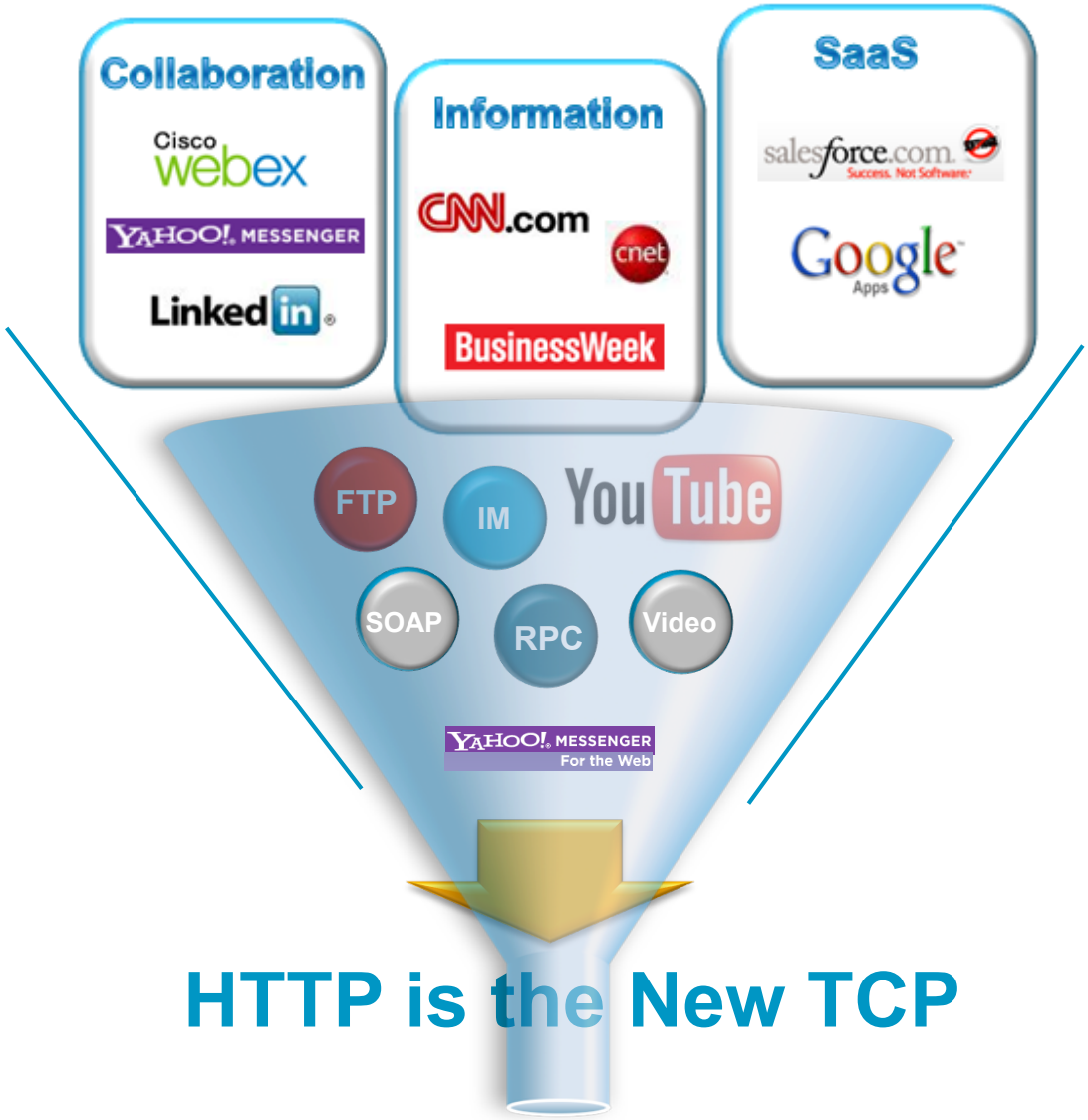
# Cisco IronPort Secure Web Gateway

**Pavel Rodionov**
**Systems Engineer, Cisco IronPort**

*prodiono@cisco.com*

# Объемы web-трафика увеличиваются

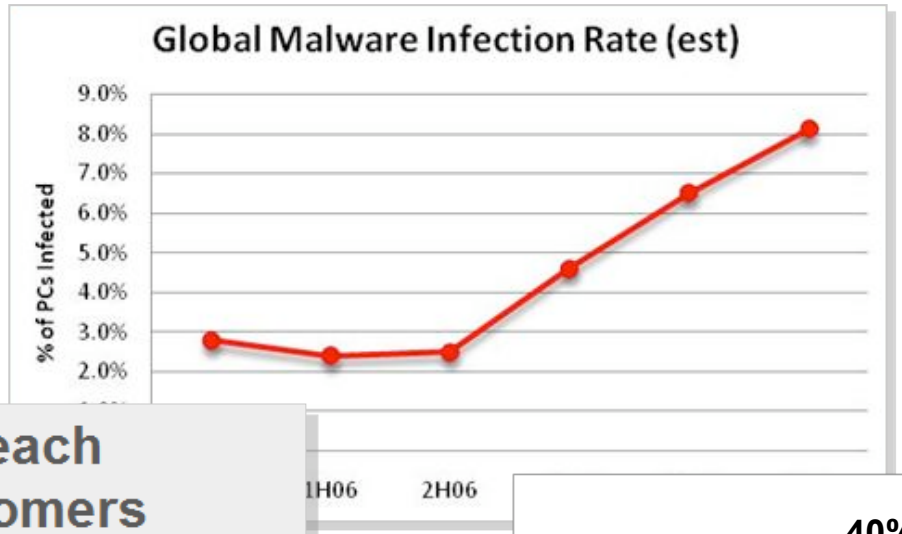
## Общий путь в сеть и их сети




- Растет использование web для бизнес-приложений
- Растет количество туннелированных приложений

# Проблемы web бизнеса

## Malware




## Утечки данных


## Нарушения правил использования

**40% потерь**
**в производительности**
в связи с использованием web для личных нужд во время работы

**Риск нарушения законодательства**
когда запрещенный контент загружается пользователями

# Взломанные Вебсайты. *Невидимая угроза*


## Massive Attack: Half A Million Microsoft-Powered Sites Hit With SQL Injection

By Scott Gilbertson ✉ April 28, 2008 | 8:04:40 AM Categories: Security

# Невидимые угозы очень видимы…

- **Взломанные web-узлы** отвечают за распространение ***более 87% всех Web-угроз сегодня***
- Более **79%** web-узлов с вредоносным кодом **легитимные****
- **9 из 10** web-узлов уязвимы к атакам**
- **Cross-site Scripting** (XSS) и **SQL Injections** лидируют в числе разных методик взлома
  - Cross-Site Scripting (7 их10 узлов)**
  - SQL Injection (1 из 5)**


*Source: IronPort TOC
**Source: White Hat Security, Website Sec Statistics Report 10/2007 & PPT 8/2008

# Хакеры атакуют легитимные web-узлы


- Botnets настраиваются и внедряют malware в web-узлы с помощью SQL Injections **используя уязвимости в web-приложениях**
- Хакеpi используют SQL Injections для вставки JavaScript iFrames, которые перенаправляют пользователей на web-сайты, на которых хостится malware

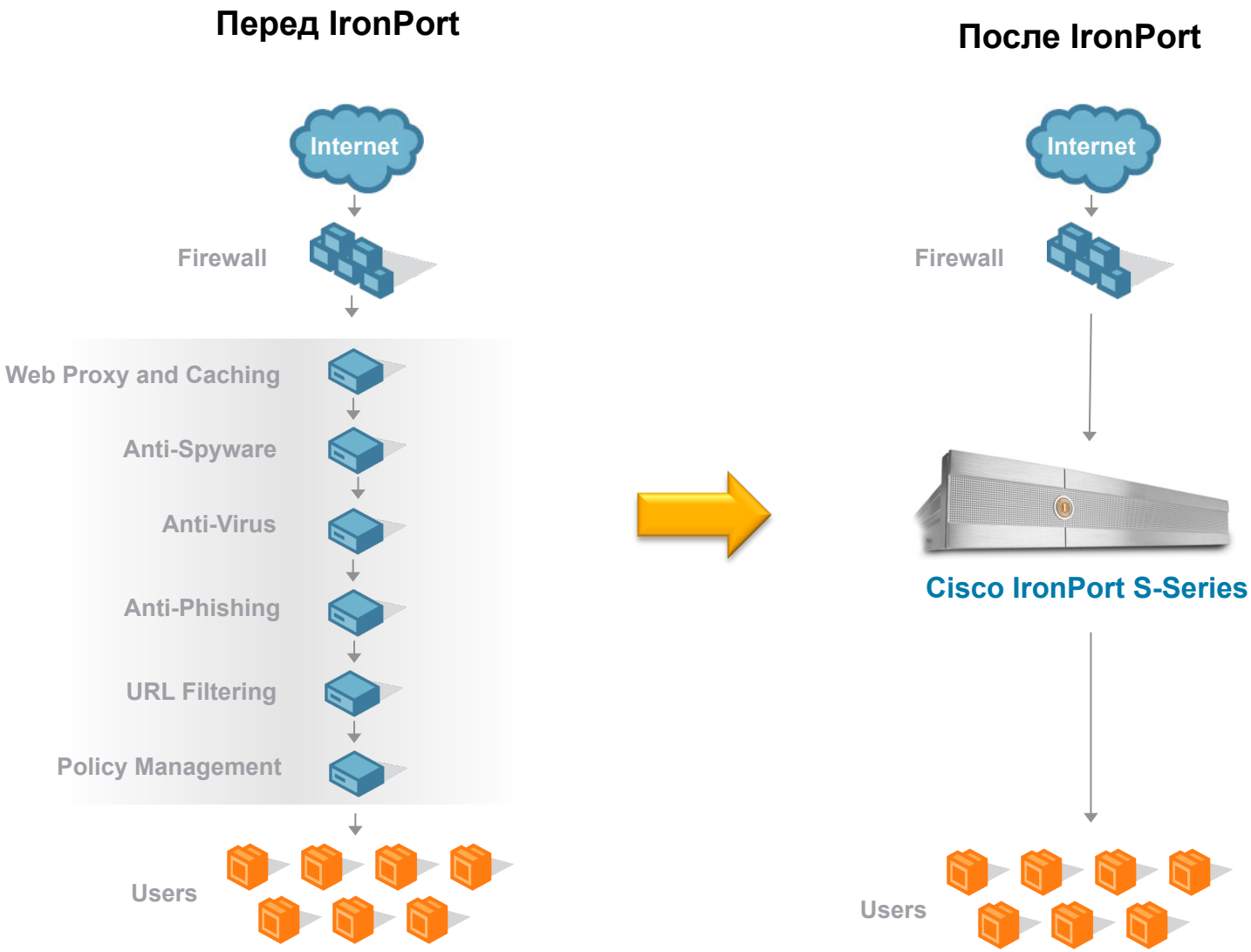
# Шлюз безопасности Web Cisco IronPort

## Направление на бизнес-проблемы

Cisco IronPort S-Series

# Шлюз безопасности Web следующего поколения

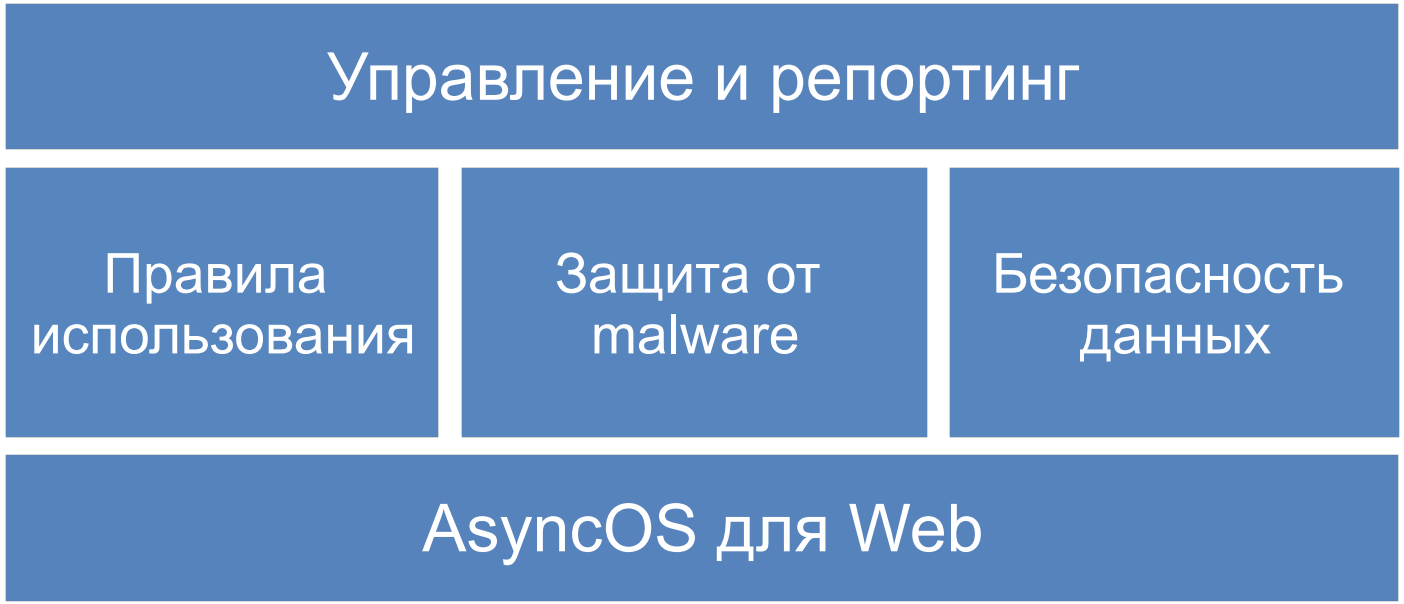
Консолидация увеличивает эффективность работы



# Cisco IronPort S-Series

## Мощное решение безопасного web-шлюза

- Наиболее эффективная защита от web-malware
- Управление правилами использования и защита от утечки данных
- Высокая производительность
- Интегрированное решение – оптимальная стоимость



# Применение правил использования

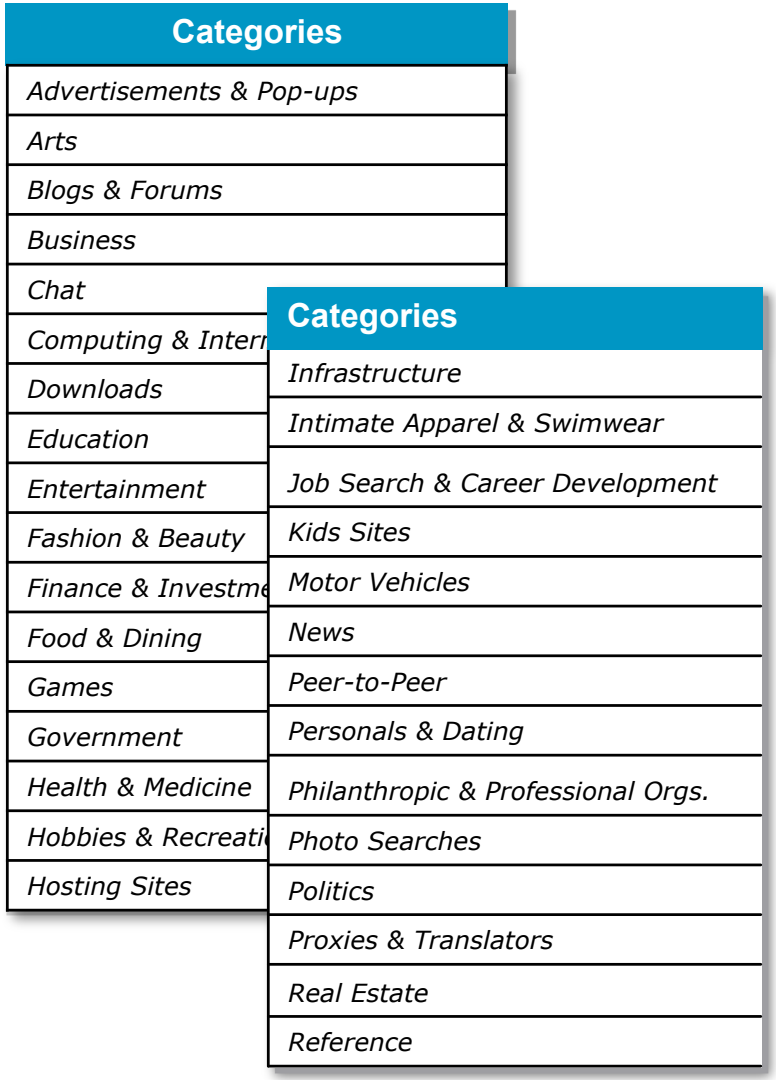
## Доступность и контроль для Web и Web приложений


