ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ОПЕРАТОРОВ СВЯЗИ

Михаил Кадер

Инженер-консультант

security-request@cisco.com

Cisco Expo 2007

Содержание

- Оператор связи и безопасность
- Стратегия Cisco по безопасности операторов связи
- 5 аспектов безопасности оператора
- Безопасность, как бизнес

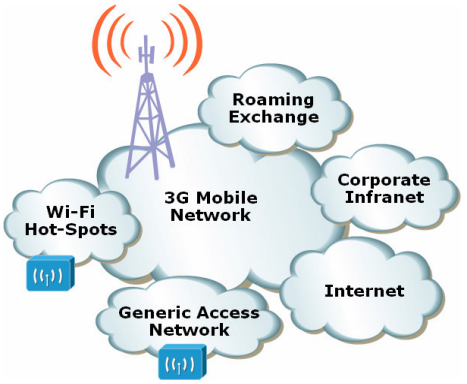
Требования современного оператора связи в области информационной безопасности

3+ кита безопасности оператора

Операторский бизнес
Рост доходности приводит к росту рисков

Базирующиеся на IP сети увеличивают опасность нанесения ущерба вследствие:

- **Увеличения числа соединения из недоверенных внешних сетей, таких как Интернет и пиринг**
- **Роста числа «открытых» сетей, протоколов и приложений и открытости для червей, вирусов и DDoS-атак**
- **Незащищенных пользовательских устройств, которые могут стать целью или источником проблем**
- **Пиринговых (P2P) приложений, которые могут захватить полосу пропускания и снизить доходность платных сервисов**



January 16, 2006	Bootton.E found
January 4, 2006	New Pbstealer variant
December 30, 2005	Sendtool.A detected
December 28, 2005	New Onehop variants detected
December 22, 2005	New Cardtrap variant
December 16, 2005	New Cdropper variant
December 16, 2005	Dampig variant detected
December 15, 2005	Cabir.AB found
December 15, 2005	New Doomboot variants
December 14, 2005	Cardtrap variants detected

В чем риск?

- Потеря контроля над трафиком
  - Атаки Denial of Service (DoS)/Distributed Denial of Service (DDoS) влияют на ядро сети или на сети заказчиков
  - Неправильно выделенная полоса пропускания (Quality of Service—QoS) для сетевого трафика
  - Трафик, нацеленный на другие сетевые сервисы, например, DNS, NTP и т.д.
  - Отказ от использования платных сервисов в пользу бесплатных, например, Skype
- Невозможность контролировать сетевые потоки является одной их основных головных болей оператора мобильной связи

Воздействие атак на бизнес оператора

- Удар по репутации и снижение лояльности клиентов
- Привлечение к уголовной или административной ответственности
- Иски и финансовые претензии со стороны клиентов
- Простои сетевых узлов и инфраструктуры
- Снижение курсовой стоимости акций
- Банкротство

Примеры атак на операторов

- …
- …
- …
- …
- …

Cisco SP Security Framework

Cisco Service Provider Security Strategy

Внедрение сервисов

Оптимизация и создание новых доходных сервисов **безопасности**

Построение сетей

Современная, расширяемая, эффективная и **защищенная** сеть, снижающая TCO

Генерация потребности

Генерация потребностей **защищенного** подключения заказчиков к сервисам оператора

Оптимизация бизнеса

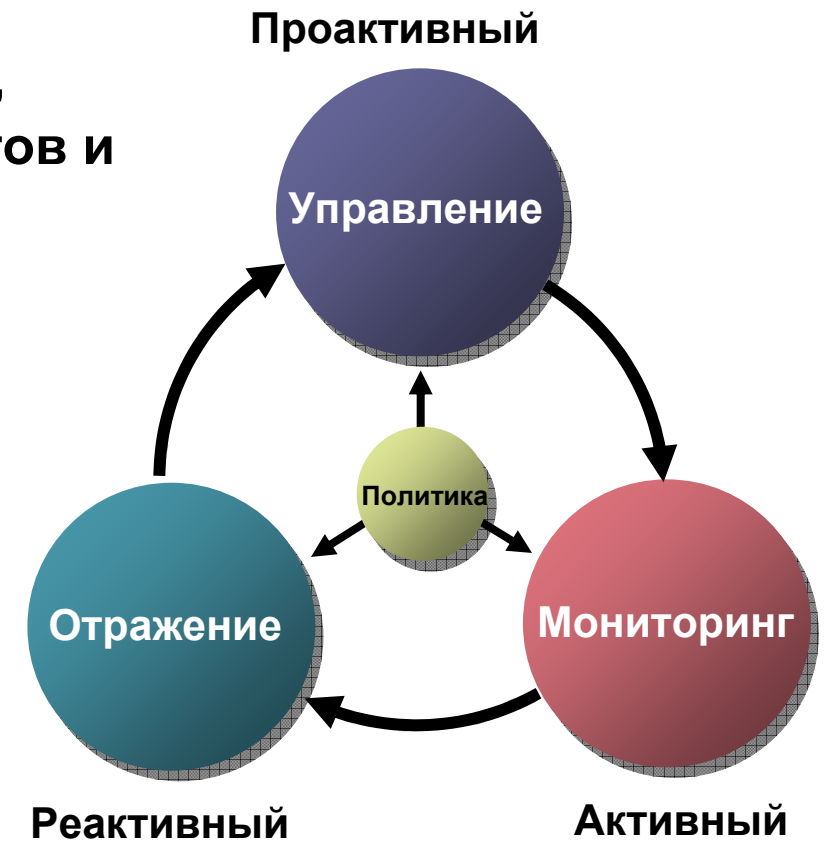
Обеспечение экспертизы для поддержки перехода к новым условиям **защищенного** бизнеса

Безопасность Cisco IP NGN
Интеграция всюду

Cisco SP Security Framework
Управление, мониторинг, отражение…

Для эффективного управления рисками в IP-сетях операторы должны внедрить непрерывный, итерационный процесс:

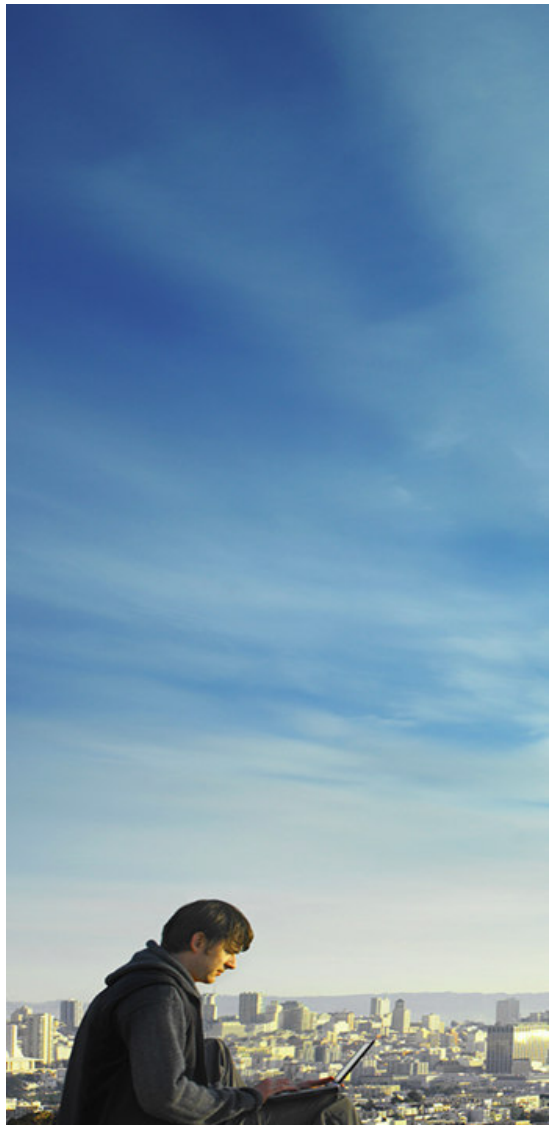
- **Проактивное применение политик, регулирующих поведение абонентов и защиту сети и сервисов**
- **Активный мониторинг сетевого и абонентского поведения для проверки соответствия политике и обнаружения событий, негативно влияющих на сервисы**
- **Быстрое реагирование на атаки, их отражение и предотвращение вредоносного поведения абонентов**



Cisco SP Security Framework
Преимущества

Cisco SP Security Framework позволяет решить следующие задачи оператора:

