



Сетевые решения для безопасности широкополосных сетей



Павел Антонов

Технический Консультант

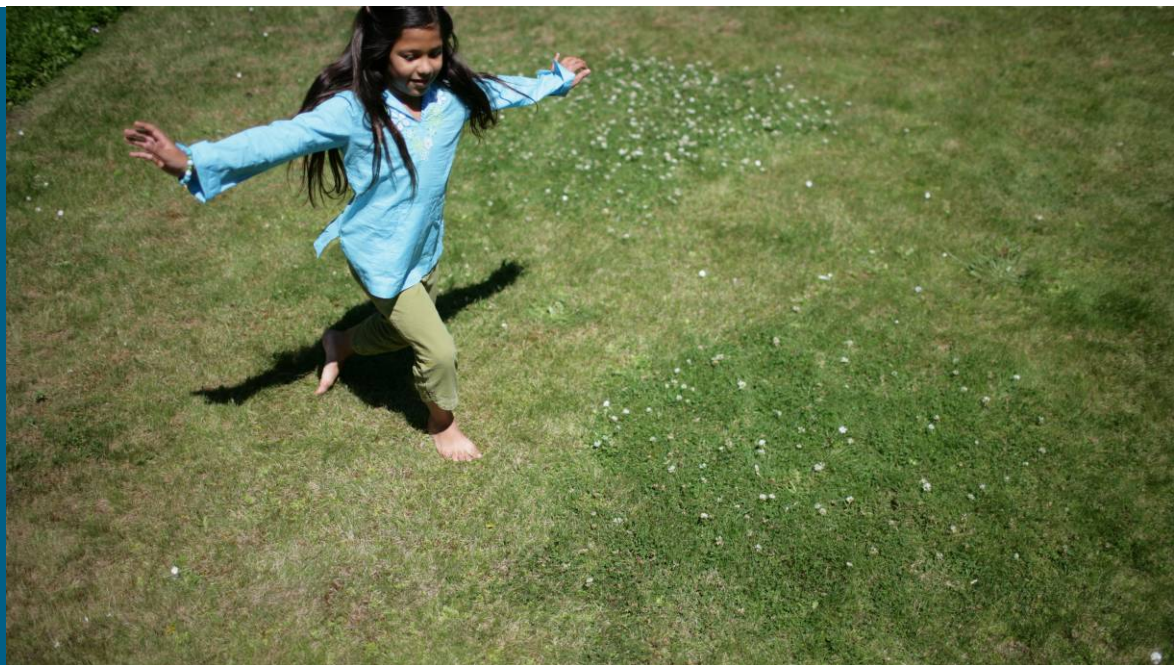
paantono@cisco.com

Cisco Networkers
2007

Содержание

- Картина безопасности широкополосных сетей
- Решения для защиты исходящего трафика и снижения издержек
 - Обнаружение
 - Предотвращение
- Решения для защиты входящего трафика и получения дополнительной прибыли
- Заключение

Картина безопасности широкополосных сетей



Многообразие угроз

Распространение вредоносного ПО

- Вирусы
- Черви
- "Троянские кони"



Использование вредоносного ПО

- Фишинг
- Навязчивая реклама
- Шпионское ПО
- Ботнеты



Виды атак

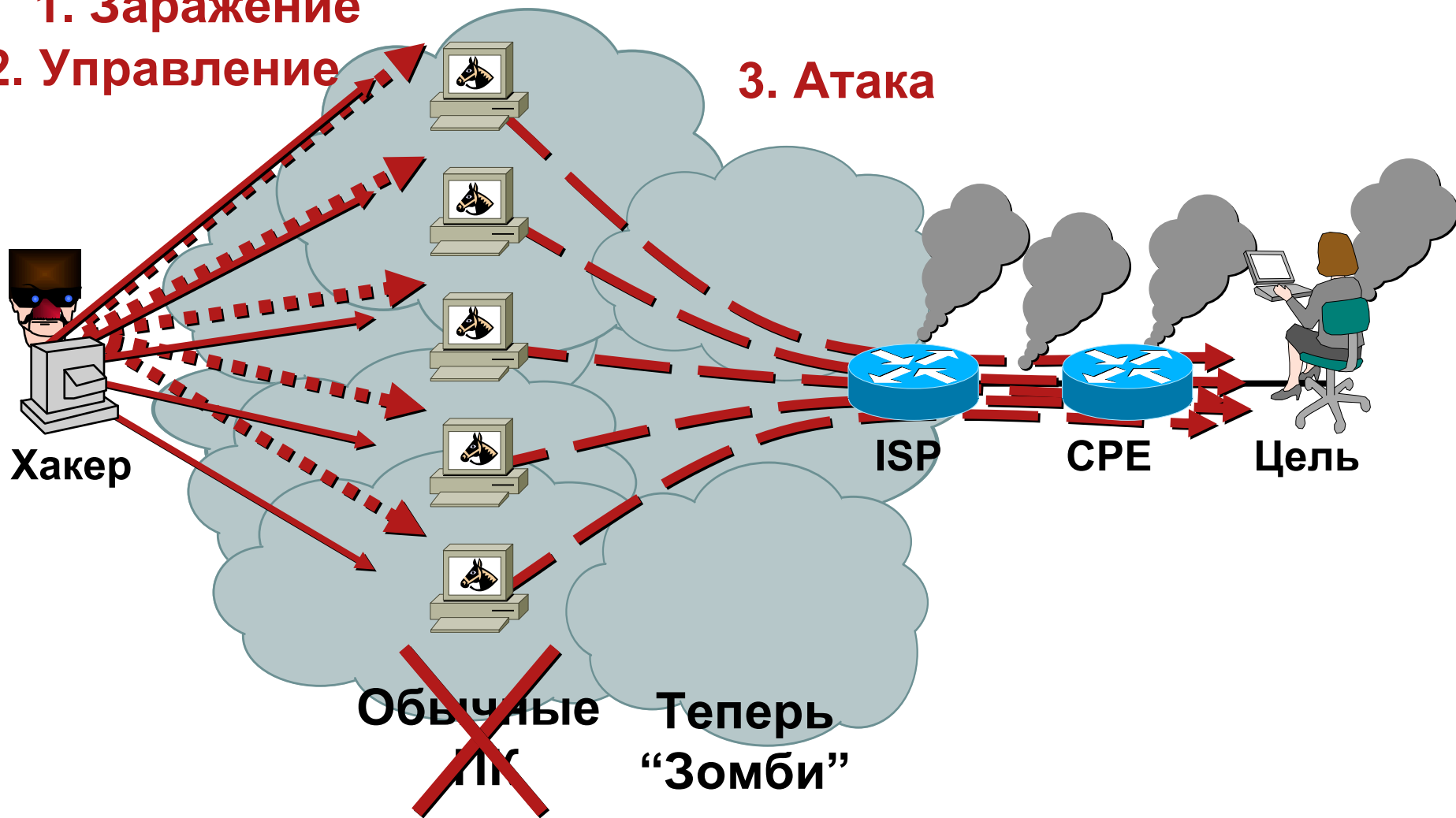
- Хищение информации
Мошенничество и кражи
- DDoS
Вымогательство
- Спам
-

Технология DDoS-атак

1. Заражение

2. Управление

3. Атака



Жизненный цикл ботнета



Zero-day атаки сложно остановить

В лучшем случае удастся ограничить их распространение

Основное направления развития – детектирование и нейтрализация червей

Применение коллекторов и приманок («honeypot»)

С переходом к P2P исчезнет роль контроллера

Выявить и нейтрализовать угрозу обычно удастся только на этом этапе

Подавление DDoS-атак защищает цель атаки, но зараженные хосты

Фильтрация спама – относительно зрелая технология

Лечение симптомов, но не причины!

Экономическое обоснование безопасности сетей ШПД

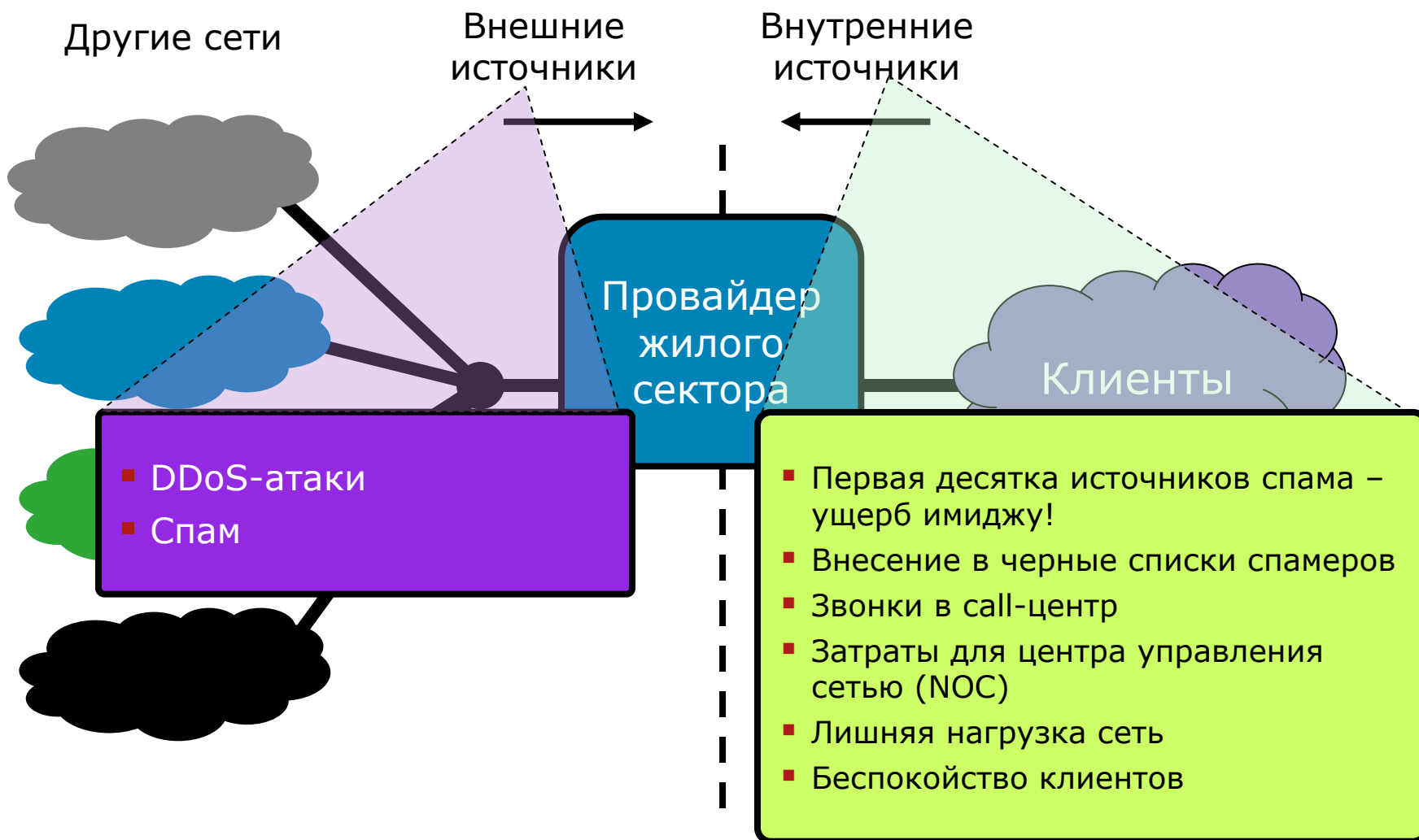


Цель – единая инфраструктура для поддержки всех функций!