- Система URL фильтрации
- Фильтрация приложений и объектов
- Интегрированная идентификация и аутентификация

# IronPort URL Filters

## Точность и контроль web трафика

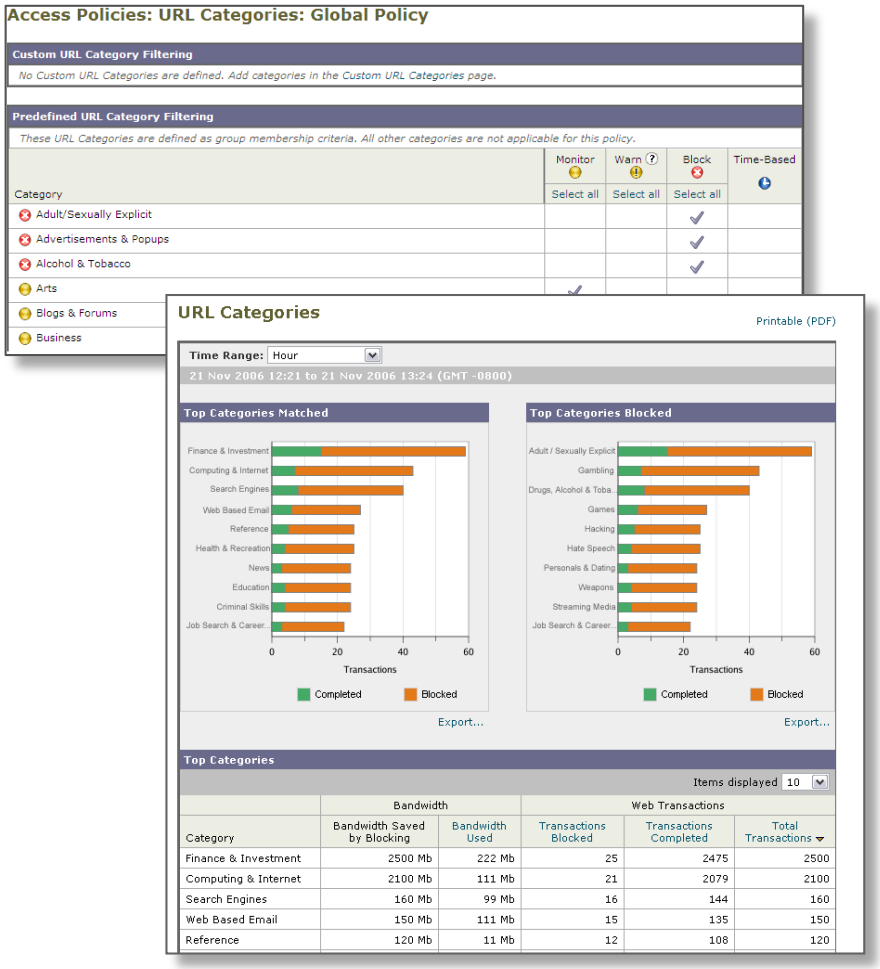
- База данный масштаба предприятия
  - 52 категории
  - Более 21 млн сайтов, ~3.5 миллиарда страниц
  - 1/3 базы международная
- 24 x 7 мониторинг
- Регулярные, автоматические обновления



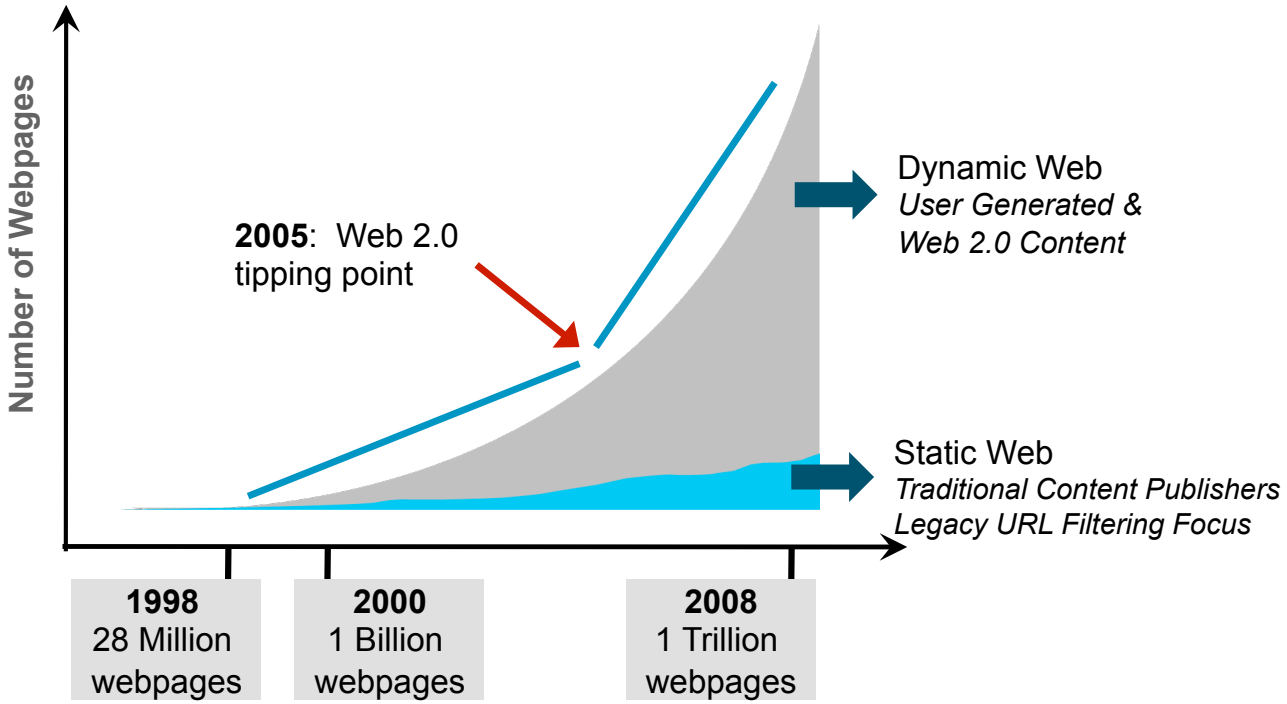
# IronPort URL Filters

## Всестороннее управление и доступность

- Гибкое управление политиками
  - Политики на группу, на пользователя
  - Набор действий – блокирование, мониторинг, предупреждение
  - Политики по времени
  - Пользовательские категории и уведомления
  - Гостевые политики
- Доступность
  - Простые для понимания отчеты
  - Система журналирования
  - Полноценная система предупреждений



# Web: Громадный, растущий и недолговечный




## Громадный

**1 триллион**
уникальных URL

## Растущий

**1 миллиард**
новых страниц каждый день

## Недолговечный

**30%**
доменов перемещаются каждый год

*Source: Multiple, including Cisco SIO, Google, Wikipedia*

# Проблема заказчика

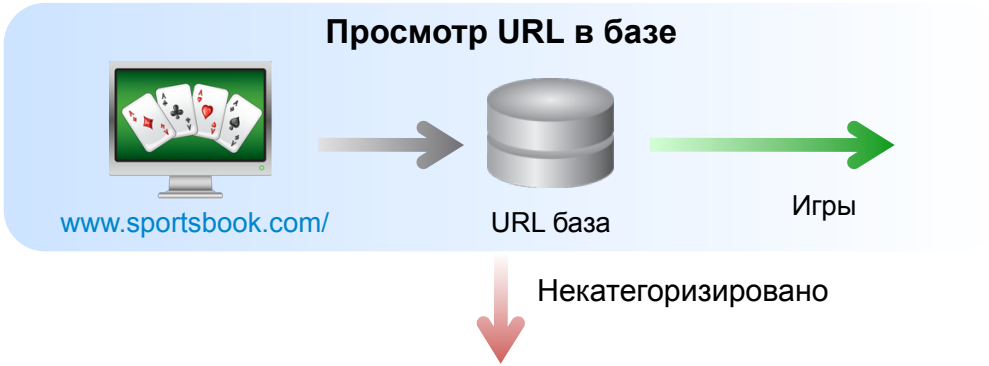
## «Темный» web

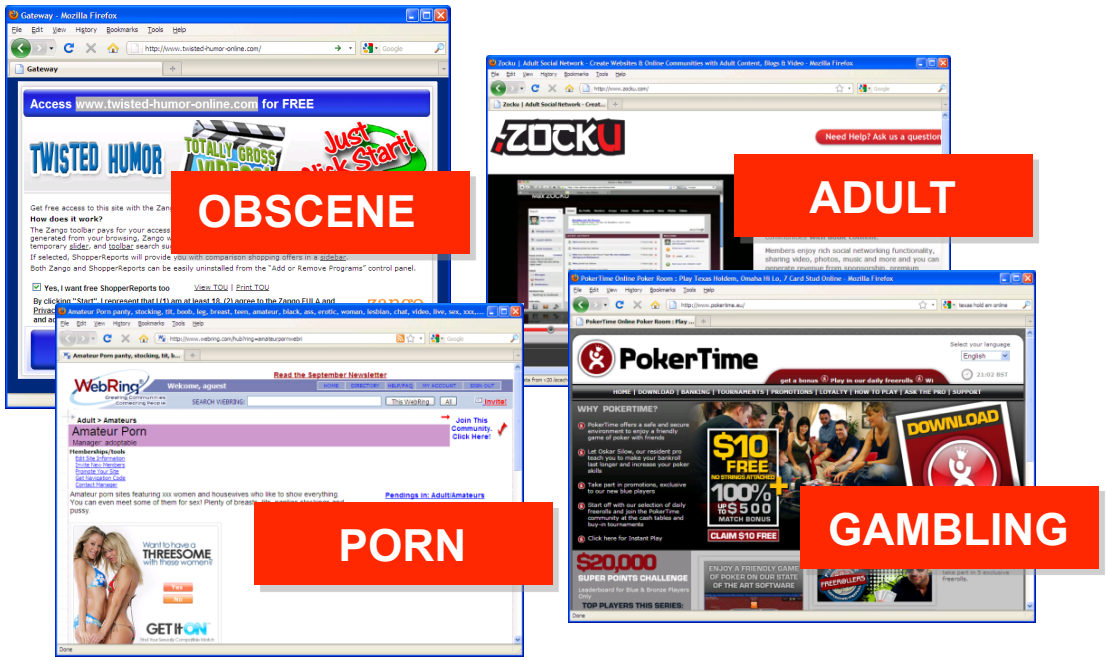
*80% web некатегоризировано, динамическое или же недоступно*

- *Динамический контент*
- *Сайты, защищенные паролем*
- *Контент, генерируемый пользователями*
- *Короткоживущие сайты*

# Проблемы «темного» Web

## Снижается эффективность систем традиционной URL фильтрации

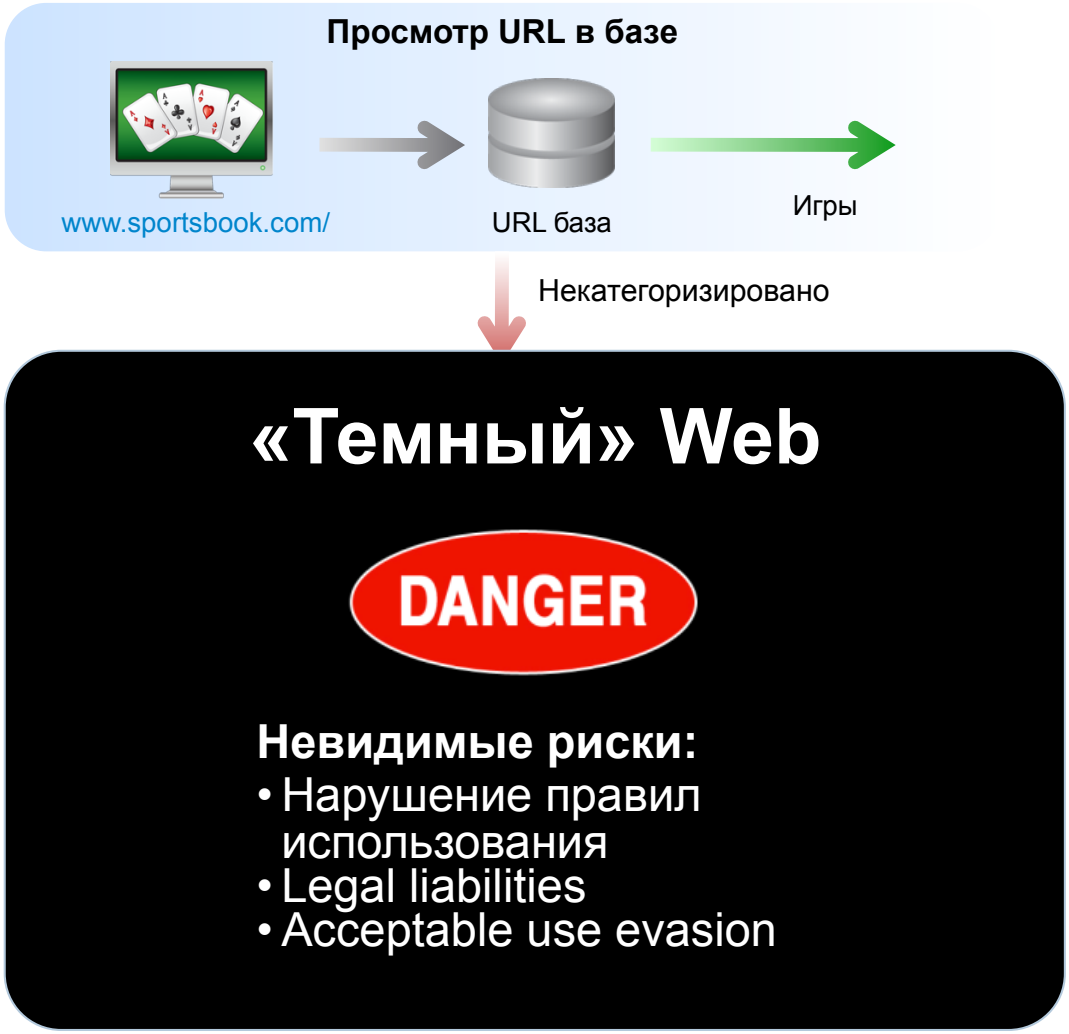



- Традиционная фильтрация основывается на web «пауках» **и ручной классификации**
- Базы данных добавляют тысячи URL в день...web добавляет **миллионы**
- **95%** web не будет категоризировано к 2015