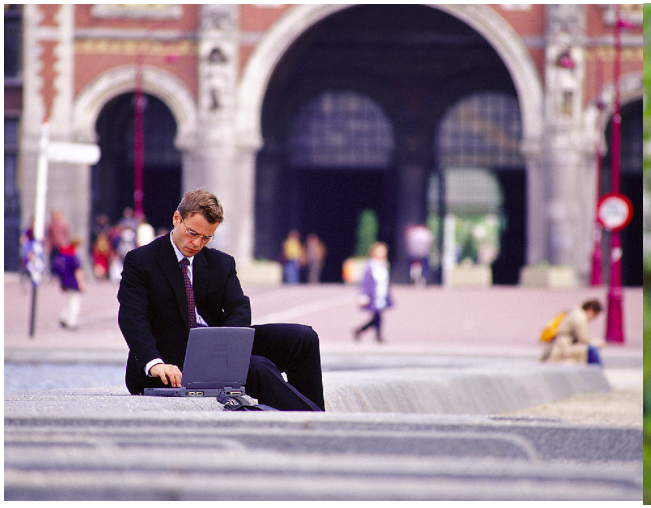
- **Максимизация доступности сервисов, максимизирующая доход**
- **Безопасность и надежность сервисов, привлекающая новых абонентов**
- **Надежность и безопасность, минимизирующие текучесть абонентов**
- **Выполнение SLA и отражение атак, спасающие от судебного преследования**
- **Выполнение локального и международного законодательства, позволяющие выйти на новые рынки**

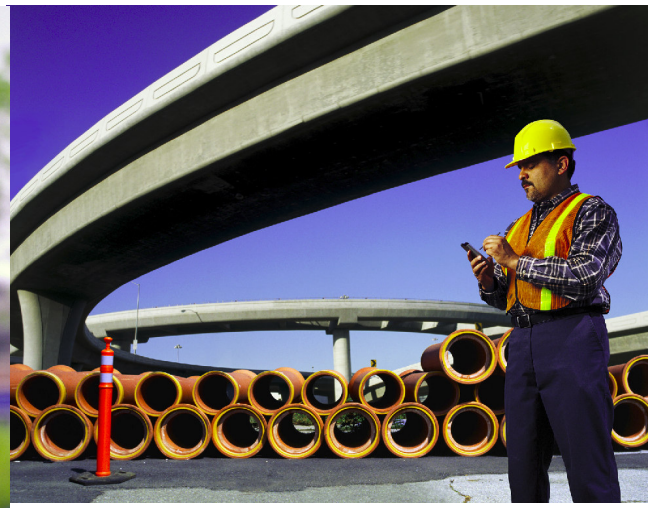


Cisco SP Security Framework
Пусть безопасность принесет вам деньги

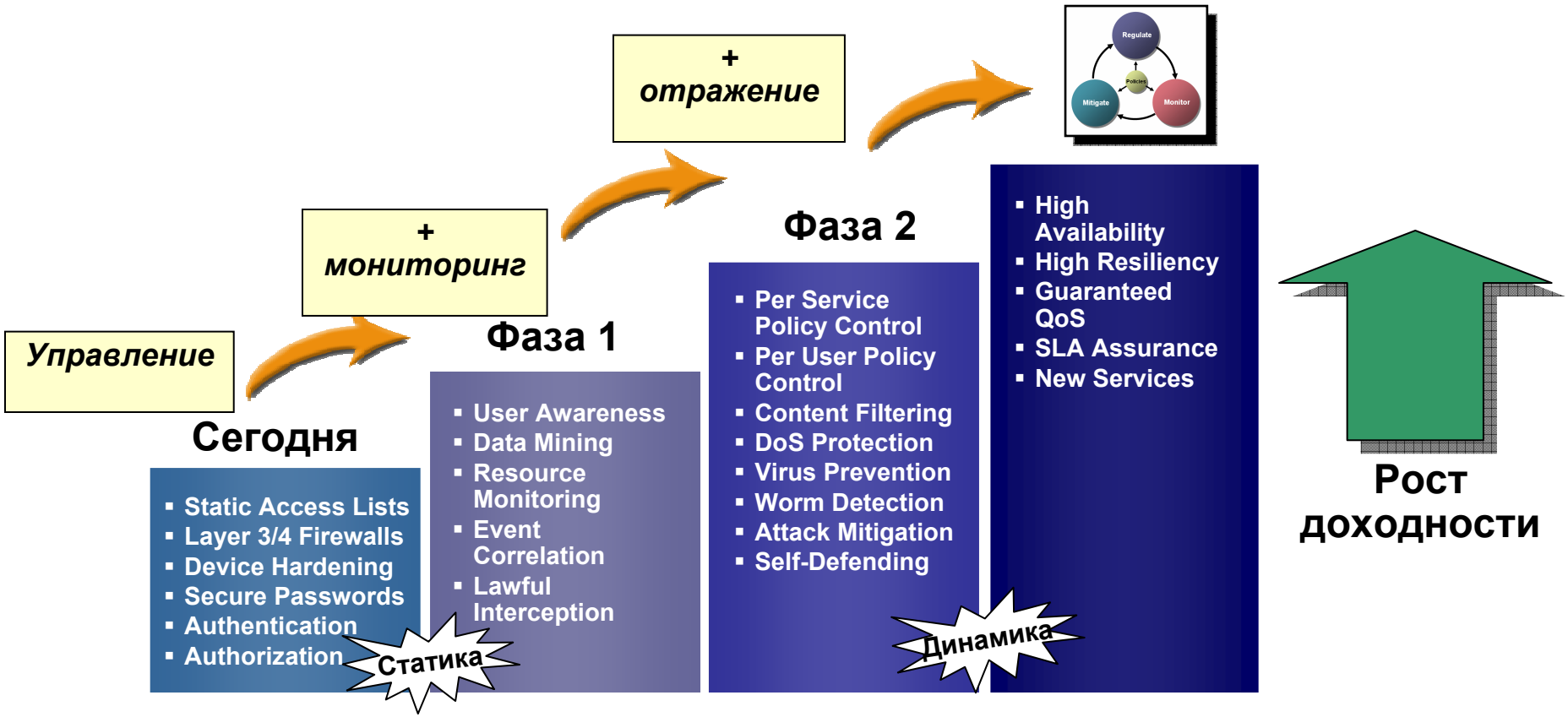
Безопасность – это не только характеристика сервиса – безопасность может стать источником доходов:

- **Фильтрация контента, родительский контроль и антиспам (включая SMS) для абонентов и корпоративных клиентов**
- **Сетевое сканирование и предотвращение атак на различные сервисы (включая HTTP, WAP, SMS и MMS)**
- **Контекстная защита от DDoS-атак для абонентов и корпоративных клиентов**





Cisco SP Security Framework
Поэтапный подход



Cisco SP Security Framework может внедряться поэтапно для постепенного обеспечения видимости, защиты и контроля, дающих рост доходности…

Разные категории операторов

- Традиционные
- Кабельные
- Мобильные
  - GSM
  - CDMA
  - WiMAX
- Интернет-провайдеры
- Хостинговые провайдеры

Об общего к частному

Ключевые направления действий

- Непрерывность и доступность сервисов
- Контроль поведения абонентов
- Защита от вирусов, червей и спама
- Защита периметра
- Выполнение законодательных требований
- Исполнение социальной роли

Cisco Network Foundation Protection

Network Foundation Protection

Защита инфраструктуры

Data Plane

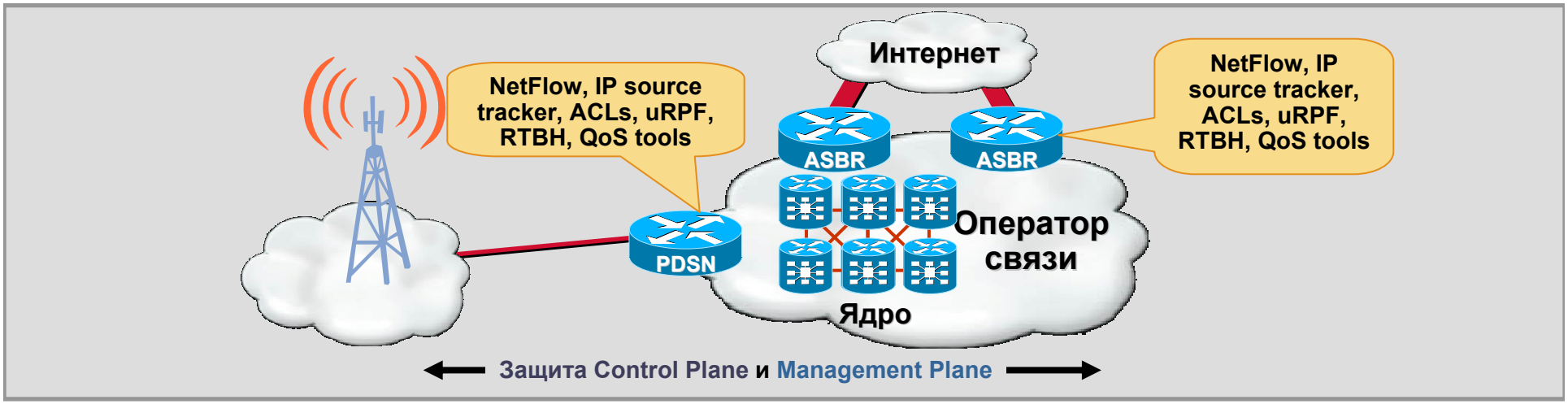
- Обнаружение аномалий и реагирование в реальном времени
- Технологии: NetFlow, IP source tracker, ACLs, uRPF, RTBH, QoS tools

