Теперь это наш мир, мир электронов и выключателей, мир красоты бодов. У нас нет национальности, цвета кожи и религиозных убеждений. Вы ведете войны, убиваете, обманываете нас и хотите, чтобы мы верили, будто вы добродетели, а мы преступники. Да, я преступник, я виновен в любознательности. Вы можете поймать меня, но вам не остановить всех. Я хакер, и это мой манифест… (цитата из фильма Хакер)

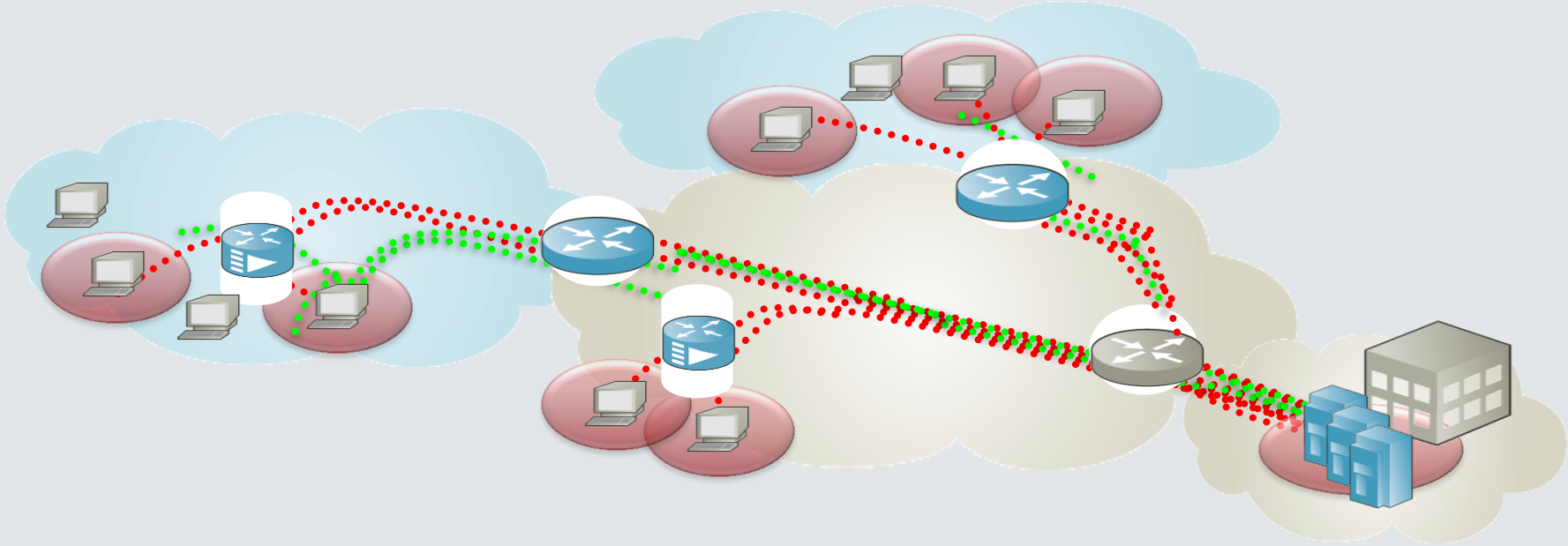
Злоумышленники похитили у европейского оператора Bitcoin на $1 млн
21-27 ноября, 2013

Anonymous заявили о взломе сайтов Microsoft

Злоумышленики атакуют серверы под управлением Apache Tomcat

Сайты полиции и резервного банка Австралии подверглись DDoS-атаке

Что такое DDoS атака?

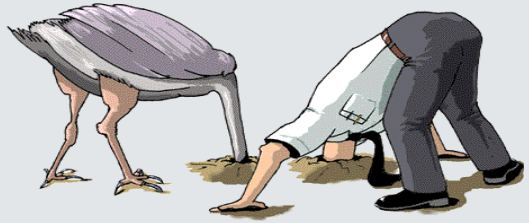


Во время **DDoS (Distributed Denial of Service)** атаки зараженные хосты (боты) из разных сетей перегружают ресурсы цели нелегитимным трафиком, вызывая **отказ в обслуживании** легитимных клиентов.