# Проблемы «темного» Web

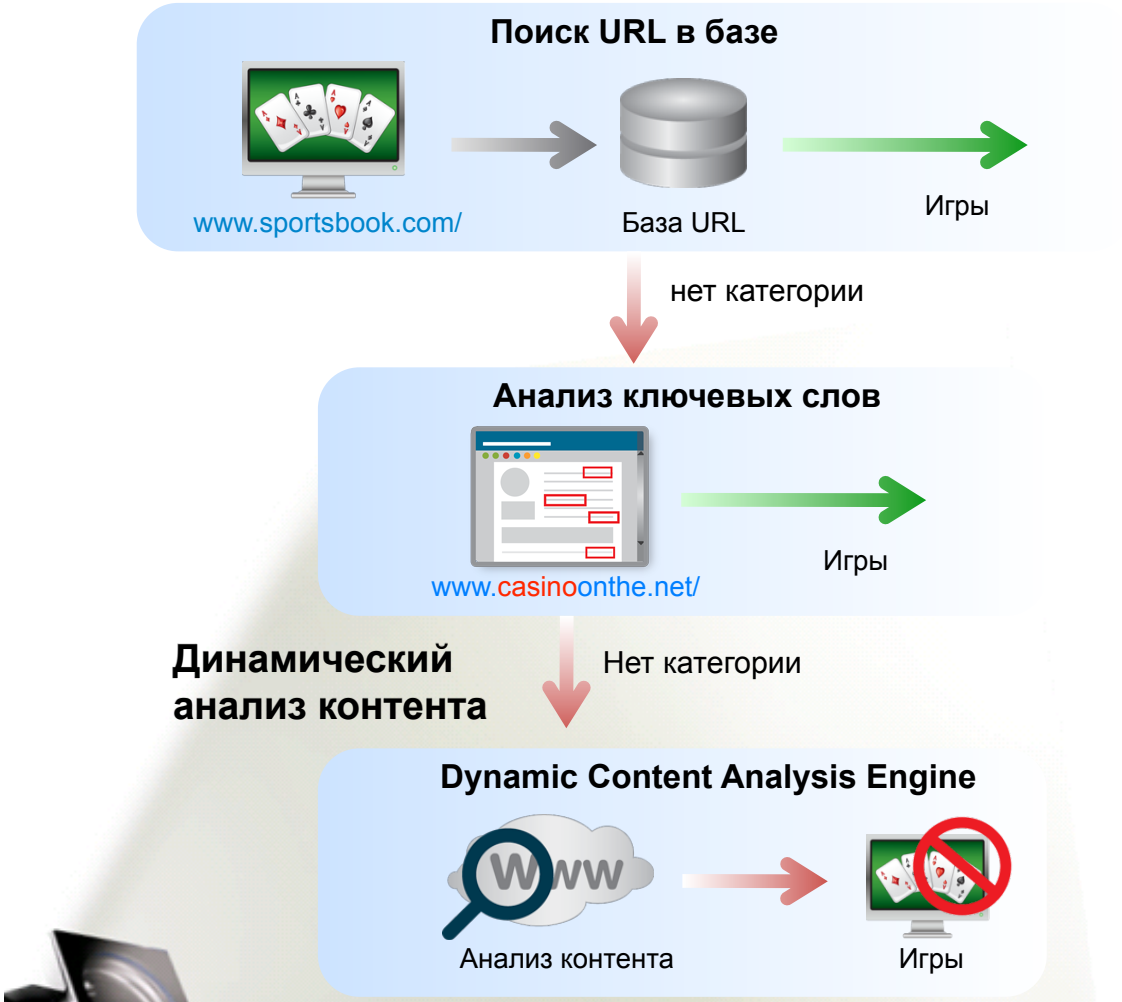
## Снижается эффективность систем традиционной URL фильтрации




- Традиционная фильтрация основывается на **и ручной классификации**
- Базы данных добавляют тысячи URL в день...web добавляет **миллионы**
- **95%** web не будет категоризировано к 2015

# Представляем технологию Cisco IronPort Web Usage Controls

Луч света в темном Web




- Одна из самых эффективных баз URL
  - 65 категорий
  - Обновления каждые 5 минут
  - Использует Cisco SIO
- Динамический анализ контента позволяет определить 90% of «темного» Web

# Механизм динамического анализа контента

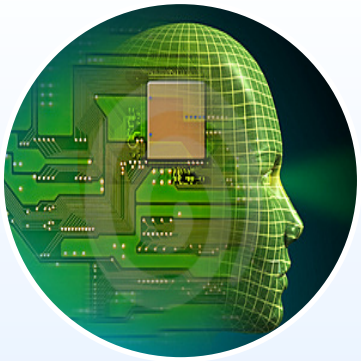
## Идентификация 90% спорного контента в «темном» Web

### Высокая производительность

- Оптимизированный конвейер вынесения решений
- Решение по категоризации меньше, чем за 10 мс
- Незаметно для пользователя

### Настройка для блокируемого контента

- Порнография и сайты «для взрослых»
- Ненависть
- Игровые сайты
- Обход прокси



### Анализ контента в «человеческих» терминах

- Расширенный эвристический анализ, основывающийся на концептном моделировании
- Более высокая точность по сравнению с обычным анализом ключевых слов

**Останавливает на 50% спорного контента больше***

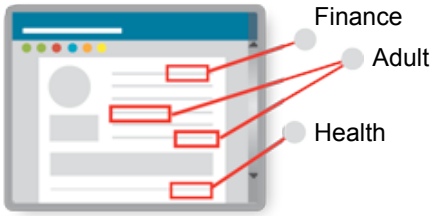
**Source: Cisco SIO, based on data from customer production traffic*

# Как работает этот механизм?

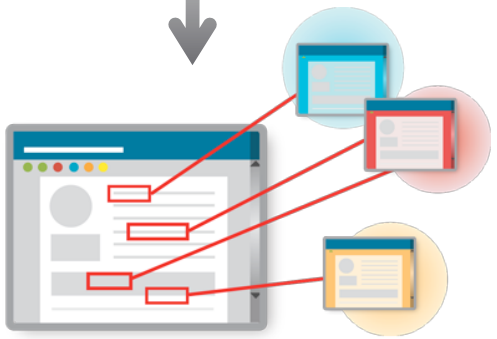
1. Пользователь запрашивает неизвестную страницу.

2. Получает HTTP ответ. Сканирует его для того, чтобы **найти важный текст**.

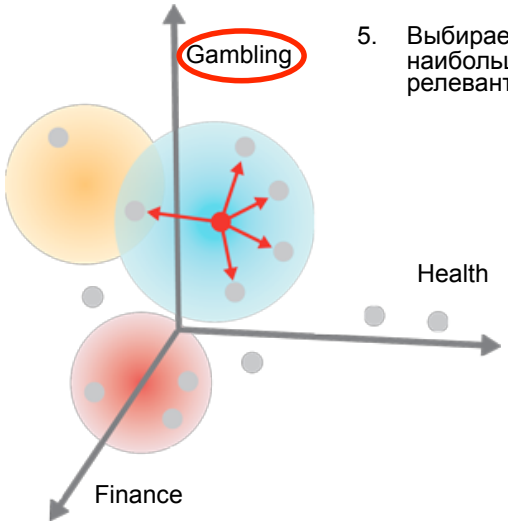
3. Вычисляет **вектор контента**. Каждое измерение – это ссответствие релевантности определенной категории.




4. Вычисляется близость вектора документа с вектором эталонных документов



5. Выбирается категория с наибольшей релевантностью




6. Применяется политика для определенной категории:
Block / Allow / Warn.

# Динамическая категоризация в действии

## Блокирования сайта с любительской порнографией


| | |
|---|---|
| **Вердикт URL списка:** | Нет категории |
| **Вердикт ключевых слов:** | Нет категории |

**Механизм динамического анализа контента**

**Термины, определенные в векторе:**

- “Amateur Porn”
- “erotic materials”
- “FEDERAL LAW”
- “laws”

**Concept Vector: Top Matches**

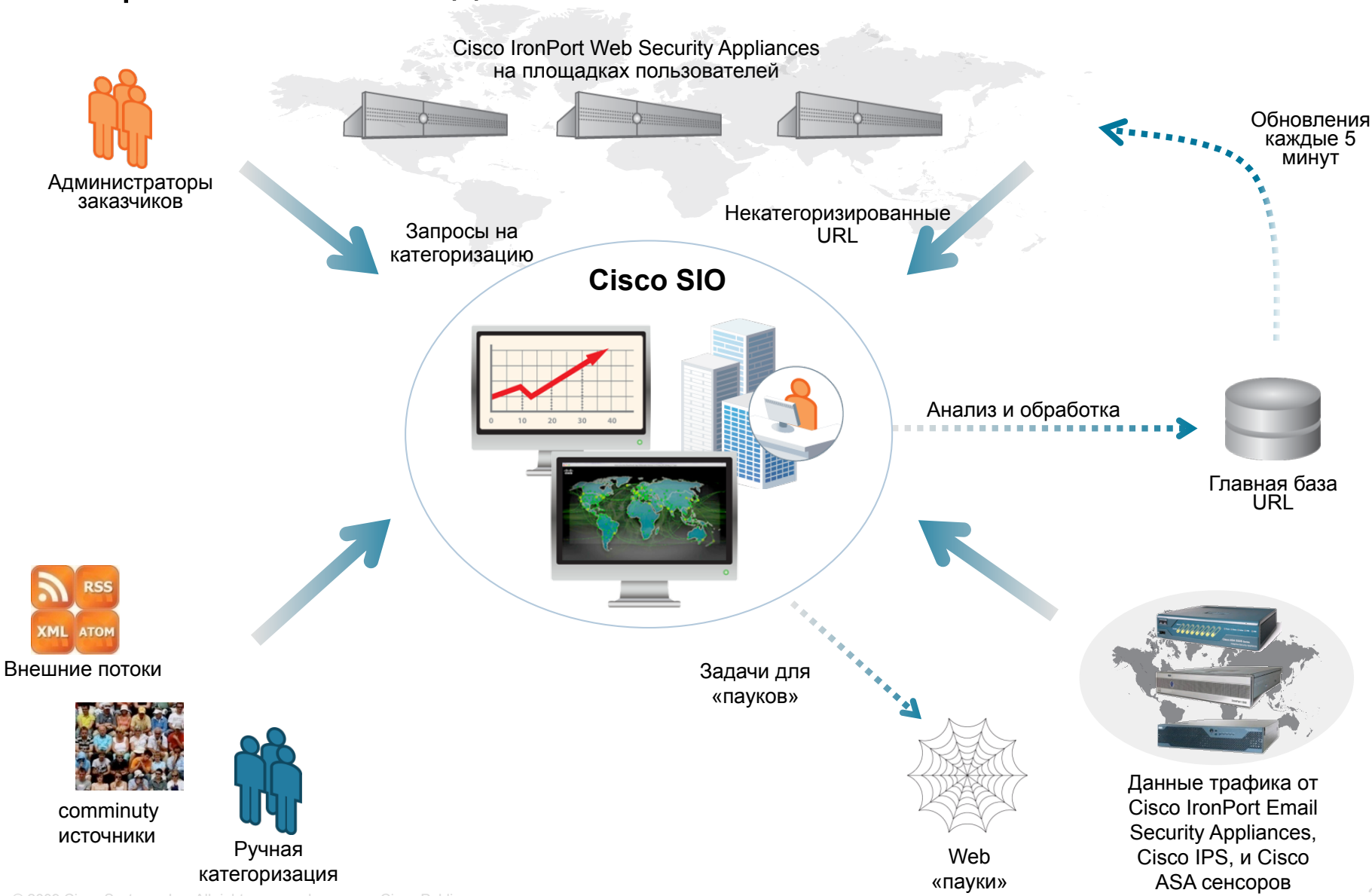
| Model Doc | Confidence | Category |
|---|---|---|
| 001357 | 67.84% | Pornography |
| 001511 | 57.65% | Adult |
| 000613 | 54.90% | Pornography |

Verdict: **Порнография**

Action: **Блокировать**

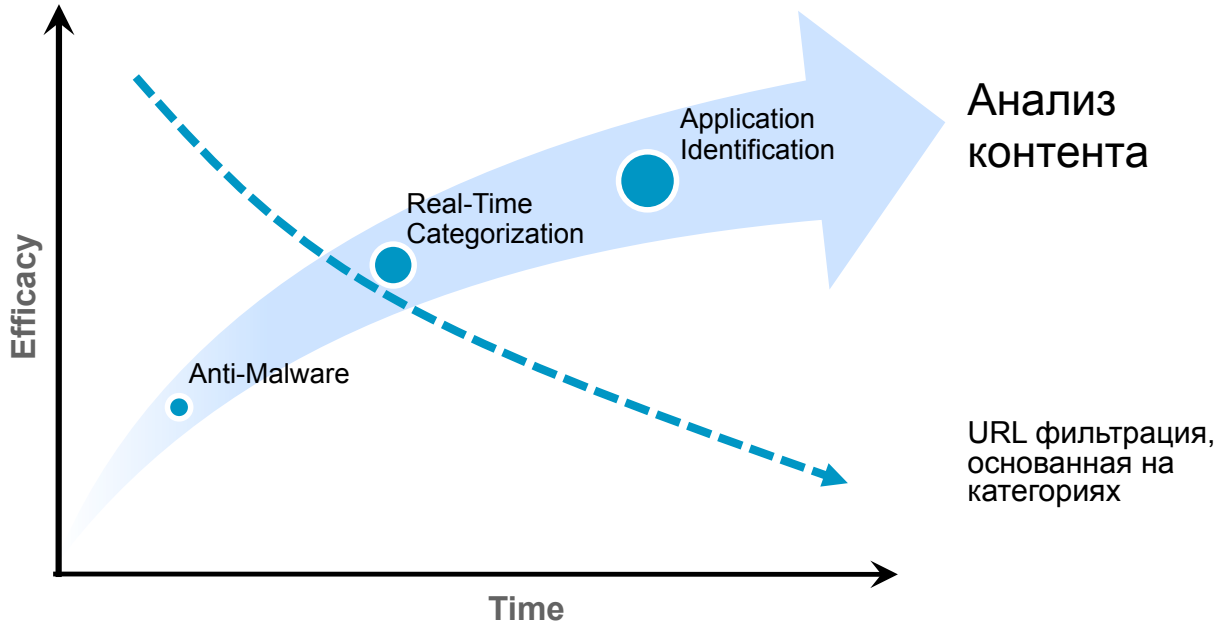
# Cisco Security Intelligence Operations (SIO)

## Великолепная эффективность благодаря объему обрабатываемых данных



# Безопасность и управление контентом

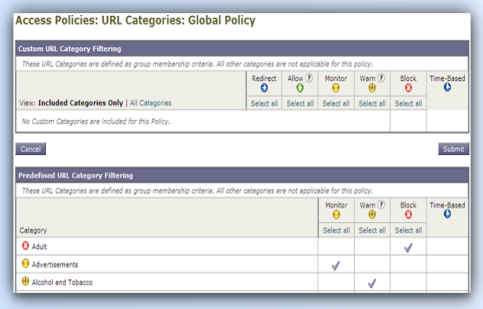
## Возможность анализа web-контента становится все более важной

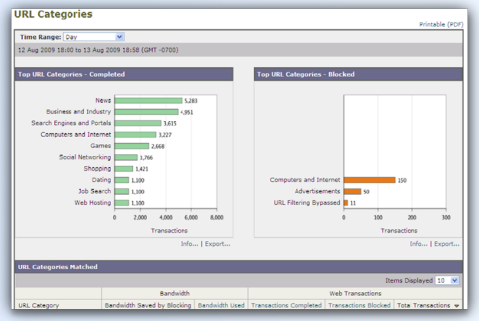



- Cisco IronPort DVS: Защита от malware в зависимости от контента
- Cisco IronPort Web Usage Controls: Политики использования в зависимости от контента

# Cisco IronPort Web Usage Controls

Прекрасная эффективность, богатые возможности управления, полная доступность данных




## Управление

- Политики на группу, на пользователя
- Несколько действий: Блокировать, предупредить, мониторить
- Политики, основанные на времени
- Неограниченные пользовательские категории
- Настраиваемые уведомления для пользователей

## Доступность

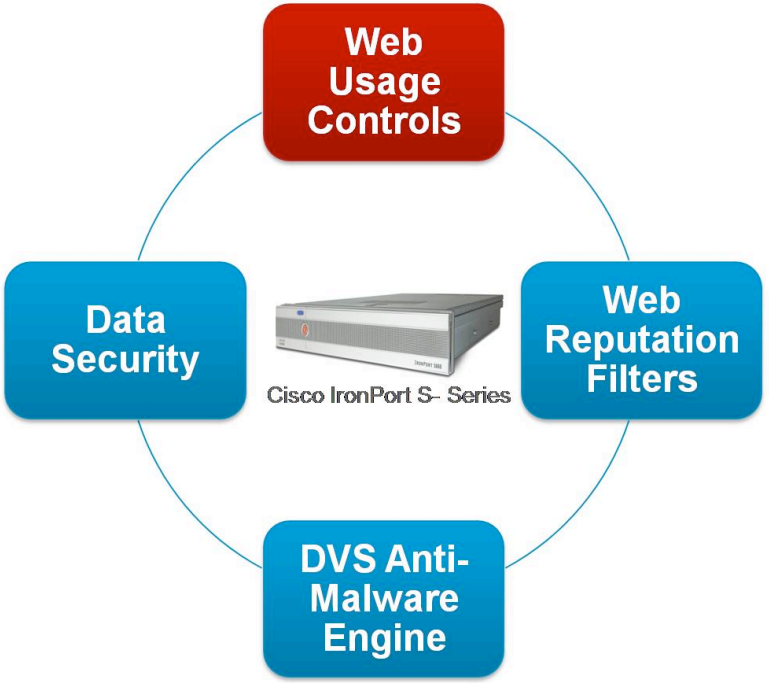
- Легко понимаемые отчеты
- Расширенные отчеты
- Полная система предупреждений

## Эффективность

- 200+ стран
- 50+ языков
- 65 категорий

# Итог

- Прекрасная защита от нарушений правил использовния Web
  - Поддерживается Cisco SIO
  - Динамическая категоризация обнаруживает 90% спорного контента в «темном» Web
  - Всестороння защита от прокси-анонимизаторов
- Богатая система политик и репортинга
- Интеграция в S-серию для полноценного решения SWG solution




Уже сейчас вы можете заказать тестирование!

