Cisco Expo 2011

Техническое введение в безопасность контента

Pavel Rodionov -- Systems Engineer, Security, Emerging Markets East

innovate together

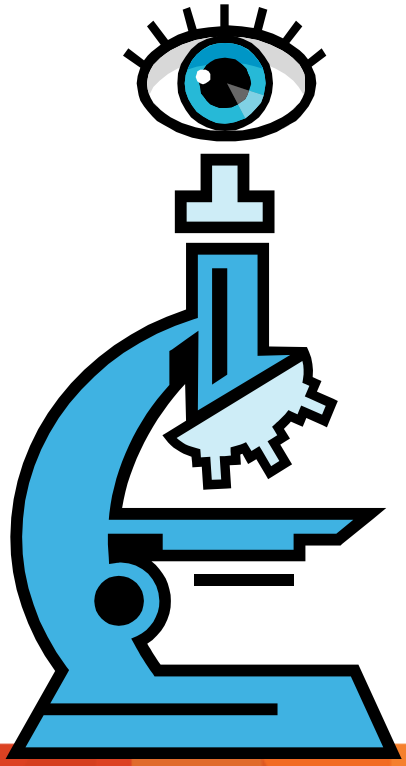
Программа

- Cisco SIO и SensorBase
- Cisco IronPort E-mail Security Appliance
- Cisco IronPort Web Security Appliance
- Cisco Cloud Services
- Вопросы и ответы

Расширенная безопасность

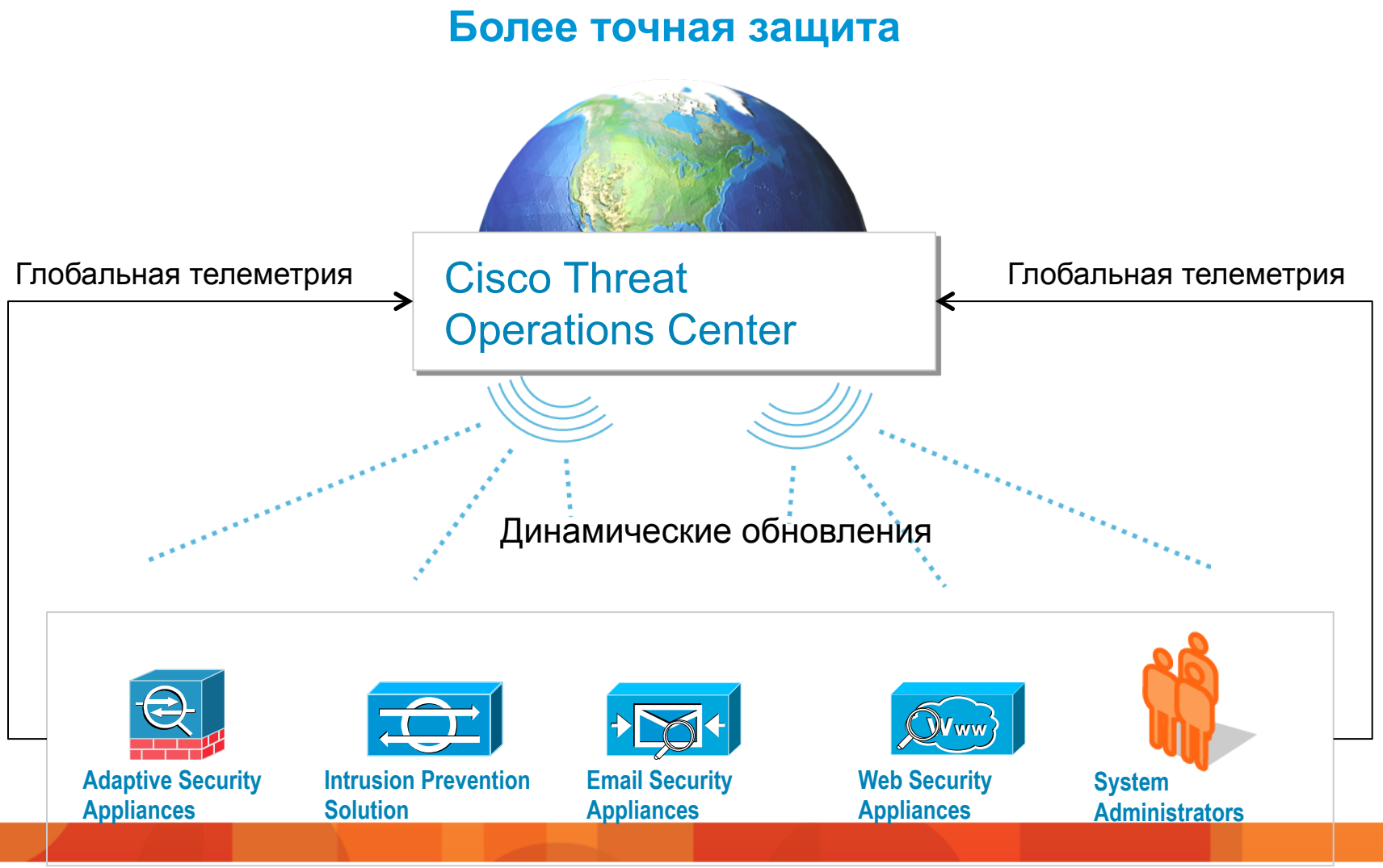
Глобальное смещение

- **2000-2008:** Продукты IT безопасности смотрят глуюже



- **2009:** Продукты безопасности Cisco смотрят шире, отзываются быстрее

Cisco Security IntelligenceOperations (SIO)
Обзор



Cisco SIO
Основные компоненты

Мощная экосистема обеспечивает быструю, точную защиту

Cisco SIO
Cisco SensorBase

Самая большая сеть, высочайшее качество данных, непревзойденный размах

Cisco SensorBase Network

Не имеющий равных уровень охвата глобальных угроз

Множество устройств

1M устройств безопасности, 10M клиентов ежегодно

Интернет-маршрутизаторы ядра

Облачные сервисы

Самый большой объем данных

30% мирового почтового и web трафика

200+ параметров

800+GB в день данных телеметрии

Разные источники

Восемь из 10 крупшейших ISPs

Источники: Fortune 500, Global 2000, университеты, SMBs

152 других источника

Мы первые совместили данные сетевого и application уровней

Cisco SensorBase Network

Непревзойденный диапазон данных

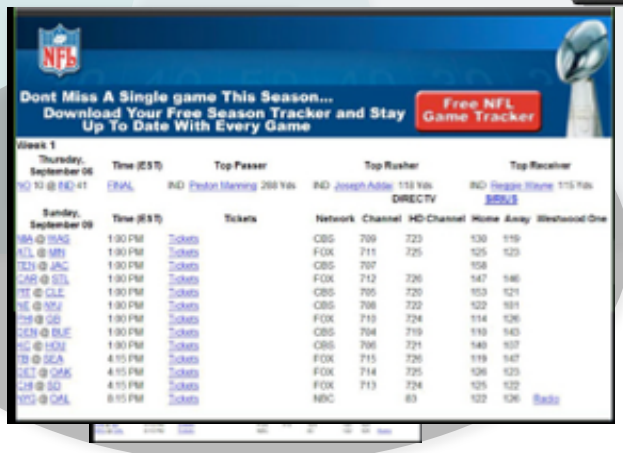
SensorBase сеть

Email

From: Bill Gates
To: John Chambers
Cc:
Subject: Free NFL Game[IronPort SUSPECTED SPAM]

Football is back, life may resume again!
Know all the games, what time what channel and
have all the details for every game with our f
http://69.247.209.124

Спам с вредоносным вложением



Сайт распространяющий malware

Firewall / IPS

Directe

Прямая атака

Cisco SIO
Cisco Threat Operations Center (TOC)

Исследование и разработка, моделирование безопасности, опытные аналитики

Cisco Threat Operation Center
Исследования и разработка

- **Миллионы инвестиций в R&D**
  - –Эксперты и статистики по угрозам
  - –Оборудование и инфраструктура
  - –Через лидерство, предотвращение и экспертиза, best practices
  - –76 патентов
- **Инновационные сервисы**
  - –Глобальная корреляция IPS
  - –ASA. Фильтры ботнет трафика
  - –Outbreak фильтры
  - –Репутационные фильтры (IPS, почта, web, и т.д.)

Cisco Threat Operations Center

Гарантирует точность и время отклика

Опытные аналитики

500 аналитиков

Европейские и азиатские языки

1 Cisco Fellow

80+ Ph.D.s, CCIEs, CISSPs, MSCEs

Работа 24x7x365

5 центров, расположенных по всему миру

San Jose, San Bruno, Austin, North Carolina, Shanghai

Мощные инструменты

Динамические обновления

Корреляция и исследование данных

Оптимизированное утверждение правил, приложения для создания и публикации

Cisco SIO
Лучшие возможности по применению

Быстрые механизмы сканирования и детальные политики

Улучшенная защита
Соберем все вместе

Продукты и сервисы Cisco: Высокопроизводительные, гибкие точки применения


Adaptive Security Appliances


Intrusion Prevention Solution

Web Security Appliances


Email Security Appliances


Hosted Email Services

Фильтры безопасности: Наиболее эффективные механизмы безопасности

- Outbreak Filters
- Anti-Spam
- Email Reputation Filters
- Web Reputation Filters
- IPS Reputation and Signature Filters
- Firewall Botnet Traffic Filters

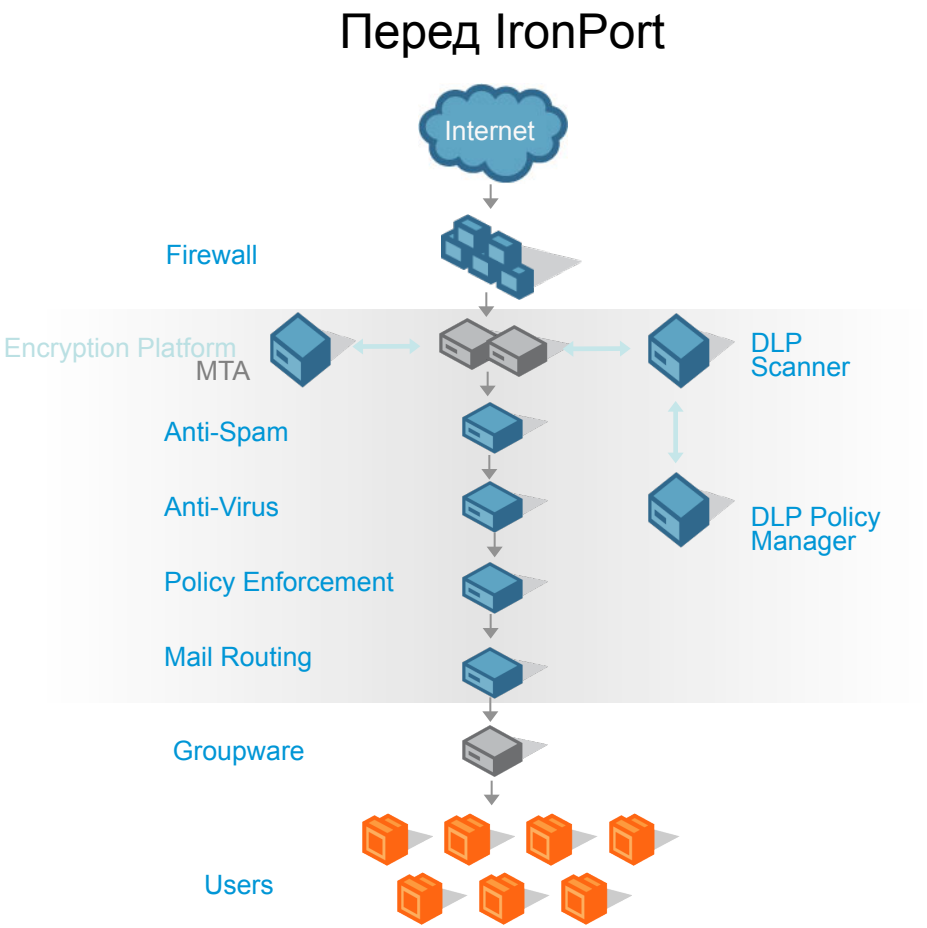
Cisco SIO: Облачные механизмы безопасности

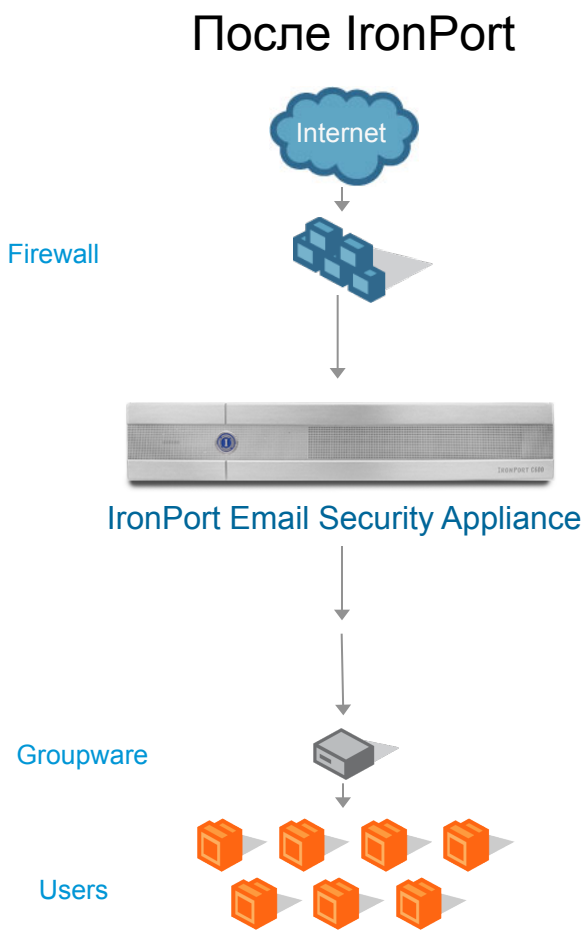
- Живые значения репутации
- Постоянное обновление сигнатур
- Разработанные наборы правил
- Динамические наборы правил
- Авто-обновления каждые 5 мин.

Cisco IronPort E-mail Security Appliances

Cisco IronPort объединяет периметр сети

Для надежности, безопасности и снижения затрат на обслуживание

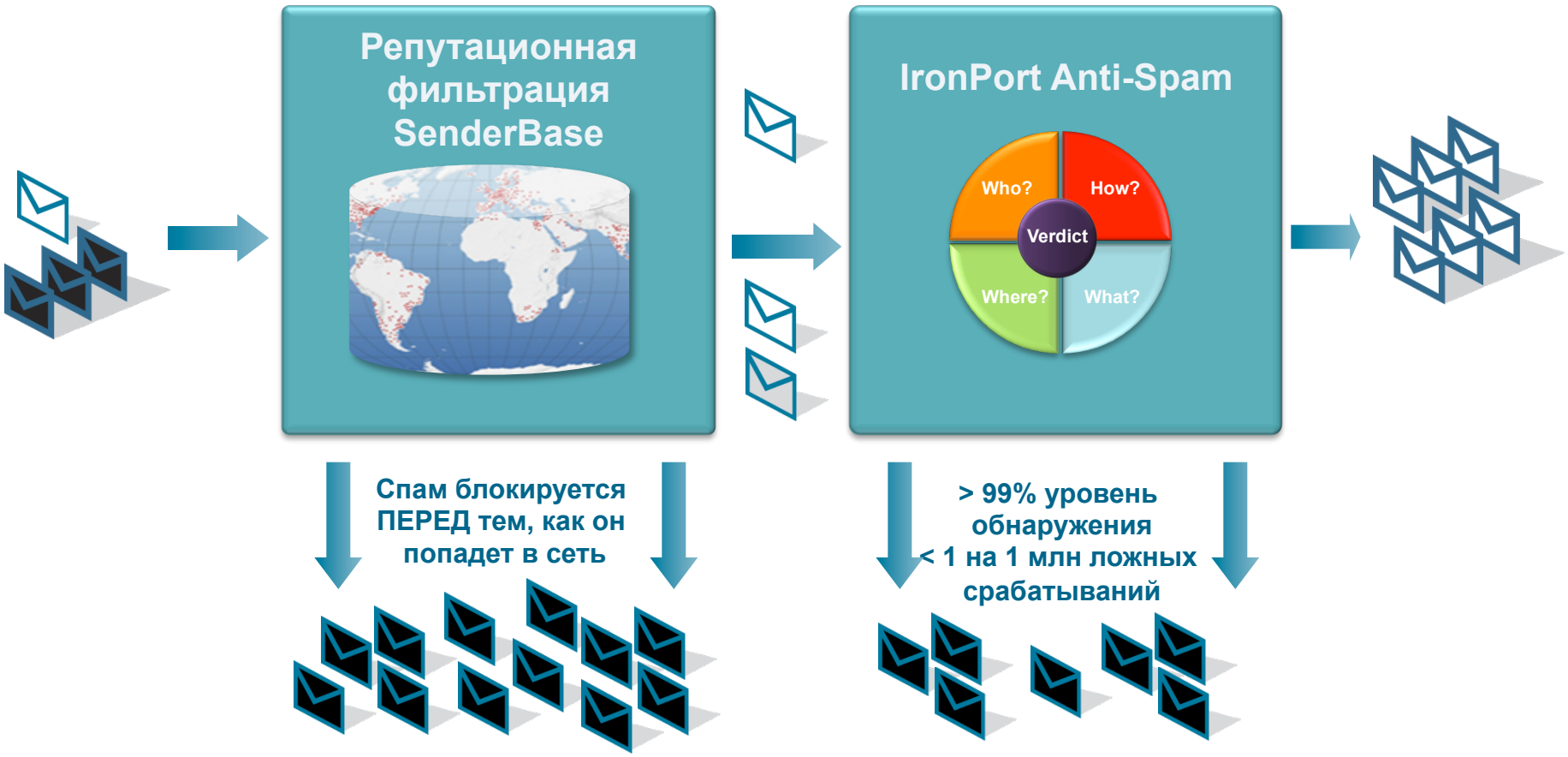




Email Security Architecture

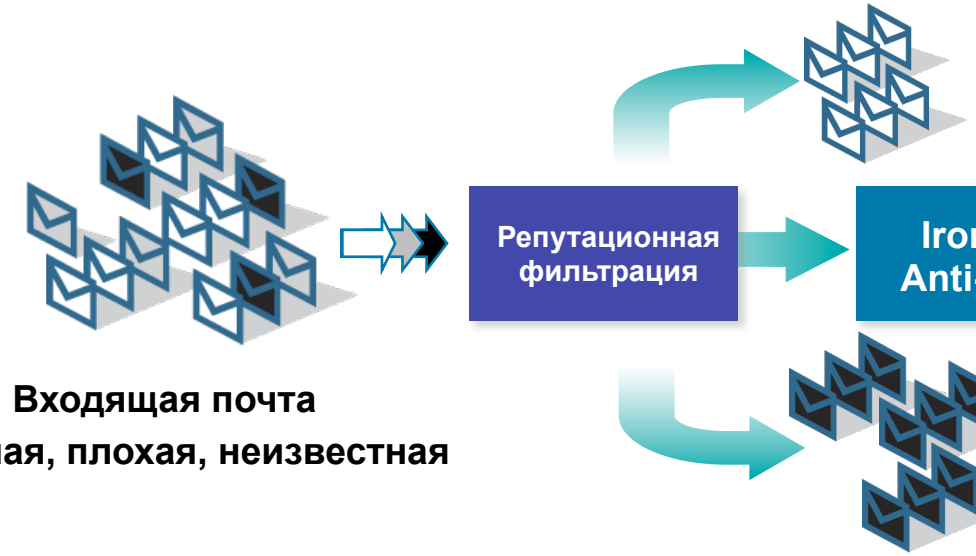
Безопасность входящих, контроль исходящих

Антиспам – эшелонированная оборона



Репутационная фильтрация SenderBase

Предотвращение угроз в реальном времени



Входящая почта
Хорошая, плохая, неизвестная

Хорошая доставляется

- **Подозрительная ограничивается и проверяется на спам**
- **Плохая блокируется**

Cisco on Cisco

Наша статистика

Message Category	%	Messages
Stopped by Reputation Filtering	**93.1%**	700,876,217
Stopped as Invalid recipients	0.3%	2,280,104
Spam Detected	2.5%	18,617,700
Virus Detected	0.3%	2,144,793
Stopped by Content Filter	0.6%	4,878,312
Total Threat Messages:	**96.8%**	**728,797,126**
Clean Messages	3.2%	24,102,874
Total Attempted Messages:		**752,900,000**

