



Cisco IronPort

Новые горизонты в обеспечении безопасности электронной почты



Pavel Rodionov

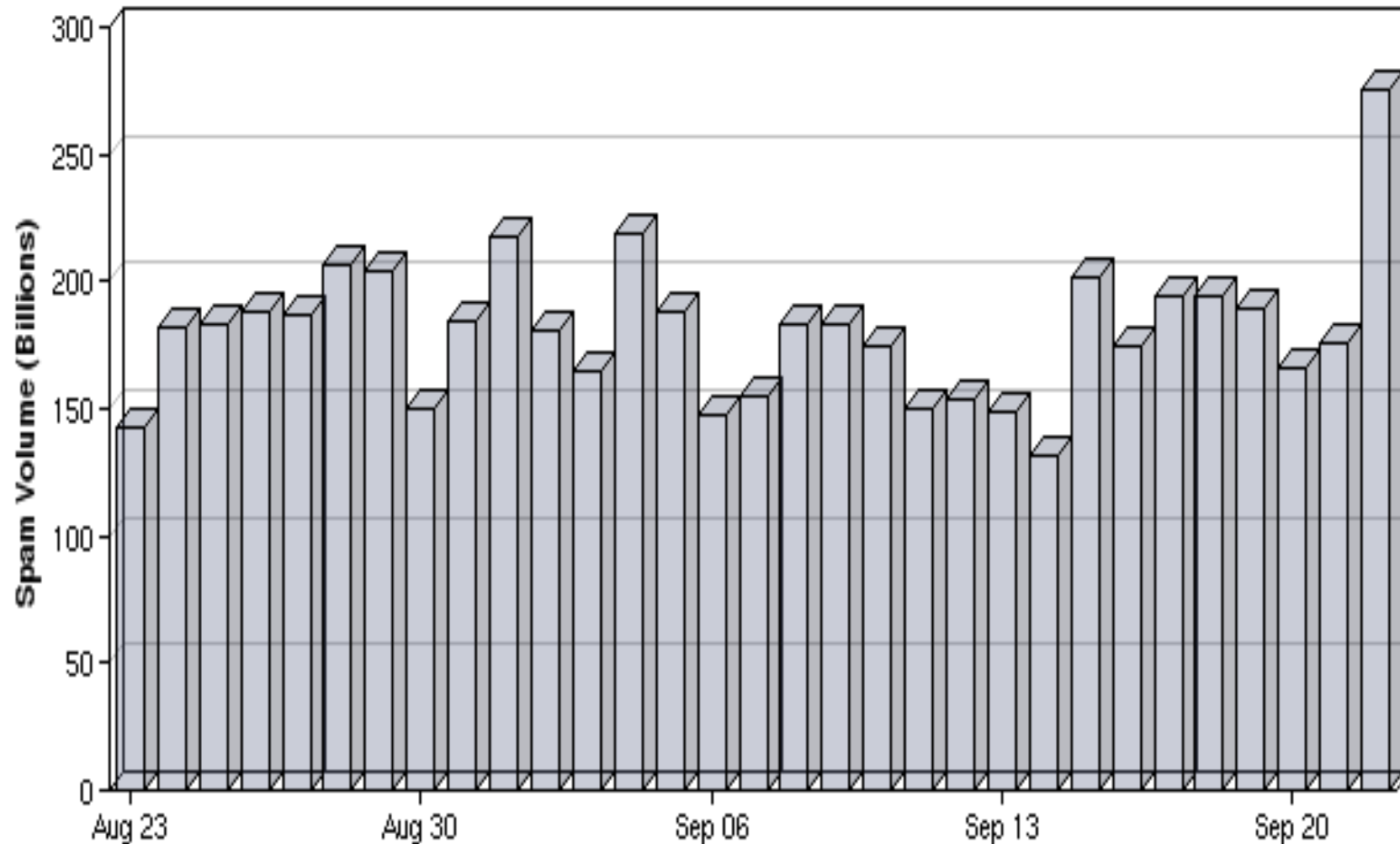
Systems Engineer

Security Technology BU

prodiono@cisco.com

Email. Угроза безопасности

Больше спама, больше спамеров



Source: Cisco Threat Operations Center

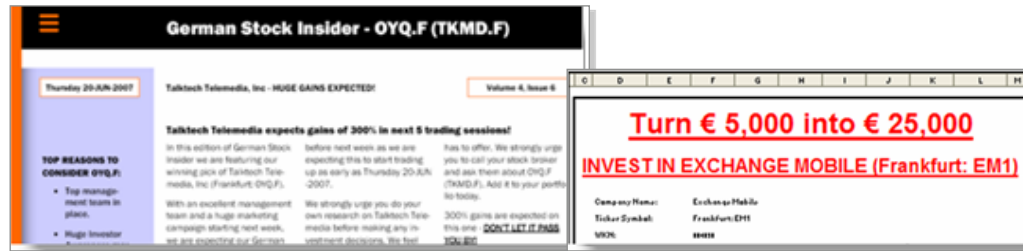
© 2009 Cisco Systems, Inc. All rights reserved.

Cisco Public

Спам усложняется



TEXT SPAM



ATTACHMENT SPAM
(PDF, EXCEL, MP3)



2005

2007

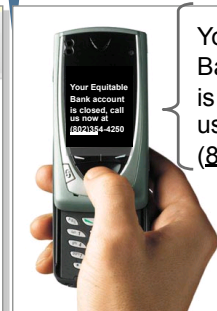
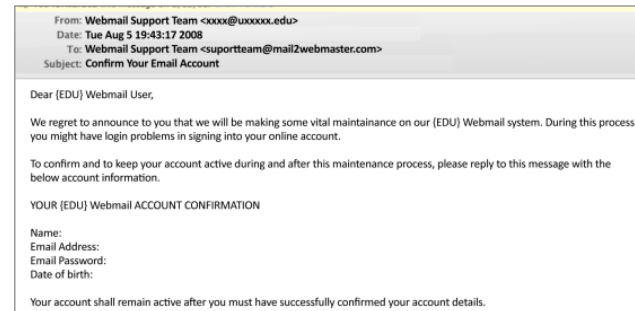
2006

2008

IMAGE SPAM



TARGETED ATTACKS

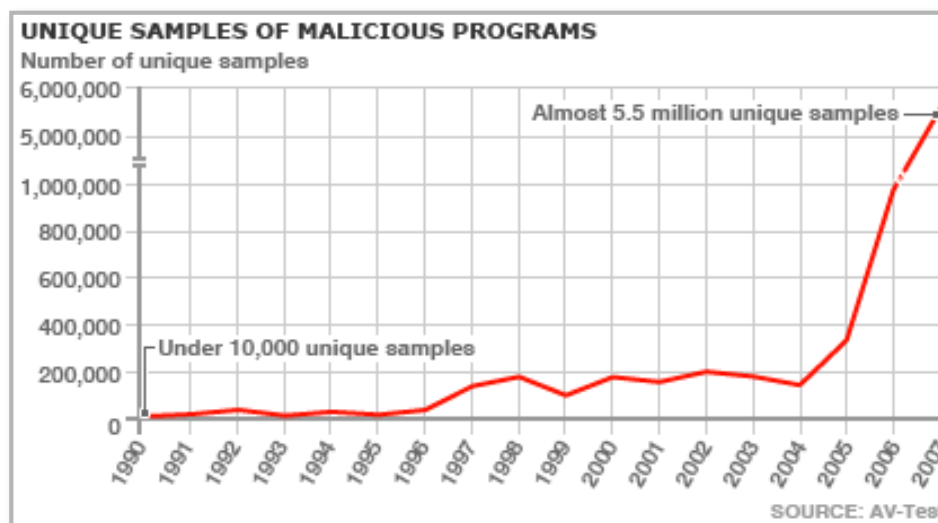
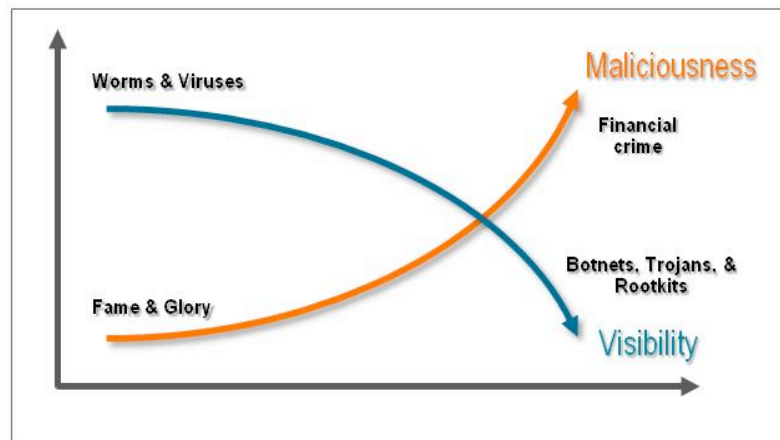


Your Equitable Bank account is closed, call us now at (802)354-4250

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

Malware на подъёме

Email – основная среда распространения



Утечка данных – еще одна проблема

Увеличивается количество отчетов, свидетельствующих об утечке данных

Errant e-mails compromise hundreds of student IDs

Student Financial Services sends 632 registration block notifications containing students' Social Security 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-mails were actually sent out late Tuesday evening. These e-mails contained the student IDs of the 632 other students

Основная среда, через которую происходит утечка -- email

many different vectors of DCP 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)

Новые законы выдвигают новые требования

Privacy & Security Task Force ADVISOR

October 7, 2008

States Adopting Aggressive New Privacy and Data Security Laws and Regulations

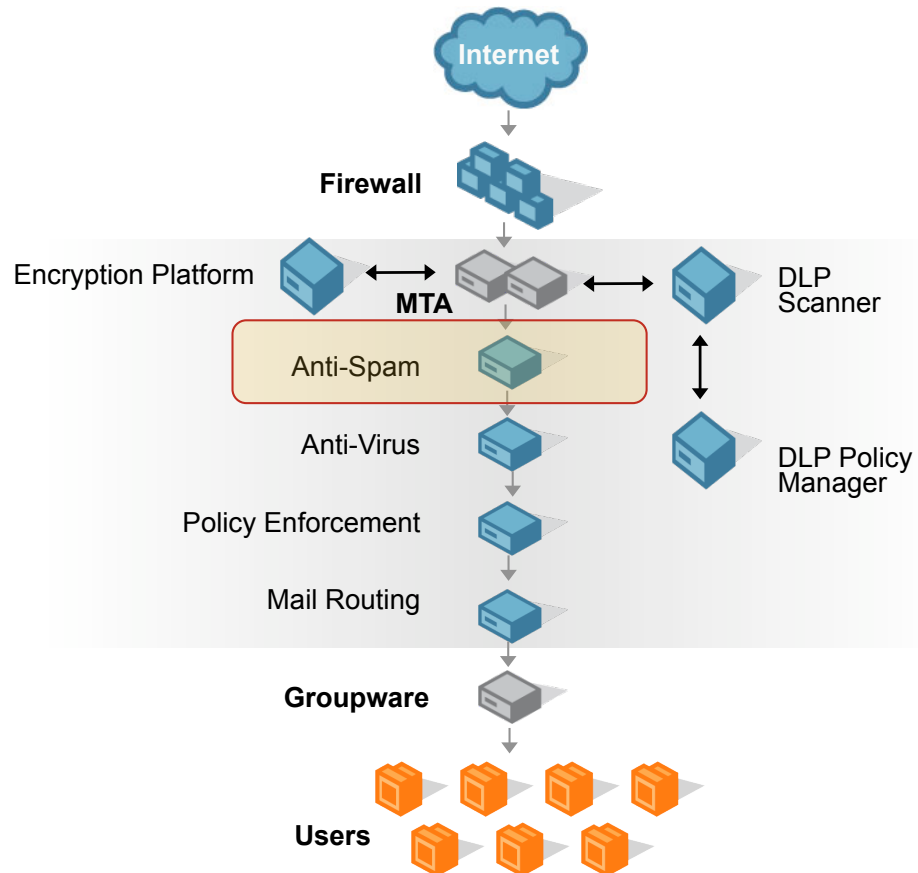
Нагрузка на администраторов

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

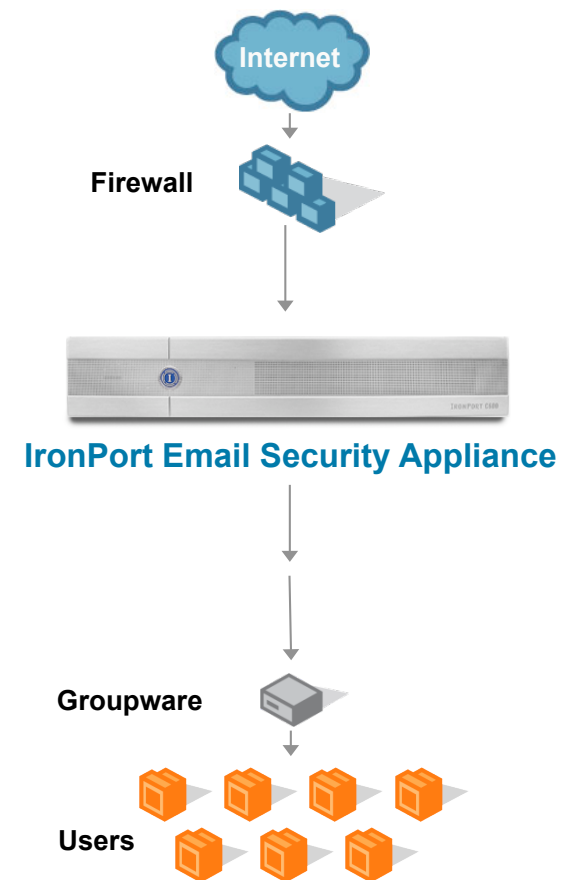


IronPort Email Security Appliance

Before IronPort

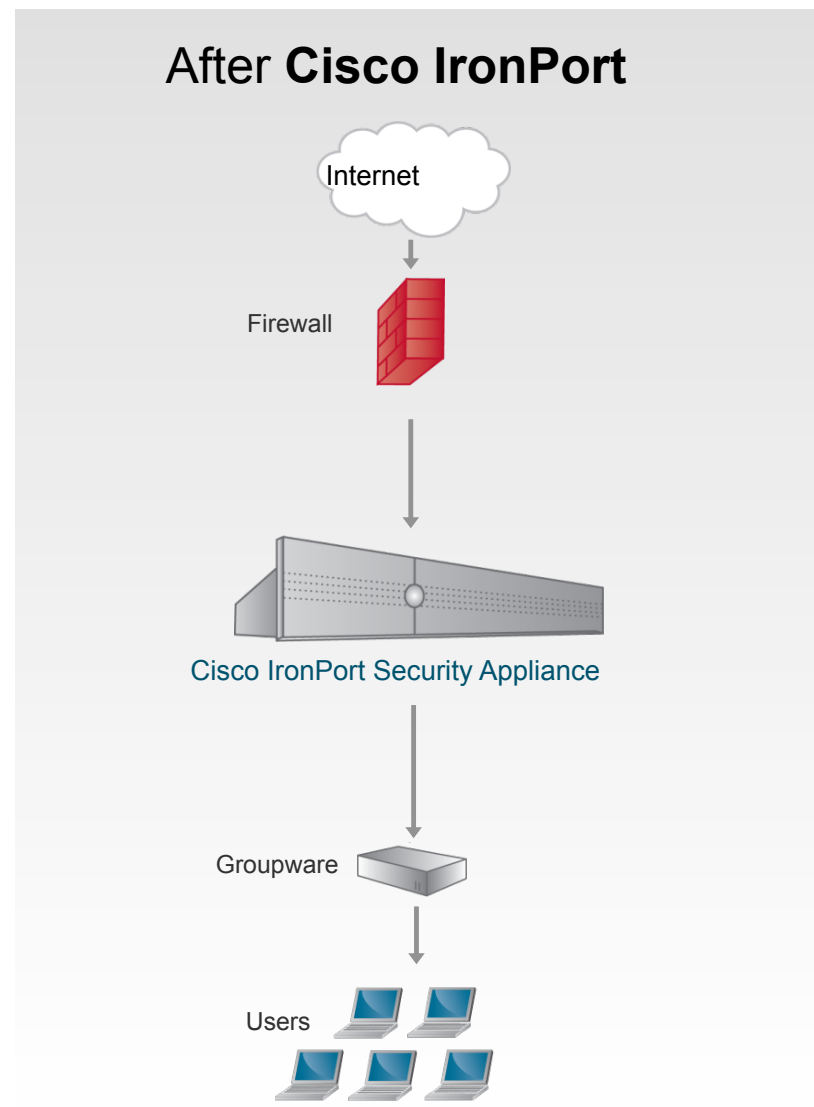
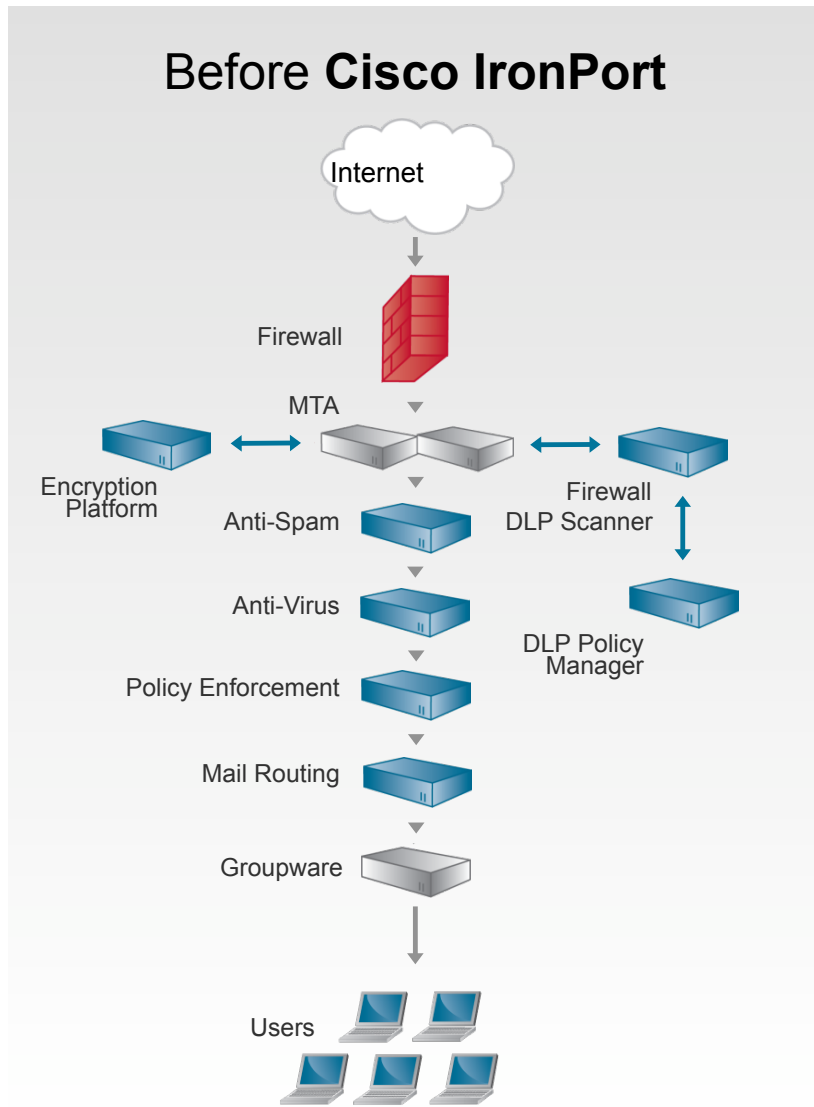


