Cisco ScanSafe

Защита web-доступа как услуга “из облака”

Павел Антонов, Инженер-консультант

paantono@cisco.com

Эволюция сервисов безопасности

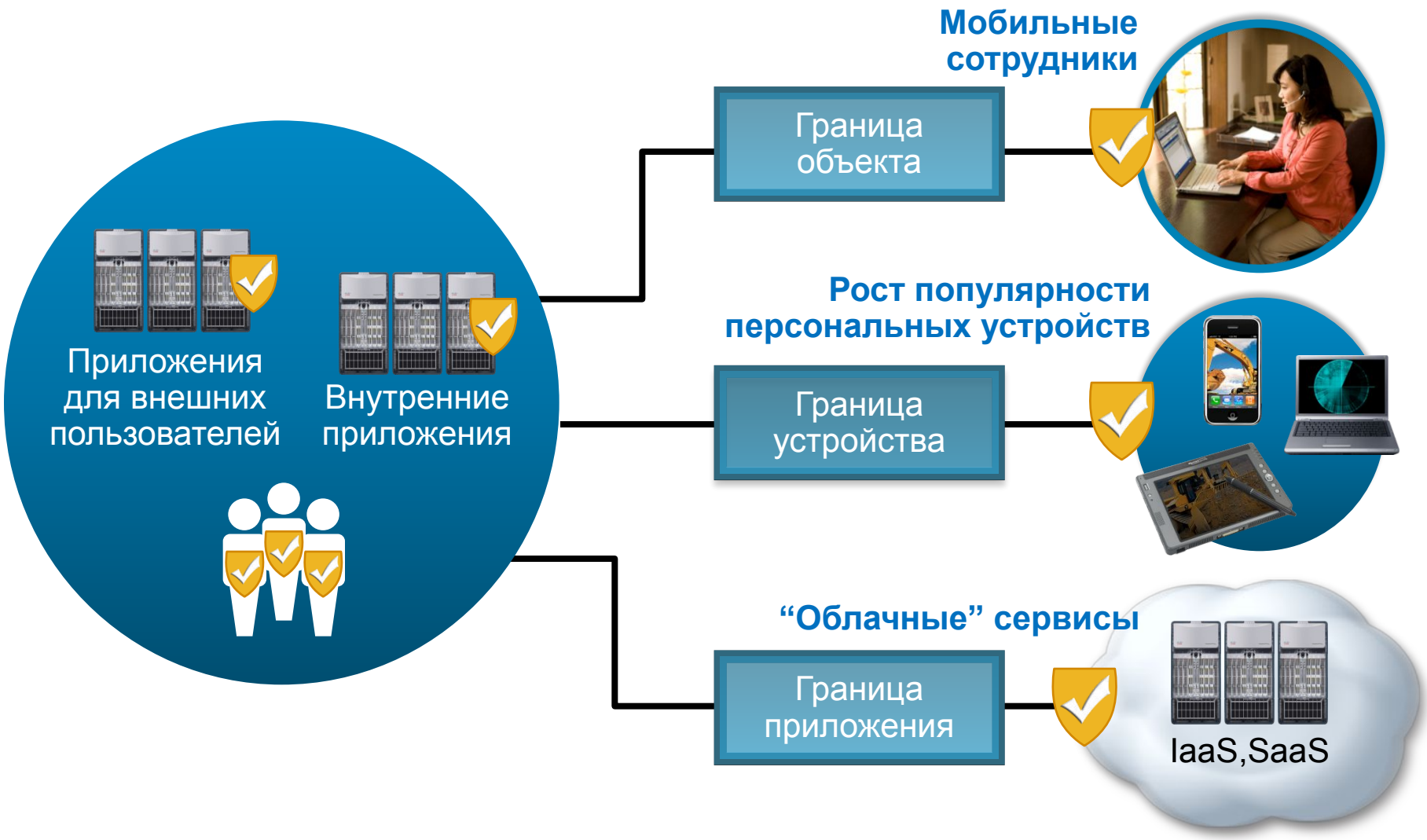
От приобретения оборудования до SaaS

Услуги из облака

Услуги Managed Services

Собственная инфраструктура

Изменение условий: размывание границ



Преимущества SaaS

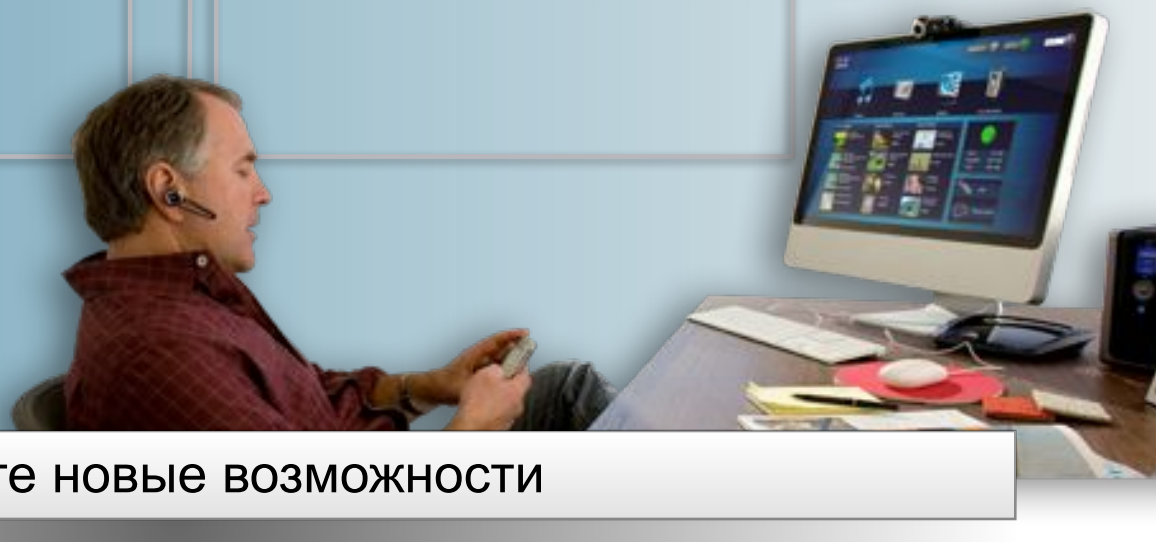
Простые и удобные средства управления

Предсказуемые OpEx

Минимальные сроки внедрения

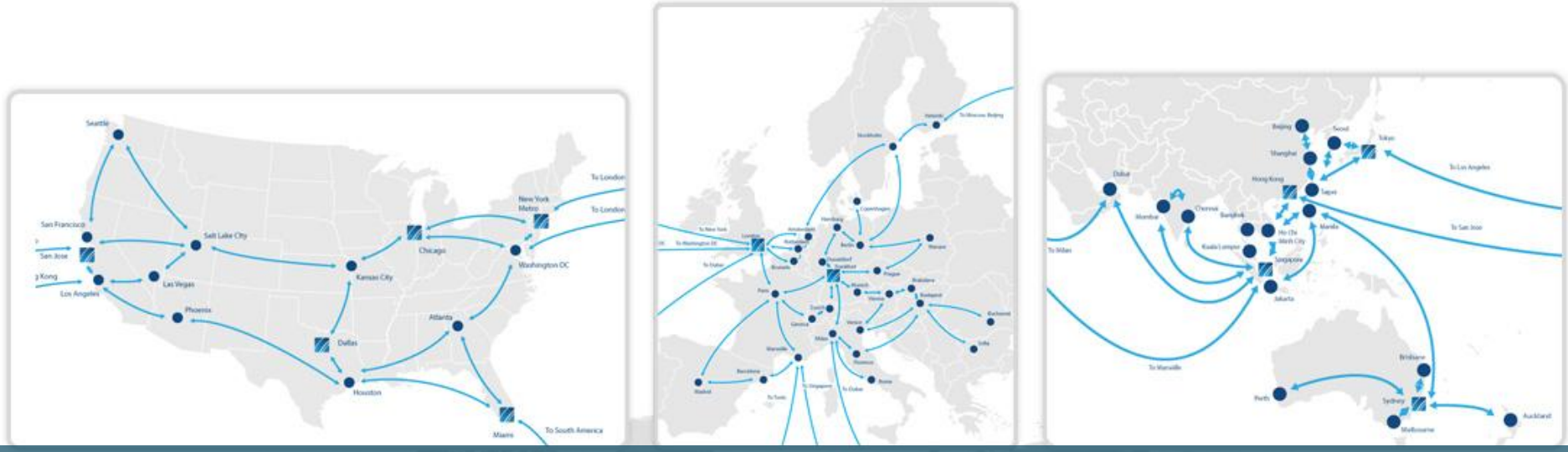
Нулевые CapEx

