Cisco IronPort
Новые горизонты в обеспечении безопасности электронной почты

Pavel Rodionov

Systems Engineer

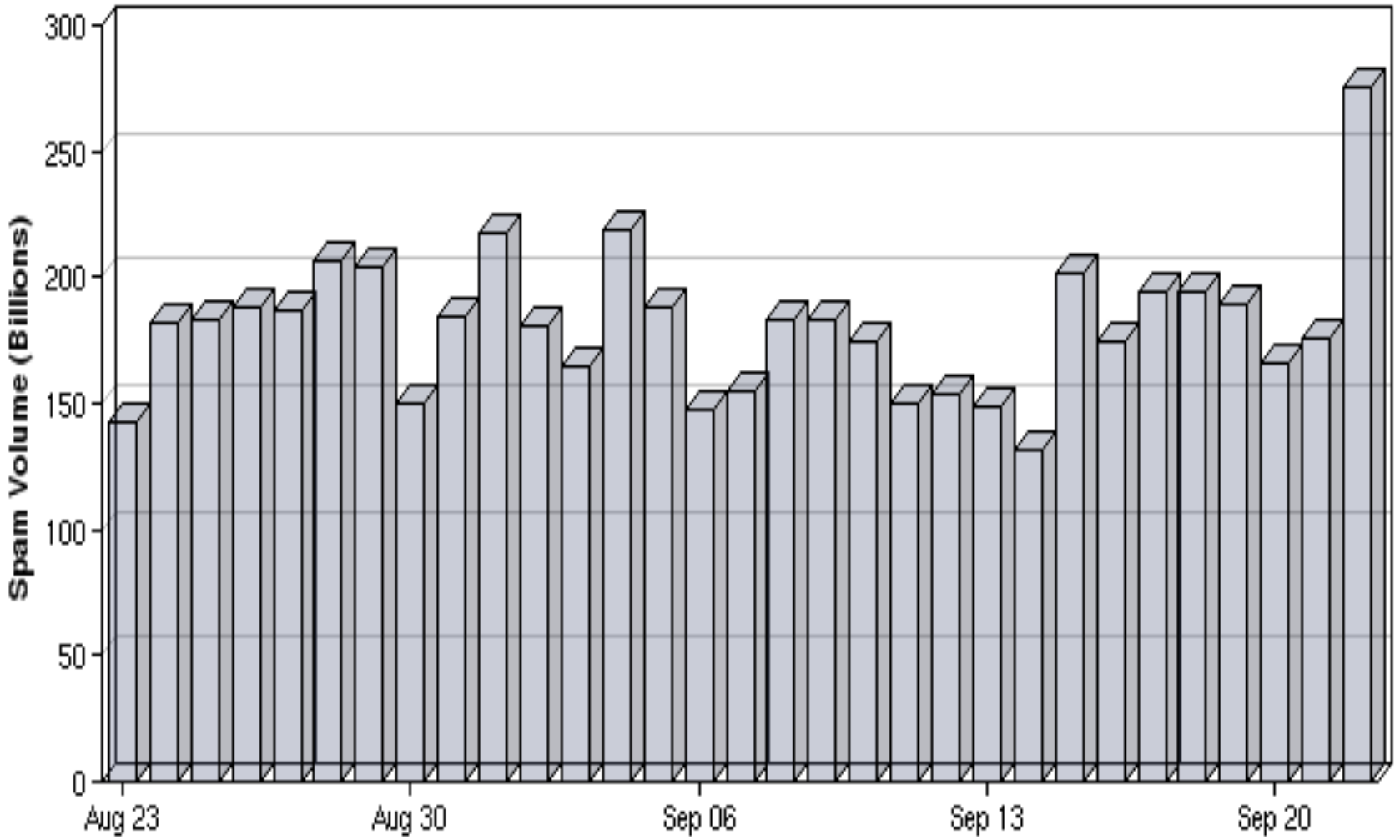
Security Technology BU

prodiono@cisco.com

© 2009 Cisco Systems, Inc. All rights reserved. Cisco Public

Email. Угроза безопасности

Больше спама, больше спамеров

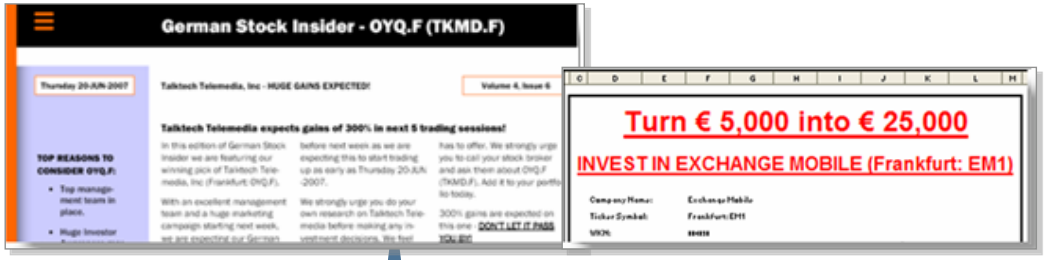


Source: Cisco Threat Operations Center

© 2009 Cisco Systems, Inc. All rights reserved. Cisco Public

Спам усложняется

TEXT SPAM



ATTACHMENT SPAM
(PDF, EXCEL, MP3)

2005

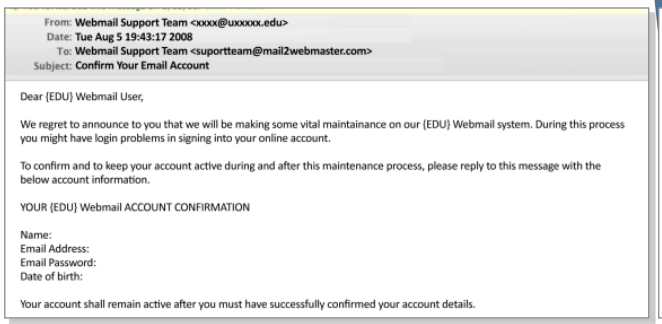
2006

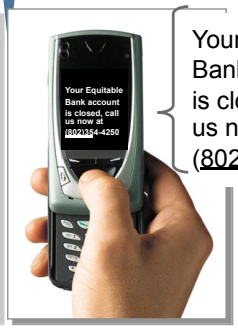
2007

2008

IMAGE SPAM

TARGETED ATTACKS





Your Equitable Bank account is closed, call us now at (802)354-4250

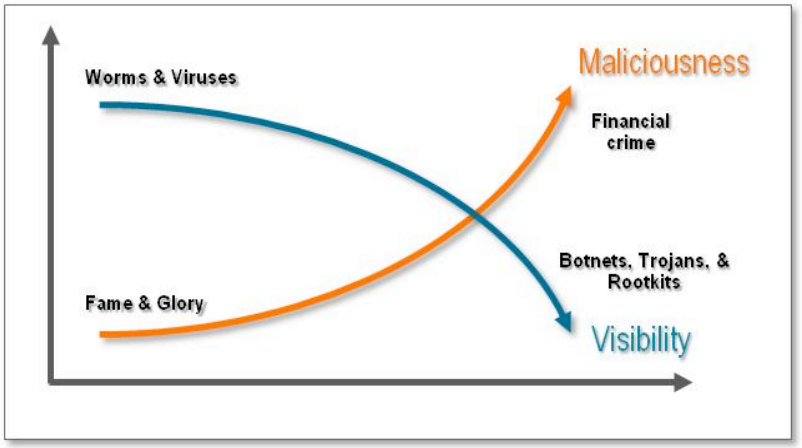
“В 2008 году спам существенно эволюционировал…киберперступники используют короткие фишинговые кампании нацеленные на определенные группы пользователей для достижения большего эффекта”

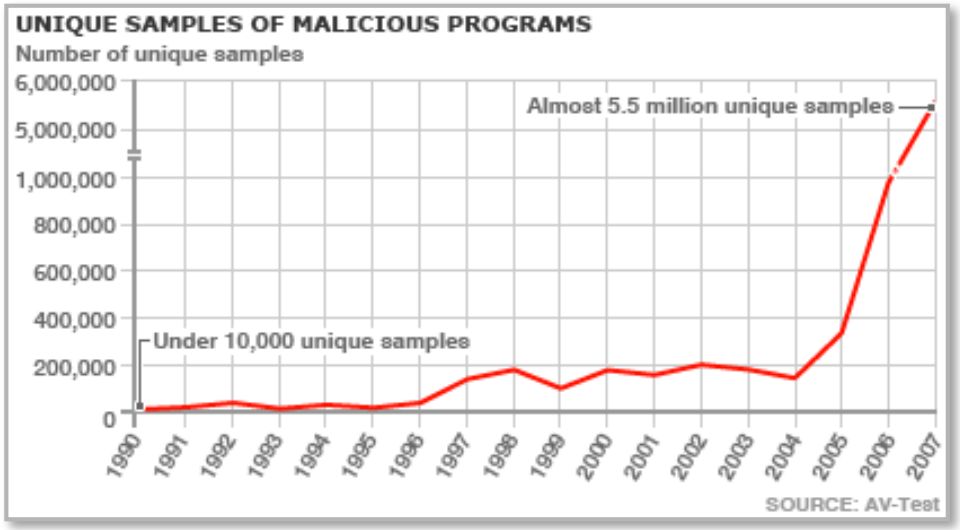
- 2008 Internet Security Trends Report Published By Cisco and IronPort

© 2009 Cisco Systems, Inc. All rights reserved.

Malware на подъёме

Email – основная среда распространения





© 2009 Cisco Systems, Inc. All rights reserved. Cisco Public

Утечка данных – еще одна проблема

Увеличивается количество отчетов, свидетельствующих об утечке даных

Основная среда, через которую происходит утечка -- email

Новые законы выдвигают новые требования

Errant e-mails compromise hundreds of student IDs

Student Financial Services sends 632 registration block notifications containing students' Social Secu numbers to the wrong students

Breanna Hockenbury, Cavalier Daily Staff Writer

Notifications from Student Financial Services intended for students whose registration was blocked were erroneously sent to the wrong students in emails that included others' Social Security numbers.

Student Financial Services intended to send 1,264 emails to alert students of registration blocks. Only 632 e-were actually sent out late Tuesday evening. These e-mails contained the student IDs of the 632 others stude

many different vectors of DLP leakage but not all equal.

Order	Leakage Concern	Percent
1	Email	56%
2	Lost Laptop	51%
3	Web	37%
4	IM	33%
5	USB	19%

Table1: IT Concerns for Leakage (IDC)

Privacy & Security Task Force ADVISOR

October 7, 2008

States Adopting Aggressive New Privacy and Data Security Laws and Regulations

© 2009 Cisco Systems, Inc. All rights reserved. Cisco Public

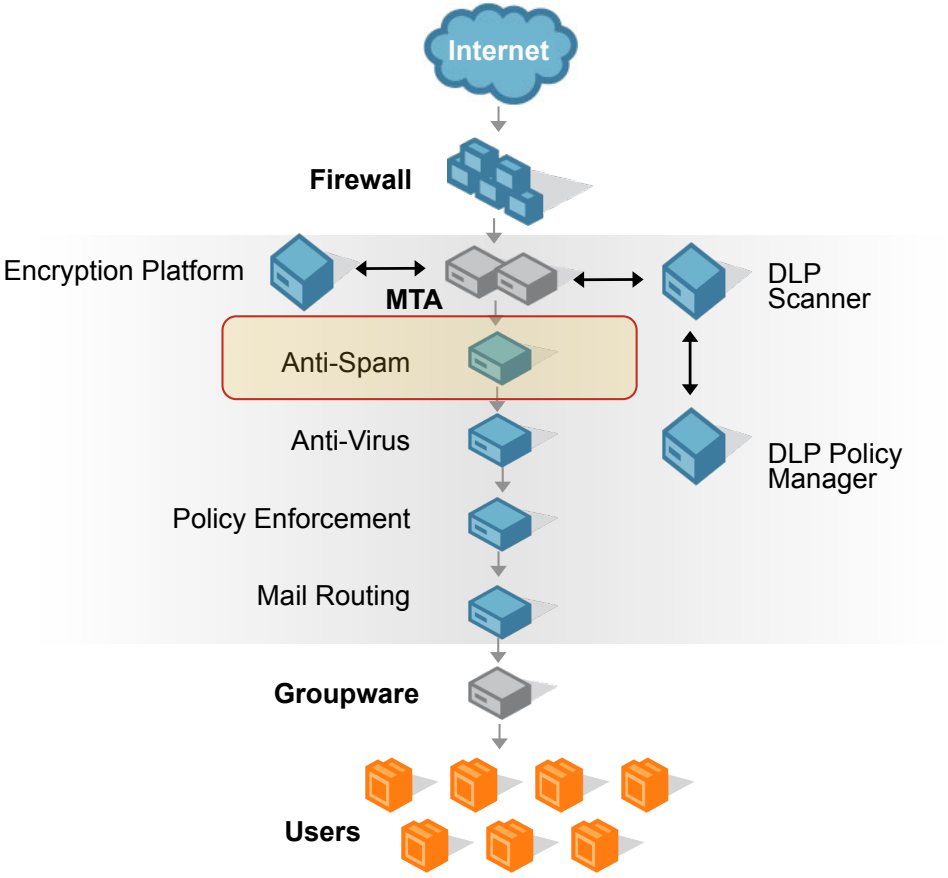
Нагрузка на администраторов

- Распространение угроз увеличивает объем работы и требует дополнительных специализированных знаний
- Сокращение бюджета приводит к тому, что административные ресурсы «распыляются» на выполнение нескольких несовместимых задач

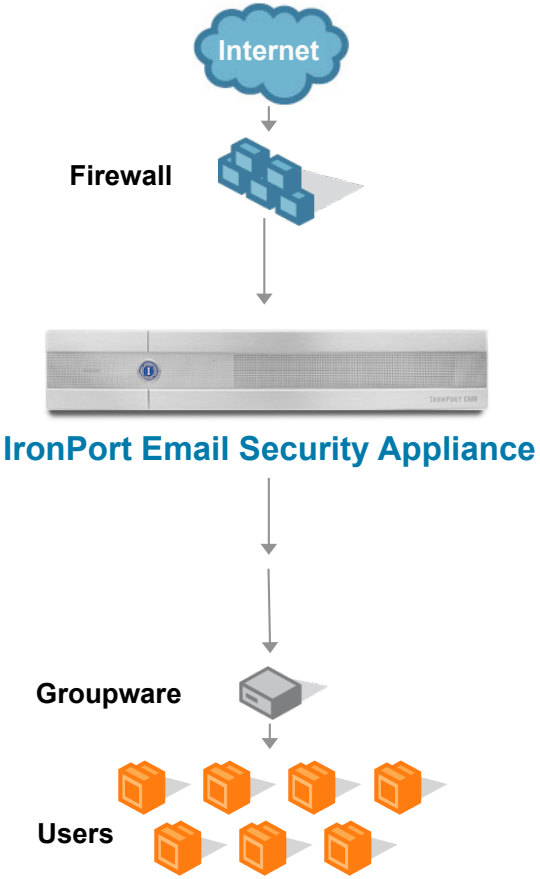
© 2009 Cisco Systems, Inc. All rights reserved. Cisco Public

IronPort Email Security Appliance

Before IronPort

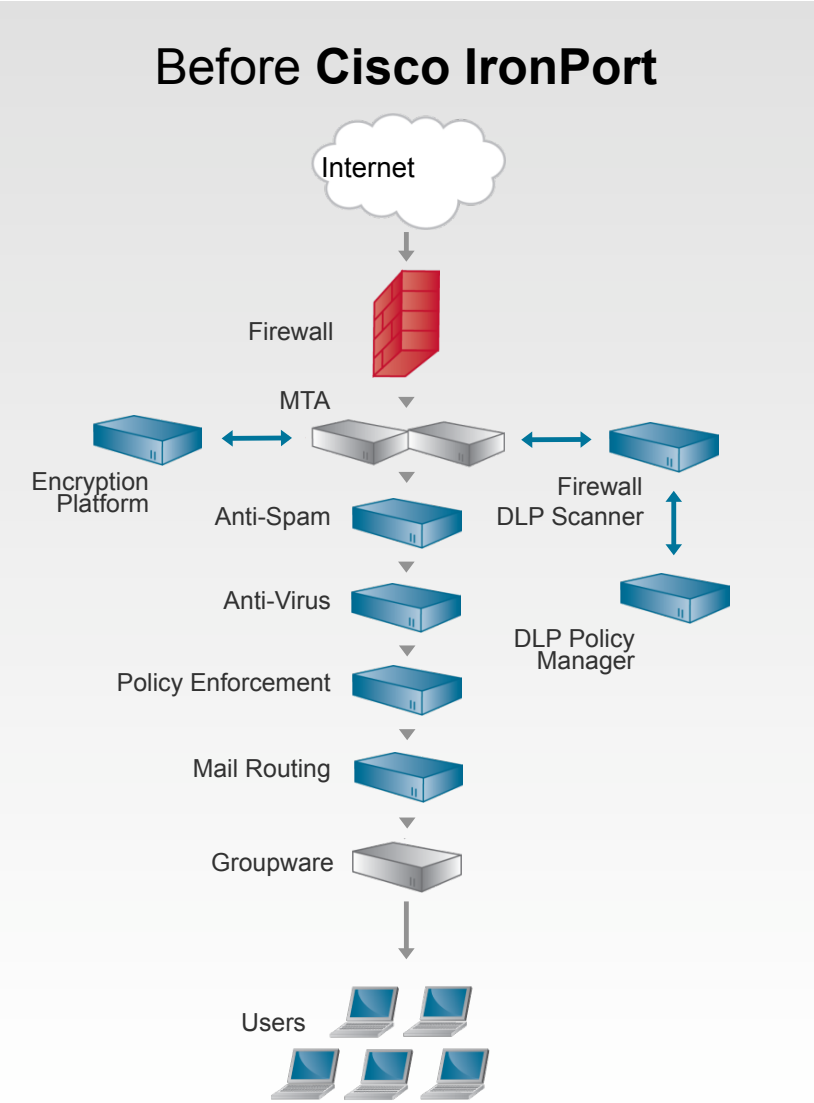


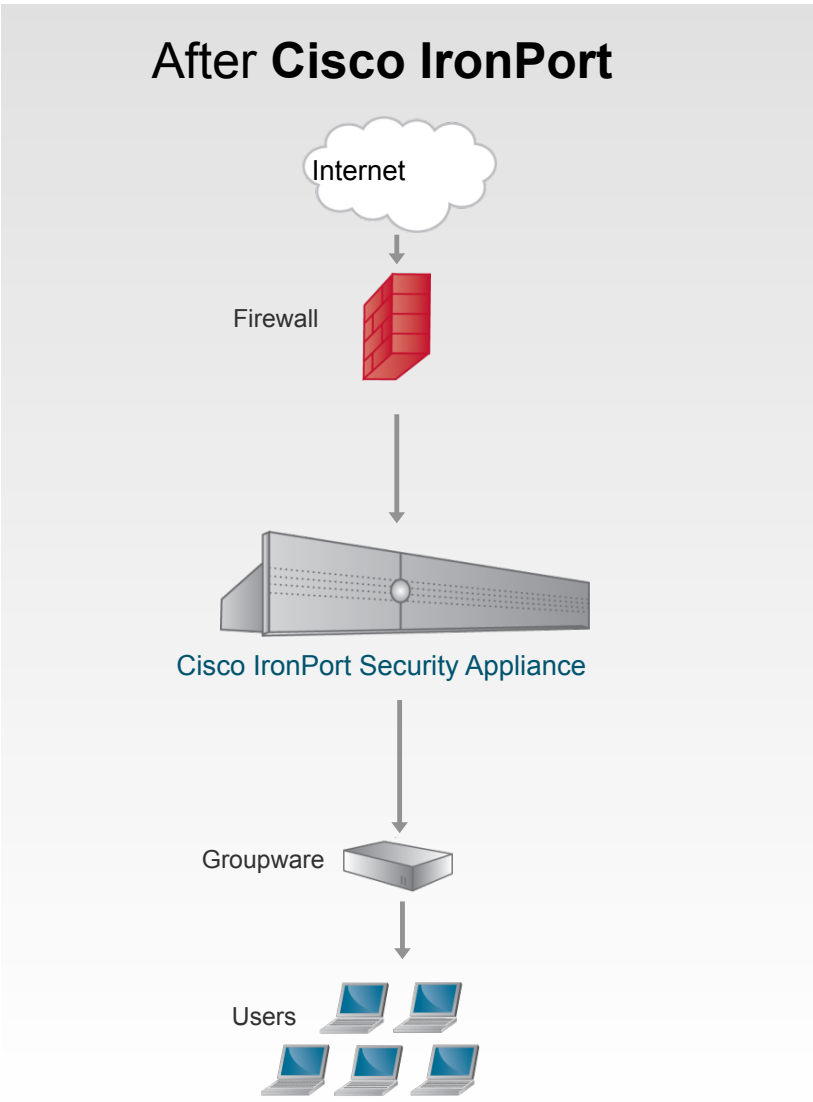
After IronPort



IronPort Email Security Solution

"Set and Forget"





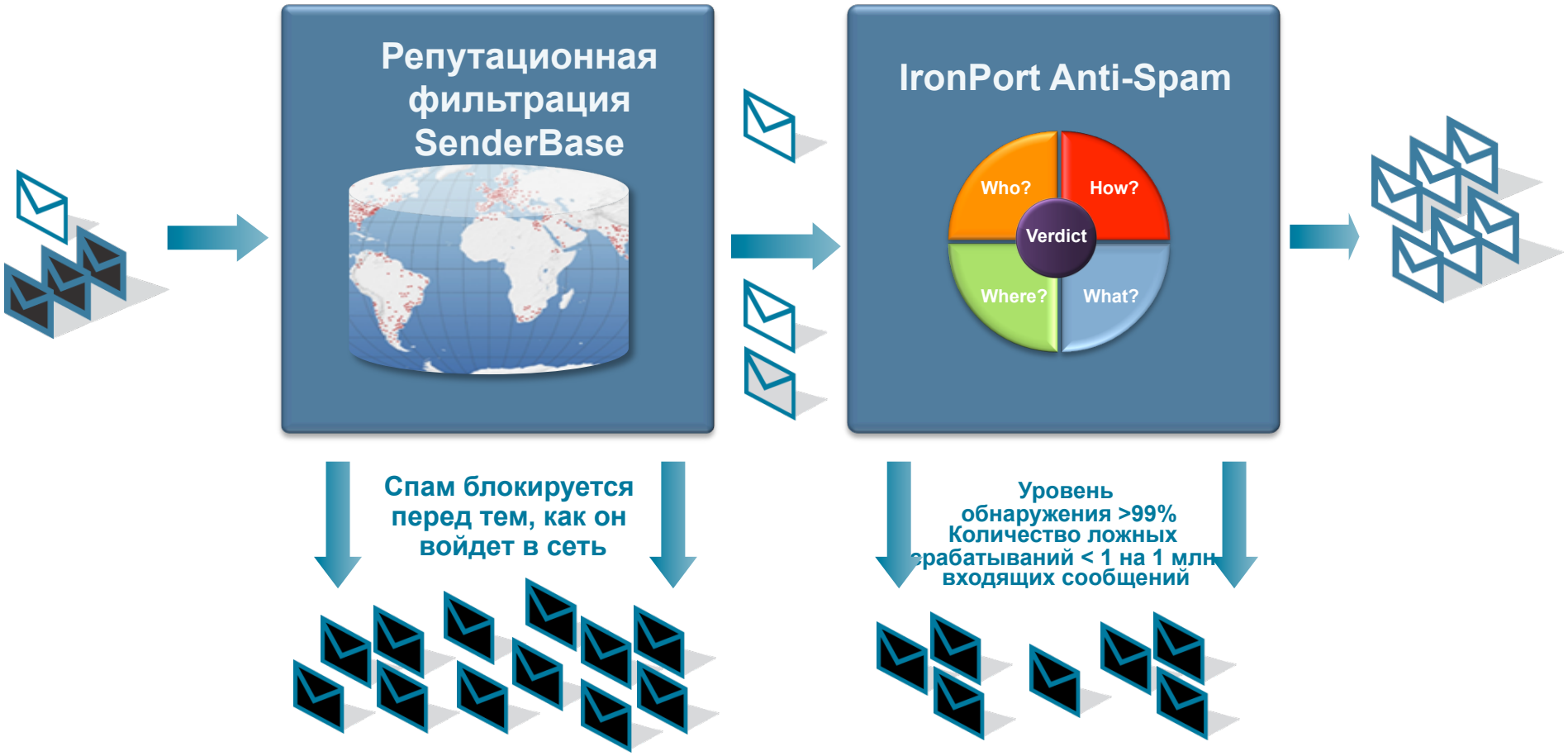
© 2009 Cisco Systems, Inc. All rights reserved. Cisco Public

Email. Архитектура безопасности.