Cisco IronPort Anti-Spam

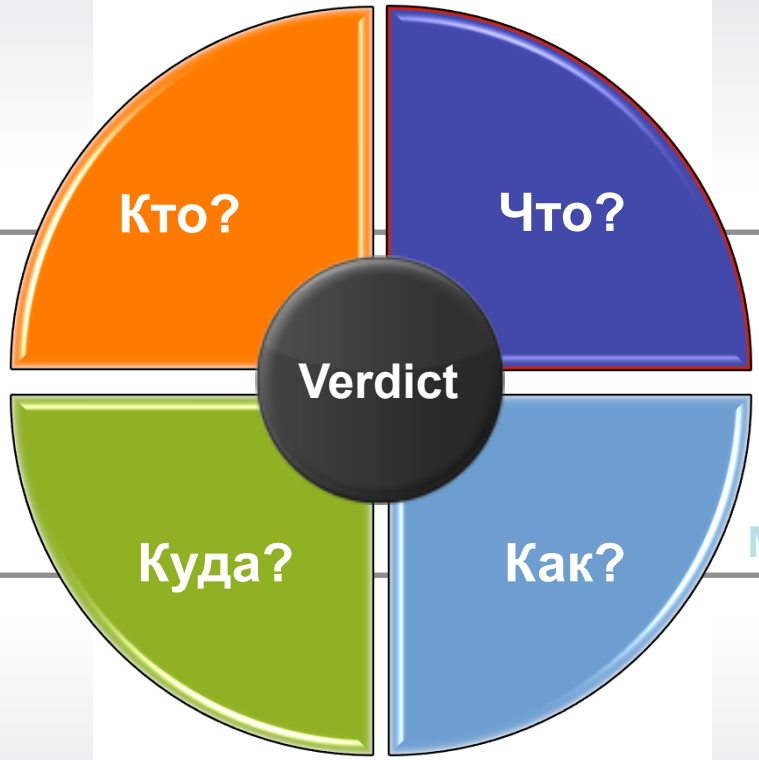
Эшелонированная защита от спама

EMAIL REPUTATION

- ✓ Spam Botnets
- ✓ Spammer Networks

MESSAGE CONTENT

- ✓ SMS Spam
- ✓ Attachment-based Spam



WEB REPUTATION

- ✓ Malware/Phishes
- ✓ Short-Texted Spam with URLs

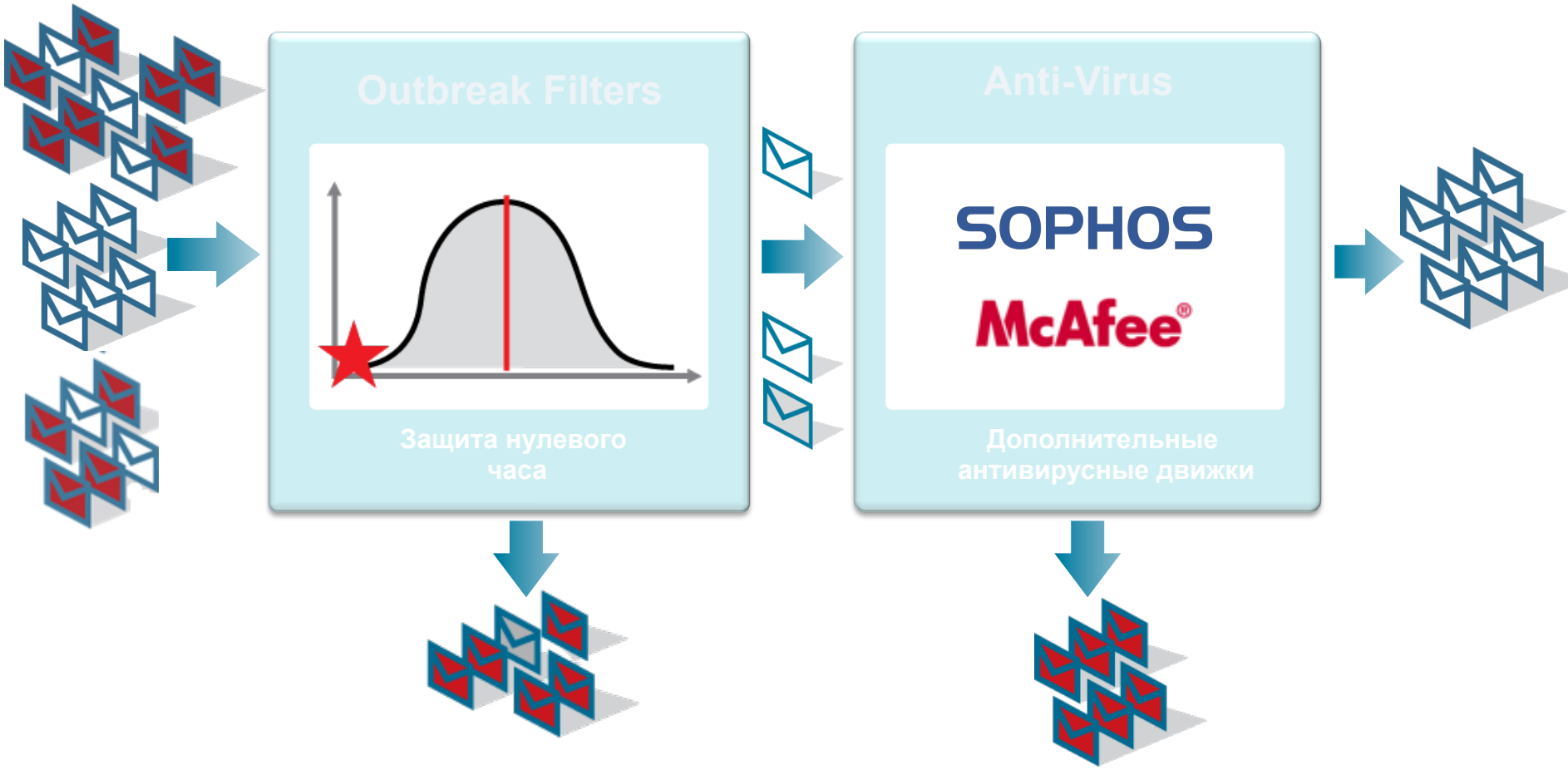
MESSAGE CONSTRUCTION

- ✓ Image Spam
- ✓ Spam created using Automation Tools

Email Security Architecture

Безопасность входящих, контроль исходящих

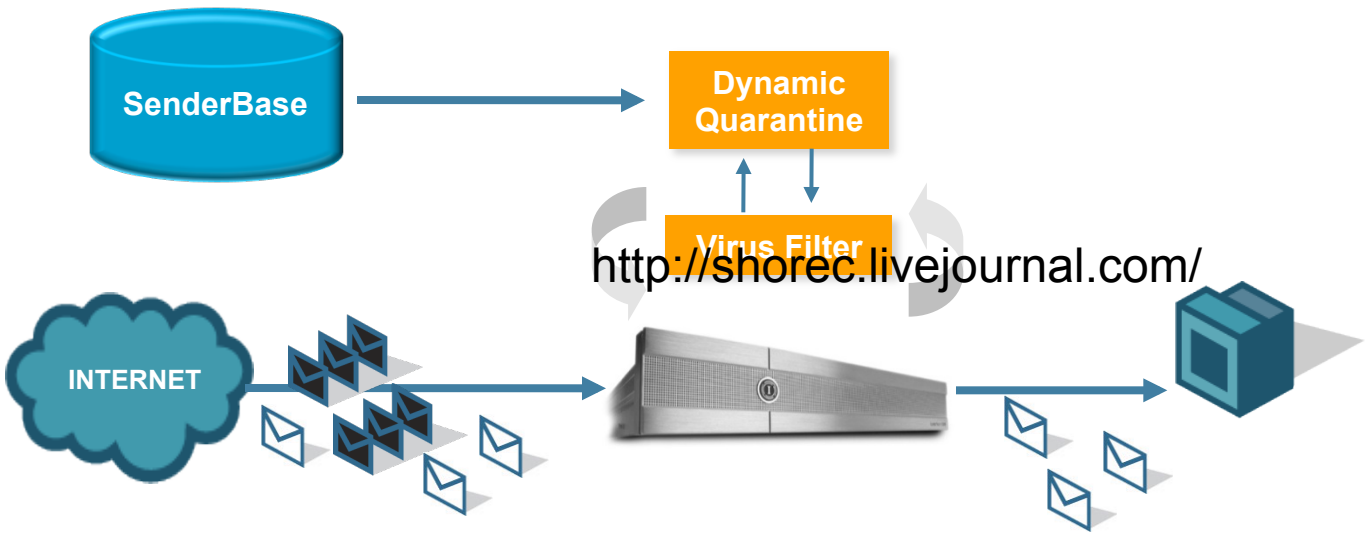
Эшелонированная антивирусная защита



Cisco IronPort Virus Outbreak Filters

Защита от malware нулевого дня

Virus Outbreak Filters в действии



http://shorec.livejournal.com/

Преимущества Virus Outbreak Filters

Average lead time*……over 13 hours

Outbreaks blocked* ……291 outbreaks

Total incremental protection*…… over 157 days

"Since VOF we have not had a single virus outbreak!"

AIR FRANCE

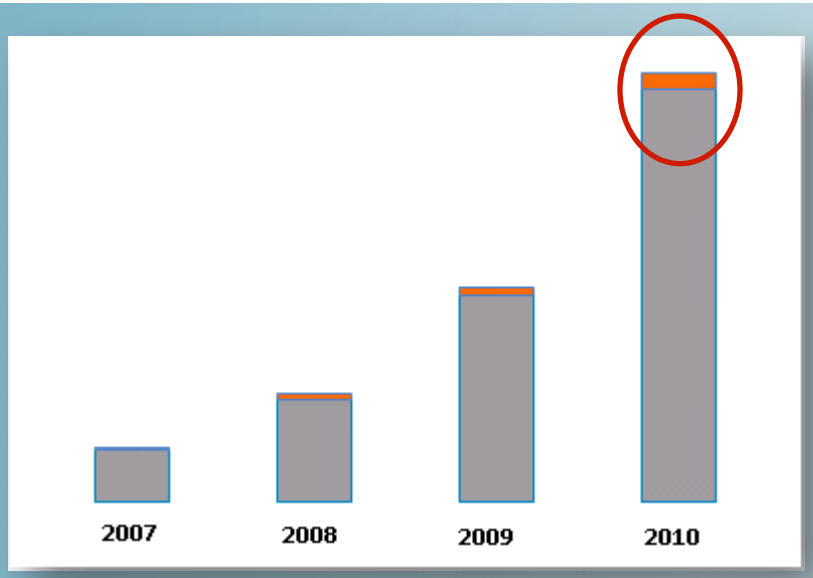
"Over 24,000 virus positive messages stopped in 9 months"

JOHNS HOPKINS UNIVERSITY

"VOF has stopped more than 12,000 separate viral messages in the last year"

Оставшийся процент

Обгоняя новые угрозы



Эволюция угроз

- URL специально созданный для сообщения
- Сокращенные URL

Эволюция защиты

Многоуровневая целевая защита

Задержка

- Подозрительные угрожающие сообщения
- Все виды угроз (спам, фишинг, целевые)

Перенаправление

- Подозрительные URL на Cisco Web Security

Изменение

- Содержимое сообщения (тема)
- Добавить предупреждение

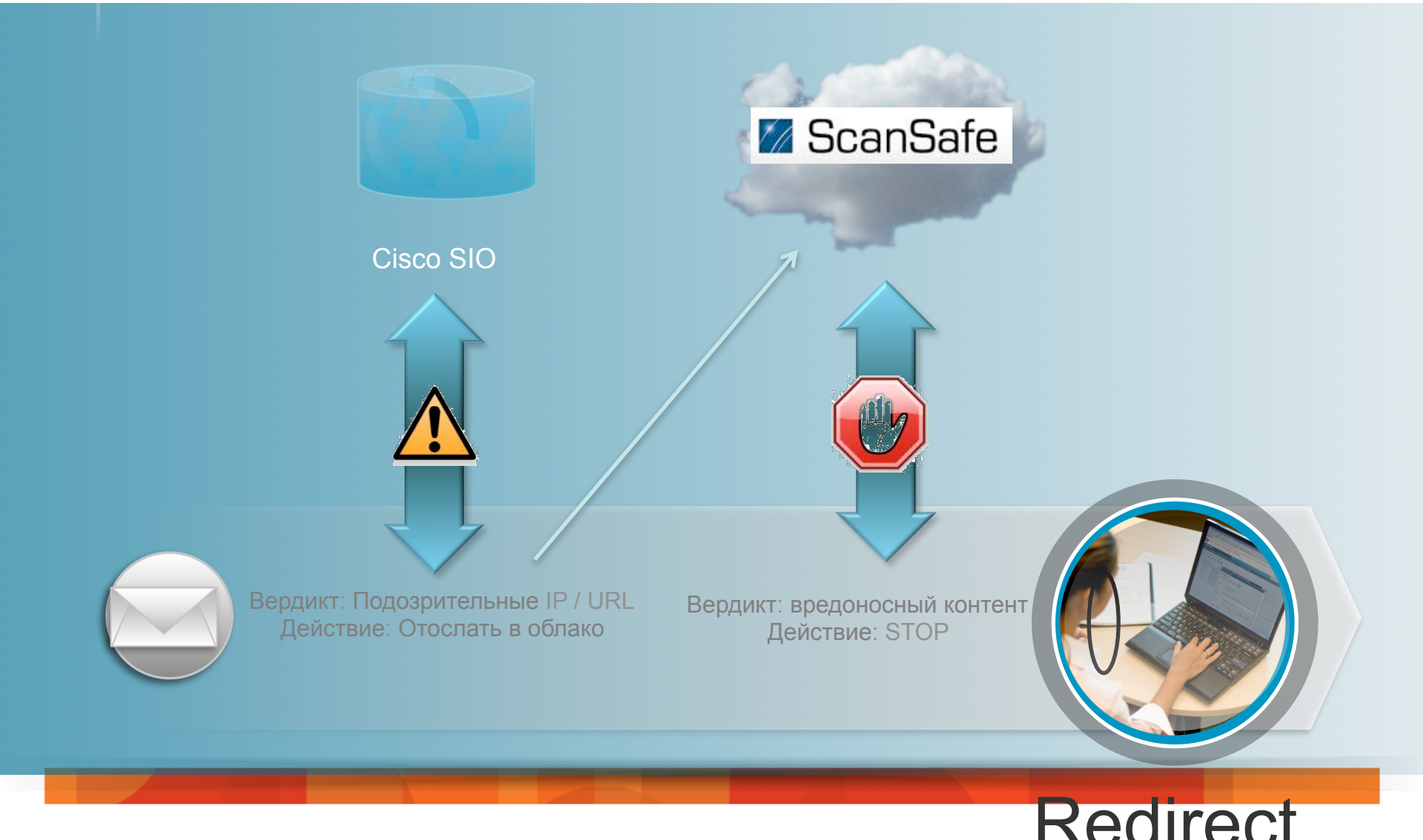
Задержка подозрительных сообщений

Outbreak фильтрация в действии

Delay

Перенаправление подозрительных URI

Outbreak фильтрация в действии



Обзор функционала

- Обнаружение фишинг-писем и URL угроз
  - Дополнительно к защите от зараженных вирусами присоединенных файлов
  - Для сканирования используется IPAS (CASE)
- Время хранения в динамическом карантине
  - CASE возвращает время хранения
  - Максимальные установки времени хранения имеют более высокий приоритет
  - Разное время хранения для вирусных и других угроз
- Повторное сканирование карантина
  - Вирусные угрозы сканируются после обновления правил TOC/AV
  - Другие угрозы сканируются согласно рекоменуемому интервалу CASE
  - Повторное сканирование CASE позволяет обнаруживать короткоживущие фишинговые угрозы

Обзор функционала - продолжение

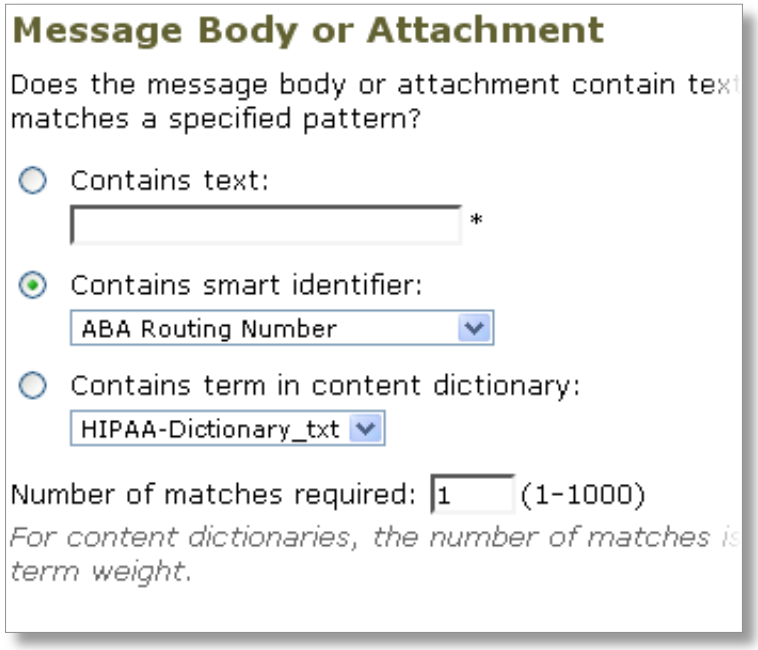
- Модификация URL
  - Перезапись URL для использования в прокси
  - Вместе работают ScanSafe и SecApps
  - Подписанные сообщения могут быть оставлены неизменными
  - Список исключений доменов
  - Поддержка IPv4 и IPv6 буквенные/CIDR, имена хостов, и домены
- Предупреждения
  - Если сообщение потенциальная угроза
  - Генерируется системой или же с помощью встроенных словарей
  - Уровень угрозы, категория, тип, описание доступны для заполнения
  - Добавляется в начало сообщения

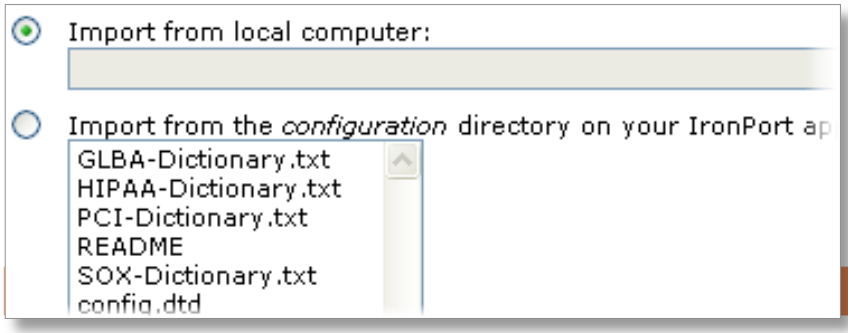
Email Security Architecture

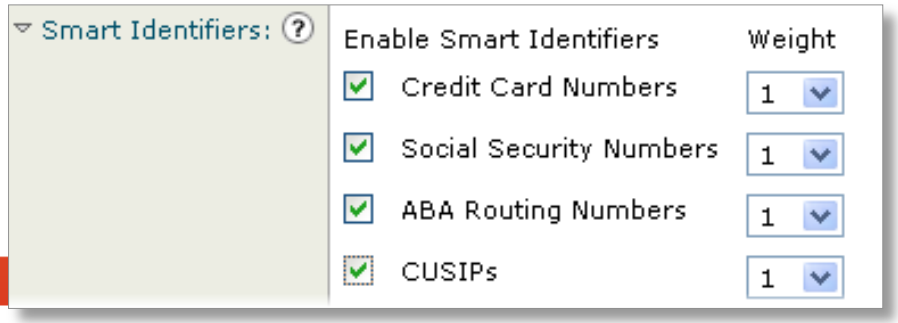
Безопасность входящих, контроль исходящих

Data Loss Prevention
Простая установка

- Простая установка в «три клика» для фильтров контента
- Испольование предопределенных категорий/ создание своих
- Могут применяться для определенных пользователей/ определенных условий