Освобождение ресурсов для бизнес задач



Откройте новые возможности

"Облачная" система безопасности Cisco



- Multi-tenant архитектура для обслуживания множества заказчиков
- Распределенная масштабируемая платформа с резервированием
- Постоянное наращивание производительности и внедрение новых ЦОД

- Глобальная система мониторинга угроз
- Встроенная система управления и формирования отчетов
- Глобальная платформа для мобильных пользователей

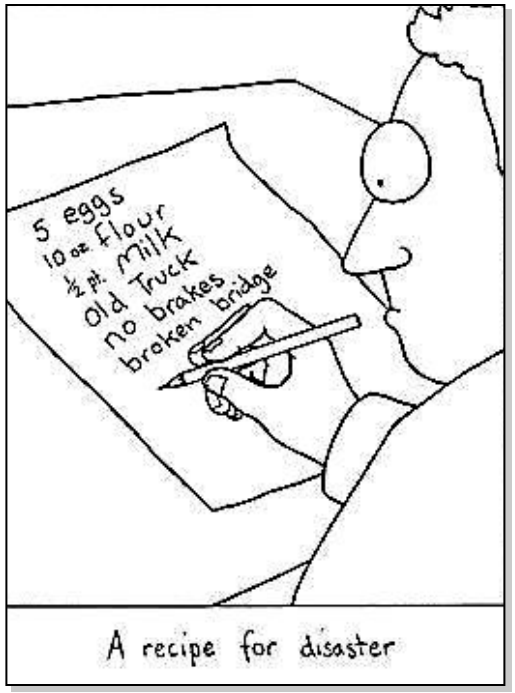
Эволюция Интернет угроз – фокус на Web

HTTP – это новый TCP?