Безопасность входящих сообщений, контроль исходящих

© 2009 Cisco Systems, Inc. All rights reserved. Cisco Public

Анти-спам в деталях

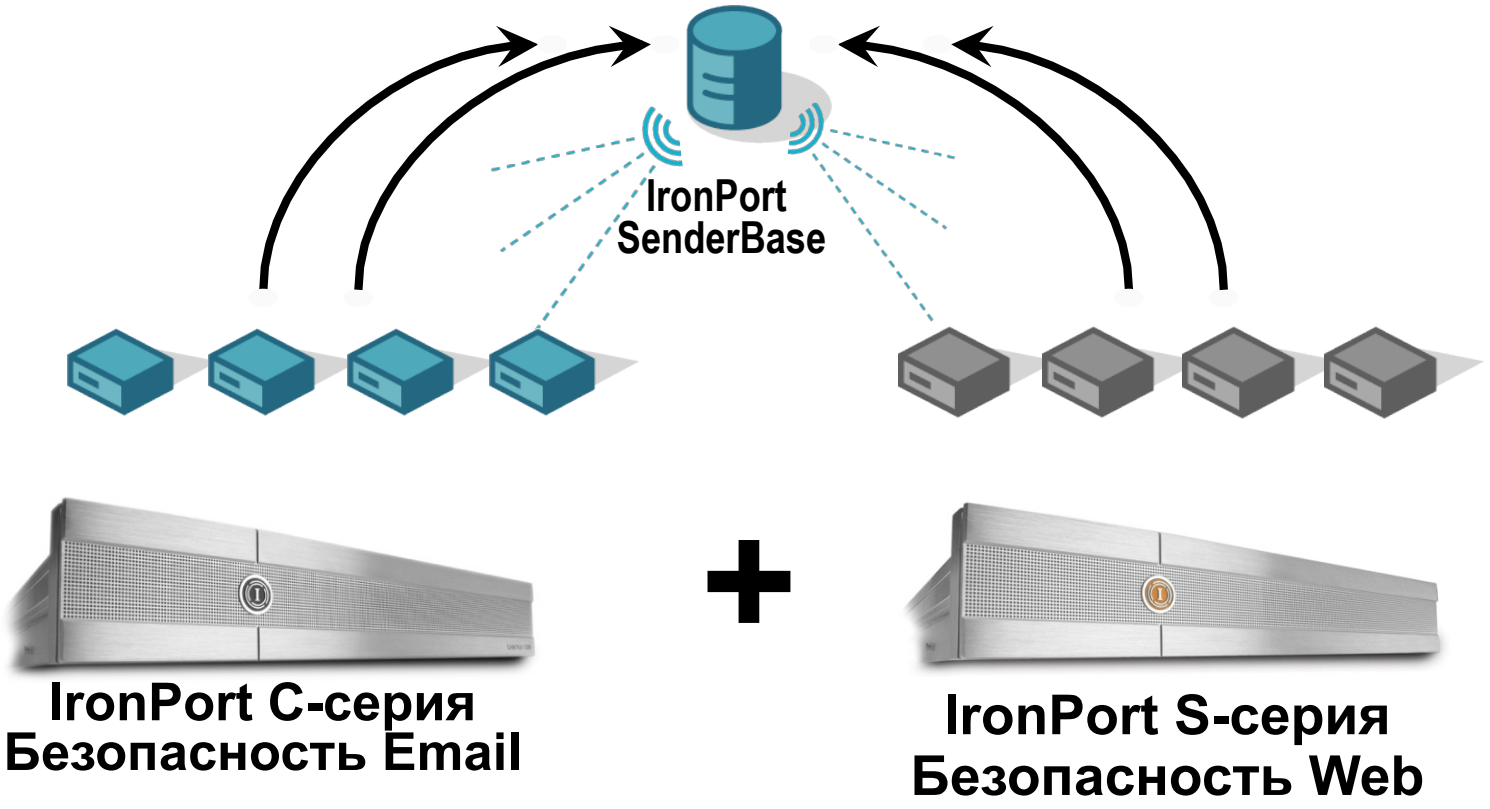


© 2009 Cisco Systems, Inc. All rights reserved.

IronPort SenderBase

Быстрое и точное обнаружение угроз

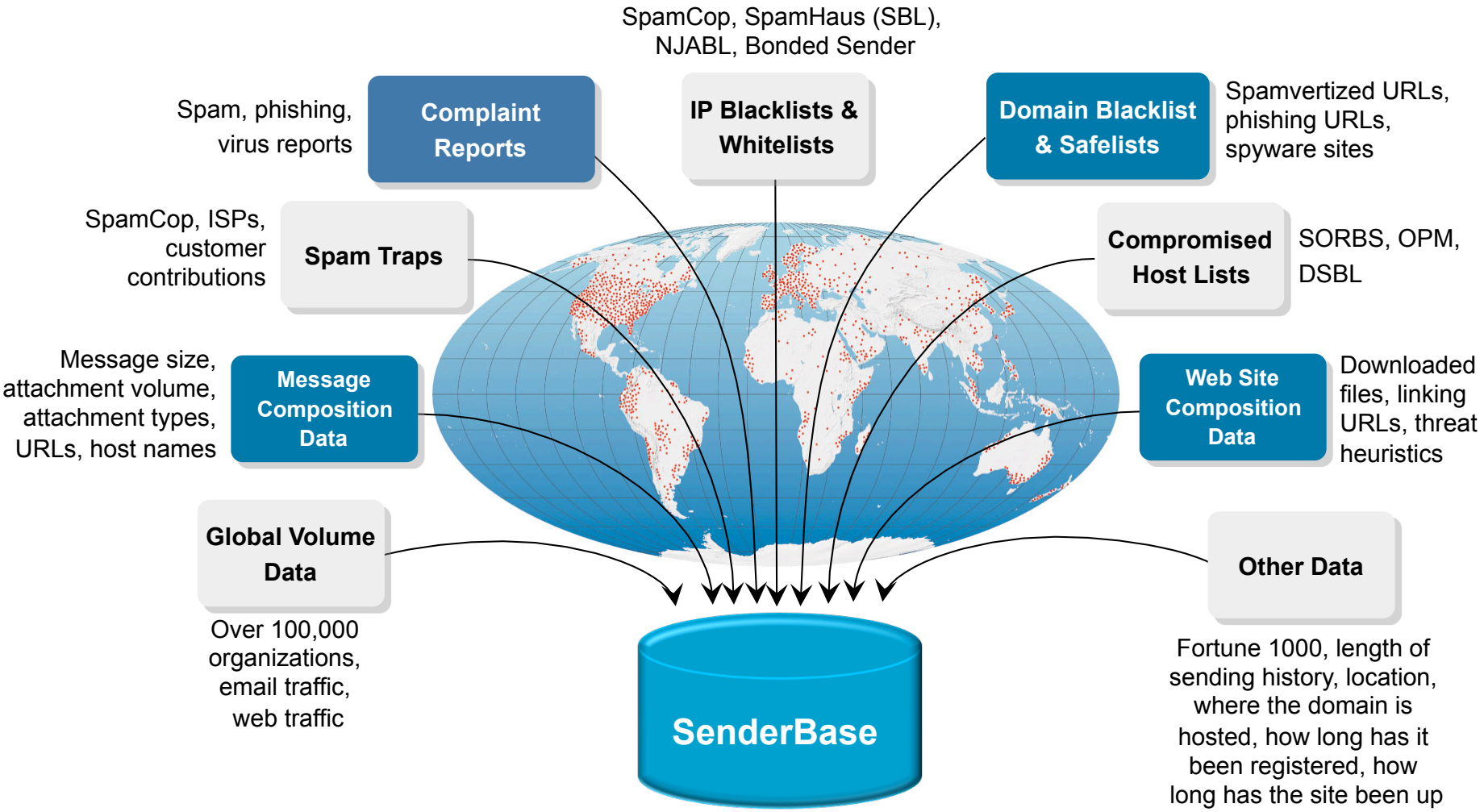
Объединенный анализ Email & Web трафика



© 2

Cisco IronPort SenderBase

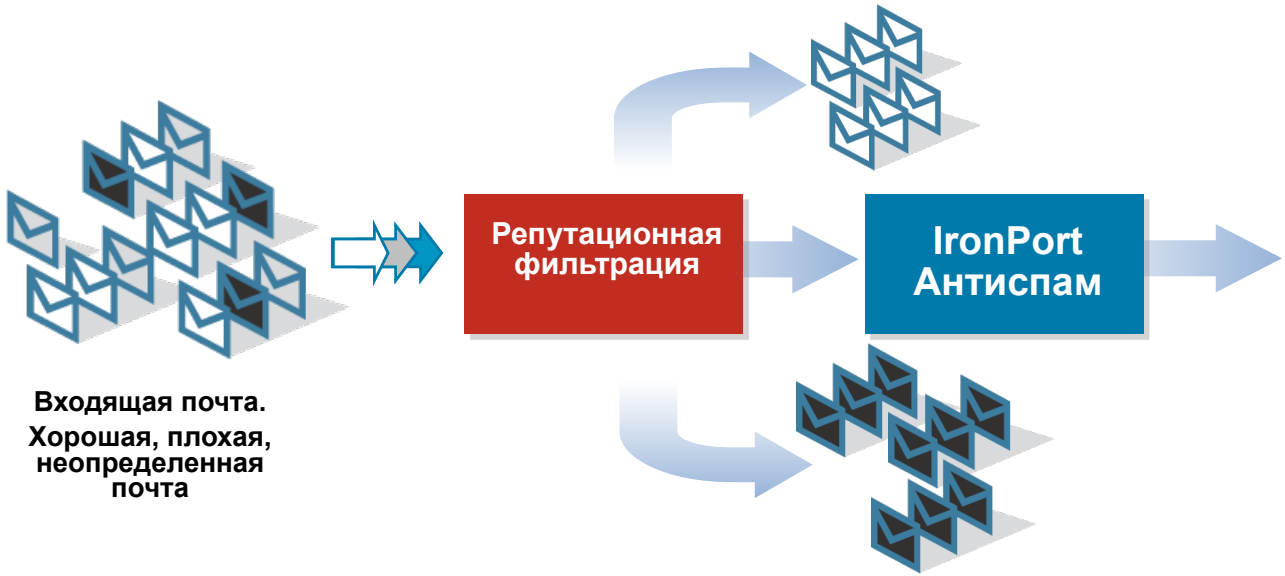
Секрет успеха -- качество и количестве данных



© 2009 Cisco Systems, Inc. All rights reserved. Cisco Public

Репутационная фильтрация SenderBase

Предотвращение угроз в реальном времени



- **Известная хорошая доставляется**
- **Подозрительная ограничивается и проверяется на спам**
- **Известная плохая блокируется**

Cisco on Cisco

Корпоративная почта Cisco

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**

© 2009 Cisco Systems, Inc. All rights reserved.
Cisco Public

Антиспам Cisco IronPort

Многоуровневая линия обороны от спама

EMAIL Репутация

- ✓ Ботнеты
- ✓ Спаммерские сети

Содержание сообщения

- ✓ SMS Spam
- ✓ Спам в присединенных файлах

WEB Репутация

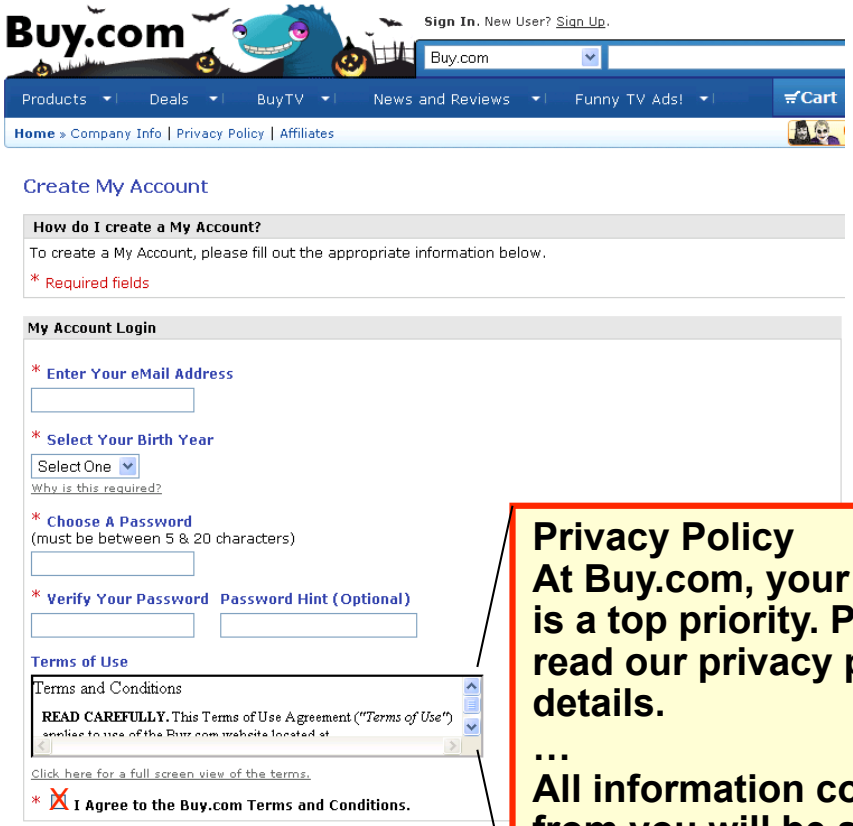
- ✓ Malware/Фишинг
- ✓ Короткие спам-письма с URL

Структура сообщения

- ✓ Спам в изображениях
- ✓ Спам создан с помощью автоматизированных инструментов

© 2009 Cisco Systems, Inc. All rights reserved. Cisco Public

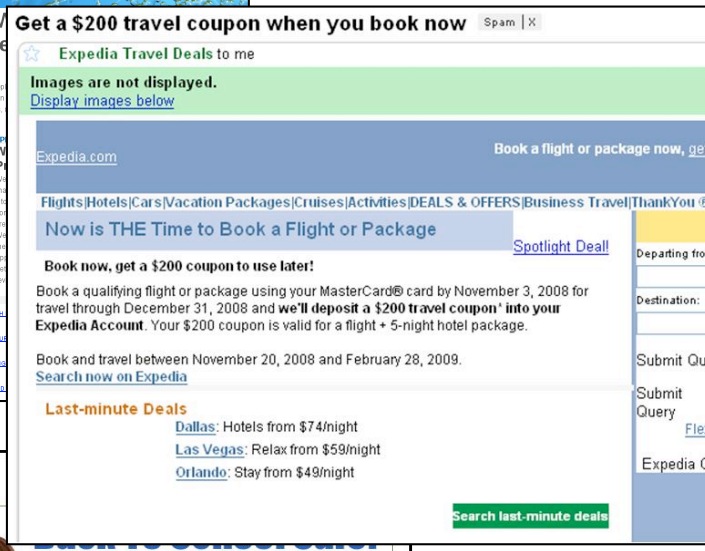
Marketing Message Detection –
The Problem



Privacy Policy
At Buy.com, your privacy is a top priority. Please read our privacy policy details.

…

All information collected from you will be shared with Buy.com and its affiliate companies.

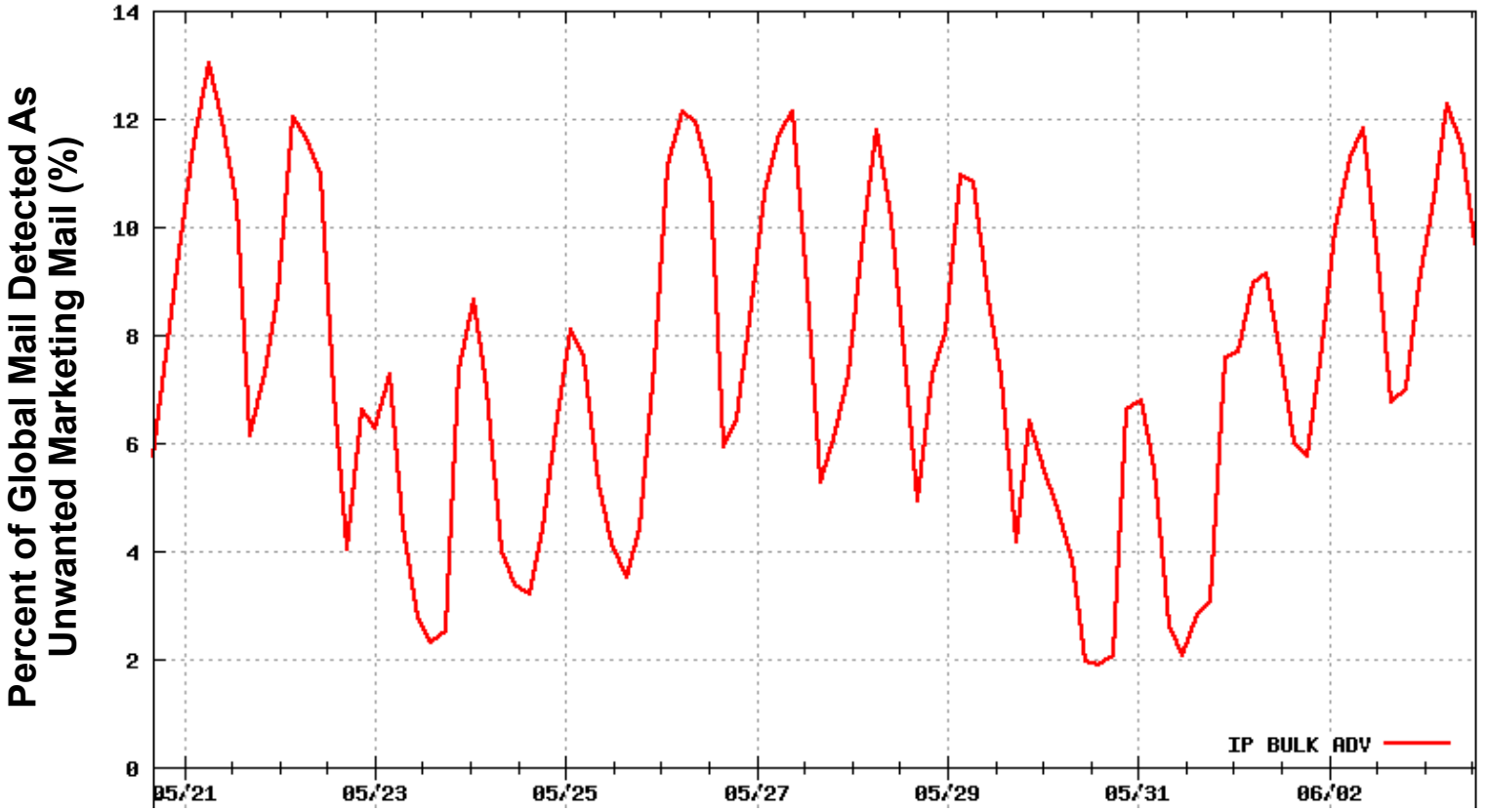


- Not Spam, because of tacit opt-in and working opt-out

© 2009 Cisco Systems, Inc. All rights reserved. Cisco Public

Marketing Message Detection – *The Solution*

- ***Blocks messages from major bulk mailers*** *(i.e. Constant Contact, Vertical Response)*
- ***Determination based on user voting*** *(i.e. Apple iTunes, Dell, United Airlines are legitimate)*