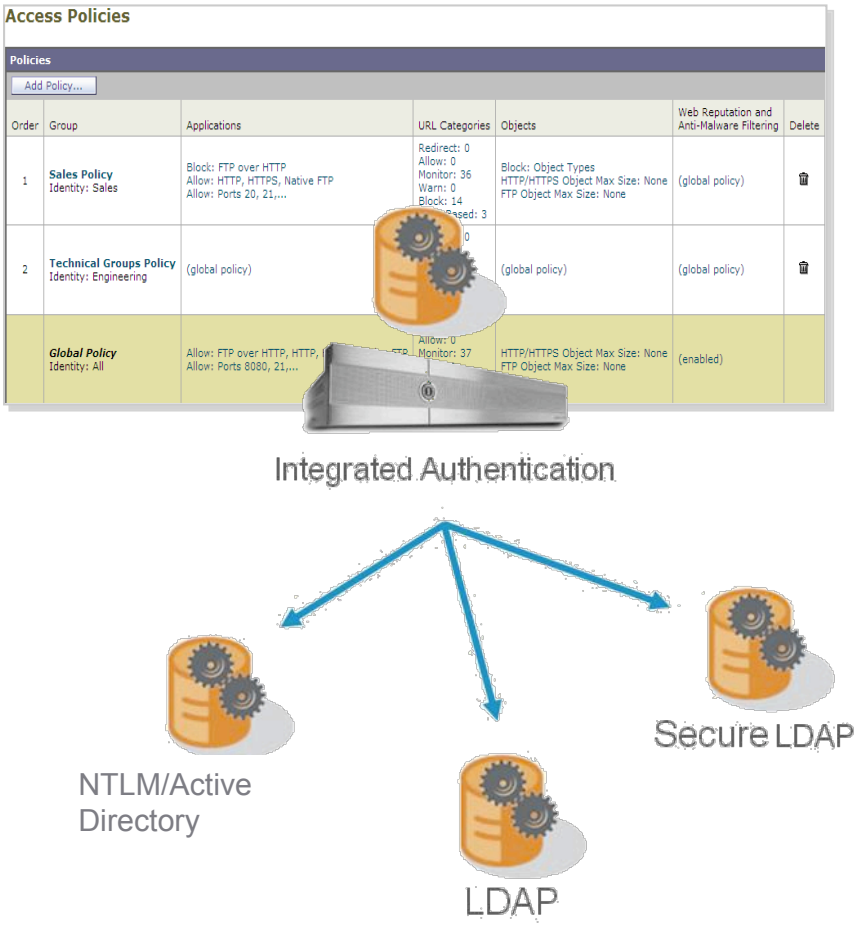
# Контроль Web приложиний

- Управление приложениями HTTP, HTTP(s), FTP
- Избирательная расшифровка SSL трафика
- Политики для приложений, которые туннелируются через HTTP—FTP, IM, видео

# Интегрированная система аутентификации и идентификации

## Политики использования и безопасности данных

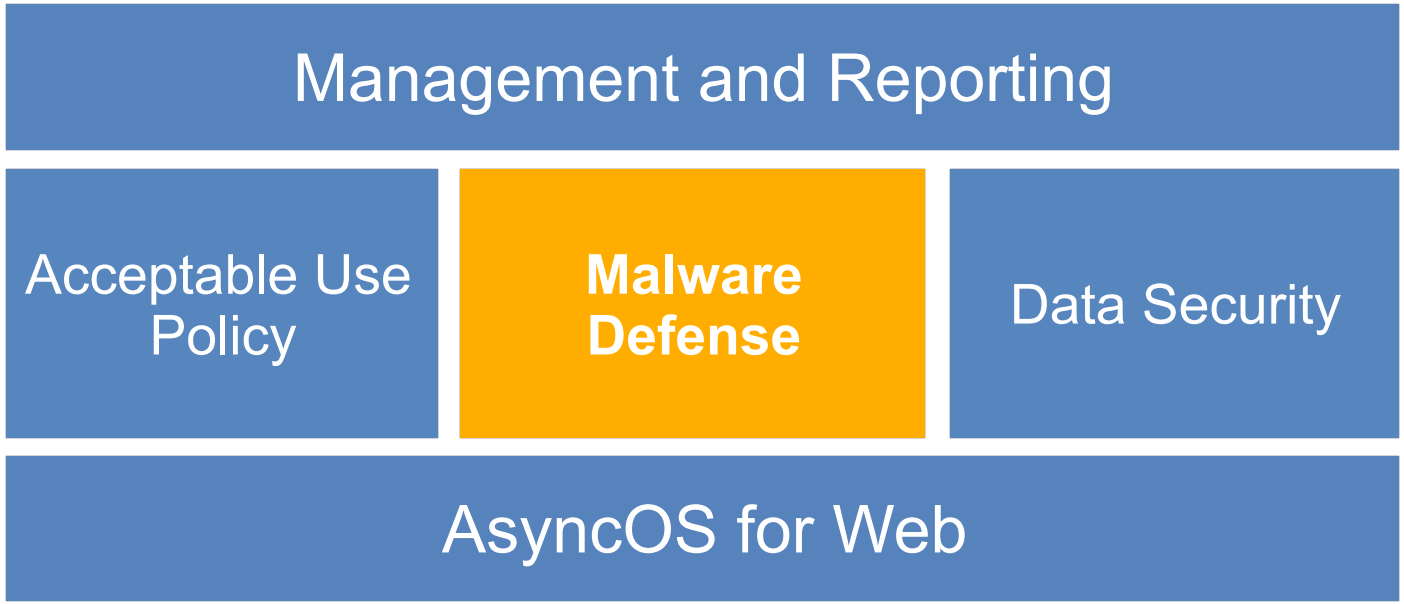
- Аутентификация на серверах LDAP
- Прозрачная аутентификация на серверах AD
- Поддержка нескольких LDAP серверов
- Мультидоменная аутентификация
- Гостевые политики
- Политики повторной аутетнификации




**Определите политики использования и безопасности данных с помощью концепции идентификации**

# Защита от Malware

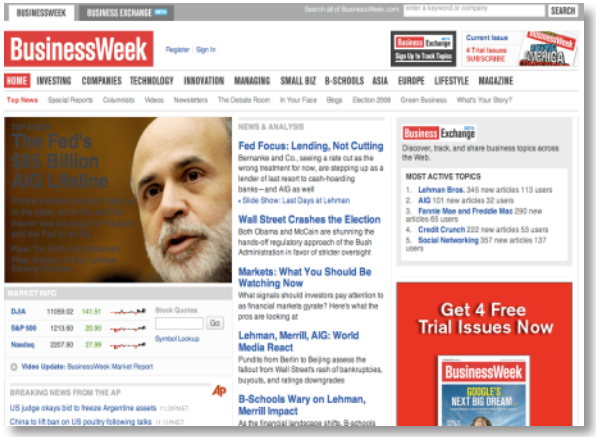
Несколько уровней защиты от malware и spyware




- Ландшафт malware
- Многоуровневая защита от malware
- Защита от трафика phone-home
- Репутационная фильтрация и сигнатурное сканирование

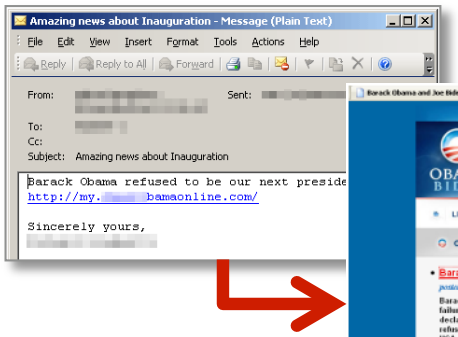
# Malware постоянно усложняется

## Взломанные сайты




- Простое посещение сайта может инфицировать компьютер пользователя
- Ответственны на 87% всех web-угроз*
- **Категория:** Новости

## Социальная инженерия



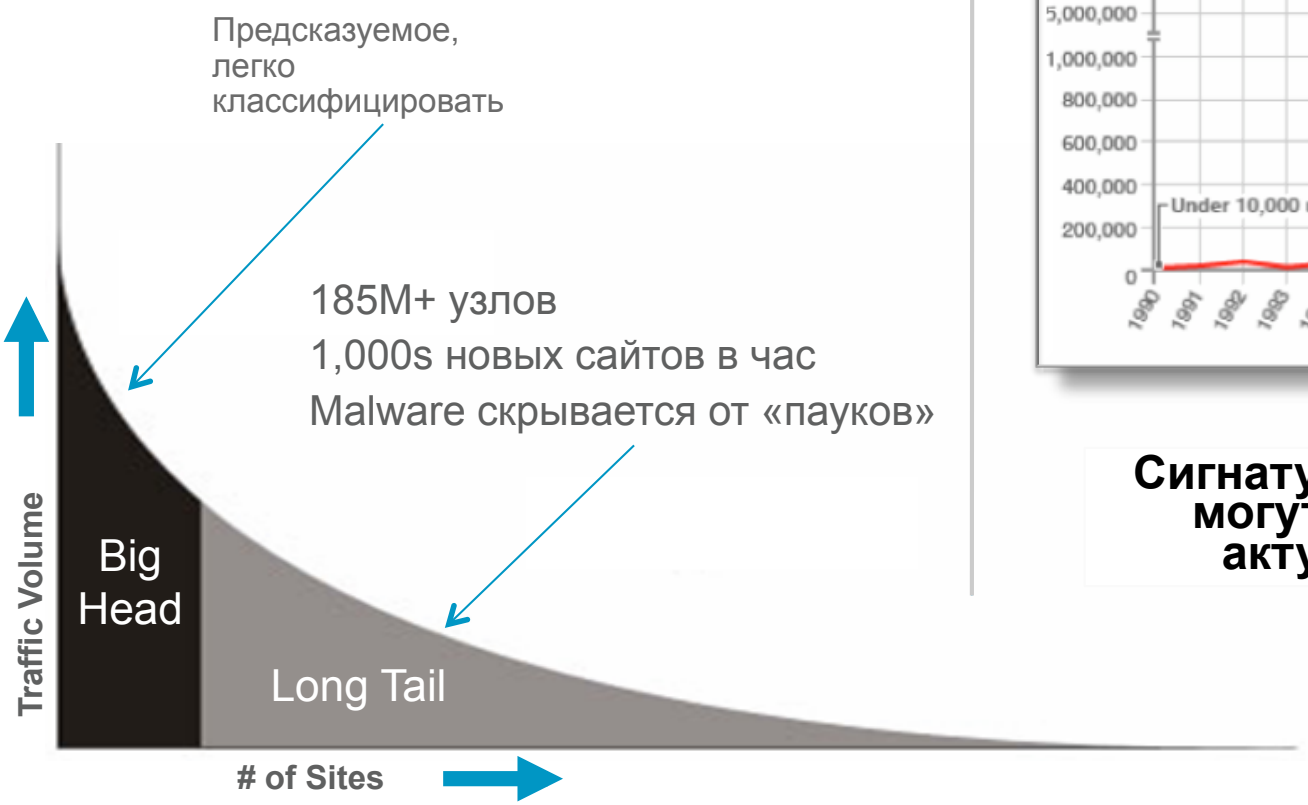

## DNS Poisoning

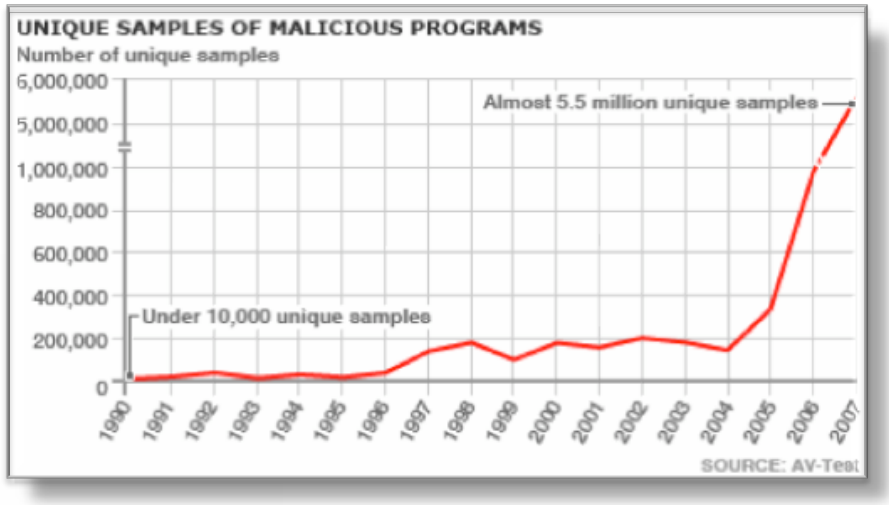

- Актуальный контент, содержащий общественный интерес
- Социальная инженерия заставляет пользователей отключать защиту на десктопе
- **Категория:** Правительство

** Source: Cisco Threat Operations Center*

# Malware избегает традиционные системы защиты


**URL классификация реактивная, слабое покрытие**




**Сигнатуры – реактивные и не могут поддерживаться в актуальном состоянии**

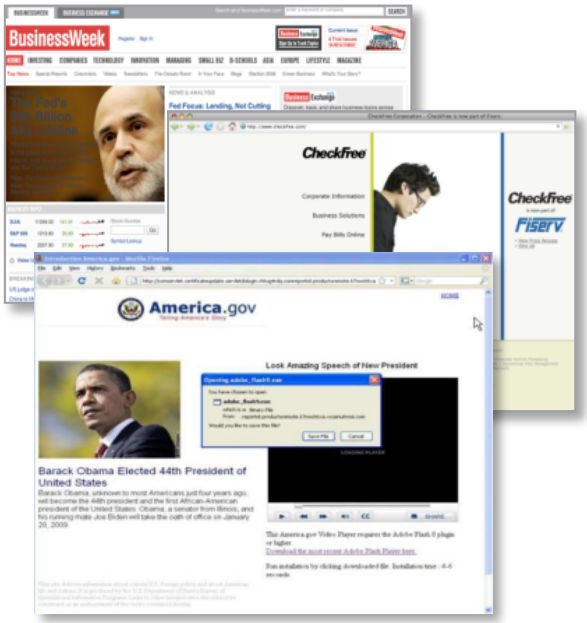
# Многоуровневая защита от Malware

## Защита от современных угроз


Layer 4 Traffic Monitor

Web Reputation Filters

Dynamic Vectoring and Streaming Engine

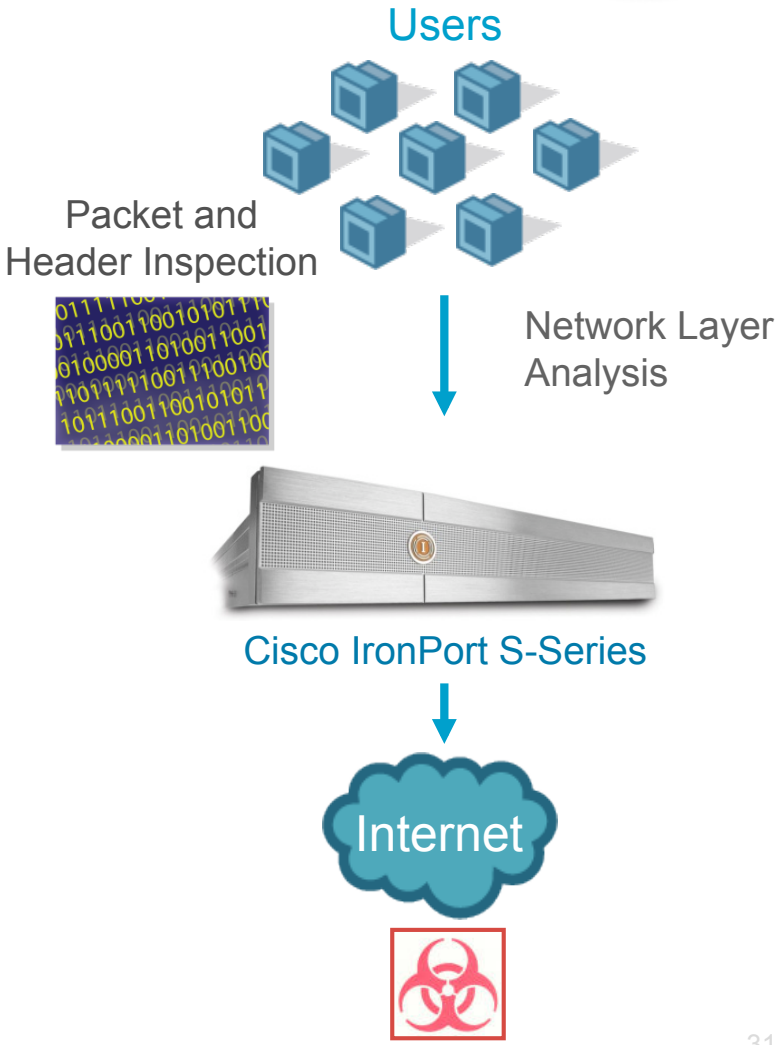



- Обнаруживает трафик ботнетов на всех портах
- Блокирует до 70% известного и неизвестного malware трафика на этапе соединения
- Блокирует malware на основе глубокого контентного анализа