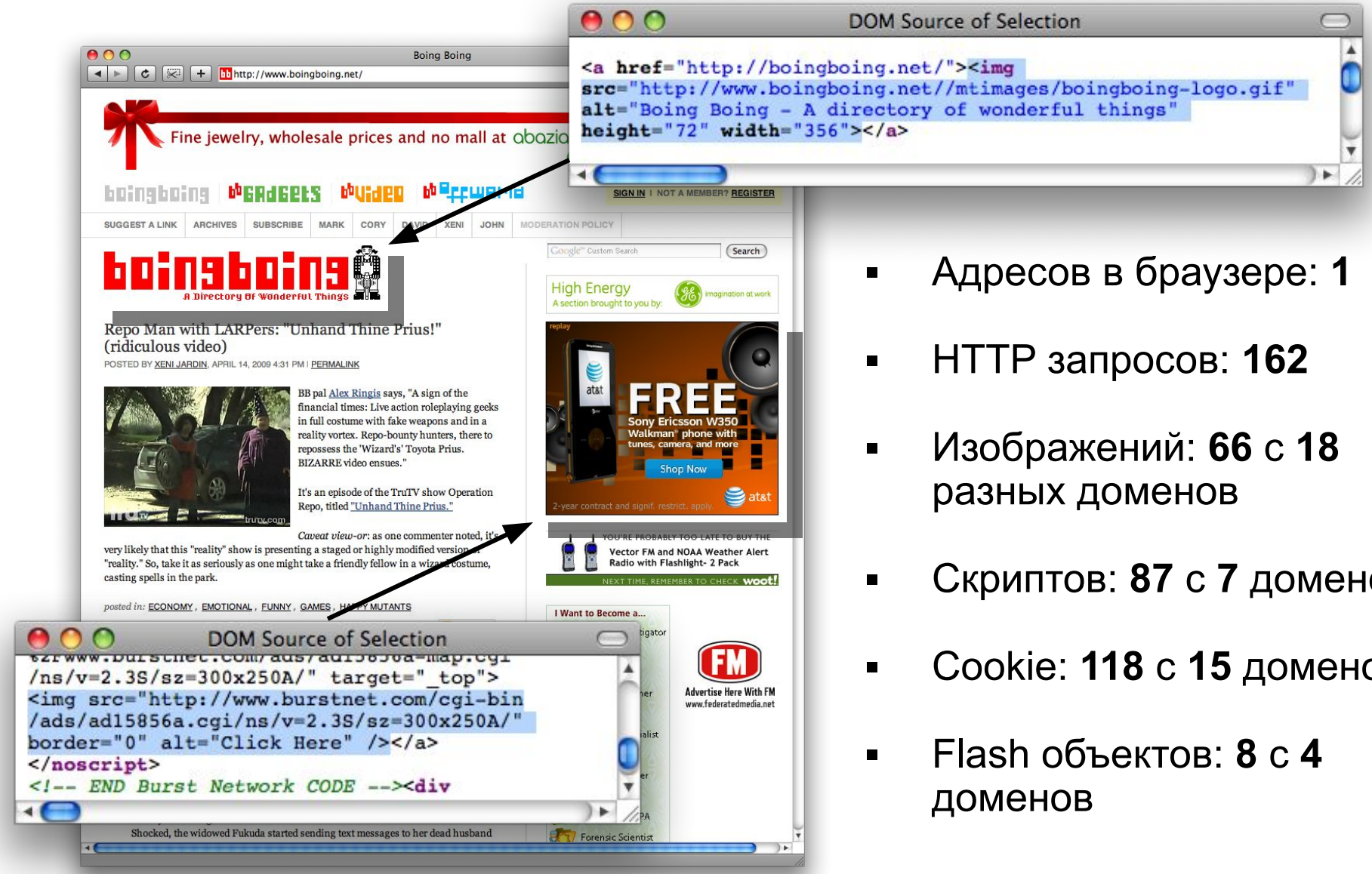
Web страница – рецепт заражения

Как работает web сайт?

1. HTML код содержит список ссылок на объекты
2. Получая этот список web-браузер скачивает с указанных источников все объекты, включая:
   - Файлы с изображениями
   - Скрипты
   - Исполняемый код
   - Другие web-страницы



Типичное поведение Вашего браузера



- Адресов в браузере: **1**
- HTTP запросов: **162**
- Изображений: **66** с **18** разных доменов
- Скриптов: **87** с **7** доменов
- Cookie: **118** с **15** доменов
- Flash объектов: **8** с **4** доменов

Уязвимая экосистема Web браузеров

SANS Top 20 Security Risks

http://www.sans.org/top20/#c1

- IE and Firefox vulnerable

  "…hundreds of vulnerabilities in ActiveX controls installed by software vendors have been discovered."

- Media Players & Browser Helper Objects (BHO)
  - RealPlayer, iTunes, Flash, Quicktime, Windows Media
  - Explosion of BHOs and third-party plug-ins
  - Plug-ins are installed (semi) transparently by website. Users unaware an at-risk helper object or plug-in is installed … introducing more avenues for hackers to exploit users visiting malicious web sites.

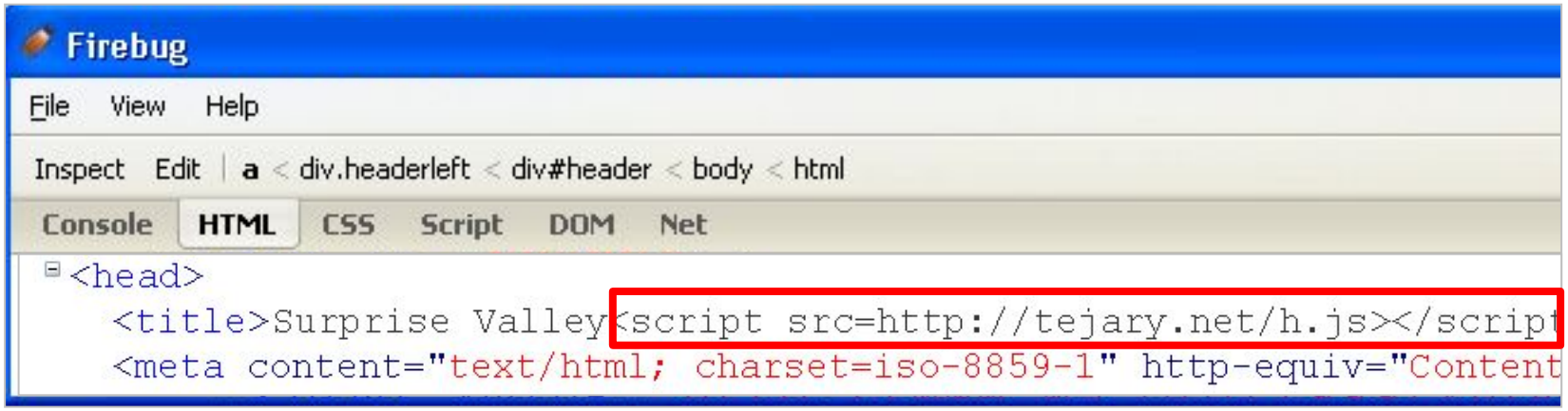
Уязвимые Web серверы

SANS Top 20 Security Risks
http://www.sans.org/top20/#s1

"Web application vulnerabilities **account for almost half the total number of vulnerabilities** being discovered in the past year**. These vulnerabilities are being exploited widely to convert trusted web sites into malicious servers serving client-side exploits and phishing scams."