After IronPort



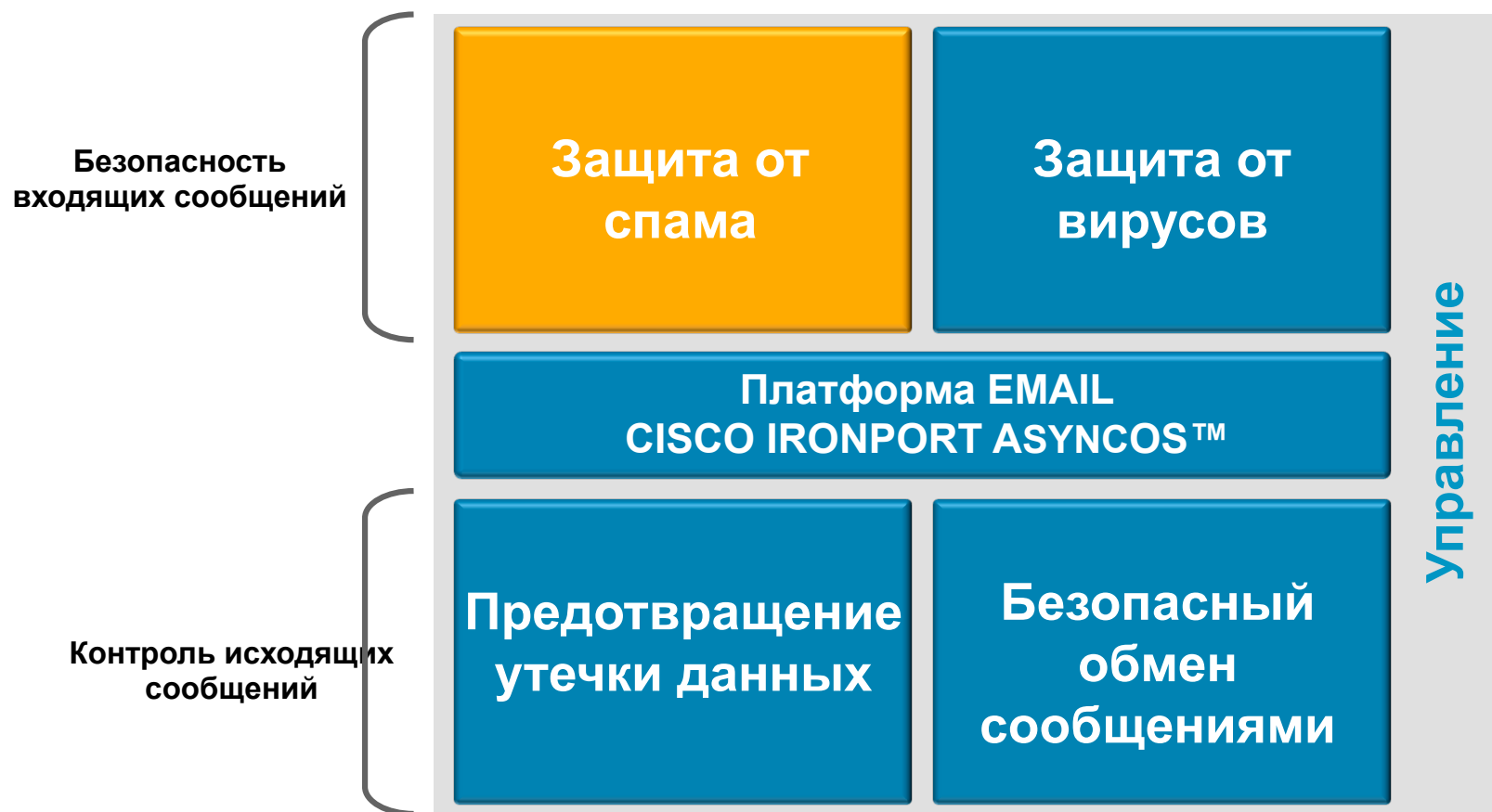
IronPort Email Security Solution

“Set and Forget”

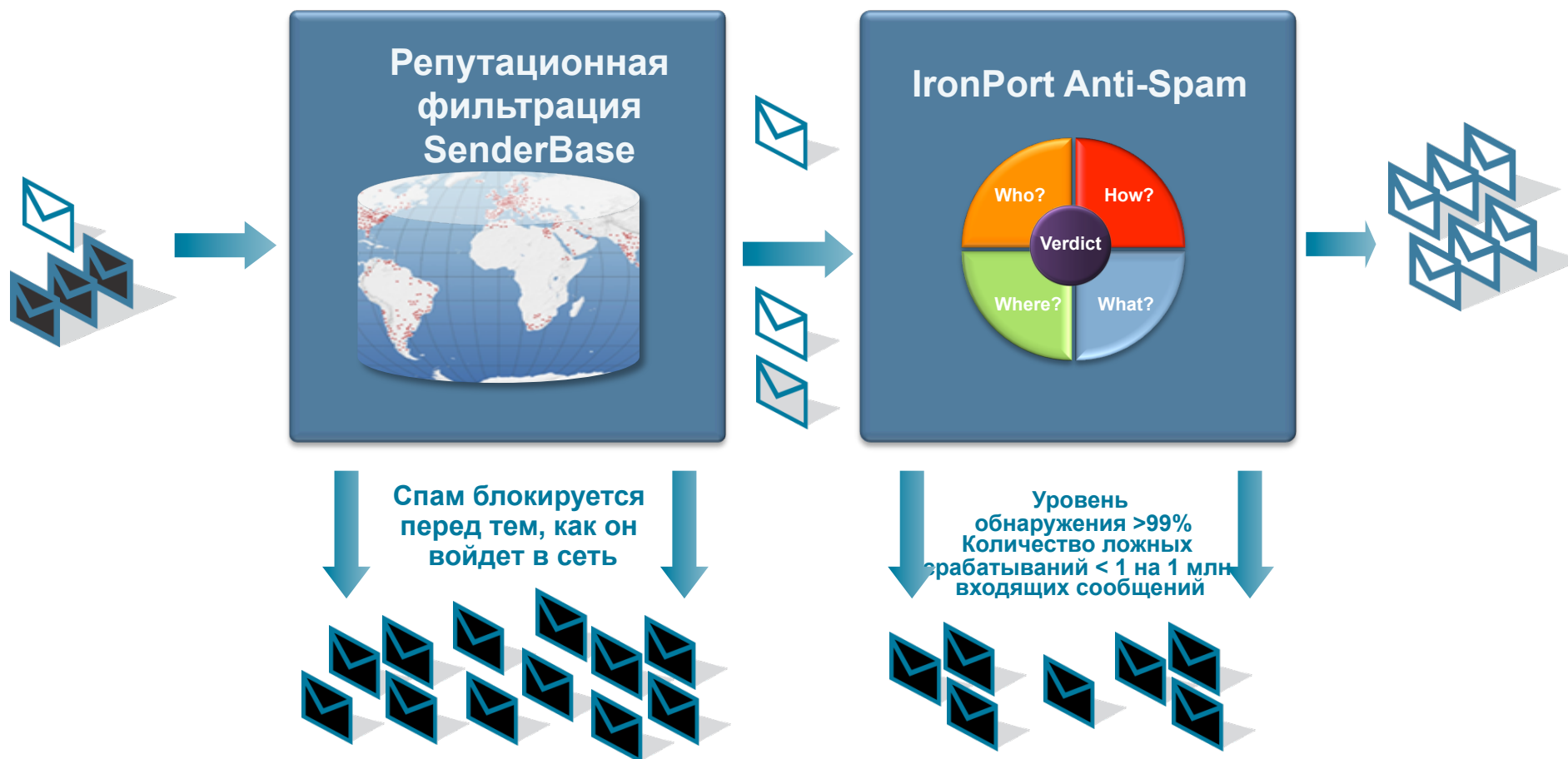


Email. Архитектура безопасности.

Безопасность входящих сообщений, контроль исходящих



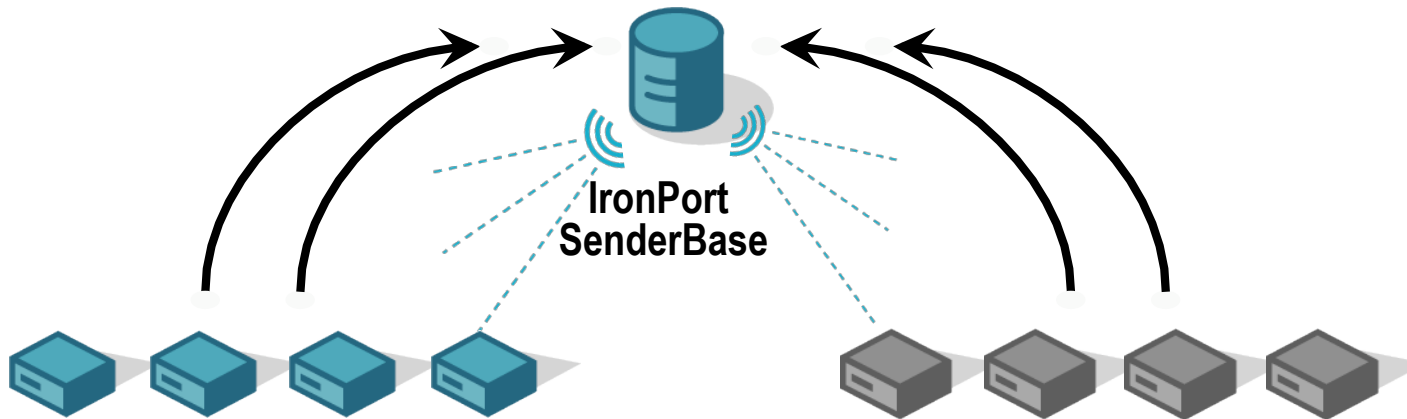
Анти-спам в деталях



IronPort SenderBase

Быстрое и точное обнаружение угроз

Объединенный анализ Email & Web трафика



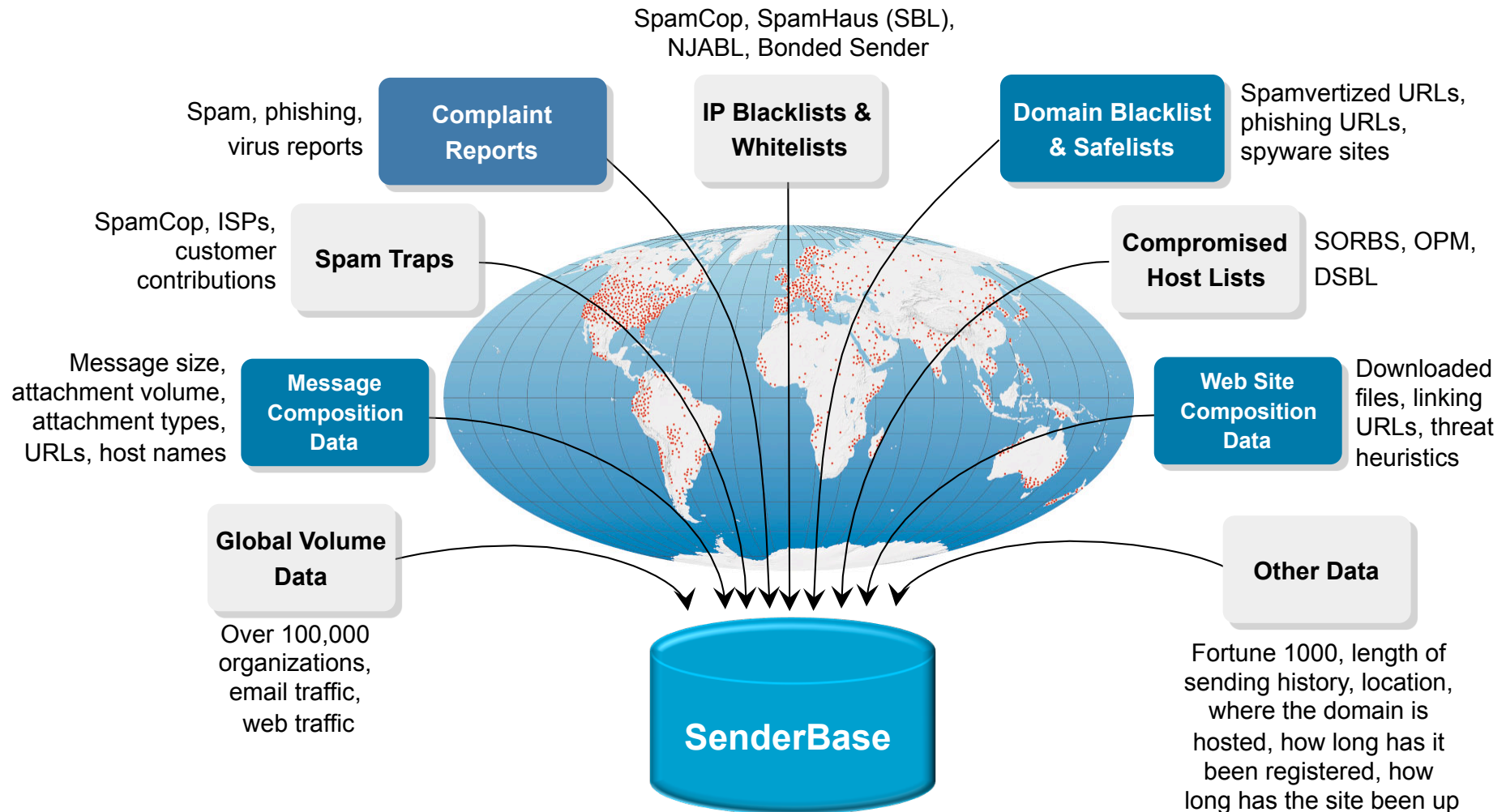
IronPort C-серия
Безопасность Email



IronPort S-серия
Безопасность Web

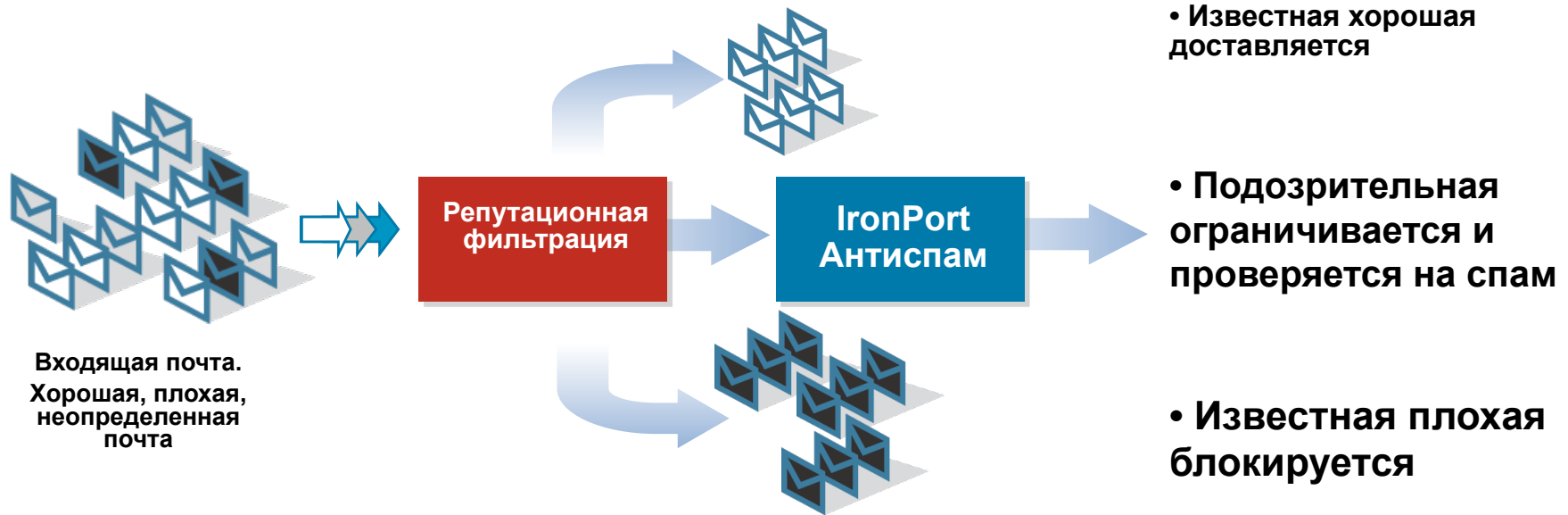
Cisco IronPort SenderBase

Секрет успеха -- качество и количество данных



Репутационная фильтрация SenderBase

Предотвращение угроз в реальном времени



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

Антиспам Cisco IronPort

Многоуровневая линия обороны от спама



Marketing Message Detection – The Problem

Buy.com Sign In. New User? Sign Up.

Products Deals BuyTV News and Reviews Funny TV Ads! Cart

Home > Company Info | Privacy Policy | Affiliates

Create My Account

How do I create a My Account?
To create a My Account, please fill out the appropriate information below.

* Required fields

My Account Login

* Enter Your eMail Address

* Select Your Birth Year
Select One
Why is this required?

* Choose A Password
(must be between 5 & 20 characters)

* Verify Your Password Password Hint (Optional)

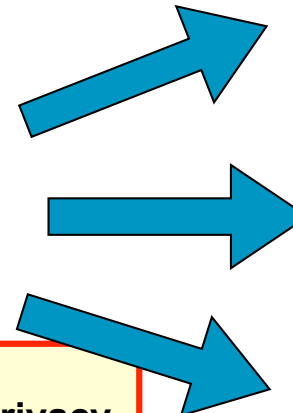
Terms of Use

Terms and Conditions
READ CAREFULLY. This Terms of Use Agreement ("Terms of Use") applies to use of the Buy.com website located at
[Click here for a full screen view of the terms.](#)

I Agree to the Buy.com Terms and Conditions.

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.



websense
September 2008
WEBSENSECONNECT
SECURE WEB GATEWAY ISSUE

Securing The Web Gateway In The Web 2.0

Does Web 2.0 have legitimate business applications or is it just a marketing gimmick? Websense shares his insights on the risks of the secure Web gateway.

Business Focus
Business Blogs, Vapid or Vital?
With 40,000 new blogs cropping up every day, it begs the question—is there a business benefit to blogging? And with the bloggers already increasingly compensated, how can the company stand out? Learn how enterprises such as General Motors have made their mark and how you can too, in this BusinessWeek story about social media and business.

Latest News
[AVIRAS CONNECT WITH FANS THROUGH...](#)
[QUICKMEDIACHECK HELPS REPAIR INTERNET SPO...](#)
[THE 2008 SUMMER OLIMPICS: THE MOST AS...](#)
[HOW MANY ACCESS TO FACEBOOK A GOWN...](#)

Get a \$200 travel coupon when you book now Spam | X

Expedia Travel Deals to me
Images are not displayed.
[Display images below](#)

Expedia.com Book a flight or package now, get...