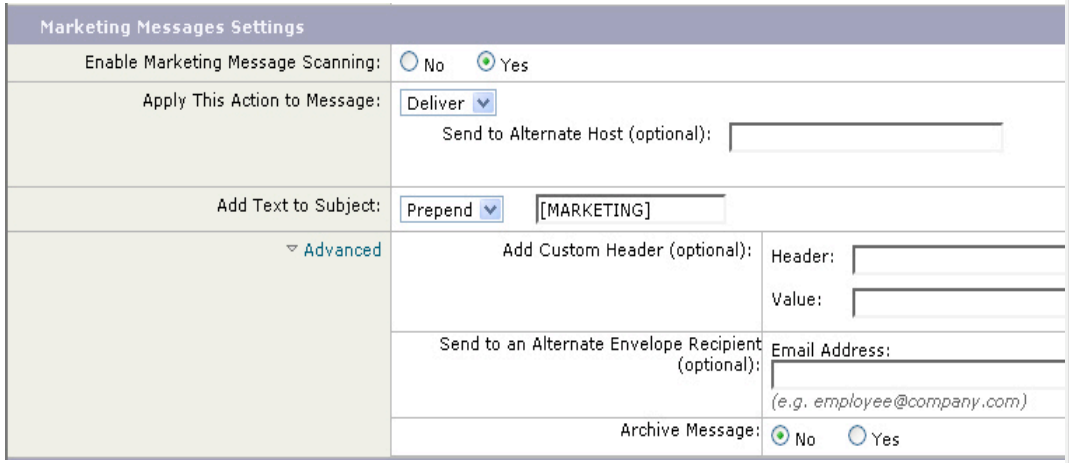


© 2009 Cisco Systems, Inc. All rights reserved. Cisco Public

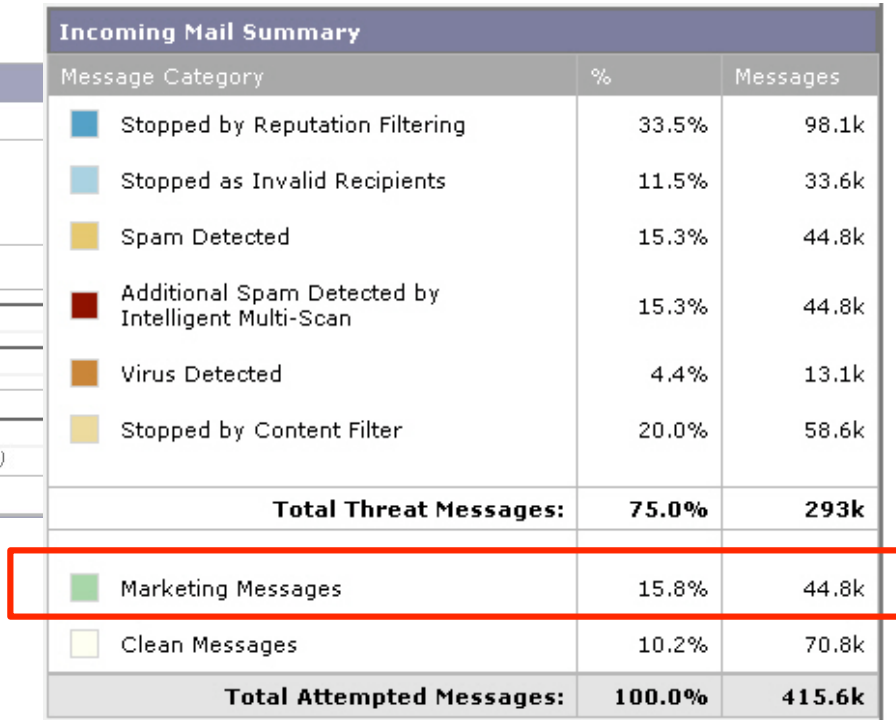
Marketing Message Detection

Configuration and Reporting Screenshots

- Config in IPAS settings



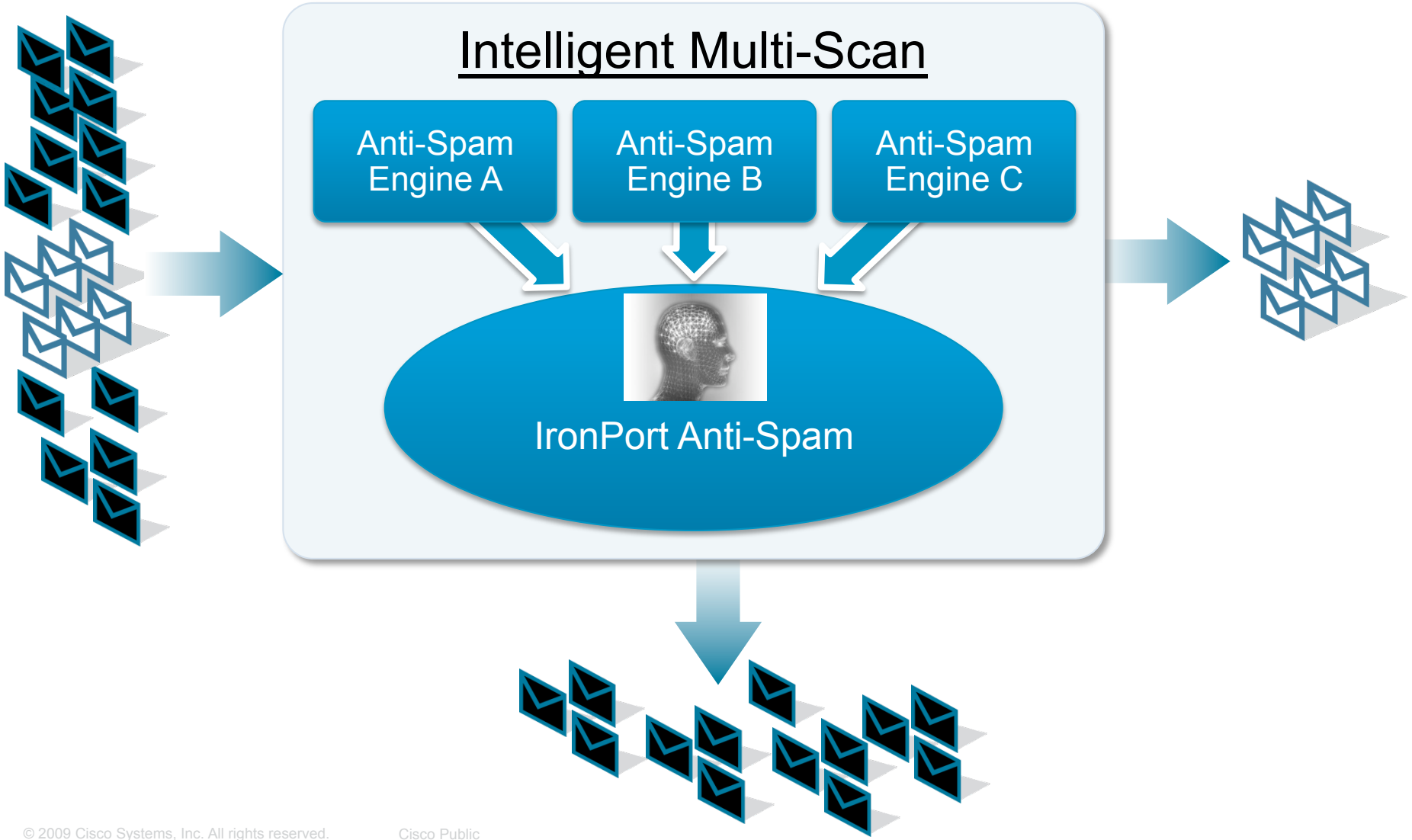
- Full Overview Reporting



© 2009 Cisco Systems, Inc. All rights reserved. Cisco Public

Intelligent Multi-Scan

Best of Both Worlds: Higher Detection with Low FPs



© 2009 Cisco Systems, Inc. All rights reserved.
Cisco Public

Intelligent Multi-Scan

Defense-In-Depth Anti Spam

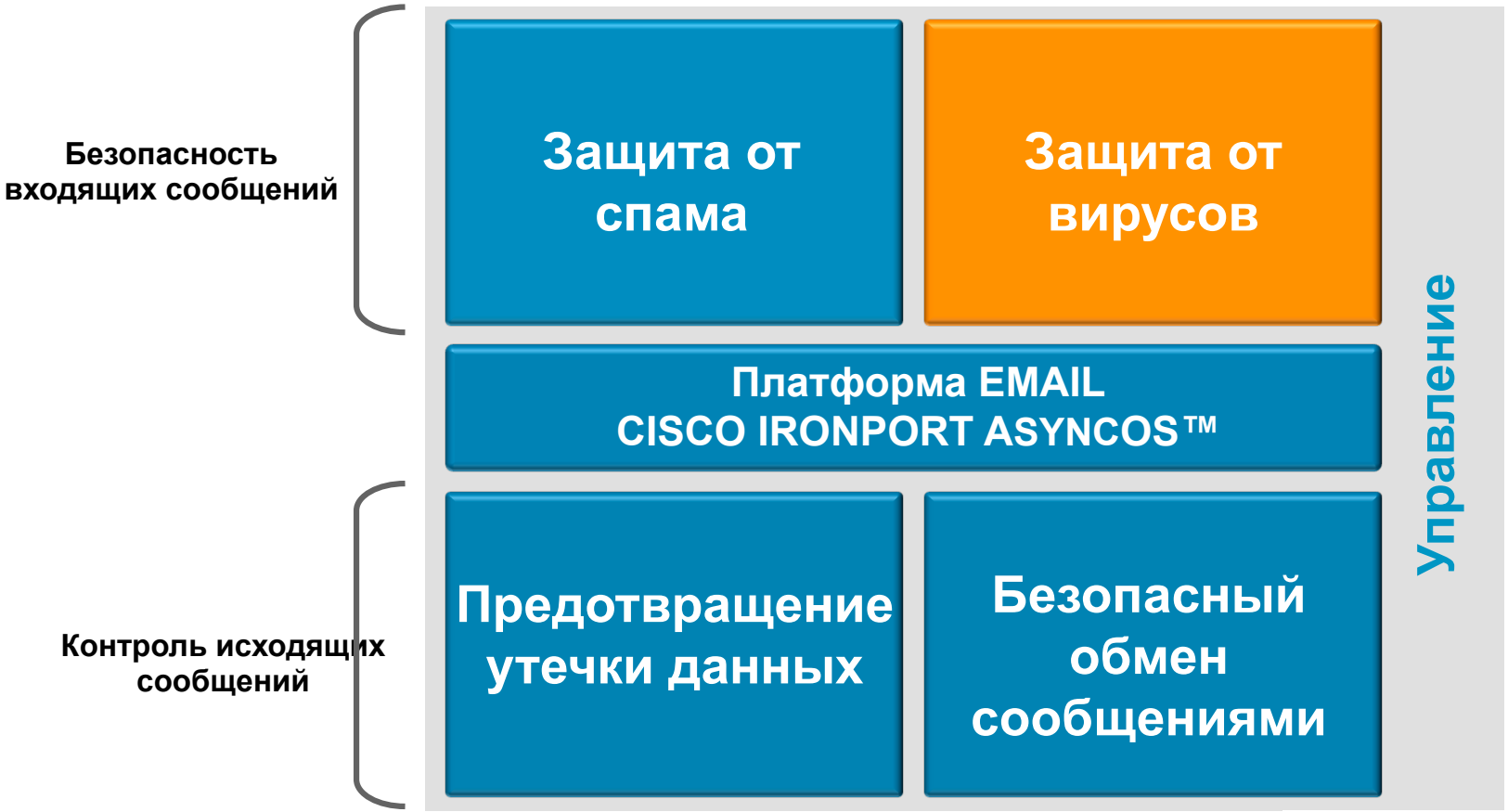
	ANTI-SPAM EFFICACY	
	Detection Rate	FP Rate
IronPort	99.60%	1 in 1 Million
+ Engine A	0.20%	18 in 1 Million
+ Engine B	0.10%	21 in 1 Million
MULTI-SCAN	99.90%	40 in 1 Million
Multi-Scan Improvement	*0.30%*	*- 4000%*

- **Greater** Spam Detection…with IronPort-Leading FP Rate

© 2009 Cisco Systems, Inc. All rights reserved.

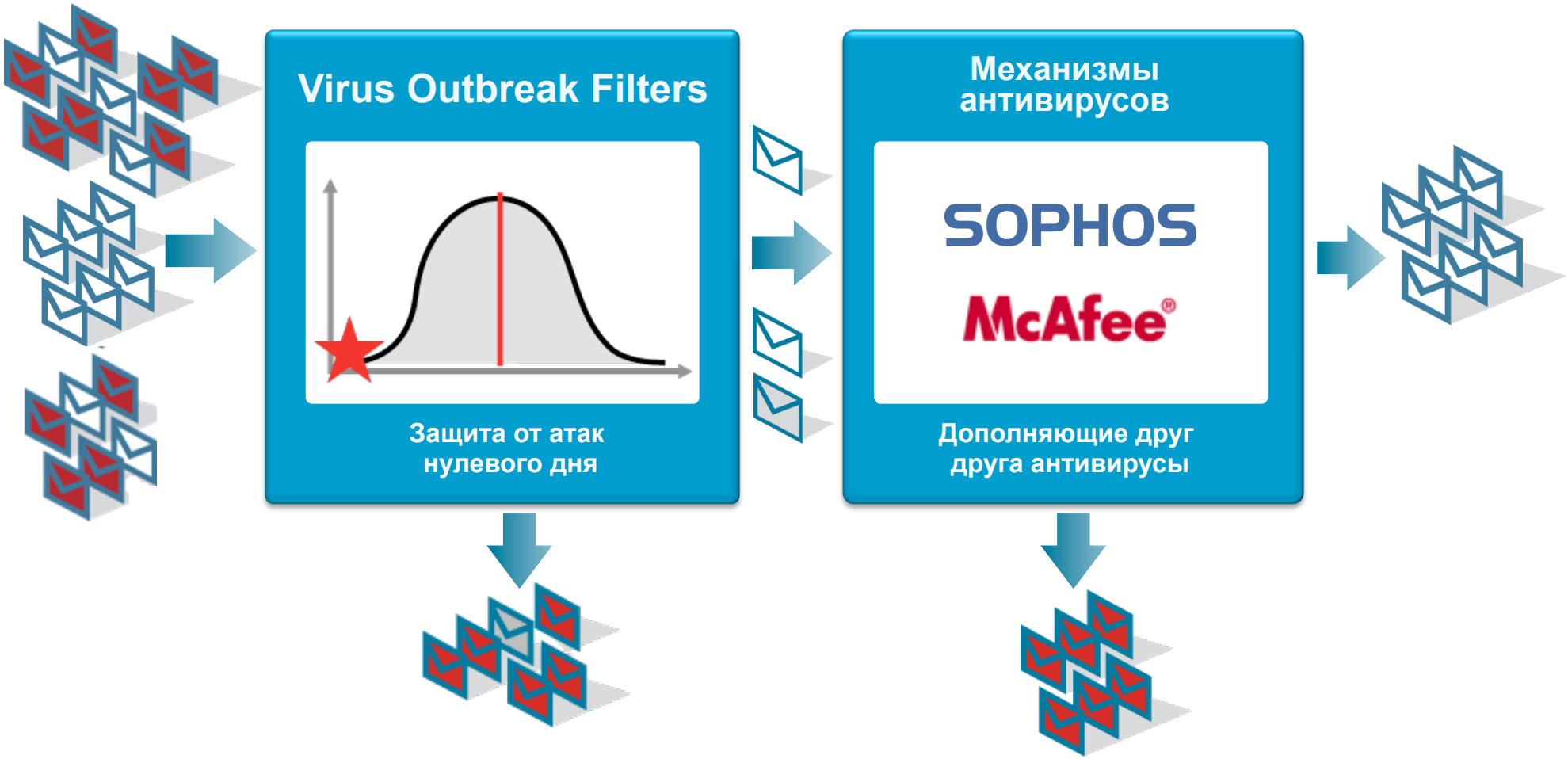
Email. Архитектура безопасности.

Безопасность входящих сообщений, контроль исходящих



© 2009 Cisco Systems, Inc. All rights reserved. Cisco Public

Многоуровневая антивирусная защита

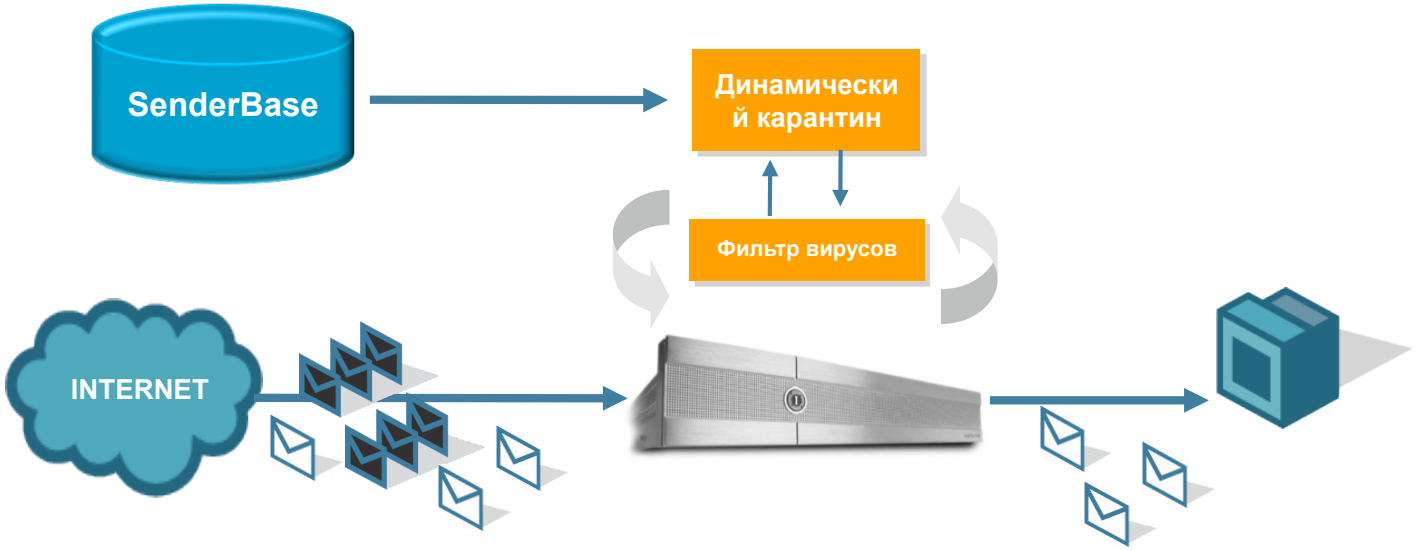


© 2009 Cisco Systems, Inc. All rights reserved. Cisco Public

Cisco IronPort Virus Outbreak Filters

Защита от атак нулевого дня

Virus Outbreak Filters в действии



“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”

ACS

Преимущество Virus Outbreak Filters

Среднее время защиты*……..более 13 часов

Количество атак* ……..…291 атака

Общее время защиты*…… более 157 дней

© 2009 Cisco Systems, Inc. All rights reserved. Cisco Public

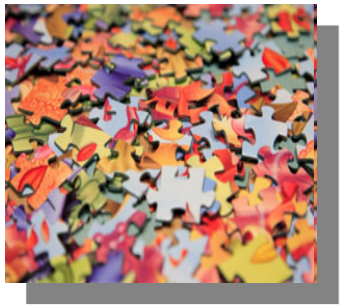
Email. Архитектура безопасности.

Безопасность входящих сообщений, контроль исходящих

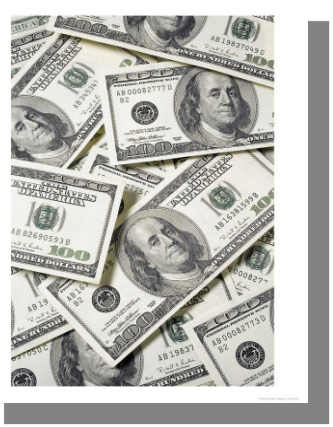
© 2009 Cisco Systems, Inc. All rights reserved. Cisco Public

Исторические барьеры, препятствующие внедреню системы предотвращения утечек

- **Низкая точность**
  - Большо количество как ложных срабатываний, так и несрабатываний
  - Требуется постоянная подстройка



- **Сложность в настройке**
  - Сложная интеграция
  - Ограниченное количество политик



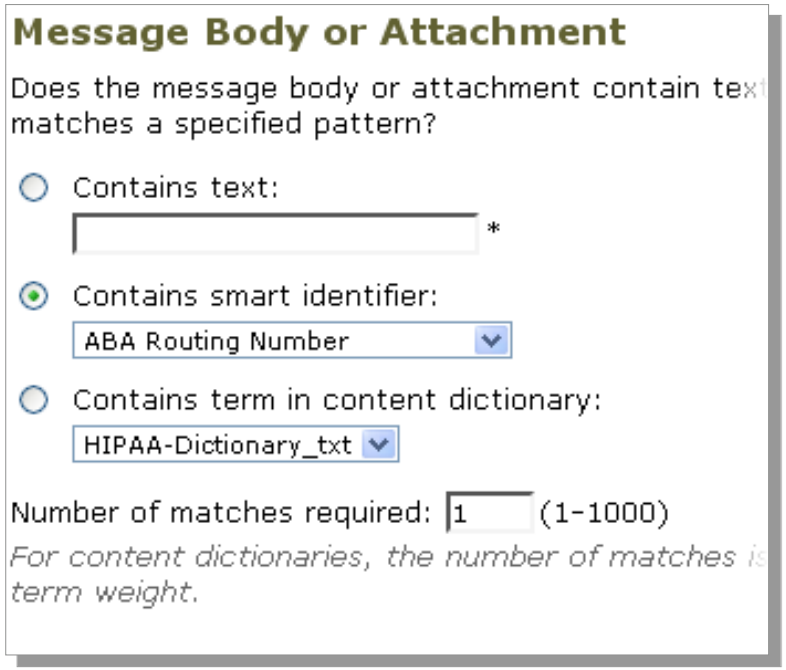
- **Дороговизна**
  - Высокая стоимость внедрения
  - Требовательность к ресурсам

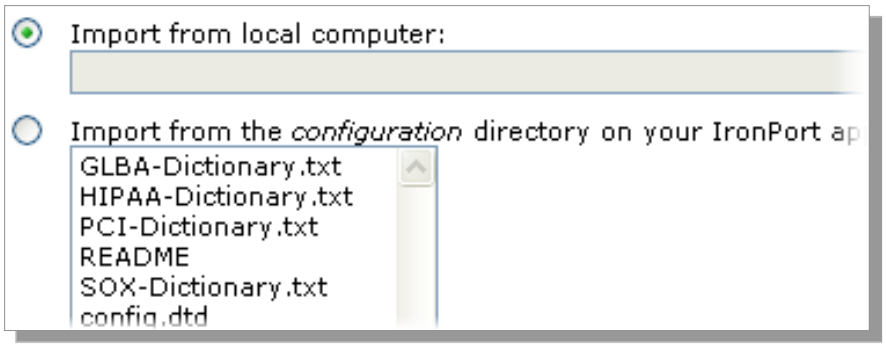
© 2009 Cisco Systems, Inc. All rights reserved. Cisco Public