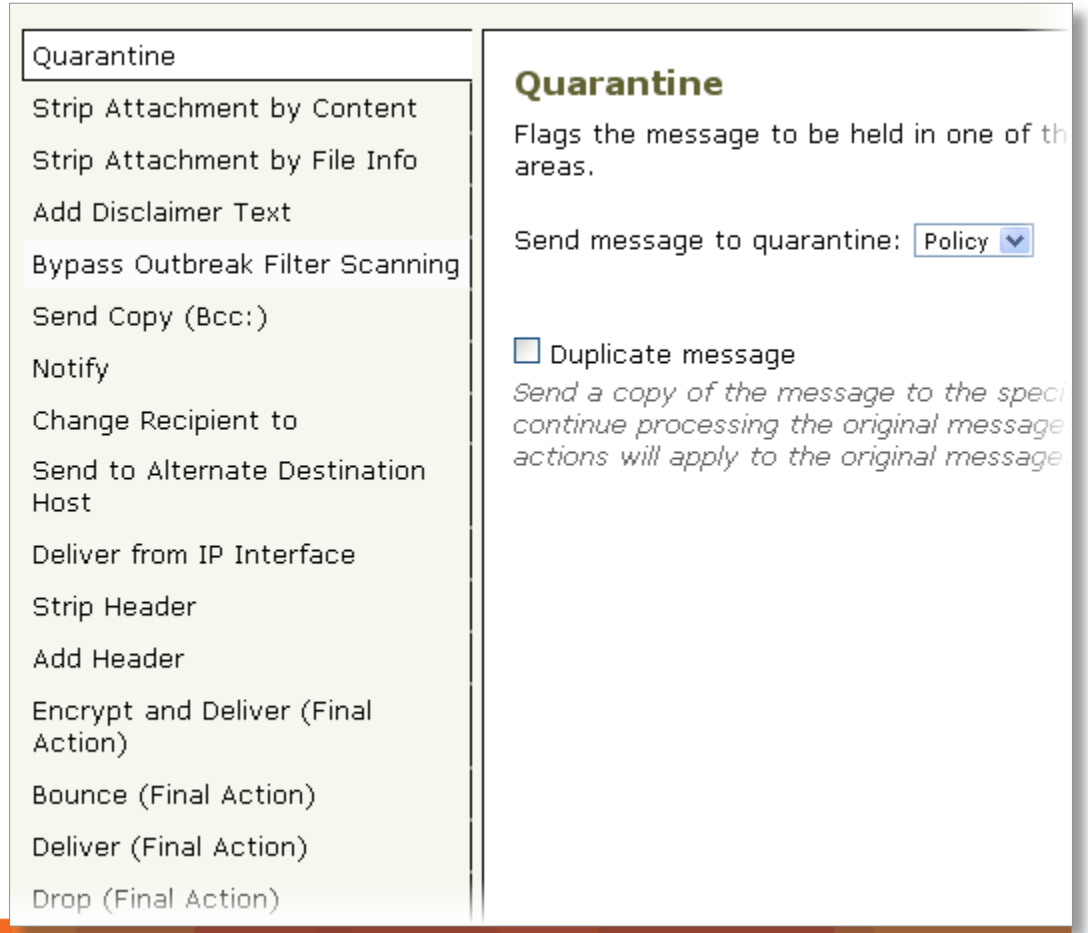




Data Loss Prevention

Всесторонние опции реагирования и отчетности

- Множество опций реагирования – шифрование, карантин, сброс, рикошет, BCC, удаление контента
- Подозрительный контент подсвечивается в карантине для простоты анализа
- Репортинг по политикам и по пользователям



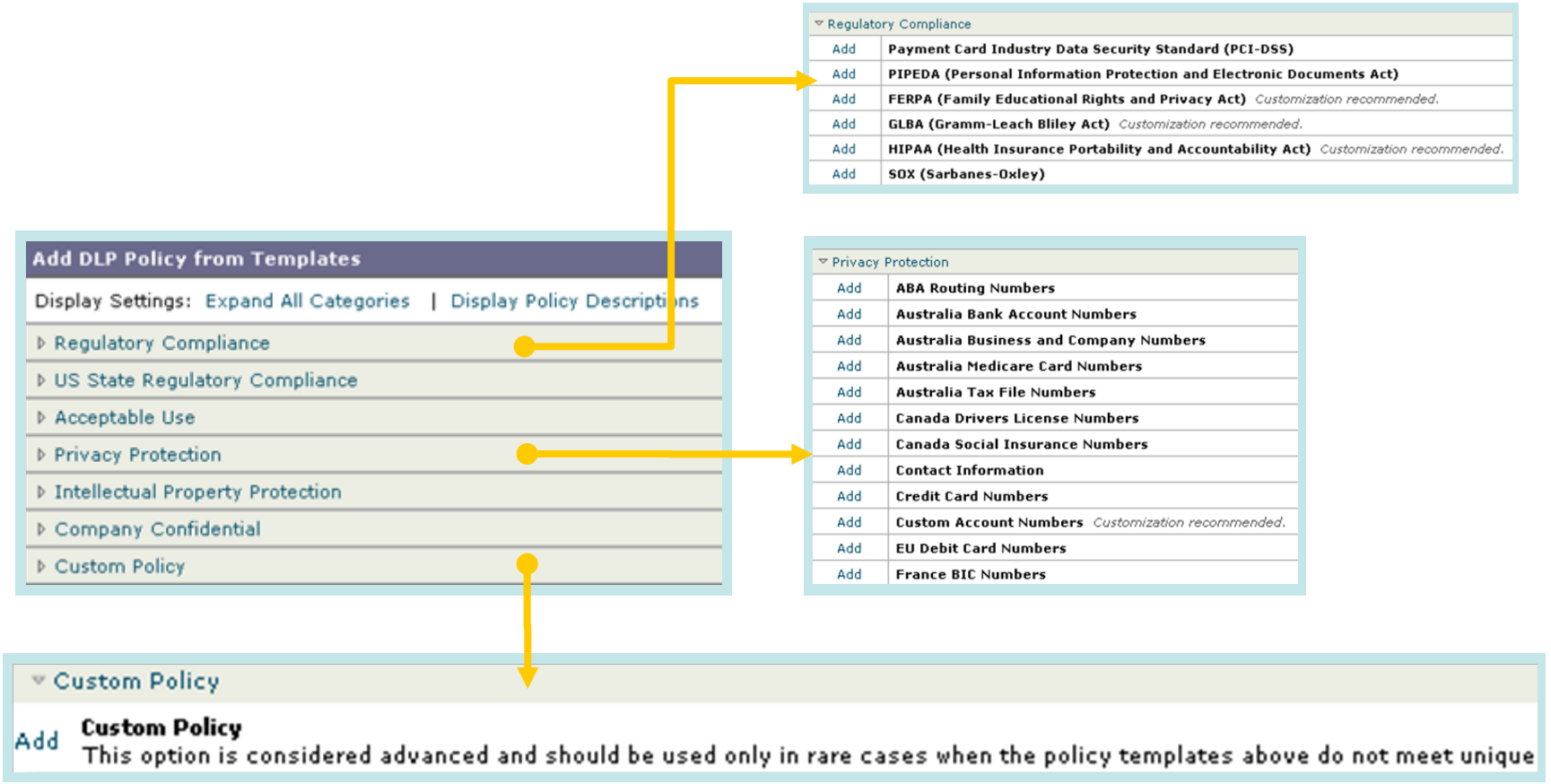
RSA – Рынок рынка и технологий

- Ranked as “Leader” in Gartner Magic Quadrant
- Focus on accuracy:
  large research team staffed specifically to write and refine content polices

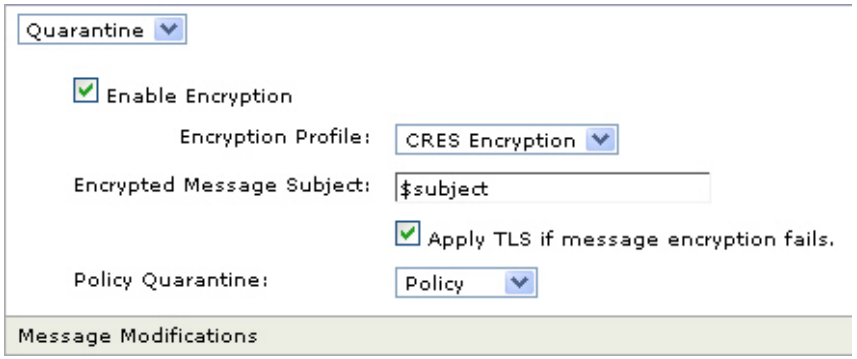
“RSA has strong described content capabilities enabled by a formal knowledge-engineering process” - Gartner

Всестороннее закрытие политиками

100+ Предопределенных политик для полного покрытия

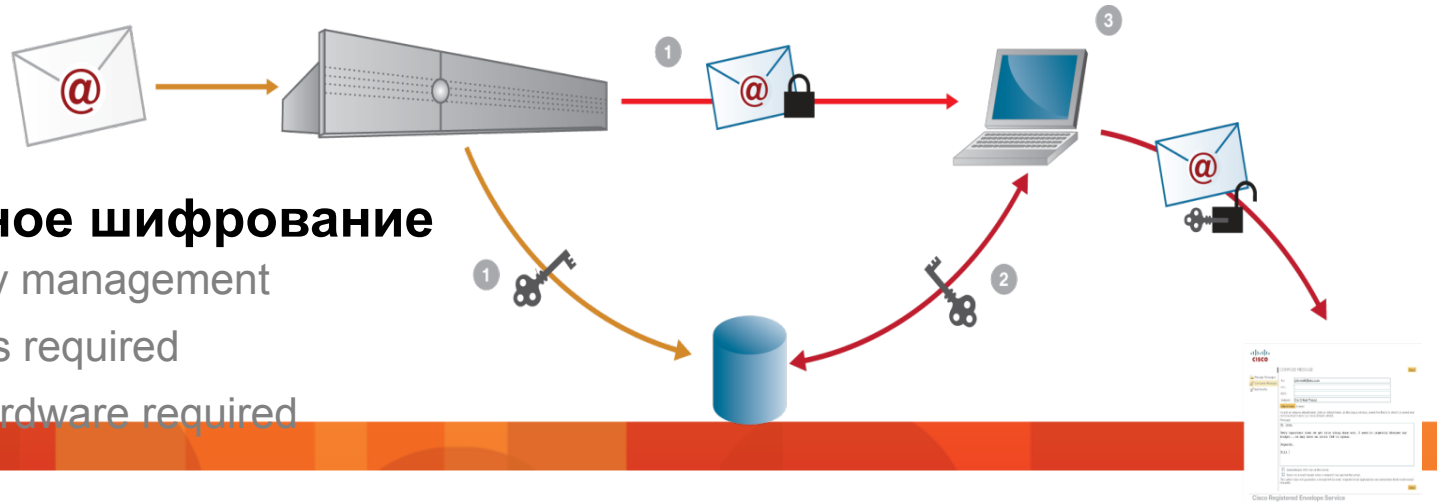


Полный набор опций реагирования



Автоматическое реагирование

- Encrypt, quarantine, deliver, or drop
- Add disclaimer, modify subject
- Copy or notify
- Guaranteed secure delivery



Встроенное шифрование

- Hosted key management
- No plug-ins required
- No new hardware required

Email Security Architecture

Безопасность входящих, контроль исходящих

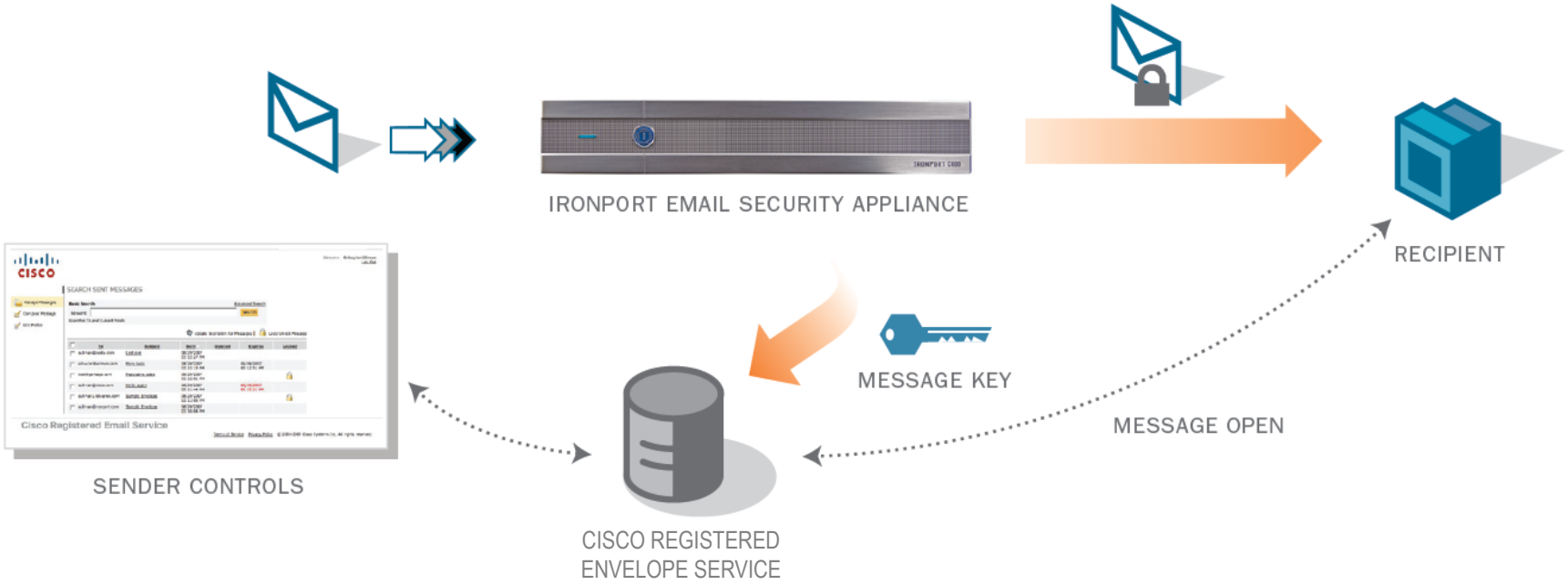
Препятствия к внедрению

Почему шифрование email еще не внедрено везде?

- **Простота использования**
  - Сложные плагины и вмешательство в работу пользователей
  - Public Key и Identity Management
- **Простота внедрения**
  - Поддержка плагинов
  - Public Key и инфраструктура Identity Management
- **Универсальность**
  - Требует уже настроенной системы криптографических связей
  - Отправка/получение ограниченным набором клиенов с плагинами

Шифрование Cisco IronPort Email

Просто для отправителя. . .

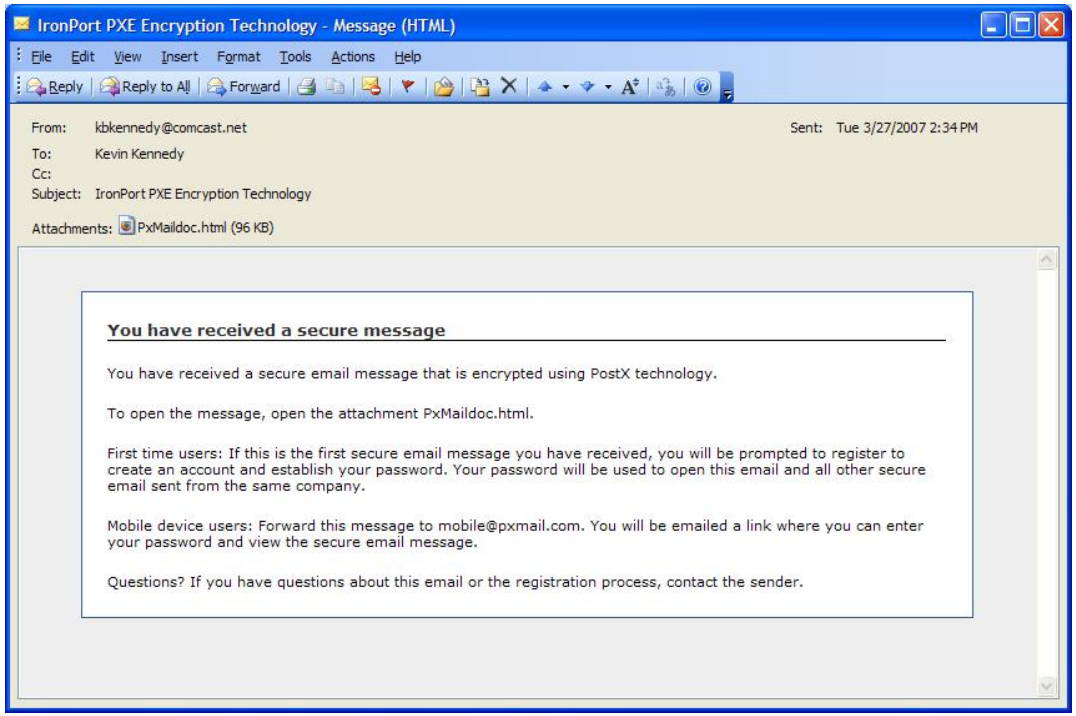


- Автоматическое управление ключами
- Не требуется дополнительное ПО
- Прозрачная отправка на любой email

Шифрование Email Cisco IronPort

Получение сообщения

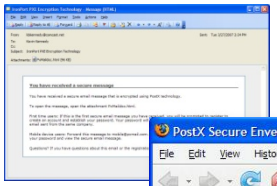
1. Получите почту, кликните для открытия присоединенного файла



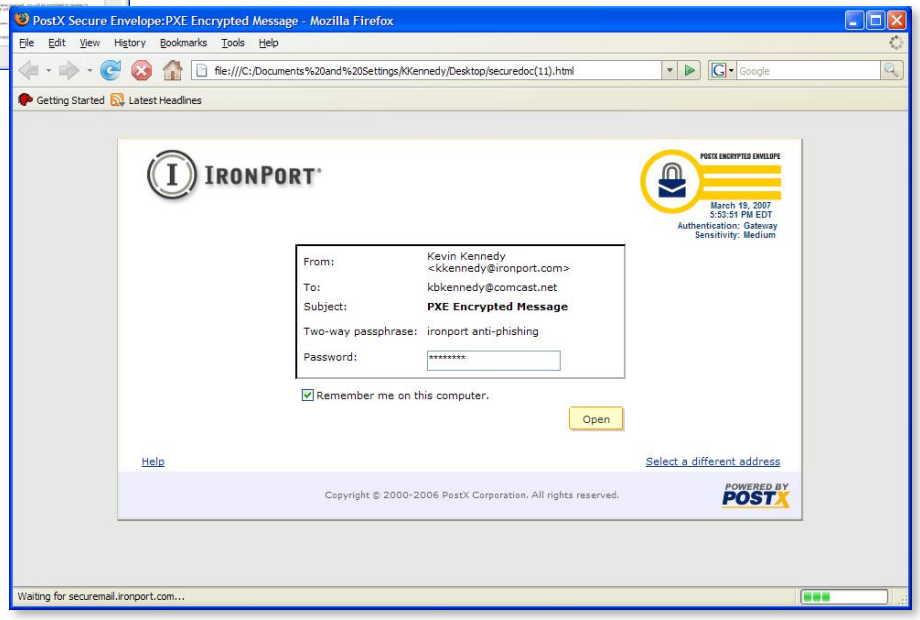
Шифрование Email Cisco IronPort

Получение сообщения

1 Получайте почту



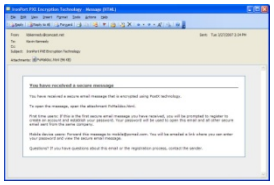
2 Введите пароль



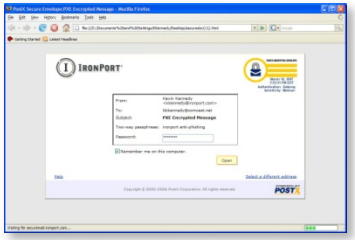
Шифрование Email Cisco IronPort

Получение сообщения

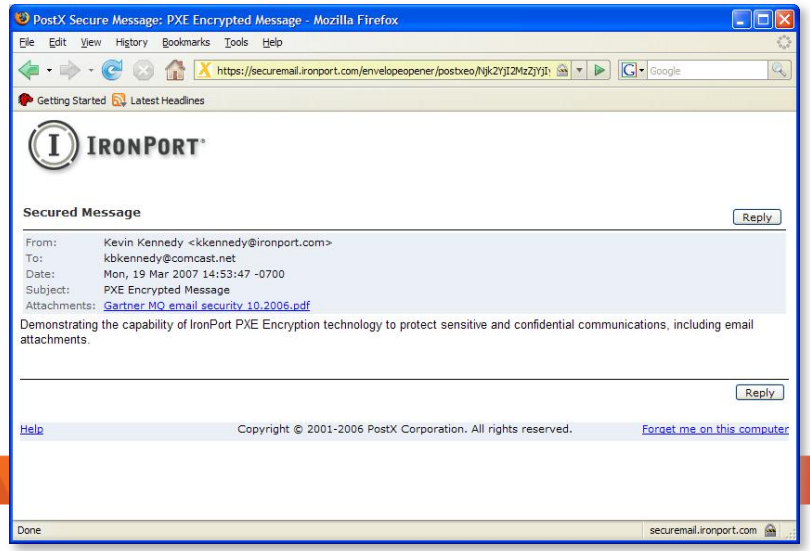
1. Получите письмо



2. Введите пароль



3. Просмотрите защищенное сообщение



Решение ограничений других продуктов шифрования Email

- **Простота использования -- решено**
  - Сложные плагины и вмешательство в работу пользователей
  - Public Key и Identity Management