Control Plane

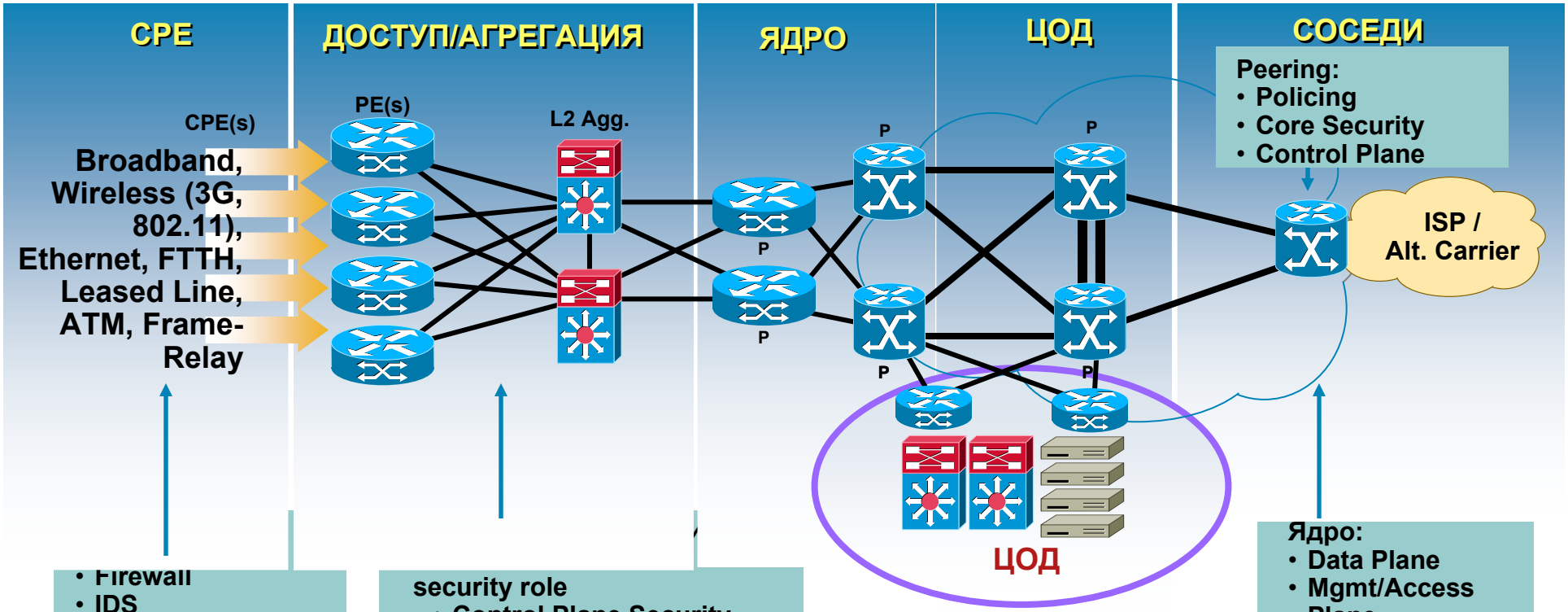
- Эшелонированная защиты для протоколов маршрутизации
- Технологии: Receive ACLs, control plane policing, routing protection

Management Plane

- Защита и защищенное управление Cisco IOS
- Технологии: CPU and memory thresholding, dual export syslog, encrypted access, SNMPv3, security audit



Роль сети, как инструмента безопасности



- Firewall
- IDS
- IPSEC
- Control Plane Security
- Forwarding Plane Security
- Re-DHCP—subscriber
- Diversion

security role
- Control Plane Security
- Data Plane Security

- Firewall
- IDS
- IPSEC
- DHCP—subscriber (dial)
- Diversion (quarantine, clean pipes)
- SSL
- Trust and Identity

Центр обработки данных:
- Remediation (quarantine)
- Intrusion Detection/Prevention
- Anomaly detection (Netflow+Arbor Peakflow DOS)
- Scrubbing (GuardXT)
- Firewall
- Security Monitoring

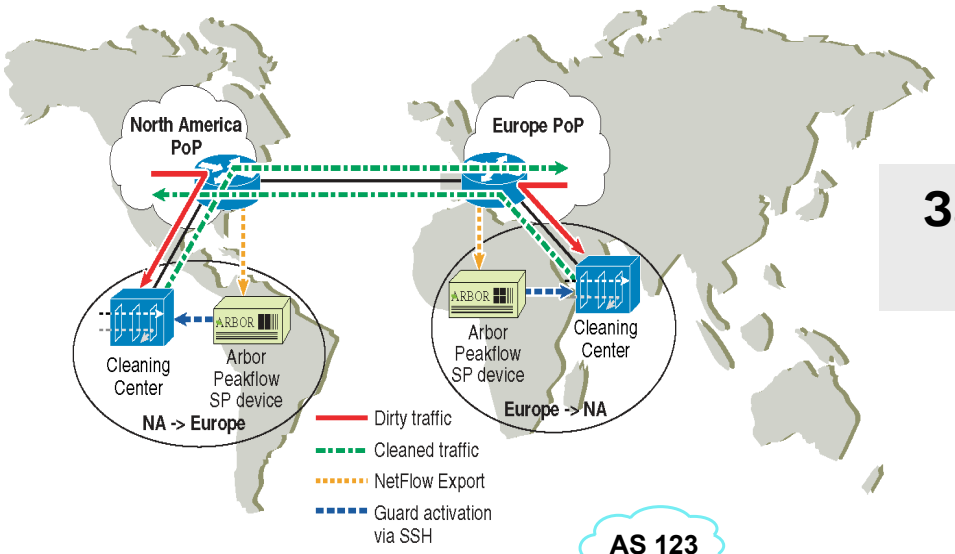
Ядро:
- Data Plane
- Mgmt/Access Plane
- Control Plane
- Core Security

Защита от DDoS-атак

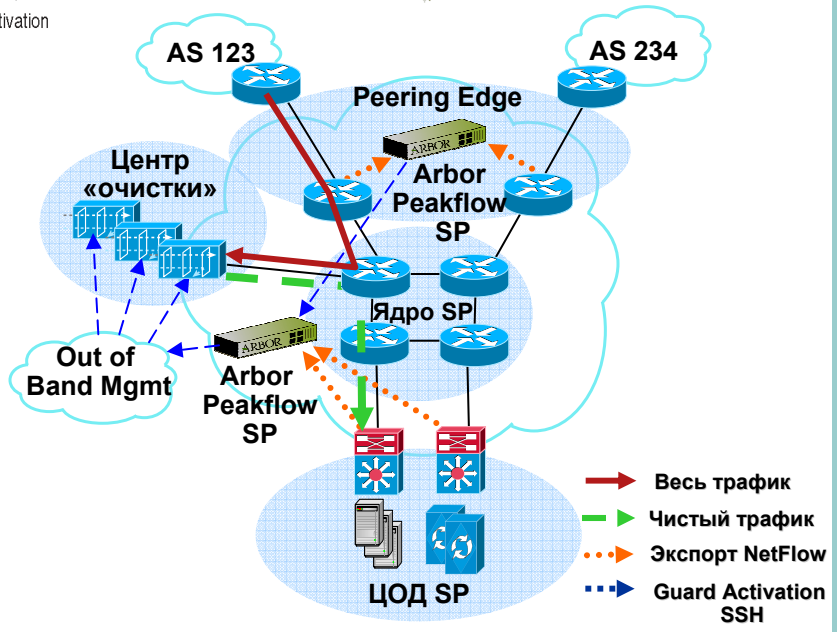
Cisco Clean Pipes

- Главная цель – удалить вредоносный трафик из канала связи и донести до заказчика только легитимные данные
- Вредоносный трафик может представлять собой
  - DoS и DDoS-атаки
  - Черви
  - Спам
- Решение должно учитывать существующую инфраструктуру оператора связи