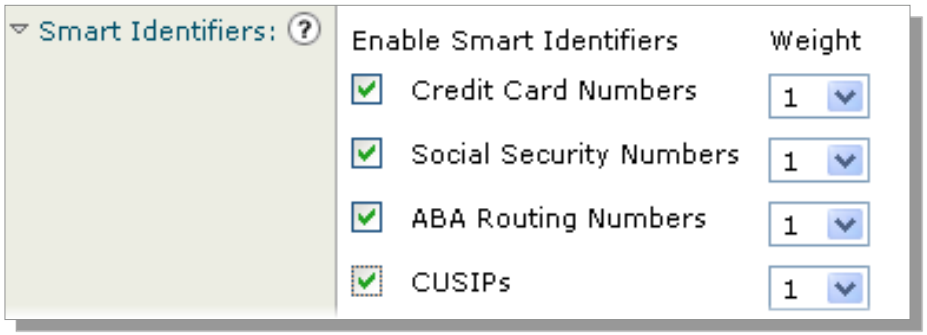
Система сканирования контента IronPort

Простая установка

- Простая установка в три щелчка мыши с помощью фильтров контента
- Используйте набор предопределенных категорий или создайте свои собственные
- Может применятся к определенным пользователям при определенных условиях





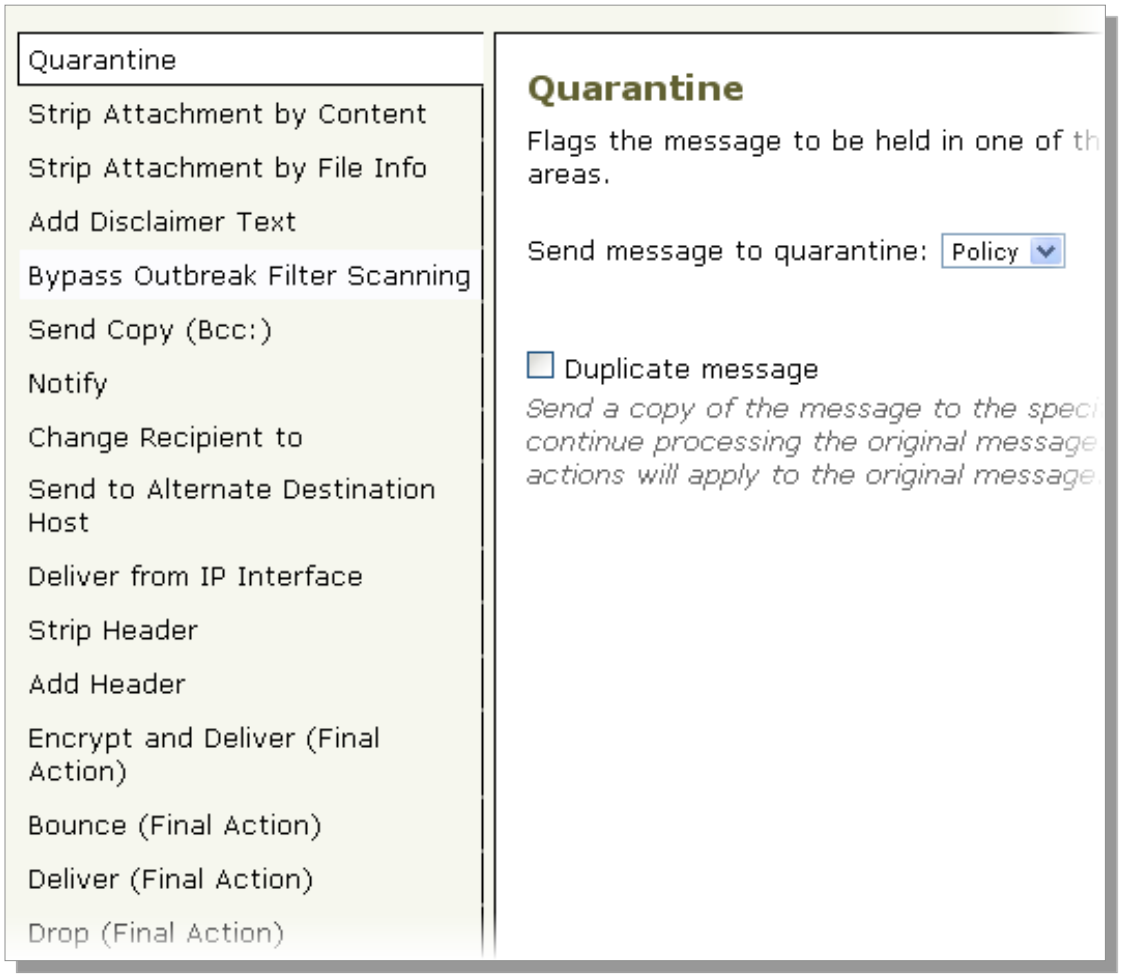


© 2009 Cisco Systems, Inc. All rights reserved. Cisco Public

Предотвращение утечки данных

Полноценная система реагирования и репортинга

- Встроенный набор реакций – шифрование, отправка в карантин, сброс, bounce, скрытая копия, вырезание содержимого, уведомление
- Подозрительный контент подсвечивается в карантине для ускорения поиска
- Построение отчетов на основе политик и пользователей



© 2009 Cisco Systems, Inc. All rights reserved. Cisco Public

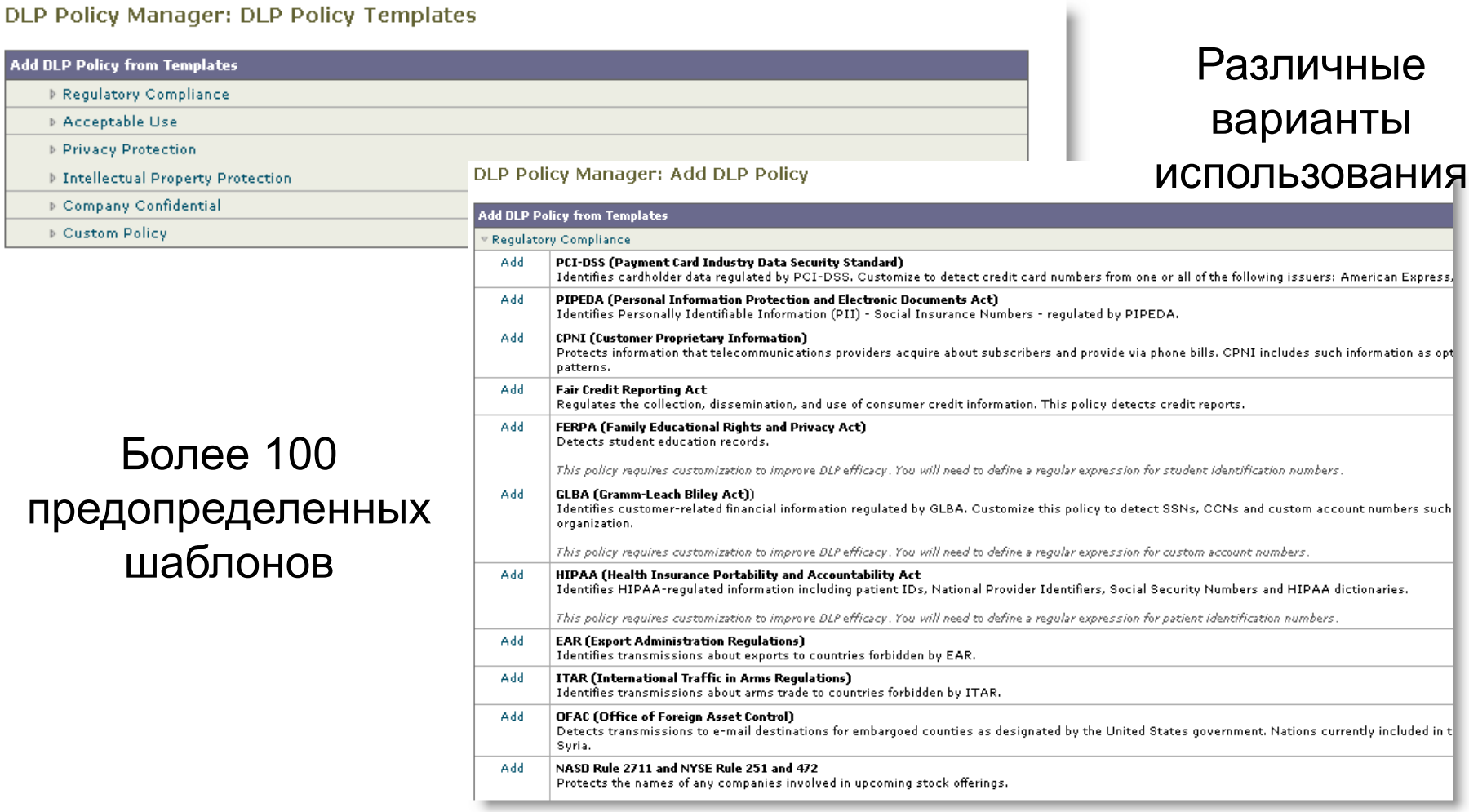
RSA – Лидер рынка и технологий

- Ranked as “Leader” in Gartner Magic Quadrant
- Фокусируется на точности: большая исследовательская команда выделена для написания и проверки политик

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

© 2009 Cisco Systems, Inc. All rights reserved.

Полное, глобальное покрытие



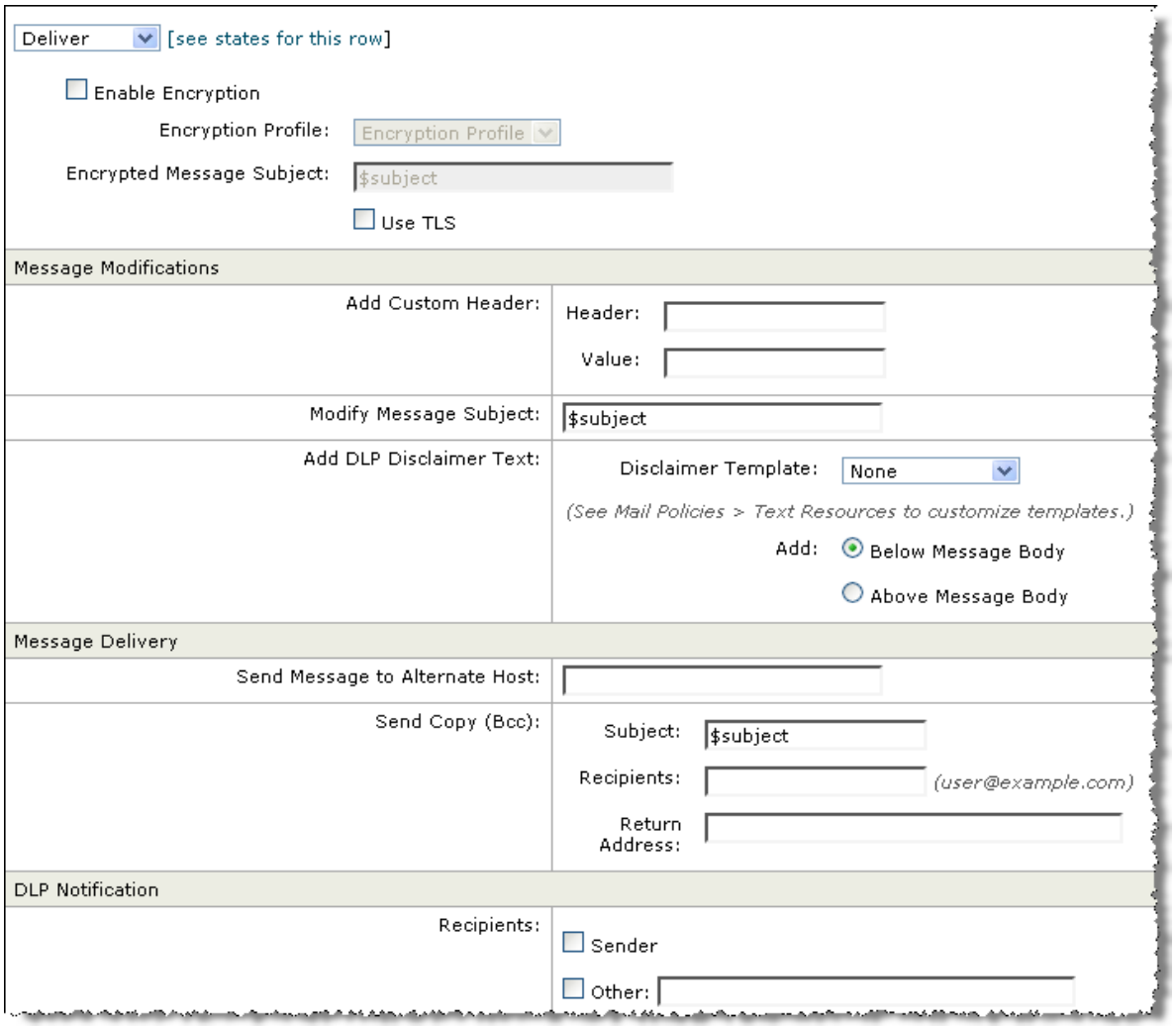
Различные варианты использования

Более 100 предопределенных шаблонов

Политики, создаваемые пользователями

© 2009 Cisco Systems, Inc. All rights reserved. Cisco Public

Широкий набор опций реагирования



1 Доставка, карантин, сброс, шифрование

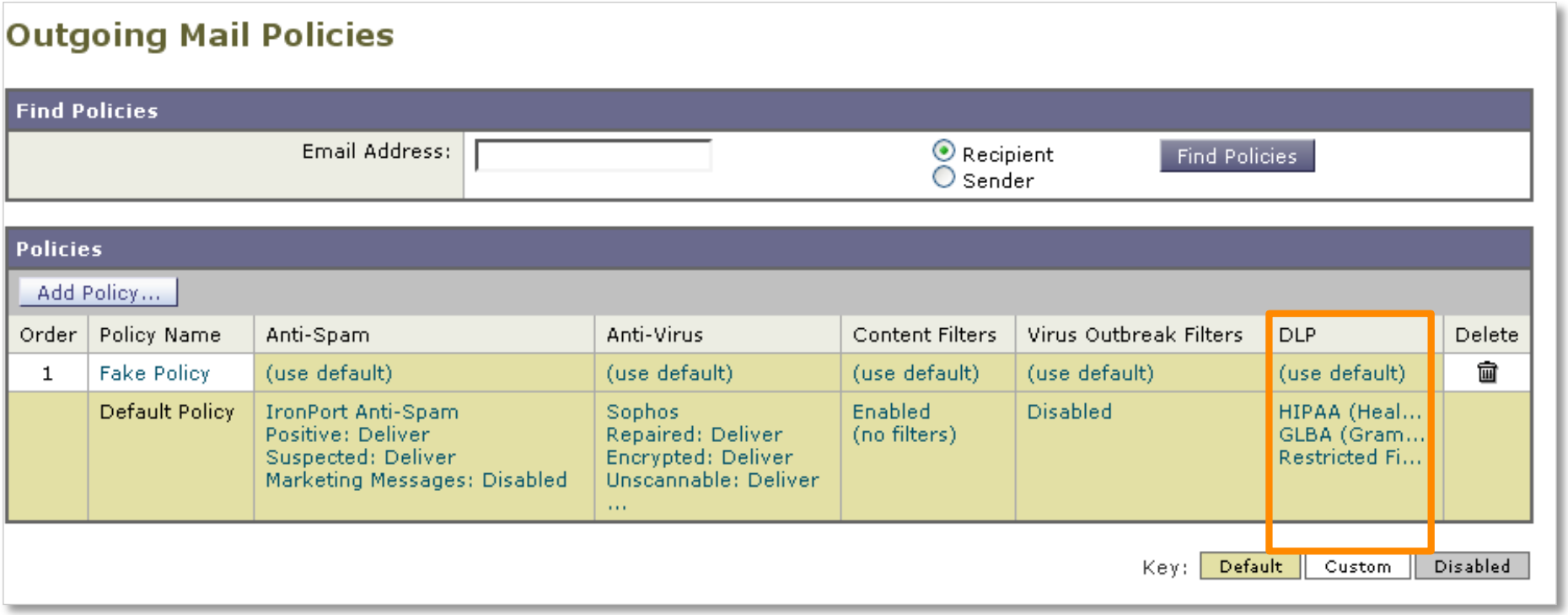
2 Добавить отказ от ответственности

3 Отослать копию администратору безопасности

4 Уведомить отправителя и/или получателя

© 2009 Cisco Systems, Inc. All rights reserved. Cisco Public

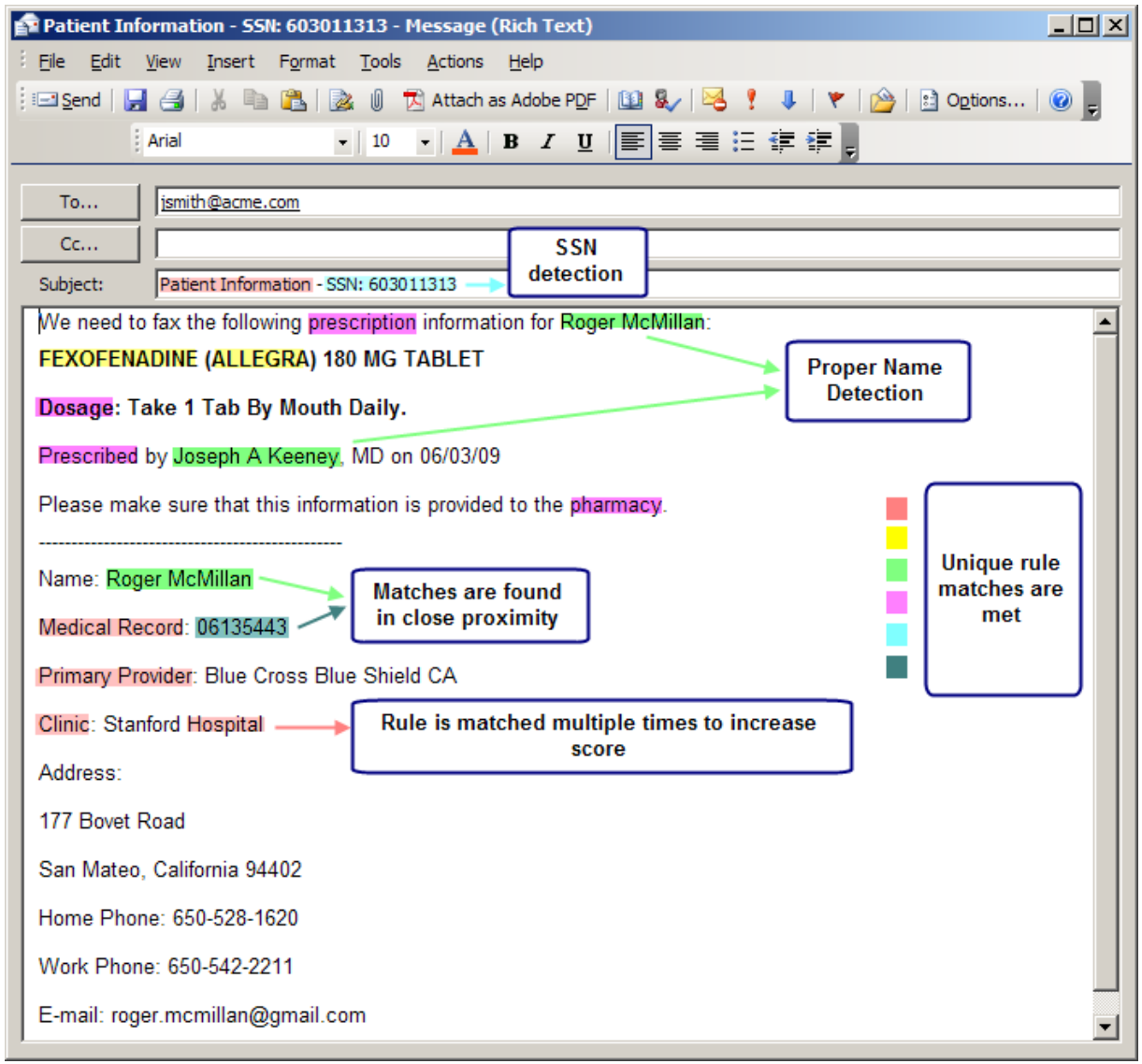
Управление всеми функциями из одной консоли



- Настраивайте анти-спам, антивирус, контентные фильтры, превентивную защиту, шифрование и DLP с помощью одного и того же пользовательского интерфейса