Flights|Hotels|Cars|Vacation Packages|Cruises|Activities|DEALS & OFFERS|Business Travel|ThankYou

Now is THE Time to Book a Flight or Package [Spotlight Deal](#)

Book now, get a \$200 coupon to use later!
Book a qualifying flight or package using your MasterCard® card by November 3, 2008 for travel through December 31, 2008 and we'll deposit a \$200 travel coupon* into your Expedia Account. Your \$200 coupon is valid for a flight + 5-night hotel package.

Book and travel between November 20, 2008 and February 28, 2009.
[Search now on Expedia](#)

Last-minute Deals
Dallas: Hotels from \$74/night
Las Vegas: Relax from \$59/night
Orlando: Stay from \$49/night

[Search last-minute deals](#)

101inks.com

SAVE up to 85%
on Printer Ink Cartridges & Toners!

FREE SHIPPING!
On Continental U.S. Orders Over \$49

100% Satisfaction Guarantee

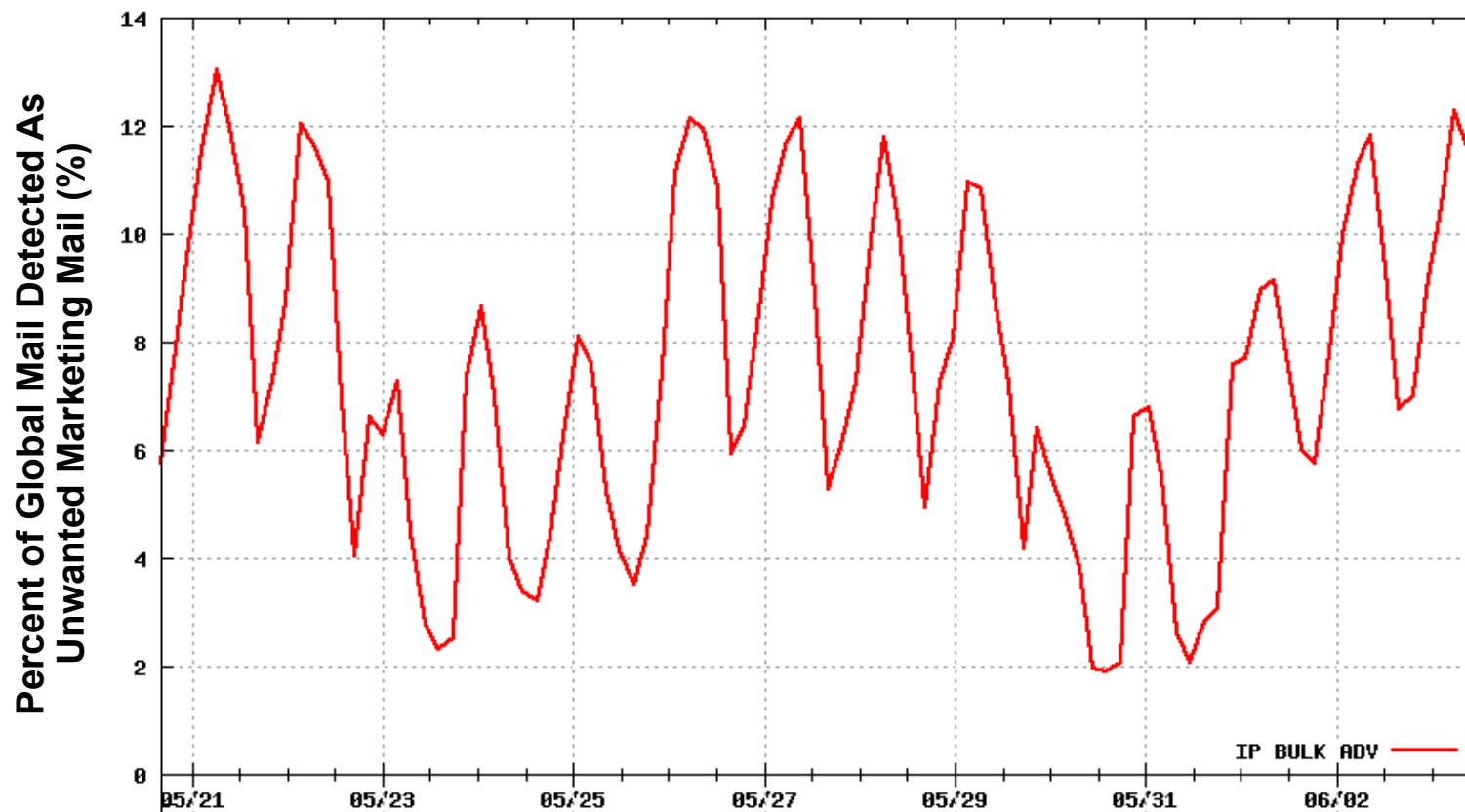
[Click Here >>](#)

- HP
- Lexmark
- Epson
- Canon
- Xerox
- Brother
- Apple
- Kodak
- Dell
- Sharp
- Samsung
- Panasonic
- Compaq
- Okidata
- Konica-Minolta
- Pitney Bowes
- IBM
- More printers...

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

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)



Marketing Message Detection

Configuration and Reporting Screenshots

- Config in IPAS settings

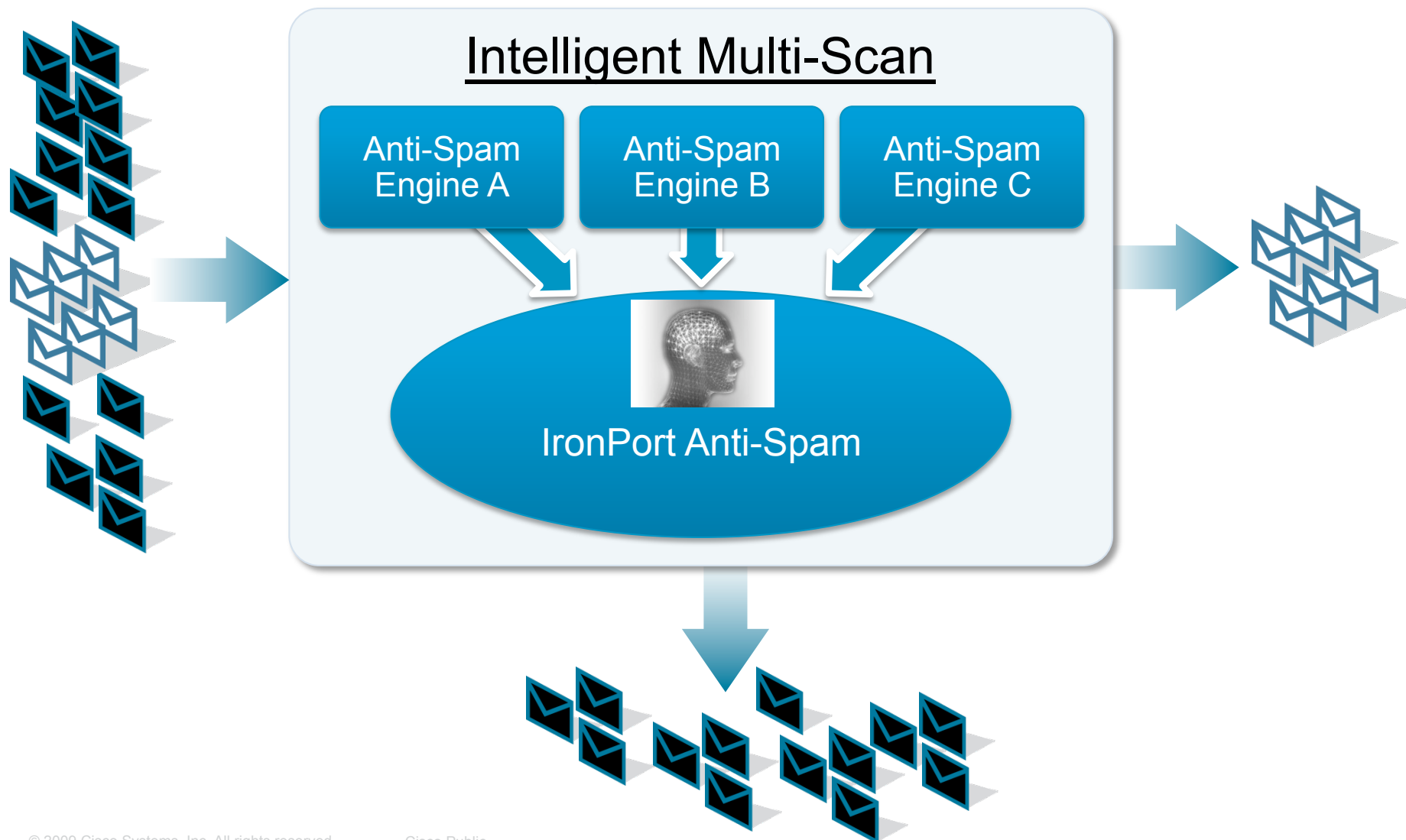
Marketing Messages Settings	
Enable Marketing Message Scanning:	<input type="radio"/> No <input checked="" type="radio"/> Yes
Apply This Action to Message:	Deliver <input type="button" value="v"/> Send to Alternate Host (optional): <input type="text"/>
Add Text to Subject:	Prepend <input type="button" value="v"/> [MARKETING]
<input type="button" value="v"/> Advanced	
Add Custom Header (optional):	Header: <input type="text"/> Value: <input type="text"/>
Send to an Alternate Envelope Recipient (optional):	Email Address: <input type="text"/> (e.g. employee@company.com)
Archive Message:	<input checked="" type="radio"/> No <input type="radio"/> Yes

- Full Overview Reporting

Incoming Mail Summary		
Message Category	%	Messages
Stopped by Reputation Filtering	33.5%	98.1k
Stopped as Invalid Recipients	11.5%	33.6k
Spam Detected	15.3%	44.8k
Additional Spam Detected by Intelligent Multi-Scan	15.3%	44.8k
Virus Detected	4.4%	13.1k
Stopped by Content Filter	20.0%	58.6k
Total Threat Messages:	75.0%	293k
Marketing Messages	15.8%	44.8k
Clean Messages	10.2%	70.8k
Total Attempted Messages:	100.0%	415.6k

Intelligent Multi-Scan

Best of Both Worlds: Higher Detection with Low FPs



Intelligent Multi-Scan

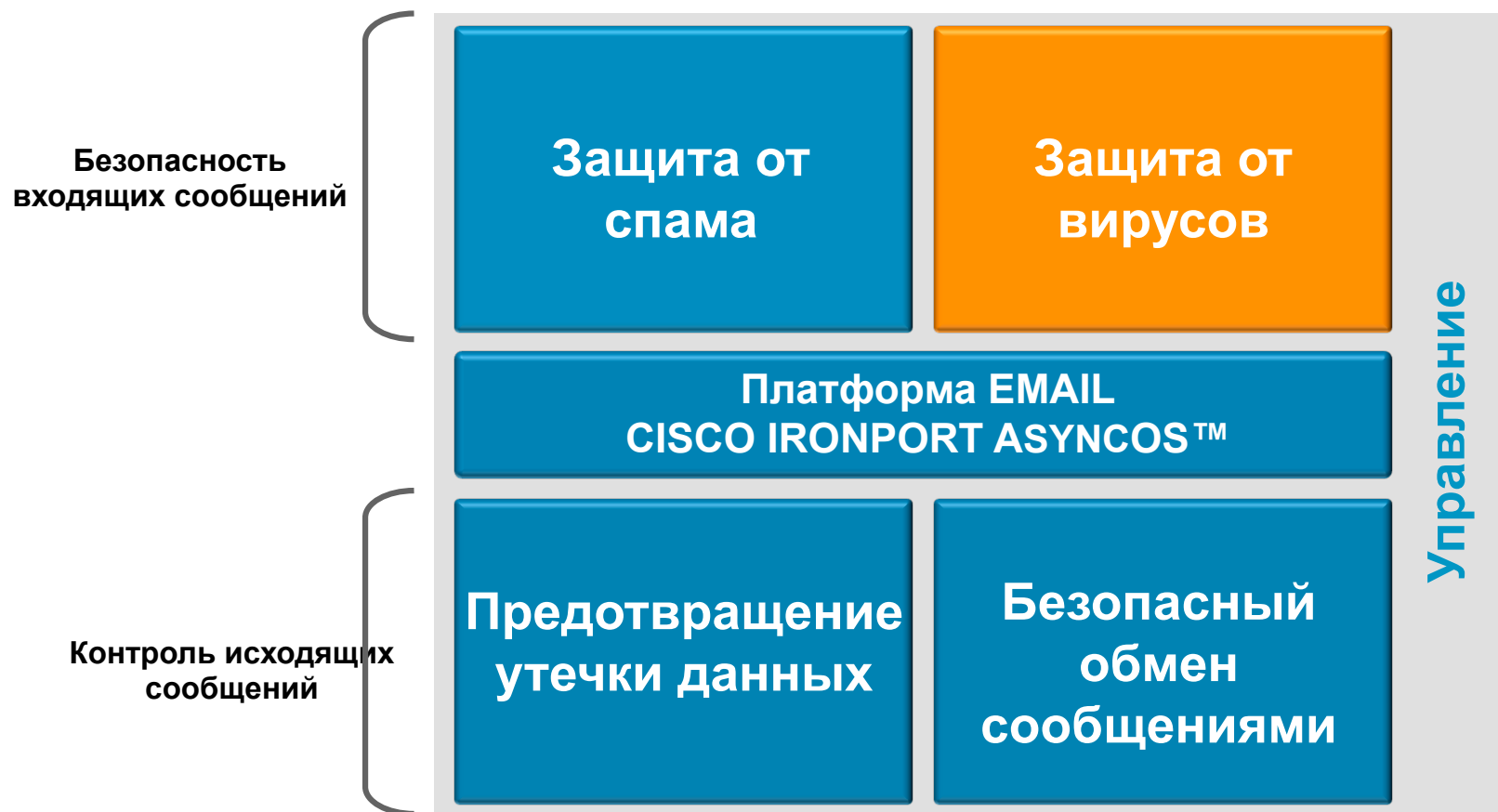
Defense-In-Depth Anti Spam

ANTI-SPAM EFFICACY		
	Detection Rate	FP Rate
IronPort	99.80%	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%

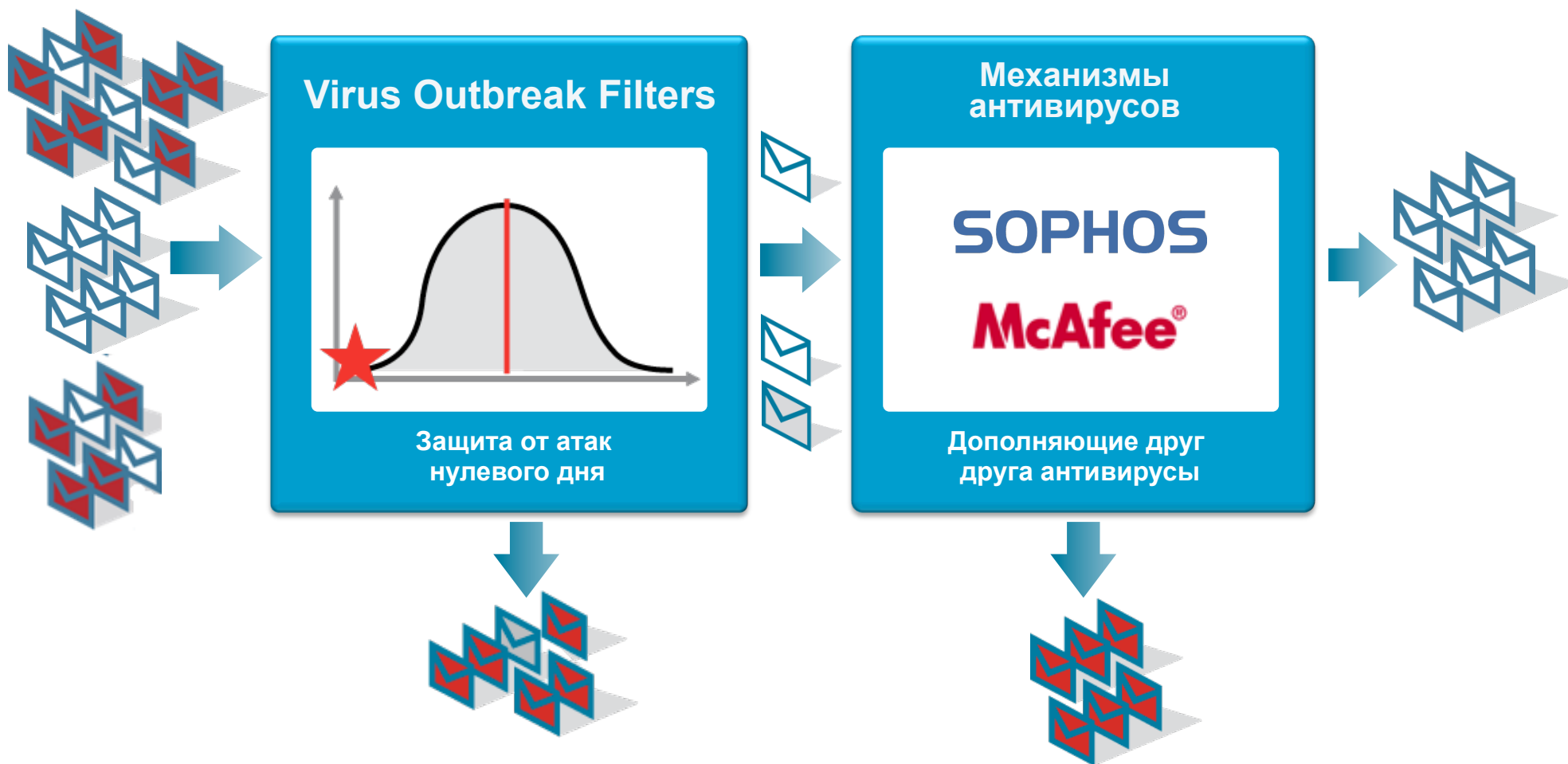
- **Greater Spam Detection...with IronPort-Leading FP Rate**

Email. Архитектура безопасности.