Защита инфраструктуры от DDoS-атак



Зарубежные соседи



ЦОД SP

Ключевые возможности

- Защита инфраструктуры от DDoS-атак
- Работа вместе с NFP для отражения атак на уровне данных, контроля, управления и сервисов
- Снижение прямых атак на ядро, периметр и соседей
- Защита критичных ресурсов в сети оператора, например, сервера DNS, HTTP, SMSC, WAP
- Снижение цены ущерба
- Снижение OPEX (сохранение полосы для дорогого трафика)

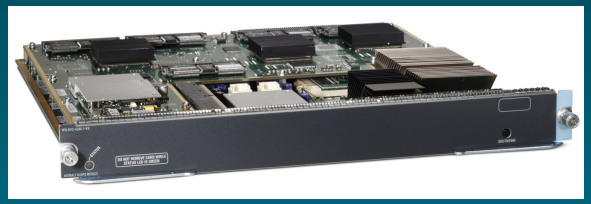
Решение Cisco DDoS

Устройства и сервисные модули

Отражение DDoS:

Cisco Guard XT 5650

Cisco Anomaly Guard Module



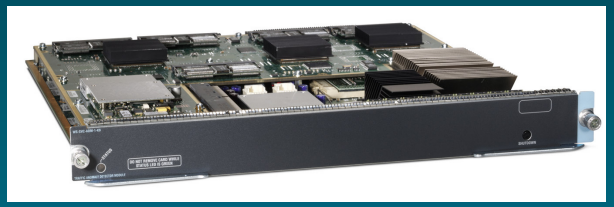
АНАЛИЗ И ОТРАЖЕНИЕ атак

ОЧИСТКА ПО ТРЕБОВАНИЮ

Обнаружение DDoS:

Cisco Traffic Anomaly Detector XT 5600

Cisco Traffic Anomaly Detector Module



ОБНАРУЖЕНИЕ атак и очистка по требованию или перенаправление

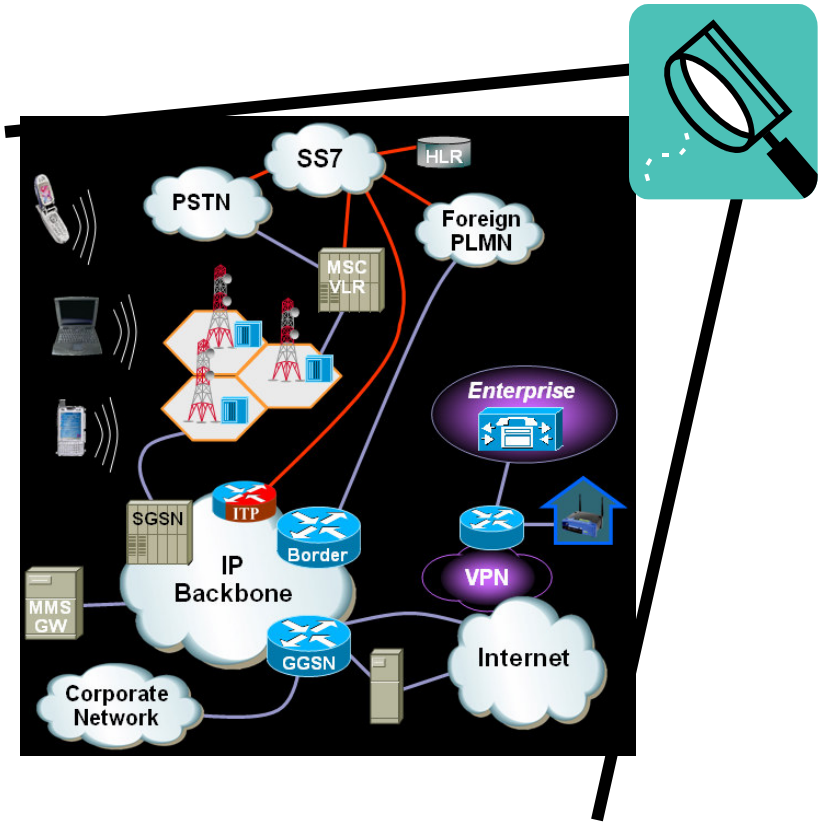
Мониторинг КОПИИ ТРАФИКА

Гибкость внедрения.
Аналогичные функции и производительность.
Взаимодействие в смешанных внедрениях.

Контроль поведения абонентов

Средства контроля поведения

Видимость – критический элемент безопасности – вы не можете контролировать то, чего не видите…



- **Протокол NetFlow (IP-FIX)**
- **Arbor Peakflow SP и CS-MARS для анализа событий безопасности (SYSLOG, SNMP Netflow) и корреляции**
- **Service Control Engine (SCE) или SPAN с Network Analysis Module для изучения приложений и предпочтения пользователей**
- **Anomaly Detector/IPS для контроля различных типов атак**

Решение Cisco Service Control

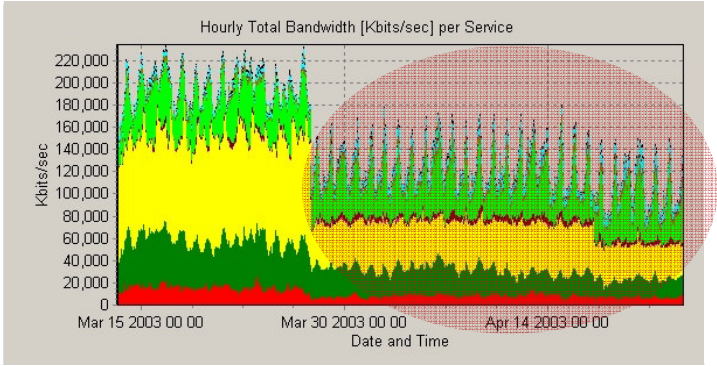
Решение Cisco Service Control использует механизм всесторонней инспекции трафика для предоставления оператору связи полной информации о поведении приложений и абонентов, а также их контроля

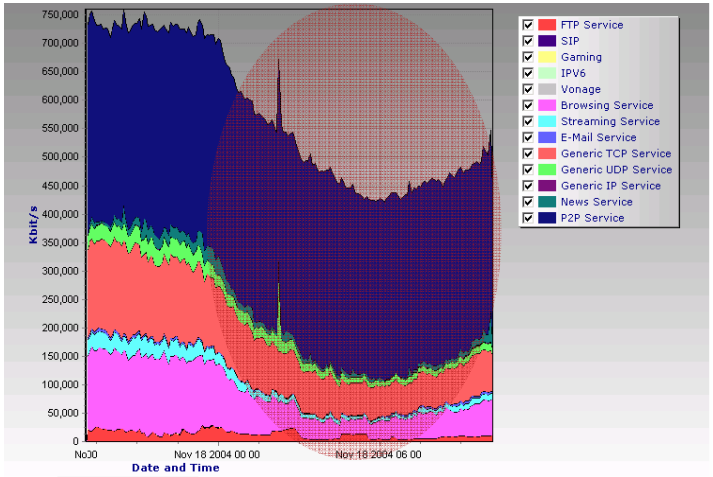
- Аккуратная идентификация и профилирование трафика приложений и абонентов
- Полный анализ на уровнях 4-7 – кто использует сеть и как?
- Реагирование путем QoS, redirect, mark или drop для отдельных абонентов, приложений, времени суток…
- Обнаружение и предотвращение DoS-атак, червей и SPAM-зомби
- Контроль пиринговых приложений, таких как Skype или Kazaa

Видимость и контроль – ключевые аспекты безопасности…

Политики Cisco Service Control

- Контроль приложений
  - По сессиям или полосе пропускания
- Контроль по времени
  - Пиковые загрузки и нерабочее время
- Контекстный контроль
  - Приоритезация трафика важных приложений
- Контроль абонентов
  - Квоты и лимиты для каждого абонента
- Контроль получателя
  - Политики для собственного, пирингового и транзитного трафика