DDoS атака? Со мной это не случится…

Психология страуса

«Напуганный страус прячет голову в землю, полагая, что если он не видит опасность, то и опасность его не видит»

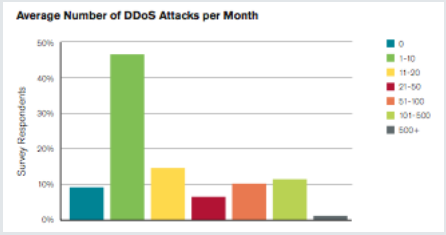


Таким же в прошлом было и восприятие DDoS-атак, но сейчас DDoS становится угрозой №1 по следующим причинам:

#1. Шире огласка
Известные DDoS атаки от «Anonymous» и «LulzSec»

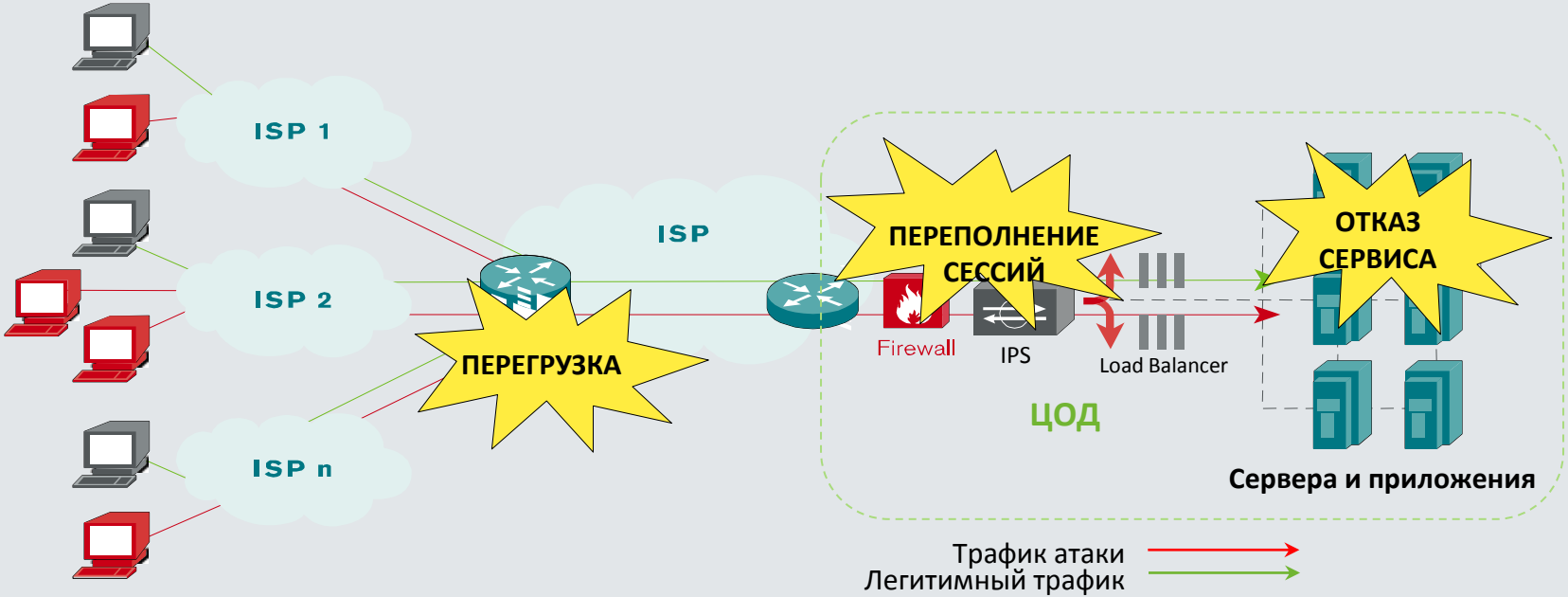
Ущерб в 2012г. – $2 трл.
(3.4% of G12 ВВП)
McKinsey & Co: Internet Matters Report May2011