Безопасность входящих сообщений, контроль исходящих



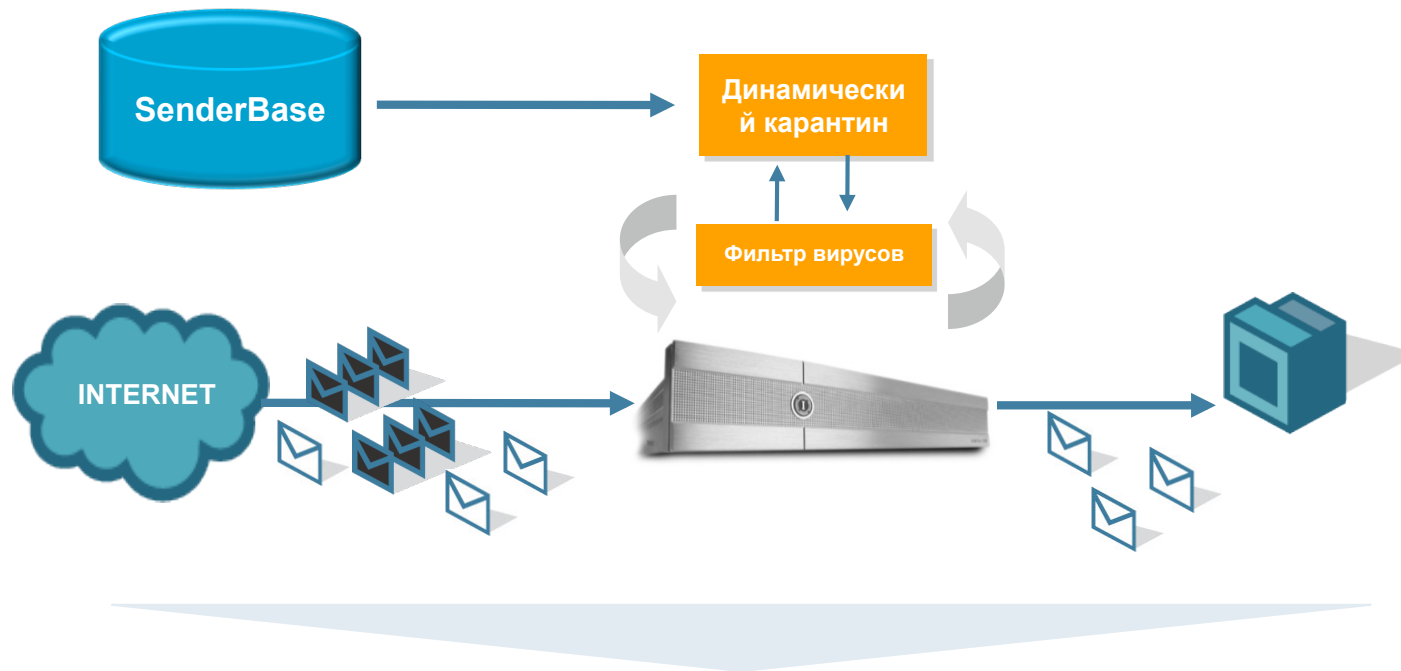
Многоуровневая антивирусная защита



Cisco IronPort Virus Outbreak Filters

Защита от атак нулевого дня

Virus Outbreak Filters в действии



Преимущество Virus Outbreak Filters

Среднее время защиты*более 13 часов
 Количество атак*291 атака
 Общее время защиты* более 157 дней

“Since VOF we have not had a single virus outbreak!”



“Over 24,000 virus positive messages stopped in 9 months”

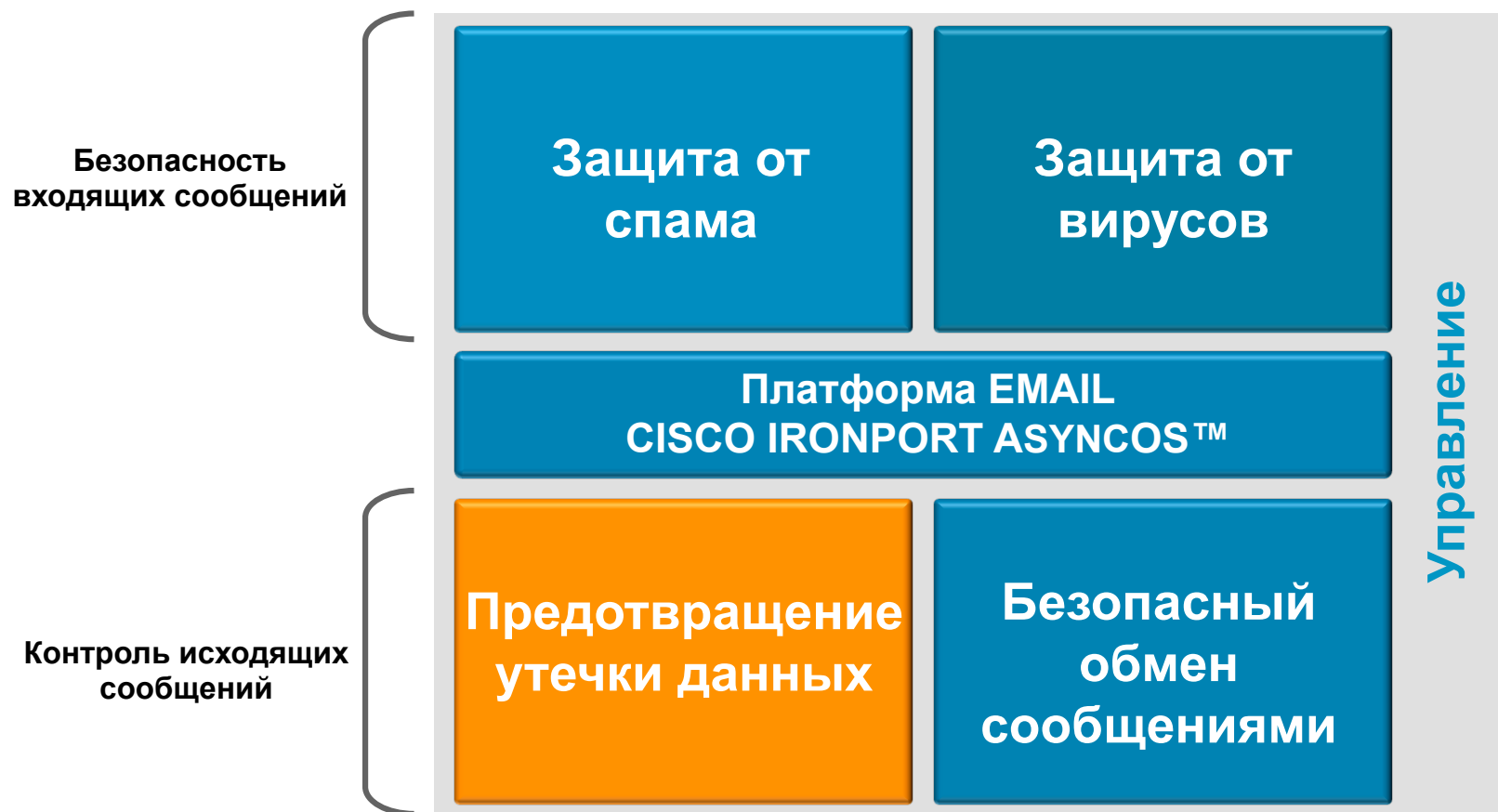


“VOF has stopped more than 12,000 separate viral messages in the last year”



Email. Архитектура безопасности.

Безопасность входящих сообщений, контроль исходящих



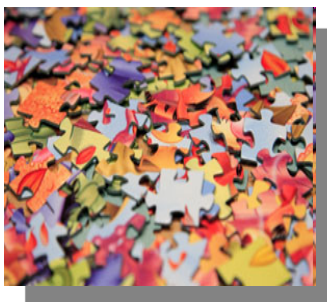
Исторические барьеры, препятствующие внедрению системы предотвращения утечек



- **Низкая точность**

Большое 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

Система сканирования контента IronPort

Простая установка

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

Message Body or Attachment

Does the message body or attachment contain text that matches a specified pattern?

Contains text:
 *

Contains smart identifier:
ABA Routing Number

Contains term in content dictionary:
HIPAA-Dictionary_txt

Number of matches required: (1-1000)
For content dictionaries, the number of matches is term weight.

Import from local computer:

Import from the *configuration* directory on your IronPort appliance

- GLBA-Dictionary.txt
- HIPAA-Dictionary.txt
- PCI-Dictionary.txt
- README
- SOX-Dictionary.txt
- config.dtd

Smart Identifiers: ?

Enable Smart Identifiers	Weight
<input checked="" type="checkbox"/> Credit Card Numbers	1
<input checked="" type="checkbox"/> Social Security Numbers	1
<input checked="" type="checkbox"/> ABA Routing Numbers	1
<input checked="" type="checkbox"/> CUSIPs	1

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

The screenshot displays a configuration interface for a quarantine system. On the left, a list of actions is shown, with 'Bypass Outbreak Filter Scanning' highlighted. On the right, the configuration for the 'Quarantine' action is detailed.

Quarantine

Strip Attachment by Content
Strip Attachment by File Info
Add Disclaimer Text
Bypass Outbreak Filter Scanning
Send Copy (Bcc:)
Notify
Change Recipient to
Send to Alternate Destination Host
Deliver from IP Interface
Strip Header
Add Header
Encrypt and Deliver (Final Action)
Bounce (Final Action)
Deliver (Final Action)
Drop (Final Action)

Quarantine

Flags the message to be held in one of the areas.

Send message to quarantine: Policy ▼

Duplicate message

Send a copy of the message to the specified quarantine area. The original message will continue processing the original message actions will apply to the original message

RSA – Лидер рынка и технологий



at&t



Microsoft



**CVS
CAREMARK**

- 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

Полное, глобальное покрытие

DLP Policy Manager: DLP Policy Templates

Add DLP Policy from Templates
▶ Regulatory Compliance
▶ Acceptable Use
▶ Privacy Protection
▶ Intellectual Property Protection
▶ Company Confidential
▶ Custom Policy

DLP Policy Manager: Add DLP Policy

Add DLP Policy from Templates	
▼ Regulatory Compliance	
Add	PCI-DSS (Payment Card Industry Data Security Standard) Identifies cardholder data regulated by PCI-DSS. Customize to detect credit card numbers from one or all of the following issuers: American Express,
Add	PIPEDA (Personal Information Protection and Electronic Documents Act) Identifies Personally Identifiable Information (PII) - Social Insurance Numbers - regulated by PIPEDA.
Add	CPNI (Customer Proprietary Information) Protects information that telecommunications providers acquire about subscribers and provide via phone bills. CPNI includes such information as opt patterns.
Add	Fair Credit Reporting Act Regulates the collection, dissemination, and use of consumer credit information. This policy detects credit reports.
Add	FERPA (Family Educational Rights and Privacy Act) Detects student education records. <i>This policy requires customization to improve DLP efficacy. You will need to define a regular expression for student identification numbers.</i>
Add	GLBA (Gramm-Leach Bliley Act) Identifies customer-related financial information regulated by GLBA. Customize this policy to detect SSNs, CCNs and custom account numbers such organization. <i>This policy requires customization to improve DLP efficacy. You will need to define a regular expression for custom account numbers.</i>
Add	HIPAA (Health Insurance Portability and Accountability Act) Identifies HIPAA-regulated information including patient IDs, National Provider Identifiers, Social Security Numbers and HIPAA dictionaries. <i>This policy requires customization to improve DLP efficacy. You will need to define a regular expression for patient identification numbers.</i>
Add	EAR (Export Administration Regulations) Identifies transmissions about exports to countries forbidden by EAR.
Add	ITAR (International Traffic in Arms Regulations) Identifies transmissions about arms trade to countries forbidden by ITAR.
Add	OFAC (Office of Foreign Asset Control) Detects transmissions to e-mail destinations for embargoed counties as designated by the United States government. Nations currently included in t Syria.
Add	NASD Rule 2711 and NYSE Rule 251 and 472 Protects the names of any companies involved in upcoming stock offerings.

Различные варианты использования

Более 100
предопределенных
шаблонов

▼ Custom Policy	
Add	Custom Policy This option is considered advanced and should be used only in rare cases when the policy templates above do not meet unique

Политики, создаваемые пользователями

Широкий набор опций реагирования

1

Deliver [see states for this row]

Enable Encryption
Encryption Profile:
Encrypted Message Subject:
 Use TLS

2

Message Modifications

Add Custom Header: Header:
Value:

Modify Message Subject:

Add DLP Disclaimer Text: Disclaimer Template:
(See Mail Policies > Text Resources to customize templates.)
Add: Below Message Body
 Above Message Body

3

Message Delivery

Send Message to Alternate Host:

Send Copy (Bcc): Subject:
Recipients:
Return Address:

4

DLP Notification

Recipients: Sender
 Other:

1 Доставка, карантин, сброс, шифрование

2 Добавить отказ от ответственности

3 Отослать копию администратору безопасности

4 Уведомить отправителя и/или получателя

Управление всеми функциями из одной консоли

Outgoing Mail Policies

Find Policies

Email Address:

Recipient Sender **Find Policies**

Policies

Add Policy...

Order	Policy Name	Anti-Spam	Anti-Virus	Content Filters	Virus Outbreak Filters	DLP	Delete
1	Fake Policy	(use default)	(use default)	(use default)	(use default)	(use default)	
	Default Policy	IronPort Anti-Spam Positive: Deliver Suspected: Deliver Marketing Messages: Disabled	Sophos Repaired: Deliver Encrypted: Deliver Unscannable: Deliver ...	Enabled (no filters)	Disabled	HIPAA (Heal... GLBA (Gram... Restricted Fi...	

Key: **Default** Custom Disabled

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

Гарантированная точность анализа

The screenshot shows a rich text message window titled "Patient Information - SSN: 603011313 - Message (Rich Text)". The message content is as follows:

To...: jsmith@acme.com
Cc...: [empty]
Subject: Patient Information - SSN: 603011313

We need to fax the following **prescription** information for **Roger McMillan**:
FEXOFENADINE (ALLEGRA) 180 MG TABLET
Dosage: Take 1 Tab By Mouth Daily.
Prescribed by Joseph A Keeney, MD on 06/03/09

Please make sure that this information is provided to the **pharmacy**.

Name: **Roger McMillan**
Medical Record: **06135443**
Primary Provider: Blue Cross Blue Shield CA
Clinic: **Stanford Hospital**
Address:
177 Bovet Road
San Mateo, California 94402
Home Phone: 650-528-1620
Work Phone: 650-542-2211
E-mail: roger.mcmillan@gmail.com

Annotations and analysis results:

- SSN detection:** A blue box highlights the subject line "Patient Information - SSN: 603011313".
- Proper Name Detection:** A blue box with arrows pointing to "Roger McMillan" and "Joseph A Keeney".
- Matches are found in close proximity:** A blue box with arrows pointing to "Roger McMillan" and "06135443".
- Rule is matched multiple times to increase score:** A blue box with an arrow pointing to "Stanford Hospital".
- Unique rule matches are met:** A legend box on the right with colored squares (red, yellow, green, pink, cyan, dark green) corresponding to the text highlights.

Просто настраивать

Остановите канал утечек в течение нескольких минут

Outgoing Mail Policies

Find Policies

Email Address:

Recipient
 Sender

Find Policies

Policies

Add Policy ...

Order	Policy Name	Anti-Spam	Anti-Virus	Content Filters	Virus Outbreak Filters	DLP	Delete
1	Fake Policy	(use default)	(use default)	(use default)	(use default)	(use default)	
	Default Policy	IronPort Anti-Spam Positive: Deliver Suspected: Deliver Marketing Messages: Disabled	Sophos Repaired: Deliver Encrypted: Deliver Unscannable: Deliver ...	Enabled (no filters)	Disabled	HIPAA (Heal... GLBA (Gram... Restricted Fi...	

Key: Default Custom Disabled

Интегрирован
в менеджер
ПОЛИТИК



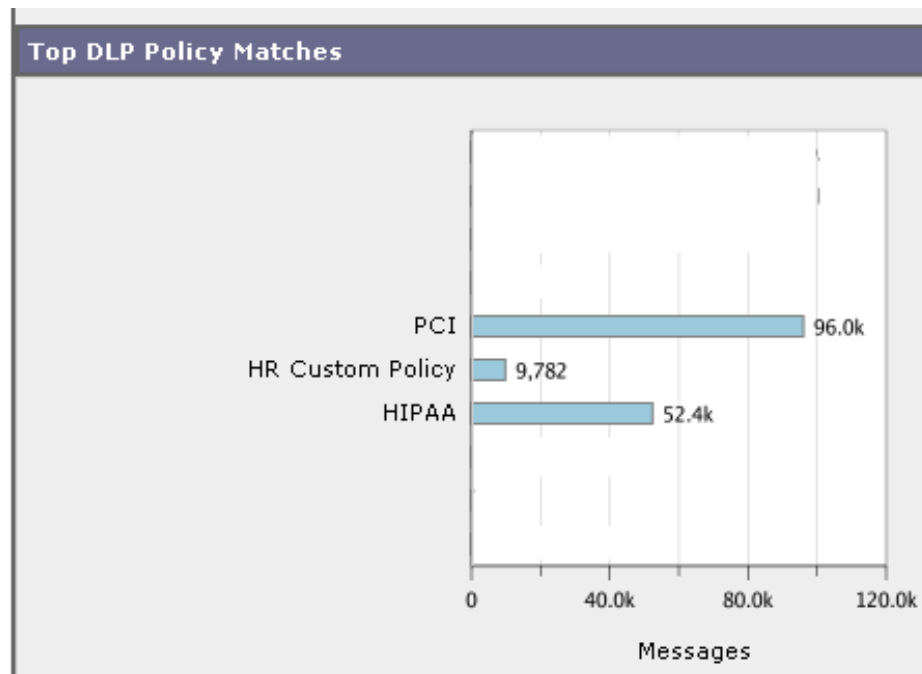
DLP Scanning Policies

Enable DLP Policies to apply to this mail policy.
To manage this list, add or remove DLP policies, go to DLP Resources.

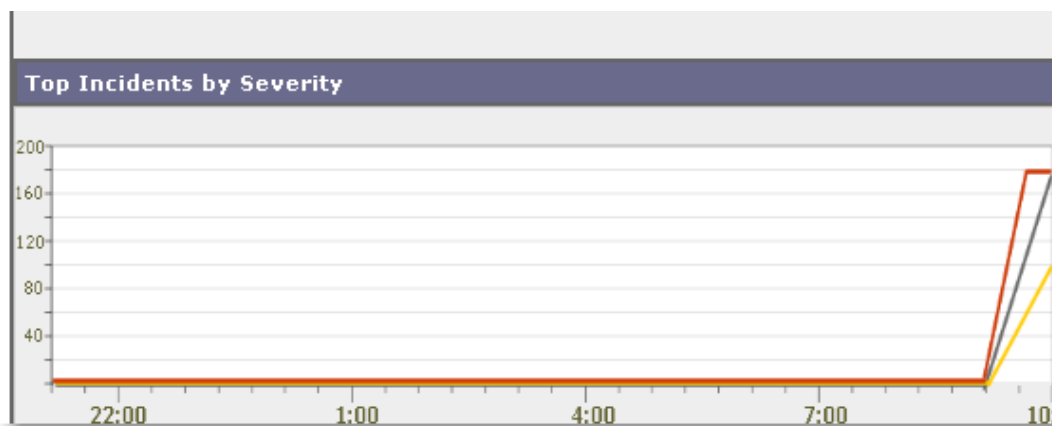
Order	DLP Policy	<input type="checkbox"/> Enable All
1	PCI-DSS (Payment Card Industry Data Security Standard) Identifies cardholder data regulated by PCI-DSS. Customize to detect credit card numbers from one or all of the following issuers: American Express, Diner's Club, Discover Card, JCB, MasterCard and Visa.	<input checked="" type="checkbox"/>
2	GLBA (Gramm-Leach Bliley Act) Identifies customer-related financial information regulated by GLBA. Customize this policy to detect SSNs, CCNs and custom account numbers such as bank, investment, or mortgage account numbers specific to your organization.	<input type="checkbox"/>
3	HIPAA (Health Insurance Portability and Accountability Act) Identifies HIPAA-regulated information including patient IDs, National Provider Identifiers, Social Security Numbers and HIPAA dictionaries.	<input checked="" type="checkbox"/>
4	Restricted Files Detects restricted files including MS Access, executable, and Oracle executable files.	<input type="checkbox"/>

Активация
ПОЛИТИК
ОДНИМ КЛИКОМ
МЫШКИ

Легко отслеживать



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



Incident Summary

Severity	%	Messages
■ Critical	54.0%	11.3k
■ High	5.0%	29.9k
■ Medium	18.0%	75.1k
■ Low	6.0%	12.0k
Total	100.0%	36.0k

Легко искать

Message Event: *Selecting multiple events will expand your search to include messages that match each with other search criteria will narrow the search.*

<input type="checkbox"/> Virus Positive	<input type="checkbox"/> Hard bounced
<input type="checkbox"/> Spam Positive	<input type="checkbox"/> Soft bounced
<input type="checkbox"/> Suspect Spam	<input type="checkbox"/> Quarantined as Spam
<input type="checkbox"/> Delivered	<input type="checkbox"/> Currently in Outbreak Quarantine
<input checked="" type="checkbox"/> DLP Violations	

DLP Policy Name:
Leave blank to search all policies.