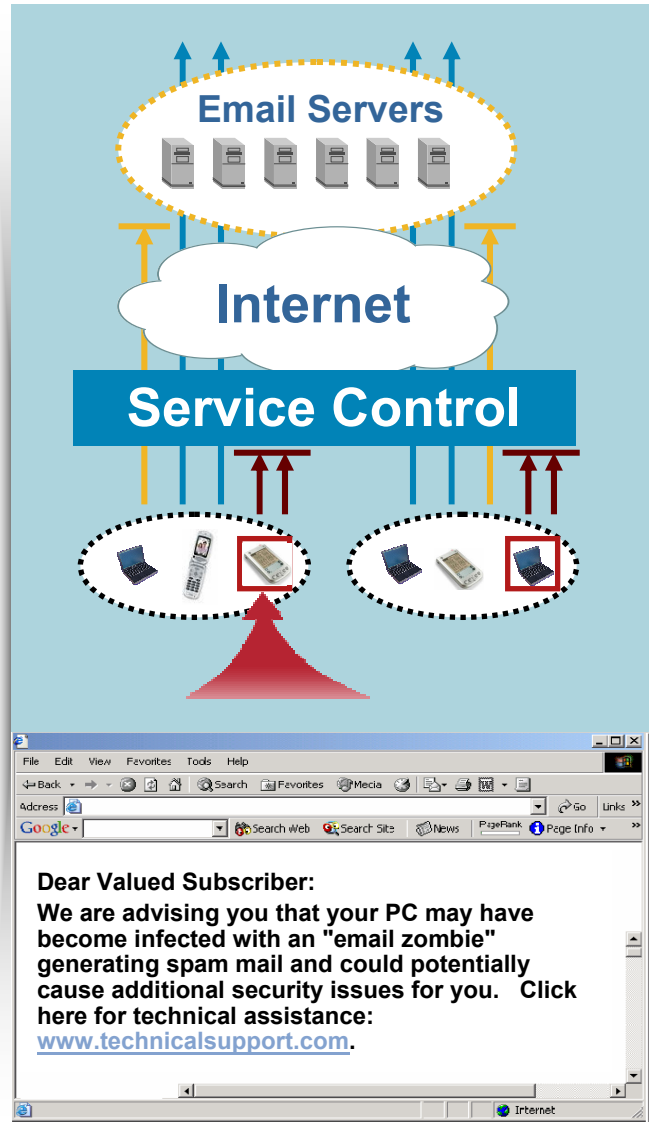


Учет практически любых требований политики безопасности

Безопасность исходящих сервисов

Значение для оператора связи

- Снижение затрат в процессе эпидемий
- Снижение числа заражений абонентов и нагрузки на Call Center
- Рост лояльности пользователей и снижение текучести абонентов
- Возможность продаж дополнительных сервисов по защите
- Сохранение пропускной способности сети



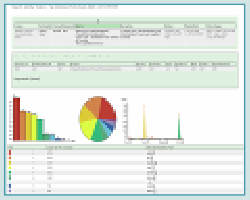
Анализ и корреляция событий

Управление угрозами

МОНИТОРИНГ

АНАЛИЗ

ОТРАЖЕНИЕ



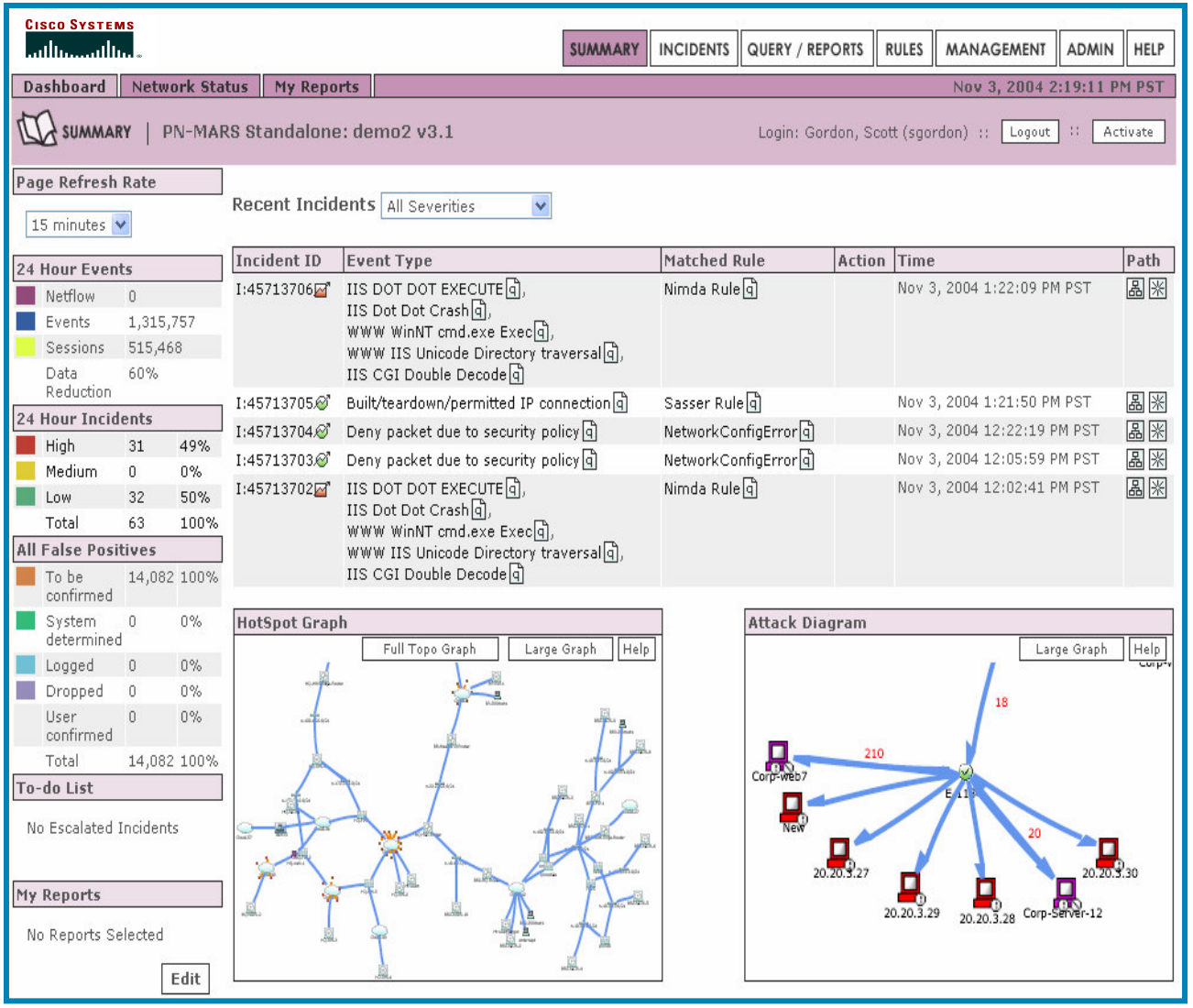
CISCO SECURITY MARS

Повышение устойчивости сети за счет мгновенного реагирования на угрозы

- Быстрая идентификация угроз
- Понимание топологии для фокусного реагирования
- Корреляция событий
- Мультивендорная поддержка

CS-MARS – Security Monitoring, Analysis, and Response

- Широкий спектр поддерживаемых средств защиты
- Анализ и корреляция
- Обнаружение аномалий
- Инвентаризация защищаемой сети и ее визуализация
- Визуализация атаки на карте сети
- Отражение атаки, в т.ч. координированное
- Рекомендации по отражению
- Интеграция с CSM



Защита от вирусов и червей

3 направления борьбы

- Network Admission Control (на клиенте)