#2. Выше риск
(Зависимость бизнеса от Сети)



#3. Больше атак и причин для них

Сложность современных DDoS атак

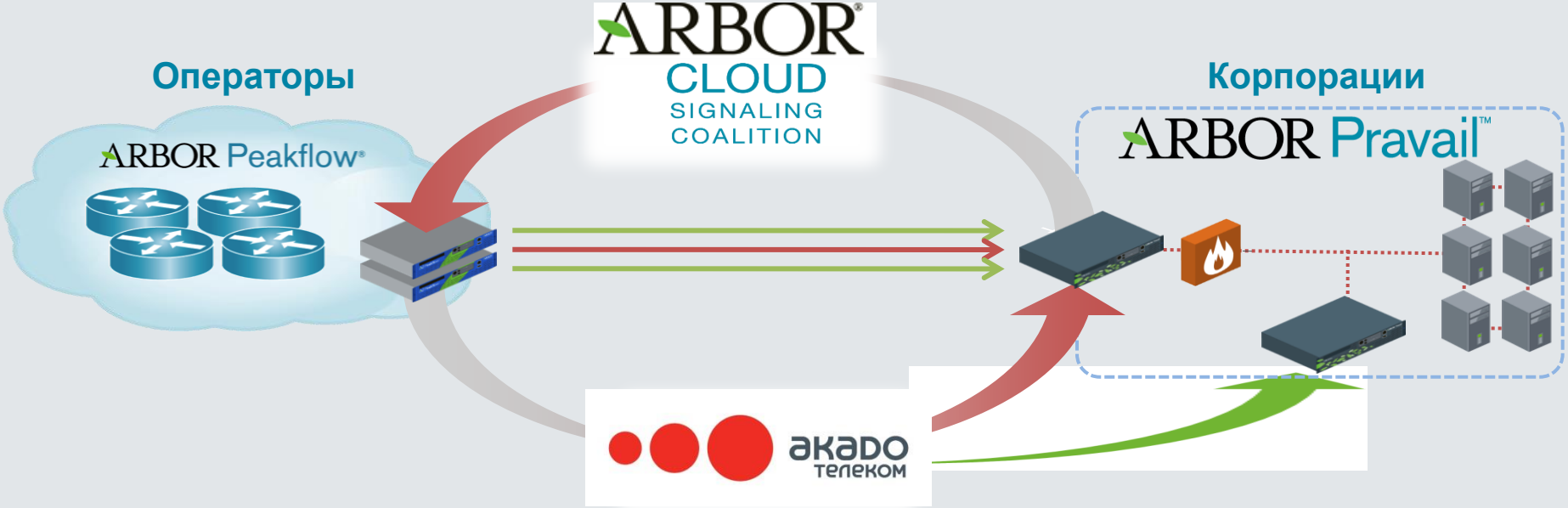


Сегодня DDoS вызывает (1) перегрузку канала, (2) переполнений таблиц сессий на stateful устройствах, (3) отказ сервиса – часто все вместе происходит при одной атаке и влечет **недоступность сервиса**.

Комплексная защита интернет-ресурсов от DDoS атак

Уникальное предложение от АКАДО

Облачная сигнализация, состоящая из операторской услуги АКАДО и оборудования находящегося на стороне клиента



Сервисы корпораций обладают полной защитой
от DDoS и сложных угроз.

Почему компания АКАДО-Телеком работает с ARBOR?