© 2009 Cisco Systems, Inc. All rights reserved. Cisco Public

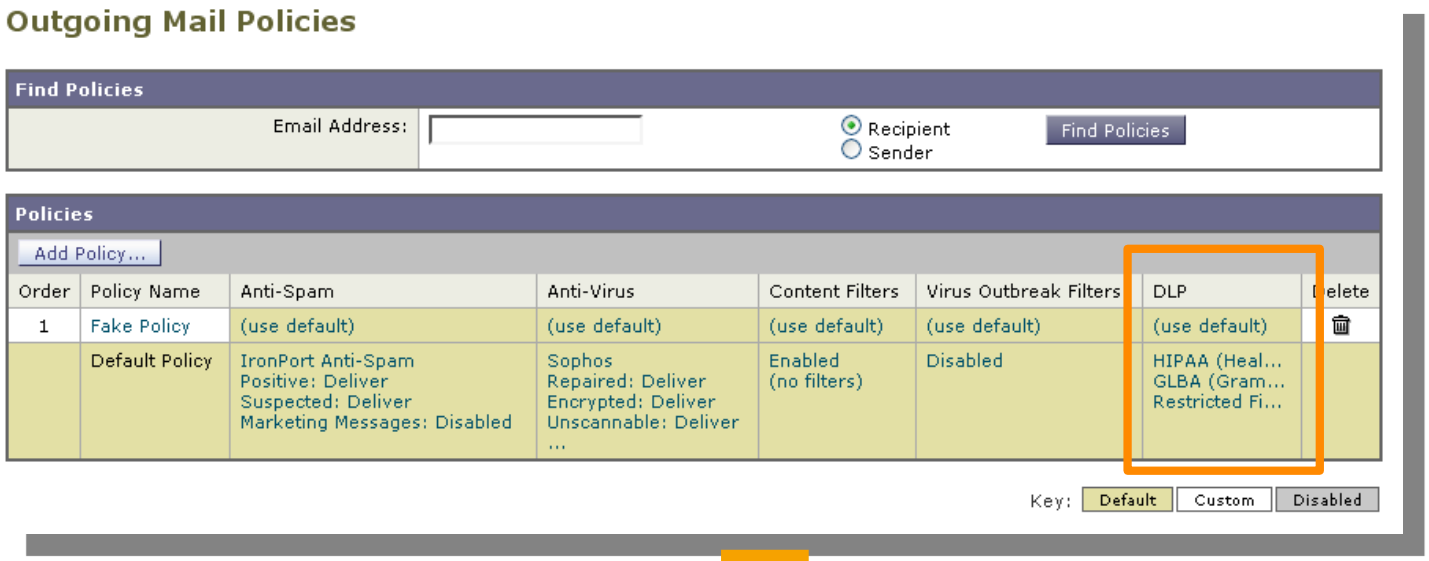
Гарантированная точность анализа



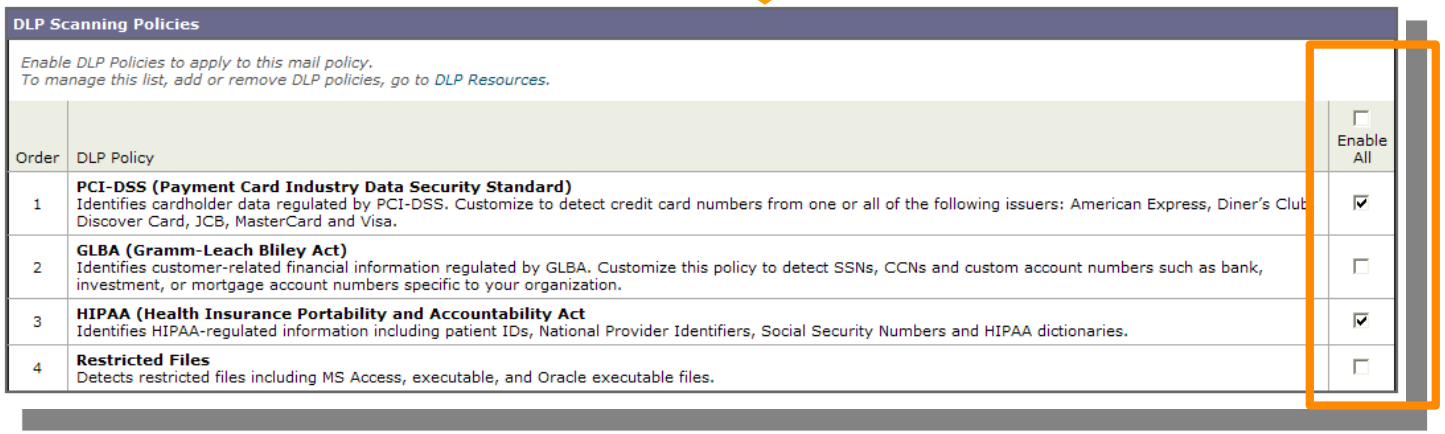
© 2009 Cisco Systems, Inc. All rights reserved. Cisco Public

Просто настраивать

Останавлите канал утечек в течение нескольких минут



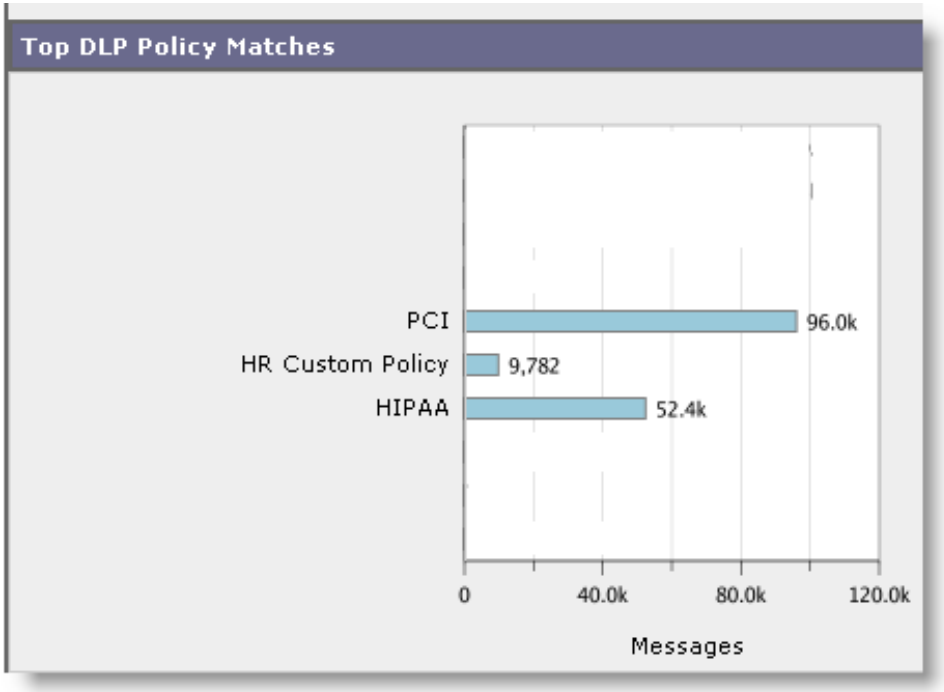
Интегрирован в менеджер политик



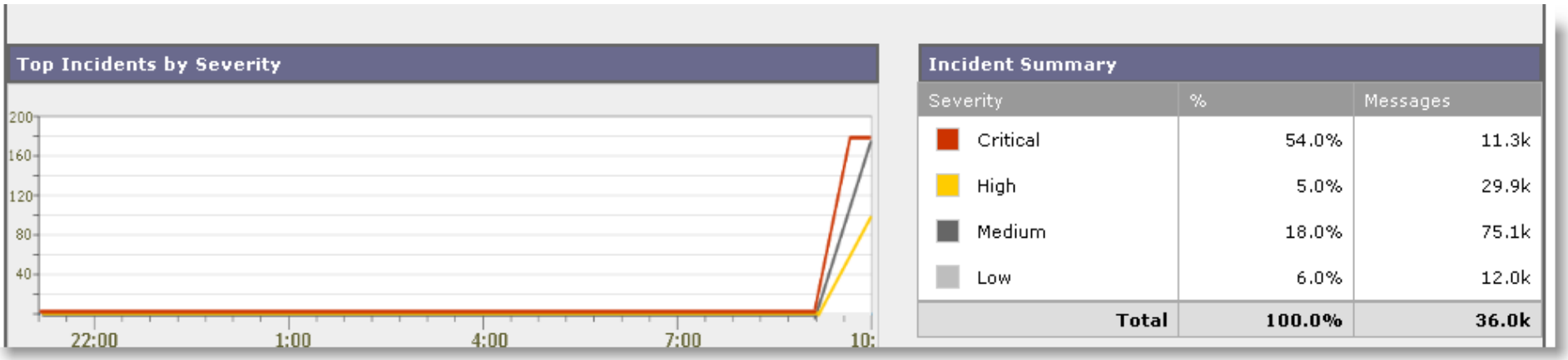
Активация политик одним кликом мышки

© 2009 Cisco Systems, Inc. All rights reserved. Cisco Public

Легко отслеживать

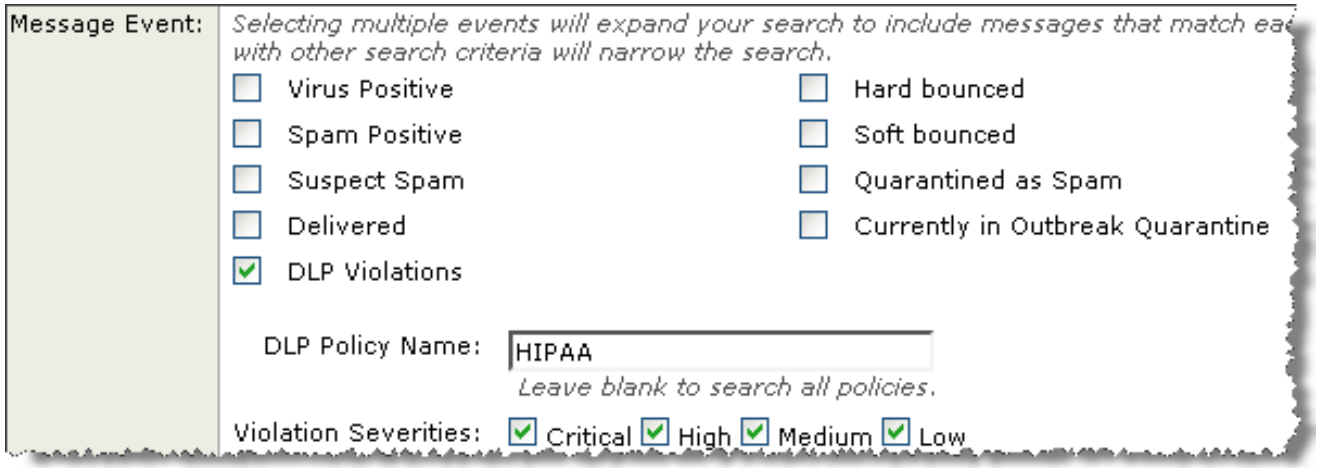


- Отчеты по политикам и по серьезности нарушения
- Доступны как отчеты в реальном времени, так и по расписанию

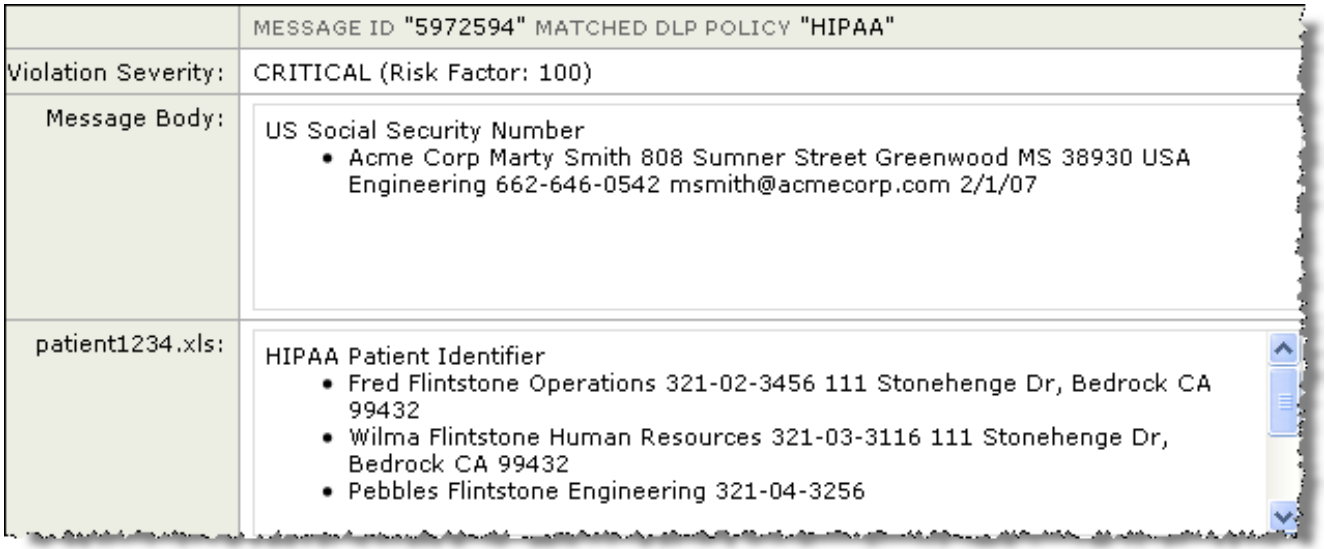


© 2009 Cisco Systems, Inc. All rights reserved. Cisco Public

Легко искать



Простой поиск сообщений



Просмотр деталей нарушения и где оно произошло

© 2009 Cisco Systems, Inc. All rights reserved. Cisco Public

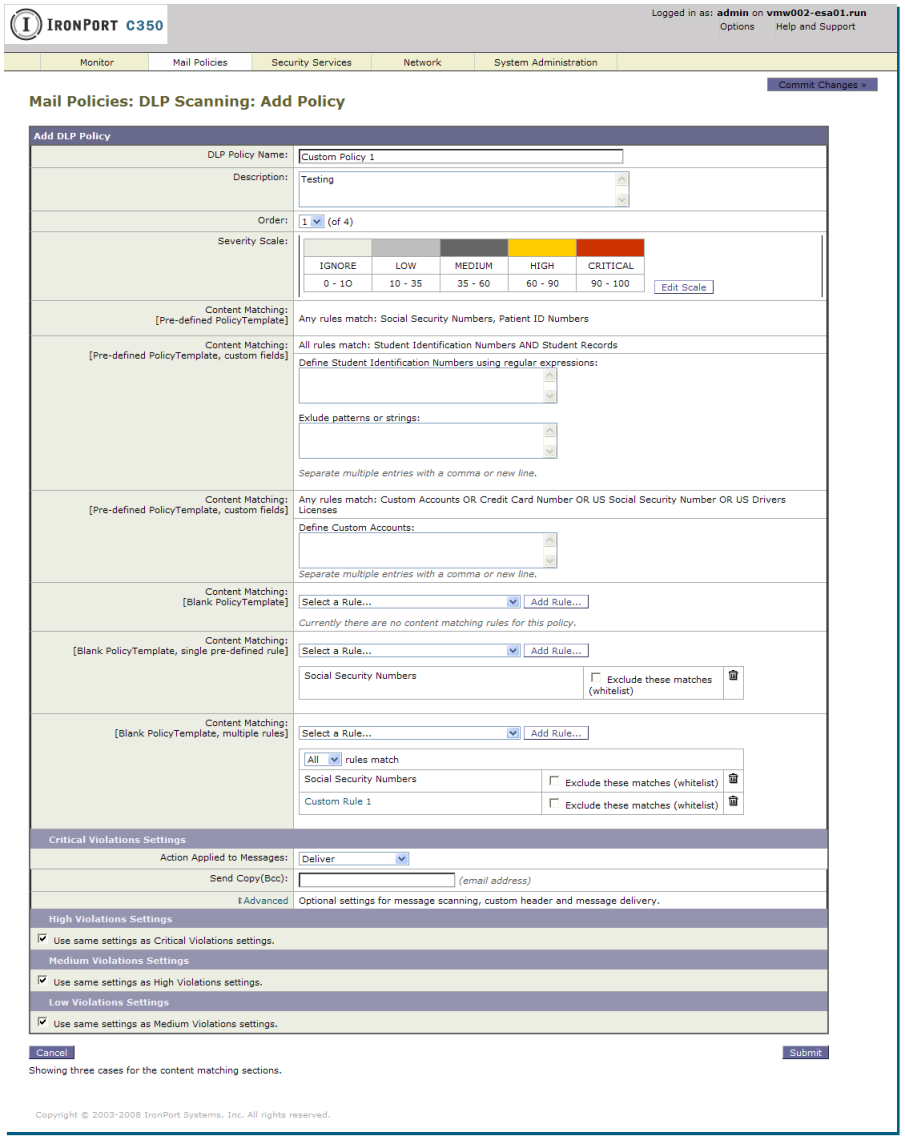
Простота создания пользовательских политик

Название политики и описание

Категория серьезности нарушения

Сканирование контента

Возможный набор действий



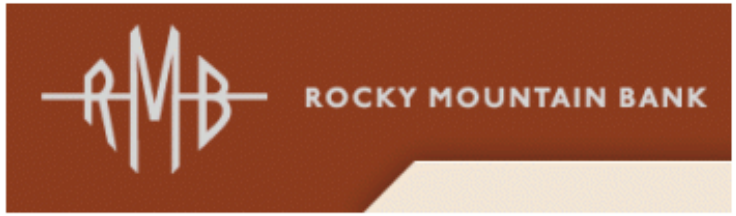
© 2009 Cisco Systems, Inc. All rights reserved. Cisco Public

Зачем все это нужно?

Bank Sends Sensitive E-mail to Wrong Gmail Address, Sues Google

By Kim Zetter September 21, 2009 | 8:20 pm | Categories: Breaches

A Wyoming bank sent an e-mail containing sensitive customer data to the wrong Gmail account, and now wants Google to reveal the identity of the account holder who received the data.



According to a court document in the case, in August a customer of the Rocky Mountain Bank asked a bank employee to send certain loan statements to a representative of the customer. The employee, however, inadvertently sent the e-mail to the wrong Gmail address. Additionally, the employee had attached a sensitive file to the e-mail that should not have been sent at all.

449 diggs

digg it

The attachment contained confidential information on 1,325 individual and business customers that included their names, addresses, tax identification or Social Security numbers and loan information.

After realizing what he'd done, the employee "tried to recall the e-mail without success."

When that didn't work, the employee sent a second e-mail to the recipient instructing the person to delete the e-mail and attachment "in its entirety" without opening or reviewing it. The employee also asked the recipient to contact the employee to "discuss his or her actions."

Silence ensued.

That's when the bank sued Google to identify the recalcitrant recipient.

© 2009 Cisco Systems, Inc. All rights reserved. Cisco Public

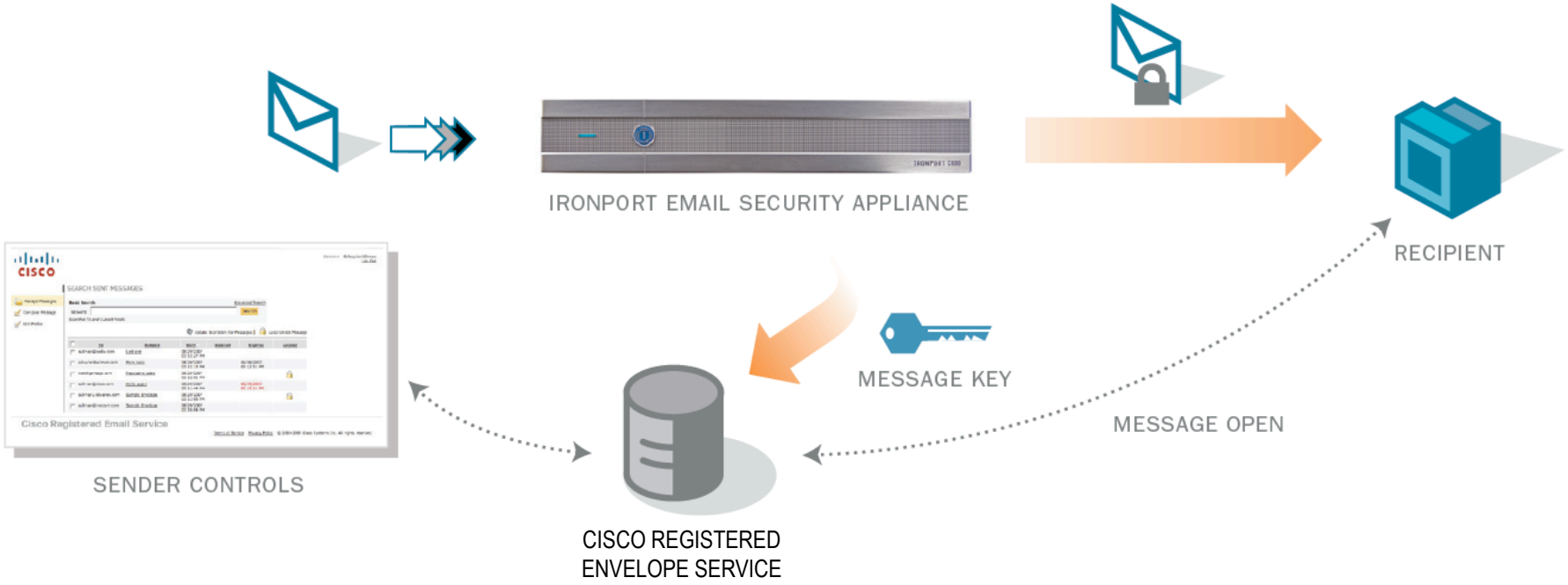
Email. Архитектура безопасности.

Безопасность входящих сообщений, контроль исходящих

© 2009 Cisco Systems, Inc. All rights reserved. Cisco Public

Шифрование Email Cisco IronPort

Легко для отправителя. . .



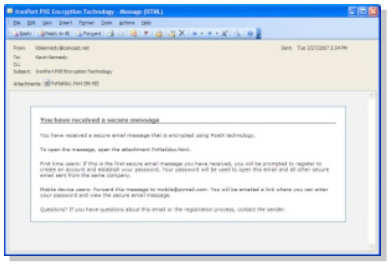
- Автоматизированное управление ключами
- Не требуется дополнительное ПО на рабочей станции пользователя
- Можно легко и быстро отослать на любой адрес

© 2009 Cisco Systems, Inc. All rights reserved.

Шифрование Email Cisco IronPort

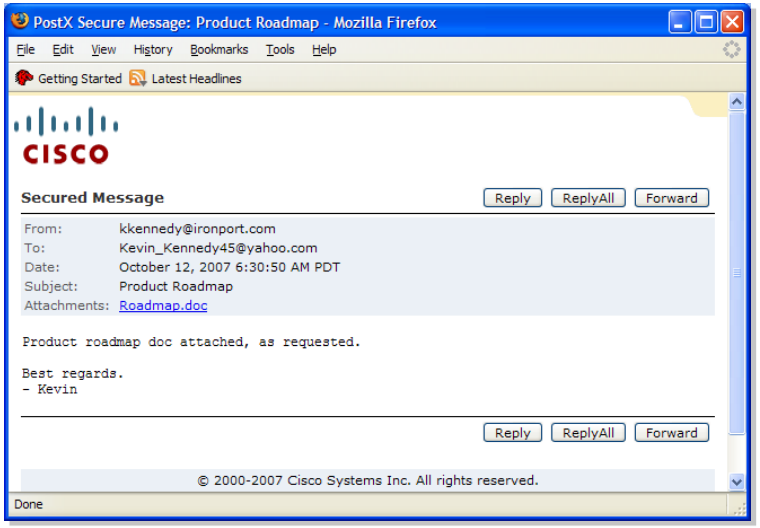
Легко для получателя. . .