  Контроль пользовательского устройства на соответствие политике безопасности

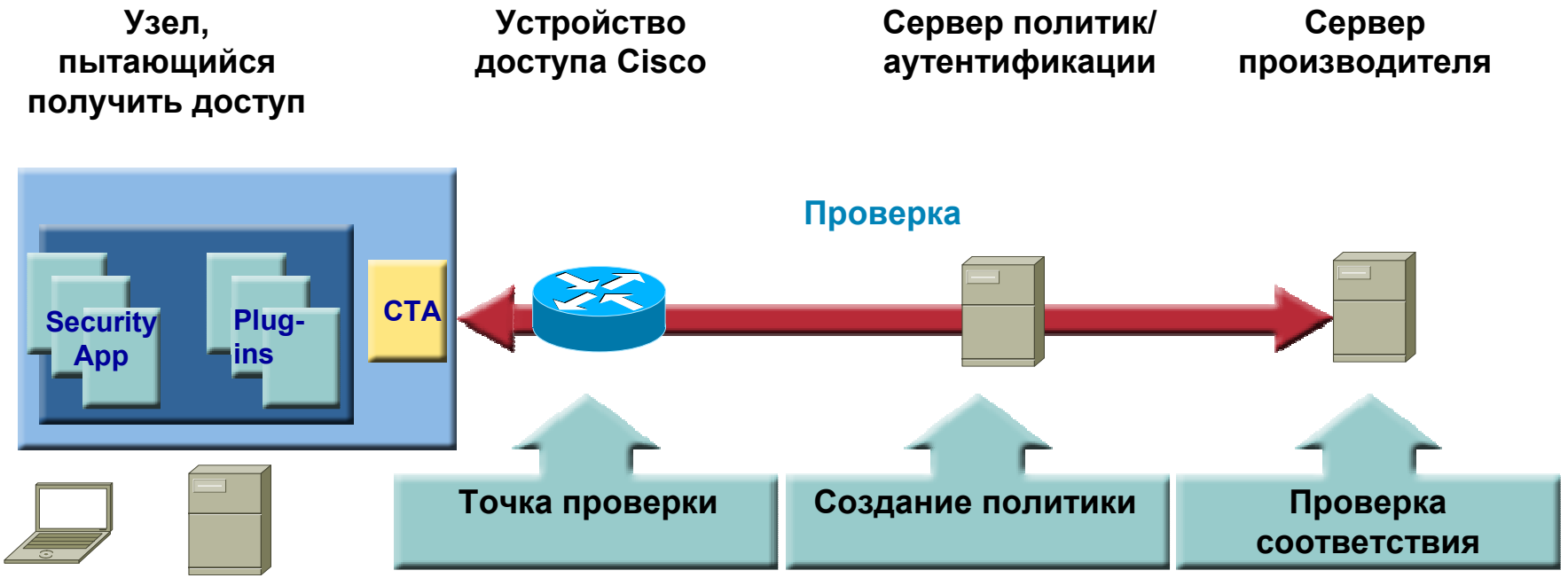
- Сетевой антивирус

  Сканирование сетевого трафика в поисках вредоносных программ

- Антивирус на клиенте

  Сканирование вирусов в памяти и на диске пользовательского устройства

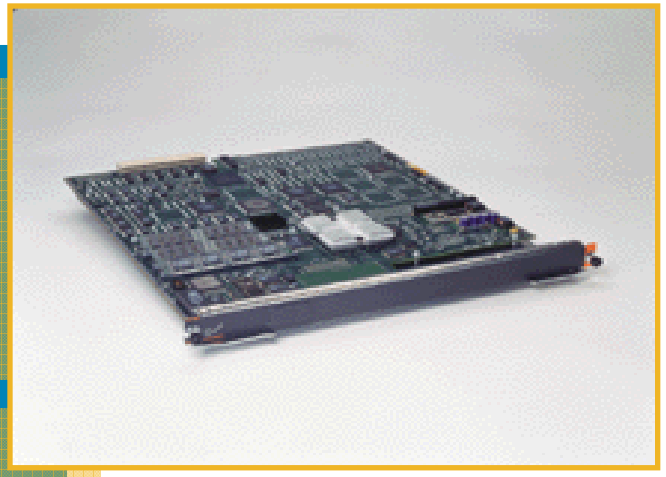
Cisco Network Admission Control (NAC)



- Базируется на политике соответствия конечного узла требования корпоративной безопасности
- Пользователя обязывают выполнять требования политики безопасности

Защита периметра

Catalyst 6500 / 7600 Router Firewall Services Module



- Идеальное решение для сетей требующих мультигигабитной пропускной способности, поддержки VLAN и контроля трафика на 2-7 уровнях

- Базируется на Cisco PIX Firewall
- Пропускная способность - 5,5 Гбит/сек
- Поддержка до 4-х модулей в шасси
- Виртуальные межсетевые экраны и прозрачный МСЭ 2-го уровня

Fabric Enabled

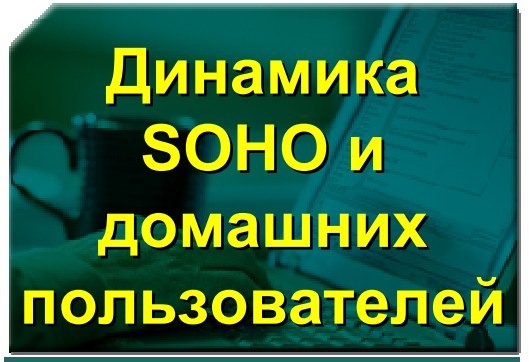
- Отказоустойчивость между модулями
- Поддержка для IOS, CatOS и гибридного режима на Catalyst 6500

Новые сервисы… сервисы безопасности

Потребность в новых сервисах

- Оптимизация затрат
- Непрофильный бизнес
- Продуктивность
- Масштабирование сервисов ИТ
- Нет ресурсов

- Необходимость технологий
- Рост бизнеса
- Нехватка экспертизы
- Продуктивность



- Много сервисов
- Много устройств
- Простота
- Безопасность
- Персонализация
- Нехватка экспертизы

Требования для Managed Services

Требования рынка

- Онлайн-бизнес
- Режим 24 x 7
- Глобализация
- Виртуальный офис
- Связь ИТ и бизнеса

Финансовые требования

- Снижение CapEx / OpEx
- Офшор
- Фокус на TCO/ROI
- Фокус на росте

Организационные требования

- Фокус на продуктивности
- Очень мало квалифицированных специалистов
- Консолидация
- Аутсорсинг

Заказчики

Партнеры

Поставщики

Сотрудники

Требования соответствия

- Контролирующие органы
- Sarbanes-Oxley Act of 2002
- Gramm-Leach-Bliley / HIPAA
- Check 21, USA PATRIOT, Basel II

Требования управления риском

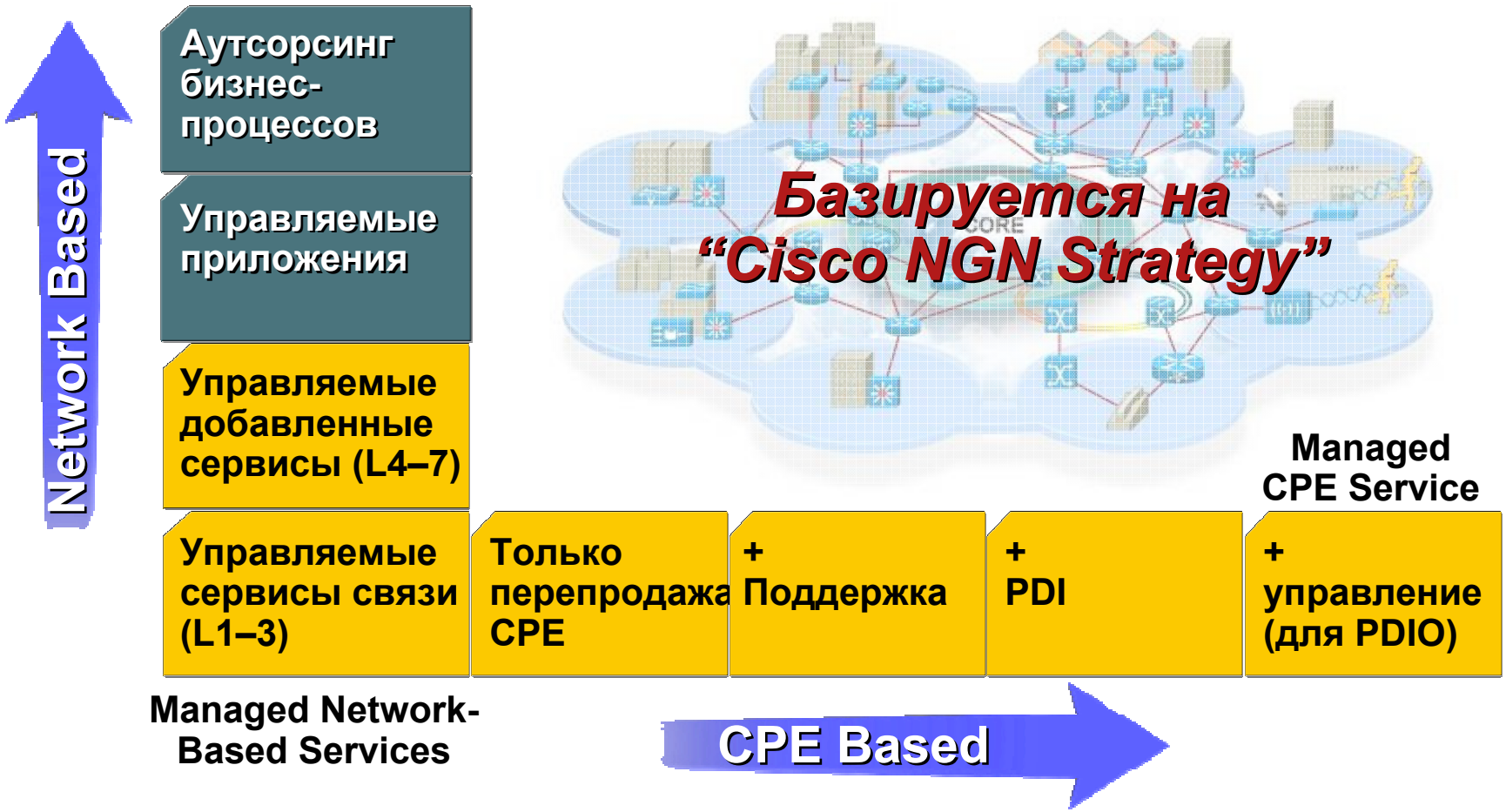
- Рост числа угроз
- Рост числа уязвимостей
- Увеличение рисков и их покрытия
- Фокус на Business Continuity