  Нет клиентского ПО, нет сертификатов

- **Простота внедрения -- решено**
  - Поддержка плагинов
  - Public Key и инфраструктура Identity Management

  IronPort Hosted Key Service

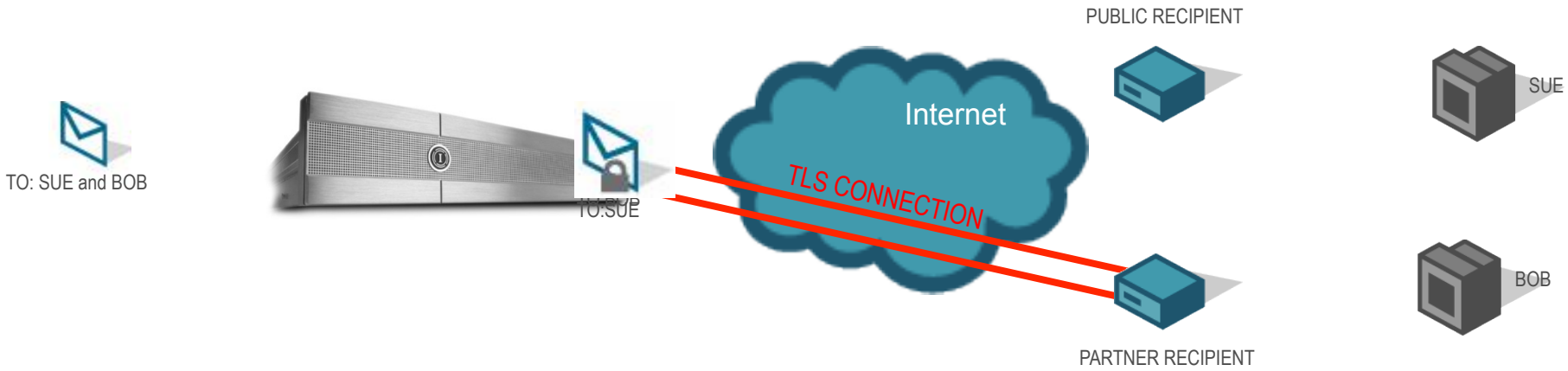
- **Универсальность -- решено**
  - Требует уже настроенной системы криптографических связей
  - Отправка/получение ограниченным набором клиенов с плагинами

  Отправка-получение с любой платформы

Гарантированная безопасная доставка

Шифрование почты по назначению

1. Если доступно, использовать TLS
2. Шифрование с помощью PXE Secure Envelope

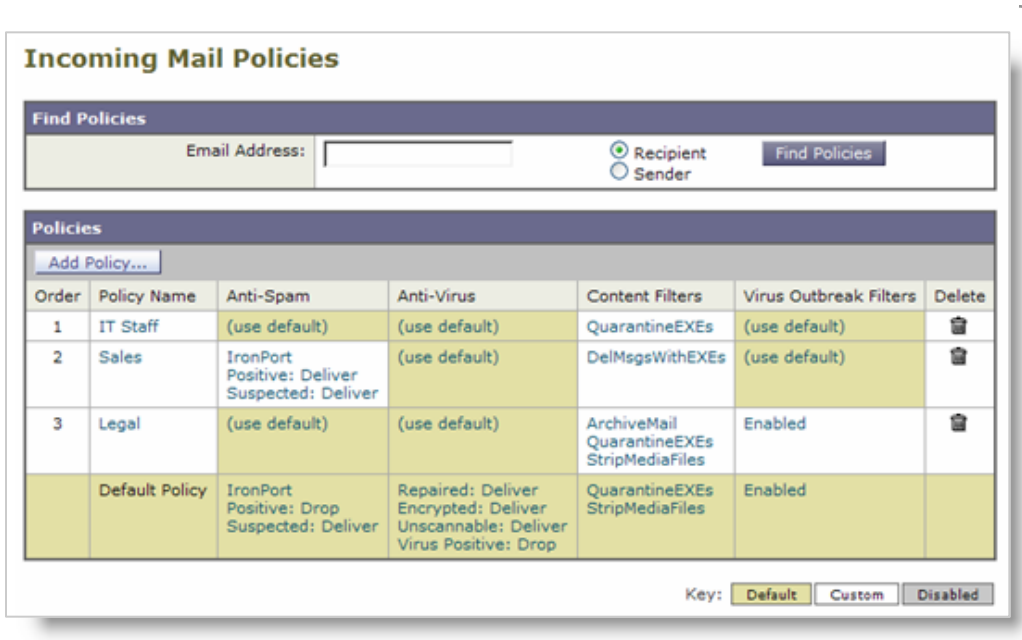


Email Security Architecture

Безопасность входящих, контроль исходящих

Cisco IronPort Email Security Manager

Просмотр политик для всей организации



Категории – домен, пользователь, LDAP группа

- Allow all media files
- Quarantine executables

IT

- Mark and Deliver Spam
- Delete Executables

SALES

- Archive all mail
- Virus Outbreak Filters disabled for .doc files

LEGAL

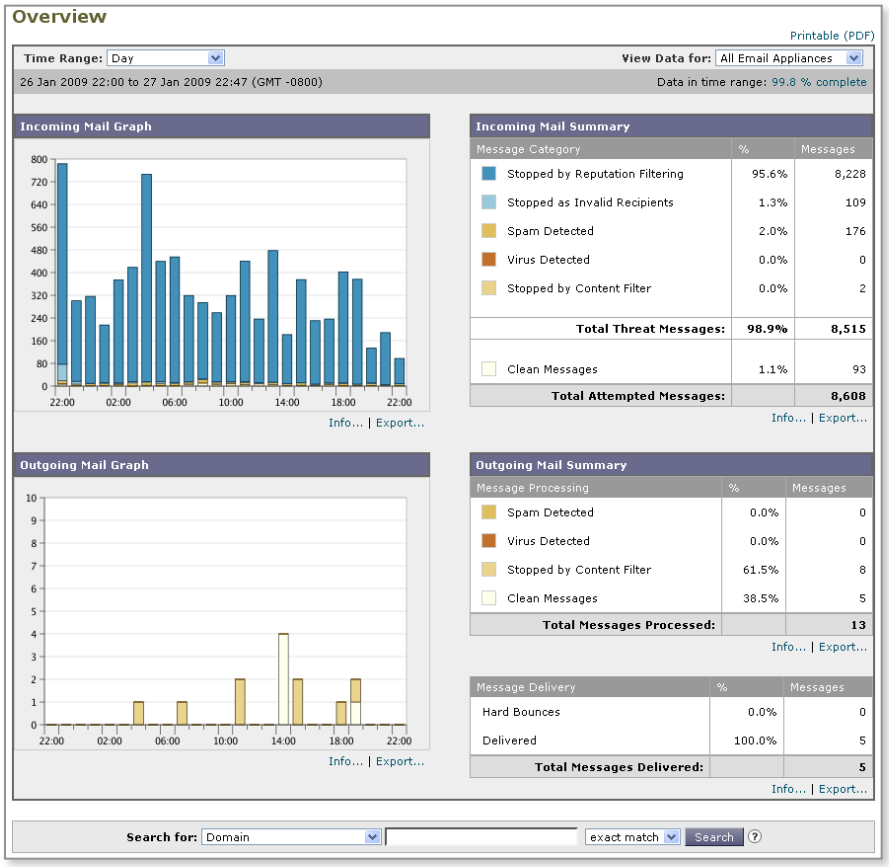
“IronPort Email Security Manager работает в качестве простой, гибкой панели всех настроек устройства.” – PC Magazine

Всесторонний просмотр

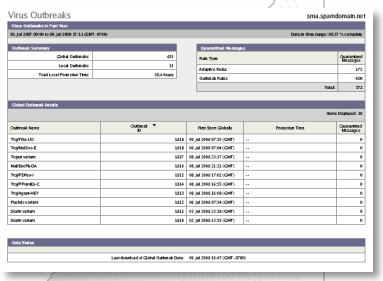
Система унифицированного репортинга

- Простой просмотр в организации
- Трафик реального времени Email и угроз
- Иерархические исполняемые отчеты

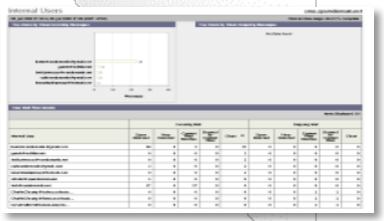
Объединенные отчеты



Несколько точек данных



Email Volumes
Spam Counters
Policy Violations
Virus Reports
Outgoing Email Data
Reputation Service
System Health View



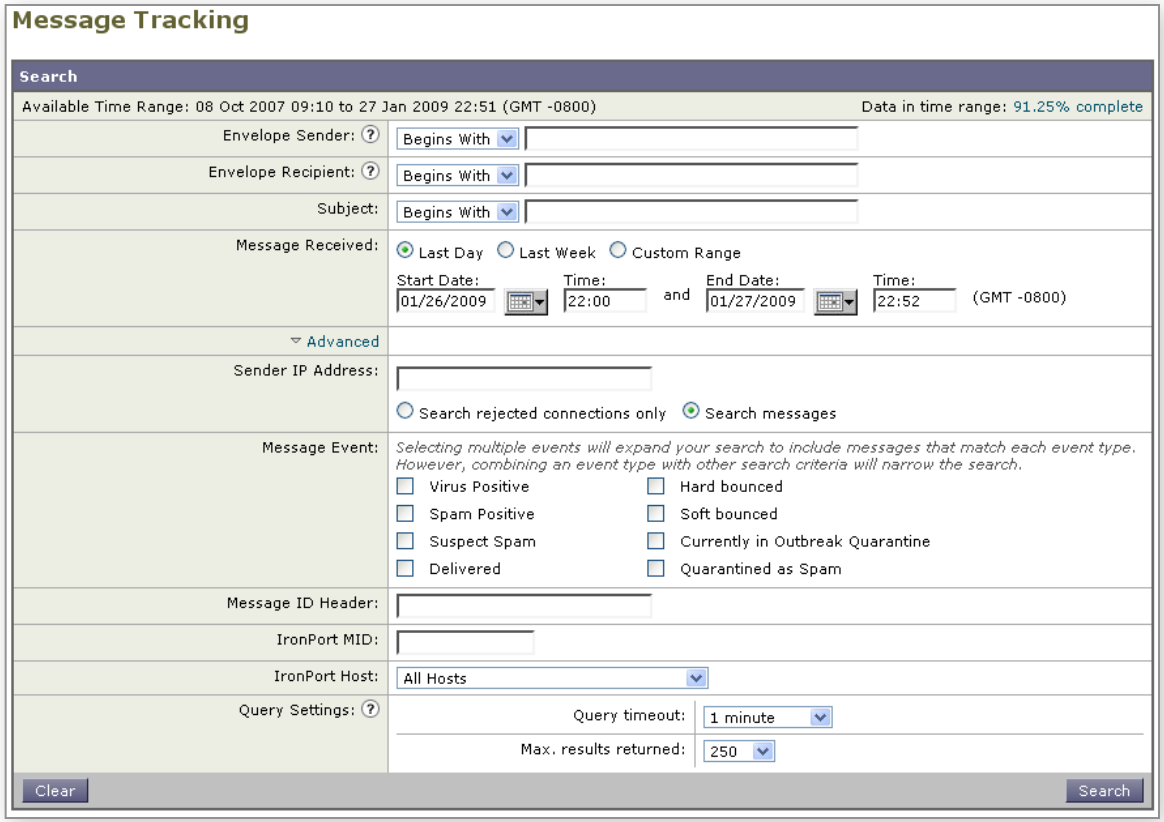
Просмотр Email
Message Tracking

Что случилось с письмом, которое я отослал 2 часа назад?

- ✓ Отслеживание индивидуальных Email сообщений

Кто еще получает такие сообщения?

- ✓ Расследование для гарании соответствия



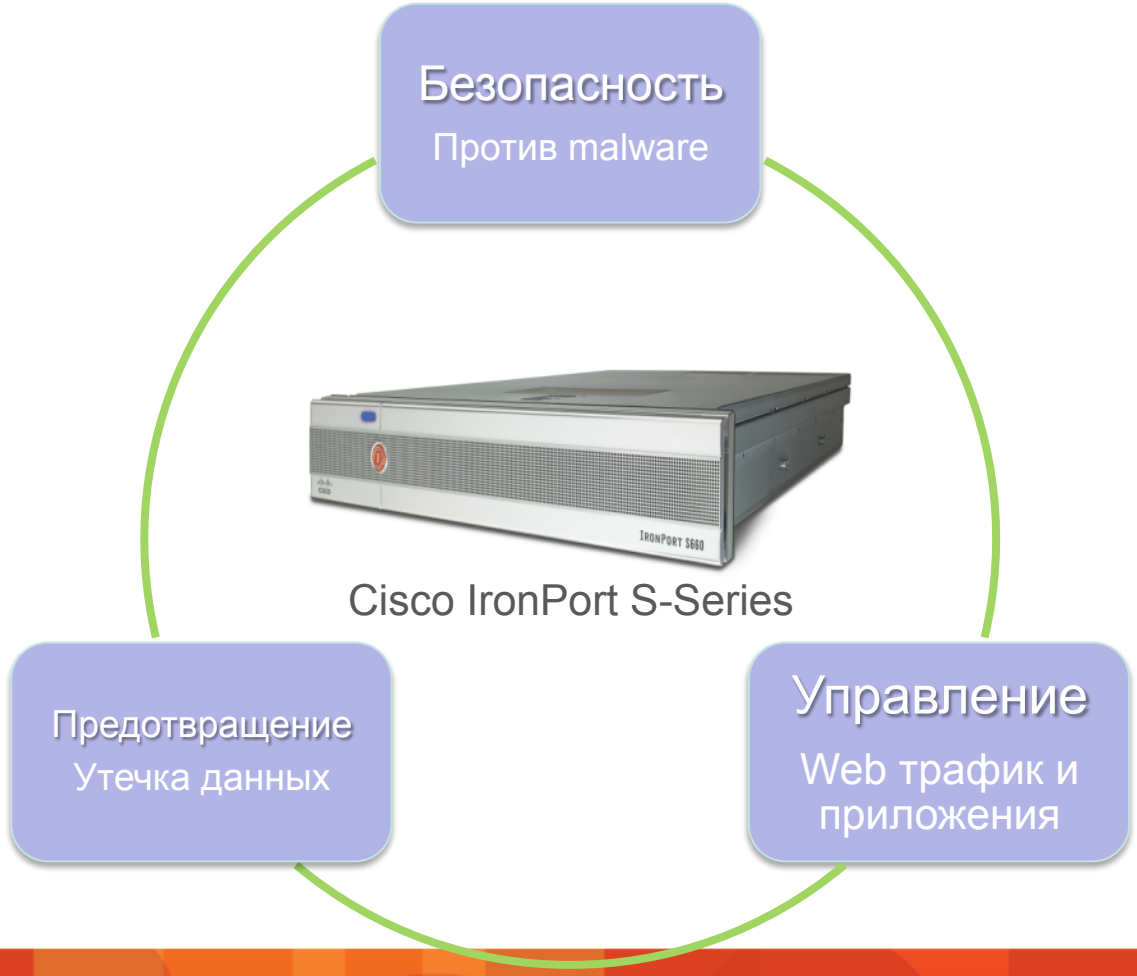
Скоро…

- Outbreak Filters
- Делегированное администрирование
- Поддержка «сильных» паролей
- SMTP Call Ahead

Cisco IronPort Web Security Appliances

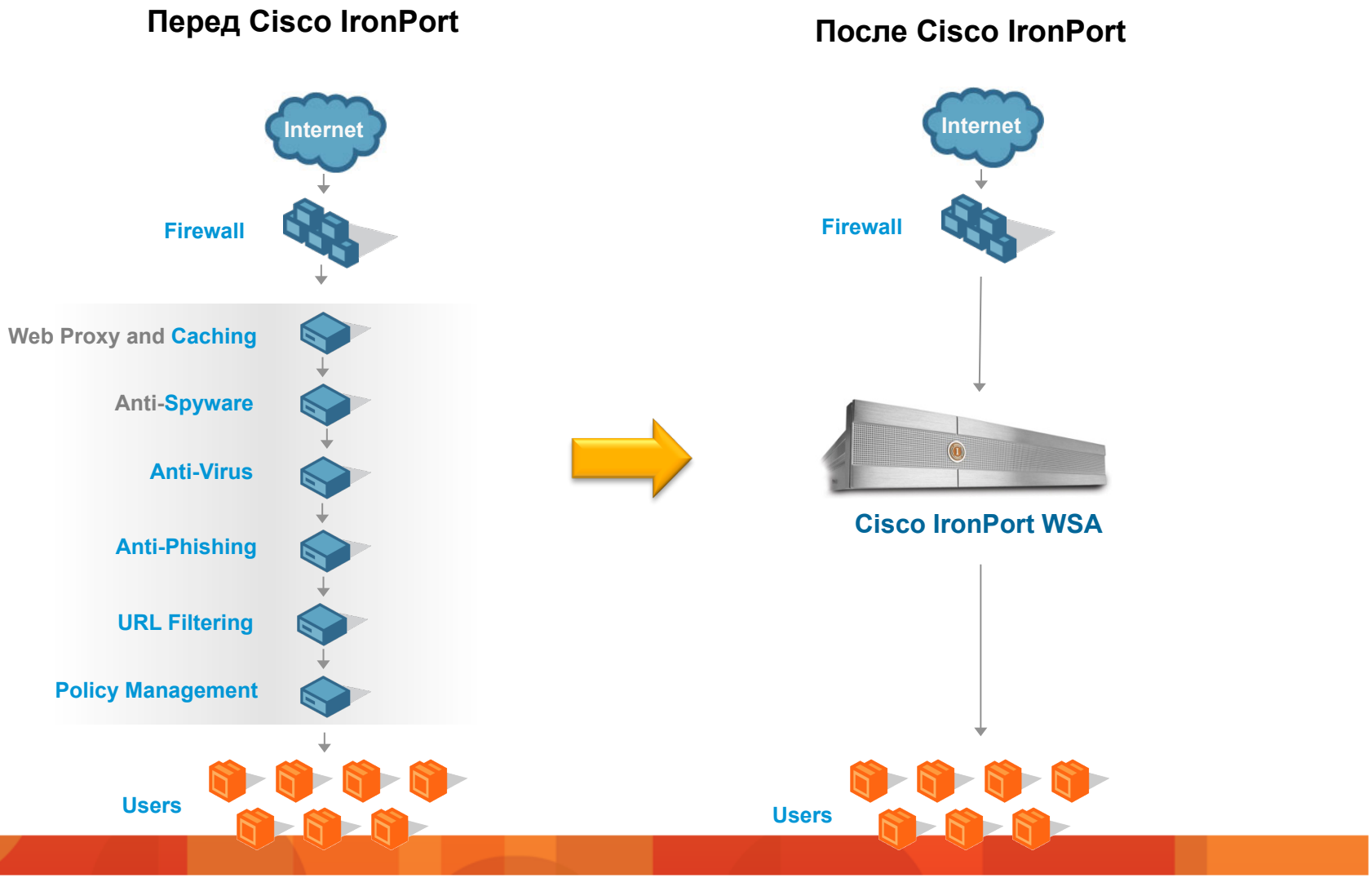
Cisco IronPort Secure Web Gateway

Решение бизнес-проблем



Шлюз Web-безопасности следующего поколения

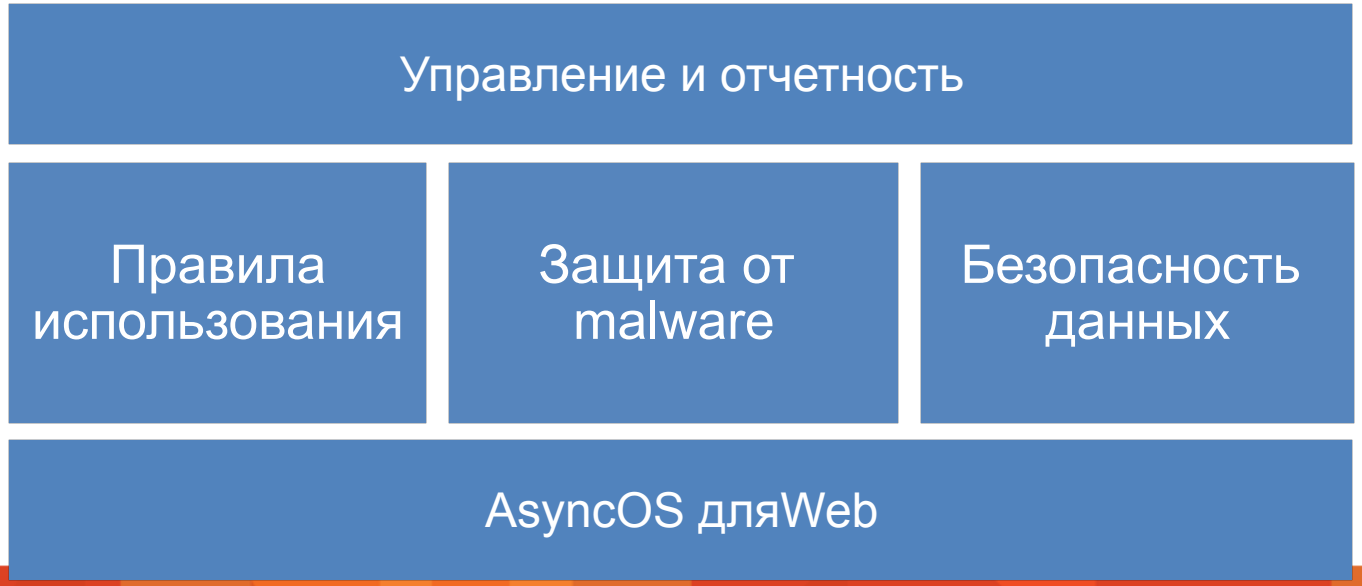
Обьединение увеличивает эффективность работы