1. Открыть присоединенный файл



2. Ввести пароль

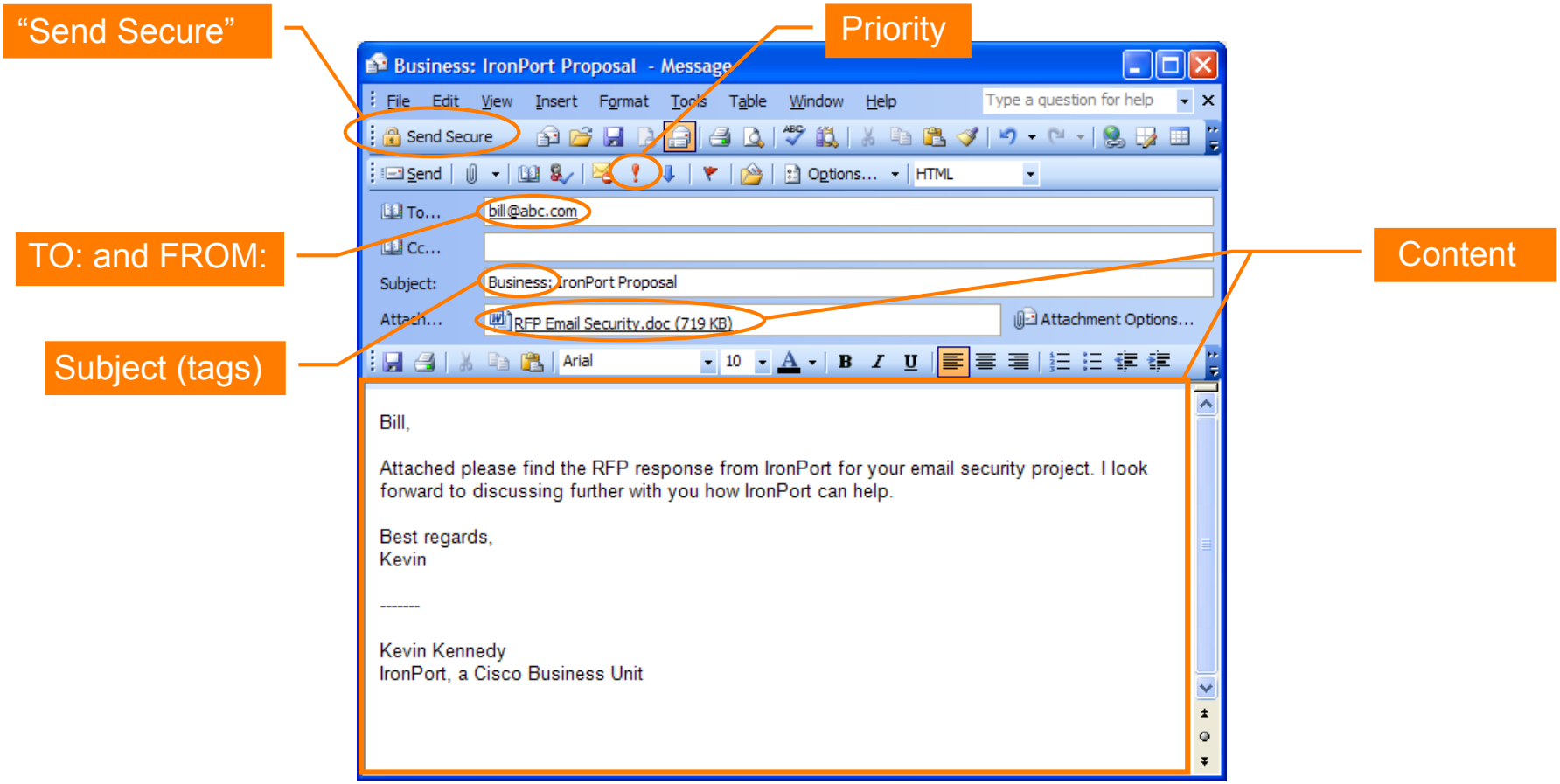
3. Просмотреть сообщение



© 2009 Cisco Systems, Inc. All rights reserved.

Гибкость и простота

Все из одного почтового клиента

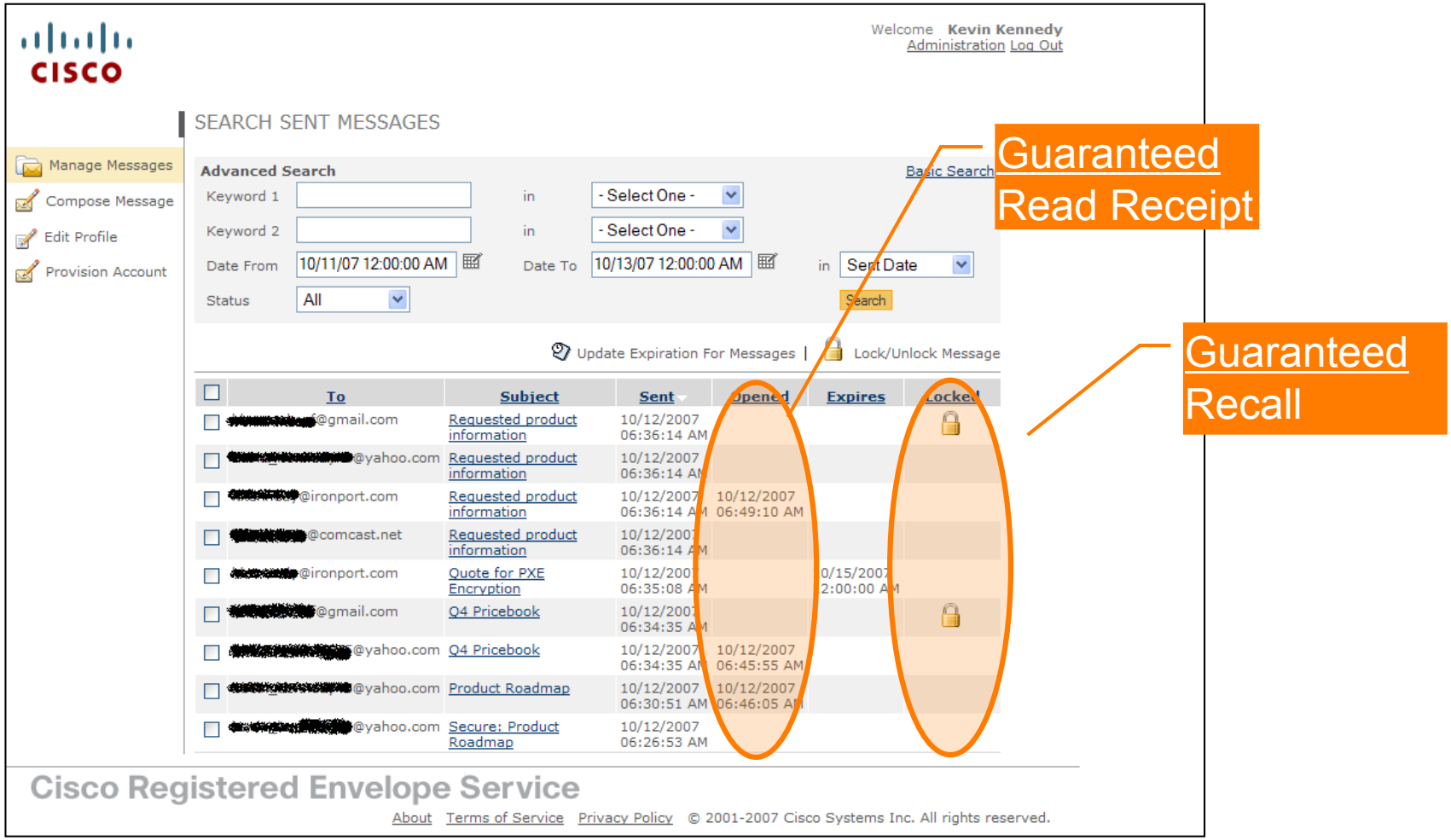


User Controls + Central Policy

© 2009 Cisco Systems, Inc. All rights reserved. Cisco Public

Email бизнес-класса

Полный контроль сообщения



© 2009 Cisco Systems, Inc. All rights reserved. Cisco Public

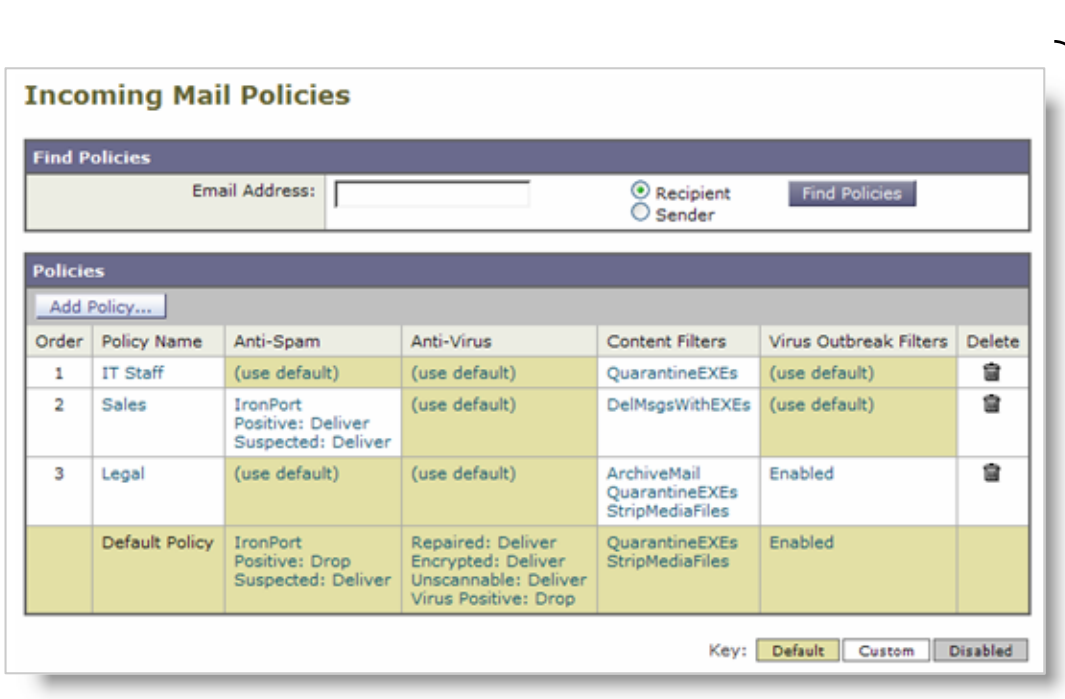
Email. Архитектура безопасности.

Безопасность входящих сообщений, контроль исходящих

© 2009 Cisco Systems, Inc. All rights reserved. Cisco Public

Cisco IronPort Email Security Manager

Простая настройка политик для всей организации



Категории: домен, имя пользователя, LDAP

IT

- Разрешить все медиафайлы
- Исполняемые файлы в карантин

SALES

- Пометить и доставить спам
- Удалить исполняемые файлы

LEGAL

- Архивировать всю почту
- Virus Outbreak Filters запрещен для doc файлов

"IronPort Email Security Manager работает как одна мощная и гибкая консоль настройки, которая позволяет управлять всеми сервисами устройства, – PC Magazine

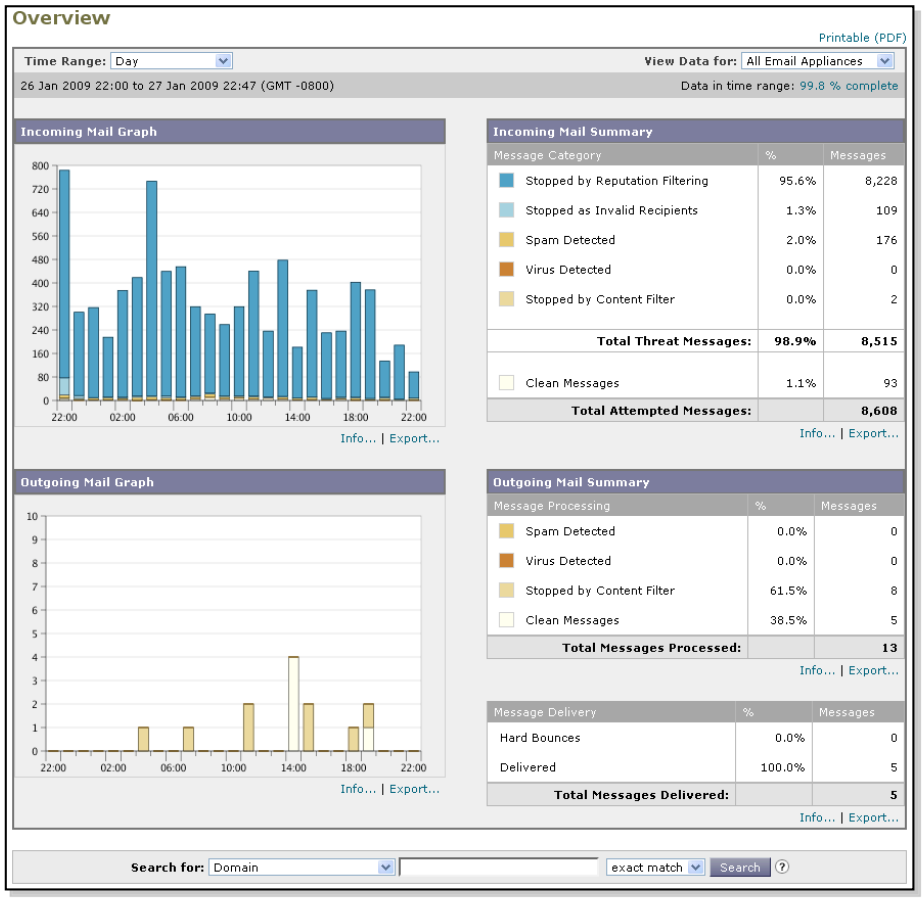
© 2009 Cisco Systems, Inc. All rights reserved. Cisco Public

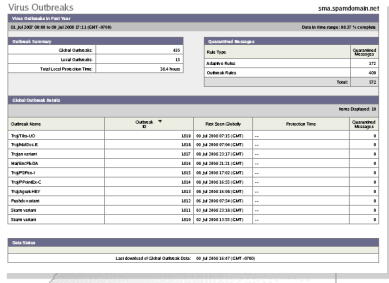
Отчеты

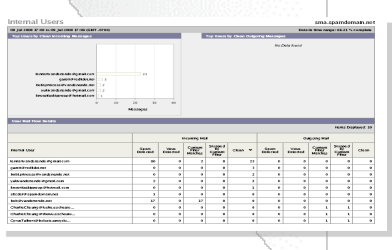
Унифицированная система построения отчетов для бизнеса

- Просмотр консолидированных отчетов для всей организации
- Подробности трафика email и угроз
- Иерархическая система отчетов

Consolidated Reports







Multiple data points

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

© 2009 Cisco Systems, Inc. All rights reserved. Cisco Public

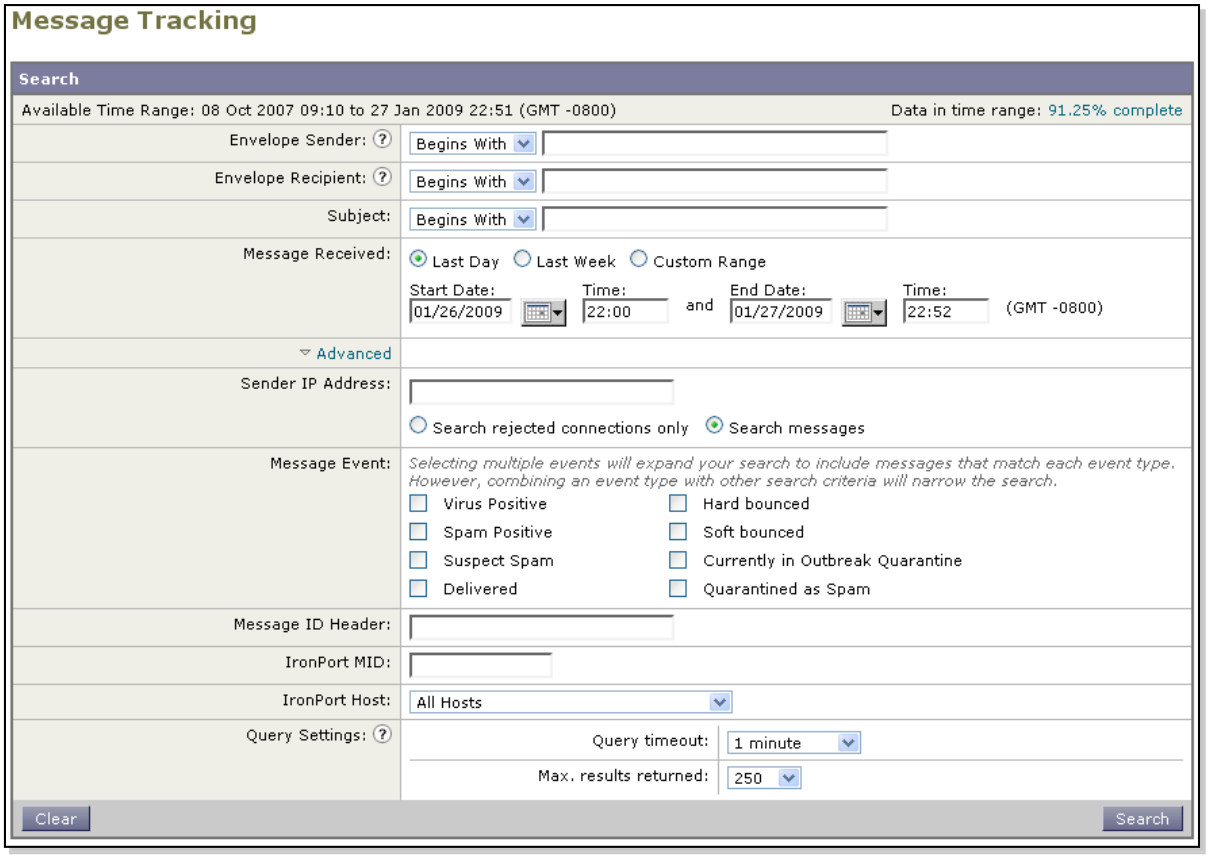
Поиск сообщений
Message Tracking

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

- ✓ Отслеживание индивидуальных сообщений

Кто еще получил такую почту?

- ✓ Расследование для того, чтобы гарантировать выполнение законодательных норм



© 2009 Cisco Systems, Inc. All rights reserved. Cisco Public

Email. Архитектура безопасности.

Безопасность входящих сообщений, контроль исходящих

© 2009 Cisco Systems, Inc. All rights reserved.

Cisco IronPort AsyncOS

Набор инструментов для защиты заказчиков

TLS шифрование
Шифрование на уровне шлюз-шлюз

HTML Sanitization
избежать поддельных URLs

SPF проверка
Проверка того, что письмо было отправено сервером, авторизованным отправлять почту для данного домена

Возможност LDAP
LDAP ссылки, несколько LDAP серверов, установка за 3 шага

DKIM подпись и проверка
Проверка отправителя

Bounce Verification
Избежать перенаправленных bounces

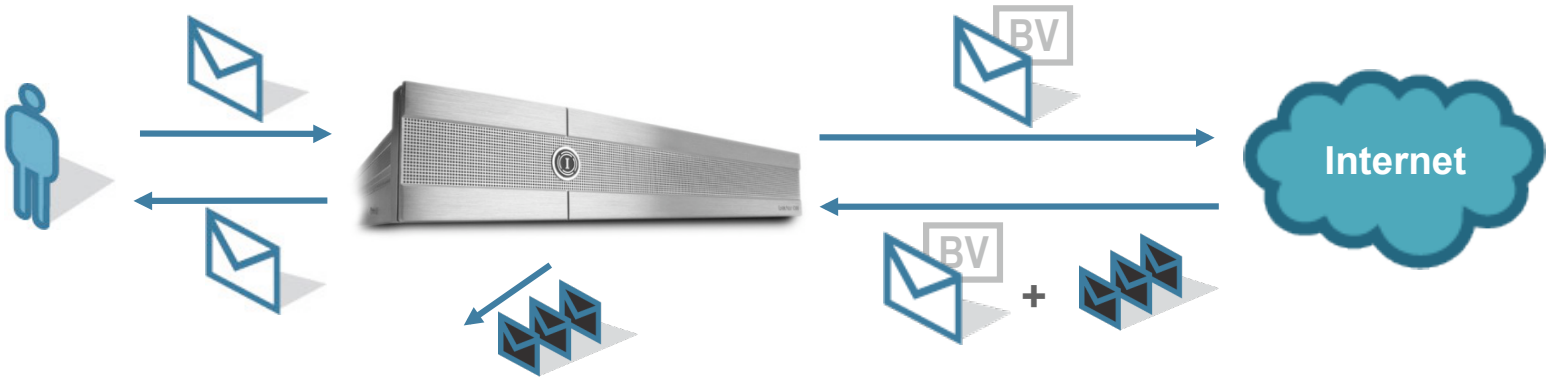
Спам-карантин, черные и белые списки для пользователей
Контроль пользователей

Проверка получателя
Удалить сообщения, которые отправлены на несуществующий адрес

© 2009 Cisco Systems, Inc. All rights reserved. Cisco Public

IronPort Bounce Verification™

Защищает от перенаправленных bounce-атак (Backscatter)



- **Вся исходящая почта специальным образом помечается для того, чтобы ее можно было идентифицировать при возвращении**
- **Прозрачно для пользователей, не требует никаких изменений в серверное ПО**
- **Помогает избеэать звонков в техподдержку от ничего не понимающих пользователей**
- **IronPort Technical “First"**

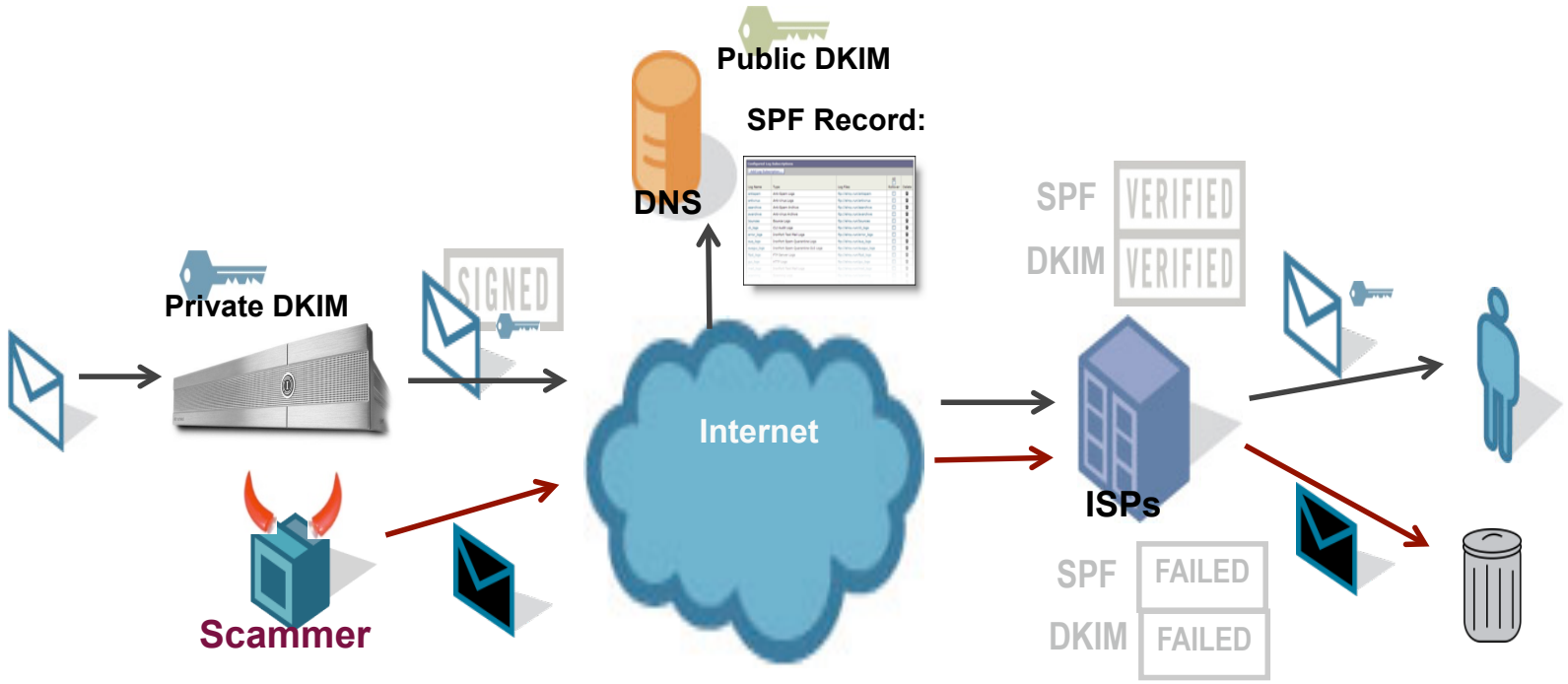
© 2009 Cisco Systems, Inc. All rights reserved. Cisco Public

