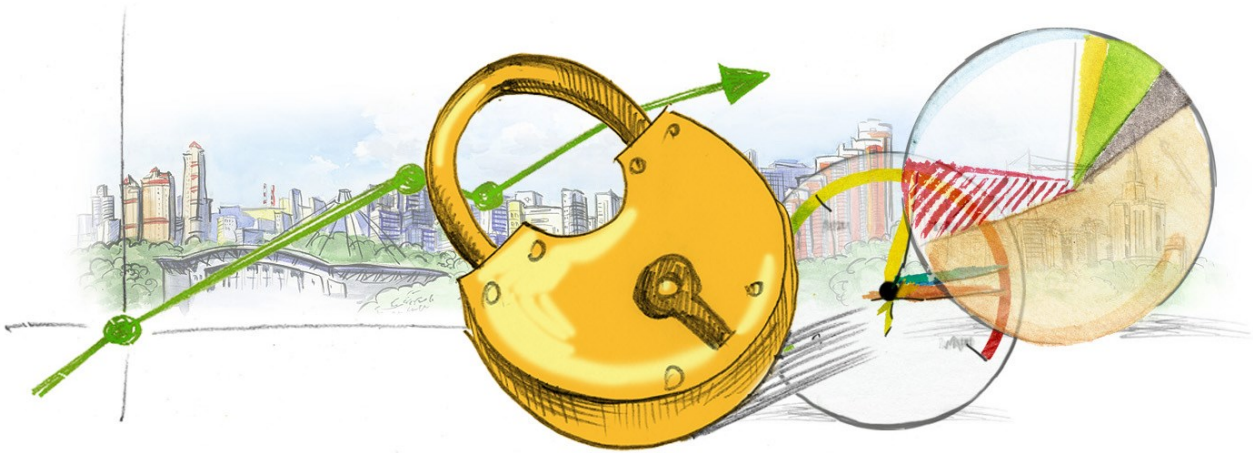
- Производительность 500 Мбит/с
- Интерфейсы: 8 x 1 GigE, copper
- Пары интерфейсов работают в режиме hardware bypass и software bypass
- Два блока питания в режиме резервирования
- Неограниченное количество защищаемых ресурсов за фиксированную стоимость

Схема реализации



Особенности реализации

- Одновременное обслуживание двух каналов связи – основного и резервного
- Arbor Pravail APS установлен перед внешним маршрутизатором и межсетевым экраном – защита от атак не только серверов, но и сетевого оборудования и СЗИ
- Система работает в отказоустойчивом режиме – резервирование блоков питания, hardware bypass на сетевых интерфейсах



Полный цикл работ:

- Обследование
- Разработка техно-рабочего проекта
- Разработка программы и методики испытаний
- Поставка Arbor Pravail APS
- Монтажные и пусконаладочные работы
- Испытания системы
- Техническая поддержка

Продолжительность проекта: 2,5 месяца

При внедрении системы специалисты Микротест провели инструктаж (мини-обучение) сотрудников банка по администрированию и эксплуатации системы

Pravail APS

Режим работы | В разрыв | Активный | Неактивный

Уровень защиты | Низкий | Средний | Высокий

Общая информация | Исследование | Группы защиты | Конфигурация | Помощь

04 Окт 2013 12:14 YEKT
Пользователь: mtzimovets (Выйти)

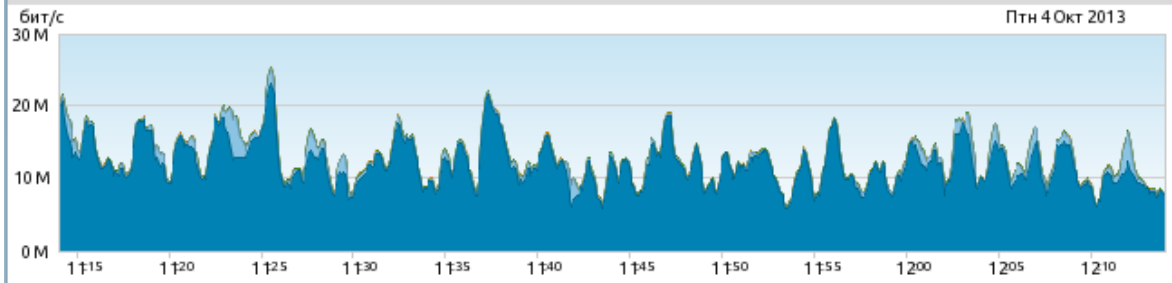
Общая информация

Просмотр обзора системной активности за последний час.