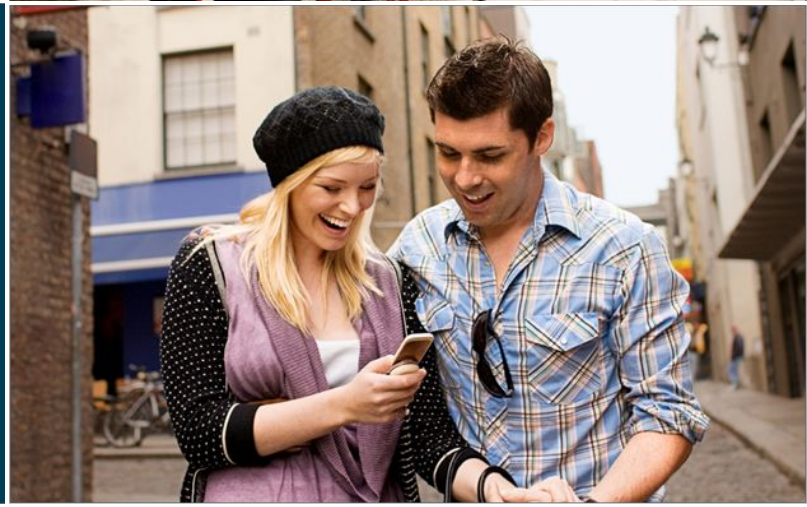
** including open-source and custom-built applications

Пример: зараженная web-страница



Скрытая ссылка на скрипт в HTML коде

Обзор сервиса ScanSafe



Кто такой ScanSafe?

ScanSafe

Профиль компании:

- Основана в 2004г.
- Пионер и мировой лидер в области SaaS услуг Web безопасности
- Клиенты - от SMB до Large Enterprise в более чем 100 странах
- 100% Uptime за всю историю предоставления услуги
- Является подразделением Cisco с Декабря 2009г.

Awards

c|net Security product of the year 2008

SC Magazine Awards 2009 Europe

SC Magazine RDS 07 RDS 08

Red Herring 100 Winner Europe

Check Point OPSEC Certified

Microsoft Gold Certified Partner

CISSP

2007 SIIA CODiE Winner

Customers

Rothschild

Shell

Disney

Bacardi

ICI

Standard Chartered

Louis Vuitton

IKEA

Quintiles Transnational

Partners

orange Business Services

at&t

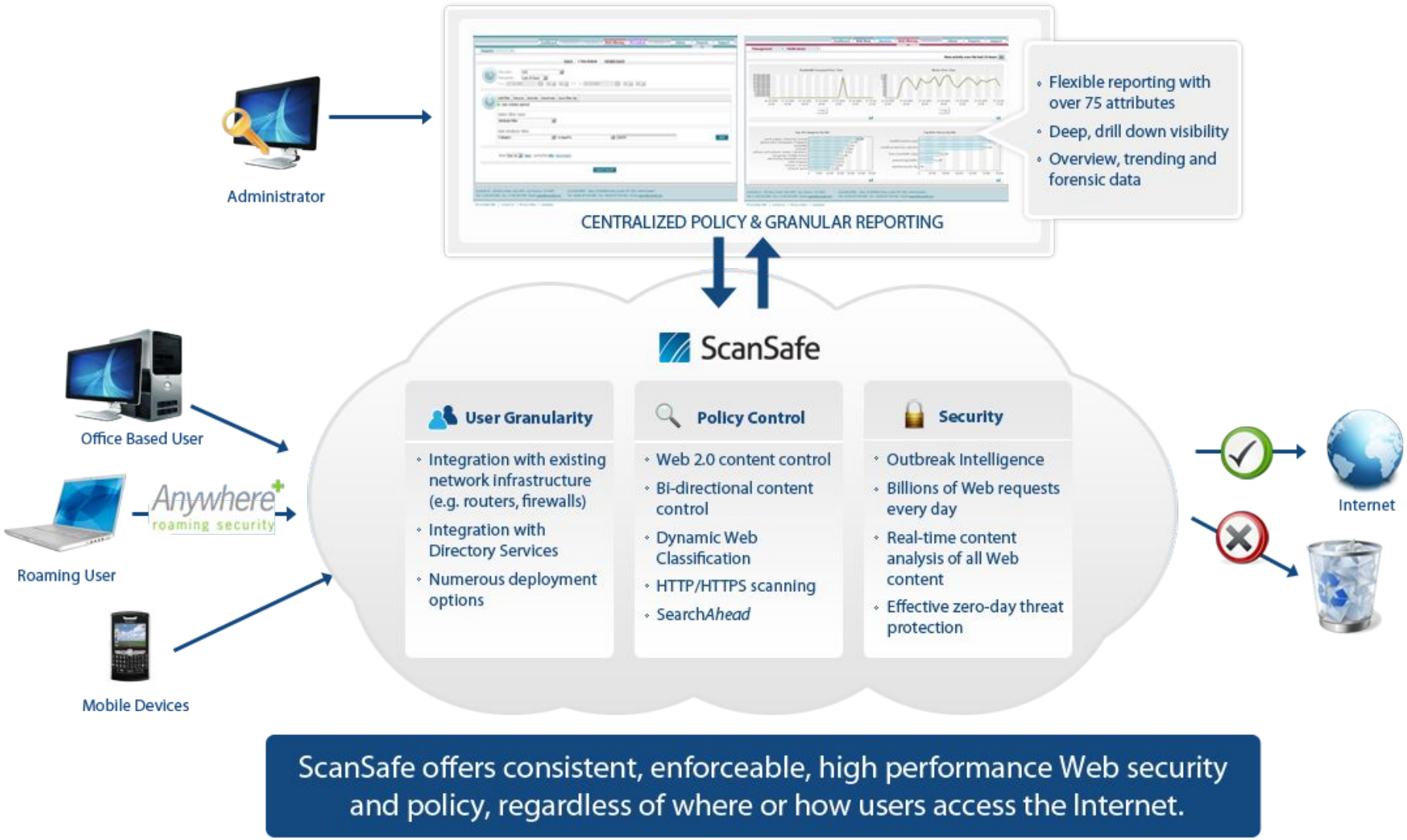
Google

Sprint

TELUS

NEC

Обзор решения



ScanSafe offers consistent, enforceable, high performance Web security and policy, regardless of where or how users access the Internet.