Аутентификация Email

SPF u DKIM

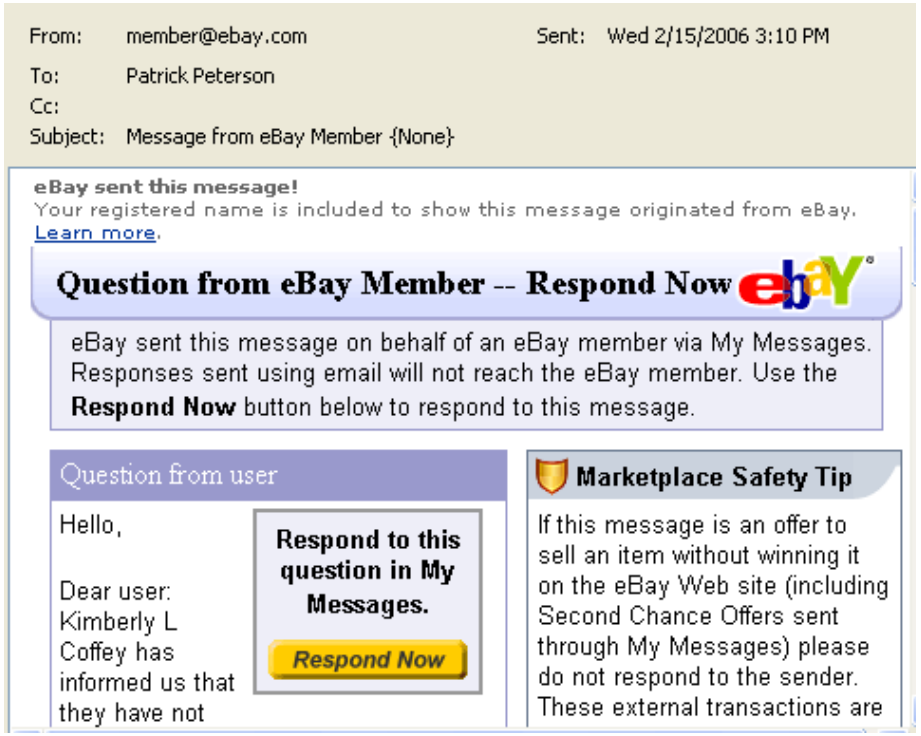
Sender Policy Framework (SPF) + DomainKeys Identified Mail (DKIM)

1. **Дополняющие технологии:** На основе обратного пути и методы криптографии
2. **Широко распространены:** >50% легитимных писем используют SPF/DKIM
3. **Блокируют фишинг-атаки:** Защита вашего бренда и заказчиков



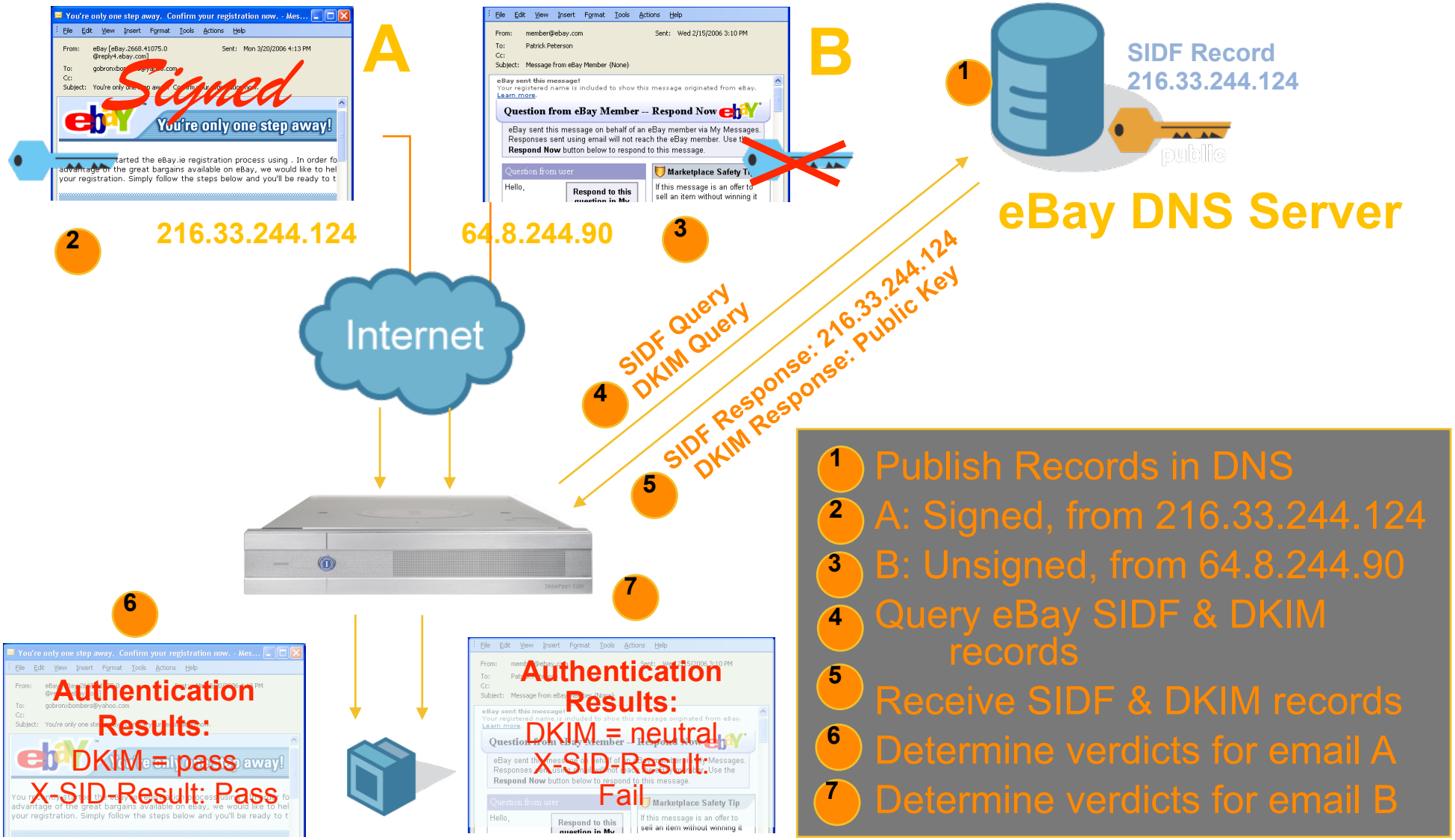
© 2009 Cisco Systems, Inc. All rights reserved. Cisco Public

Пример – какое сообщение настоящее?



© 2009 Cisco Systems, Inc. All rights reserved. Cisco Public

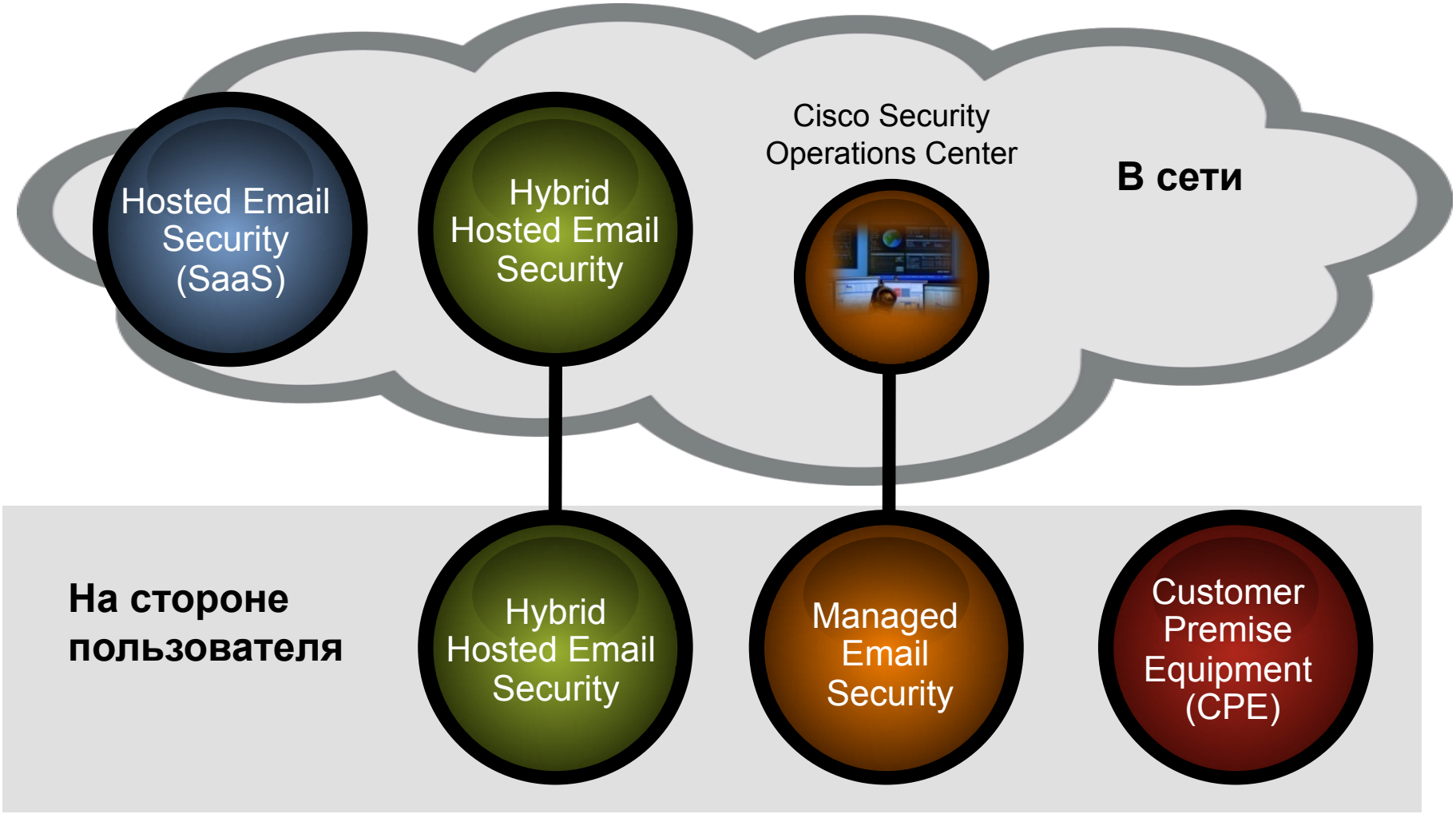
Пример: Как это работает?



1. Publish Records in DNS
2. A: Signed, from 216.33.244.124
3. B: Unsigned, from 64.8.244.90
4. Query eBay SIDF & DKIM records
5. Receive SIDF & DKIM records
6. Determine verdicts for email A
7. Determine verdicts for email B

© 2009 Cisco Systems, Inc. All rights reserved.

Набор гибких опций внедрения



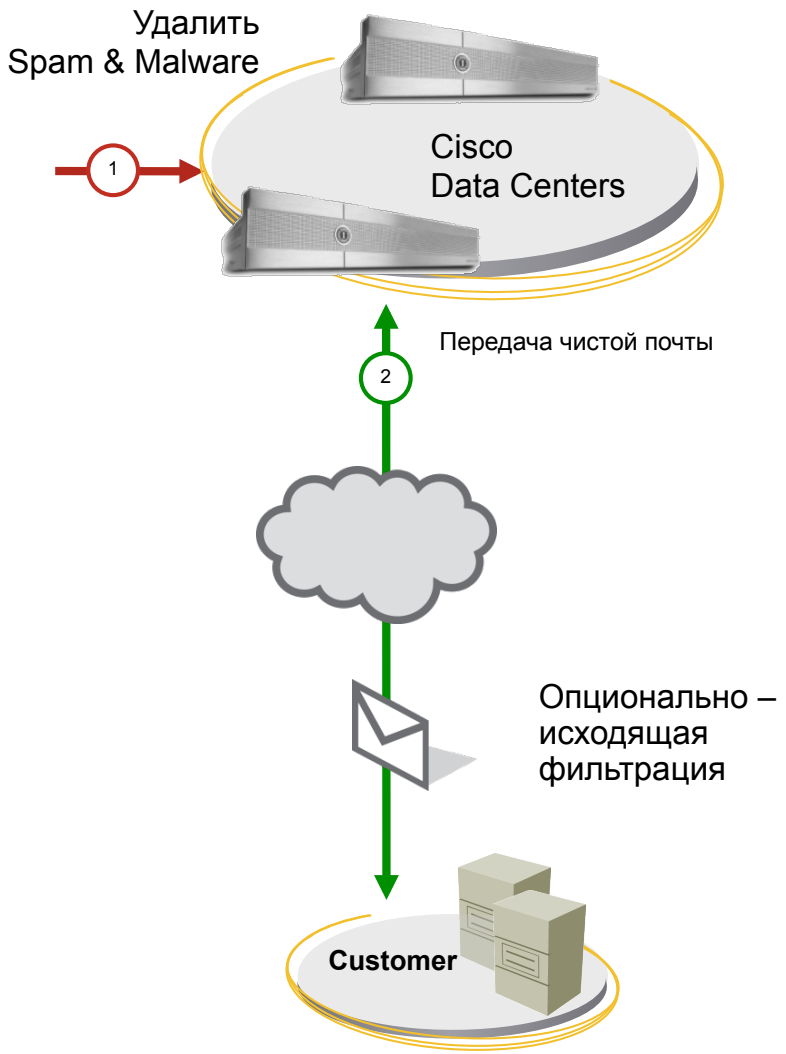
Common Policy | Centralized Reporting | Consistent Protection

© 2009 Cisco Systems, Inc. All rights reserved. Cisco Public

Hosted Email Security

Выделенное решение снижает нагрузку и ускоряет внедрение

- Безопасностьи Email в облаке снижает нагрузку на ЦОД
- «Выделенное» решение снижает риск общего сбоя (‘shared fate’ risk)
- Управляемая инфаструктура гарантирует производительность для будущего роста



© 2009 Cisco Systems, Inc. All rights reserved.

Когда это необходимо?

...

HOSTED

…снизить нагрузку на ЦОД…

…**получить эффективное решение hosted email**…

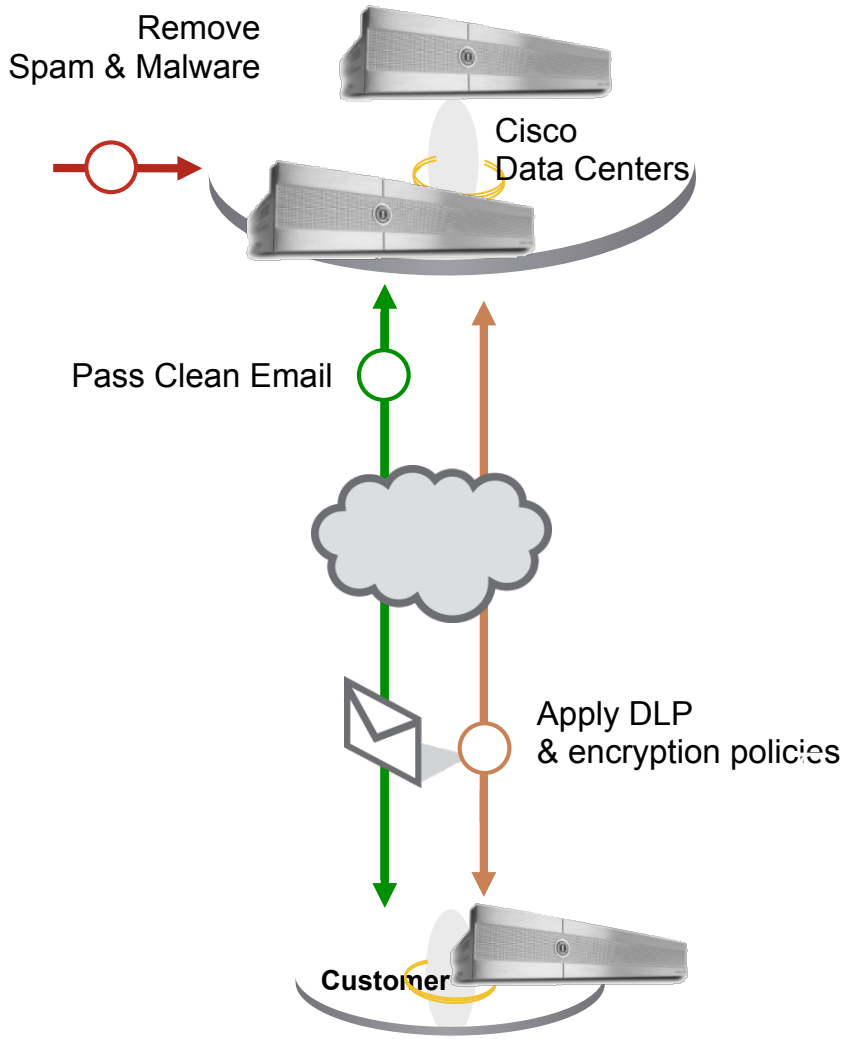
…отдать обработку email на аутсорс…

…не хочу терять контроль над устройствами…

Гибридный Hosted Email Security

Оптимальный дизайн, максимальная гибкость

- Гибридный дизайн подразумевает разнесенное управление – на площадке и в облаке
- Устройства на площадке пользователя контролируют исходящую почту, политики DLP и шифрование

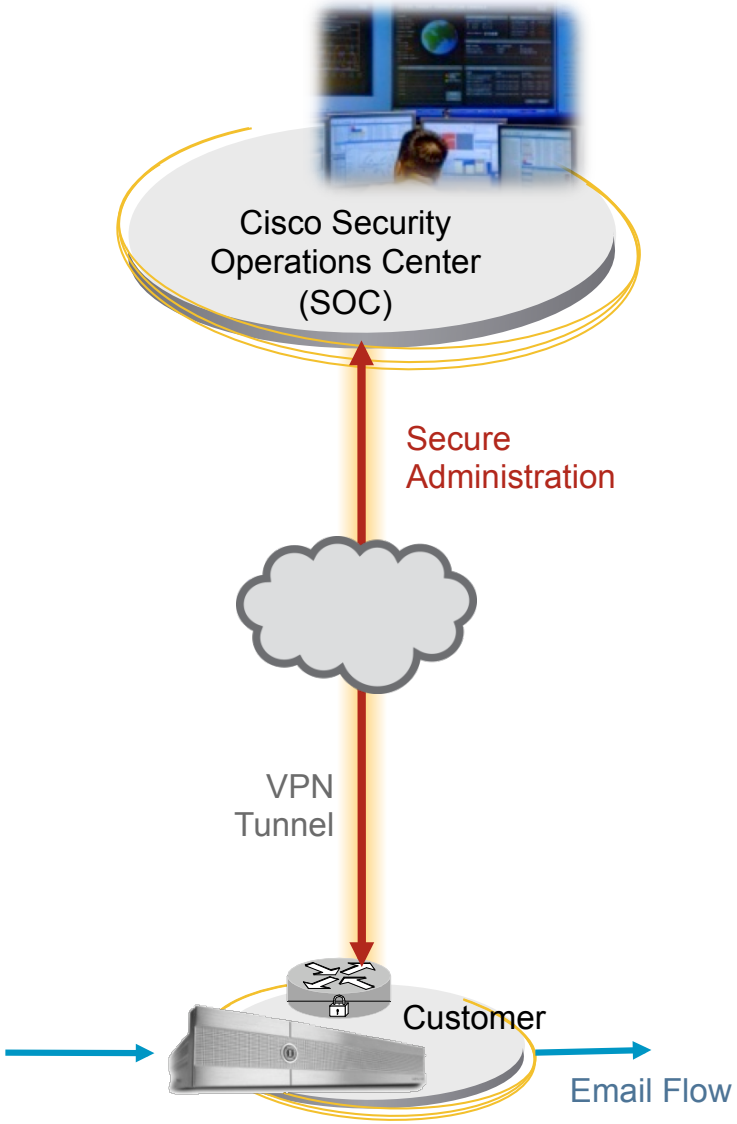


© 2009 Cisco Systems, Inc. All rights reserved.

Managed Email Security

Возложите задачу обеспечения безопасности email на экспертов

- Самый высокий уровень аутсорсинга.
- Предсказуемая модель стоимости
- Сервисная архитектура позволяет приложениям располагаться на площадке пользователя
- Cisco SOC предлагает удаленный мониторинг и управление в режиме 24/7



© 2009 Cisco Systems, Inc. All rights reserved. Cisco Public

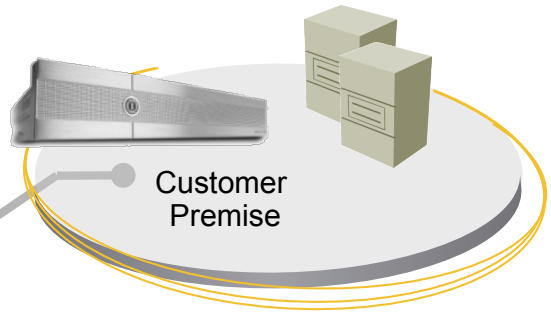
Гибкость в работе

Объединенное управление

Customer

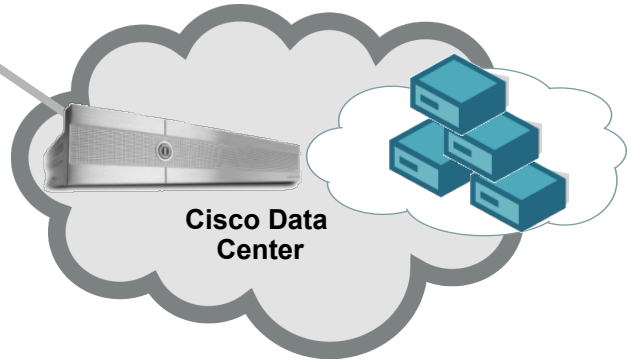
Message Tracking | Ticket Management | Reporting

Reporting



Shared Access & Control

Configuration



Cisco

System Health | System Upgrades | Config Changes

© 2009 Cisco Systems, Inc. All rights reserved.