Защита
исходящего
трафика
Обнаружение



Последствия заражения тысяч хостов для оператора связи



Что мы можем предпринять в мире широкополосных сетей?

- DDoS-атаки, черви и т.п. необходимо выявлять и нейтрализовывать на минимальном расстоянии от места вхождения в сеть.
- Нас волнуют зараженные **источники**
 - Точная идентификация
 - Масштаб
- Для выявления инфекции применяется **анализ трафика**
 - Статистический анализ
 - Выявление аномалий
 - Сигнатурный анализ
 - Репутация

Какой способ обнаружения выбрать?

- Способ обнаружения зависит от приоритетов

Обнаружение и блокирование основных источников угроз

Автоматизация исправлений для зараженных абонентов

Фокус на определенных видах атак и протоколов (например, спам)

Адаптируемость в условиях изменяющихся атак

Готовое решение

Собственное решение на основе ПО с открытым исходным кодом

Способы обнаружения

- **Телеметрия + корреляция**
DNS, NetFlow, Syslog, SNMP...
- **Мониторинг трафика**
Сигнатурный анализ, выявление аномалий и т.п.
- **Использование баз репутации**

Способы обнаружения Источники данных о репутации

- IronPort SenderBase <http://www.senderbase.org>
- DShield <http://www.dshield.org>
- MyNetWatchman <http://www.mynetwatchman.com>
- Shadowserver Foundation <http://shadowserver.org>
- CompleteWhois <http://www.completewhois.com>

Телеметрия и корреляция



DNS

- Служба DNS работает незаметно для нас, но за день мы обращаемся к ней многократно
- Многие виды приложений обращаются к DNS: веб-браузеры, серверы электронной почты и **вредоносное ПО** – "трояны" и боты на зараженных хостах
- Анализируя журналы и статистику DNS, можно выявить активность, требующую дальнейшего расследования

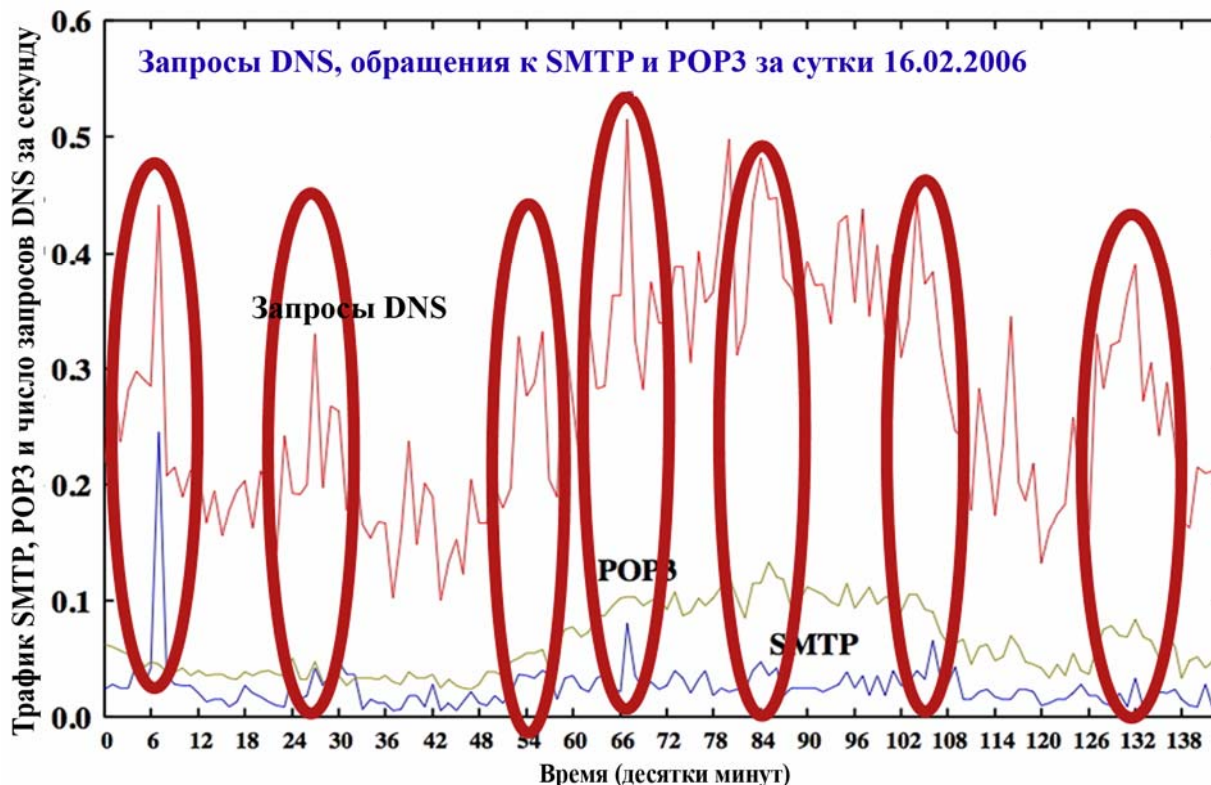
Корреляция DNS

- Корреляция журналов DNS с другими видами мониторинга (NetFlow, анализ трафика, журналы приложений и т.п.), позволяет обнаружить необычную активность в сети
- Спам-боты имеют собственные SMTP-движки и не обращаются к почтовым серверам провайдера
- Отправка запросов MX с хостов конечных пользователей – верный признак работы спам-бота
- Анализ запросов DNS и их корреляция с SMTP помогают подтвердить наличие спам-бота

Токийский университет “Кумамото” опубликовал ряд интересных работ по этой теме:

<http://www.cc.kumamoto-u.ac.jp/~musashi/musashicsec27.pdf>

Пример: корреляция DNS и SMTP



Источник: Университет Кумамото, Токио

Заметна четкая корреляция всплесков обращений к DNS и трафика SMTP! Всплески DNS говорят о работе спам-ботов

Практичность выявления угроз посредством DNS

- Журналы DNS – недорогое решение для выявления спам-ботов
- Отличный способ нахождения крупнейших источников спама в сети
- Сегодня есть бесплатные инструменты начального уровня

<http://dns.measurement-factory.com/tools/dnstop/>

<http://www.enyo.de/fw/software/dnslogger/>

- Располагая списком известных хостов – контроллеров ботнетов, можно анализировать запросы DNS для поиска зараженных абонентов, пытающихся выйти на связь с контроллером ботнета

Боты выявляются до рассылки ими вредоносного трафика!

- Появляются коммерческие продукты, использующие DNS для выявления аномалий (Trend InterCloud, Simplicita...)

Cisco NetFlow

<http://www.cisco.com/go/netflow>

- Статистика трафика для мониторинга сети и безопасности, планирования сетевых ресурсов, анализа трафика и IP-аккаунтинга
- В NetFlow версии 9 добавлены богатые функциональные возможности (Multicast, MPLS...), расширяющие базовые средства анализа IP-потоков в 5-й версии

Используются шаблоны для опеределенения экспортируемых данных

Основа для стандарта IETF – рабочая группа по экспорту информации о потоках IP (IPFIX)

Важное предварительное условие для Flexible Netflow

- Для сбора и анализа Netflow доступно множество бесплатных программных продуктов

<http://www.cisco.com/warp/public/732/Tech/nmp/netflow/partners/freeware/index.shtml>

Flexible NetFlow

Характеризация потоков регулируется пользователем
Принципиально новый подход к контролю потоков

- **Настраиваемый** и детализированный обзор сетевых параметров на 2-м – 7-м уровнях
- Архитектура с множественным кэшированием позволяет приложениям NetFlow отбирать необходимые им данные
 - Пример: для контроля безопасности и анализа трафика используются различные наборы данных NetFlow
- Расширение контроля безопасности сверх сегодняшних возможностей NetFlow
 - Создание виртуальных коллекторов NetFlow для анализа конкретных сетевых инцидентов. **Экспорт секций пакетов.**
- Экспорт ключевых наборов данных приложениям для содействия в поиске и устранении неполадок.
- Доступность с версии 12.4(9)T

Пример контроля безопасности с использованием Flexible NetFlow

- Система обнаружения отслеживает неклассифицированную информацию
- Если в сети обнаруживаются аномалии, формируется виртуальный кэш для сбора определенных сведений



- Кэши создаются по мере необходимости и накапливают конкретную информацию для подробной характеристики атаки
 - Экспорт секций пакетов для идентификации признаков атаки

Пример использования Flexible NetFlow

Пример настройки для контроля безопасности

```
flow record syn-floods
  match transport tcp flags syn
  collect counter packets
flow exporter export-to-server
  destination 172.16.1.1
  transport udp 90
flow monitor my-security-monitor
  record syn-floods
  exporter export-to-server
interface Ethernet 1/0
  ip flow monitor my-security-monitor input
```

NetFlow и обнаружение аномалий

- В систему вводятся **диапазоны сетевых IP-адресов**, позволяющие получить информацию о **направлениях, источниках и адресатах трафика**
- **Изучение** обычно выполняется на протяжении значительного периода времени, охватывающего интервалы максимальной и минимальной активности в сети
- Перед вводом в действие корректируются пороговые значения, интервалы блокирования оповещений и сообщений об ошибках, критерии поведения и другие параметры
- Существенное изменение скоростей или характеристик трафика со временем может потребовать подстройки
- Статистическое выявление аномалий выполняется такими продуктами, как Arbor (Peakflow SP), Narus (Secure Suite), Lancopе (StealthWatch Xe), Q1 Labs (QRadar) и т.п.