Производитель, которому доверяют защиту сетей самые крупные и требовательные компании мира

90%	Процент Tier 1 операторов, являющихся клиентами Arbor
105	Количество стран, в которых успешно внедрены решения Arbor
22.7 Тб/с	Трафик, отслеживаемый системой ATLAS в данный момент – это 25% всего Интернет трафика.
#1	Позиция Arbor на рынке оборудования защиты от DDoS в сегментах Carrier, Enterprise, Mobile – 61% всего рынка [Infonetics Research Декабрь 2011]
11 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

Предложение №1

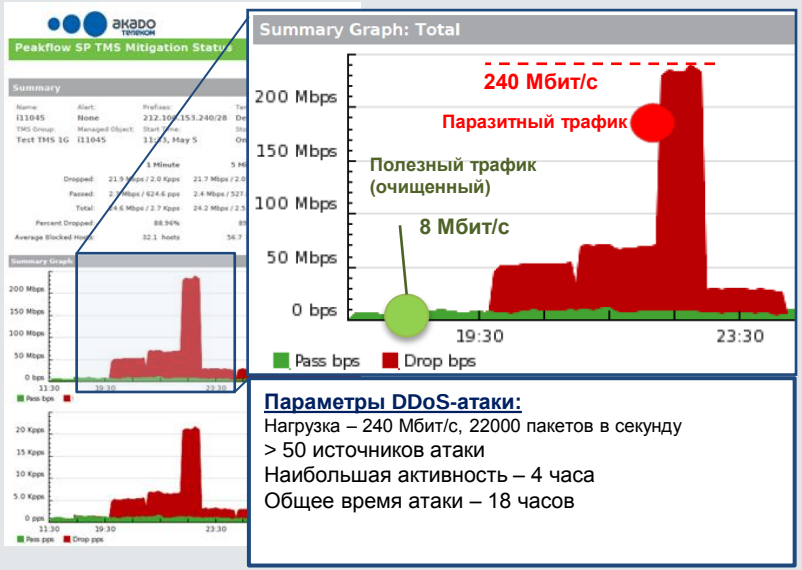
Операторская услуга защиты

«АКАДО Телеком» защитит ваши web-ресурсы от DDoS-атак из Интернет

Услуга защиты от DDoS-атаки включает:

- постоянный анализ Интернет-трафика
- обнаружение и локализацию DDoS-атак
- уведомление о начале и источнике DDoS-атаки
- автоматическую блокировку или по указанию клиента
- очистку Интернет-трафика посредством направления злонамеренного IP-трафика на устройство очистки
- предоставление ежемесячных отчетов