ЦОДы Cisco ScanSafe

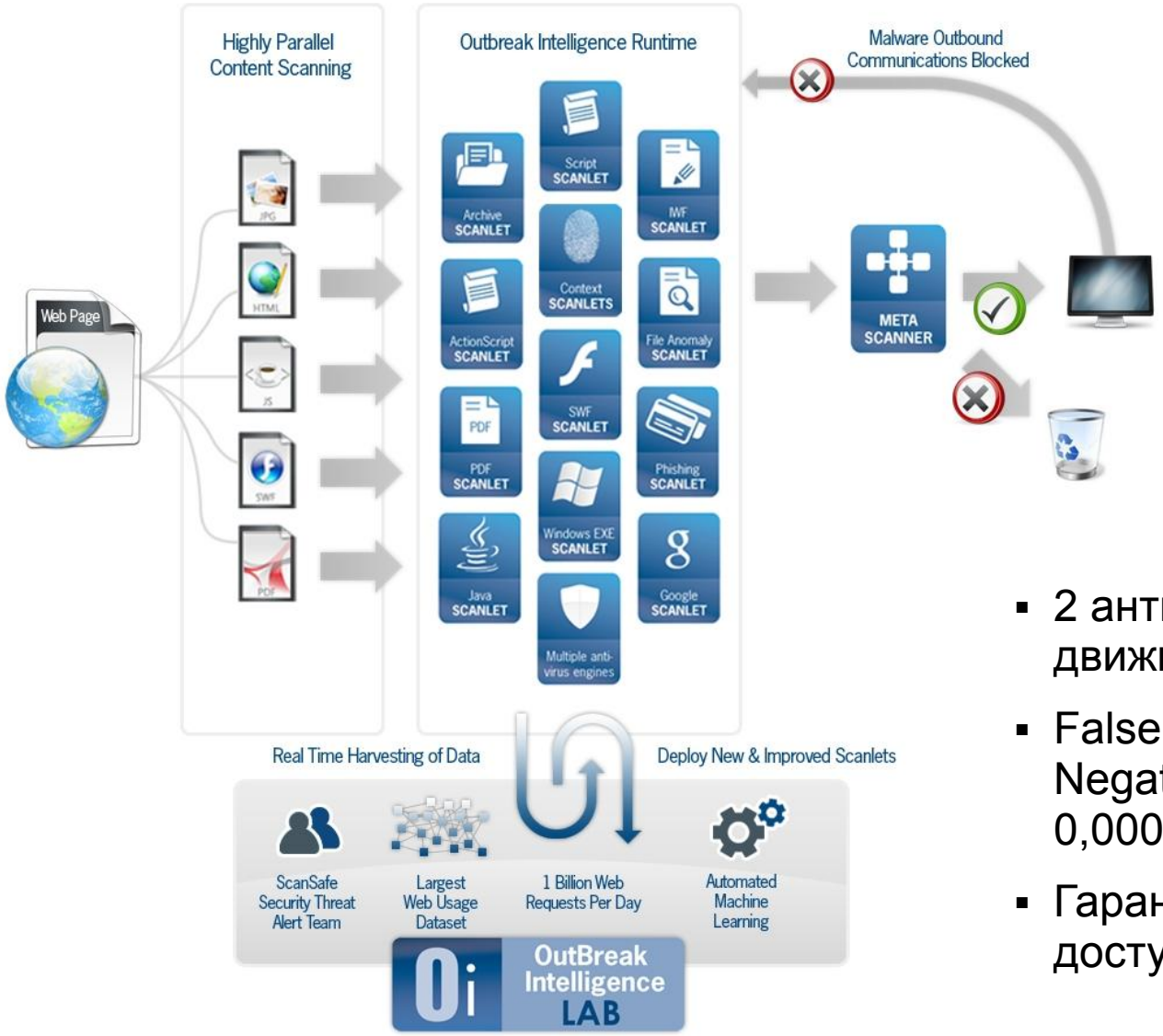
Надежность

- 15 ЦОДов
- 100% доступность сервиса за всю историю
- SLA по непрерывности и эффективности работы

Масштабируемость

- Multitenant архитектура
- Обрабатывает ~3Млрд. web-транзакций в день
- Постоянное масштабирование

Архитектура защиты от Web-угроз



- 2 антивирусных движка (Symantec+ЛК)
- False Positive \ False Negative rate < 0,0004%
- Гарантированная доступность – 99,999%

Фильтрация контента Web 2.0

- Традиционная URL-фильтрация
- Расширенная функциональность
  - Протоколы HTTPS, FTP over HTTP
  - DLP, «предупредить, но не блокировать» (AUP) и анонимизация
- Динамическая классификация неизвестных сайтов
  - За 1/1000 секунды
  - Эффективность детектирования сайтов для взрослых, криминальных и т.п. = 99%
- Обработка поисковых запросов Search*Ahead*
  - Классификация и уведомление пользователя

Как трафик попадает в облако

Опция 1 – при помощи имеющейся инфраструктуры заказчика

С изменениями настроек браузера:

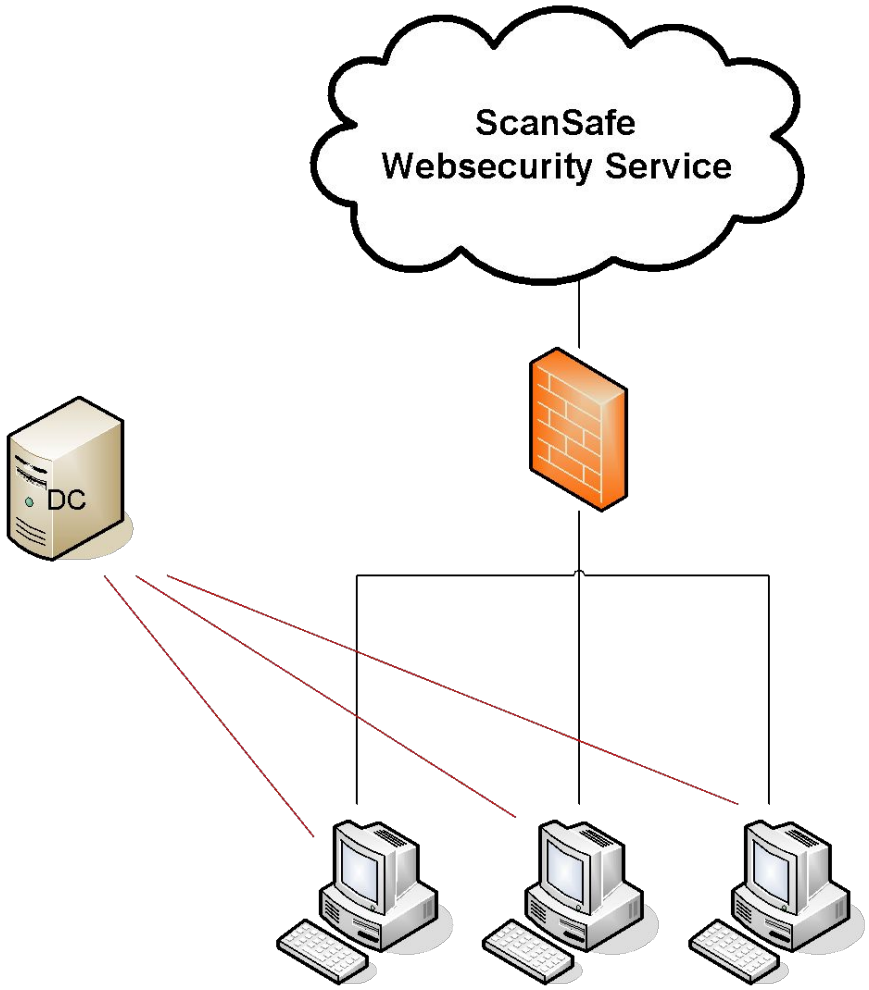
- Настройки Proxy загружаются на компьютеры из AD (GPO / PAC file) или по DHCP
- МСЭ блокирует исходящий HTTP трафик на все адреса кроме ScanSafe

Без изменения настроек браузера:

- Имеющееся у заказчика устройство перенаправляет трафик в облако помощи функций Cascade Proxy или Port Foreward

Опционально - Passive Identity Management (PIM):

- В HTTP-запросы пользователей добавляется защищенная (хеши) информация об имени пользователя/группы при помощи Login скриптов/GPO
- Прозрачно для пользователя

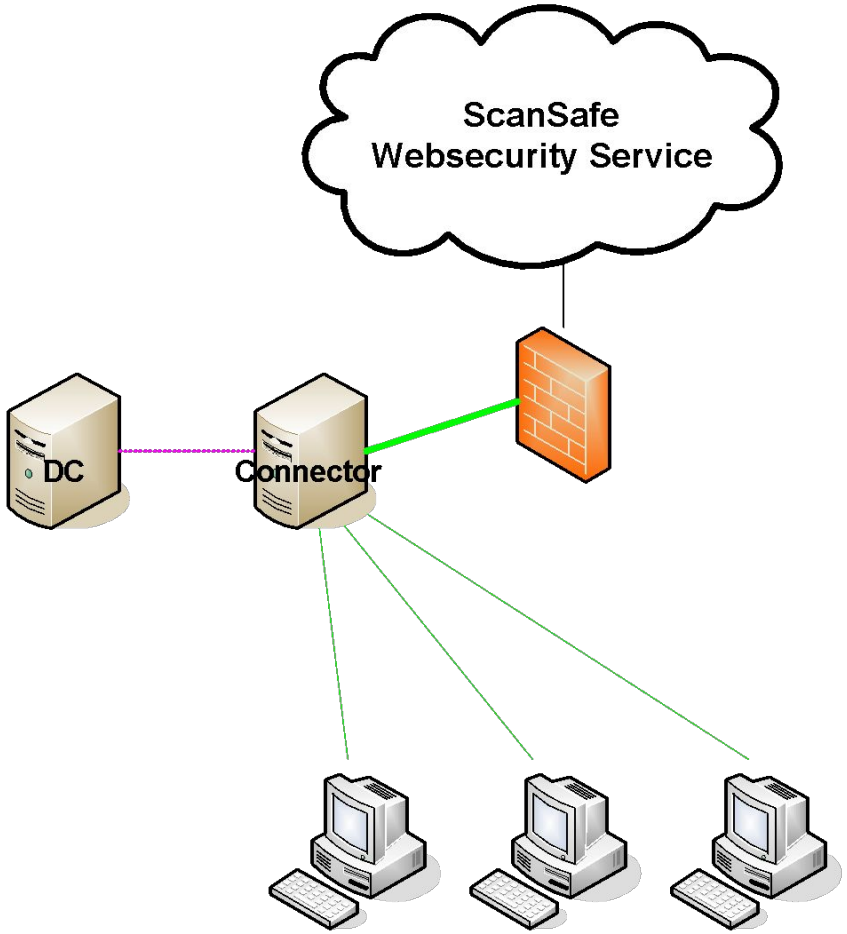


Как трафик попадает в облако

Опция 2 – при помощи Connector

ПО ScanSafe Connector

- Устанавливается и настраивается один раз, в дальнейшем не требует администрирования и обновлений
- Перенаправляет Web трафик в облако
- Отвечает за взаимодействие с AD и предоставляет в облако защищенную информацию о пользователе/группе
- В будущем – функциональность Connector интегрированная в маршрутизаторы и МСЭ Cisco



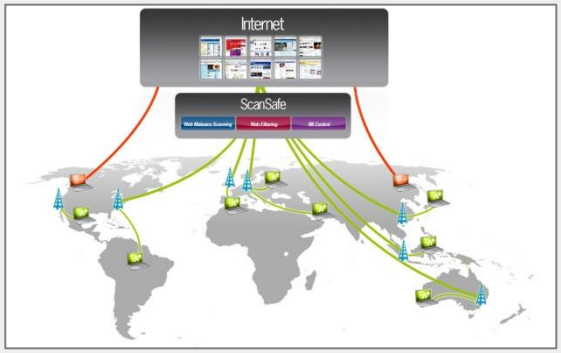
Как трафик попадает в облако

Опция 3 – клиент Anywhere+ для мобильных пользователей

Anywhere+

- Устанавливается как сетевой драйвер, незаметен для пользователя
- Автоматически определяет ближайший к пользователю ЦОД
- Перенаправляет Web трафик пользователя в облако
- Обеспечивает User/Group Granularity
- Защищен от выключения пользователем