Cisco IronPort Web Security Appliance

Мощное, безопасное решение Web-шлюза

- Наиболее эффективная защита от Web-malware
- Просмотр и управление системами использования Web и DLP
- Высокая производительность для гарантии прозрачности
- Интегрированное решение предлоагает оптимальное TCO



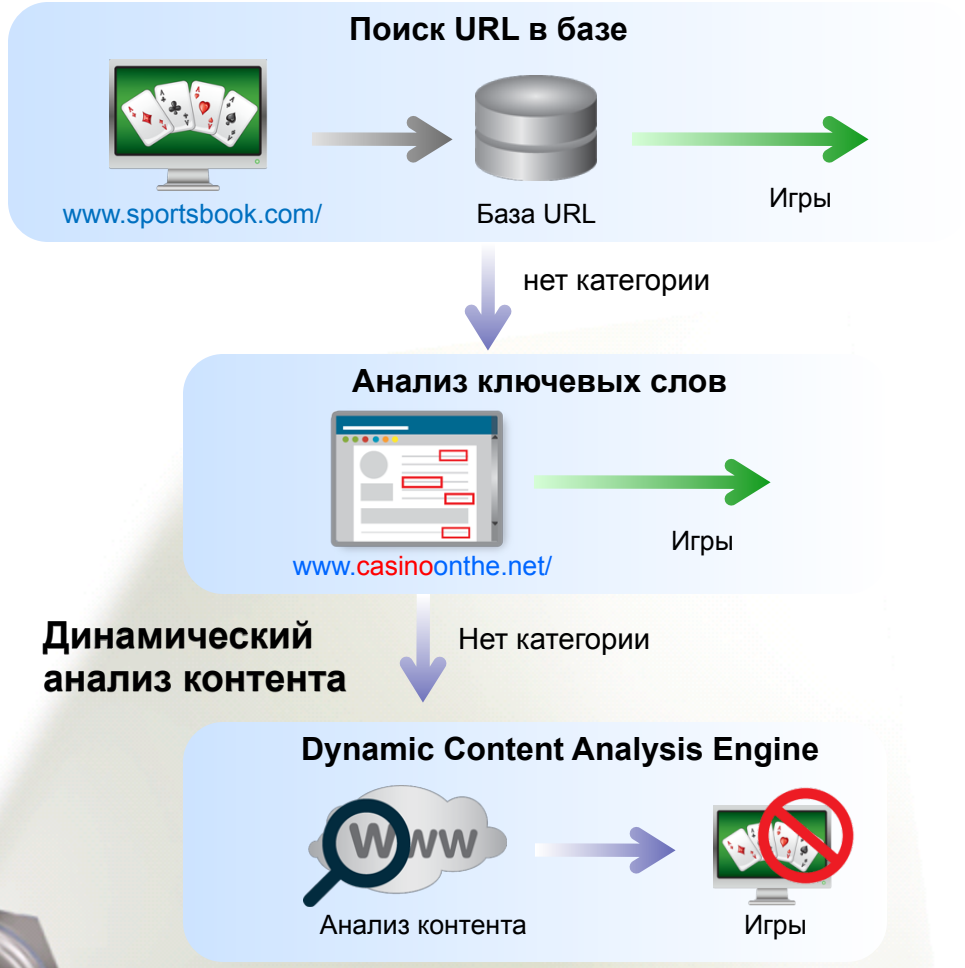
Правила использования

Просмотр и управление Web-трафиком и Web-приложениями

- URL фильтрация
- Фильтрация объектов и приложений
- Интегрированная идентификация и авторизация

Представляем технологию Cisco IronPort Web Usage Controls

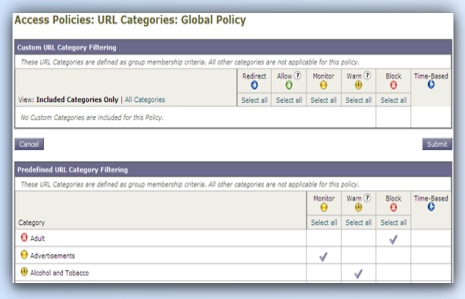
Луч света в темном Web

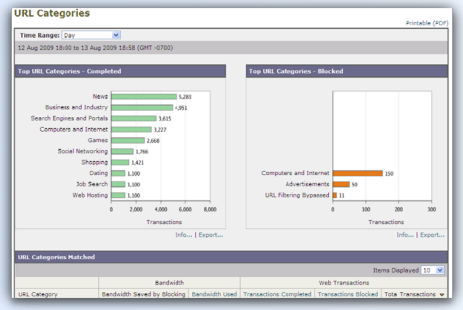


- Одна из самых эффективных баз URL
  - 65 категорий
  - Обновления каждые 5 минут
  - Использует Cisco SIO
- Динамический анализ контента позволяет определить 90% of «темного» Web

Cisco IronPort Web Usage Controls

Эффективность, управление, **обзор**





Управление

- Политики на пользователя/группу
- Набор действий: block,warn,monitor
- Политики по времени
- Пользовательские категории
- Пользовательские уведомления

Обзор

- Простые для понимания отчеты
- Всестороннее журналирование
- Полные предупреждения

Эффективность

- 200+ стран
- 50+ языков
- 65 категорий
- Низкий уровень ложных срабатываний

Контроль Web приложений

- Управление приложениями HTTP, HTTPS, Native FTP
- Избирательная расшифровка трафика HTTPS
- Политики для приложений, туннелирующихся через HTTP – IM, FTP
- Приложения, которые используют HTTP CONNECT

Контроль web-приложений

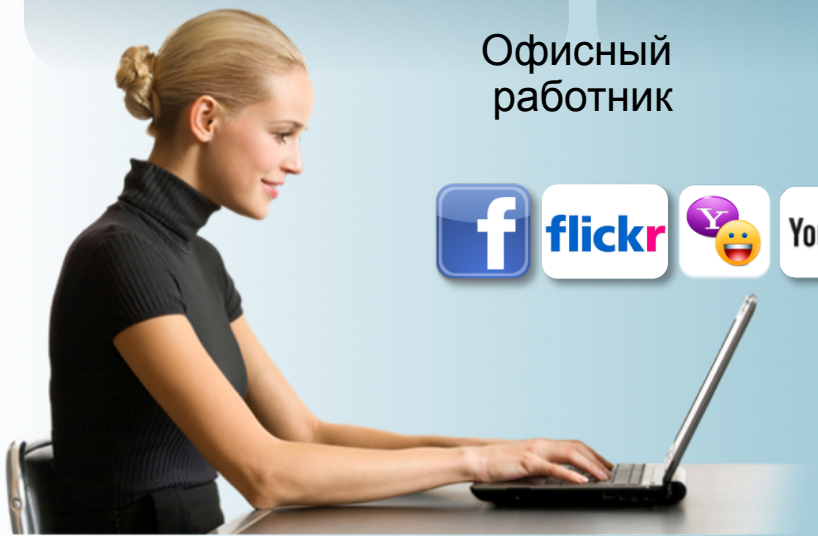
Access Control Policy

Instant Messaging
Facebook: приложения
Видео: 512 kbps макс

Access Control Violation

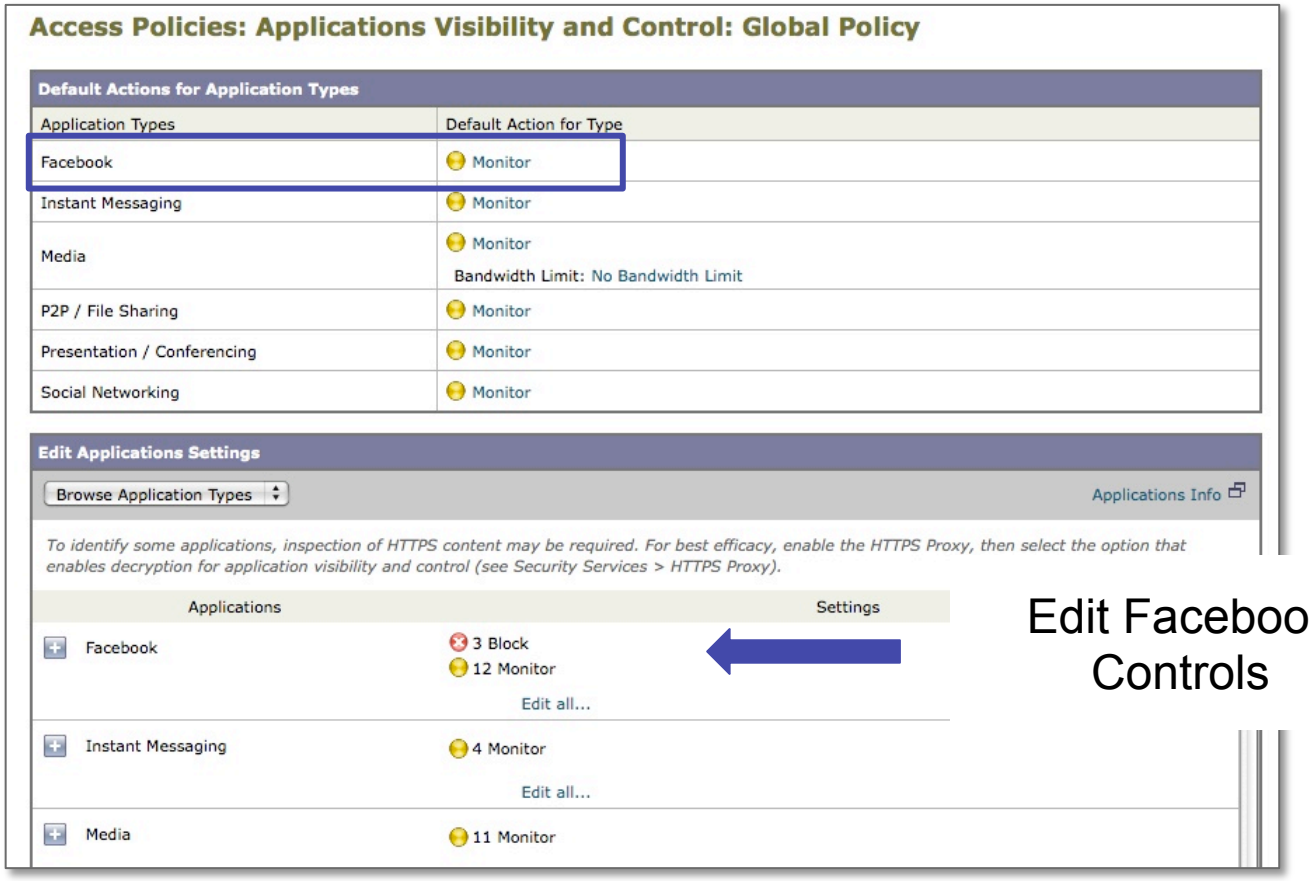
File Transfer over IM
Facebook Chat, Email
P2P

- Точный контроль приложений HTTP, HTTP(s), FTP
- Динамические обновления сигнатур от Cisco SIO



Точный контроль над использованием Web

Новые приложения: Facebook



Edit Facebook Controls

Детальный контроль Facebook

- Chat
- Messages (Email)
- Events
- Notes
- Video
- Photos
- Places
- 3rd Party Applications

Детальный контроль приложений Facebook

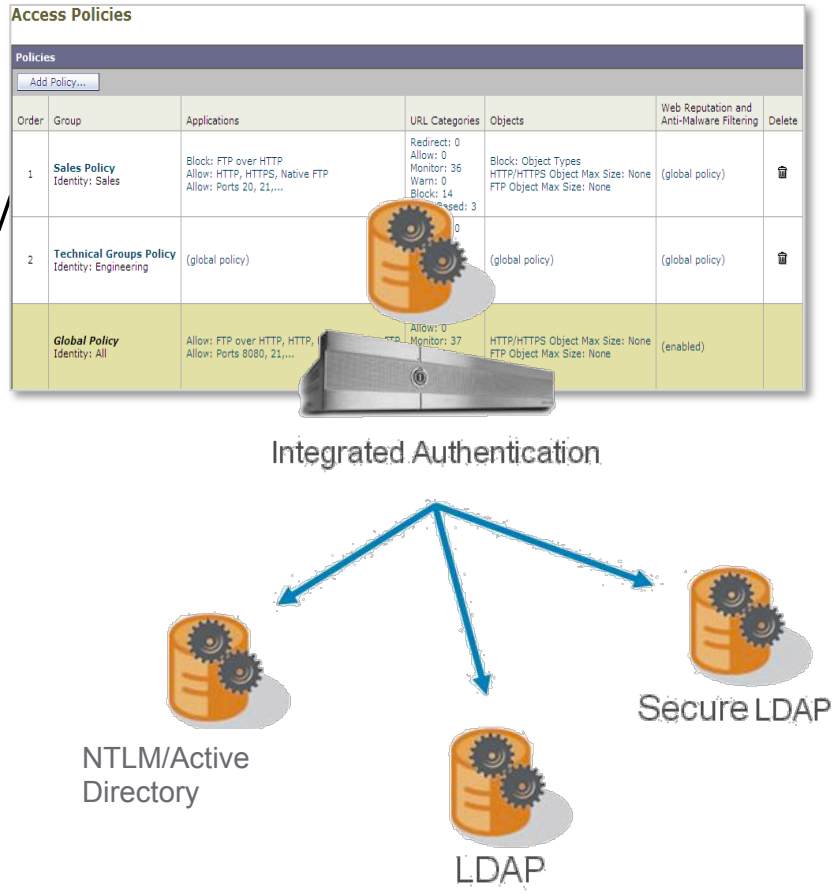
- Business
- Community
- Education
- Entertainment
- Games
- Sports
- Other
- Utilities

Control 75K+ Facebook Applications

Интегрированная идентификация и аутентификация

Правила использования и безопасность данных

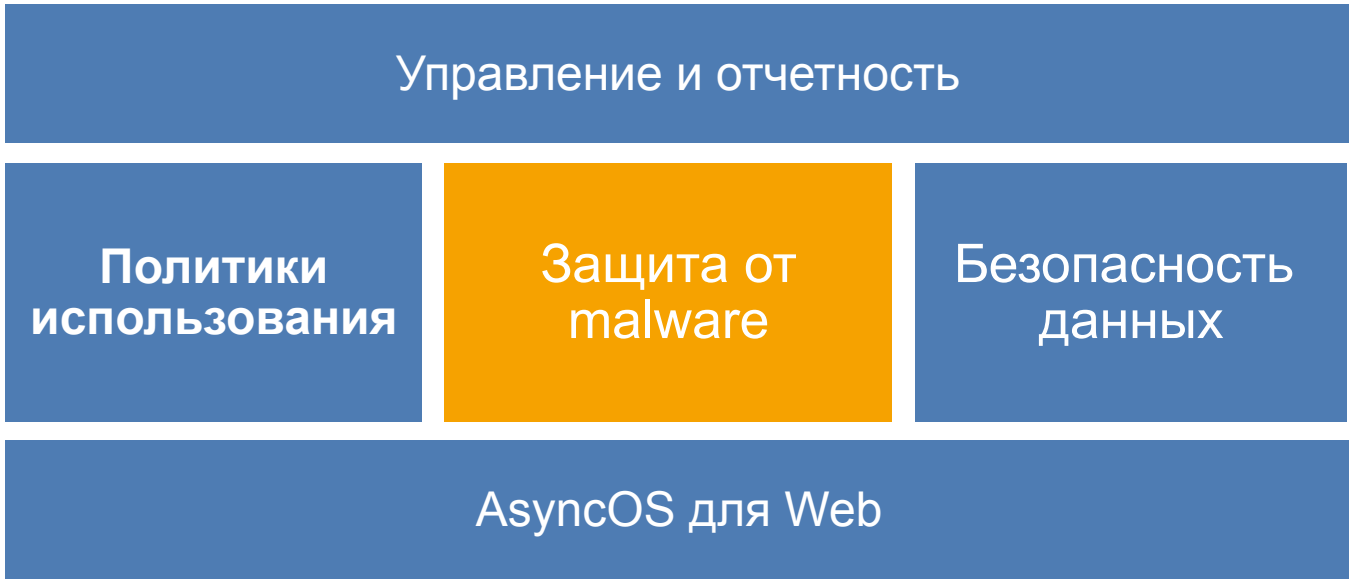
- Аутентификация на LDAP серверах
- Прозрачная, Single Sign On (SSO) аутентификация на NTLM
- Перебор нескольких областей LDAP
- Мультидоменная аутентификация LDAP
- Гостевые политики
- Политики повторной аутентификации и ошибок



Define Acceptable Use and Data Security Policies using Rich Identity Constructs

Правила использования

Просмотр и управление Web-трафиком и Web-приложениями



- URL фильтрация
- Фильтрация объектов и приложений
- Интегрированная идентификация и авторизация