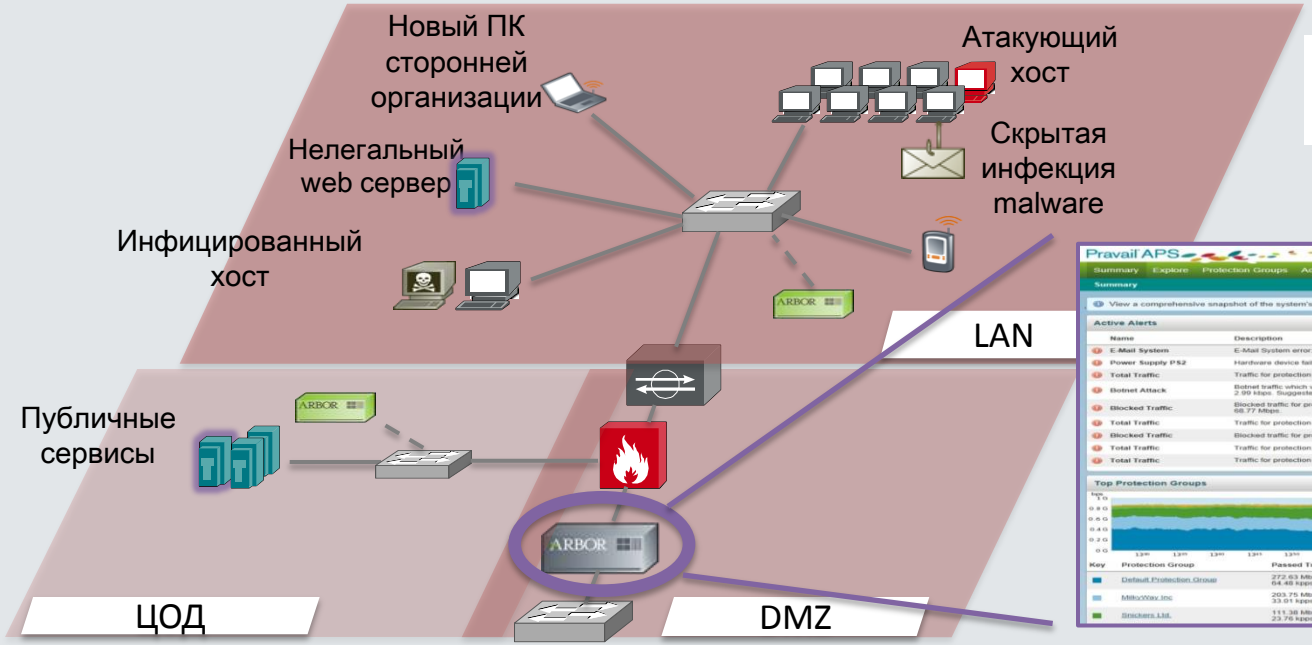
Пример отражения DDoS-атаки

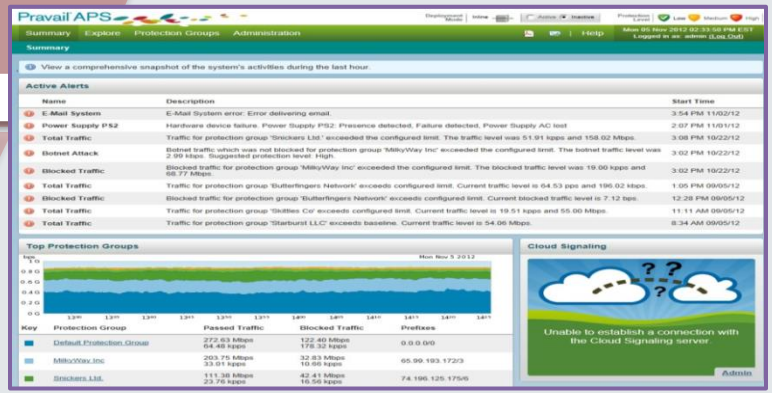


Параметры DDoS-атаки:
Нагрузка – 240 Мбит/с, 22000 пакетов в секунду
> 50 источников атаки
Наибольшая активность – 4 часа
Общее время атаки – 18 часов