Внедрение

© 2009 Cisco Systems, Inc. All rights reserved.

Hardware Specs

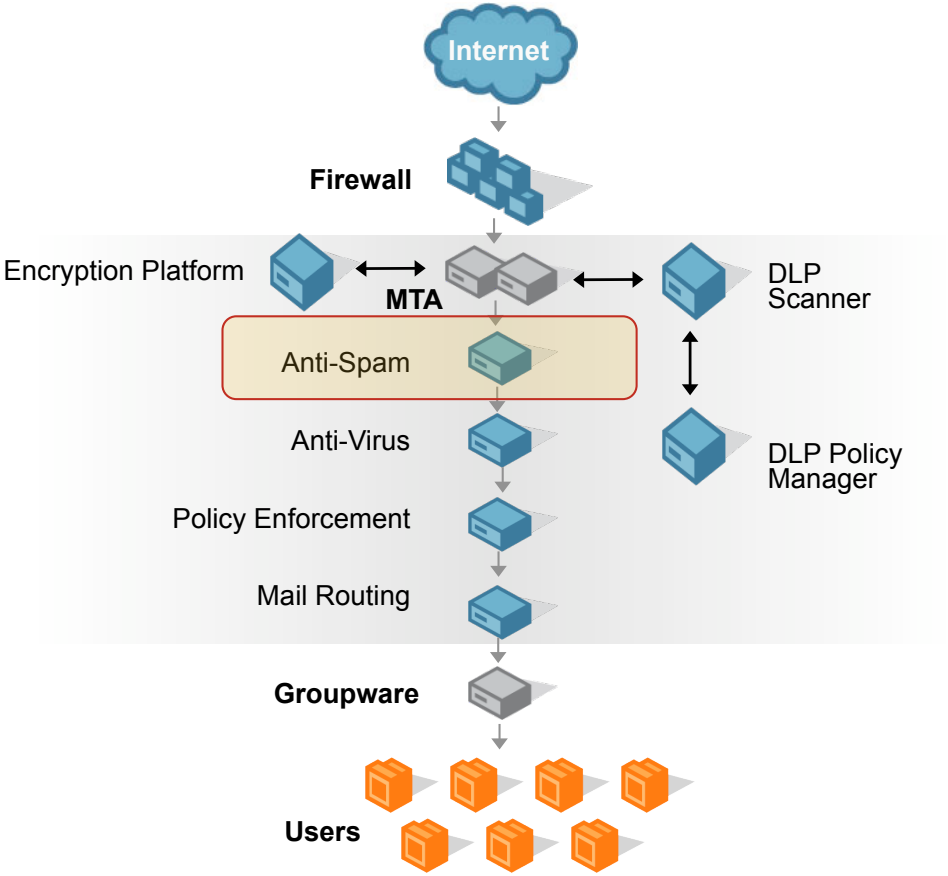
C-Series, X-Series

MODEL	C160 1RU	C360 2RU	C660 2RU	X1060 2RU
CPU	1 X 2 Pentium 2.33 G	2x2 Xeon 2.33 G	2x4 Xeon 2.33 G	2x4 Xeon 2.833 G
RAM	4GB	4GB	4GB	4GB
Disk	2 x 250 GB RAID 1	2 x 300 GB RAID 1	4 x 300 GB RAID 10	6 x 300 GB RAID 10
Queue	10GB	35GB	70GB	70GB
PSU	1	2	2	2
Ethernet	2	3	3	3 (fiber option)

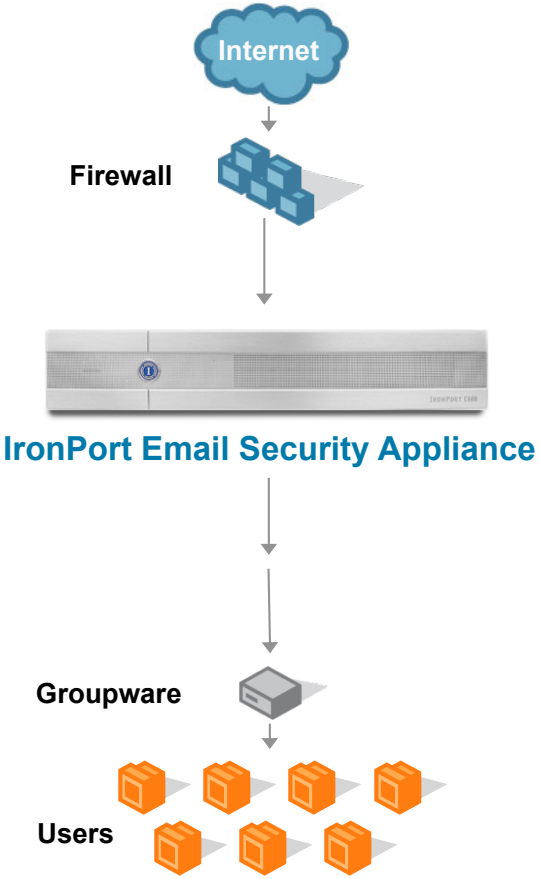
© 2009 Cisco Systems, Inc. All rights reserved. Cisco Public

Внедрение IronPort

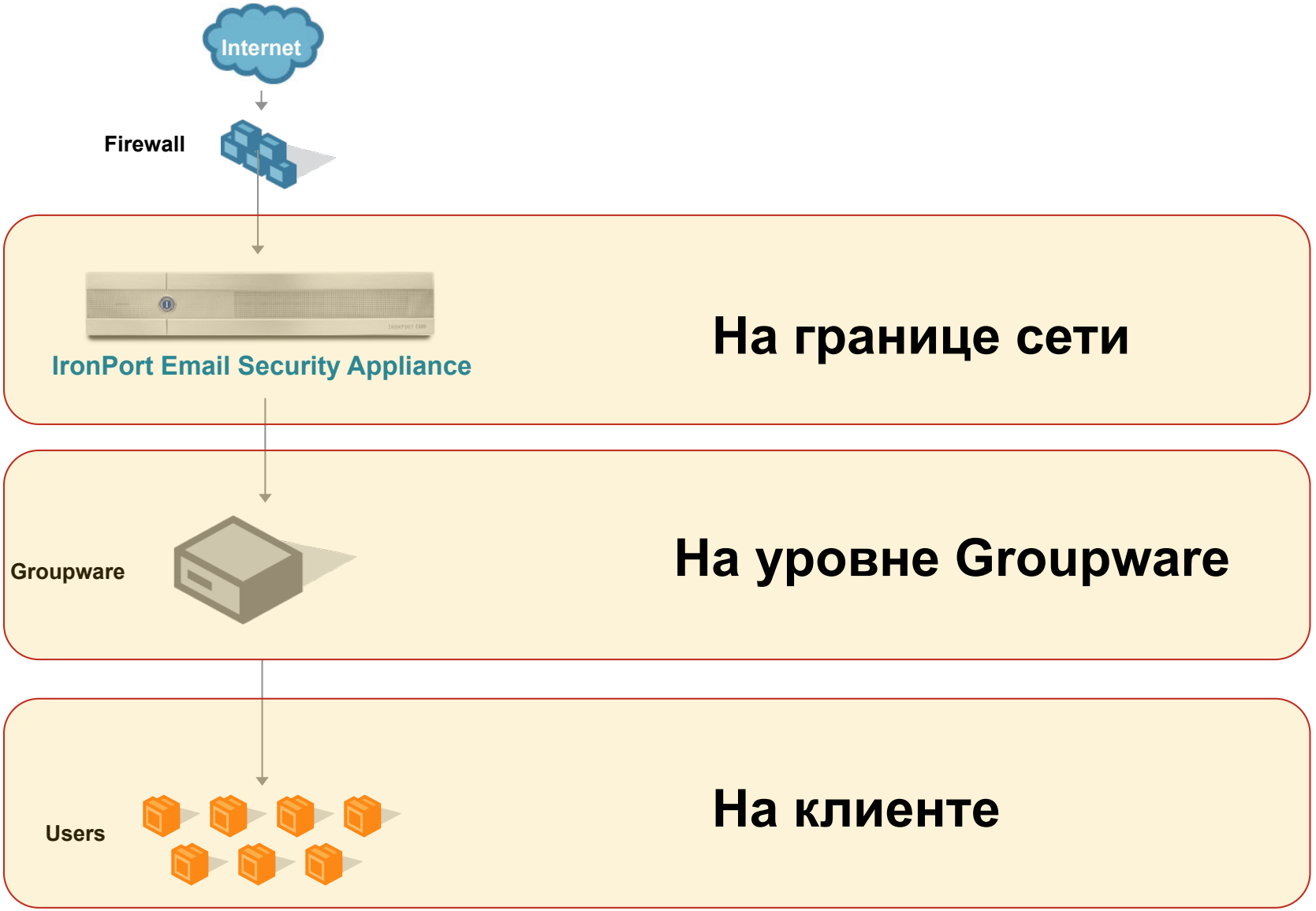
Before IronPort



After IronPort



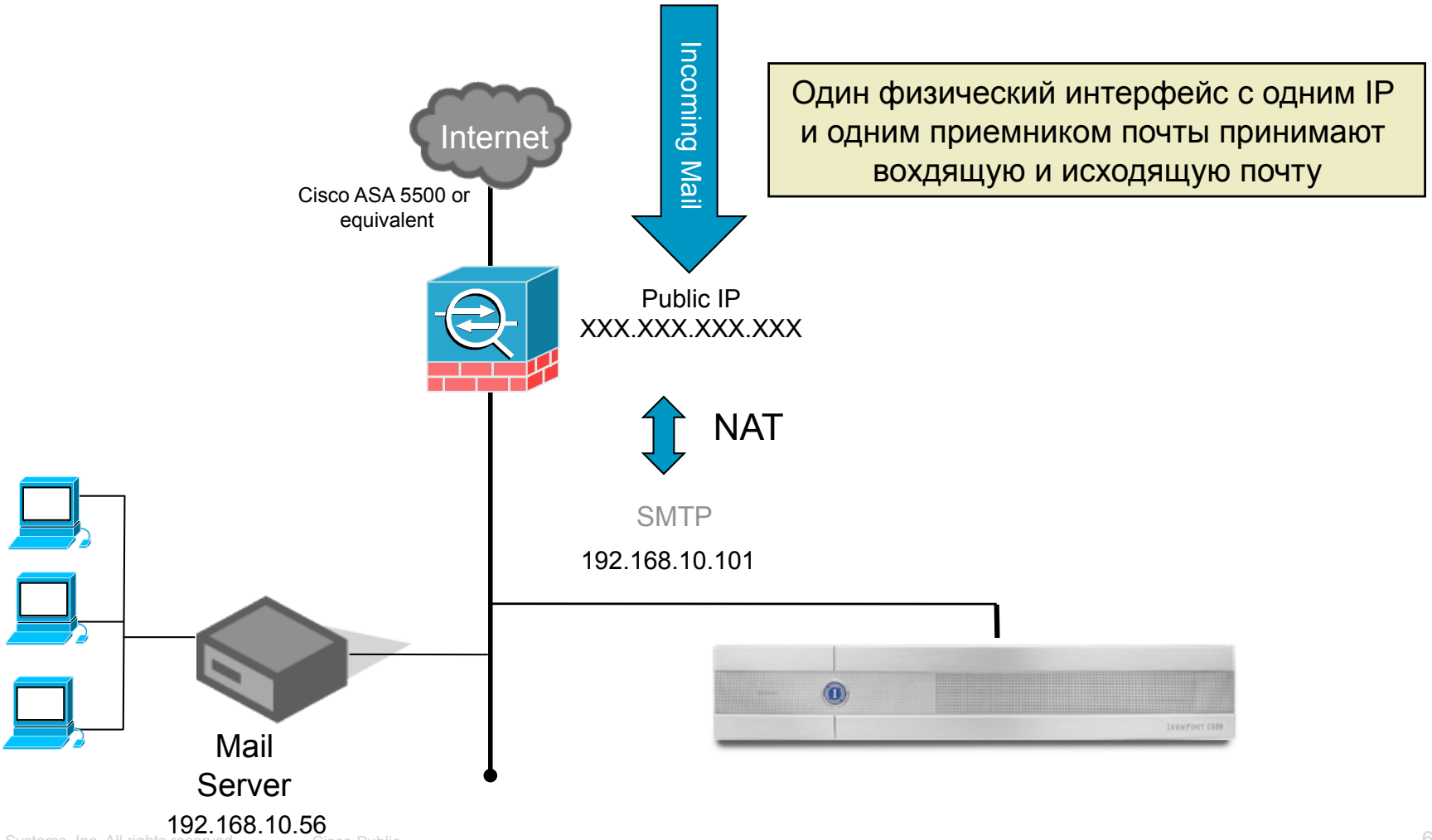
Где мы будем фильтровать?



© 2009 Cisco Systems, Inc. All rights reserved.

Внедрение с одним интерфейсом

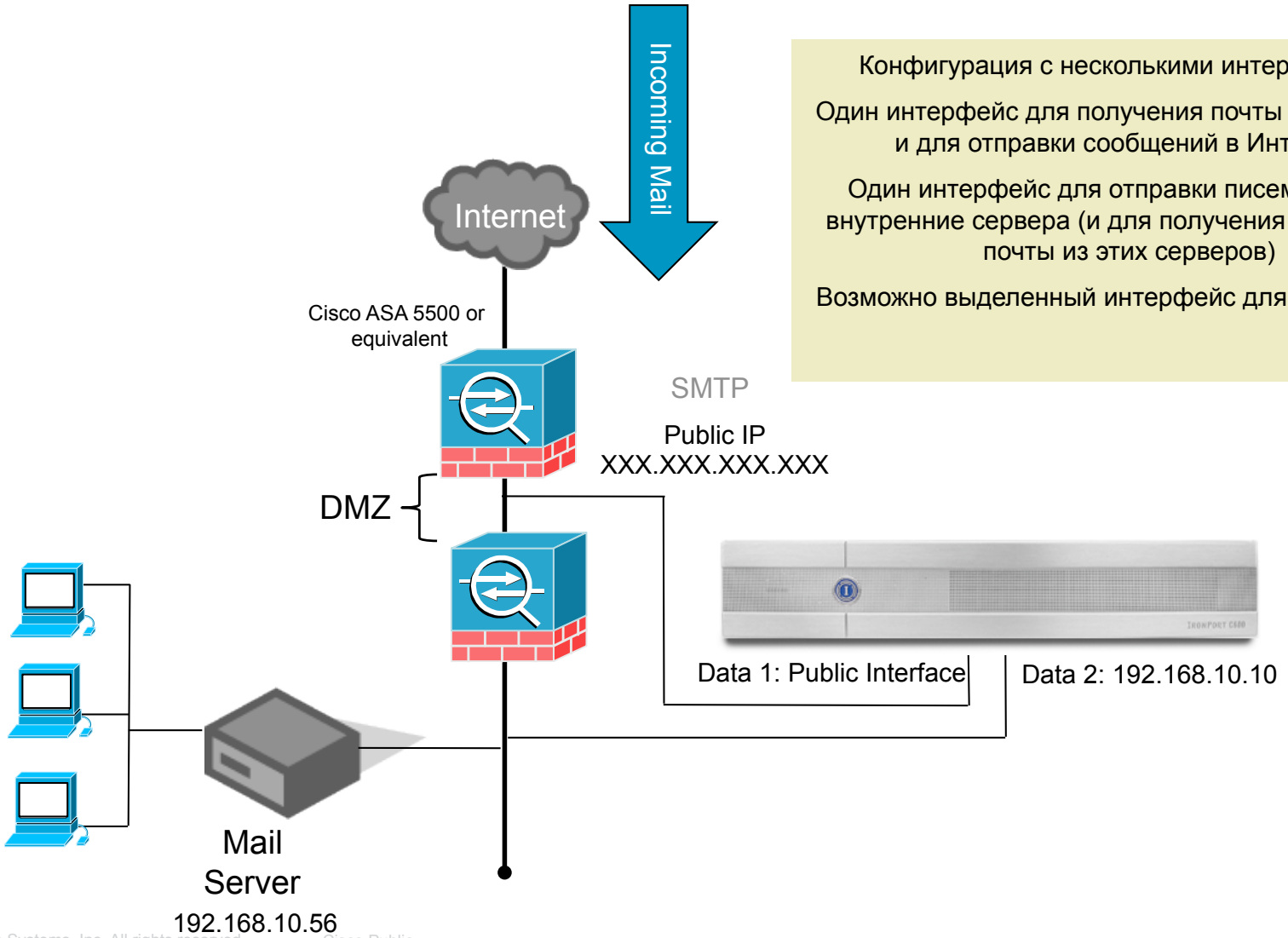
Сохраняются первоначальные IP и MX записи. Правила МЭ перенаправляют публичный IP на приватный IP C-серии. Внутренние почтовые сервера маршрутизируют исходящую почту на приватный IP C-серии. Не требуется создание отдельного DMZ.



© 2009 Cisco Systems, Inc. All rights reserved. Cisco Public

Внедрение с двумя интерфейсами и DMZ

Мне нужен почтовый сервер с интерфейсом в DMZ для приема электронной почты. Этот интерфейс не может отправлять почту внутрь сети.



Конфигурация с несколькими интерфейсами

Один интерфейс для получения почты из Интернет и для отправки сообщений в Интернет.

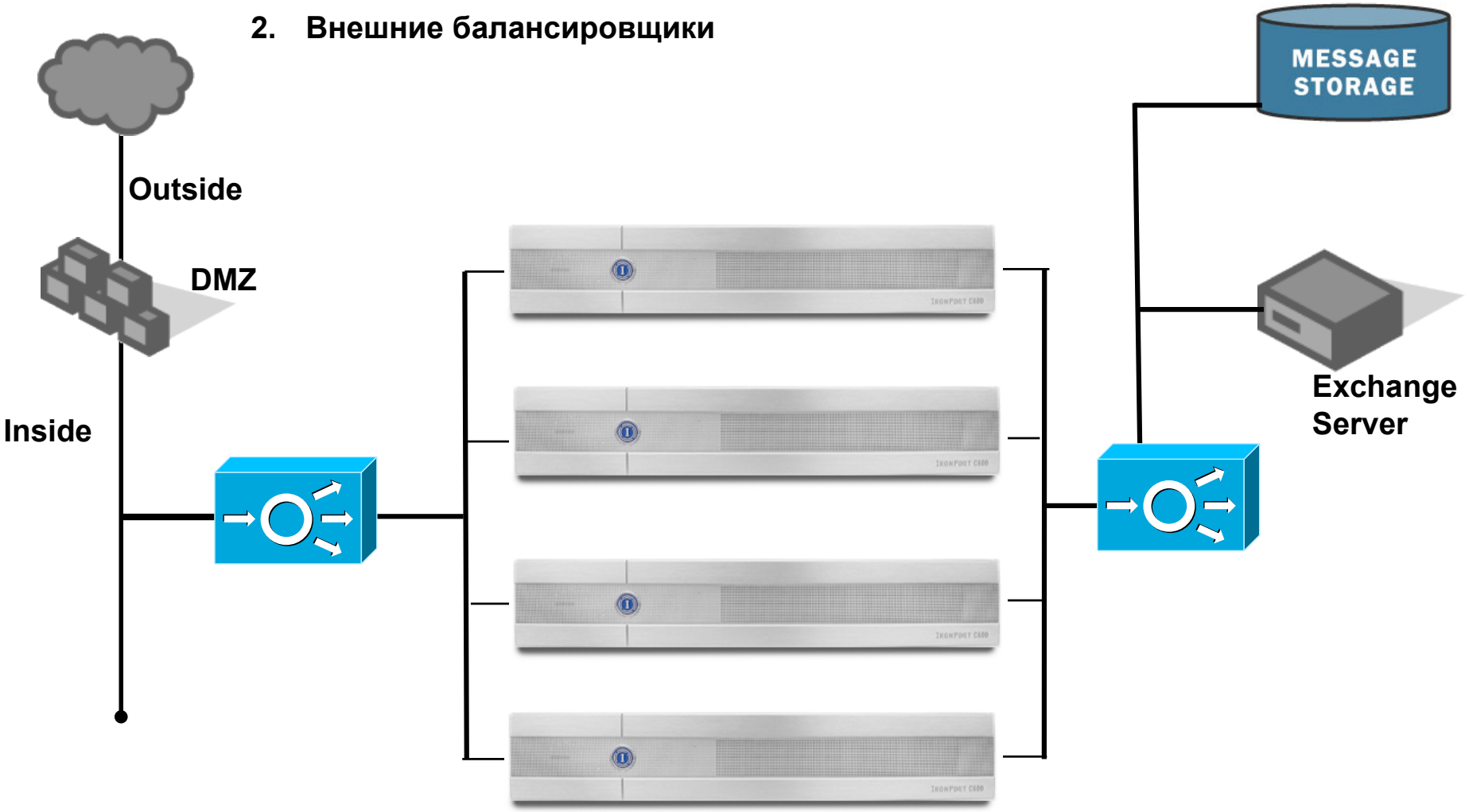
Один интерфейс для отправки писем на ваши внутренние сервера (и для получения исходящей почты из этих серверов)

Возможно выделенный интерфейс для управления.

© 2009 Cisco Systems, Inc. All rights reserved. Cisco Public

Отказоустойчивость и балансировка нагрузки

1. Несколько MX записей в DNS с одинаковым preference
2. Внешние балансировщики



© 2009 Cisco Systems, Inc. All rights reserved. Cisco Public

95% of companies who try Cisco IronPort become customers.

Contact:
Your Cisco IronPort Rep

© 2009 Cisco Systems, Inc. All rights reserved.

Вопросы и Ответы

© 2009 Cisco Systems, Inc. All rights reserved.