Мониторинг “живого” трафика



Обнаружение конкретных видов атак

■ Спам

Пересылка SMTP-трафика на основе политик (PBR) с отдельных портов на выделенный сервер фильтрации спама

Весь SMTP-трафик анализируется в **исходящем направлении** – просто односторонняя переадресация

Подробный анализ сводит к минимуму ложные срабатывания

Отчетности позволяют найти как основные источники спама, так и отдельные зараженные узлы

Нагрузка на сеть невысока – для большинства случаев достаточно пропускной способности 1 Гбит/с

Применение ограничено только обнаружением спама (очевидно)

Универсальное обнаружение атак

- “Глубокий” анализ пакетов (DPI)

Устройство следит за всем трафиком без переадресации

Анализ обычно является двусторонним

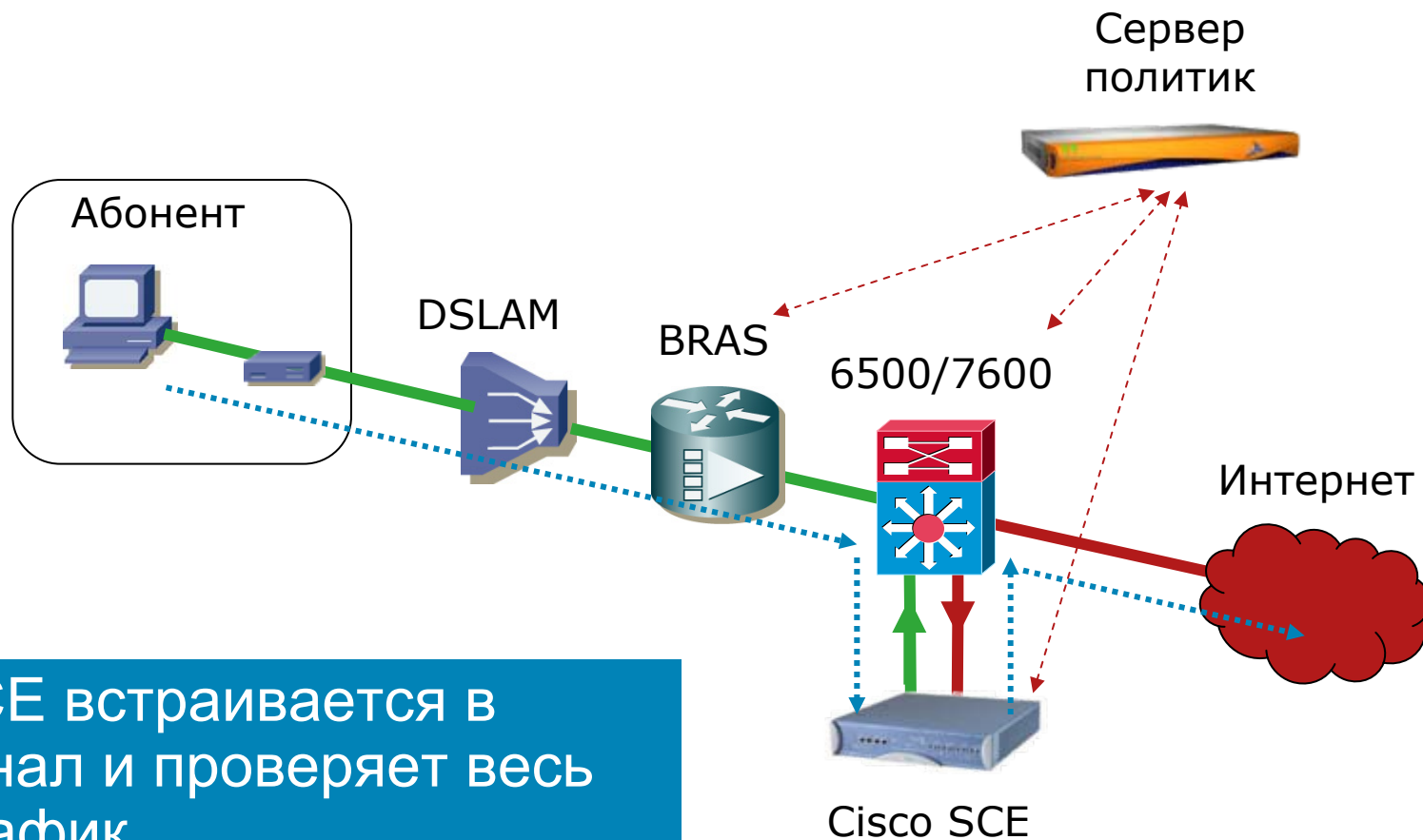
Пропускная способность должна составлять несколько Гбит/с

Сигнатурный анализ, Статистический анализ, Выявление аномалий

Высокая гибкость: выявление аномалий возможно для любых протоколов

Cisco SCE

Расположение в сети



Cisco SCE

Обнаружение

- **Спам-боты – выявление на основе анализа SMTP**

 - Чрезмерно большое число SMTP-соединений с одного адреса

- **DDoS-атака – выявление по аномалиям трафика**

 - Аномальное число соединений от одного внутреннего адреса один внешний адрес

 - Аномальное число соединений от нескольких внутренних адресов один внешний адрес

- **Сканирование/Распространение – выявление по аномалиям трафика**

 - Аномальное число соединений от одного хоста на один или несколько других хостов:

 - Несколько портов, один адресат

 - Один порт, несколько адресатов

- **Заражение червями – выявление по сигнатурам**

 - Динамическая загрузка сигнатур в SCE посредством редактора сигнатур

 - Сигнатуры создаются вручную – компания Cisco в настоящий момент НЕ предоставляет сигнатуры для SCE

Обнаружение аномалий средствами SCE

- Трафик хоста классифицируется как аномальный, если скорость установления соединений превышает порог **или** скорость установления подозрительных (односторонних) соединений превышает порог **И** доля подозрительных соединений превышает порог

- Настройка отдельных порогов выполняется на следующих уровнях:

Тип аномалии: сканирование, DoS, DDoS

Интерфейс (абонент / сеть)

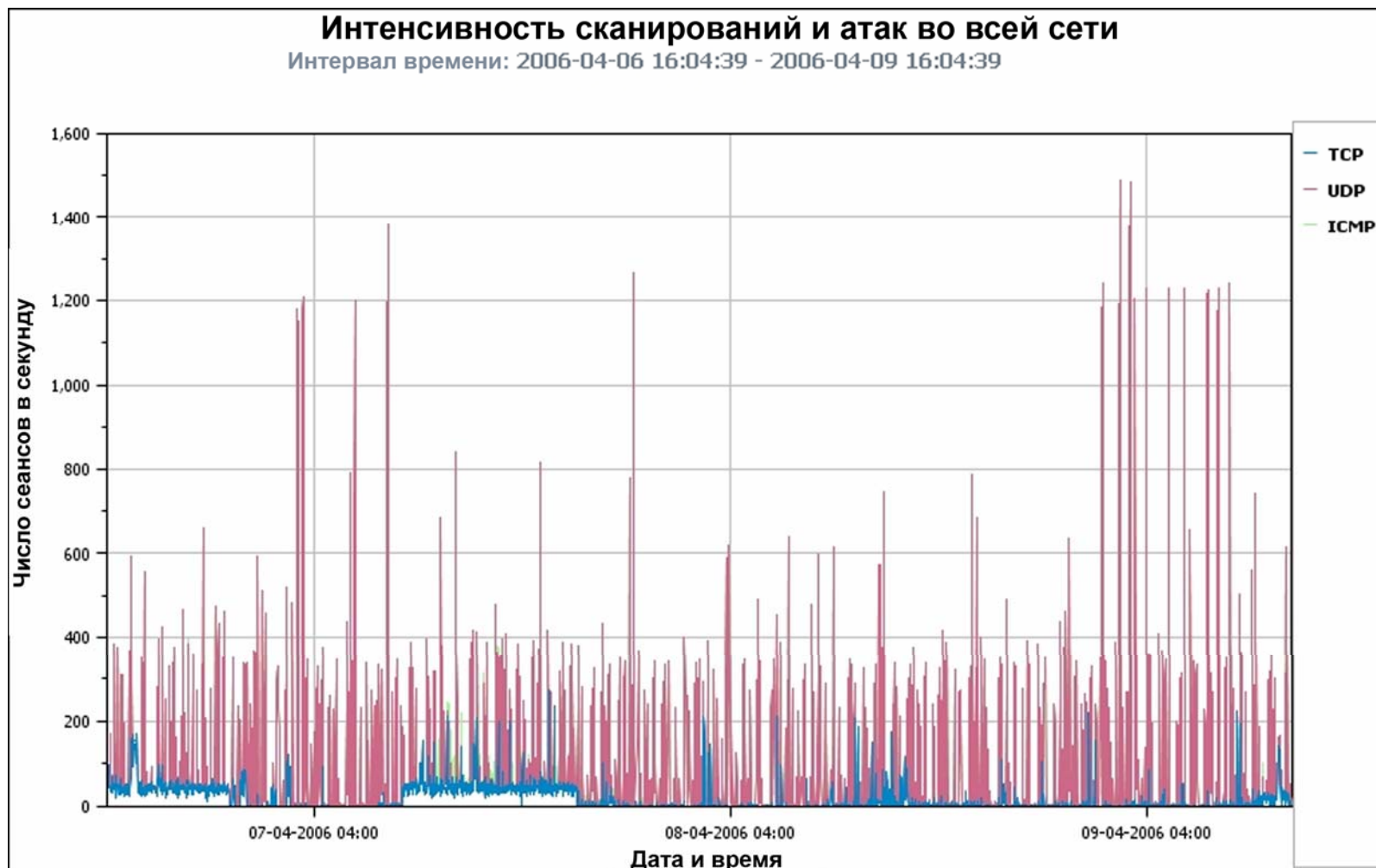
Список хостов

Протокол IP (контроль групп портов или отдельных портов)