Технологические требования

- Интеллектуальная сеть
- Рост объемов хранения
- Мобильность / PDA / Wi-Fi / Wider-Fi
- Управление приложениями
- Сетевые вычисления

Стратегия Cisco Managed Services

Максимизация доходов SP через Network и CPE-Based Managed Services



Безопасность, как способ заработать

- Managed Security Services – набор услуг по защите сети заказчика, не имеющего собственных ресурсов
- Способ зарабатывать на безопасности
  - Безопасность периметра клиента и защита от DDoS-атак
  - Защита от спама и контроль содержимого
  - Обеспечение конфиденциальности (VPN)
  - Управление средствами защиты клиента
  - Сканирование сети заказчика
  - Реагирование на инциденты
  - Защита хостинга
  - Сдача в аренду средств защиты
- Конкурентное преимущество

Преимущества для оператора

- Рост доходов
- Быстрая окупаемость инвестиций
- Повышение удовлетворенности и лояльности клиентов
- Расширение клиентской базы
- Отличие от конкурентов

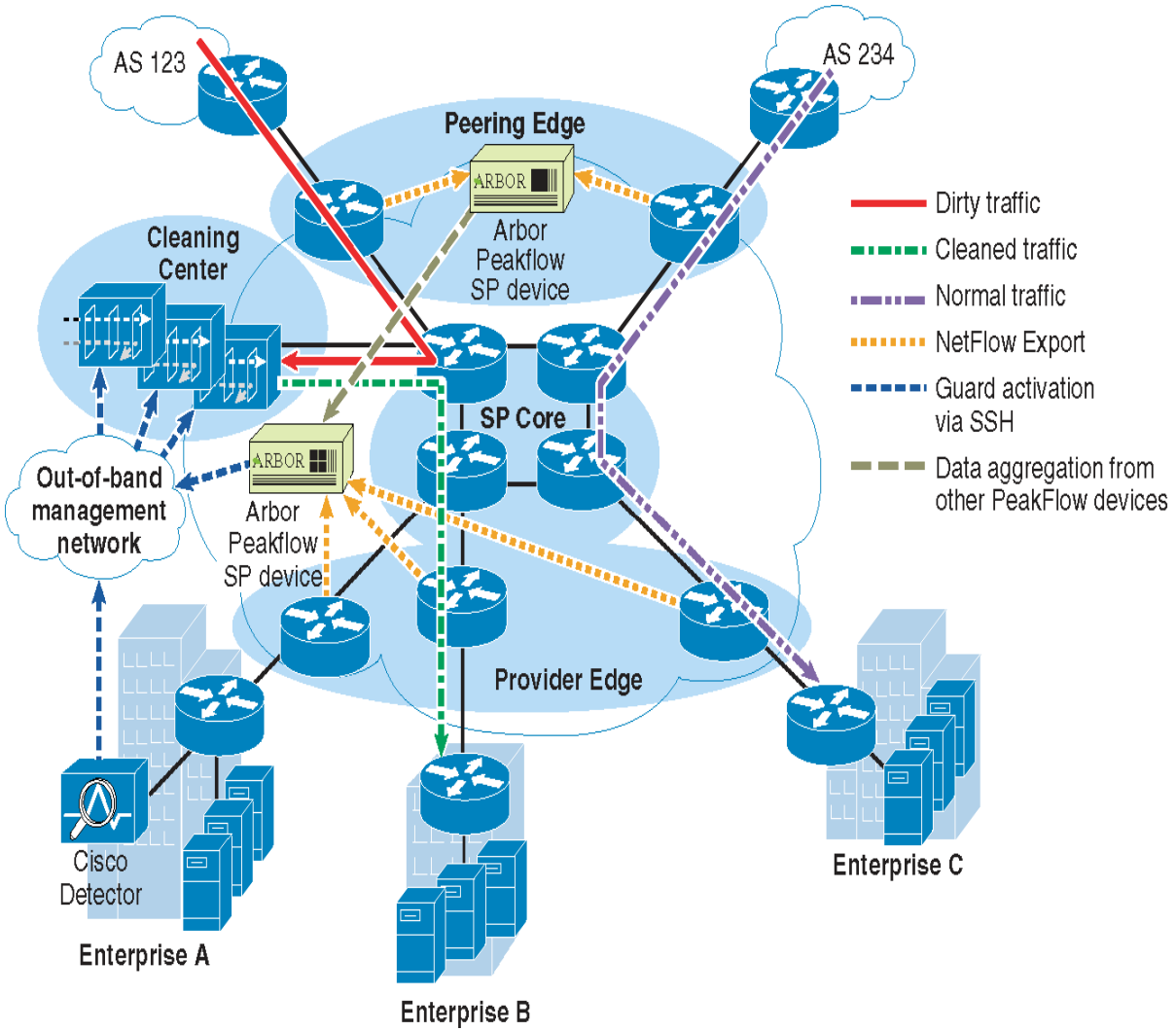
Преимущества для клиента

- Концентрация на профильном бизнесе
- Снижение TCO своей инфраструктуры защиты
- Снижение стоимости ущерба в случае атаки
- Снижение времени простоев
- Повышение надежности и доступности бизнес-процессов

Категории получения доходов от ИБ

- Clean Pipes. Набор сервисов, которые клиент покупает у SP для повышения уровня своей доступности
- Service Control. Набор сервисов, которые могут продаваться или бесплатно предлагаться клиентам SP. Это решение фокусируется на трафике, приходящем из сетей клиентов SP
- Управляемая безопасность CPE/CE. Набор защитных сервисов, которые SP использует для управления CPE
- Network Based Security Services. Virtual Firewall, Virtual IDS и другие защитные сервисы, предлагаемые клиентам для повышения уровня защищенности
- Контроль границ. Защита взаимодействия с другими SP.
- И многое другое…