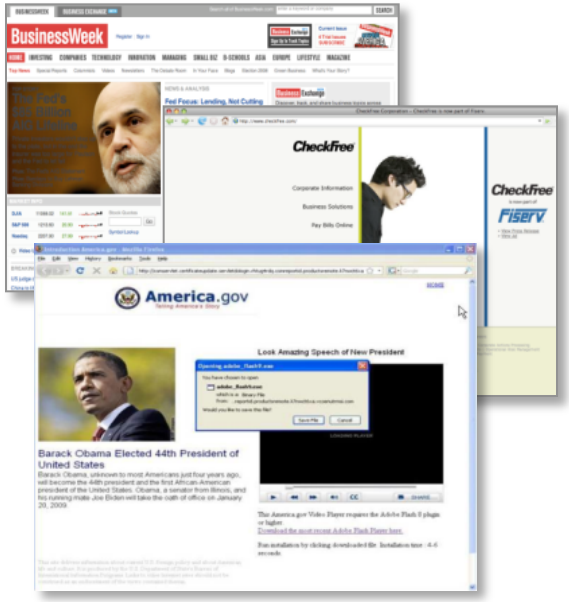
Многоуровневая защита от Malware

Защита от современных угроз

Layer 4 Traffic Monitor

Web Reputation Filters

Dynamic Vectoring and Streaming Engine

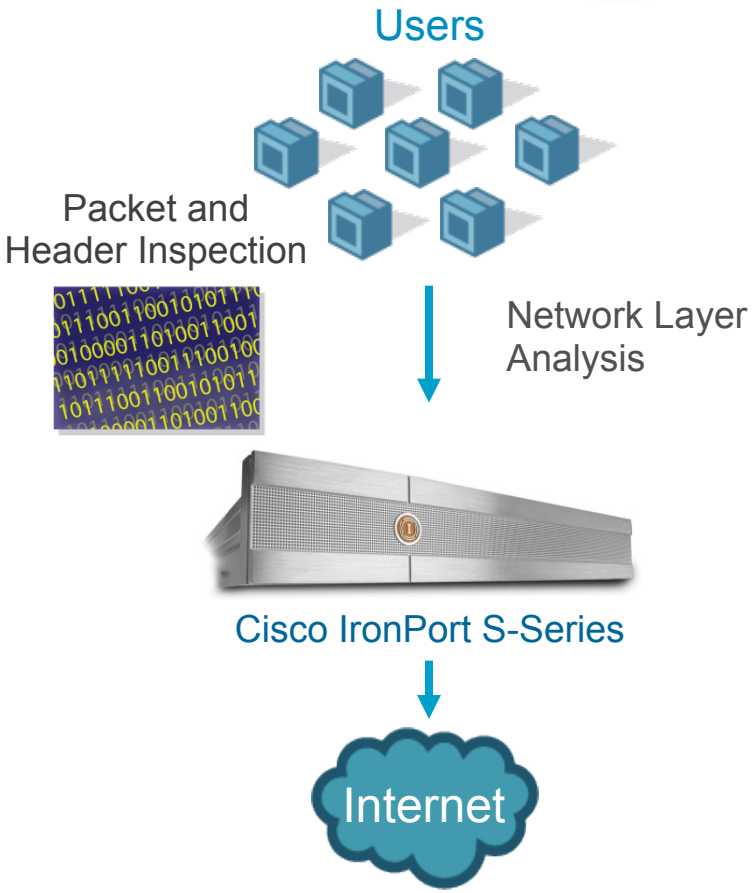


- Обнаруживает трафик ботнетов на всех портах
- Блокирует до 70% известного и неизвестного malware трафика на этапе соединения
- Блокирует malware на основе глубокого контентного анализа

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

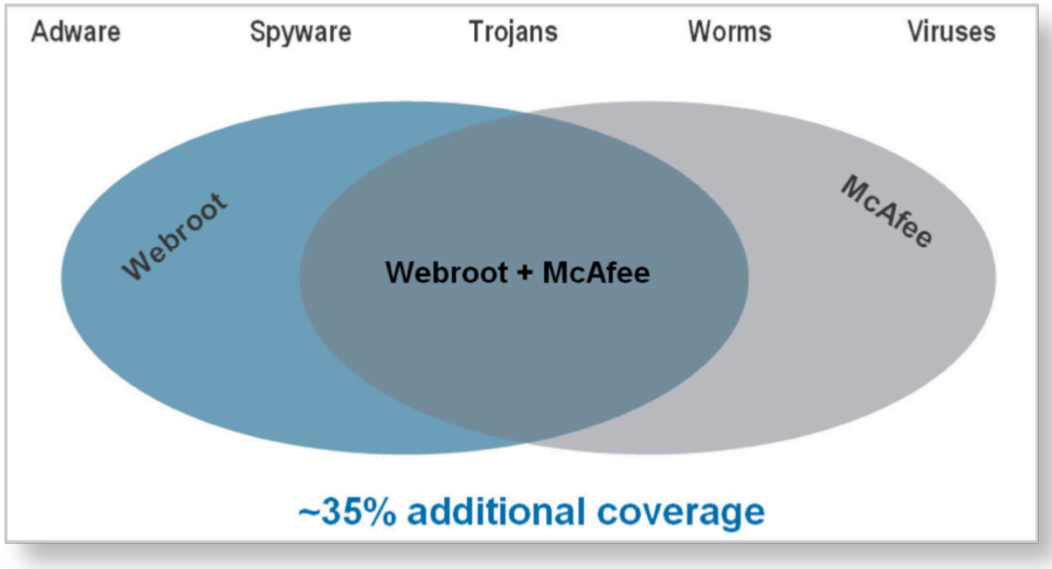
Security Modeling

Web Reputation Scores (WBRS) -10 to +10

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



Правила использования

Просмотр и управление Web-трафиком и Web-приложениями

- URL фильтрация
- Фильтрация объектов и приложений
- Интегрированная идентификация и авторизация

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

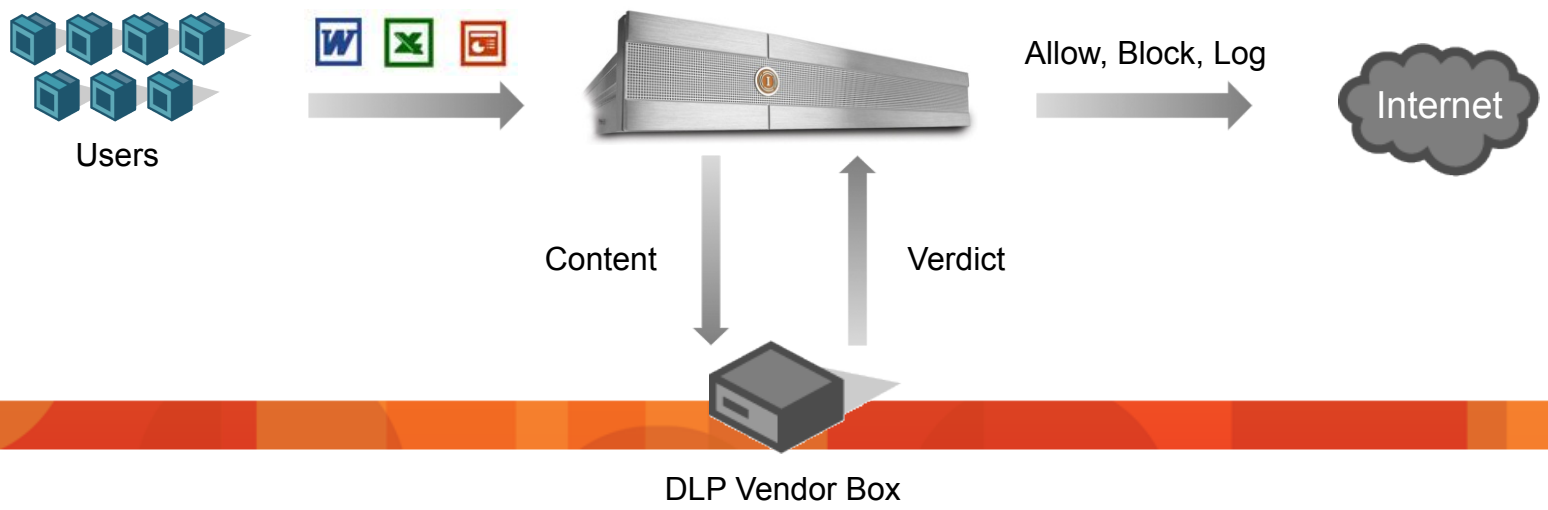
Политики «здравого смысла»

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	✗	✓	✗

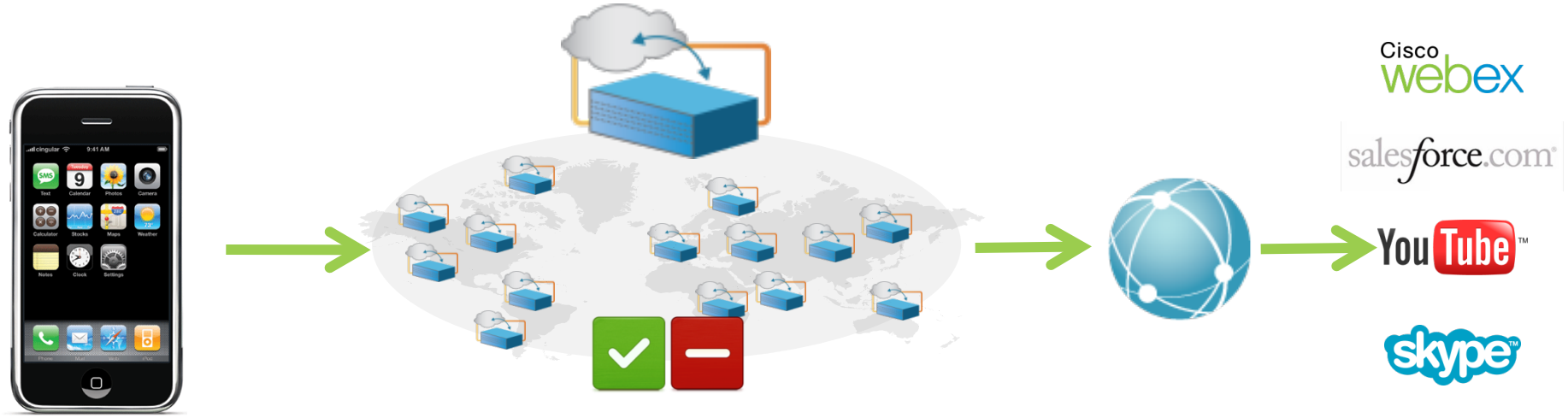
Безопасность данных
Расширенная безопасность off-box

- Прозрачная интеграция
- Глубокая проверка контента
  - Структурированное и неструктурированное соответствие
- Оптимизация производительности
  - Работает в тандеме со встроенной системой безопасности данных



Mobile User Security

Безопасный доступ в любое время из любой точки



Cisco Security Enforcement Array (SEA)

1 Cisco Connection Manager

Always-on, location-aware, extremely lightweight, invisible to user

Supported on all major devices and OS

2 Powerful Enforcement Engines

High Performance

Application and Identity Aware

Hybrid Hosted Delivery

3 Политика

Abstracted from enforcement layer

Acceptable Use, Access Control, Data Security, Anti-Malware

Mobile User Security

Безопасный доступ к Web в Borderless Network

- Предоставляется как объединенное решение продуктов безопасности Cisco

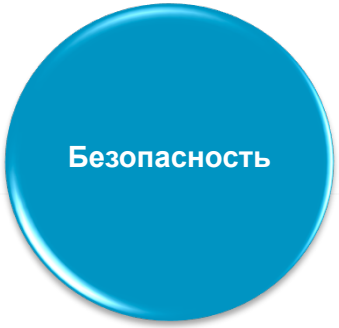
  S-Series, ASA, и AnyConnect

- Мобильным пользователям доступна полная функциональность WSA
- Управление политиками и отчетность на WSA может разделять мобильных и локальных пользователей
- Single sign-on с AnyConnect на WSA
- Широкий набор клиентских программ
- Пока требует перенаправления всего Web трафика с клиентского устройтсва на WSA

  но в будущем…

Cisco Secure Web Gateway

Самое высокопроизводительное решение в индустрии

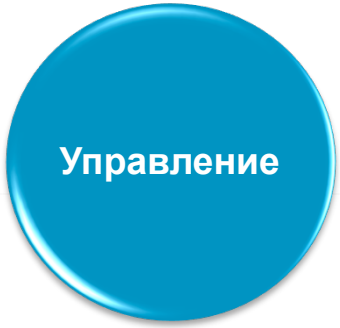


Многоуровневая защита от malware

Фильтры Web-репутации

Ускоренное сканирование сигнатур(механизм DVS)

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

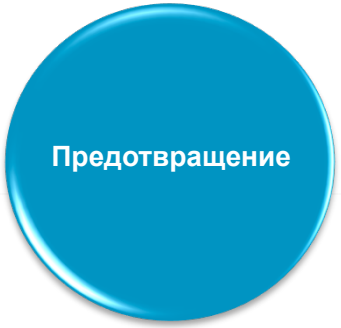


Интегрированная аутентификация и SSO

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)

Right-Sized Hardware Platforms

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

Управление безопасностью Web

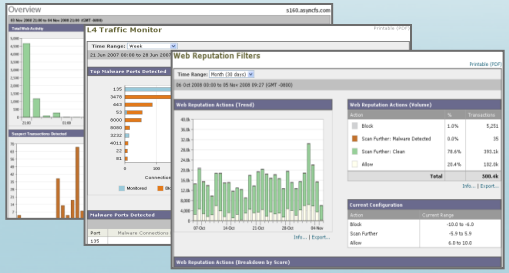
Security Management Appliance (M-серия)

Централизованное управление

Централизованное управление политиками

Делегированное администрирование

Централизованный репортинг



Глубокий просмотр угроз

Широкие возможности по расследованию

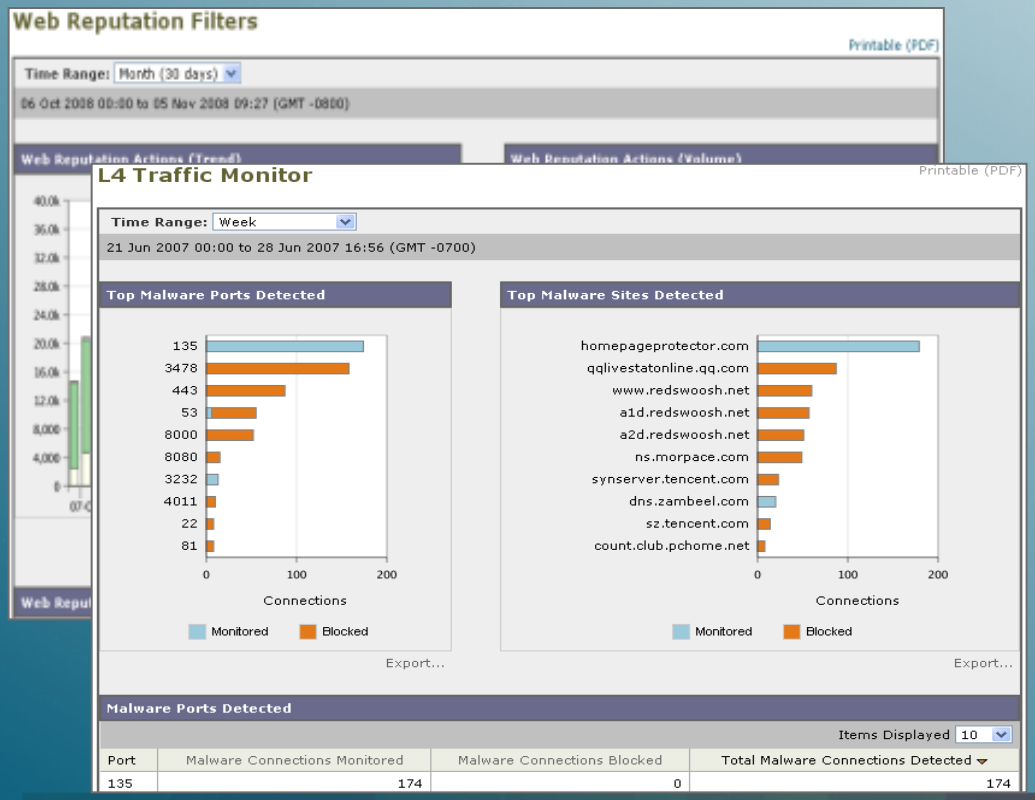
Просмотр
Приложений, угроз и пользователей

Управление
Общие политики между разными подразделениями и удаленными пользователями

Обзор
Разные устройства, сервисы, сетевые услуги

Точные метрики для управления

- WSA: Локальные отчеты
- SMA: Централизованные отчеты (полученные с WSA)



Понимание тенденций

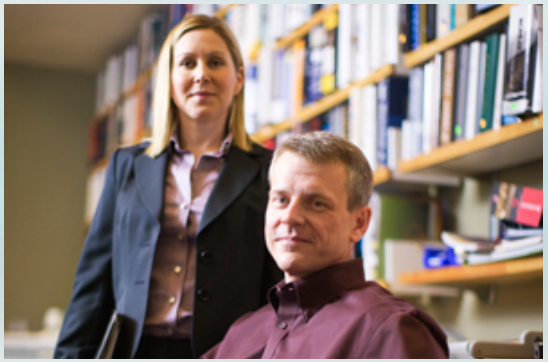
Измерить производительность

Анализ угроз

План на будущее

Отчеты для разных целевых горупп

HR и юристы



- Расследования
- Измерения
- Производительность
- Применение политик

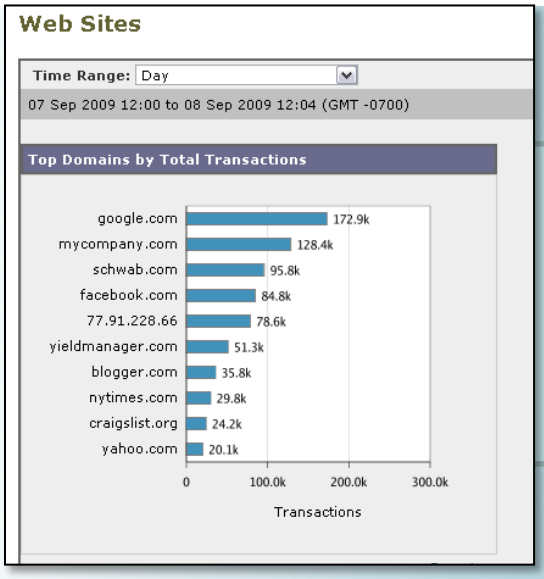
Безопасность

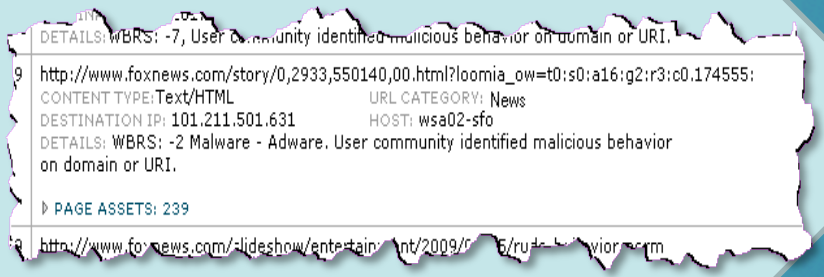
- Анализ угроз
- Расследования
- Управление политиками безопасности

Network Operations

- Управление полосой пропускания
- Планирование мощностей

Иерархия от высокоуровневых отчетов до отдельных транзакций





Высокий уровень:

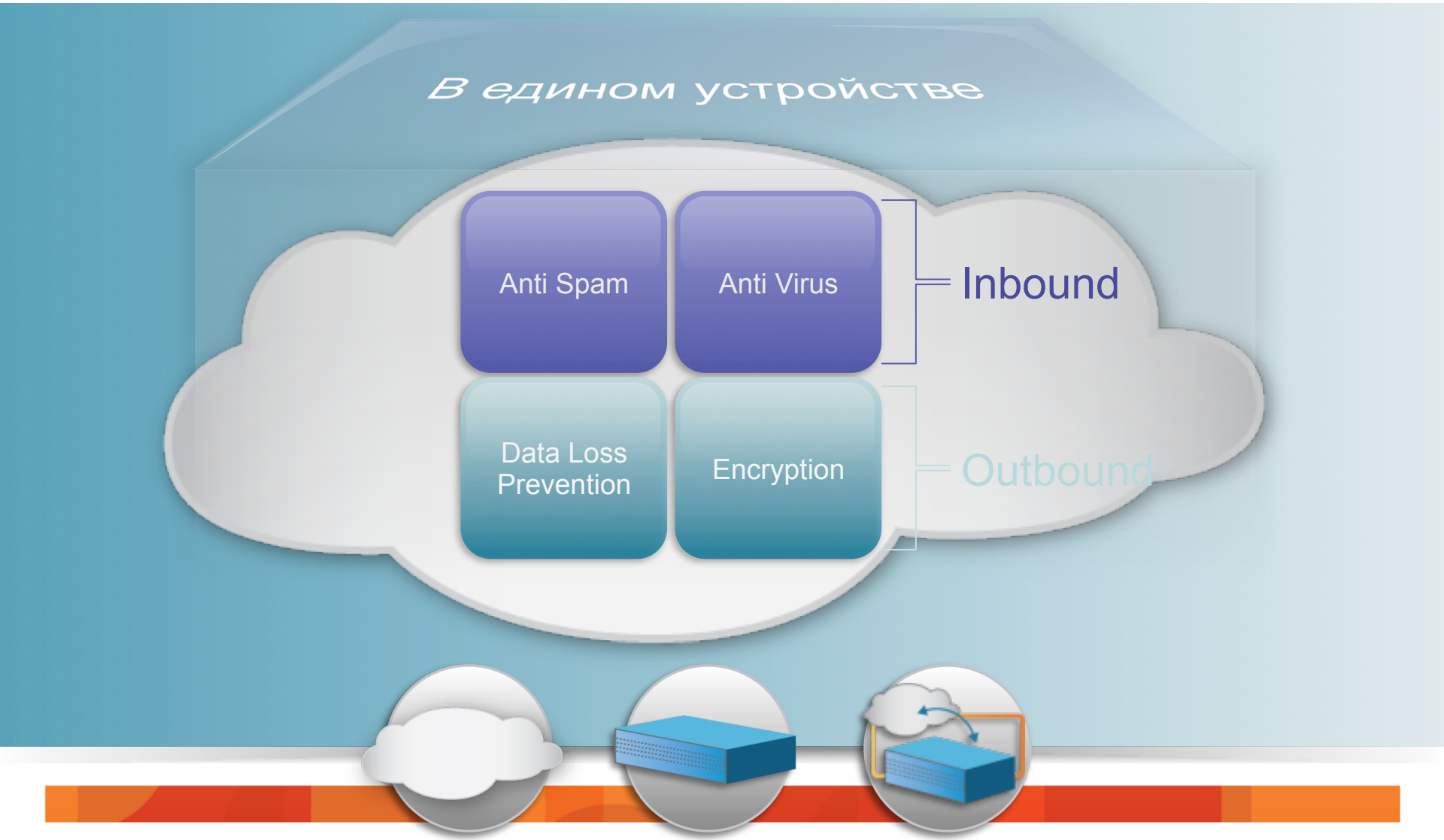
- Приложения
- Узлы
- Пользователи
- Категории