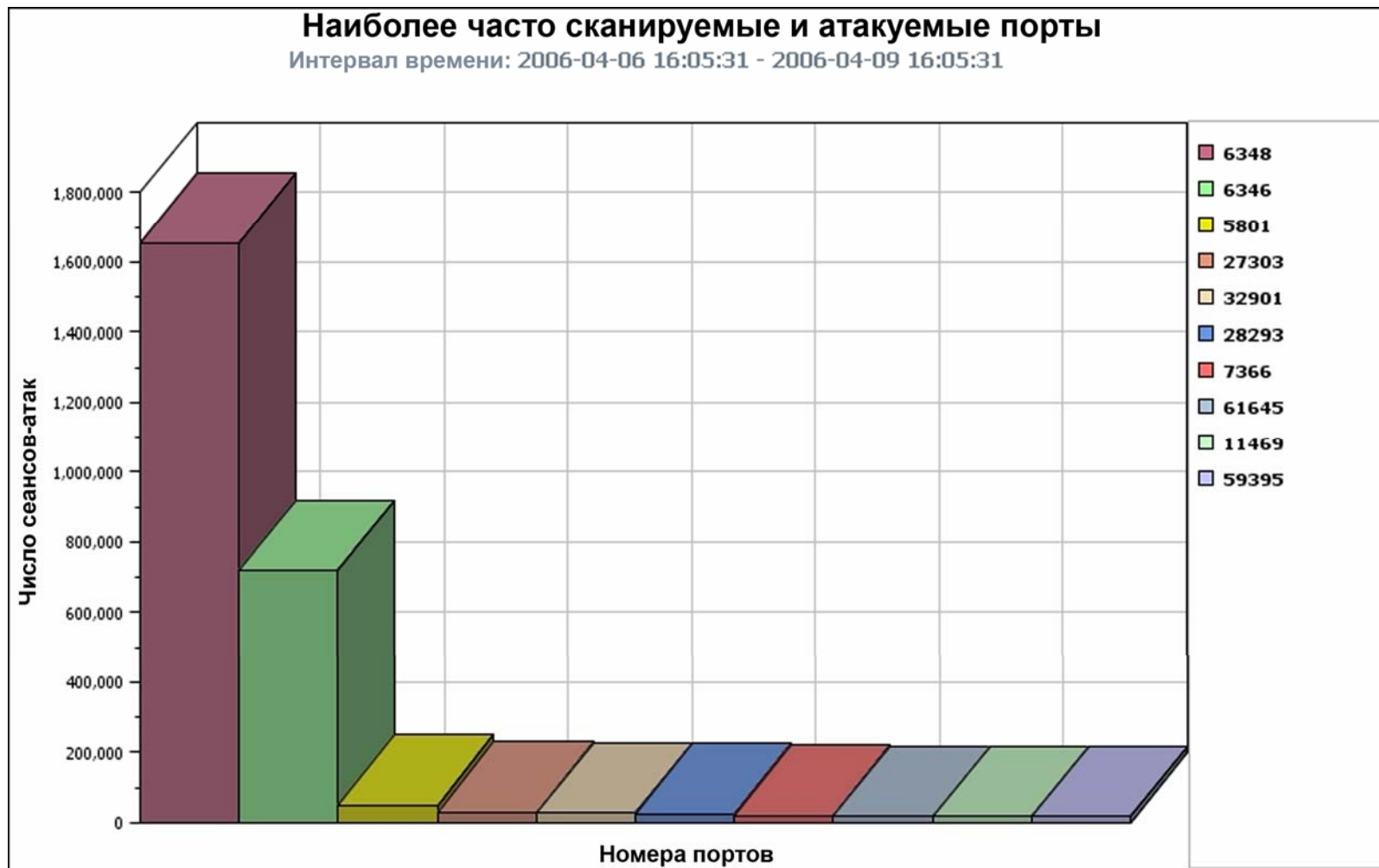
Список портов

The screenshot shows the 'Anomaly Detector Wizard' window, specifically the 'Anomaly Detection Thresholds' step. The window title is 'Anomaly Detector Wizard' and the subtitle is 'Anomaly Detection Thresholds'. Below the subtitle, it says 'Define attack detection thresholds, or use the Default Detector's values'. There are two sections for configuring thresholds. The first section is 'Malicious Traffic Detection Thresholds' and contains a checkbox labeled 'Use the Default Detector's settings:' which is currently unchecked. Below this checkbox, there is a text description: 'An anomaly will be detected once flow rate exceeds this threshold.' and a text input field for 'Flow Open Rate (flows/sec)' with the value '1000'. The second section is for 'Suspected Flows' and contains a text description: 'An anomaly will be detected once suspected flow rate exceeds threshold AND suspected flows ratio exceeds threshold.' Below this, there are two text input fields: 'Suspected Flows Rate (flows/sec)' with the value '500' and 'Ratio of Suspected Flow Rate (%)' with the value '50'. At the bottom of the window, there are four buttons: '< Back', 'Next >', 'Finish', and 'Cancel'.

«Какова общая картина подозрительной активности в сети?»



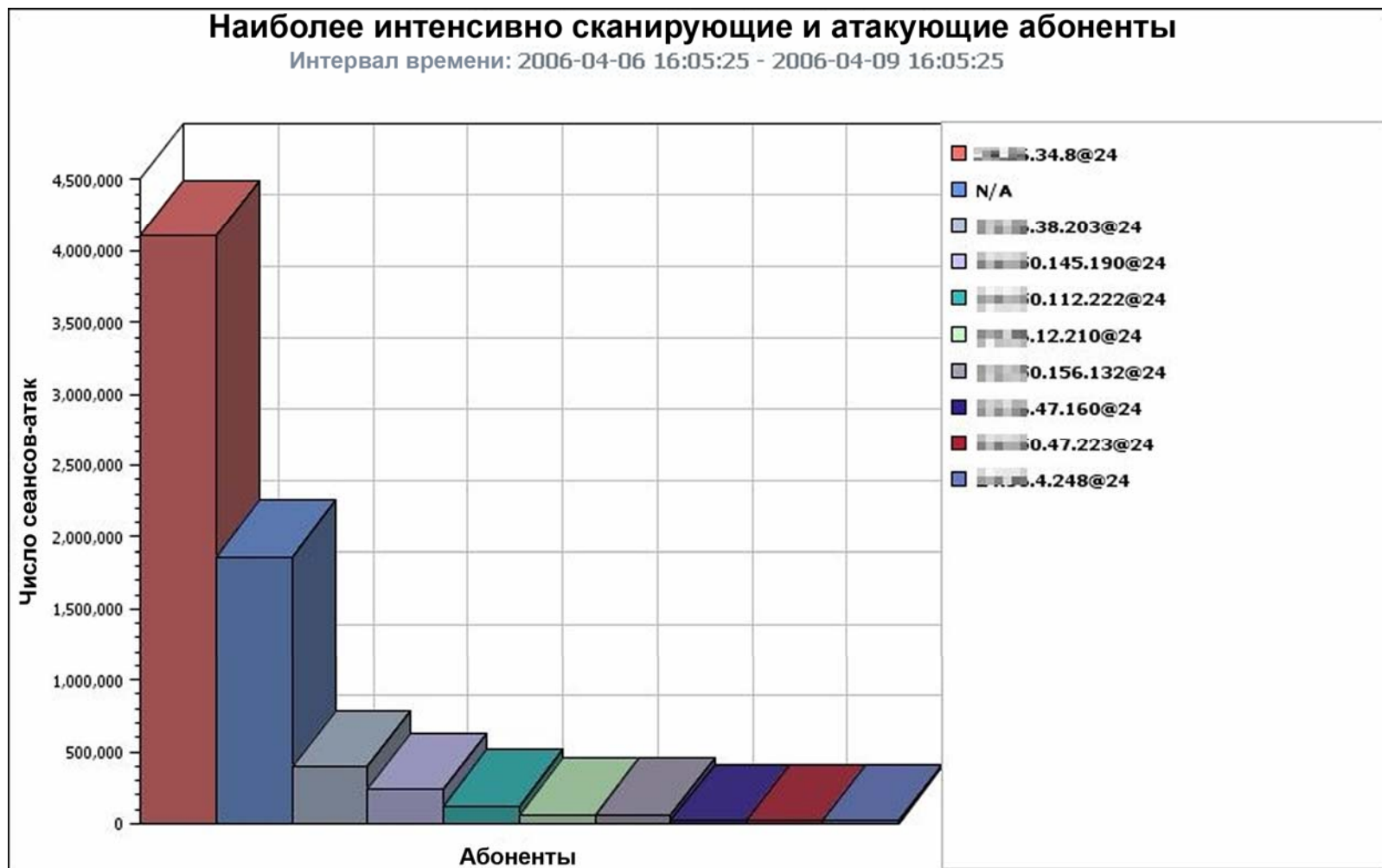
«Какие порты могут являться целями для вредоносного трафика?»



«Сколько абонентов выполняют вредоносные действия в сети?»



«Как определить первую десятку абонентов, генерирующих основной объем вредоносного трафика?»



SCE + дополнительные сервисы (VAS)

■ Задачи

Возможность пересылать выбранный трафик на устройства сторонних производителей, реализующие **дополнительные сервисы, которые не поддерживаются собственными средствами SCE**

- Обработка на основе политик абонентов
- Обработка на основе портов (TCP/UDP)

Возможность использования серверов VAS, для которых **нежелательна постоянная работа in-line** (ограничения пропускной способности, невозможность работы in-line и т.п.)

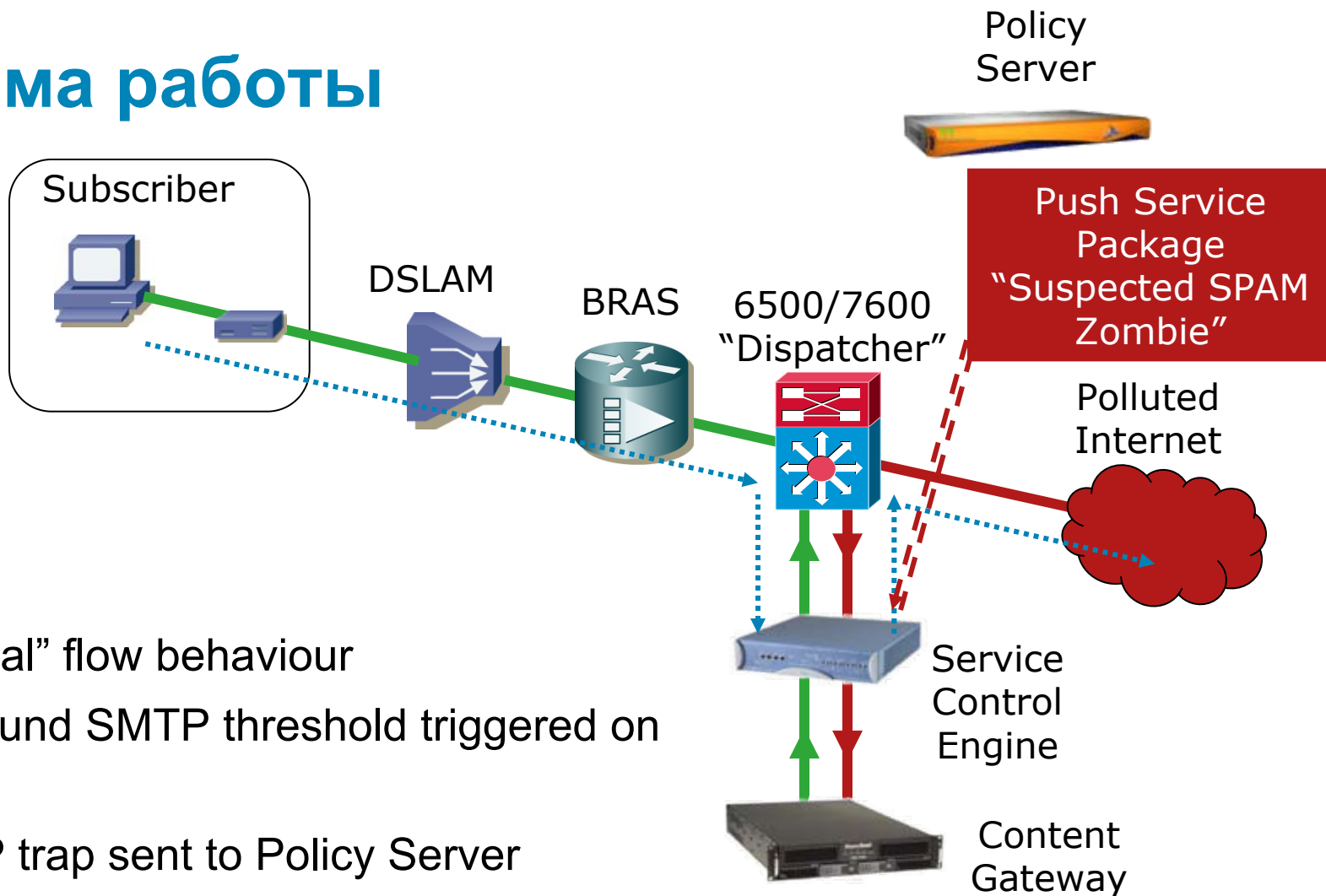
Сокращение ложных срабатываний за счет подробного анализа