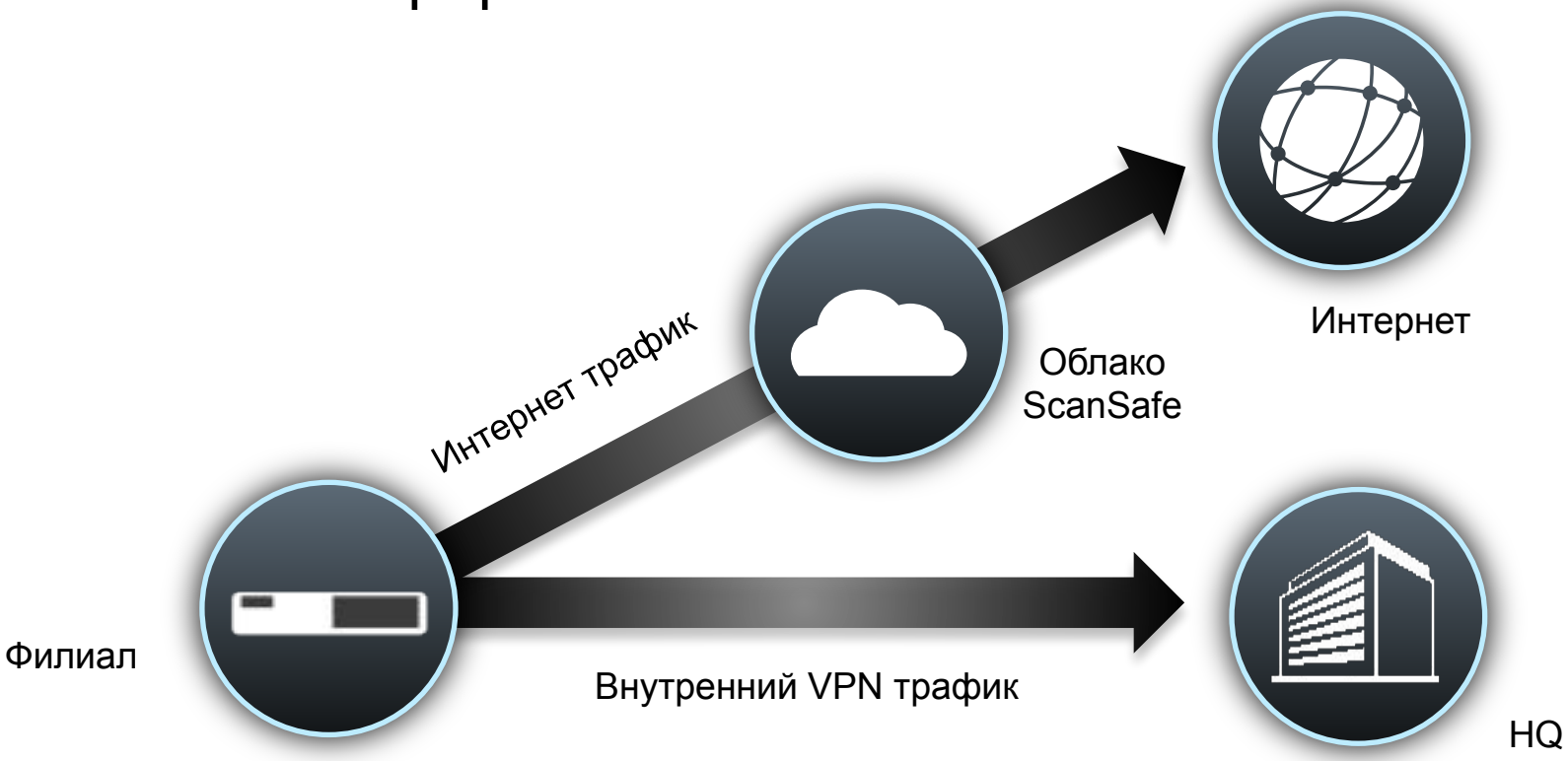
Факт: Мобильные пользователи только 17% времени в Интернет проводят в корпоративном VPN. Как контролировать оставшиеся 83%?



Anytime. Anyplace. Anywhere+

Интеграция ScanSafe с маршрутизаторами Cisco ISR G2

ISR G2 с интегрированным Connector



Удобное перенаправление web-трафика в облако ScanSafe
Гибкие возможности внедрения
Оптимальные пути прохождения трафика