Активные события

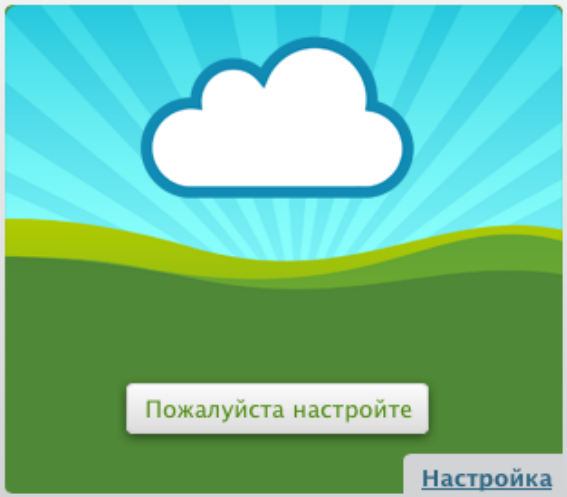
Имя	Описание	Время начала
Blocked Traffic	Blocked traffic for protection group 'Группа защиты по умолчанию' exceeded the baseline. The blocked traffic level was 201.82 kbps.	11:20 04/10/13

Основные Группы Защиты



Ключ	Группа защиты	Пропущенный трафик	Отброшенный трафик	Префиксы
	Группа защиты по умолчанию	11.66 Мбит/с 1.52 кпакетов/с	49.80 кбит/с 10.36 пакетов/с	0.0.0.0/0
	Входящие почтовые сервера ОАО «Хан...	614.08 кбит/с 76.69 пакетов/с	0.25 бит/с 0 пакетов/с	[redacted].khmb.ru) [redacted].khmb.ru)

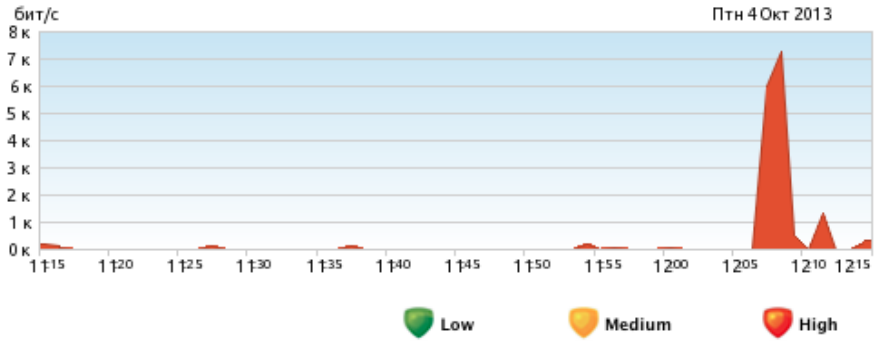
Облачная Сигнализация



Трафик соответствующий AIF

Последнее обновление AIF: Успешно, Вчера (13:30 03/10/13)

Количество сиг... 192
Заблокировано... 0



Groups with AIF-detected traffic	0	0	2
Веб-сервер ОАО «Ханты-Мансийский банк»	**0 бит/с** *	0 бит/с	256.34 бит/с
Интернет-банк ОАО «Ханты-Мансийский банк» - ibank.khmb.ru	**0 бит/с** *	0 бит/с	5.58 бит/с
Входящие почтовые сервера ОАО «Ханты-Мансийский банк»	**0 бит/с** *	0 бит/с	0 бит/с
Сервер 1С ОАО «Ханты-Мансийский банк»	**0 бит/с** *	0 бит/с	0 бит/с
Терминальный Сервер 51.22	0 бит/с	**0 бит/с** *	0 бит/с
5 Прочие	0 бит/с	0 бит/с	0 бит/с
Total detected traffic	0 бит/с	0 бит/с	261.92 бит/с
Всего отброшено трафика	0 бит/с	0 бит/с	0 бит/с

*Отбрасываемый трафик на текущем уровне защиты

Конфигурация AIF

Общая информация | Системный статус | Журнал

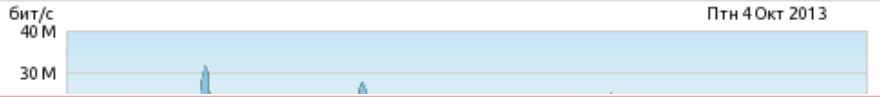
Всего Трафика		Всего: **5.60 ГБ** **12.45 Мбит/с**
Пропущено Трафика		Всего: **5.58 ГБ** **12.40 Мбит/с**
Заблокировано Трафика		Всего: **22.60 МБ** **50.22 кбит/с**
Заблокировано Хостов		В среднем: **5.63 хостов**

Суммарный трафик

Поисковые роботы

График	Поисковый робот	Суммарный трафик	Скорость трафика
	Mail.ru	42.42 МБ 46.14 к пакетов	94.26 кбит/с 12.82 пакетов/с
	Yandex	1.86 МБ 26.11 к пакетов	4.13 кбит/с 7.25 пакетов/с
	Google	478.02 кБ 7.11 к пакетов	1.06 кбит/с 1.97 пакетов/с
	Rambler	403.51 кБ 336 пакетов	896.68 бит/с 0.09 пакетов/с
	Microsoft Bing	23.25 кБ 98 пакетов	51.66 бит/с 0.03 пакетов/с