# Обнаружение существующих зараженных клиентов

Предотвращение трафика “Phone-home”


- Cisco IronPort Layer 4 Traffic Monitor
  - Сканирует весь трафик, все порты, все протоколы
  - Обнаружение malware, которое не использует порт 80
  - Блокирует трафик ботнетов
- Мощные данные анти-malware
  - Автоматически обновляемые правила
  - Генерирование правил в реальном времени с помощью механизма “Dynamic Discovery”



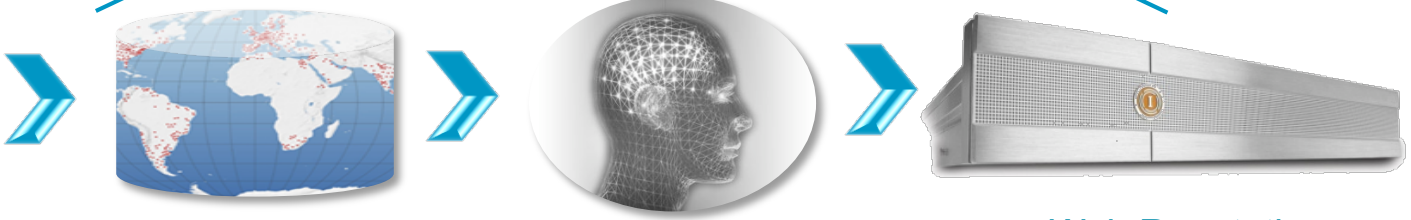
# Фильтры web-репутации

Предсказуемое предотвращение проникновения malware в реальном времени


## 200+ Параметров

- URL Blacklists
- URL Whitelists
- Dynamic IP Addresses
- Bot Networks
- URL Behavior
- Global Volume Data
- Domain Registrar Information
- Compromised Host List
- Real-Time Cloud Analysis
- Network Owners
- Known Threat URLs

## Cisco Security Intelligence Operations



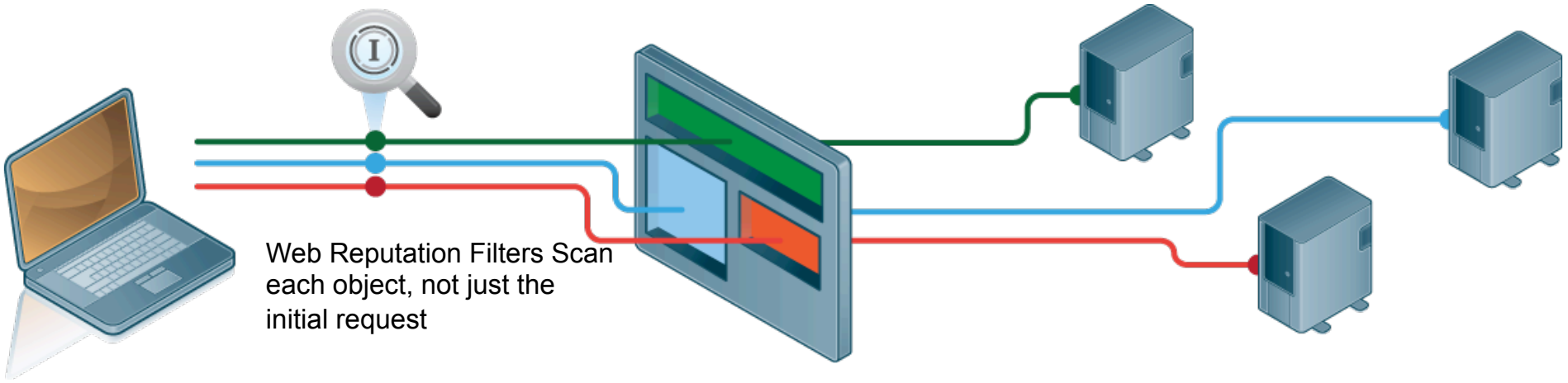
SensorBase Network

Security Modeling

Web Reputation Scores (WBRS) -10 to +10

# Безопасность в современном мире Web 2.0

## Что стоит за попыткой атаки




- Веб-страницы создаются из объектов, которые находятся на разных источниках
- Объекты – это изображения, html-код, JavaScript…

- Скомпрометированные узлы берут вредоносное содержимое из внешних источников
- Безопасность – это просмотр каждоно объекта в отдельности, а не только первоначального запроса.

# Взломанные сайты; *Невидимая угроза*


## Massive Attack: Half A Million Microsoft-Powered Sites Hit With SQL Injection

By Scott Gilbertson ✉ April 28, 2008 | 8:04:40 AM Categories: Security

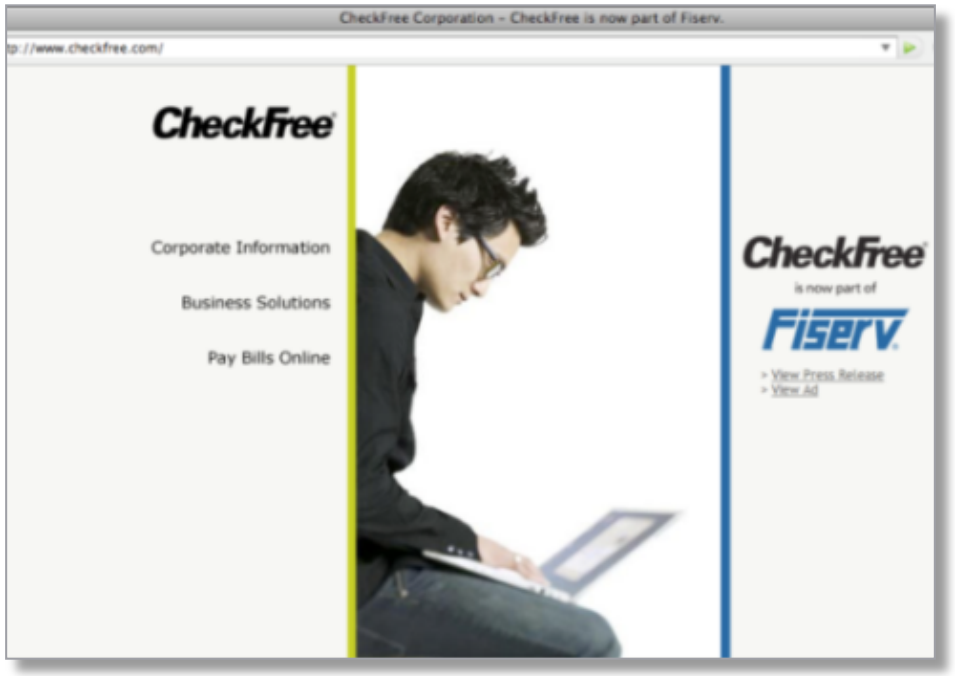
# На самом деле невидимая угроза*очень* видимая…

- **Взломанные сайты** ответственны более чем за 87% всех web-угроз*
- Более **79%** web-узлов с вредоносным кодом легитимные**
- **9 из 10** web узлов уязвимы к атакам**
- **Кросс-сайт скриптинг** (XSS) и **SQL Injections** находятся на первом месте среди всех методов внедрения кода
  - Cross-Site Scripting (7 из 10 сайтов)**
  - SQL Injection (1 из 5 сайтов)**


*Source: IronPort TOC
**Source: White Hat Security, Website Sec Statistics Report 10/2007 & PPT 8/2008

# Репутационные фильтры в действии

## Остановить приближающиеся угрозы




- DNS poisoning перенаправляет пользователей на веб-сайт, находящийся в Украине
- Фильтры web-репутации защищают пользователей за **12 дней до атаки**

### Фильтры web-репутации Cisco IronPort

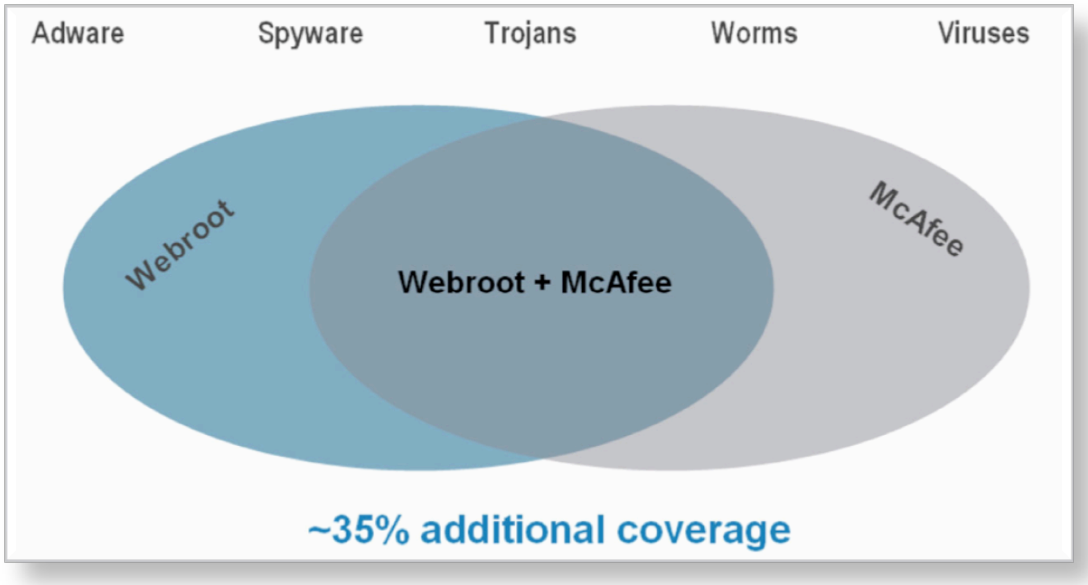
**Преимущество**

- Предсказывают риск угрозы на основе поведения URI
- Функция Exploit Filtering защищает от скомпрометированных web-узлов
- Проверяет каждый запрос и защищает от атак iFrame

# Механизм IronPort DVS

## Dynamic Vectoring and Streaming

- Ускоренное сигнатурное сканирование
  - Параллельное сканирование
  - Потоковое сканирование
- Несколько механизмов вынесения вердикта
  - McAfee и Webroot
- Автоматические обновления
- Расшифровывает и сканирует трафик SSL
  - Избирательно, на основе категории и репутации



# Webroot vs McAfee

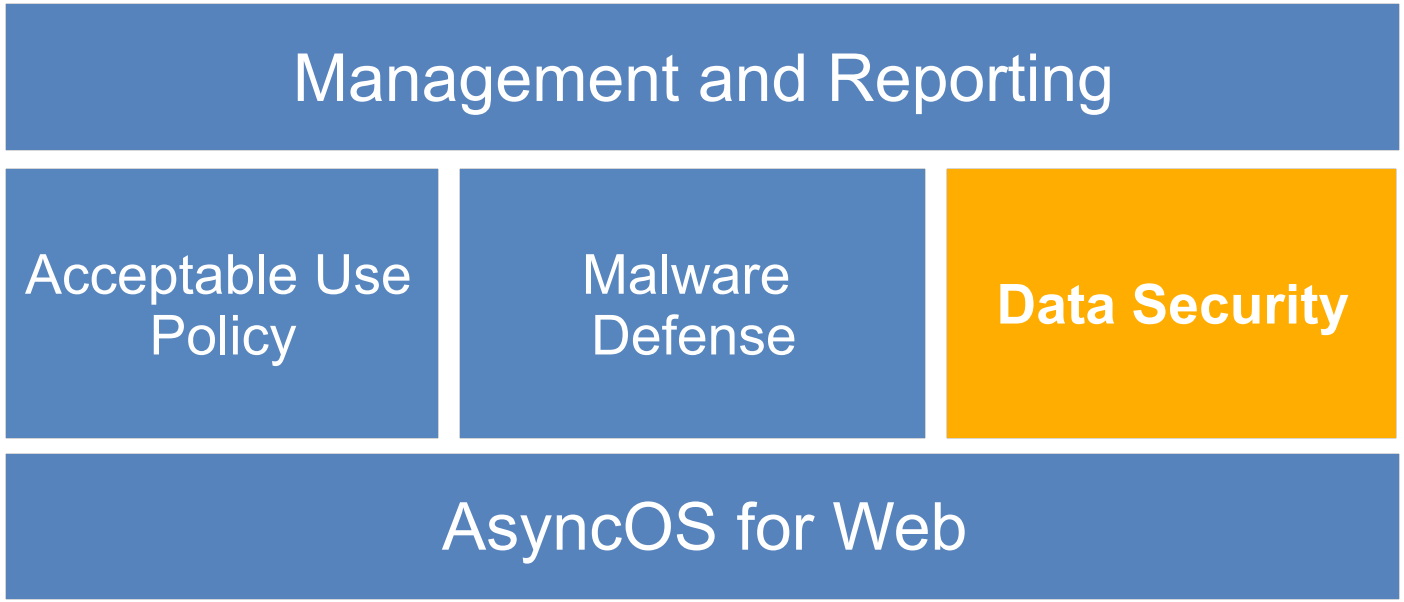
*Обзор функционала*

- Мощная система обнаружения
  - Более 150,000 сигнатур
  - Обнаружение подозрительного Spyware
- Широкий диапазон обнаружения:
  - Фишинг и Malware URL и домены
  - Двоичный код Malware, короткие контрольные суммы
  - Malware User Agents
- Механизм распаковывает и проверяет malware в архивах
  - ZIP , RAR, CAB, TAR
- Правила анти-malware может инициировать:
  - Прервать загрузку
  - Не проверяет исходящие POST данные на malware

1. Работа McAfee Avert Labs, одним из самых известных исследовательских центров
2. Сигнатуры закрывают **malware и вирусы**
3. Находится на первых местах в рейтинге и рекомендуется независимыми исследователями
4. Сигнатурное и эвристическое сканирование

# Полная безопасность данных

Простота и выбор




- Безопасность данных. Цели и реальность.
- Простые механизмы on-box
- Расширенные механизмы off-box

# Цели системы безопасности данных

**SAIC warns of possible data breach**

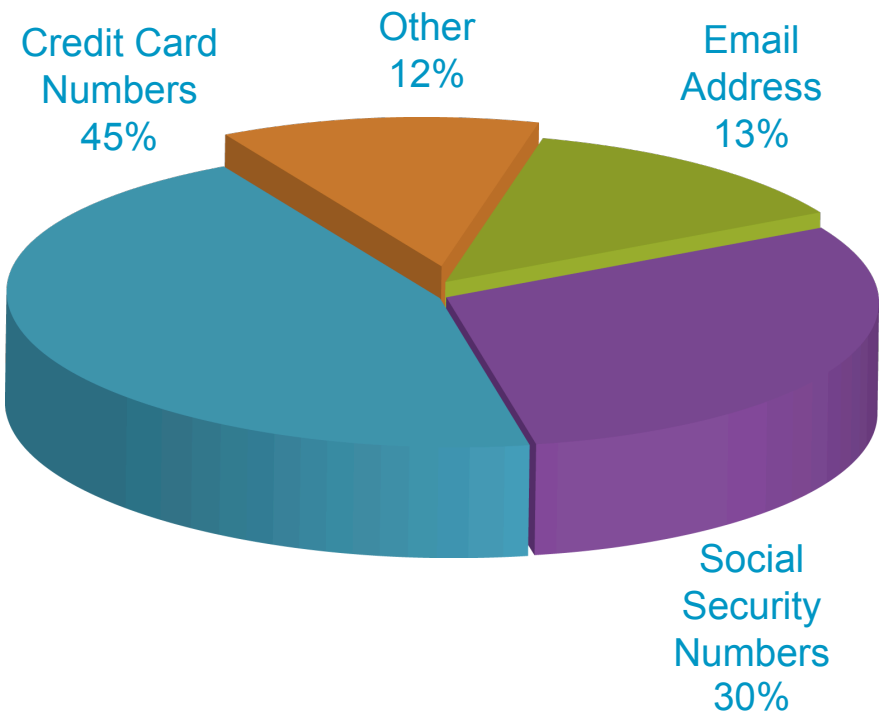
Associated Press

**By Donna Borak, AP Business Writer | July 20, 2007**

WASHINGTON --Pentagon contractor SAIC Inc. may have compromised personal information about more than half a million military personnel and their relatives because it did not encrypt data transmitted online.