Детальные:

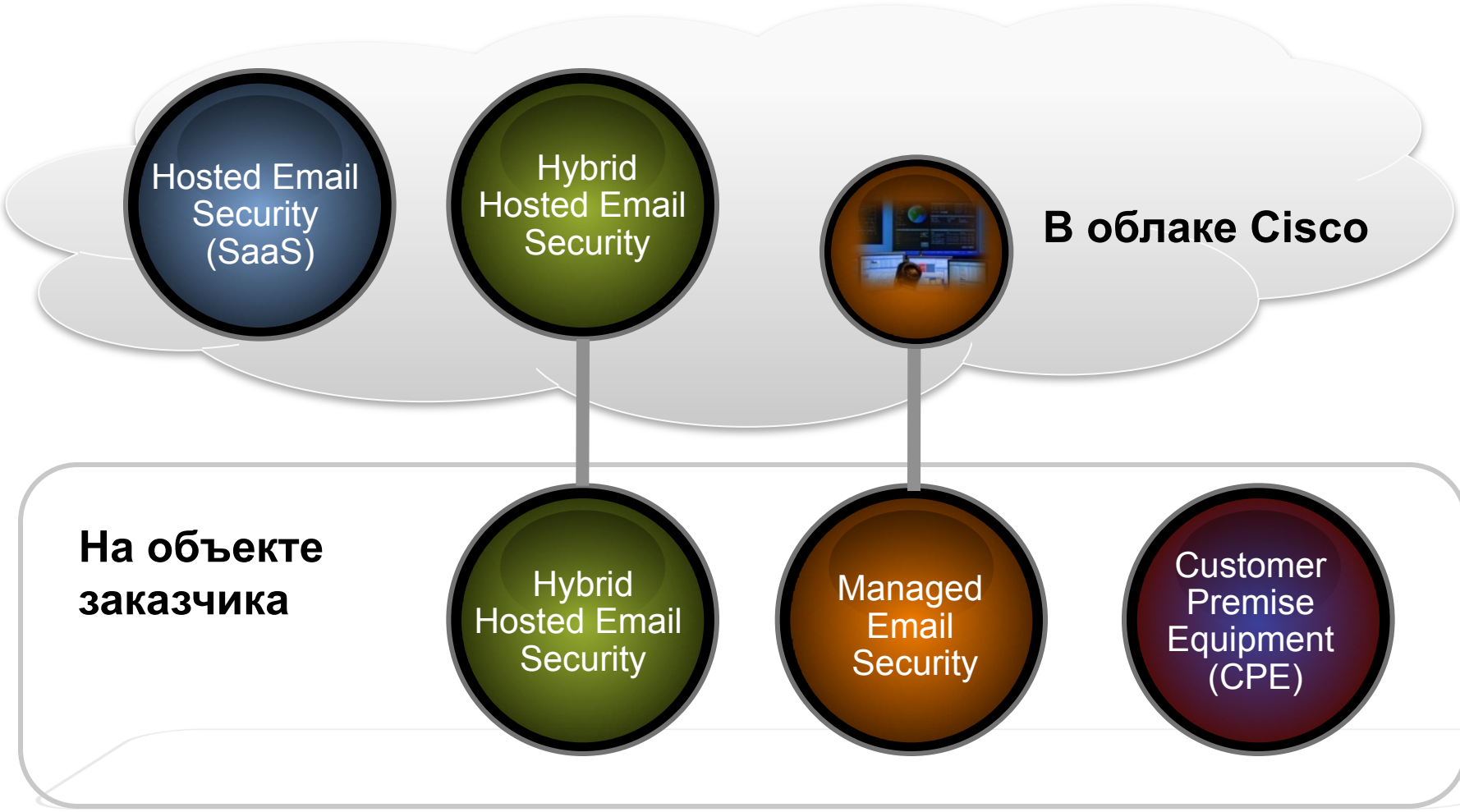
- Детальная информация о каждой транзакции

Cisco Cloud Email

Архитектура решения IronPort ESA



Форматы размещения



Единые политики | Централизованное управление | Единообразная защита

Hosted Email Security

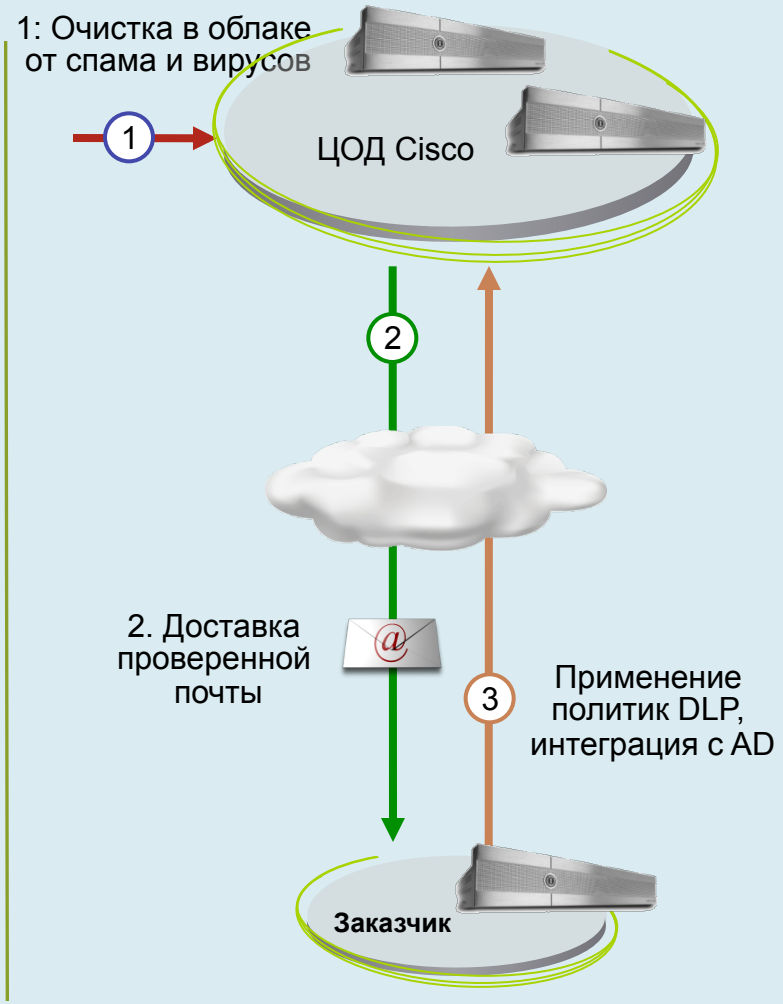
Преимущества размещения в облаке Cisco:

- Быстрое развертывание
- Снижение нагрузки по обслуживанию
- Размещение, масштабирование, отказоустойчивость – наши заботы

Hybrid Hosted Email Security

Лучшее из обоих миров

- Очистка входящей почты – в облаке Cisco
- Обработка исходящей почты, в т.ч. и DLP – у заказчика
- Конфиденциальная информация не покидает сети заказчика
- Единый интерфейс мониторинга



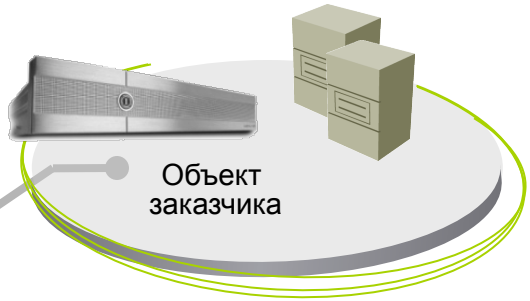
Co-Managed

Мы администрируем, Вы контролируете

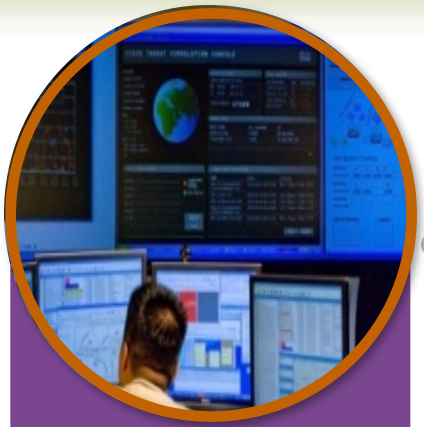
Заказчик

Отслеживание сообщений | Кейсы | Отчеты

Отчеты

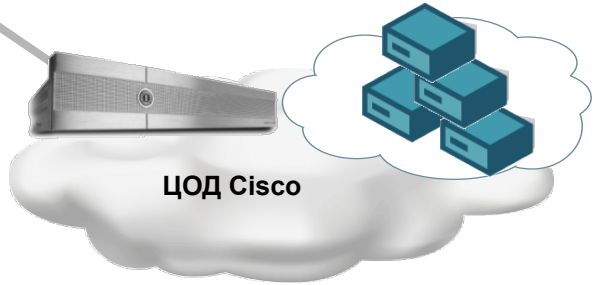


Разделяемый доступ



Cisco

Обслуживание



Мониторинг работоспособности | Обновления | Настройки

ScanSafe Web Security

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 Europe 2009 RDS 08 07

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

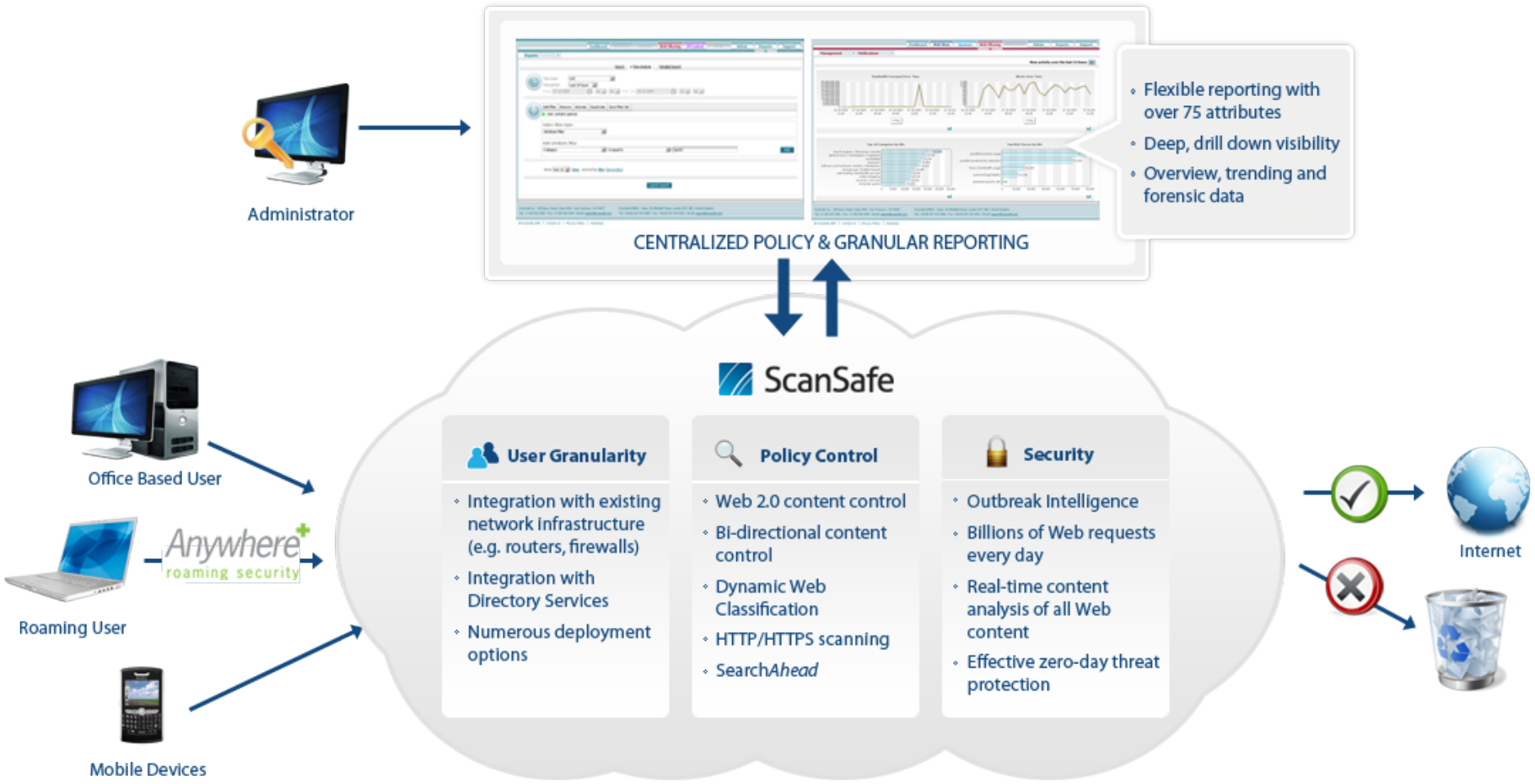
Google

Sprint

TELUS

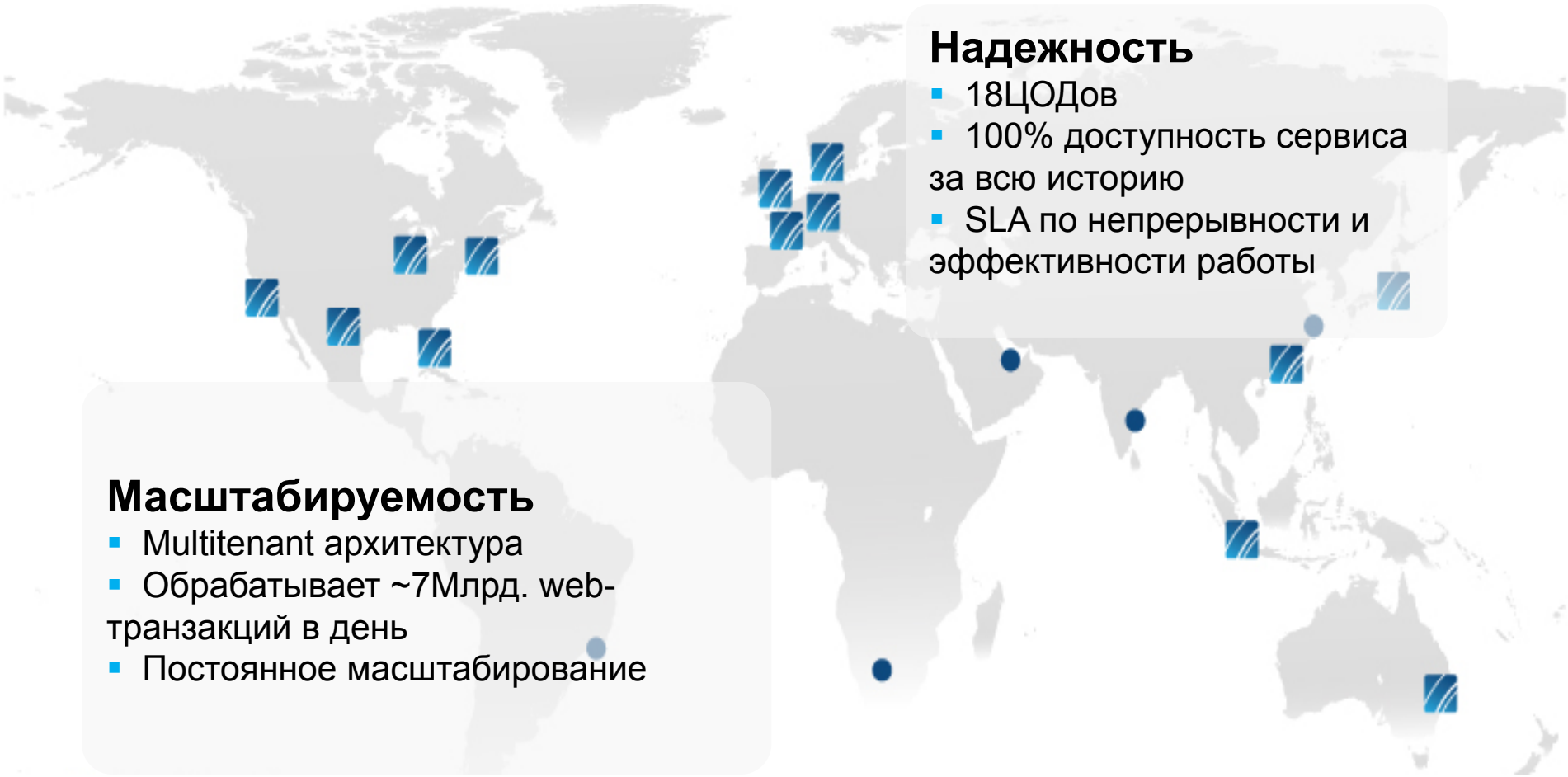
NEC

Обзор решения



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

ЦОДы Cisco ScanSafe



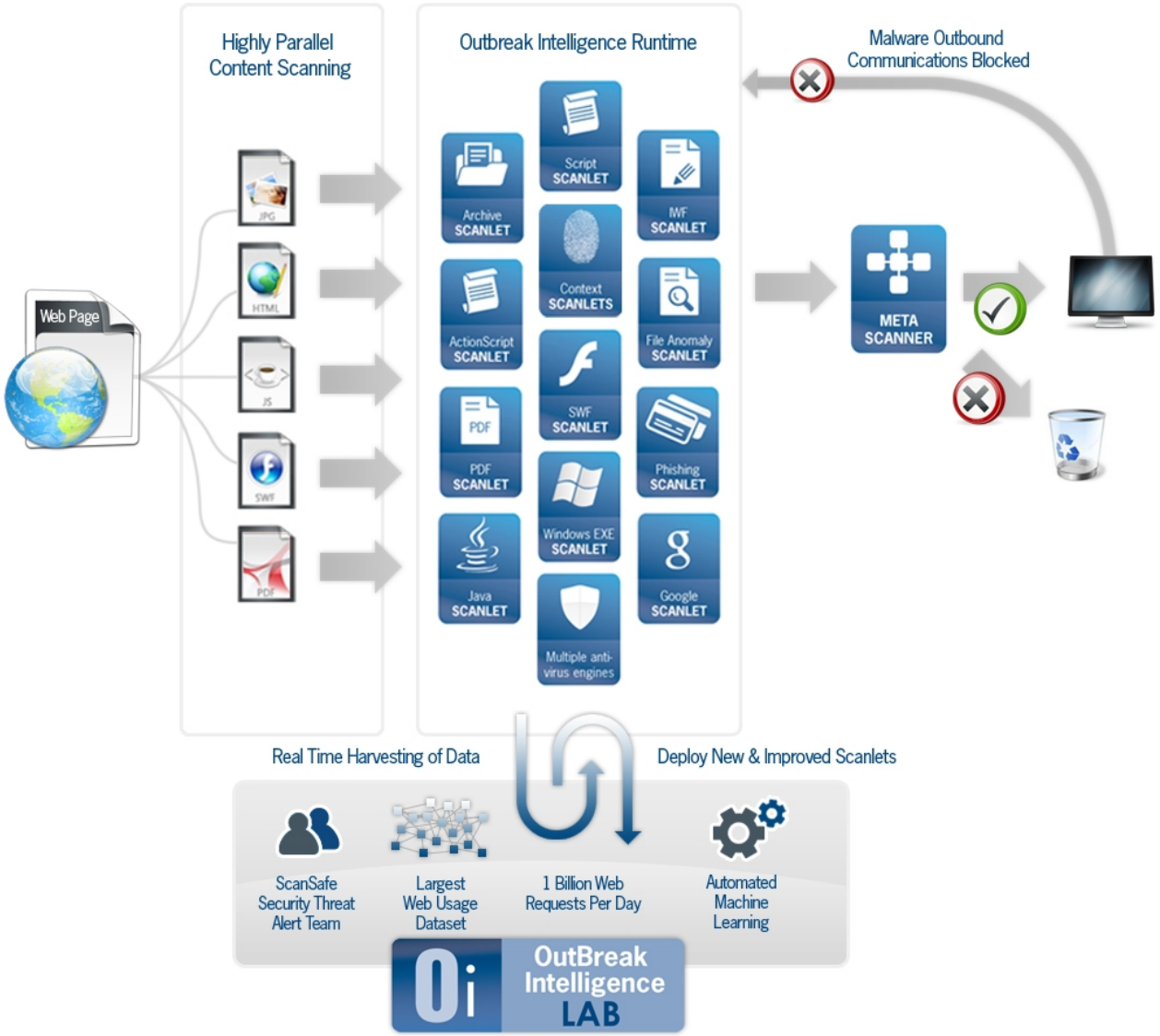
Надежность

- 18ЦОДов
- 100% доступность сервиса за всю историю
- SLA по непрерывности и эффективности работы