Violation Severities: Critical High Medium Low



	MESSAGE ID "5972594" MATCHED DLP POLICY "HIPAA"
Violation Severity:	CRITICAL (Risk Factor: 100)
Message Body:	US Social Security Number <ul style="list-style-type: none">Acme Corp Marty Smith 808 Sumner Street Greenwood MS 38930 USA Engineering 662-646-0542 msmith@acmecorp.com 2/1/07
patient1234.xls:	HIPAA Patient Identifier <ul style="list-style-type: none">Fred Flintstone Operations 321-02-3456 111 Stonehenge Dr, Bedrock CA 99432Wilma Flintstone Human Resources 321-03-3116 111 Stonehenge Dr, Bedrock CA 99432Pebbles Flintstone Engineering 321-04-3256

Простой поиск сообщений

Просмотр деталей нарушения и где оно произошло

Простота создания пользовательских политик

Название политики и описание

Категория серьезности нарушения

Сканирование контента

Возможный набор действий


The screenshot shows the 'Add DLP Policy' configuration page in the IronPort C350 management console. The page is titled 'Mail Policies: DLP Scanning: Add Policy' and includes a 'Commit Changes' button. The configuration is organized into several sections:

- DLP Policy Name:** Custom Policy 1
- Description:** Testing
- Order:** 1 (of 4)
- Severity Scale:** A table with five columns: IGNORE (0-10), LOW (10-35), MEDIUM (35-60), HIGH (60-90), and CRITICAL (90-100). The MEDIUM column is highlighted in yellow.
- Content Matching:** Multiple sections for defining rules. The first section is for 'Social Security Numbers, Patient ID Numbers'. The second is for 'Student Identification Numbers AND Student Records'. The third is for 'Custom Accounts OR Credit Card Number OR US Social Security Number OR US Drivers Licenses'. Each section has a 'Define' field and an 'Exclude patterns or strings' field.
- Critical Violations Settings:** Action Applied to Messages: Deliver; Send Copy(Bcc): (email address).
- High Violations Settings:** Use same settings as Critical Violations settings.
- Medium Violations Settings:** Use same settings as High Violations settings.
- Low Violations Settings:** Use same settings as Medium Violations settings.

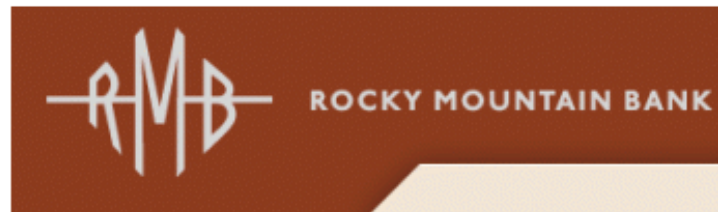
At the bottom, there are 'Cancel' and 'Submit' buttons, and a note: 'Showing three cases for the content matching sections.'

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.

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.

449
diggs

digg it

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

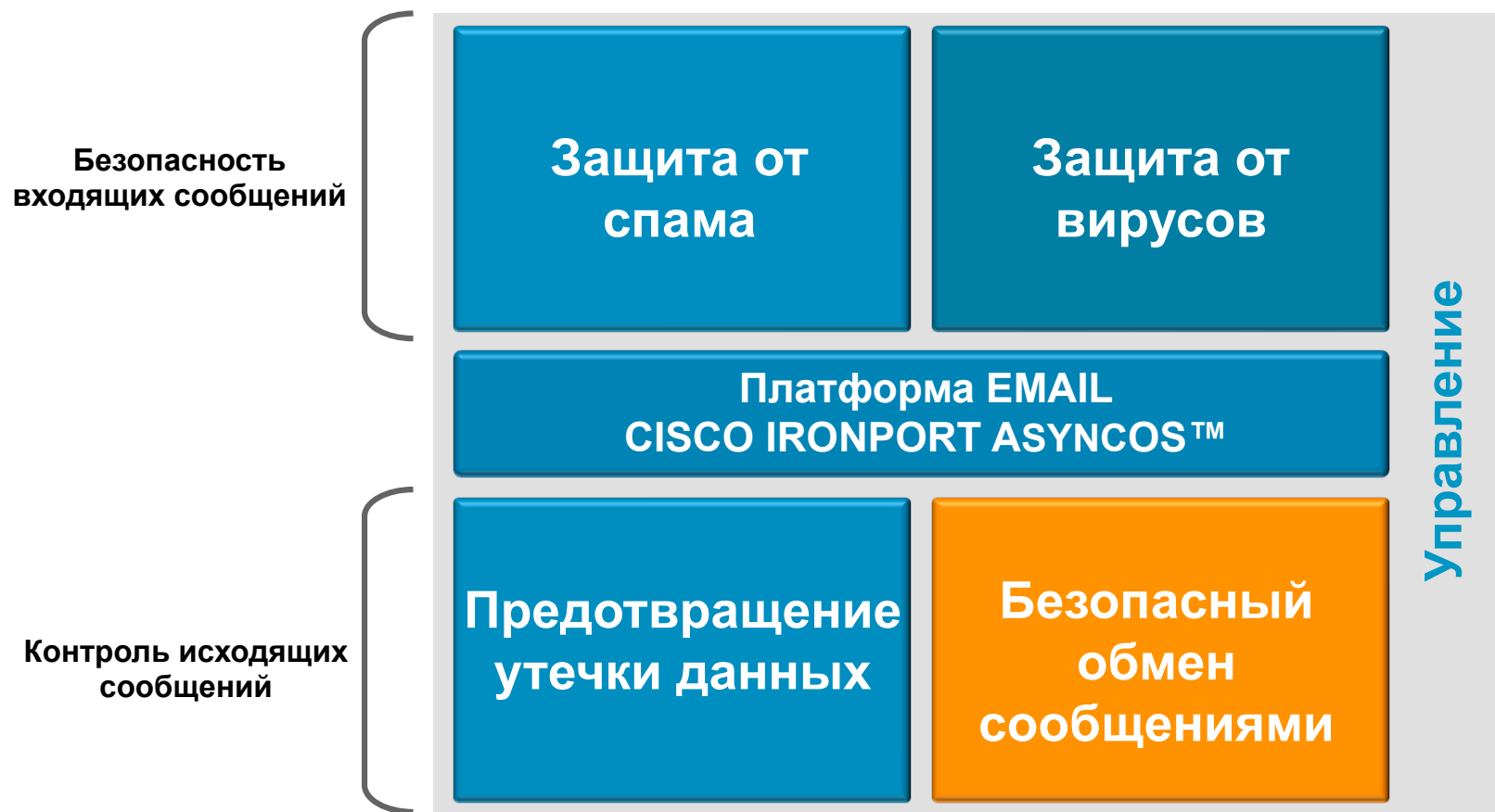
When that didn't work, the employee sent a second e-mail to the recipient instructing the person to delete the e-mail and attachment "in its entirety" without opening or reviewing it. The employee also asked the recipient to contact the employee to "discuss his or her actions."

Silence ensued.

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

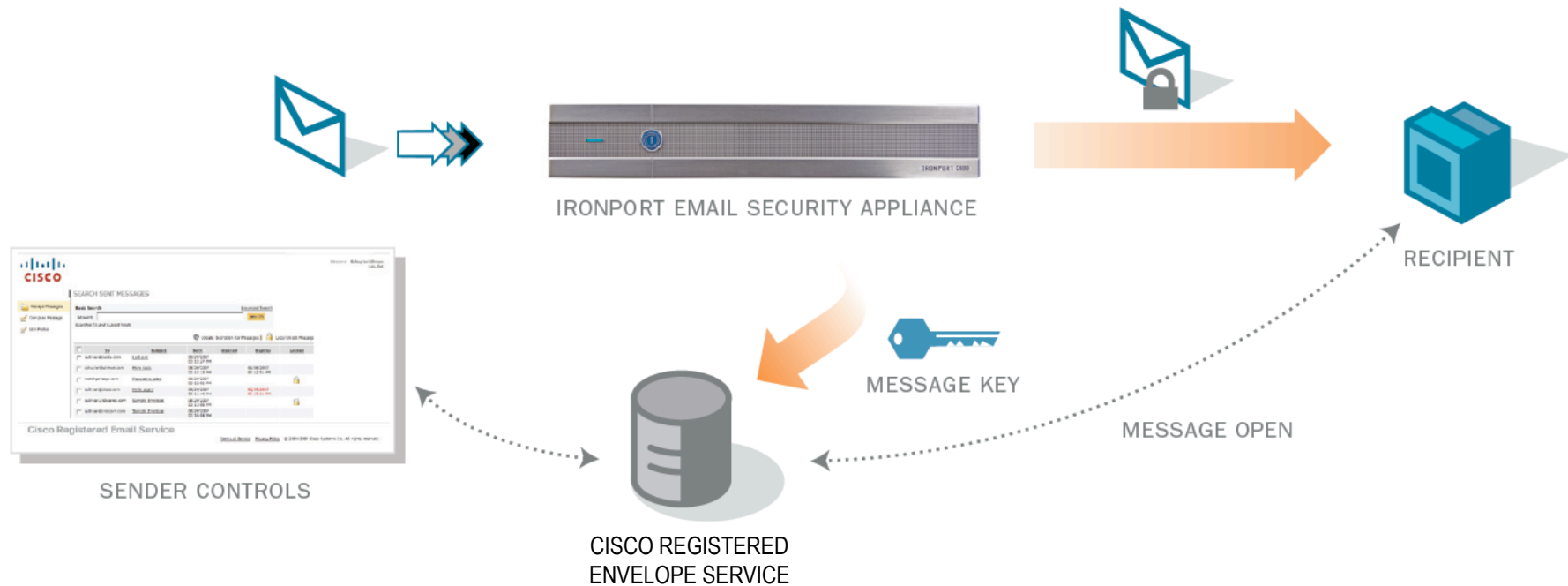
Email. Архитектура безопасности.

Безопасность входящих сообщений, контроль исходящих



Шифрование Email Cisco IronPort

Легко для отправителя. . .

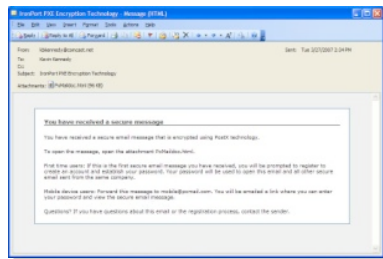


- Автоматизированное управление ключами
- Не требуется дополнительное ПО на рабочей станции пользователя
- Можно легко и быстро отослать на любой адрес

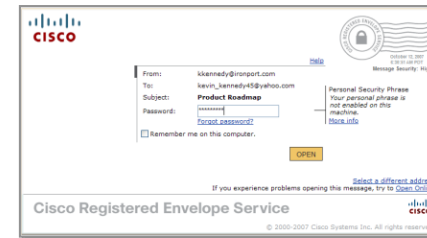
Шифрование Email Cisco IronPort

Легко для получателя. . .

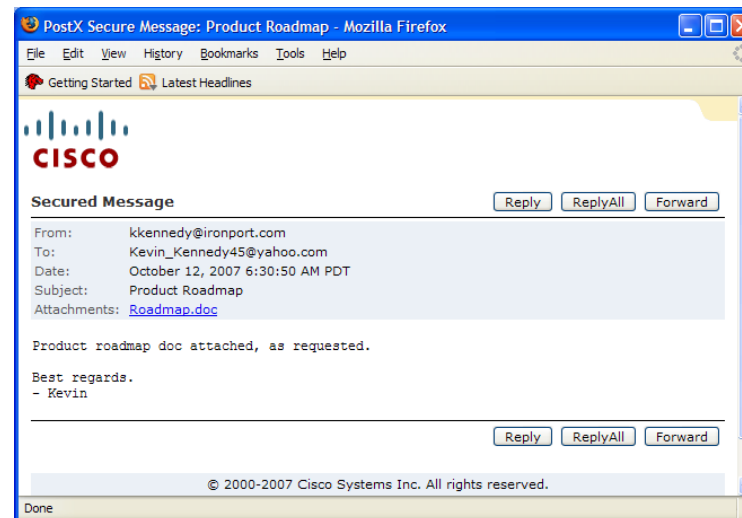
1. Открыть присоединенный файл



2. Ввести пароль

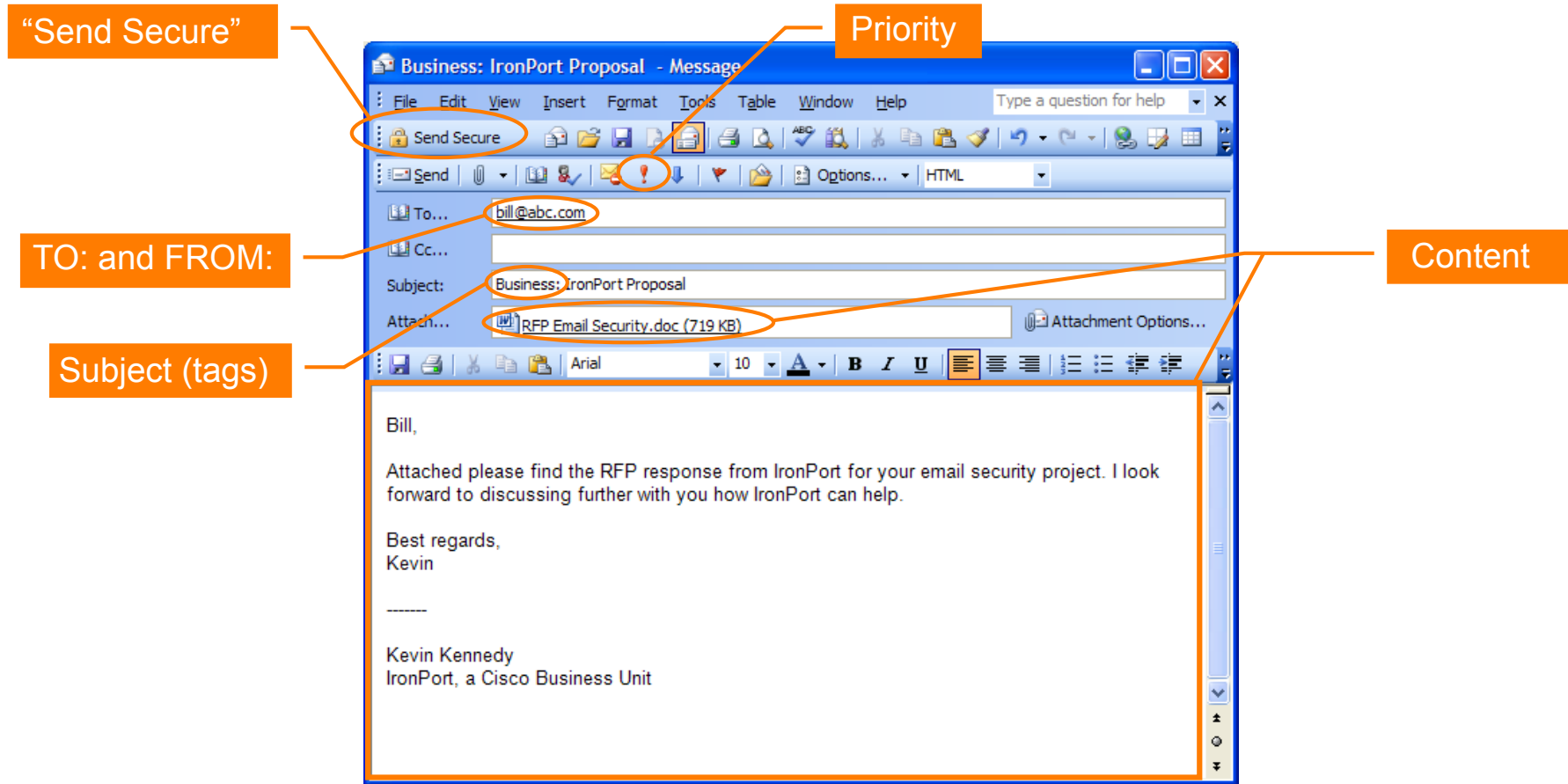


3. Просмотреть сообщение



Гибкость и простота

Все из одного почтового клиента



User Controls + Central Policy

Email бизнес-класса

Полный контроль сообщения

Welcome **Kevin Kennedy**
[Administration](#) [Log Out](#)

CISCO

SEARCH SENT MESSAGES

Manage Messages
Compose Message
Edit Profile
Provision Account

Advanced Search
Keyword 1 in - Select One -
Keyword 2 in - Select One -
Date From 10/11/07 12:00:00 AM Date To 10/13/07 12:00:00 AM in Sent Date
Status All

Update Expiration For Messages | Lock/Unlock Message

	To	Subject	Sent	Opened	Expires	Locked
<input type="checkbox"/>	[redacted]@gmail.com	Requested product information	10/12/2007 06:36:14 AM			<input type="checkbox"/>
<input type="checkbox"/>	[redacted]@yahoo.com	Requested product information	10/12/2007 06:36:14 AM			<input type="checkbox"/>
<input type="checkbox"/>	[redacted]@ironport.com	Requested product information	10/12/2007 06:36:14 AM	10/12/2007 06:49:10 AM		<input type="checkbox"/>
<input type="checkbox"/>	[redacted]@comcast.net	Requested product information	10/12/2007 06:36:14 AM			<input type="checkbox"/>
<input type="checkbox"/>	[redacted]@ironport.com	Quote for PXE Encryption	10/12/2007 06:35:08 AM		10/15/2007 12:00:00 AM	<input type="checkbox"/>
<input type="checkbox"/>	[redacted]@gmail.com	Q4 Pricebook	10/12/2007 06:34:35 AM			<input type="checkbox"/>
<input type="checkbox"/>	[redacted]@yahoo.com	Q4 Pricebook	10/12/2007 06:34:35 AM	10/12/2007 06:45:55 AM		<input type="checkbox"/>
<input type="checkbox"/>	[redacted]@yahoo.com	Product Roadmap	10/12/2007 06:30:51 AM	10/12/2007 06:46:05 AM		<input type="checkbox"/>
<input type="checkbox"/>	[redacted]@yahoo.com	Secure: Product Roadmap	10/12/2007 06:26:53 AM			<input type="checkbox"/>