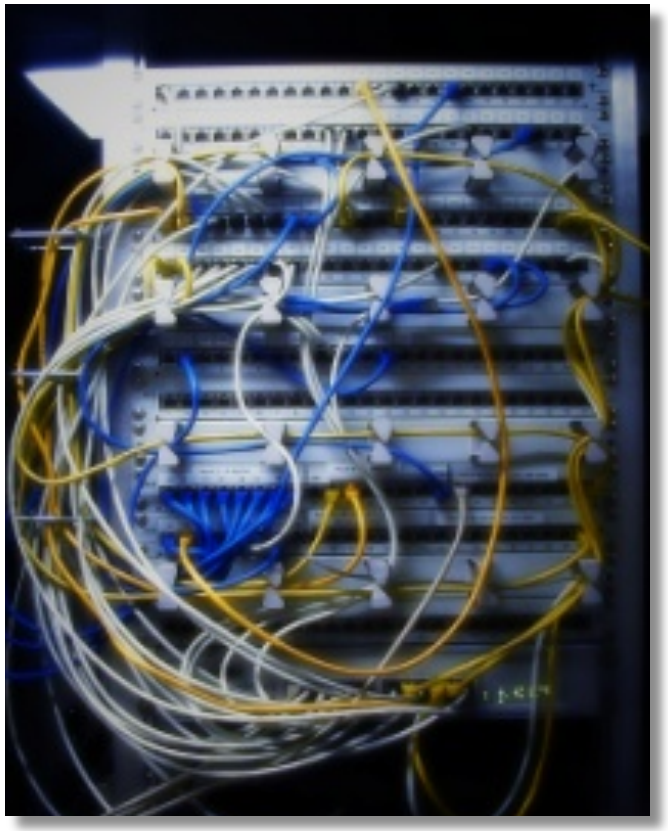
| Company | Data Loss Event | Estimated Cost |
|---|---|---|
| **Best Western Hotel Group** | 8M customer records from online booking system | $400M-1.5B |
| **Hannaford** | 4M credit and debit card numbers | $160-788M |
| **Monster.com** | 1.6M personal records | $80-315M |

## Потерянные записи



# Реальность…

**Сложное законодательство**



**Сложная реализация**

# Безопасность данных
## Общие механизмы

- Общая проверка метаданных с точки зрения видимости и соответствия правилам
- Allow , block, log

  на основе метаданных, URL категориям, пользователю и репутации
- Мультипротокольное

  HTTP(s), FTP, HTTP туннель

# Политики «здравого смысла»

## Простой подход к безопасности данных

| | | | |
|---|---|---|---|
| **Who?** | John Smith, Finance | John Smith, Finance | Jane Doe, Sales |
| **What?** | FiscalPlan.xls | FiscalPlan.xls | CustomerList.doc |
| **Where?** | Webmail.com | Taxfirm.com | Personal-site.com, -9 Reputation score |
| **How?** | HTTPS (Encrypted) | HTTPS (Encrypted) | FTP |
| **Verdict** |  |  |  |

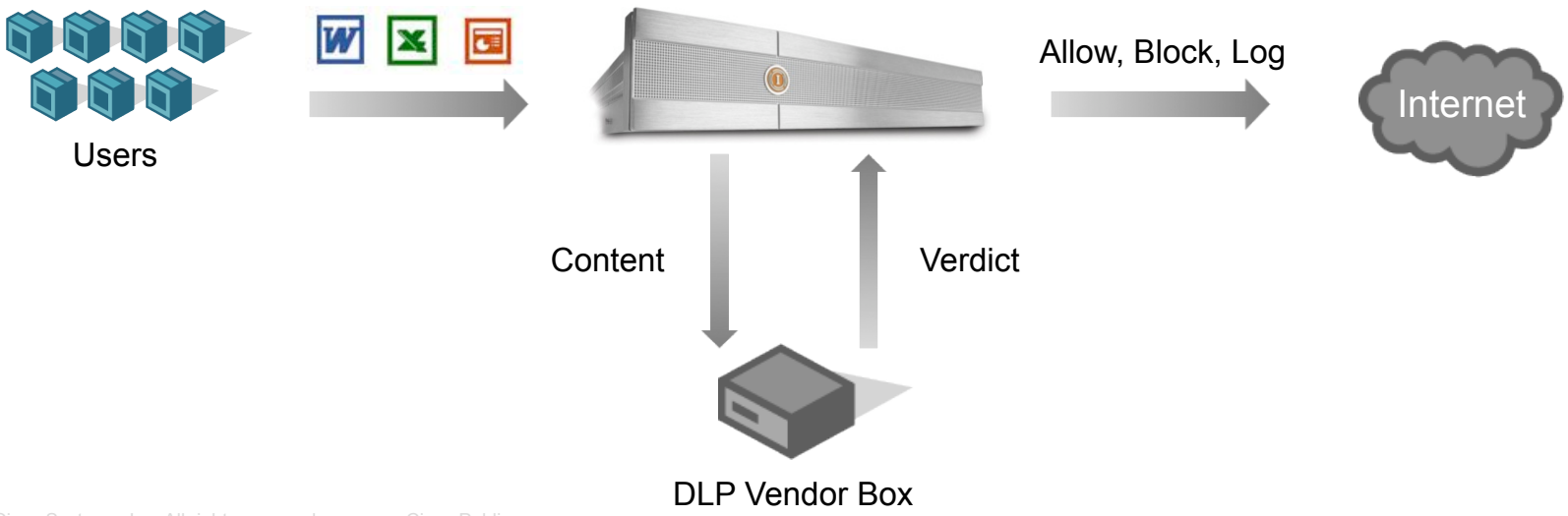
# Безопасность данных

## Расширенная безопасность off-box

- Прозрачная интеграция
- Глубокая проверка контента

  Структурированное и неструктурированное соответствие
- Оптимизация производительности

  Работает в тандеме со встроенной системой безопасности данных



# Бреши в данных, инициированные malware

## Критический элемент безопасности данных

**Gozi Trojan**

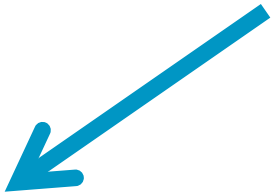
- Устанавливается через присоединенный файл PDF
- Зашифровывает сам себя
- Крадет данные из потоков SSL

**Trojan.PWS.ChromeInject.B**

- Firefox plug-in
- Собирает учетные записи e-banking

**Sinowal Trojan**

- Скомпрометировано более 500,000 банковские учетных записей
- Связан с RBN



**Layer 4 Traffic Monitor**

**Web Reputation Filters**

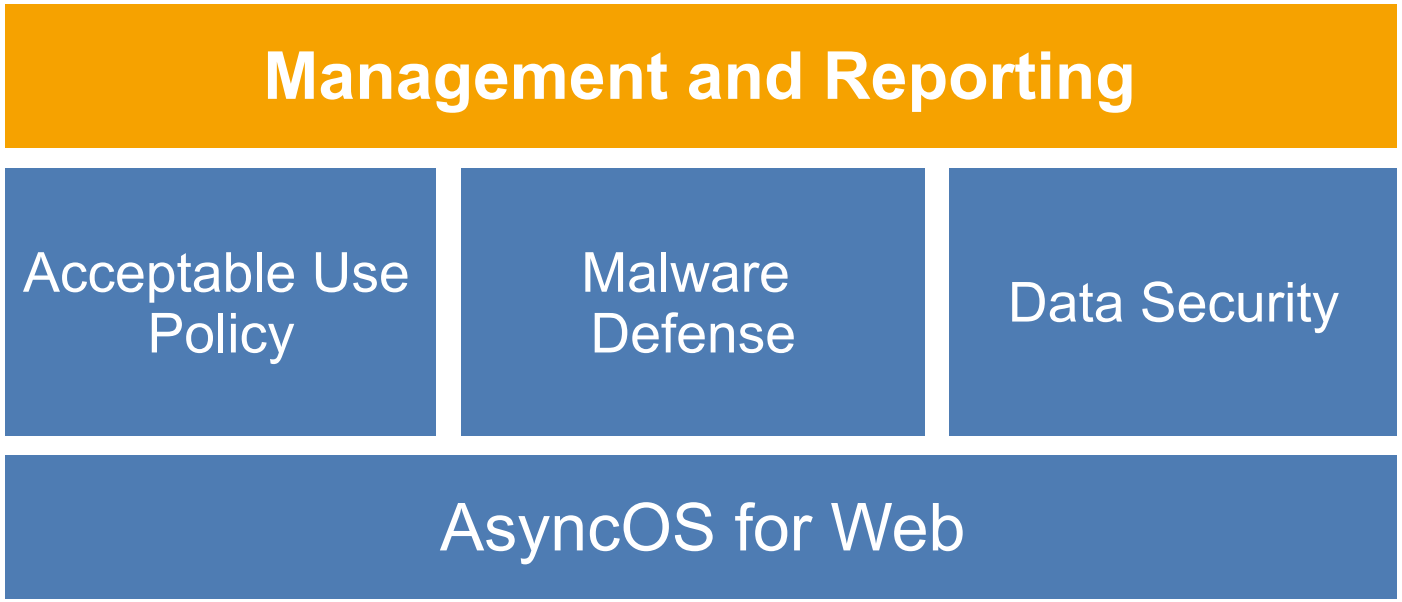
**Dynamic Vectoring and Streaming Engine**

**Блокирует возможность потери данных от действий phone-home**

**Предотвращает попадание malware в сеть**

# Управление и построение отчетов

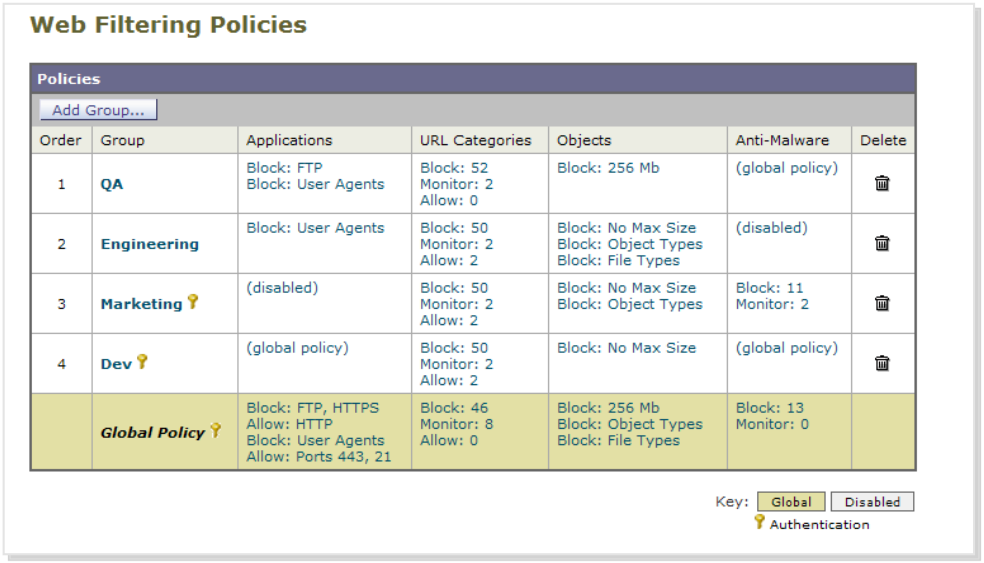
## Управление и видимость web-трафика




- Управление
- Ролевое администрирование и делегирование ролей
- Детальные отчеты по URL и по пользователям
- Отслеживание пользователей

# Cisco IronPort Web Security Manager

## Простой просмотр политик для всей организации




Marketing

- Block FTP uploads
- Allow media files
- Route requests to partner site

Sales

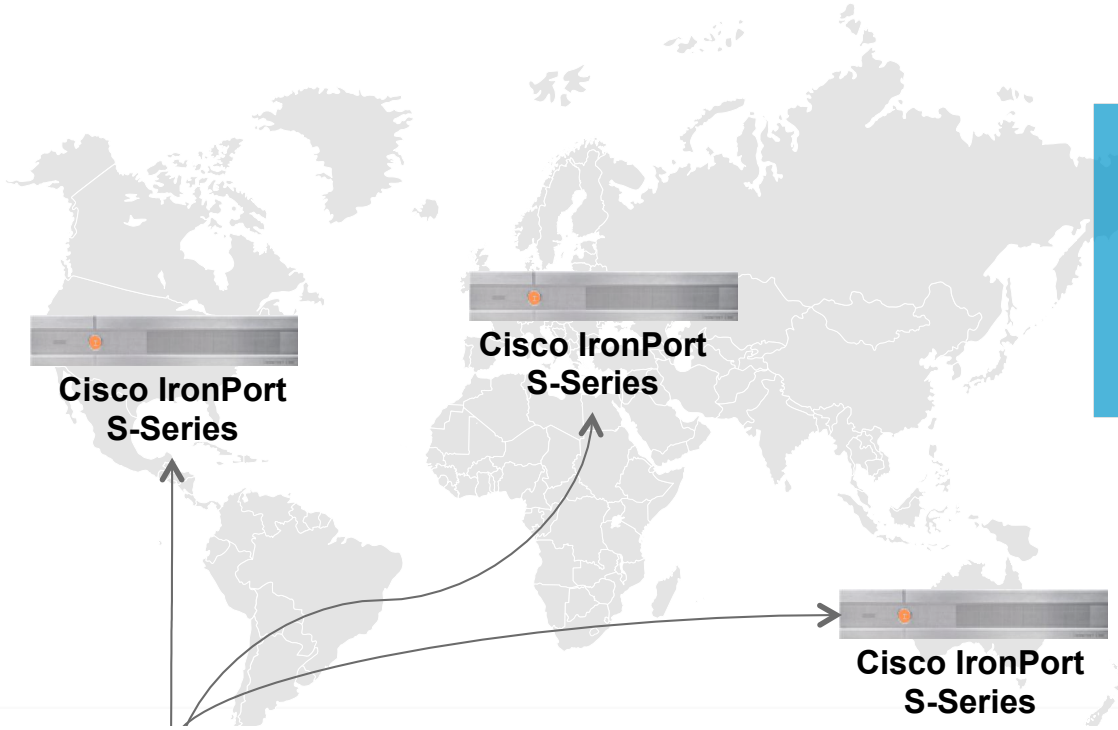
- Block executables
- Block sports sites 9am-5pm M-F
- Decrypt HTTPS connections

IT

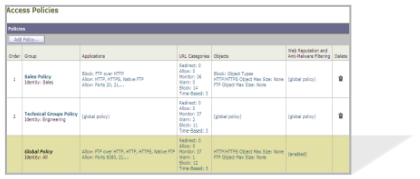
- Allow all URL categories
- Exempt Adobe updates from authentication
- Block all malware