■ Подписчикам сервисов VAS присваивается набор сервисов, связанный с сервером VAS

Изменение набора может вызываться определенным событием, например превышением порога исходящего трафика SMTP

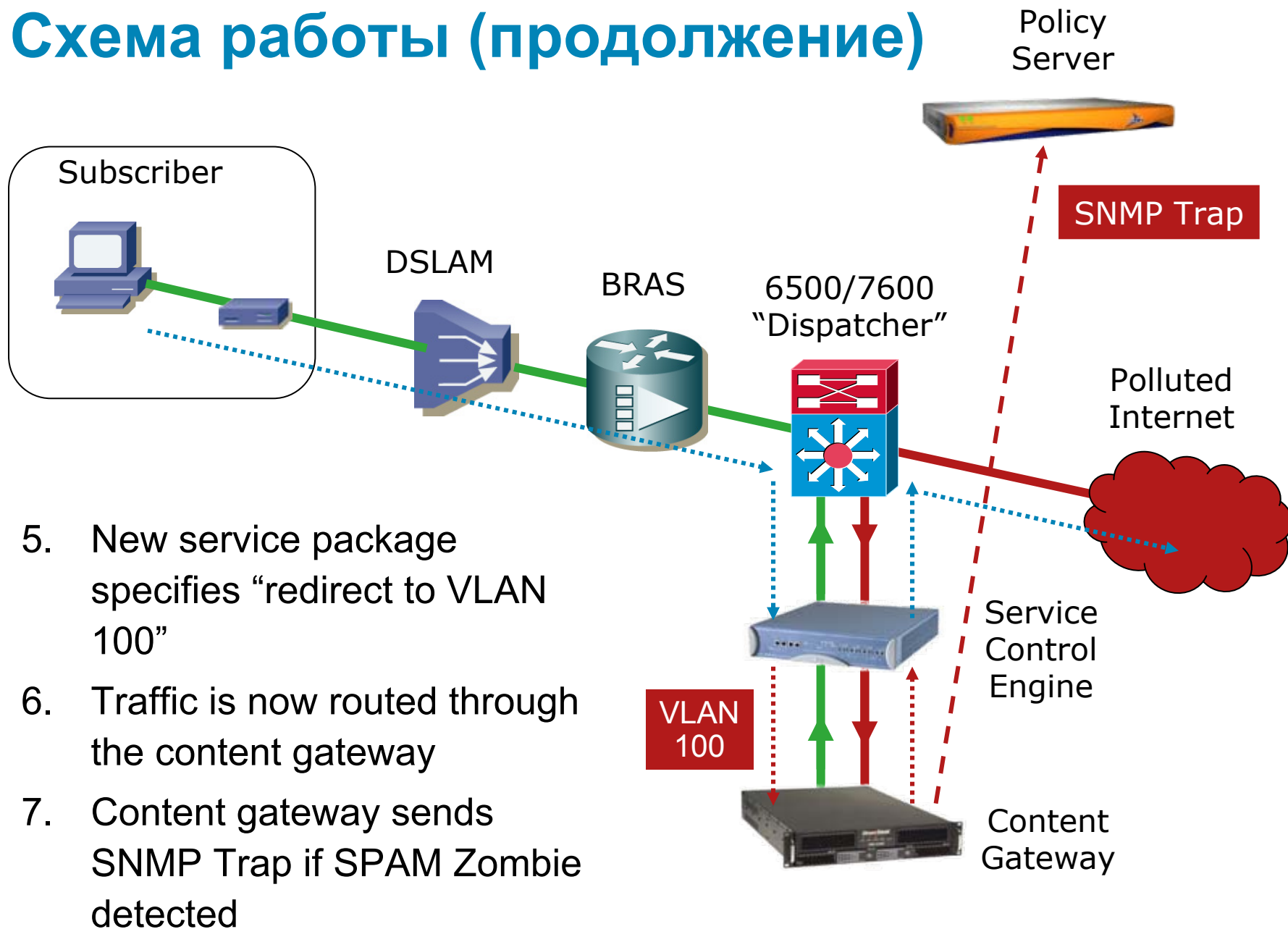
- Переадресация конкретным серверам (например, анти-спам) для анализа

Схема работы



1. "Normal" flow behaviour
2. Outbound SMTP threshold triggered on SCE
3. SNMP trap sent to Policy Server
4. Policy Server configures new service package "Suspected SPAM Zombie"

Схема работы (продолжение)



5. New service package specifies "redirect to VLAN 100"
6. Traffic is now routed through the content gateway
7. Content gateway sends SNMP Trap if SPAM Zombie detected

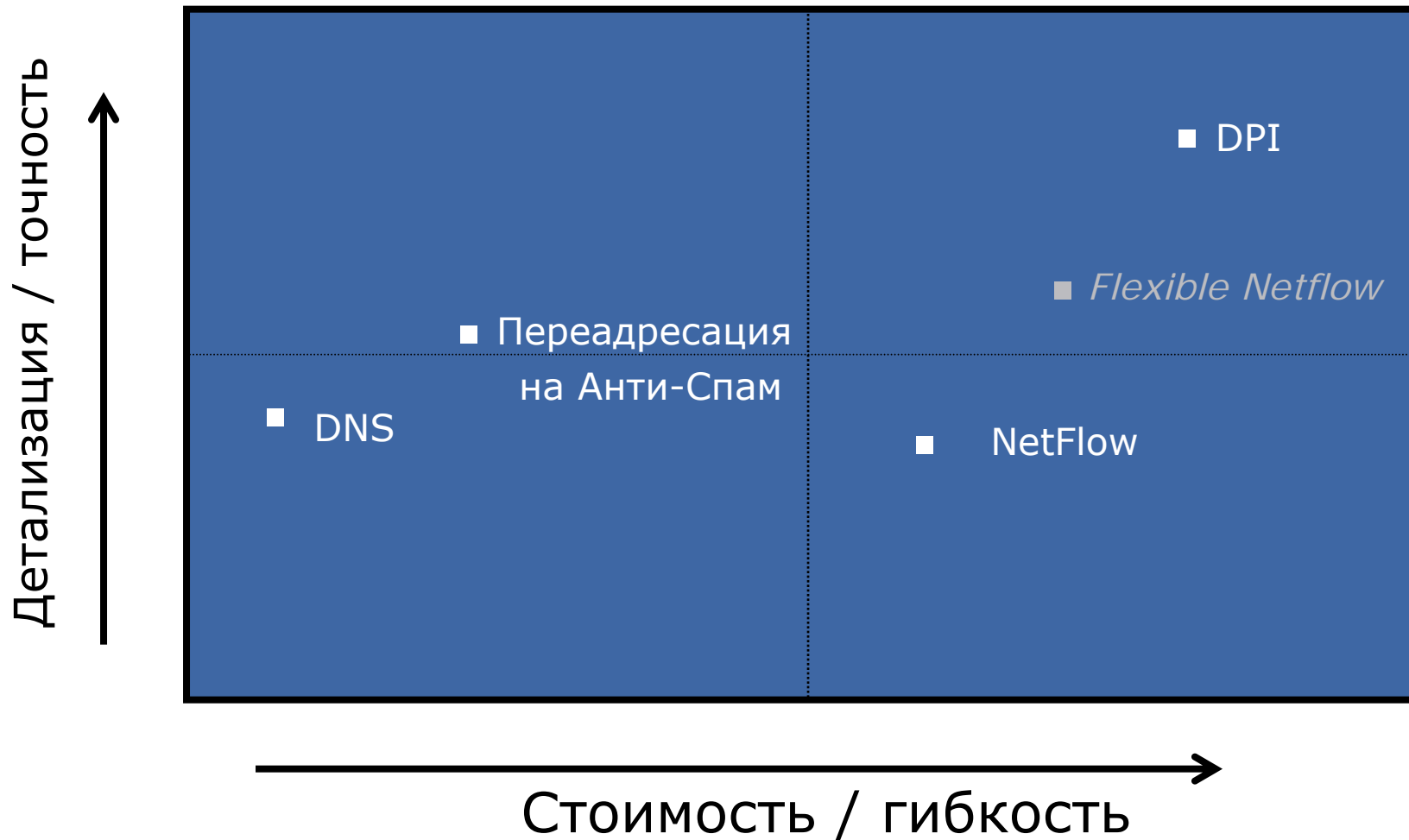
Какой способ обнаружения выбрать?

- Способ обнаружения зависит от приоритетов
 - Обнаружение и блокирование основных источников угроз
 - DNS, Netflow, SCE...
 - Автоматизация исправлений для зараженных пользователей
 - SCE + сервер VAS ...
 - Фокус на определенных видах атак и протоколах
 - Мониторинг SMTP...

Какой способ обнаружения выбрать? (продолжение)

- Способ обнаружения зависит от приоритетов...
 - Адаптируемость в условиях изменчивости атак
 - SCE, Netflow...
 - Готовое решение
 - SCE, Netflow, Анализ статистики DNS...
 - Самостоятельная разработка
 - Свыше 1000 инструментов с открытым исходным кодом => что выбрать для корреляции?

Характеристики средств обнаружения



Защита
исходящего
трафика
Предотвращение



Что мы можем предпринять в мире широкополосных сетей?

- Клиент в отношении себя должен ощущать поддержку или «помощь жертве», а не рассматриваться как источник атаки

Нюанс: крупнейшие источники спама часто оказываются постоянными ботнетами, чем невинными жертвами

- Опыт подчеркивает важность внесения исправлений в системы

Безопасность для новых клиентов – защита перед получением доступа в сеть

Карантинная зона для существующих клиентов
(возможность внести исправления сейчас или позднее)

Изоляция на 2-м/3-м уровне

- Непрерывная защита клиентов посредством сетевого сервиса фильтрации контента (дополнительный источник дохода)

Какому способу предотвращения отдать предпочтение?