Интерфейсы

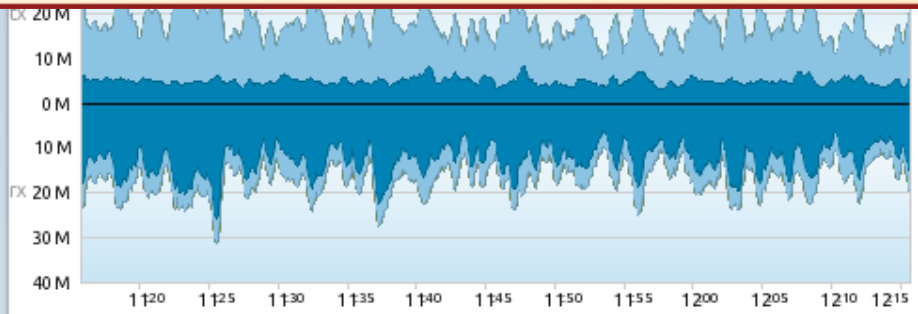


Основные страны

	График	Пропущено	Заблокировано	Доля
▸		7.39 Мбит/с 1.16 кпакетов/с	46.71 кбит/с 4.48 пакетов/с	65.06%
▸		2.13 Мбит/с 291.39 пакетов/с	3.43 кбит/с 6.01 пакетов/с	18.68%
▸		1.02 Мбит/с 93.76 пакетов/с	0 бит/с 0 пакетов/с	8.91%
▸		511.46 кбит/с 60.22 пакетов/с	0.09 бит/с 0 пакетов/с	4.48%
▸		328.71 кбит/с 98.42 пакетов/с	0 бит/с 0 пакетов/с	2.88%

Основные источники трафика

График	Источник	Суммарный трафик	Скорость трафика
	[redacted]	221.11 МБ 156.83 к пакетов	491.35 кбит/с 43.56 пакетов/с
	[redacted]	144.53 МБ 104.81 к пакетов	321.17 кбит/с 29.11 пакетов/с
	[redacted]	103.64 МБ 74.00 к пакетов	230.31 кбит/с 20.56 пакетов/с
	[redacted]	102.66 МБ 72.82 к пакетов	228.13 кбит/с 20.23 пакетов/с
	[redacted]	102.00 МБ 72.67 к пакетов	226.66 кбит/с 20.19 пакетов/с

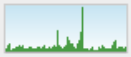
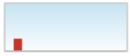


Ключ	Имя	Скорость	Статус	График	Получено	Передано
	ext0	100.00 Мбит/с	Up		12.75 Мбит/с 1.84 кпакетов/с	4.43 Мбит/с 1.69 кпакетов/с
	int0	100.00 Мбит/с	Up		4.43 Мбит/с 1.69 кпакетов/с	12.74 Мбит/с 1.84 кпакетов/с
	ext2	100.00 Мбит/с	Up		1.24 кбит/с 2.02 пакетов/с	52.94 бит/с 0 пакетов/с
	int2	100.00 Мбит/с	Up		52.95 бит/с 0 пакетов/с	1.24 кбит/с 2.02 пакетов/с
	ext1	0 бит/с	Down		0 бит/с 0 пакетов/с	0 бит/с 0 пакетов/с
	int1	0 бит/с	Down		0 бит/с 0 пакетов/с	0 бит/с 0 пакетов/с
	ext3	0 бит/с	Down		0 бит/с 0 пакетов/с	0 бит/с 0 пакетов/с
	int3	0 бит/с	Down		0 бит/с 0 пакетов/с	0 бит/с 0 пакетов/с

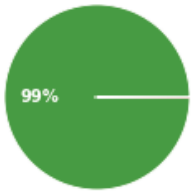
Интерфейс системы

Время -5м -1ч -24ч -7д От... Байты Пакеты

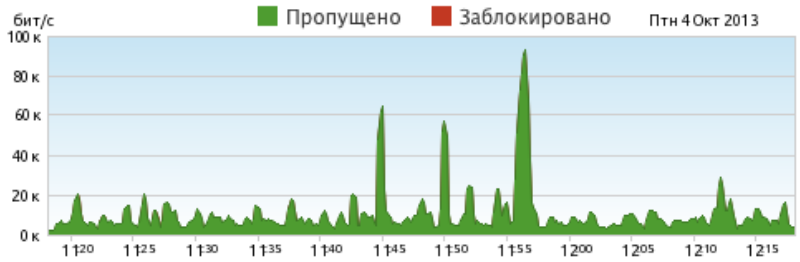
Обзор группы защиты

Всего Трафика		Всего: **4.33 МБ** **9.63 кбит/с**
Пропущено Трафика		Всего: **4.33 МБ** **9.62 кбит/с**
Заблокировано Трафика		Всего: **2.41 кБ** **5.35 бит/с**
Заблокировано Хостов		В среднем: **0.08 хостов**