## Настройка точных политик на основе набора параметров

# Глобальное управление политиками и конфигурациями




**Централизованное управление и контроль политик доступа к web**

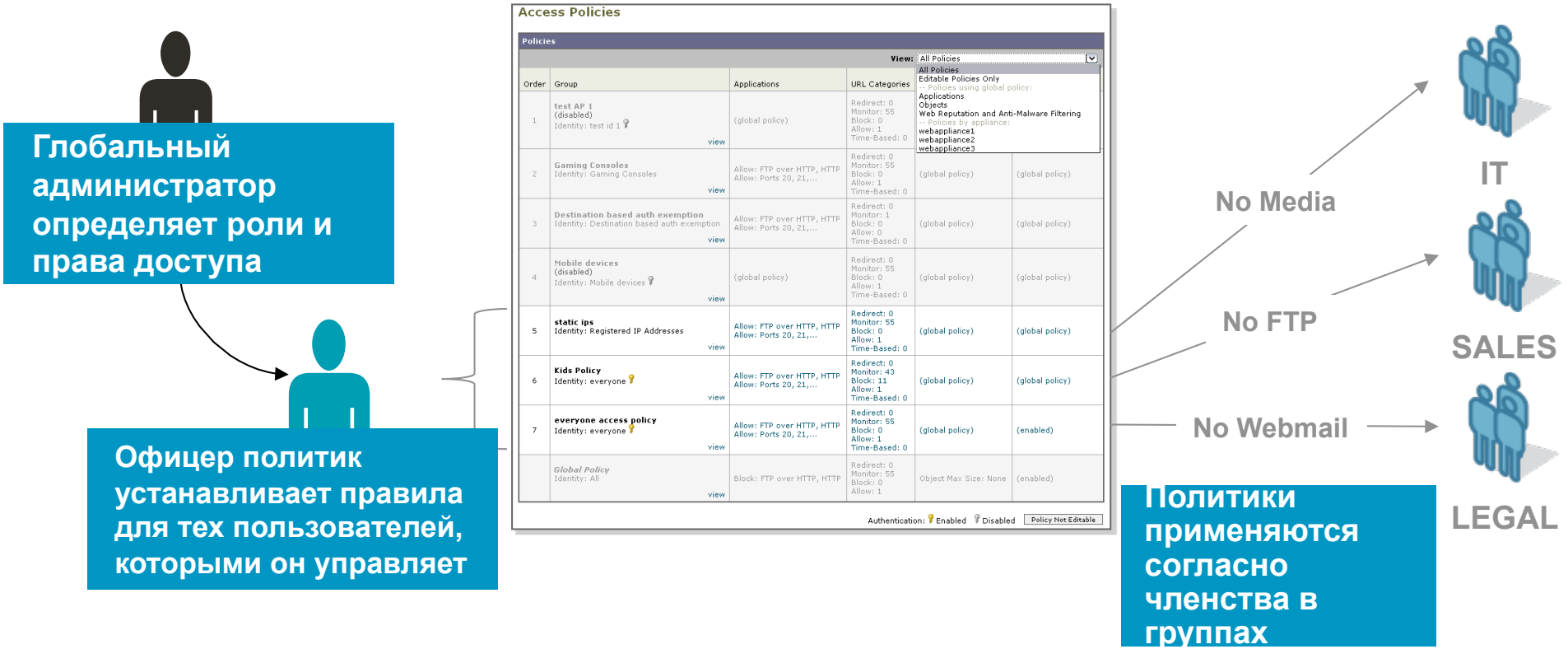


Cisco IronPort
M-Series

- Одновременный ввод в действие политик для сотен устройств Cisco IronPort S-Series
- Гибкость в использовании локальных политик через делегирование
- Поддержка нескольких версий AsyncOS
- Аудит и резервирование политик для контроля

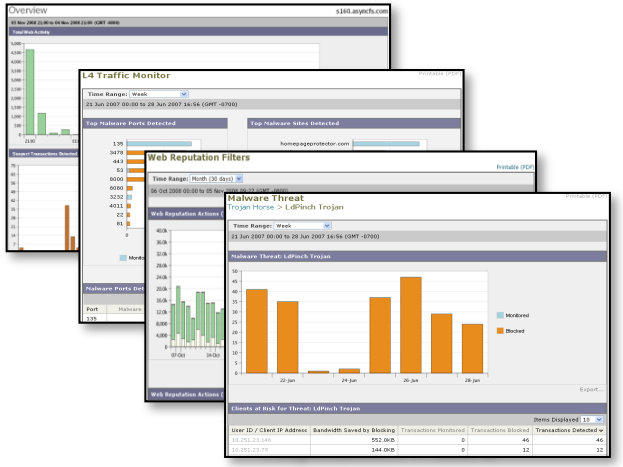
# Делегированное администрирование

## Гибкая поддержка организационных требований

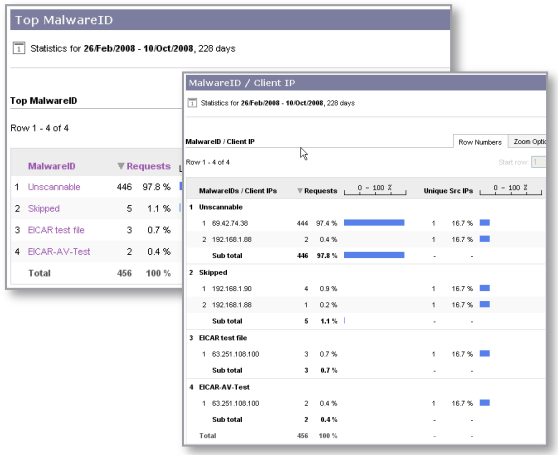



- Назначаются администраторы для групп пользователей, подсетей, устройств, адресов назначения
- Гранулированное ролевое разделение доступа

# Комлексная система построения отчетов



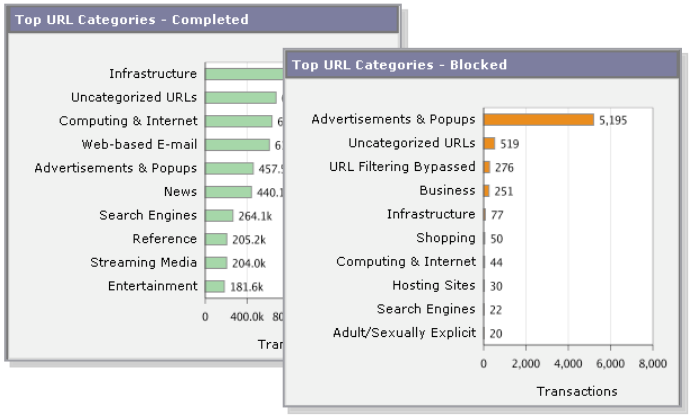

- Тщательный просмотр угроз
  - Обзор Web трафика
  - Layer 4 Traffic Monitor
  - Категория и детали угроз anti-malware
  - Риск клиента
  - Детализация активности клиента
  - Фильтры Web-репутации
  - Активность сайта и детали



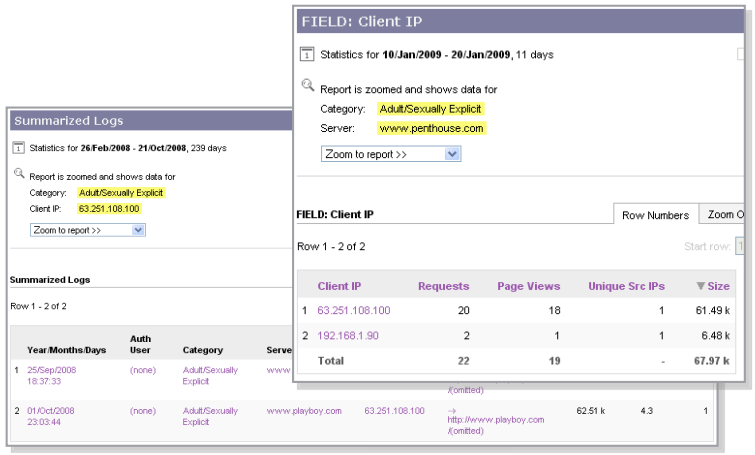

- Детальный внешний анализ
  - Разгрузка устройства от обработки большого количества данных
  - Отчеты класса Top N
  - Client, источник, название Malware и категория

SAWMILL for IronPort

# Критические отчеты – правила использования




- Отчеты в реальном времени
  - Просмотр использования web и тенденций
  - Мониторинг тенденций правил использования
  - Идентифицировать поведение рисков



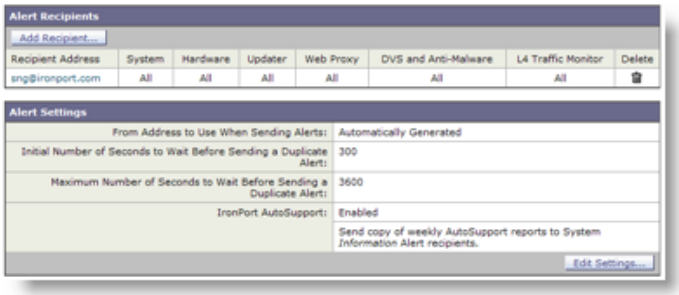

- Расширенные возможности
  - Расследование нарушений правил использования
  - Углубленный анализ
  - Соответствование требованиям законодательства

SAWMILL for IronPort

# Мониторинг системы

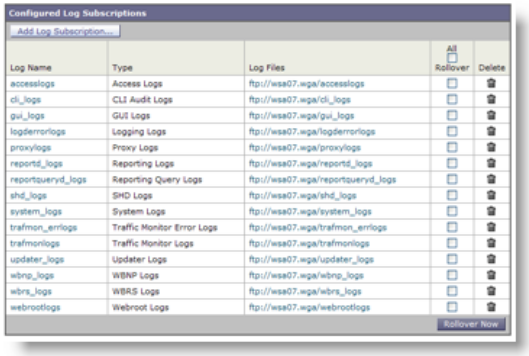
## Простая интеграция с существующими процессами

### Центр предупреждений



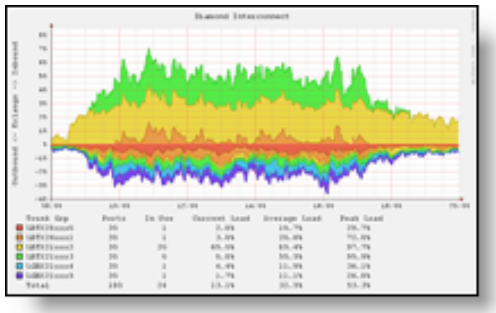

- Подпись на предупреждения для администраторов
- Разные регионы управления

### Журналы регистрации




- Squid, Apache, W3C,
- Доставка через SCP, syslog, FTP

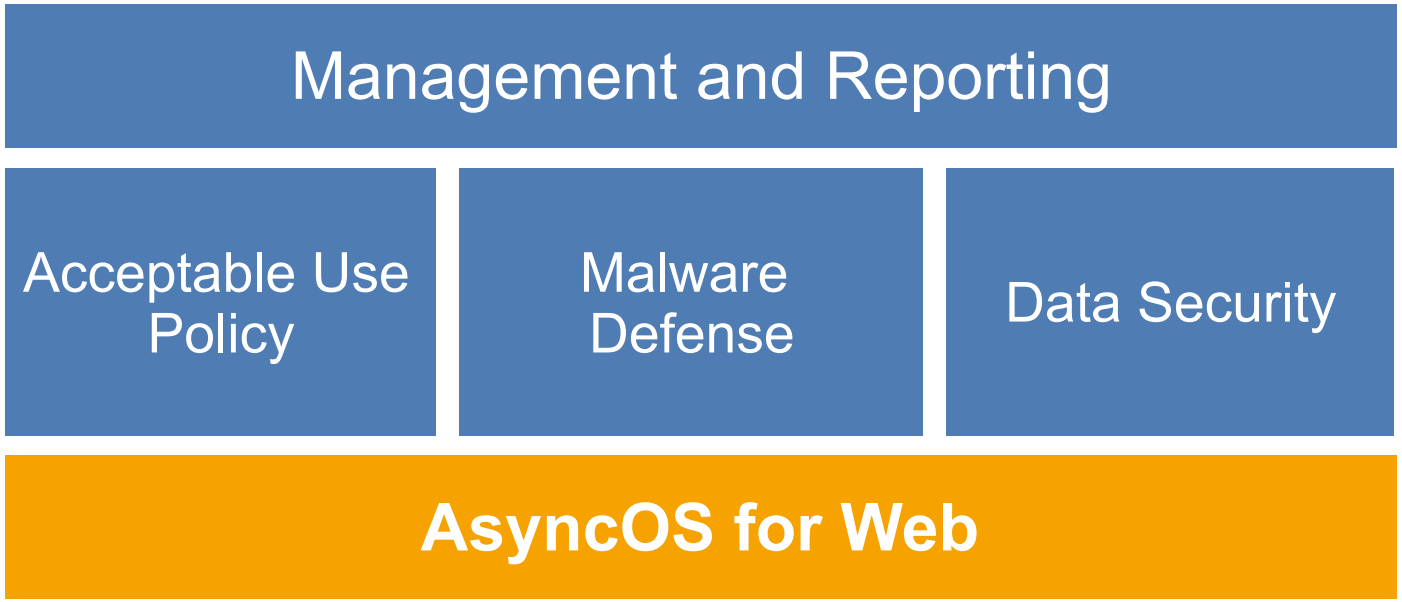
### SNMP



- IronPort MIB
- Интеграция с SNMP инструментарием
- SNMP v1, v2, v3

# Платформа AsyncOS для Web

Создана для производительности




- Высокопроизводительный прокси + кеш
- Многоядерное сканирование
- Разные форм-факторы
- Гибкие возможности по вводу в эксплуатацию

# Высокопроизводительный прокси + кеш

## Управление соединениями и файловой системой

Соединения со стороны клиента

**Cisco IronPort S-Series**

Соединения со стороны сервера

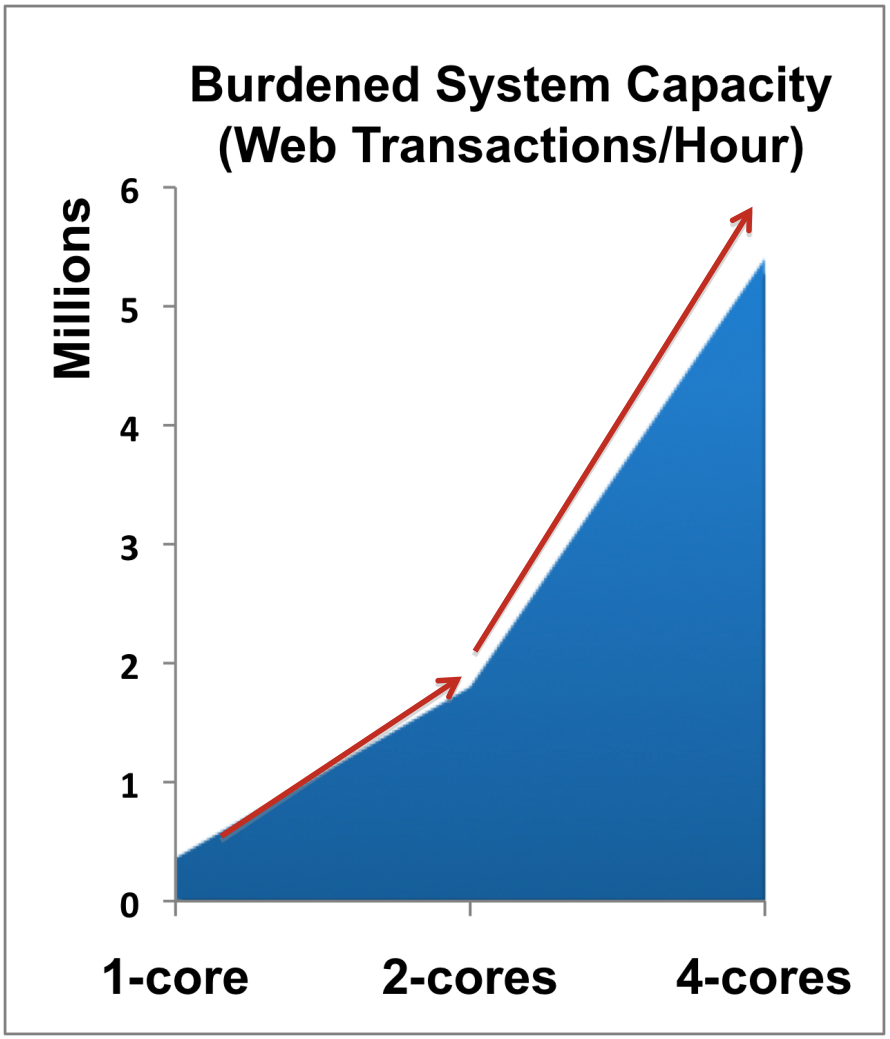
Управление пулом постоянных TCP соединений (со стороны клиента и сервера) → Поддержка очень высоких объемов трафика