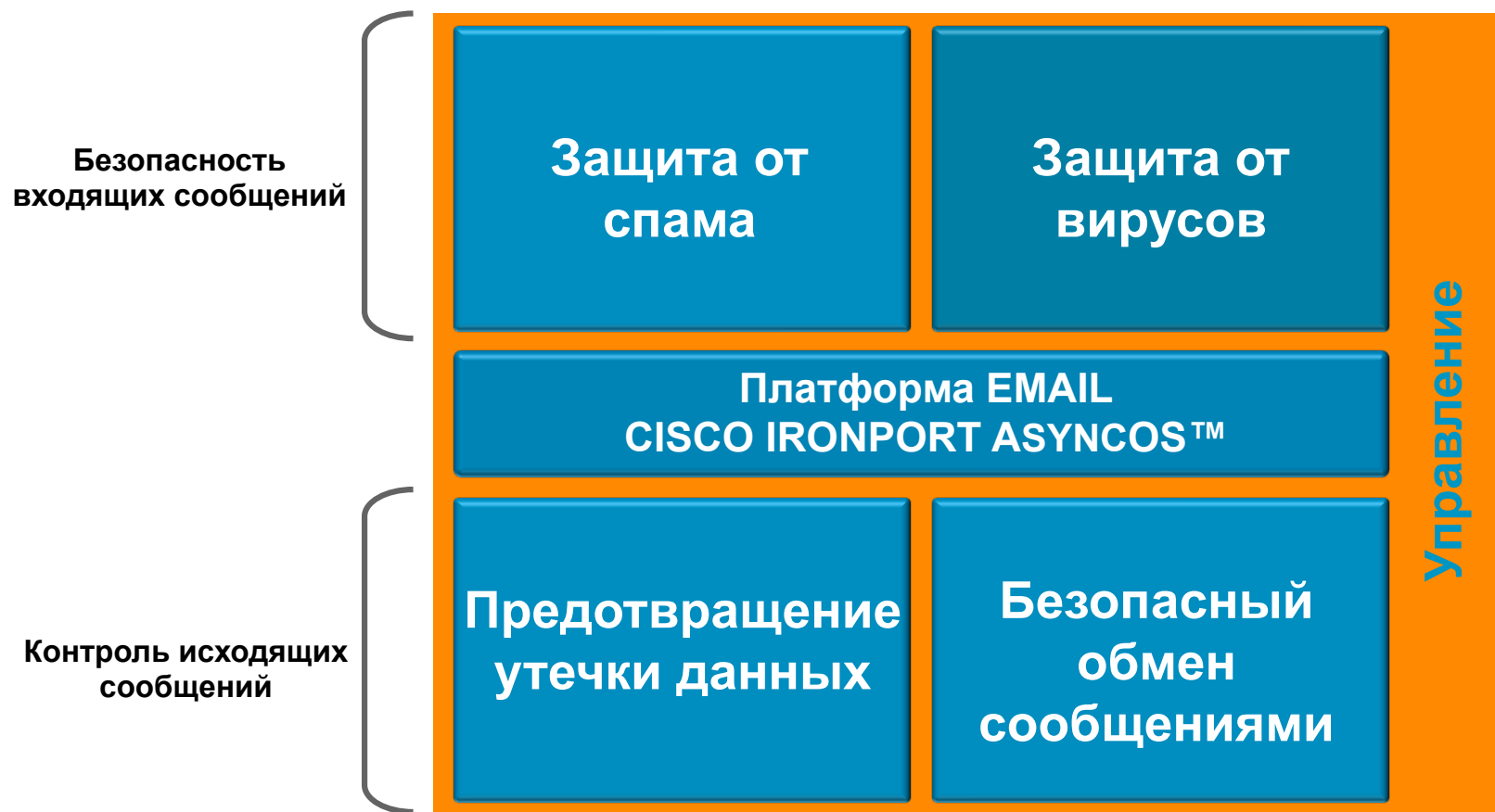
Guaranteed Read Receipt

Guaranteed Recall

Cisco Registered Envelope Service
[About](#) [Terms of Service](#) [Privacy Policy](#) © 2001-2007 Cisco Systems Inc. All rights reserved.

Email. Архитектура безопасности.

Безопасность входящих сообщений, контроль исходящих



Cisco IronPort Email Security Manager

Простая настройка политик для всей организации

Incoming Mail Policies

Find Policies

Email Address: Recipient Sender

Policies

Order	Policy Name	Anti-Spam	Anti-Virus	Content Filters	Virus Outbreak Filters	Delete
1	IT Staff	(use default)	(use default)	QuarantineEXEs	(use default)	
2	Sales	IronPort Positive: Deliver Suspected: Deliver	(use default)	DelMsgsWithEXEs	(use default)	
3	Legal	(use default)	(use default)	ArchiveMail QuarantineEXEs StripMediaFiles	Enabled	
	Default Policy	IronPort Positive: Drop Suspected: Deliver	Repaired: Deliver Encrypted: Deliver Unscannable: Deliver Virus Positive: Drop	QuarantineEXEs StripMediaFiles	Enabled	

Key:

Категории: домен, имя
пользователя, LDAP

- Разрешить все медиафайлы
- Исполняемые файлы в карантин



IT

- Пометить и доставить спам
- Удалить исполняемые файлы



SALES

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



LEGAL

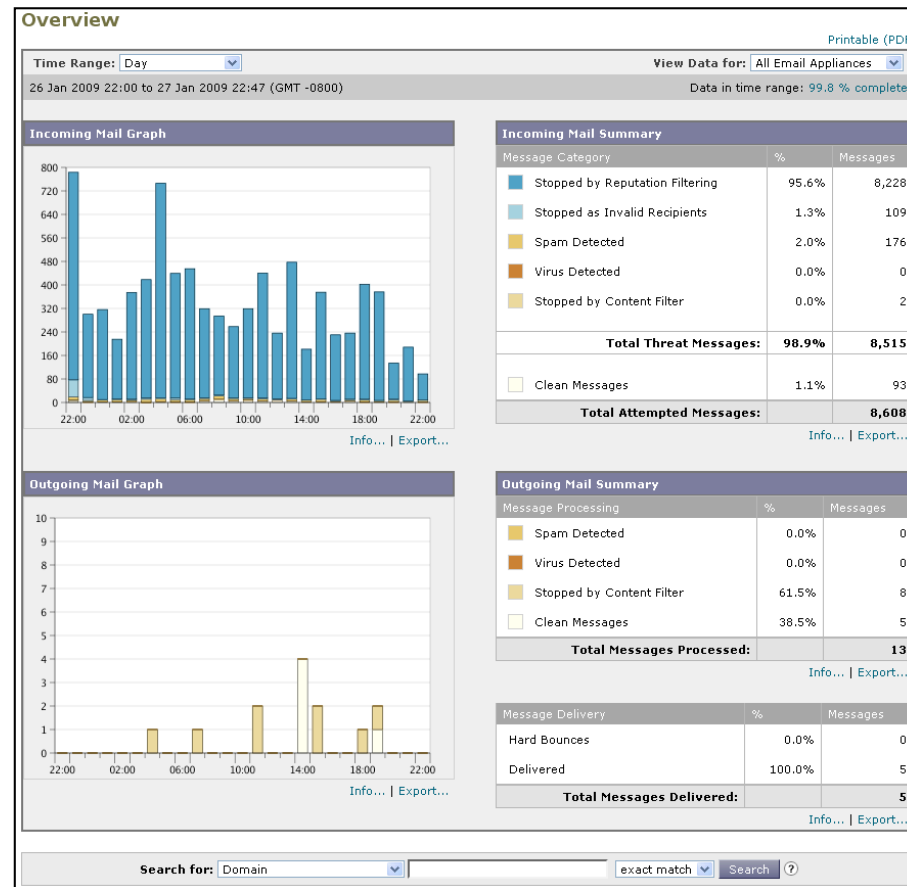
“IronPort Email Security Manager работает как одна мощная и гибкая консоль настройки, которая позволяет управлять всеми сервисами устройства,
– PC Magazine

Отчеты

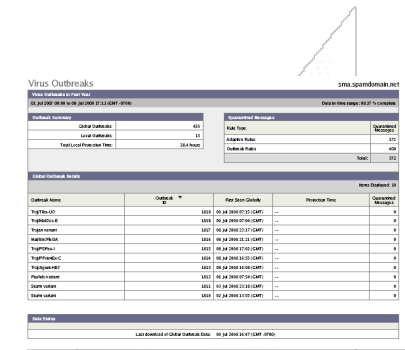
Унифицированная система построения отчетов для бизнеса

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

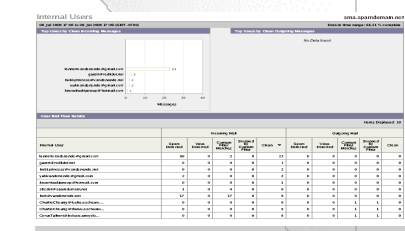
Consolidated Reports



Multiple data points



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



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

Message Tracking

Search

Available Time Range: 08 Oct 2007 09:10 to 27 Jan 2009 22:51 (GMT -0800) Data in time range: 91.25% complete

Envelope Sender: ?	Begins With					
Envelope Recipient: ?	Begins With					
Subject:	Begins With					
Message Received:	<input checked="" type="radio"/> Last Day <input type="radio"/> Last Week <input type="radio"/> Custom Range					
	Start Date:	Time:	and	End Date:	Time:	(GMT -0800)
	01/26/2009	22:00		01/27/2009	22:52	
Advanced						
Sender IP Address:						
	<input type="radio"/> Search rejected connections only <input checked="" type="radio"/> Search messages					
Message Event:	Selecting multiple events will expand your search to include messages that match each event type. However, combining an event type with other search criteria will narrow the search.					
	<input type="checkbox"/> Virus Positive	<input type="checkbox"/> Hard bounced				
	<input type="checkbox"/> Spam Positive	<input type="checkbox"/> Soft bounced				
	<input type="checkbox"/> Suspect Spam	<input type="checkbox"/> Currently in Outbreak Quarantine				
	<input type="checkbox"/> Delivered	<input type="checkbox"/> Quarantined as Spam				
Message ID Header:						
IronPort MID:						
IronPort Host:	All Hosts					
Query Settings: ?	Query timeout: 1 minute					
	Max. results returned: 250					

Clear Search

Email. Архитектура безопасности.

Безопасность входящих сообщений, контроль исходящих



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 отправлено сервером, авторизованным отправлять почту для данного домена



Возможность LDAP

LDAP ссылки, несколько LDAP серверов, установка за 3 шага

DKIM подпись и проверка

Проверка отправителя

Bounce Verification

Избежать перенаправленных bounces

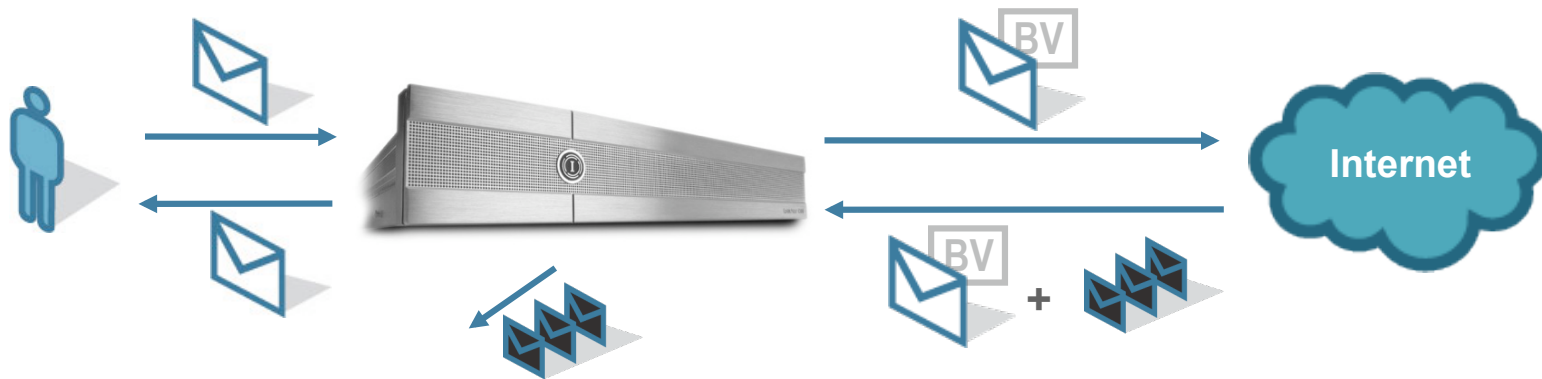
Спам-карантин, черные и белые списки для пользователей
Контроль пользователей

Проверка получателя

Удалить сообщения, которые отправлены на несуществующий адрес

IronPort Bounce Verification™

Защищает от перенаправленных bounce-атак (Backscatter)



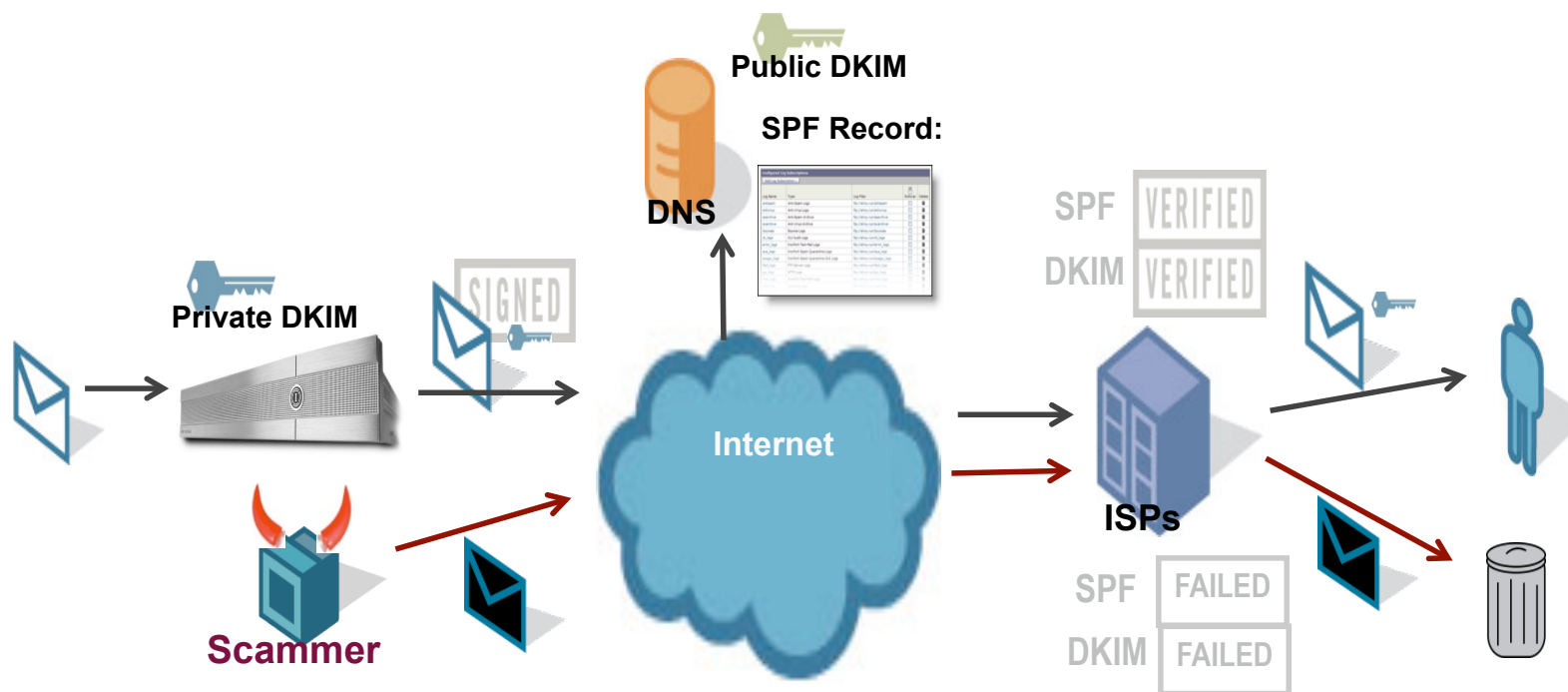
- Вся исходящая почта специальным образом помечается для того, чтобы ее можно было идентифицировать при возвращении
- Прозрано для пользователей, не требует никаких изменений в серверное ПО
- Помогает избежать звонков в техподдержку от ничего не понимающих пользователей
- IronPort Technical "First"

Аутентификация Email

SPF и 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



Пример – какое сообщение настоящее?

From: eBay [eBay.2668.41075.0@reply4.ebay.com] Sent: Mon 3/20/2006 4:13 PM

To: gobronxbombers@yahoo.com

Cc:

Subject: You're only one step away. Confirm your registration now.



You're only one step away!

You recently started the eBay.ie registration process using . In order for advantage of the great bargains available on eBay, we would like to help your registration. Simply follow the steps below and you'll be ready to t

To make it easier, print off this mail so you can refer to it a

step 1 [Click here to go to the registration scr](#)


From: member@ebay.com Sent: Wed 2/15/2006 3:10 PM

To: Patrick Peterson

Cc:

Subject: Message from eBay Member {None}

eBay sent this message!
Your registered name is included to show this message originated from eBay.
[Learn more.](#)

Question from eBay Member -- Respond Now 

eBay sent this message on behalf of an eBay member via My Messages. Responses sent using email will not reach the eBay member. Use the **Respond Now** button below to respond to this message.