Предложение №2

Защита с помощью оборудования Pravail





Моментальная защита от угроз доступности

Фаза 1: Установка на периметре

Фаза 2: Обнаружение угрозы online

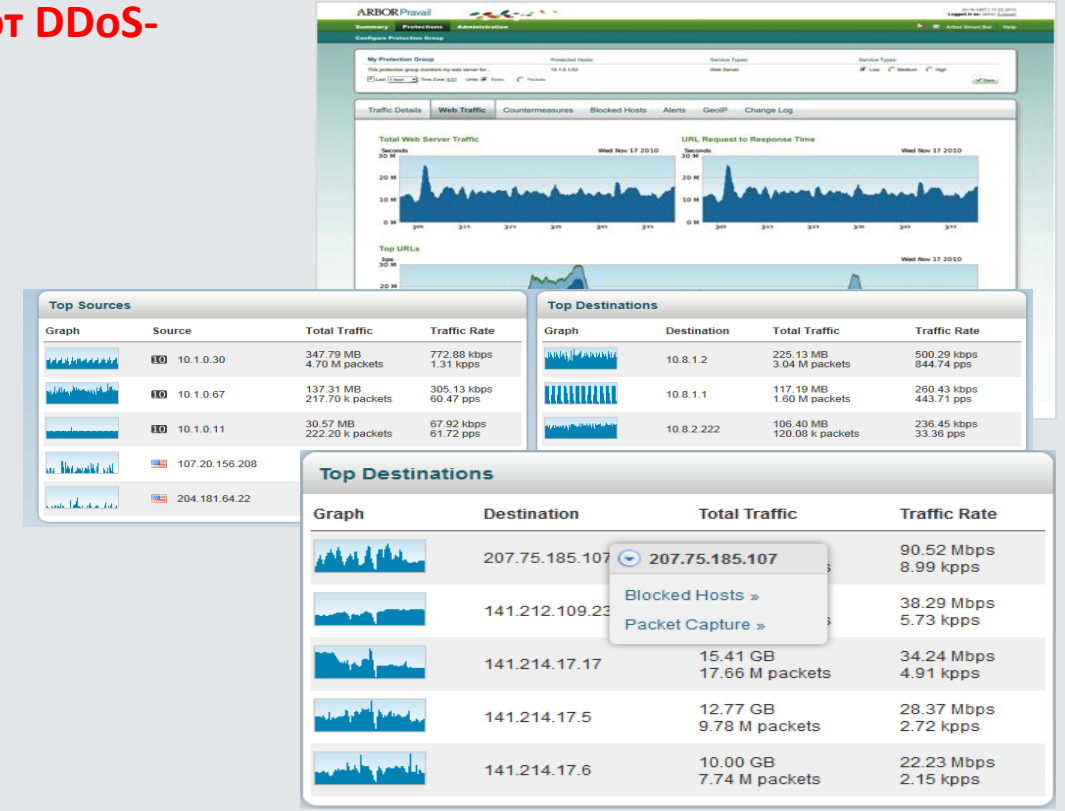
Фаза 3: Подавление угрозы online

Фаза 4: Извещение администратора online

Простая установка и мгновенная защита Pravail

Цель Pravail – 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

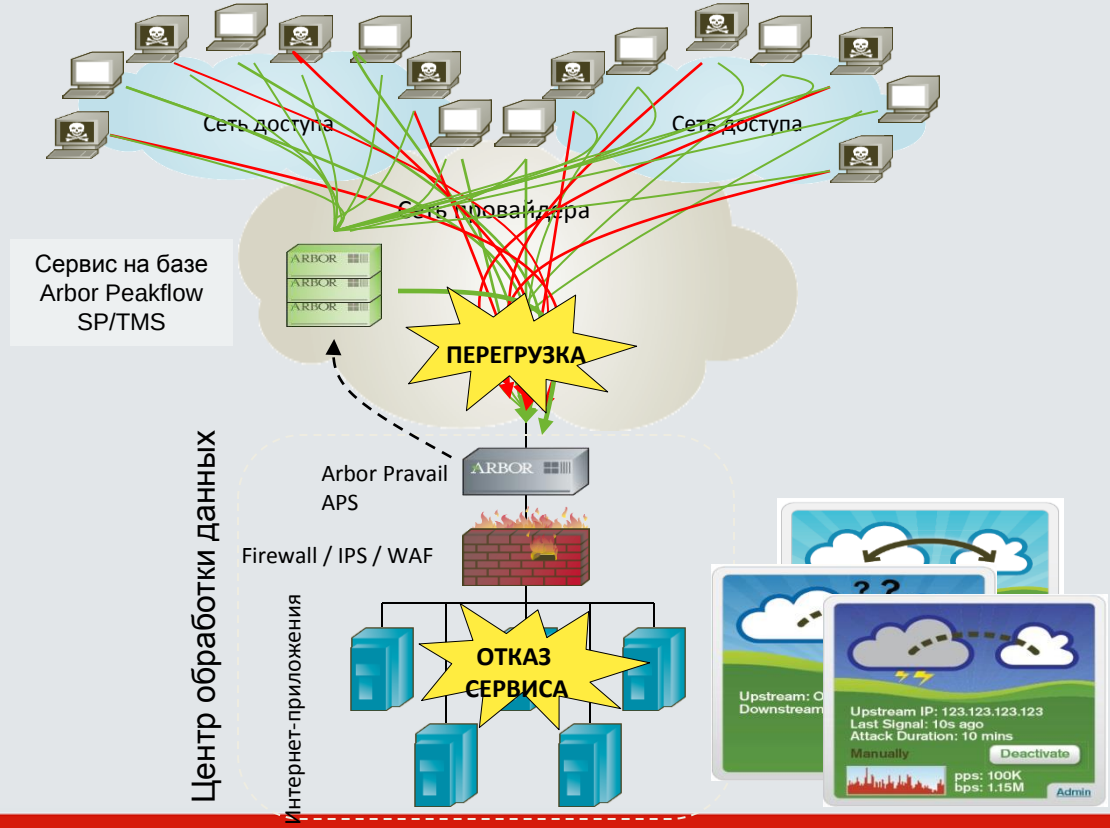