- Что является приоритетом для вас и приемлемо для ваших клиентов?

Ручные механизмы для злостных нарушителей?

Блокирование атак без уведомления клиентов и исправления хостов?

Уведомление клиентов о факте заражения и способах самостоятельного решения проблемы?

Карантин – принудительная нейтрализация источников атак?

Продажа дополнительных сервисов безопасности?

Варианты предотвращения

Ручные действия

- Некоторые сервис-провайдеры предпочитают сосредоточиться на работе со злостными нарушителями, информируя их по телефону и электронной почте
- Должны быть четко определены нормы пользования сетью
- Иногда законодательно запрещено принудительное отключение, в частности в Германии.

Варианты предотвращения Блокирование определенных видов трафика

■ Блокирование

В Канаде предпринята *государственная* инициатива по блокированию всего не адресованного серверам провайдера SMTP-трафика – по ее условиям все Интернет-провайдеры должны пропускать трафик через собственные Mail Relay для мониторинга и фильтрации

Некоторые операторы в России также придерживаются этой практики

Блокирование радикально сокращает долю спама, но

- Простое блокирование превышения SMTP-трафика ухудшает точность детектирования спама
- Более точный подход требует прохождения SMTP-трафика через анти-спам устройства

Варианты предотвращения Уведомление

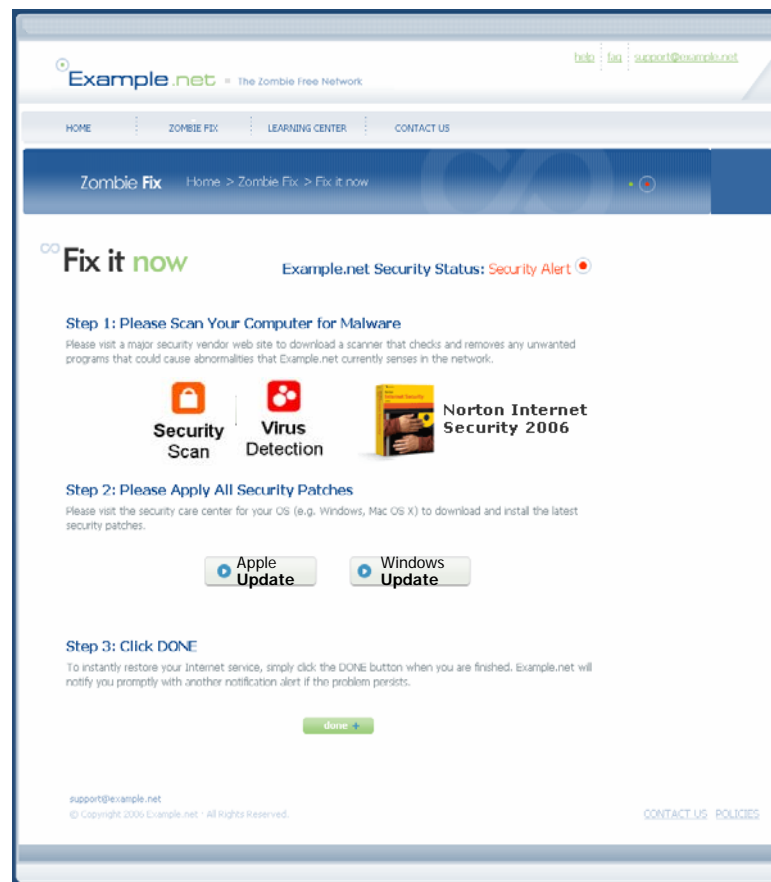
- Многие устройства, например Cisco SCE, могут уведомлять абонентов о заражении посредством переадресации по HTTP

Устройство должно работать in-line, либо перехватывать DNS-трафик

Уведомление **не означает ограничения доступа**

Возможность отложить внесение исправлений крайне важна – именно она отличает ограничение доступа от запрета доступа

В основе лежит модель *доверия*.



Веб-сайт направляет пользователей на сайты, позволяющие найти и обезвредить вредоносное ПО, а также установить патчи

Варианты предотвращения Карантин

- Предполагает ограничение доступа пользователя до исправления ситуации
 - Изоляция на 2-м/3-м уровнях
 - Списки контроля доступа (ACL)
- Перенаправление пользователей в зону карантина – технически несложное решение
 - RADIUS – маршрутизация на основе политик, присвоение VRF...
 - Перенаправление DNS
 - Сервер политик
- Нормальный доступ восстанавливается после подтверждения исправления

Какую роль играет SCE? Предотвращение

■ Функции SCE по предотвращению

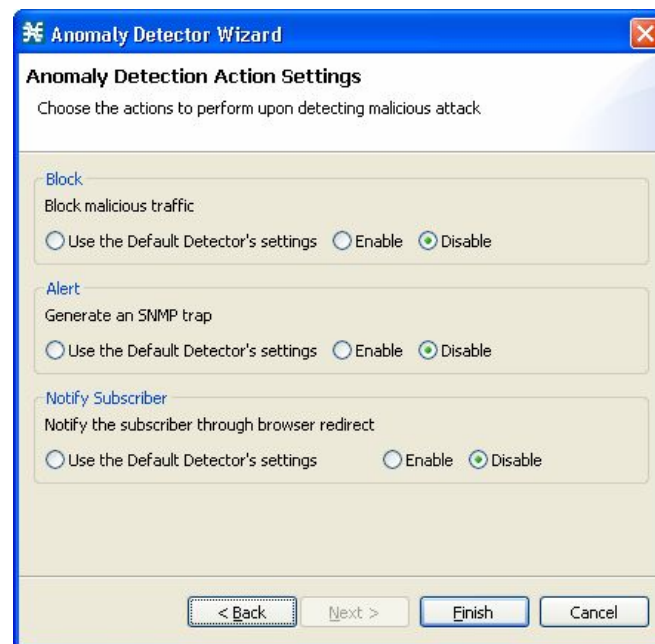
Блокирование подозрительного трафика, например, по сигнатурам

Переадресация HTTP на определенную веб-страницу

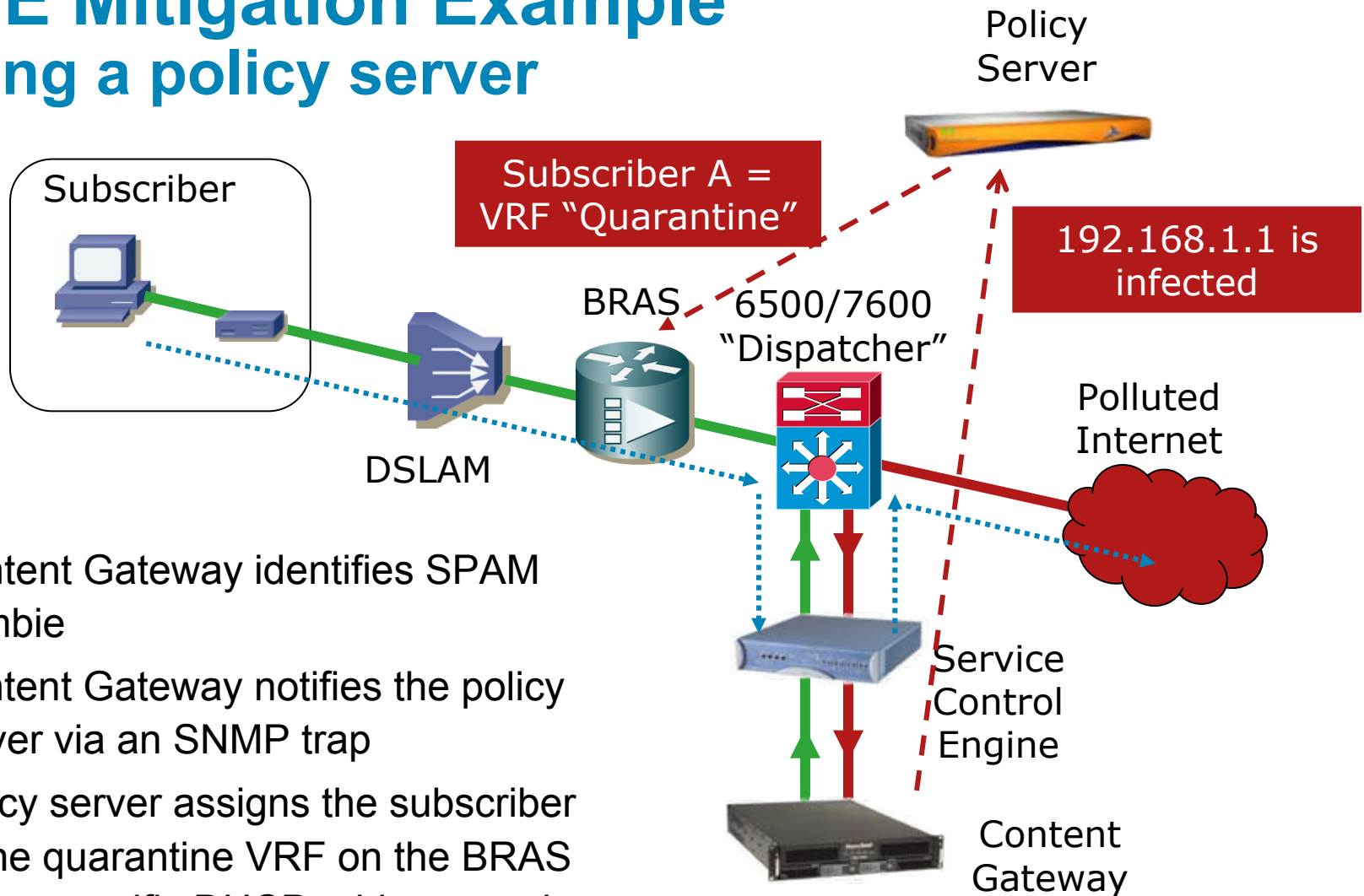
Возможно совместно с блокированием

Оповещение по SNMP – серверы политик могут перенастраивать другие сетевые устройства, например, присвоение VLAN зараженным пользователям

Контроль входящего конента, родительский контроль и перенаправление трафика на *VAS*