Question from user

Hello,

Dear user:
Kimberly L Coffey has informed us that they have not

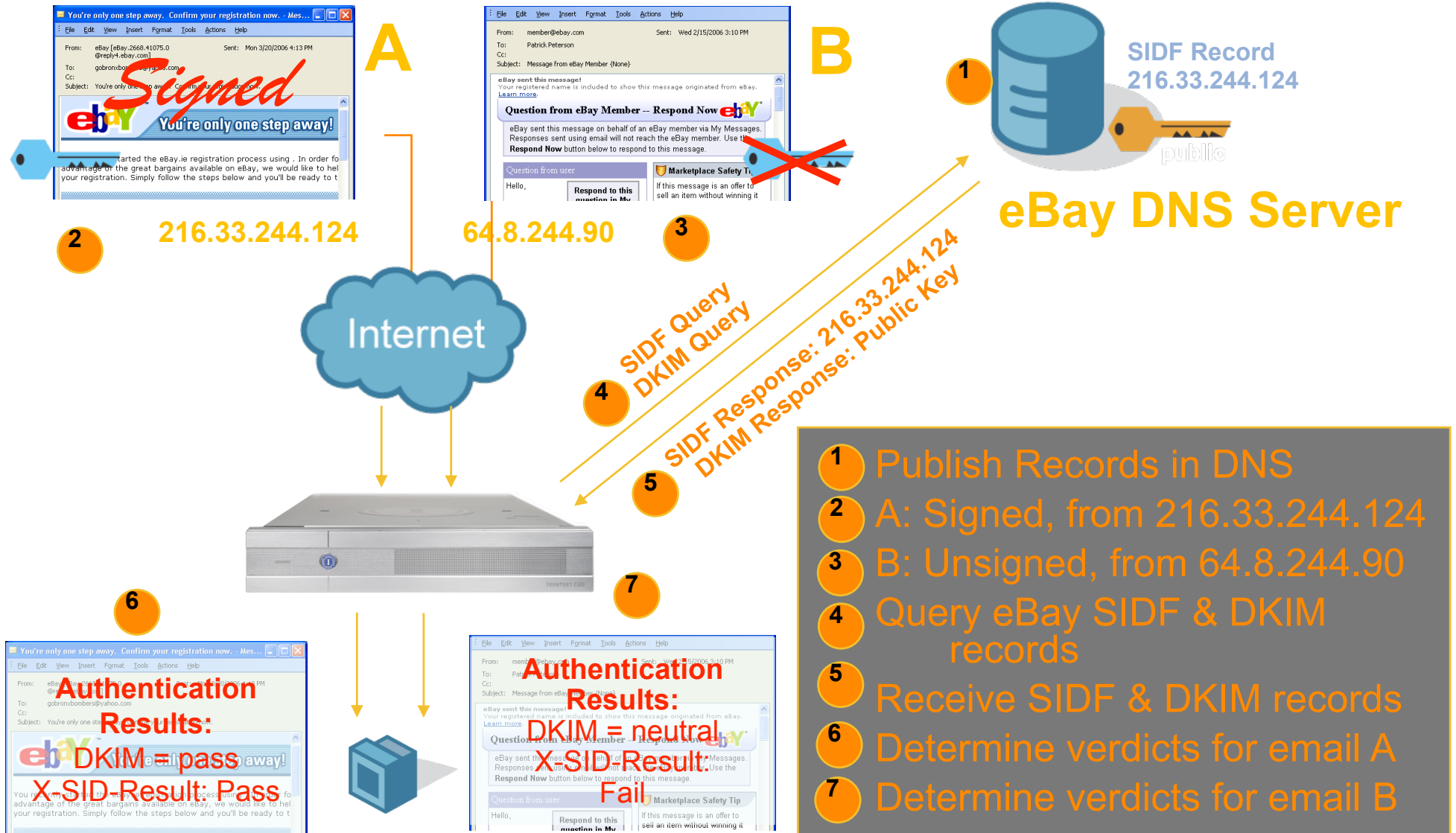
Respond to this question in My Messages.

Respond Now

Marketplace Safety Tip

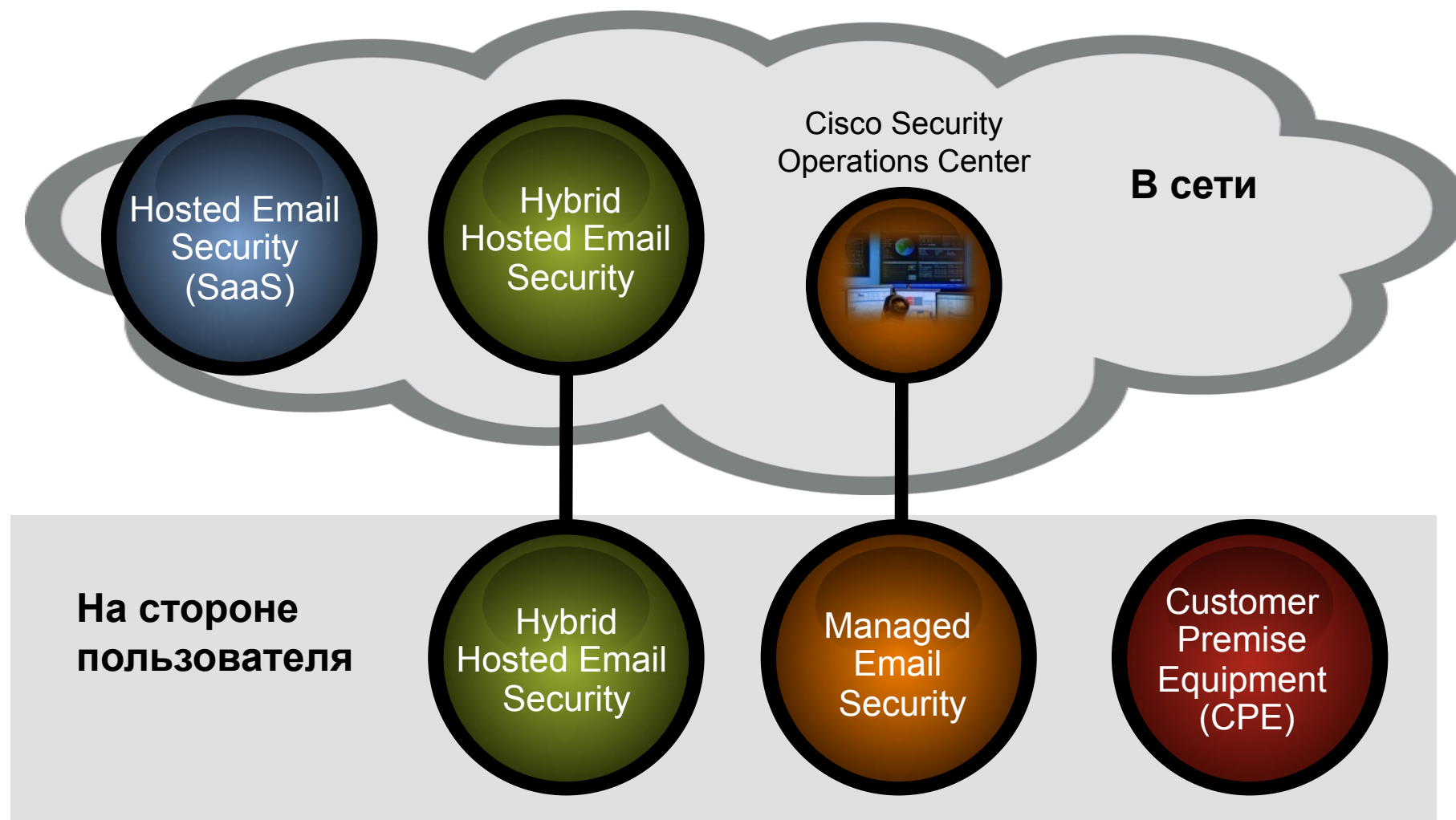
If this message is an offer to sell an item without winning it on the eBay Web site (including Second Chance Offers sent through My Messages) please do not respond to the sender. These external transactions are

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

Набор гибких опций внедрения

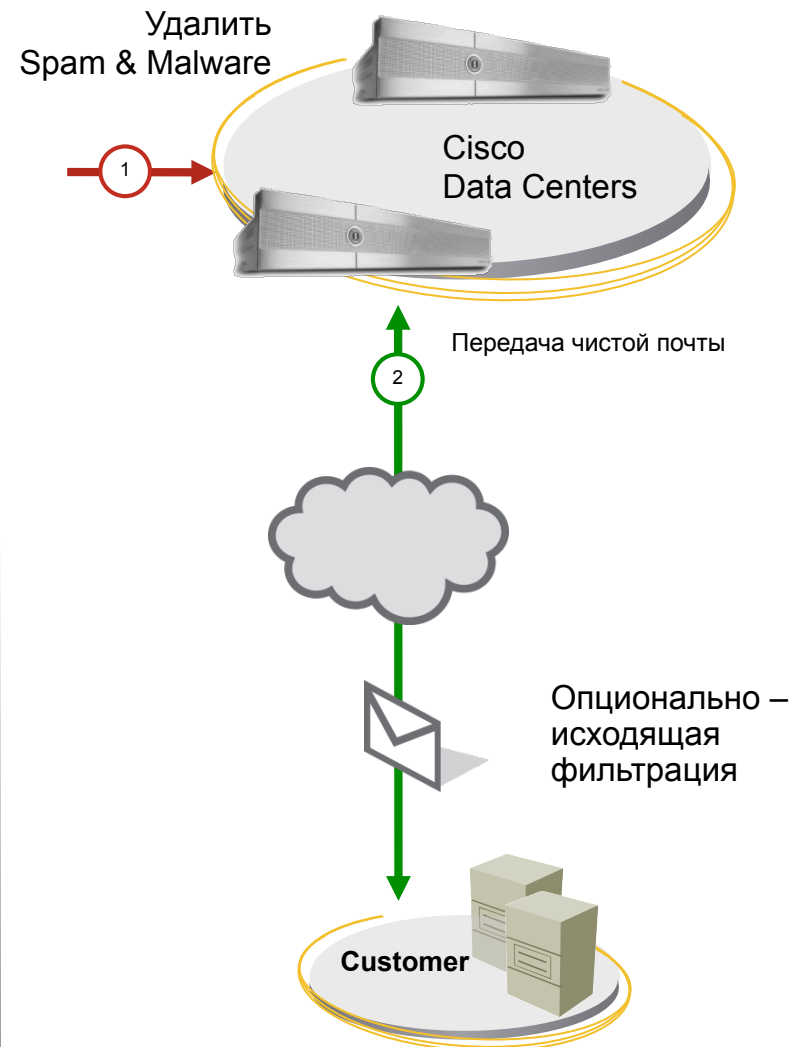


Common Policy | Centralized Reporting | Consistent Protection

Hosted Email Security

Выделенное решение снижает нагрузку и ускоряет внедрение

- Безопасности Email в облаке снижает нагрузку на ЦОД
- «Выделенное» решение снижает риск общего сбоя ('shared fate' risk)
- Управляемая инфраструктура гарантирует производительность для будущего роста



Когда это необходимо?

HOSTED

...

...снизить нагрузку на ЦОД...

...получить эффективное решение hosted email...

...отдать обработку email на аутсорс...

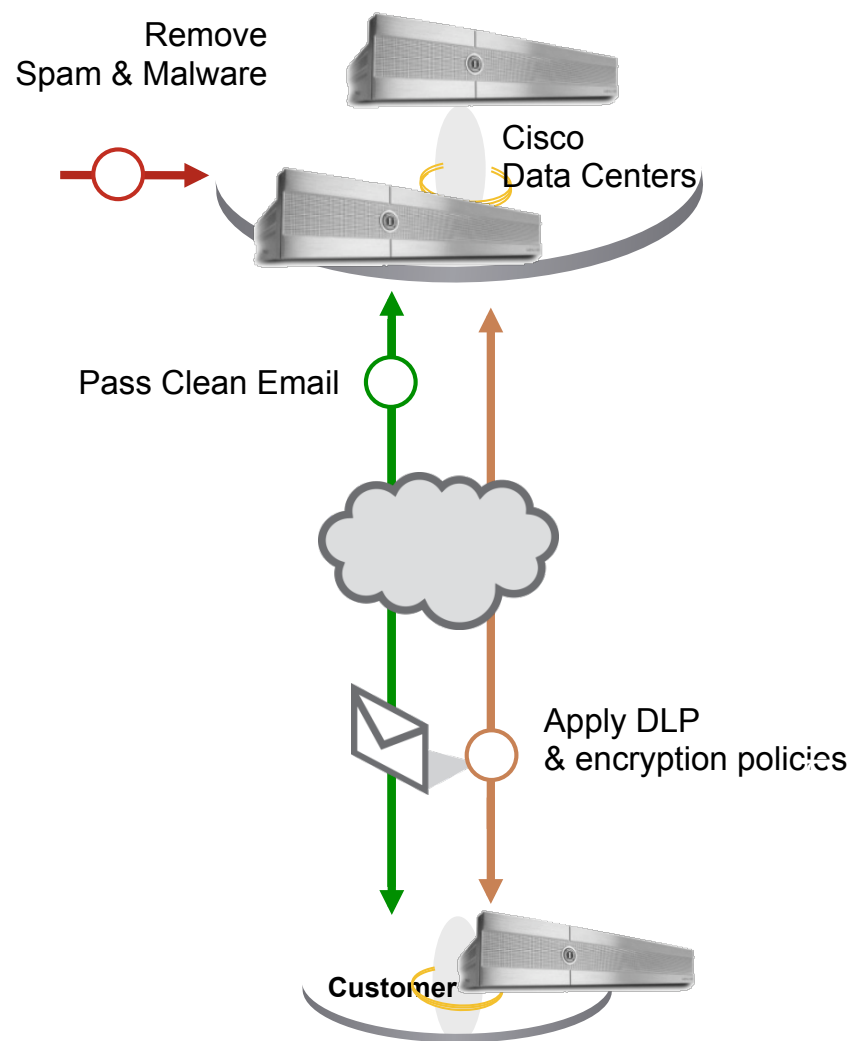


...не хочу терять контроль над устройствами...

Гибридный Hosted Email Security

Оптимальный дизайн, максимальная гибкость

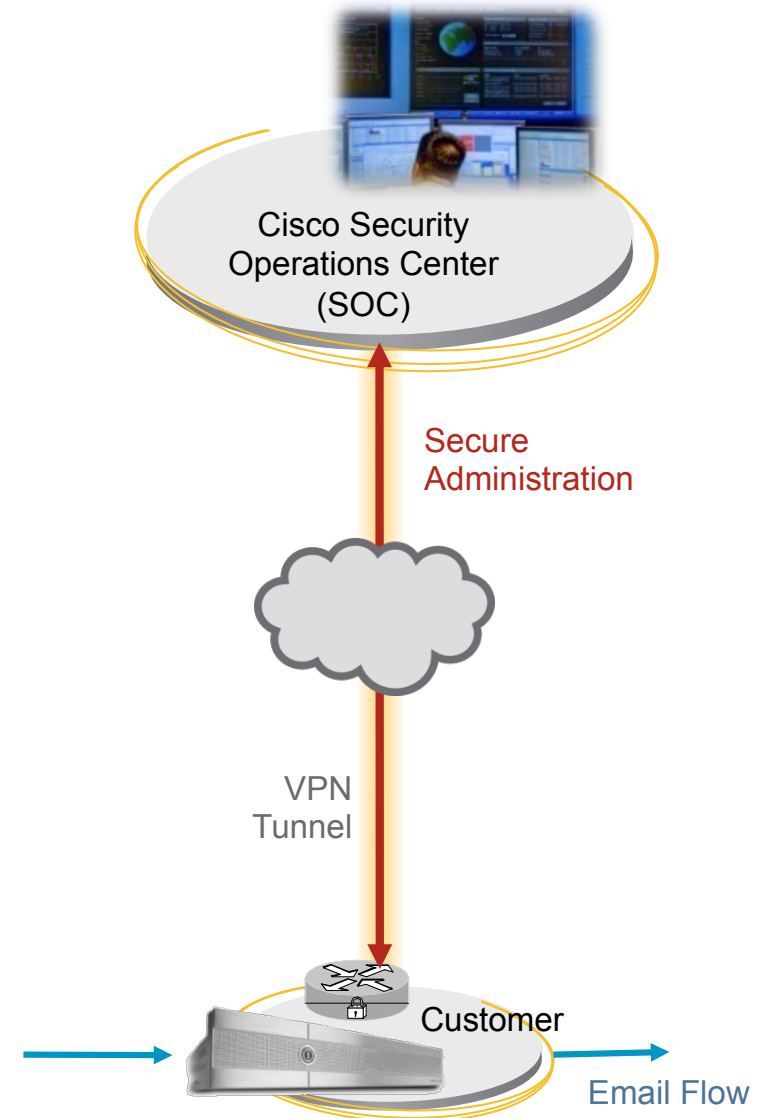
- Гибридный дизайн подразумевает разнесенное управление – на площадке и в облаке
- Устройства на площадке пользователя контролируют исходящую почту, политики DLP и шифрование