Предложение №3

Альянс Cloud Signaling

Подключение с помощью протокола облачной сигнализации.

1. Сервис работает нормально
2. Атака начинается и блокируется Pravail
3. Количество трафика атаки растет
4. Запуск облачной сигнализации
5. Клиент полностью защищен



Остановка сложных DDoS атак

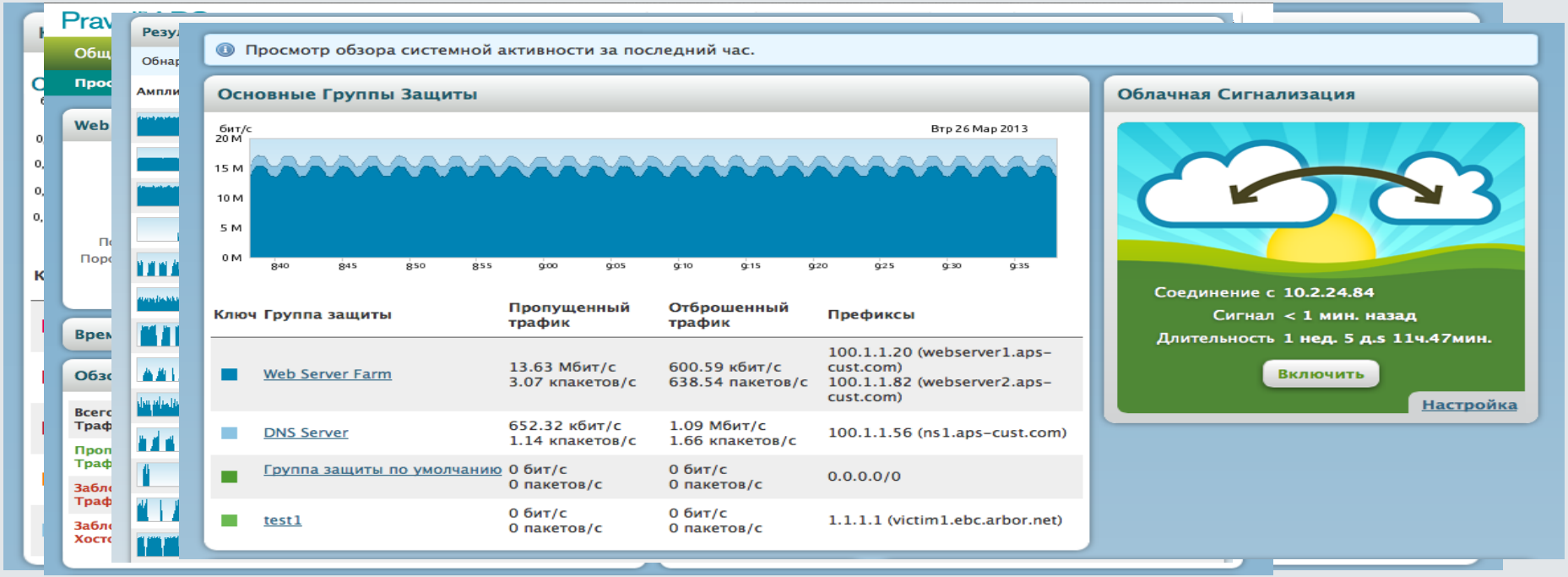
Блокируются все виды DDoS, включая прикладные атаки и атаки на TCP