Сохраняет циклы ЦПУ и памяти с помощью механизма уведомления о системных событиях → Существенное снижение утилизации ресурсов

Объединенная система хранилища объектов и высокопроизводительного кеширования → Снижение времени отклика

# Высокопроизводительное сигнатурное сканирование

## Многоядерная оптимизация

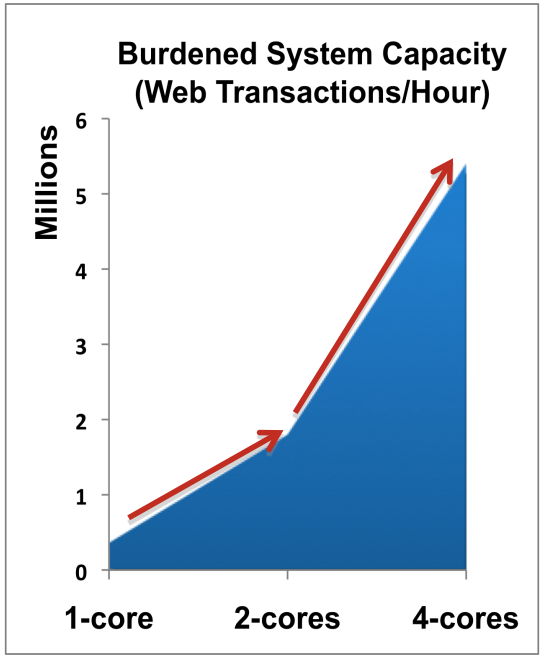



- Решает проблемы с задержкой во время сигнатурного сканирования
- Используется функция мульти-сканирования для эффективной безопасности
- Оптимизировано для «тяжелого» контента

**Best User Experience.**
**No-Compromise Security.**

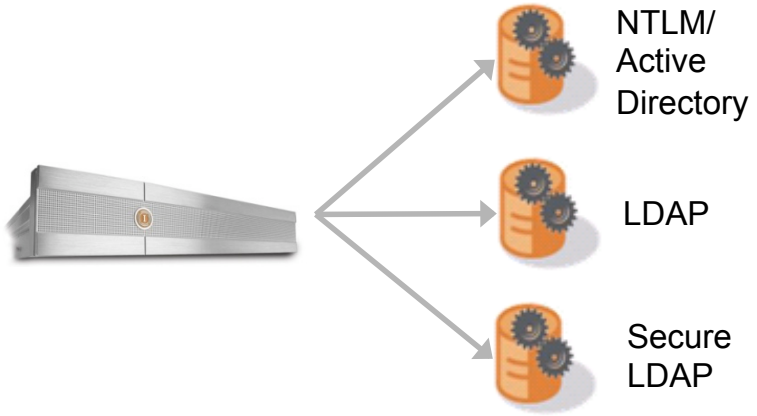
# Высокопроизводительная платформа прокси

## Многоядерная оптимизация




- Решает проблемы с задержкой во время сигнатурного сканирования
- Используется функция мульти-сканирования для эффективной безопасности
- Оптимизировано для «тяжелого» контента

## Интегрированная аутентификация и идентификация




- Identity Based Policies
- Transparent, single sign-on (SSO) authentication against Active Directory
- Guest Policies, Re-Auth

# Внедрение

# Выберите правильную платформу

## Remote Office and Back Office (ROBO) to Enterprise

Capacity and Throughput

- Несколько опций интеграции (прозрачное перенаправление L4, PAC файл, WPAD, WCCP)
- Встроенные функции отказоустойчивости – RAID 10, сдвоенные блоки питания
- Высокая доступность – WCCP, DNS, L4
- Гибкая система маршрутизации

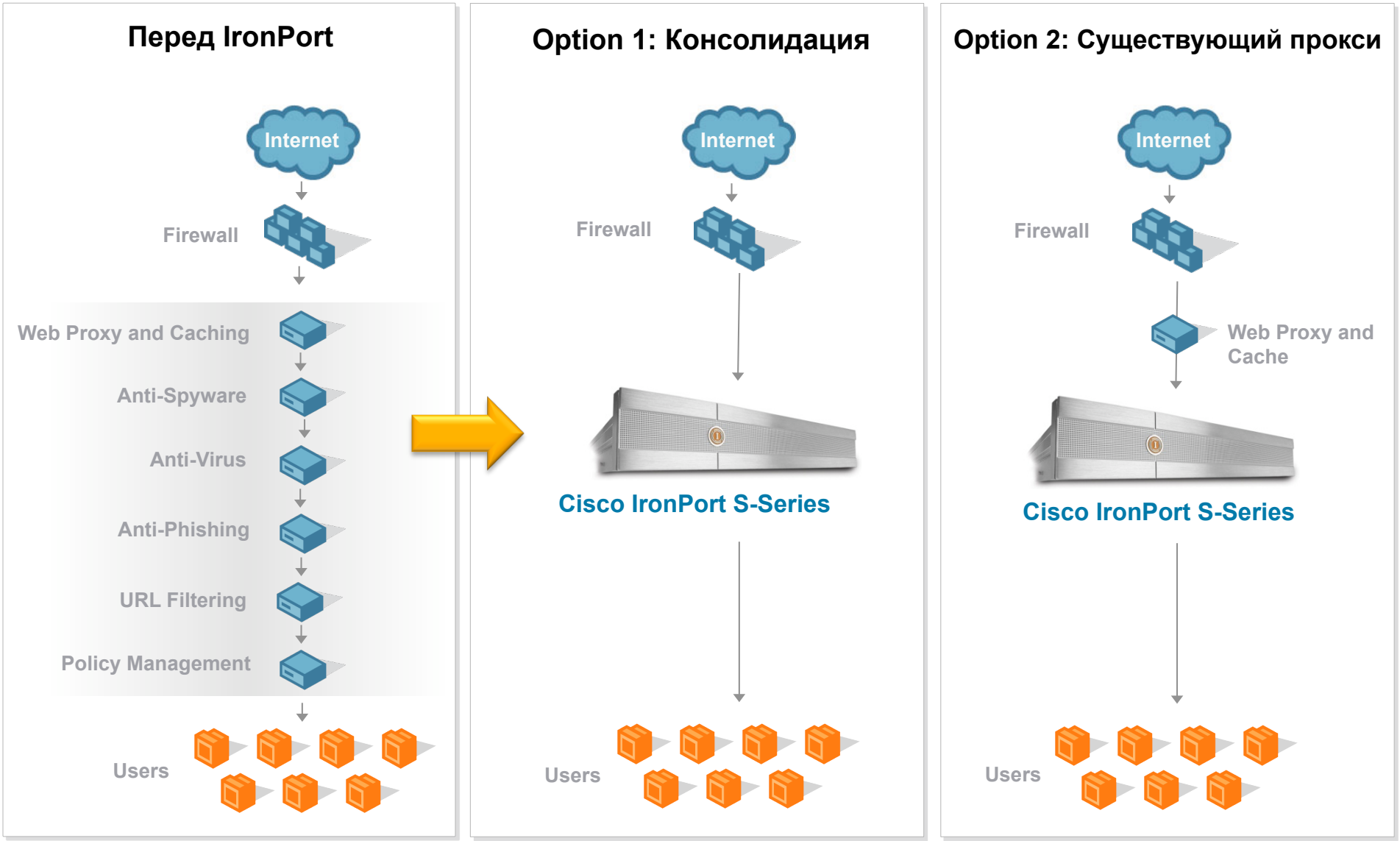
| Cisco IronPort S160 | Cisco IronPort S360 | Cisco IronPort S660 |
|---|---|---|
| 1-1,000 users | 1,000-10,000 users | 10,000-30,000 users |

ROBO | Regional HQ / Mid-Market | Corporate HQ

**Market Segment**

# Шлюз безопасности Web следующего поколения

## Несколько опций внедрения



# Режимы работы прокси

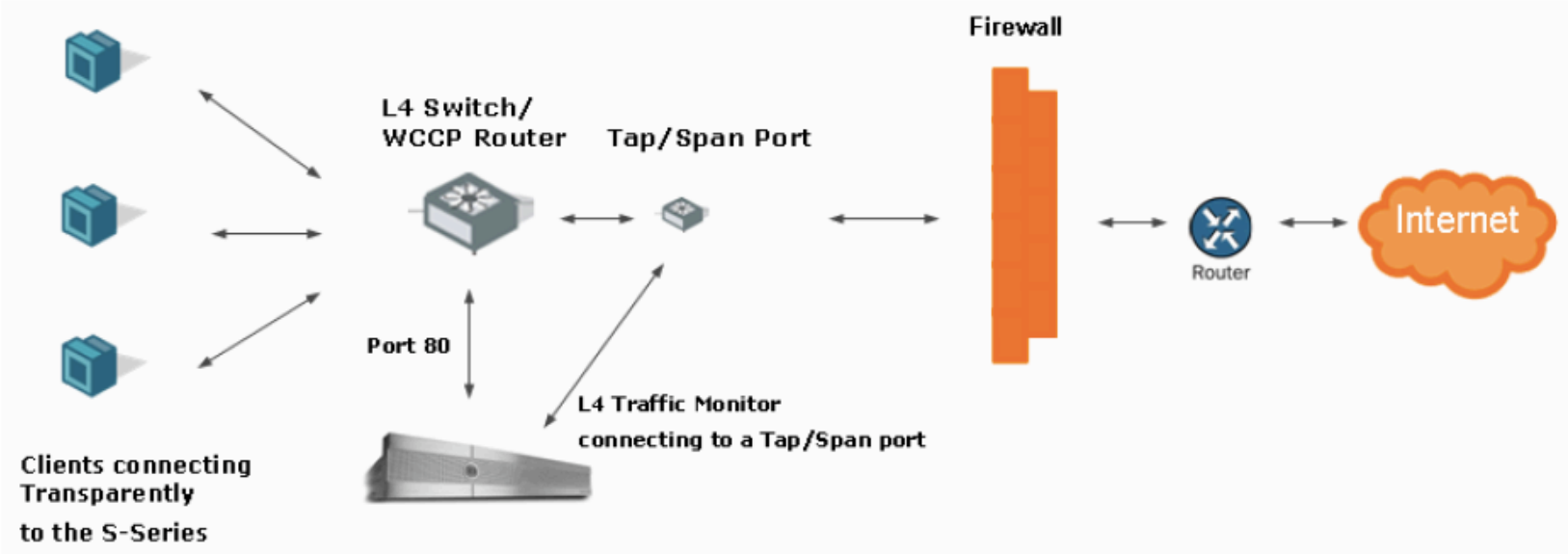
- Явно заданный прокси

  PAC файлы, WPAD

- Прозрачный режим

WCCP, PBR, IP спуфинг, заголовки

- Режим нескольких upstream прокси



# PAC – Proxy Auto-Config Files

- Внедрение прокси сервера на большом количестве клиентов
  - Избегайте настроек на desktop
  - Отказоустойчивость и балансировка нагрузки
  - Производительность
- PAC хостинг
  - Локально на десктопе, на сервере, или на S-серии
- Web Proxy Autodiscovery Protocol (WPAD)
  - В средах DHCP используйте опцию 252 “auto-proxy-config”
  - Безопасность!!!!

# Создание PAC файла

```
function FindProxyForURL(url, host) {
// If IP address is internal or hostname resolves to internal IP, send direct.
  var resolved_ip = dnsResolve(host);
  if (isInNet(resolved_ip, "10.0.0.0", "255.0.0.0") ||
    isInNet(resolved_ip, "172.16.0.0",  "255.240.0.0") ||
    isInNet(resolved_ip, "192.168.0.0", "255.255.0.0") ||
    isInNet(resolved_ip, "127.0.0.0", "255.255.255.0"))
    return "DIRECT";
  // Use a different proxy for each protocol.
      if (shExpMatch(url, "http:*"))  return "PROXY proxy1.domain.com:3128";
      if (shExpMatch(url, "https:*")) return "PROXY proxy2.domain.com:3128";
      if (shExpMatch(url, "ftp:*")) return "PROXY proxy3.domain.com:3128";
 // If I`m not in corporate network, send direct
      if (!isInNet(myIpAddress(),"144.254.0.0","255.255.0.0"))
      { return "DIRECT"; }
 // URL based load balancing
      function FindProxyForURL(url,host){switch(URLHash(url)%2){
      case 1:  return "PROXY proxy1.domain.com:3128";
      default: return "PROXY proxy2.domain.com:3128";}}
      function URLHash(url) {server_name=url.split("/")[2]
      if(!server_name) {return url.length;}return server_name.length;}
  // All other traffic uses below proxies, in fail-over order.
      return "PROXY 1.2.3.4:8080; PROXY 4.5.6.7:8080; DIRECT";
}
```

# Внедрение прозрачного прокс

- Настройте прозрачное перенаправление
  - PBR – L4 коммутатор, простая настройка
  - WCCP – WCCPv2 маршрутизатор, более сложно, но более гибко
- Метод возвращения
  - Layer 2 или GRE
- Настройте IP спуфинг или заголовки X-Forwarded-For
  - Когда вышестоящий прокси требует идентификации клиента
  - Заголовки Via
- Настройте список необрабатываемых узлов
  - Для того, чтобы исключить список узлов, которые не поддерживают прокси

# WCCP и устройства Cisco

- WCCP на ASA

  Поддерживается только редирект GRE, нет поддержки отказоустойчивости WCCP table

  WCCP редирект только на входящем интерфейса, WSA и клиенты должны быть в одной сети

- WCCP и коммутаторы Catalys 3560/3750

  Вы не можете сконфигурировать WCCP и PBR, WCCP и VRF, WCCP и PVLAN на одном интерфейса

  Internet, WSA и клиенты должны быть вразных подсетях

- WCCP и маршрутизаторы IOS

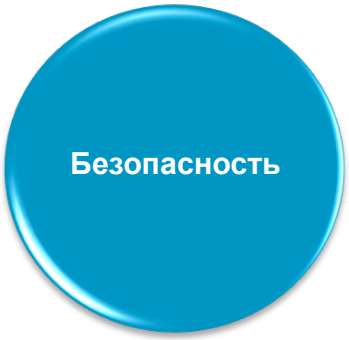
  Вы не можете сконфигурировать WCCP и PBR, WCCP и VRF на одном интерфейса и WCCP на туннельных интерфейсах

  Рекомендуемая версия IOS зависит от версии

Проконсультируйтесь с вашим Cisco SE перед внедрением ☺

# Cisco Secure Web Gateway

## Самое высокопроизводительное решение в индустрии

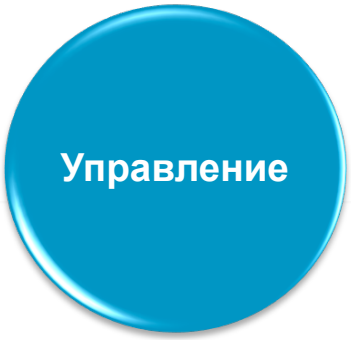



Многоуровневая защита от malware

Фильтры Web-репутации

Ускоренное сканирование сигнатур(механизм DVS)

Предотвращение работы ботнетов и malware, которые обходят порт 80(L4TM)

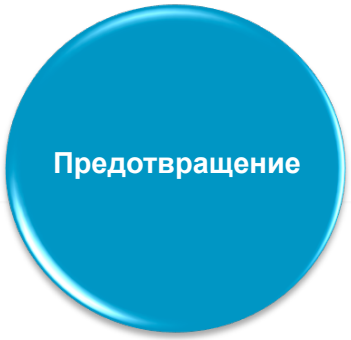



Интегрированная аутентификация и SSO

Мощные механизмы URL категорий и фильтрации

Фильтрация приложений и контента

Web usage visibility and tracking




Простая безопасность данных on-box

Взаимодействие с DLP системами 3-х производителей

Предотвращение брешей в защите, инициируемых malware (L4TM)

# Iron Port Training @ Fast Lane

- Единственный авторизованный партнер на территории России
- Трек курсов включает
  - 2 тренинга по C-Series
  - 1 тренинг по S-Series
- Инструктор CCIE

- Возможность проведения курсов по WEBEX для регионов

- Специальное предложение для партнеров Cisco и Iron Port
  -20% скидка на обучение по IronPort


95% of companies who try Cisco IronPort become customers.

*Contact:*

Your Cisco IronPort Rep
650-989-6530
sales@cisco.com

# Вопросы и Ответы