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

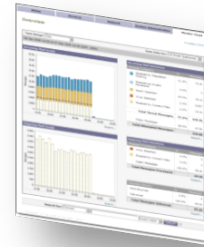


Гибкость в работе

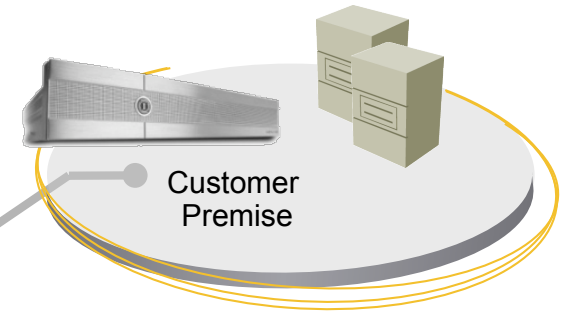
Объединенное управление

Customer

Message Tracking | Ticket Management | Reporting



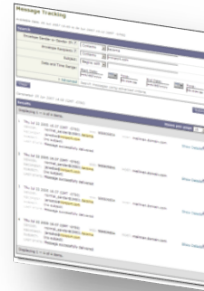
Reporting



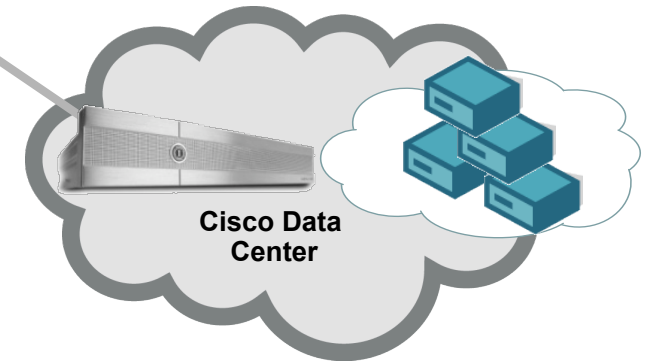
Shared Access & Control



Cisco



Configuration



System Health | System Upgrades | Config Changes



Внедрение



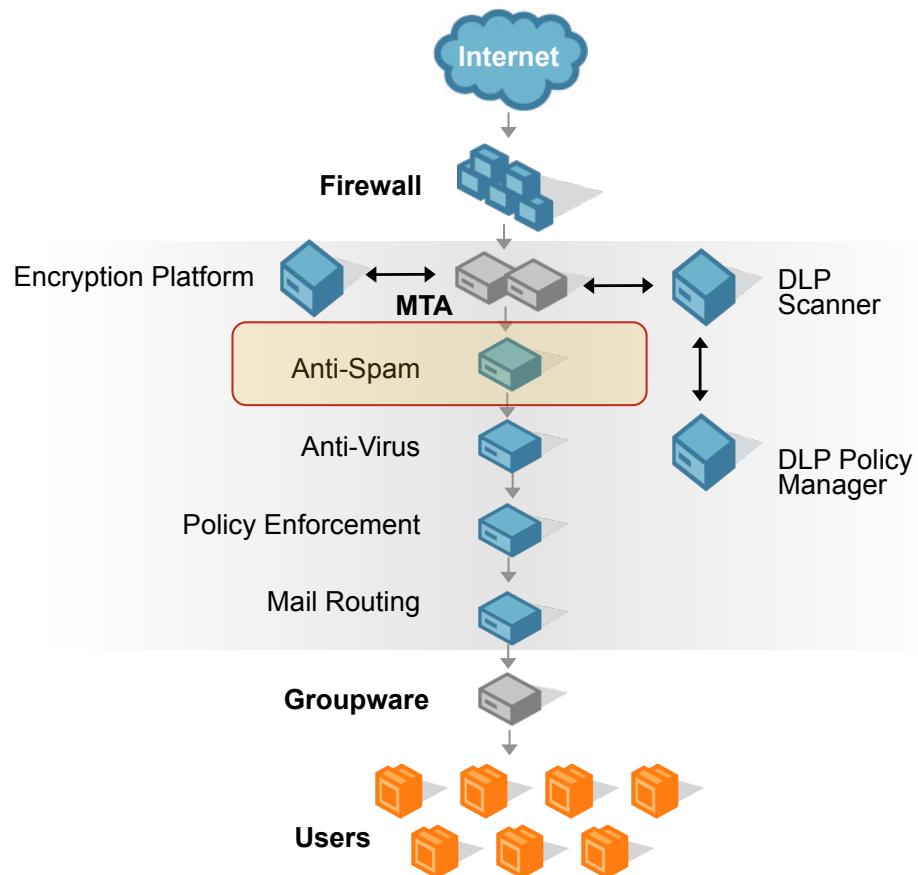
Hardware Specs

C-Series, X-Series

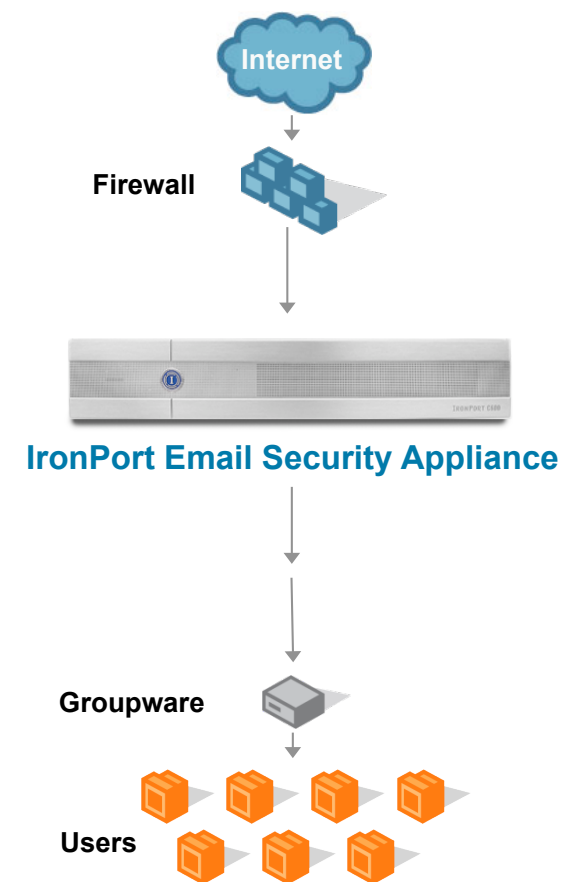
MODEL	C160	C360	C660	X1060
	1RU	2RU	2RU	2RU
CPU	1 X 2 Pentium 2.33 G	2x2 Xeon 2.33 G	2x4 Xeon 2.33 G	2x4 Xeon 2.833 G
RAM	4GB	4GB	4GB	4GB
Disk	2 x 250 GB RAID 1	2 x 300 GB RAID 1	4 x 300 GB RAID 10	6 x 300 GB RAID 10
Queue	10GB	35GB	70GB	70GB
PSU	1	2	2	2
Ethernet	2	3	3	3 (fiber option)

Внедрение IronPort

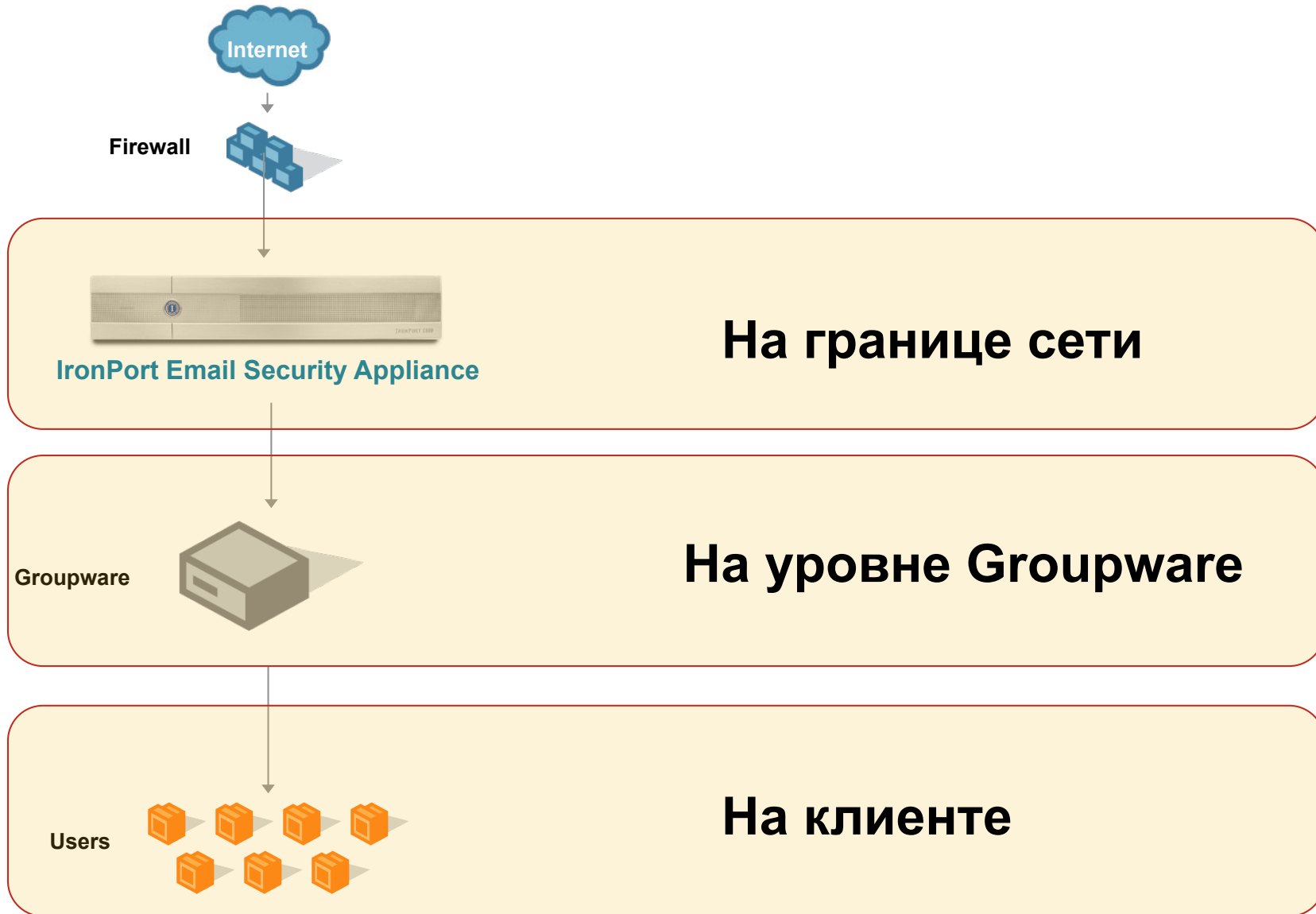
Before IronPort



After IronPort

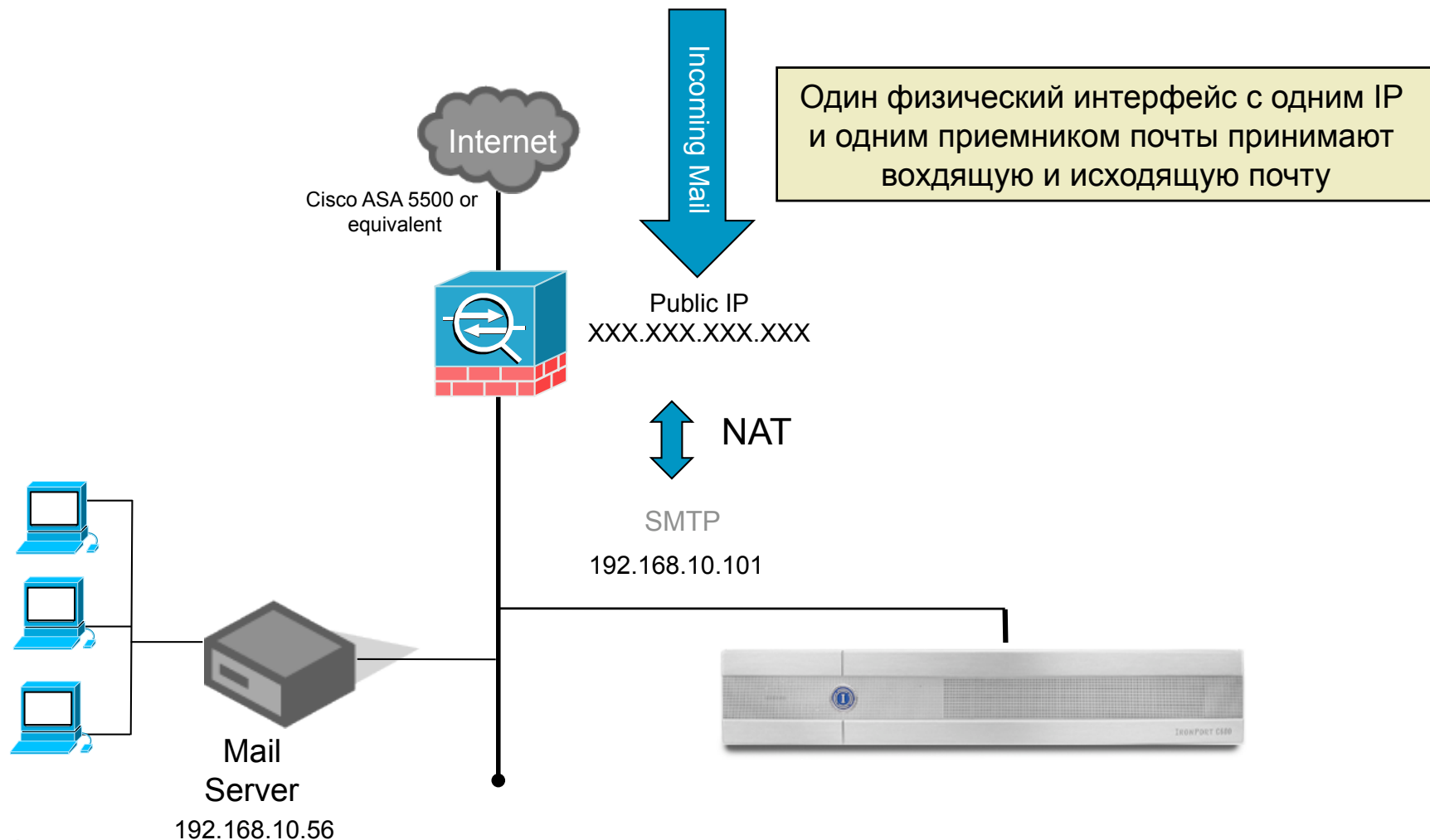


Где мы будем фильтровать?



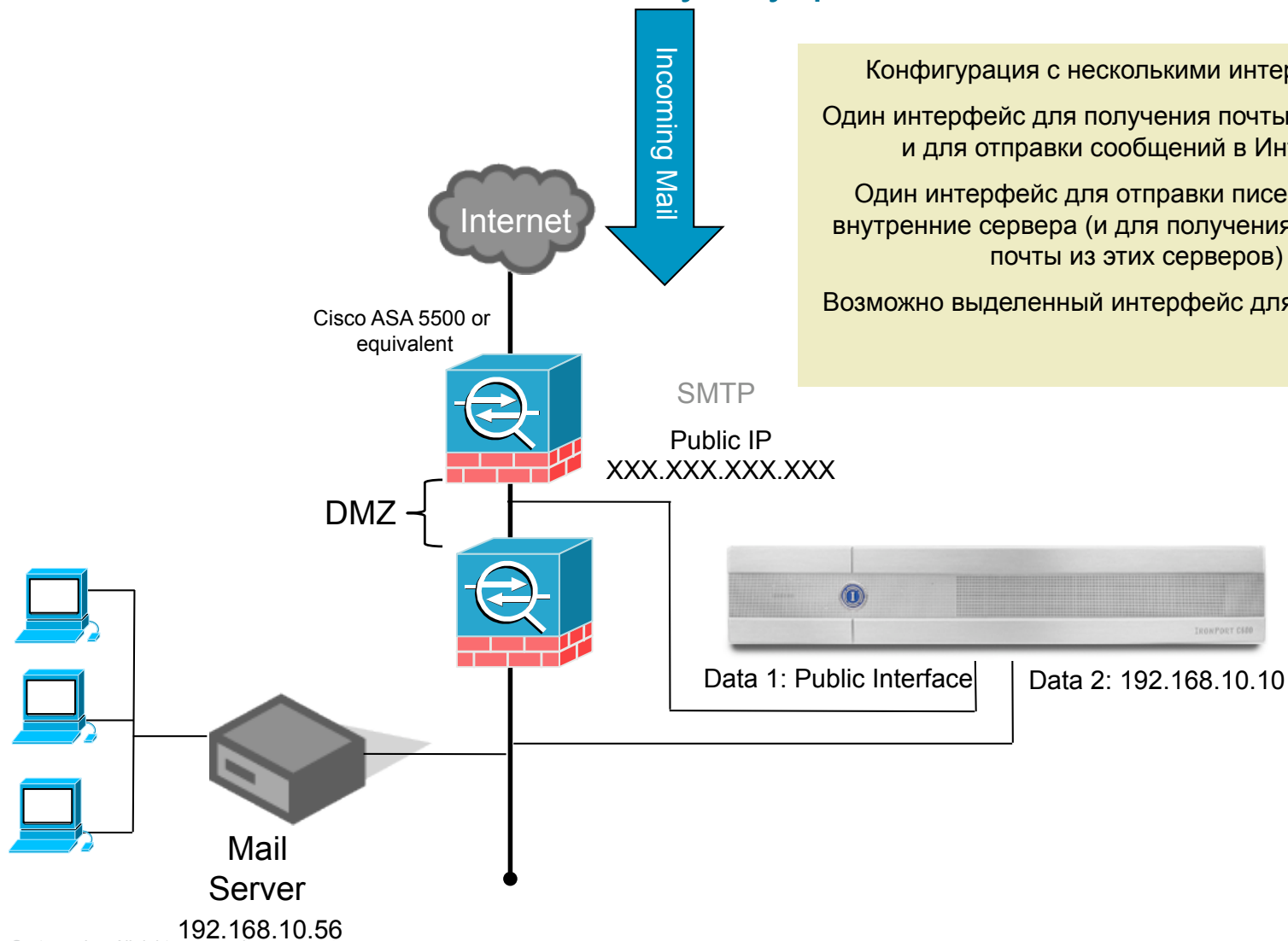
Внедрение с одним интерфейсом

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



Внедрение с двумя интерфейсами и DMZ

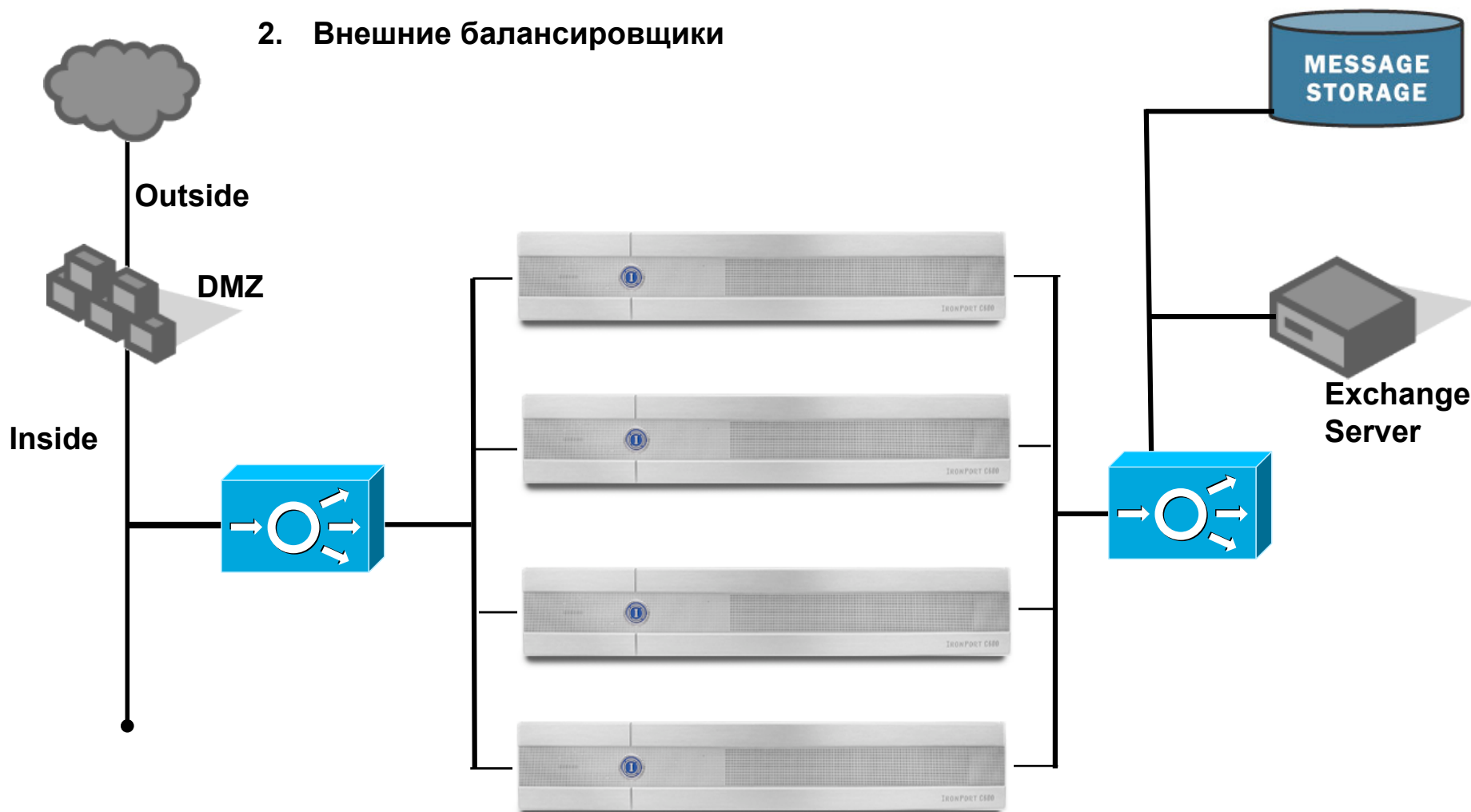
Мне нужен почтовый сервер с интерфейсом в DMZ для приема электронной почты. Этот интерфейс не может отправлять почту внутрь сети.



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.

Отказоустойчивость и балансировка нагрузки

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





95% of companies who try Cisco IronPort become customers.

Contact:
Your Cisco IronPort Rep

Вопросы и Ответы