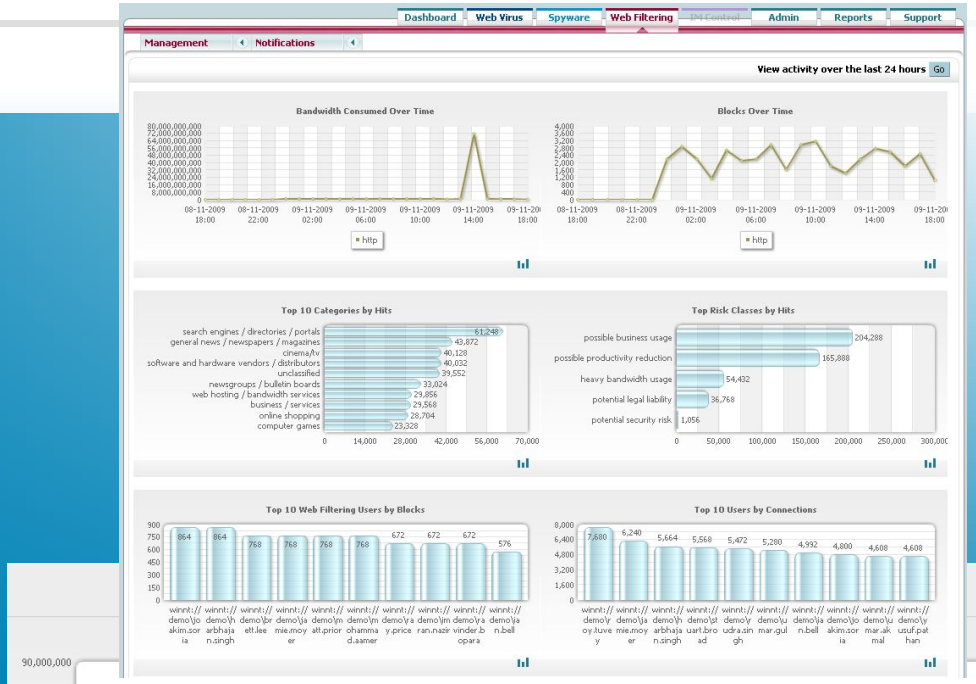
Единый клиент – Cisco AnyConnect 3.0

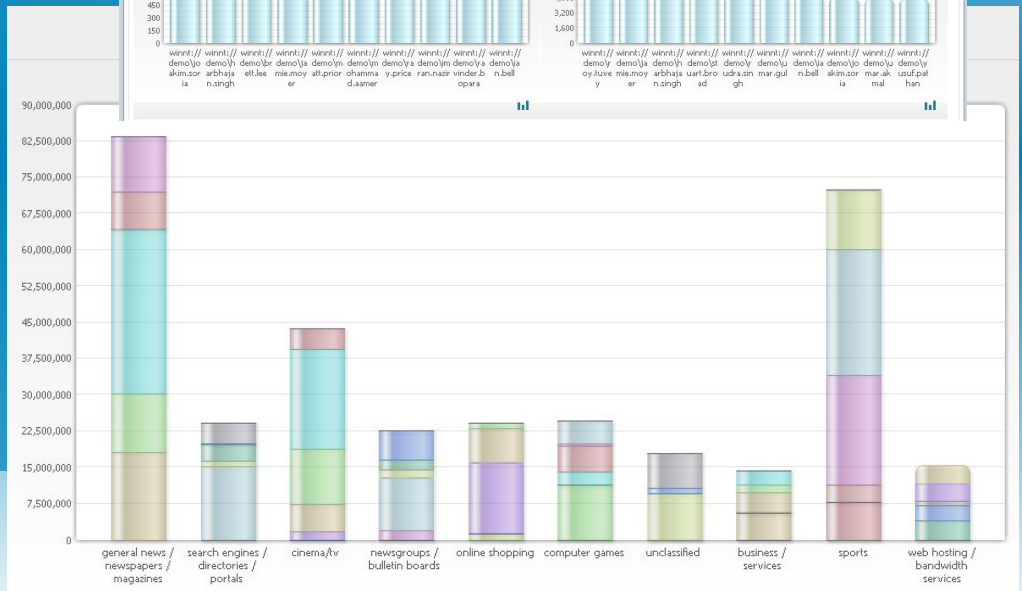
С интегрированным Anywhere+

Клиентский портал ScanCenter

Настройка политик, отчеты, мониторинг

- Все настройки выполняются на портале
- Более 5000 шаблонов отчетов
- Возможность создания своих шаблонов отчетов и политик
- 75 анализируемых параметров трафика
- Отчеты по расписанию
- Информация как по клиенту так и глобальные тенденции





Условия

- Полнофункциональный пробный доступ на 30 дней
- Варианты ценообразования:
- По кол-ву рабочих мест – несколько $ за одно рабочее место в месяц (зависит от общего числа рабочих мест в организации)
- По полосе пропускания – Стоимость за 1Мбит/с пропускаемого Web-трафика. Предназначено для отелей, кафе, аэропортов, магазинов.

Примеры использования

CUSTOMER SPOTLIGHT

Надежность

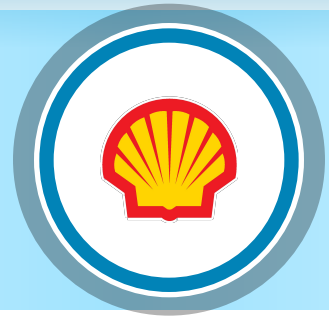
Задача

- Web 2.0 стал неотъемлемым инструментом бизнеса , необходима передовая защита

Результаты

- “Ряд механизмов безопасности лучше реализовывать в "облаке" для повышения уровня защищенности”

Децентрализация



Задача

- Для поддержки офисов по всему миру и мобильных пользователей требовались существенные ресурсы

Результаты

- “Достоинством решения является невиданная ранее простота развертывания"

Унификация

Задача

- Требовалось обеспечить развертывание политик и обеспечение отчетности по множеству объектов

Результаты

- "Контроль за ситуацией восстановлен, изменения политики распространяются практически мгновенно"

В чем преимущество ScanSafe?

- **Защита основного канала распространения угроз**: Защиты от ВПО, ограничение доступа к сайтам по категориям, DLP, проверка HTTPS
- **Предсказуемые затраты**: переход от CapEx к OpEx
- **Для клиентов с большим кол-во филиалов**: нет необходимости покупать много устройств или пропускать весь трафик через HQ
- **Для клиентов с мобильными сотрудниками**: возможность обеспечить защиту от угроз и политику доступа в Интернет вне зависимости от местоположения сотрудника
- **Унификация и централизация**: настройка политик и мониторинг из одной точки
- **Скорость внедрения:** Не нужно ждать оборудования и окончания его запуска

Спасибо!

http://www.facebook.com/CiscoRu
http://twitter.com/CiscoRussia
http://www.youtube.com/CiscoRussiaMedia
http://www.flickr.com/photos/CiscoRussia
http://vkontakte.ru/Cisco

Справочная информация

- “Облачная” безопасность Cisco
  http://www.cisco.com/go/cloudsecurity
- Решения и продукты Cisco в области ИБ
  http://www.cisco.com/go/security (eng)
  http://www.cisco.com/web/RU/products/vpn.html (рус)
- Центр ИБ Security Intelligence Operations
  http://tools.cisco.com/security/center/home.x
- Ежегодный отчет Cisco о угрозах ИБ
  http://www.cisco.com/en/US/prod/vpndevc/annual_security_report.html
- Брошюры по ИБ (рус) http://www.cisco.com/web/RU/broch.html