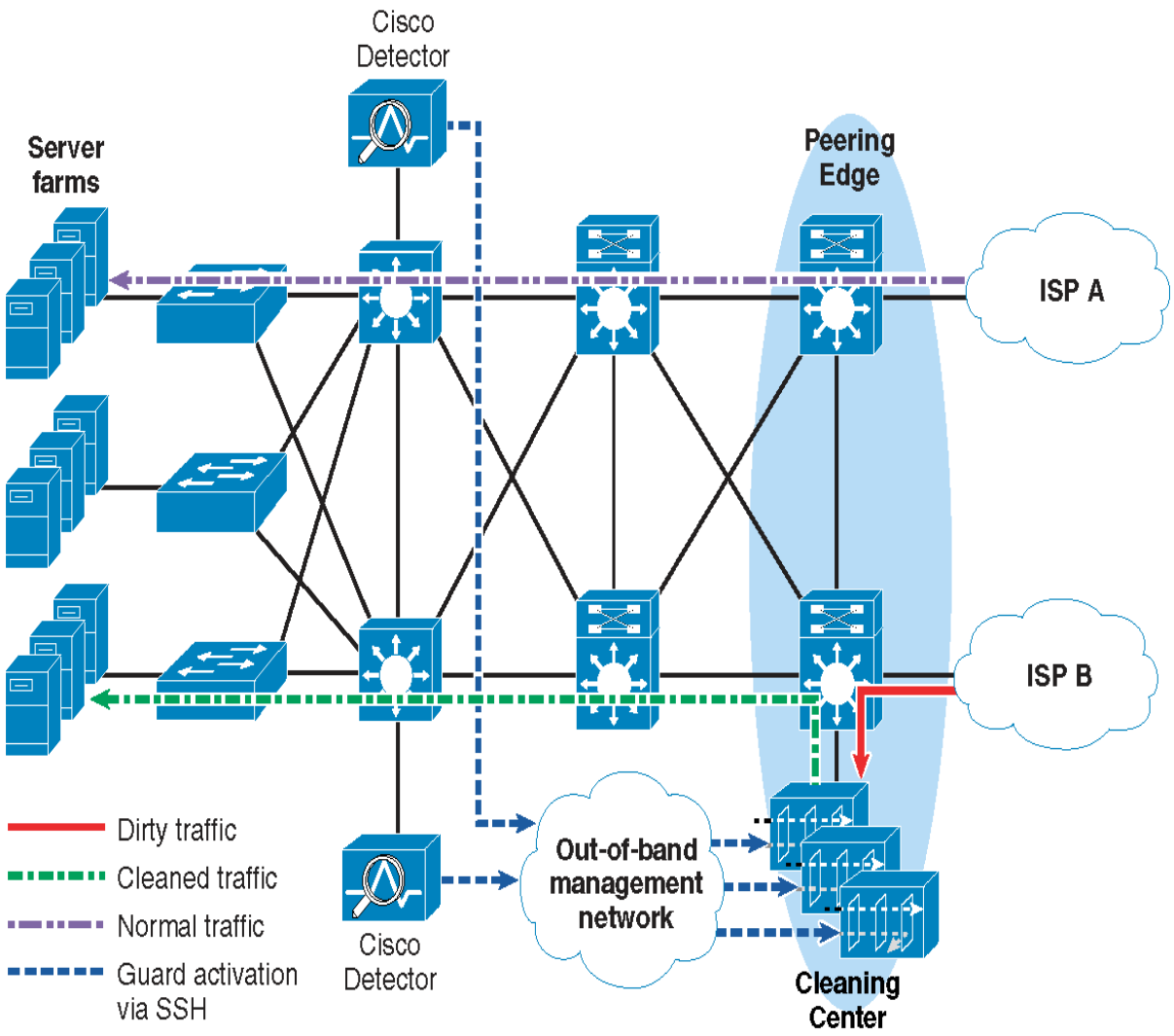
Managed Network DDoS Protection



Ключевые возможности

- **Новая модель генерации доходов для оператора**
- **Защита последней мили**
- **Дополнительная страховка клиентов от нарушения доступности бизнеса**
- **Cisco Detector (как CPE) обеспечивает взаимодействие с центральным Cisco Guard**
- **NetFlow + Peakflow SP обеспечивают взаимодействие с Guard**
- **Отражение при помощи Guard по подписке или по требованию**
- **Отчет об атаках на клиента экспортируется и помещается на портал оператора**

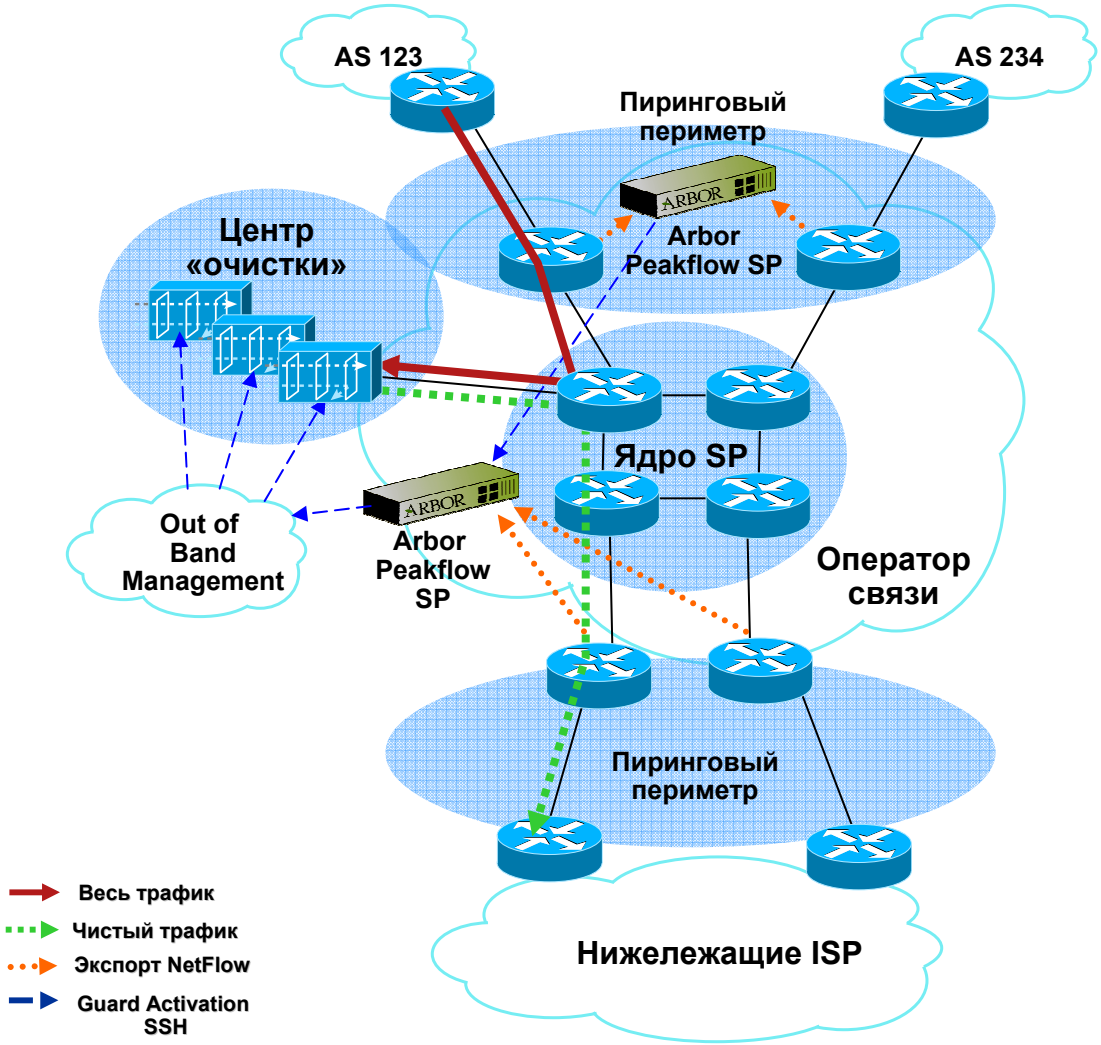
Managed Hosting DDoS Protection



Ключевые возможности

- Новая модель генерации доходов для хостинговых компаний
- Защита критичных серверов Web и приложений
- Cisco Detector обеспечивает обнаружение аномалий с глубоким анализом трафика
- Отражение - ближайшее к цели атаки
- Guards размещается ближе к точке входа
- Отражение при помощи Guard по подписке или по требованию

Managed Peering Point DDoS Protection



Ключевые возможности

- Новая модель генерации доходов для оператора
- Нижележащие ISP получают свободные от DDoS соединения
- Максимизация полосы пропускания для легитимного трафика
- Netflow + Arbor Peakflow SP обеспечивают анализ и видимость сети
- Снижает DDoS в Интернет

Модель лицензирования услуг

- Модель получения дохода

  Subscription service – клиент платит X% от стоимости передачи трафика или полосы пропускания за гарантии обеспечения доступности

  Subscription service – клиент платит обычную стоимость за передачу трафика или полосу пропускания, а затем доплачивает фиксированную стоимость за обнаружение и отражение атак

  On-demand – клиент платит за очистку полосы пропускания после звонка о начале атаки

  Оплата за выделенную или разделяемую инфраструктуру

  Перепродажа downstream SP, которые покупают транзит – перепродажа сервиса, например, ‘Clean Pipes’

Managed CPE Service

- Лучше чем управлять множеством устройств
  - Ниже CapEx
  - Ниже TCO
  - Быстрота внедрения
  - Эффективность управления
  - Интеграция функций защиты с другими сервисами
- Сертифицированный VPN

Пример ROI

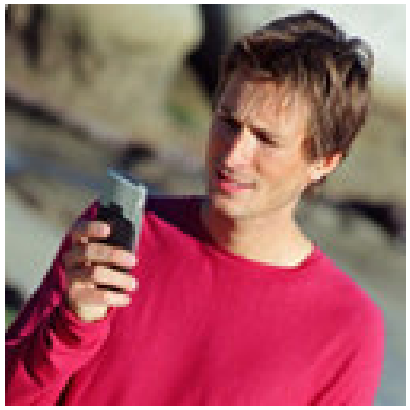
- Защита крупных клиентов от DDoS-атак
  - Решение – Cisco Guard\Traffic Anomaly Detector
  - Ежемесячная плата – 2000 у.е.
  - ROI – 6-7 месяцев при 15 заказчиках в год
- Базовый уровень защиты домашних пользователей
  - Решение – на базе IOS Advanced Security в Cisco 7301
  - Ежемесячная плата – 5 у.е.
  - ROI – 4-5 месяцев при 1000 заказчиков
- Расширенный уровень защиты корпоративных пользователей
  - Решение – Catalyst 6503 с МСЭ Cisco FWSM
  - Ежемесячная плата – 100 у.е.
  - ROI – 6 месяцев при 100 заказчиках

Заключение

Cisco SP Security Framework

Cisco Systems SP Security Framework позволяет операторам связи:

- **Модель получения дохода от безопасности**
- **Защищенное внедрение новых сервисов**
- **Защита и сохранение абонентов**
- **Защита инфраструктуры от атак**



- **Эффективное регулирование поведения абонента**
- **Идентификация и реагирование на аномалии и нарушения безопасности**
- **Обеспечение видимости и контроля действий абонентов и сети**
- **Соответствие законодательству**

Вопросы и ответы