- 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

Приятные мелочи

- Интерфейс и документация на русском языке



Решение АКАДО Телеком

Защита доступности: Очистка трафика от DDoS атак и трафика ботнетов

Анализ безопасности: Визуализация и анализ угроз для выявления и отслеживания зараженных хостов и фактов некорректного использования важных приложений, а так же чувствительных систем

Ситуационный анализ сети: Изучение и профилирование трафика для понимания контекста потенциальных сложных угроз

Виды сложных угроз	Защита и анализ сложных угроз
DDoS	Защита от DDoS и Облачная Сигнализация
Ботнеты	Защита от атак ботнетов
Воровство данных	Анализ на основе поведения
Неуправляемые устройства	Отслеживание пользователей
Динамические приложения	Глубокий анализ пакетов

Помните !!! Целью DSoS атаки является затруднение или полная остановка работы вашего веб-сайта или сервиса.

Какой будет цена потерь для бизнеса в случае остановки работы данного сервиса на 4, 8, 12, или 24 часа; на неделю; или даже на две недели?

Последние проведенные опросы относительно частоты и силы DDoS атак показывают определенный тренд, а именно – сила и изощренность атак постоянно возрастают. Среднее количество атак на бизнес составляет 1,6 в год, при этом среднее время простоя – 6,7 часа. Это эквивалентно одному 12 часовому простою вашего бизнеса вызванного DDoS атакой. Исследования компании «Ponemon» позволяют сделать вывод, что ущерб от DDoS атак превышает совокупный ущерб от всех прочих видов кибер преступности.

О компании

- Компания «КОМКОР» основана в 1992 году;
- Работает под торговой маркой «АКАДО Телеком», входит в Группу компаний «АКАДО»;
- «АКАДО Телеком» – один из трех крупнейших Интернет-провайдеров Московского региона;
- На базе собственной волоконно-оптической сети предлагает интегрированные телекоммуникационные решения для организаций различных сфер деятельности;
- Центр управления телекоммуникационной сетью- 100 рабочих мест дежурных операторов;
- Дата центр с уровнем резервирования Tier 3+.

Клиенты

АКАДО Телеком предоставляет услуги связи более 240 банкам.

К МЦИ БАНКА РОССИИ подключены более 200 кредитных организаций, среди наших клиентов:

АлтайЭнергоБанк, Альфа-Банк, Банк Петрокоммерц, Банк Российская финансовая корпорация, Банк Русский Стандарт, Банк Северный морской путь, Банк Столичный Кредит, ВнешТоргБанк, Газпромбанк,АБ «Россия», ГенБанк, «Коммербанк (Евразия)», ОТП-БАНК, Интрастбанк, Капитал-Москва Банк, КБ Росэнергобанк, МАК-Банк, МДМ-Банк, Международный акционерный банк, Московский индустриальный банк, Пробизнесбанк, Проминвестбанк, Промсвязьбанк, РБА Банк, Регионфинансбанк, Русский элитарный банк, РУССЛАВБАНК, СБЕРБАНК РОССИИ, Софрино Банк, Союзпромбанк, Трансинвестбанк, ТрансКредитБанк, УРАЛСИБ, УФК по Московской области, УФК по г.Москве, Финамбанк, Фьючер Банк и др.

Сеть КОМКОР

К сети «АКАДО Телеком» подключено ~ 80% зданий столицы

- Протяженность волоконно-оптических линий связи сети превышает 18 500 км
- Покрытие сети: Москва и города ближайшего Подмосковья в радиусе 30–50 км
- Плотность покрытия сети 200-500 м
- 390 магистральных и 25000 узлов доступа
- Внешние Интернет-каналы > 270 Гбит/с
- Телефонная емкость – 180 тыс. номеров
- Прямые стыки со всеми крупнейшими международными и российскими операторами

??????