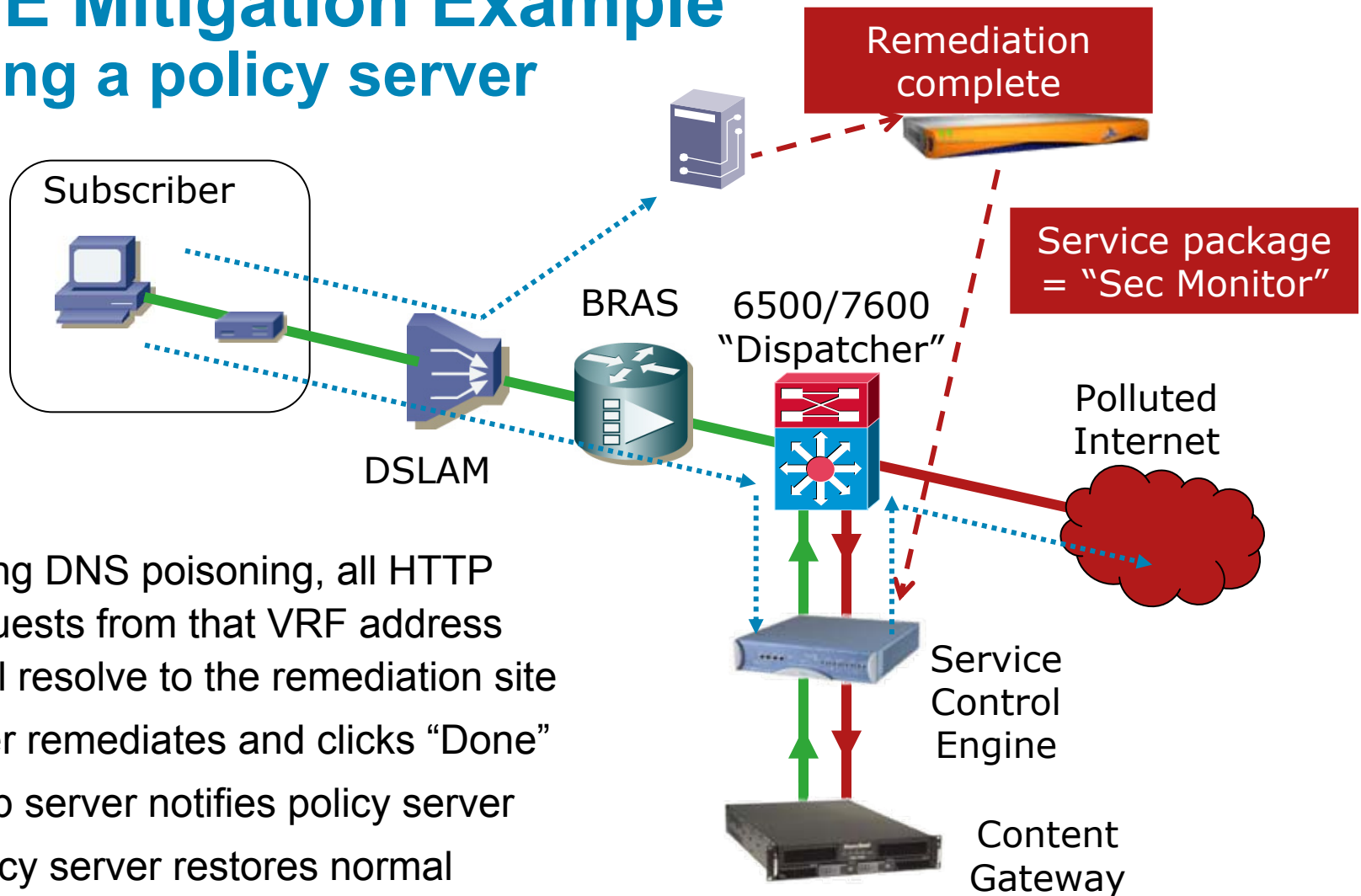


SCE Mitigation Example Using a policy server



1. Content Gateway identifies SPAM Zombie
2. Content Gateway notifies the policy server via an SNMP trap
3. Policy server assigns the subscriber to the quarantine VRF on the BRAS with a specific DHCP address pool to the BRAS

SCE Mitigation Example Using a policy server



4. Using DNS poisoning, all HTTP requests from that VRF address pool resolve to the remediation site
5. User remediates and clicks "Done"
6. Web server notifies policy server
7. Policy server restores normal access and original service package

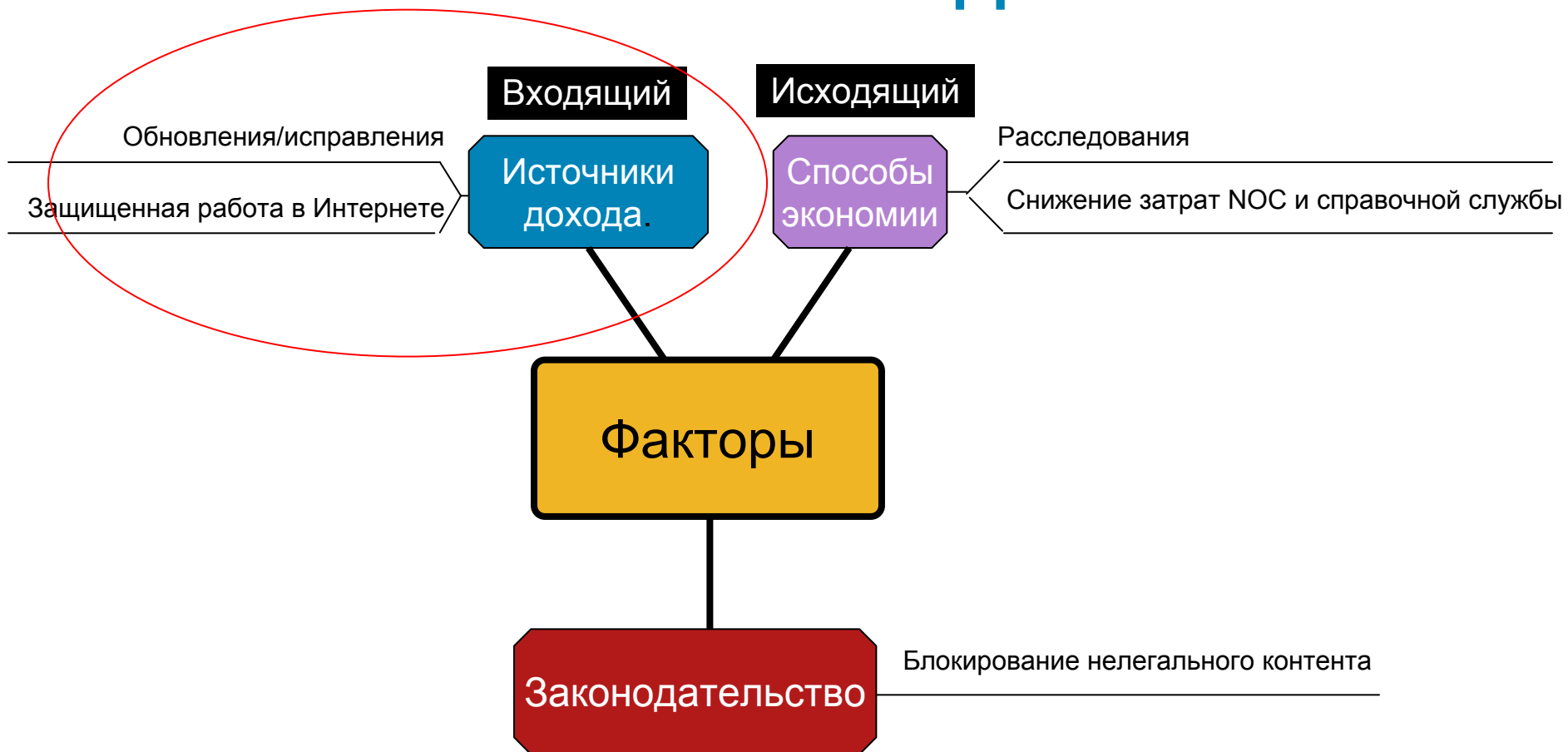
Какой способ предотвращения выбрать?

- Отключение – неприемлемый методы работы с жертвами заражений
- Защита от организации ботнета возможна только путем эффективной очистки, внесения исправлений и *непрерывной защиты*
- Исправление **возможно** – достаточно обычной модели доверия, поскольку определить эффективность исправления хоста не составляет труда
- Залогом успешного исправления ситуации является понятный для пользователя веб-интерфейс

Защита
входящего
трафика
Получение
прибыли



Экономическое обоснование безопасности сетей ШПД



Цель – единая инфраструктура для поддержки всех функций!

Продажа сервисов безопасности как вариант предотвращения

- Постоянная защита хоста от заражений
- В уведомительном сообщении присутствует ссылка, позволяющая подписаться на услугу

Входящий трафик фильтруется

Фильтрация контента – антивирус, anti-spyware

Родительский контроль

Межсетевой экран

Фильтрация трафика определенных приложений

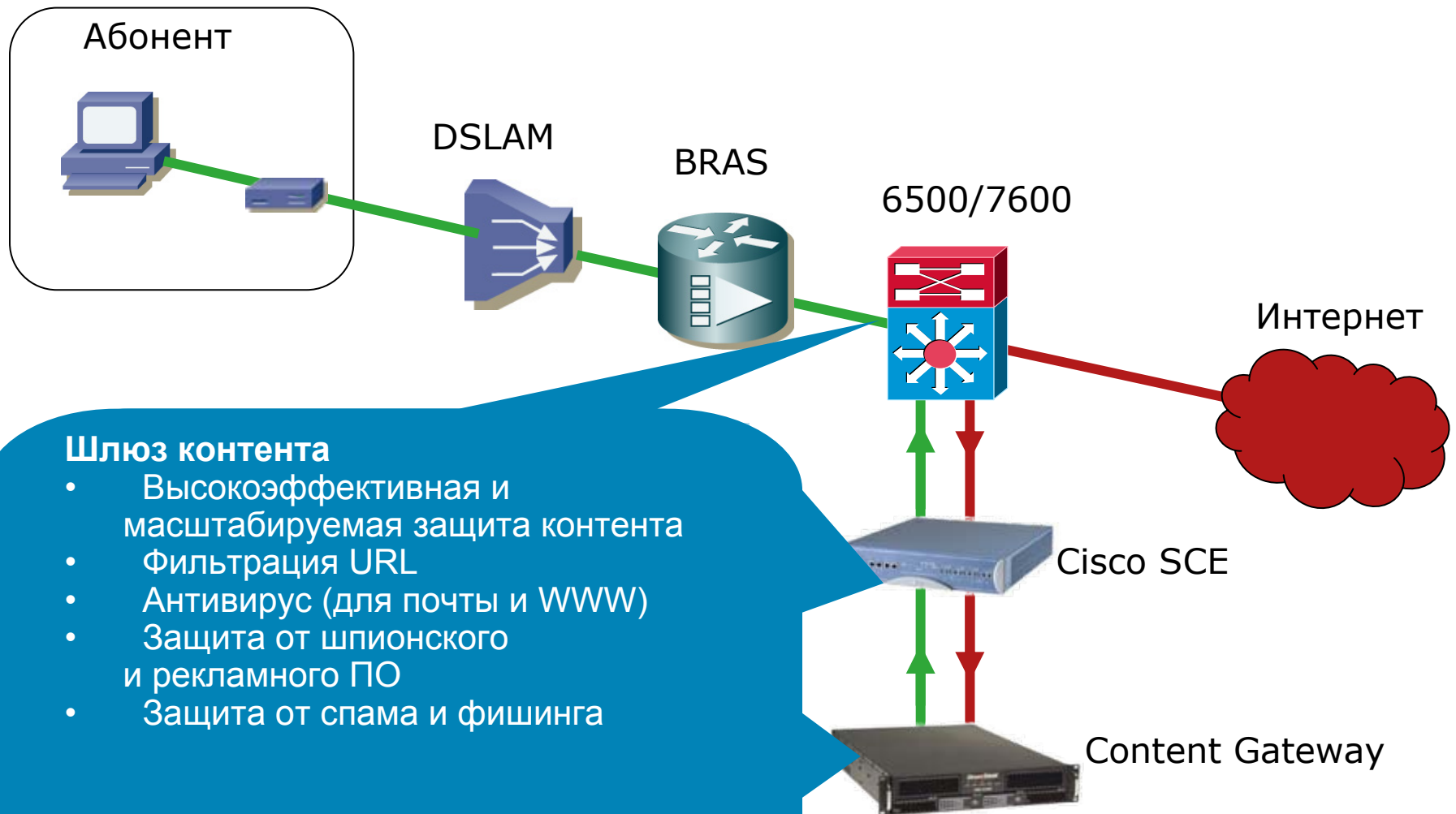
Практический опыт показывает, что предложение подобных сервисов только при обращениях в службу поддержки доводит аудиторию их пользователей до 50%