Масштабируемость

- Multitenant архитектура
- Обрабатывает ~7Млрд. web-транзакций в день
- Постоянное масштабирование

Архитектура защиты от Web-угроз



- Статистика за 2009г.:
  - 28M уникальных JavaScript в день
  - 560K уникальных PDF в день
  - 244 уникальных ShockWave в день
- 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:

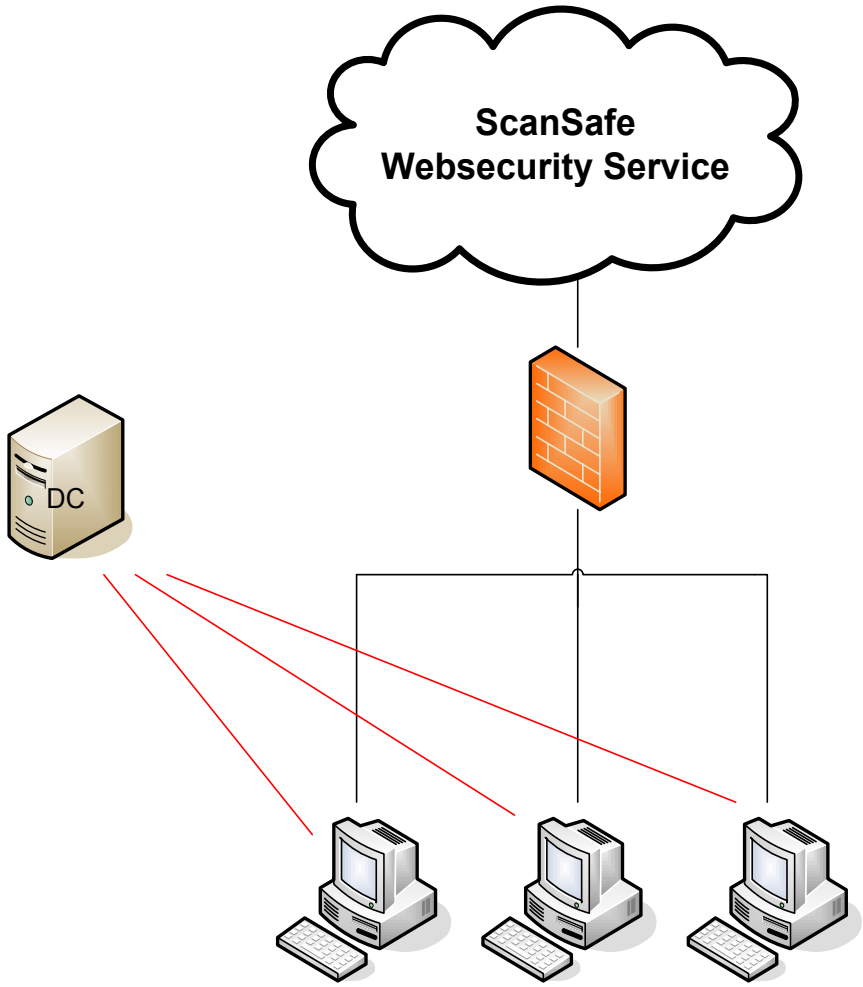
- Настройки Proxy загружаются на компьютеры из AD (GPO / PAC file) или по DHCP
- МСЭ блокирует исходящий HTTP трафик на все адреса кроме ScanSafe

Без изменения настроек браузера:

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

Опционально – User/Group Granularity:

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

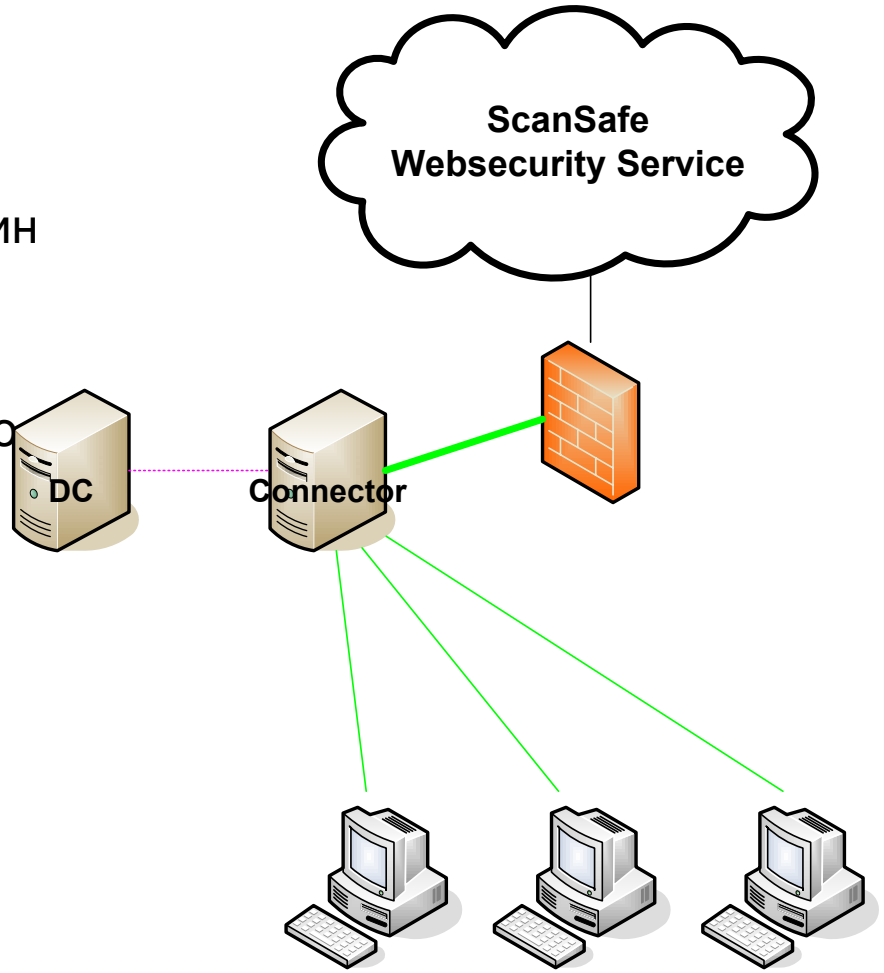


Как трафик попадает в облако

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



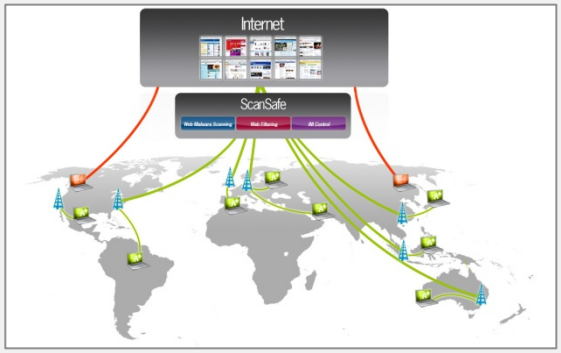
Как трафик попадает в облако

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

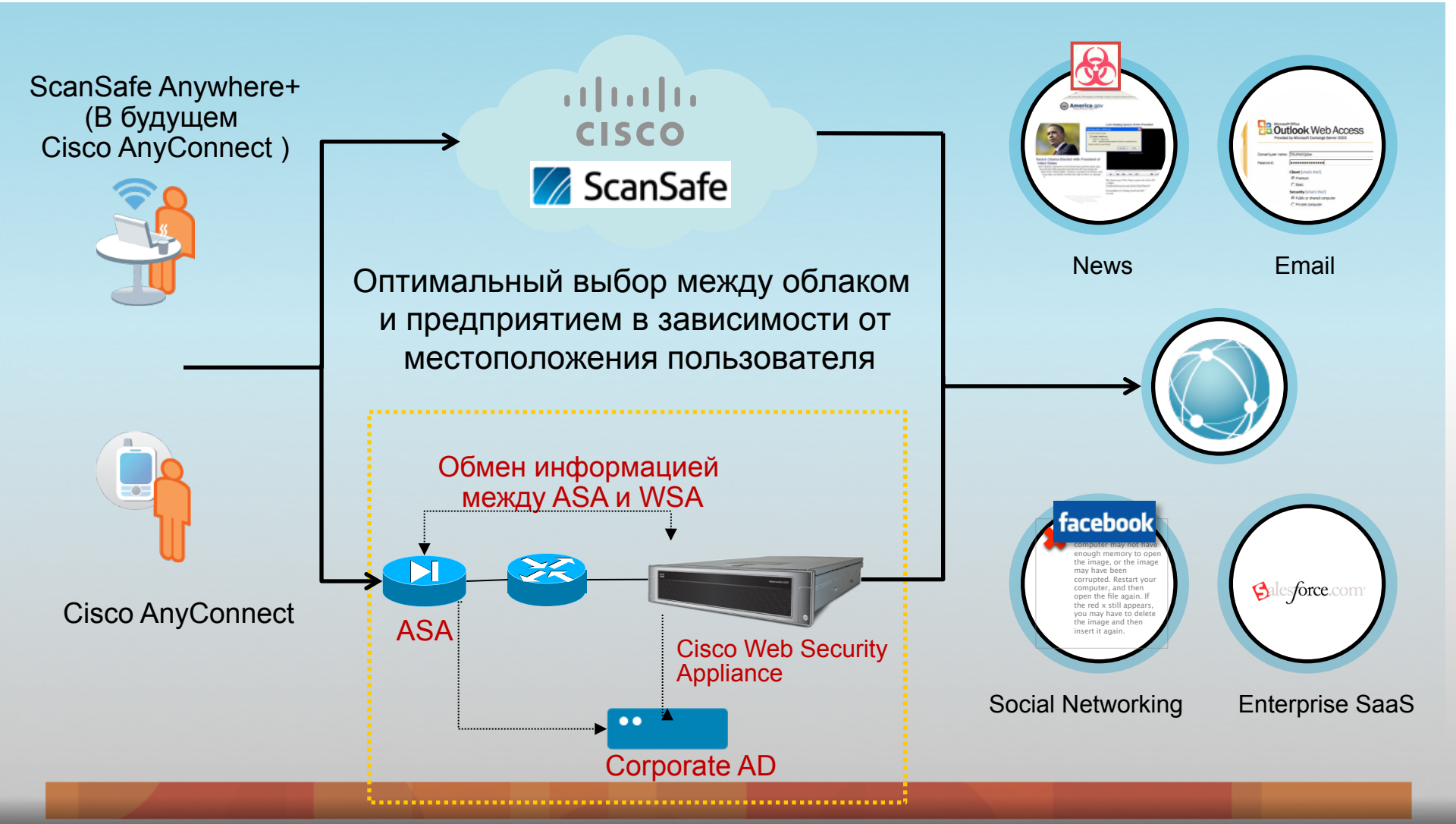
Факт: Мобильные пользователи только 17% времени в Интернет проводят в корпоративном VPN. Как контролировать оставшиеся 83%?



Anytime. Anyplace. Anywhere+

Защита мобильных пользователей

Автоматический выбор: в облаке или на предприятии



ISR G2 + ScanSafe: Функционал

- Коннектор уже доступен на IOS .
- Поддерживается на платформах 880, 890, 19XX, 29XX и 39XX/E ISR G2.
- Перенаправление HTTP/HTTPS трафика.
- Не требуется дополнительного агентского ПО, установленного на рабочие станции пользователей.

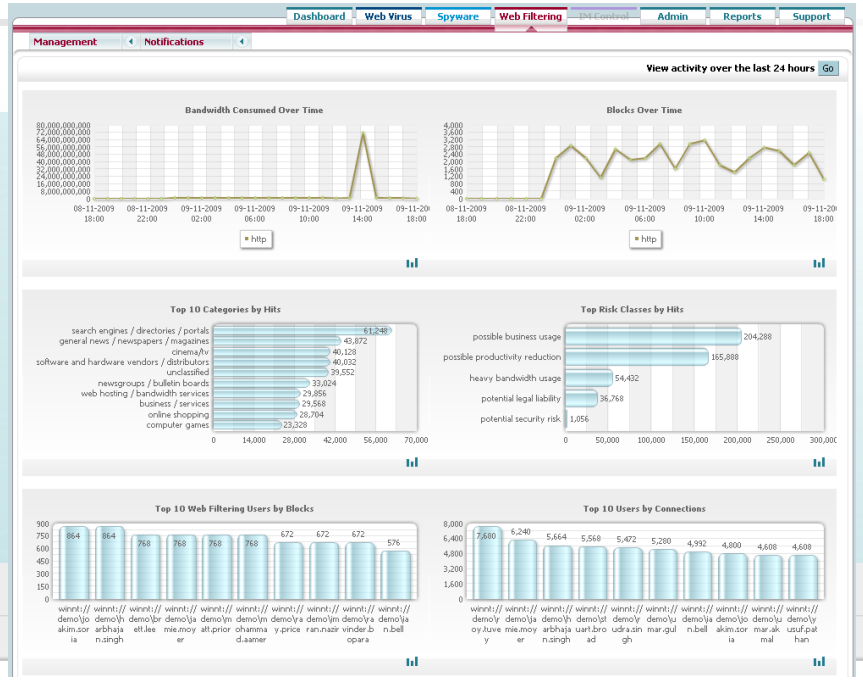
ISR G2 + ScanSafe: Functionality

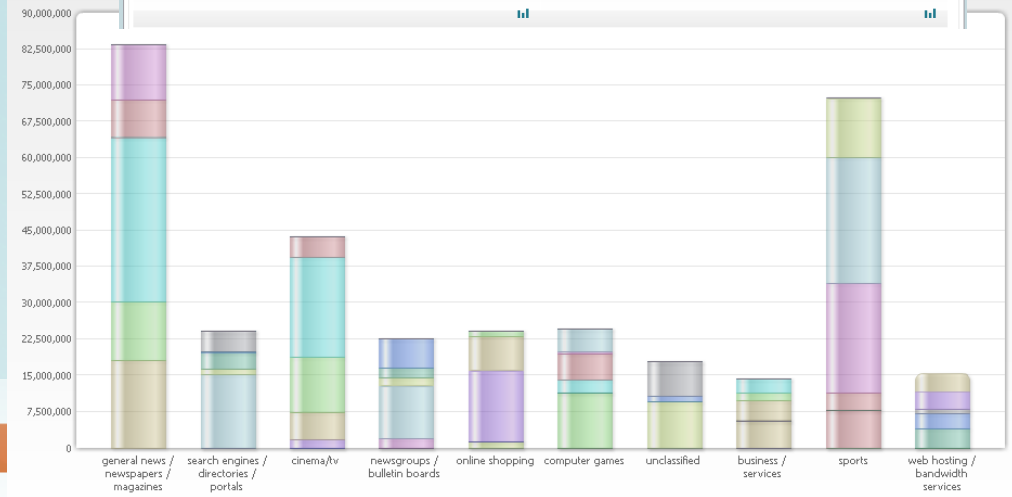
- Установки HTTP прокси не меняются.
- Идентификация Single Sign On с помощью LDAP и AD синхронизации.
- Пользователи настраиваются на ScanCenter Web Portal. Отчеты (Доступ по пользователям, группам и т.д. …)
- ISR работает независимо от других сервисов безопасности (IOS FW, IPS, VPN)

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





Сервисы ScanSafe

Делаем	Не делаем
Управляем HTTP, HTTPS, FTP over HTTP Web фильтрация Фильтрация контента Сканирование Web malware Отчеты об использовании Защита мобильных пользователей	Не-HTTP/s трафик P2P IDS/IPS Маршрутизатор/МЭ Отчеты об общей полосе пропускания QoS для всего трафика VPN Оптимизация WAN

Условия

- Полнофункциональный пробный доступ на 30 дней
- Небольшой одноразовый платеж за включение услуги
- Несколько $ за одно рабочее место в месяц (зависит от общего числа рабочих мест в организации)

CISCO IRONPORT
СХЕМА ЛИЦЕНЗИРОВАНИЯ

Pavel Rodionov
Systems Engineer
prodiono@cisco.com

Лицензии Email

- Анти-Спам
- Анти-вирус
  - Sophos
  - McAfee
- Virus Outbreak Filters
- RSA Data Loss Prevention
- Intelligent Multiscan
- Image Analizer

Репутационная фильтрация и остальной функционал включен в базовую поставку

Лицензии выдаются на количество пользователей и ограничены по времени (1 год, 3 года, 5 лет)

Лицензии Web

- Web Reputiation Filters (репутационных фильтров в базовой поставке нет!)
- Anti-Malware
  - Sophos
  - McAfee
  - Webroot
- Web Usage Controls (URL фильтрация и Application Visibility)
- AnyConnect Secure Mobility (Бесплатно!)
- ~~IronPort URL Filters~~

Лицензии выдаются на количество пользователей и ограничены по времени (1 год, 3 года, 5 лет)

Лицензии на устройстве - Web

Feature Keys

Feature Keys for Serial Number: 00188B453402-JRK67C1

Description	Status	Time Remaining	Expiration Date
IronPort L4 Traffic Monitor	Active	Perpetual	N/A
IronPort HTTPS Proxy	Active	Perpetual	N/A
Cisco IronPort Web Usage Controls	Active	63 days	Tue Apr 12 01:12:04 2011
Sophos	Active	63 days	Tue Apr 12 06:12:03 2011
McAfee	Active	63 days	Tue Apr 12 01:12:04 2011
Webroot	Active	63 days	Tue Apr 12 01:12:04 2011
IronPort Web Proxy & DVS™ Engine	Active	Perpetual	N/A
Cisco Mobile User Security	Active	63 days	Tue Apr 12 06:12:03 2011
IronPort Web Reputation Filters	Active	63 days	Tue Apr 12 01:12:04 2011

Pending Activation

No feature key activations are pending.

Check for New Keys

Feature Activation

Feature Key:

Submit Key

Лицензии на устройстве - Email

Feature Keys

Feature Keys for Serial Number: 001D09F07B0B-2FMT8F1

Description	Status	Time Remaining	Expiration Date
RSA Email Data Loss Prevention	Active	49 days	29 Mar 13:44 (GMT)
Bounce Verification	Active	Perpetual	N/A
IronPort Email Encryption	Active	49 days	29 Mar 13:44 (GMT)
IronPort Anti-Spam	Active	49 days	29 Mar 13:44 (GMT)
Incoming Mail Handling	Active	Perpetual	N/A
Virus Outbreak Filters	Active	49 days	29 Mar 13:44 (GMT)
Sophos Anti-Virus	Active	49 days	29 Mar 13:44 (GMT)
McAfee	Active	816 days	04 May 16:15 (GMT)

Pending Activation

No feature key activations are pending.

Check for New Keys

Feature Activation

Feature Key:

Submit Key

95% of companies
who try Cisco IronPort
become customers.

Contact:
Your Cisco IronPort Rep

Cisco Expo 2011

Спасибо!

Просим Вас оценить эту лекцию.
Ваше мнение очень важно для нас.

Онлайн-анкеты: www.ceq.com.ua

innovate together