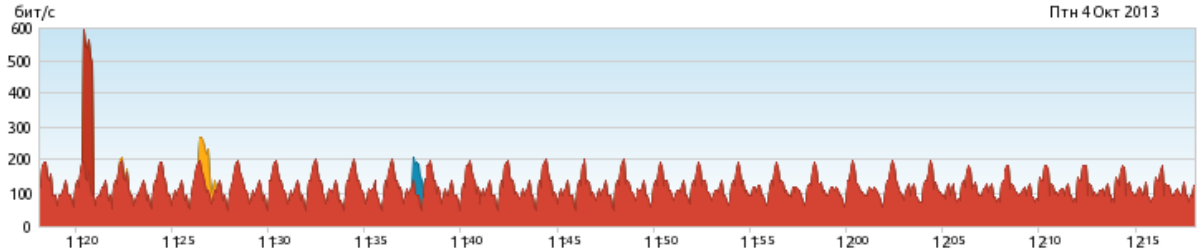
Суммарный трафик

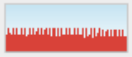
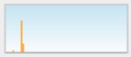


Общий трафик группы защиты

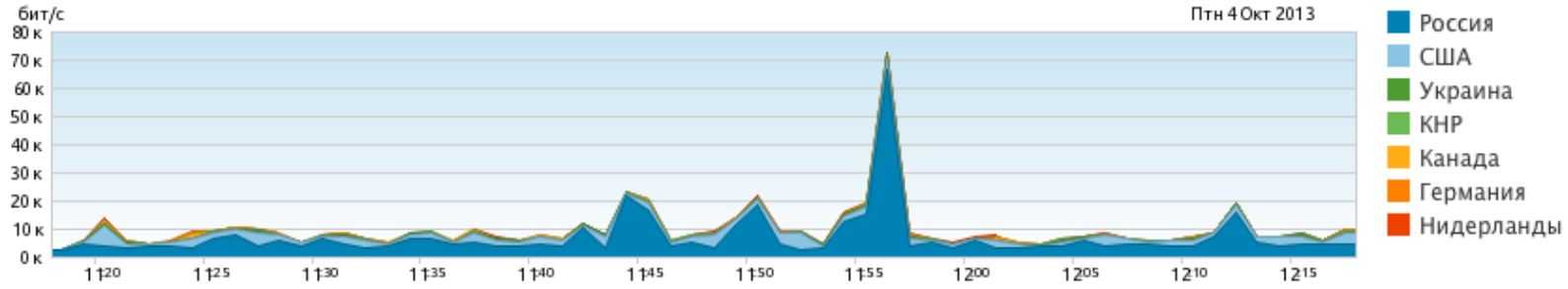


Категории атак



Ключ	График	Категория	Байт отброшено	бит/с отброшено	Пакетов отброшено	пакетов/с отброшено	
		Блокировка приватных подсетей	50.14 кБ	111.43 бит/с	177 пакетов	0.05 пакетов/с	
		Некорректные пакеты	1.50 кБ	3.33 бит/с	0 пакетов	0 пакетов/с	Подробности
		Разрыв соединений TCP	549 Б	1.22 бит/с	7 пакетов	0.00 пакетов/с	Подробности
		Очистка от некорректного DNS трафика	357 Б	0.79 бит/с	6 пакетов	0.00 пакетов/с	

География IP



Ключ	График	Страна	Пропущенный трафик	Отброшенный трафик	Доля в байтах	
		Россия	6.00 кбит/с	1.22 бит/с	65.71%	Черный список
		США	2.10 кбит/с	3.33 бит/с	22.99%	Черный список
		Украина	292.65 бит/с	0 бит/с	3.20%	Черный список
		КНР	222.08 бит/с	0.79 бит/с	2.44%	Черный список
		Канада	179.78 бит/с	0 бит/с	1.97%	Черный список
		Германия	99.03 бит/с	0 бит/с	1.08%	Черный список
		Нидерланды	80.41 бит/с	0 бит/с	< 1%	Черный список

Спасибо за внимание!

security-microtest.ru

security@microtest.ru

Илья Яблонко, CISSP
заместитель руководителя направления ИБ Микротест
iyablonko@microtest.ru
+7 965 545 09 66

Михаил Родионов
Enterprise sales manager, CIS
mrodionov@arbor.net
+7.916.934.61.99