Основы решения для очистки трафика абонентов ШПД

- Дополнение возможностей базовых сетевых сервисов
- Подключение не требует особых затрат
 - Подписка через пользовательский портал
 - Автоматическая инициализация
 - Гибкие уровни обслуживания (пакеты сервисов)
- Защита сети и контента
- Масштабируемость, устойчивость, гибкость

Общая архитектура со средствами защиты исходящего трафика!

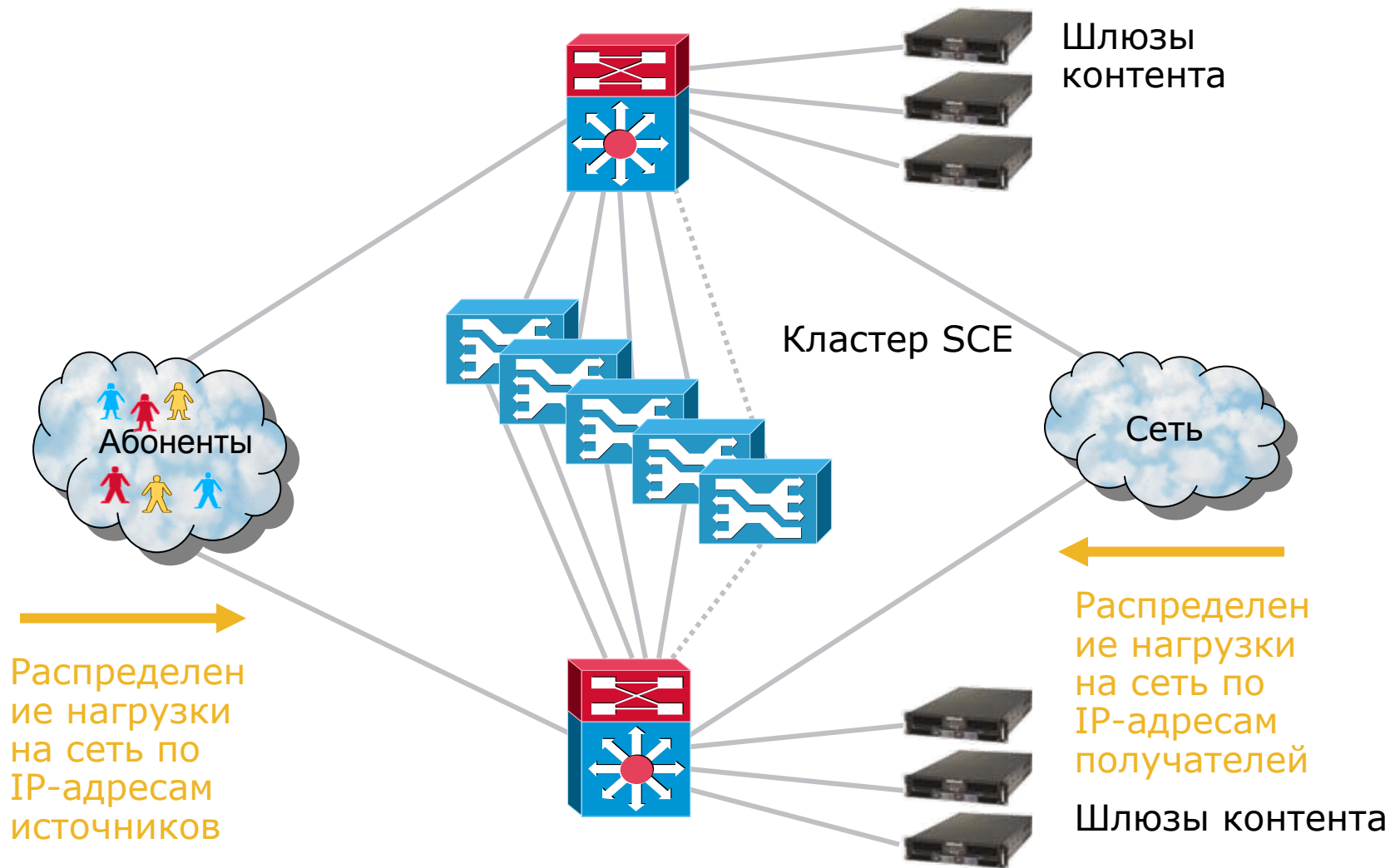
Логическая архитектура



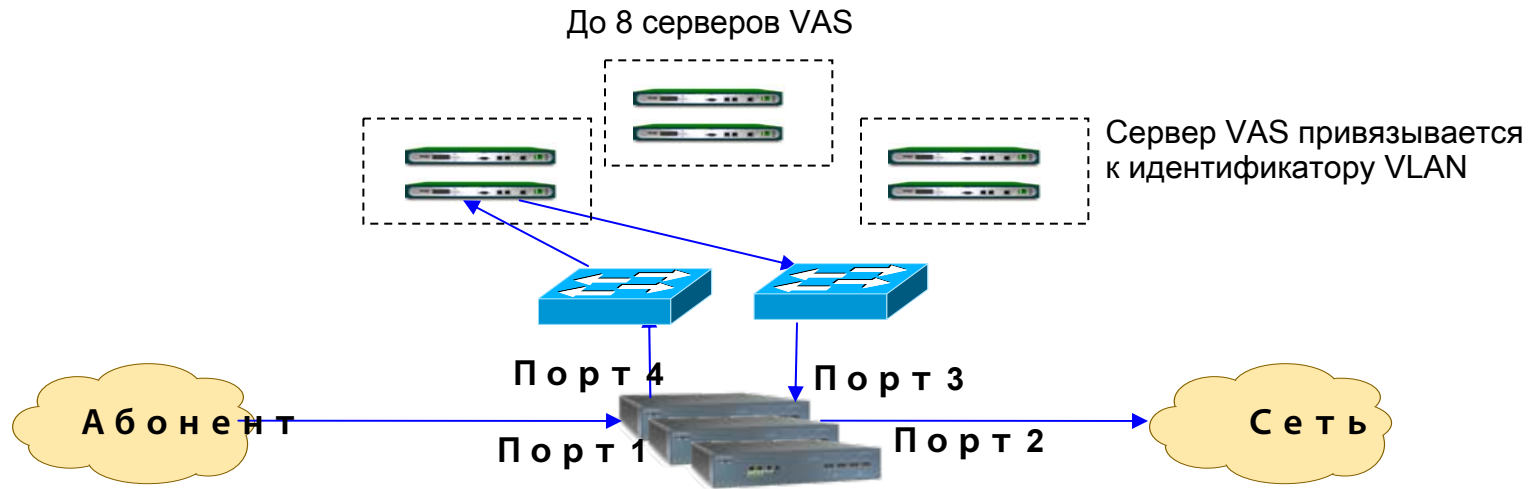
Шлюз контента

- Высокоэффективная и масштабируемая защита контента
- Фильтрация URL
- Антивирус (для почты и WWW)
- Защита от шпионского и рекламного ПО
- Защита от спама и фишинга

Физическая архитектура



Обзор VAS



- Решение доступно только для SCE 2020
- Каждый SCE может использовать до 8 серверов VAS
- Серверы могут быть сгруппированы в соответствии с типами сервисов.
- Маршрутизация на сервер VAS выполняется посредством тэгов VLAN

Серверы VAS

- Функциональная совместимость с устройствами сторонних поставщиков

Специальная поддержка не требуется => упрощение стыковки устройств и реализации сервисов

- Примеры потенциальных сервисов VAS:

Фильтрация контента (защита от вирусов, шпионского ПО и т.п.)

Межсетевой экран

Защита от вторжений

Защита от спама

«Сторож» трафика

- Примеры предложений существующих поставщиков VAS:

Aladdin – фильтрация контента, фильтрация URL, DPI, фильтрация спама

StreamShield – фильтрация контента, фильтрация URL, фильтрация спама

Интеграция

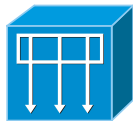
Тарификация



AAA



Сервер политик



Управление сервисами
для абонентов

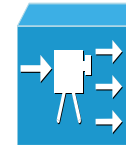
Портал



VoIP



Видео



Приложения и сервисы

Физическая интеграция

- Тэги VLAN – основа механизма пересылки трафика на серверы VAS
- Серверы VAS должны работать в режиме L2 transparent и поддерживать VLAN тэги
- 7600/6500 отвечает за распределение нагрузки и привязку сессий

Интеграция с управлением сервисами для абонентов

Высший уровень интеграции – соответствие между абонентом и адресом на сервере AAA

Все устройства имеют опубликованные программные интерфейсы взаимодействия серверами политик

И

Заключение



Тенденции...

- Растущая распространенность и доступность сетей ШПД.
- Различные варианты доступа – Ethernet, Home PNA, xDSL, Cable, Wireless, Mobile...
- “Безлимитные” тарифы
- Снижение стоимости
- **Разнообразии бытовых устройств с возможностью/необходимостью подключения к Интернет**

Чистая вода.... чистый Интернет

100 лет назад



Вода из грязных источников
Перед употреблением кипятить



**Трубы
очистных станций**



Сегодня



Сегодня
Безопасная вода –
дело водопроводной компании

Сегодня



Загрязненный Интернет
ПО на ПК делает доступ в
Интернет безопасным?



**Чистые каналы
Интернета**



Безопасный Интернет
Безопасность Интернета –
работа Оператора Связи!

Вопросы и ответы



