

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

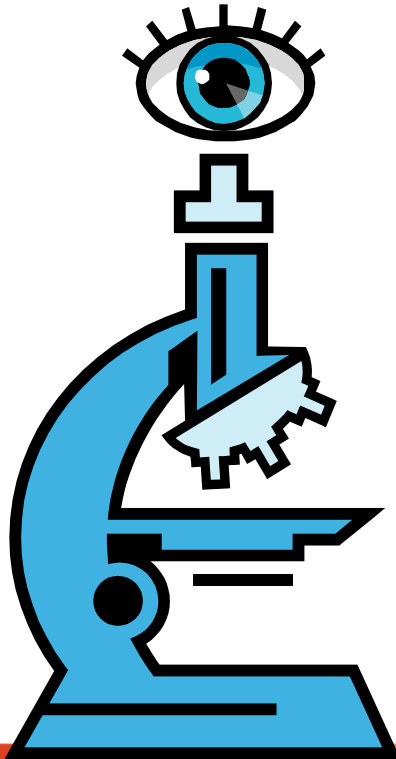


Расширенная безопасность



Глобальное смещение

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



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



Cisco Security Intelligence Operations (SIO) Обзор

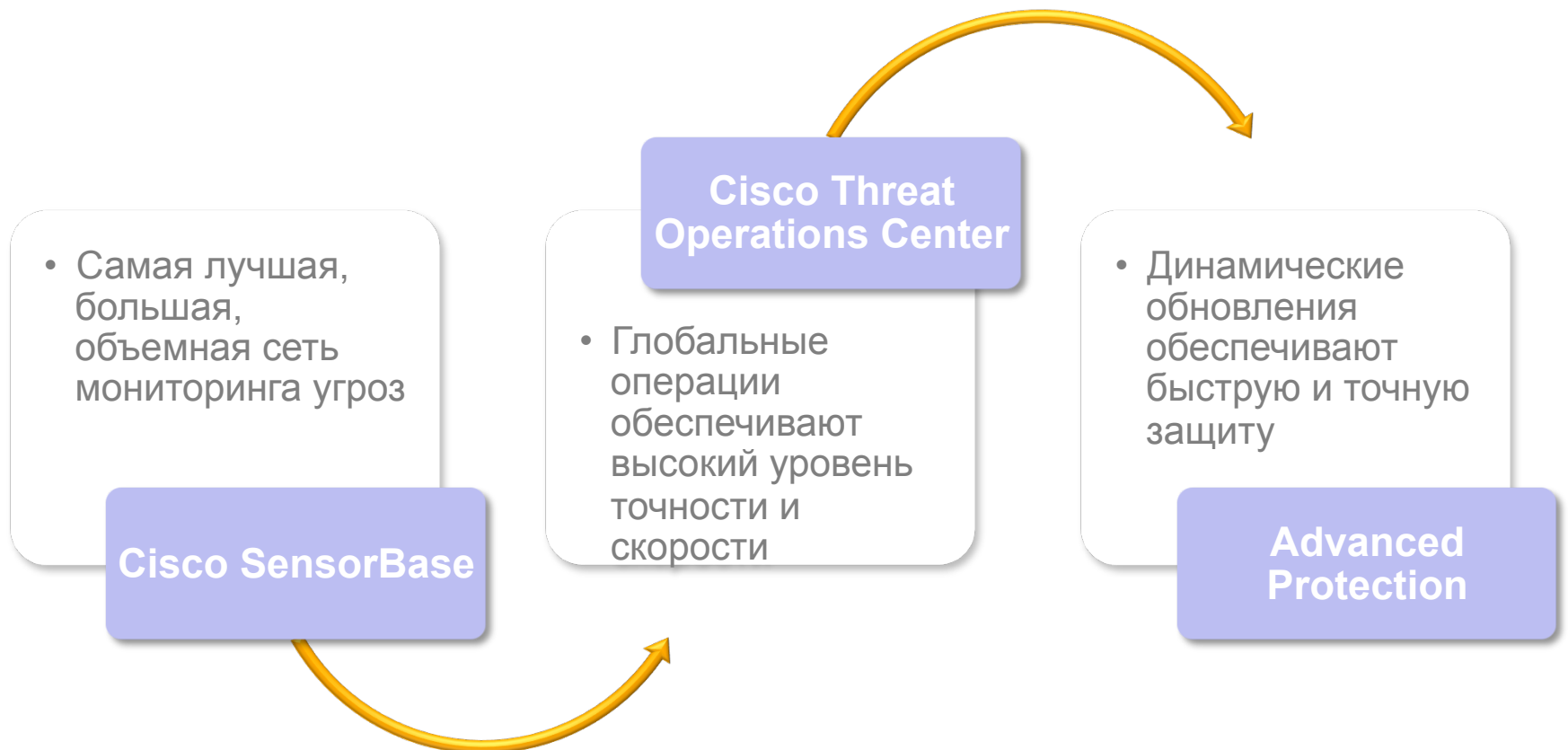
Более точная защита



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

1М устройств безопасности,
10М 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 крупнейших
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!
...channel and
with our f

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



Firewall / IPS



Directe

Прямая атака

Week 1	Thursday, September 08	Time (EST)	Top Passer	Top Rusher	Top Receiver			
	NO 10 @ BAL 4:15 PM	4:15 PM	IND Peyton Manning 268 Yds	IND Joseph Addai 118 Yds	IND Reggie Miller 115 Yds			
				DIRECTV	ESPN2			
Sunday, September 09	Time (EST)	Tickets	Network	Channel	HD-Channel	Home	Away	Weekend One
	SEA @ WAS 1:00 PM	Tickets	CBS	709	723	130	119	
	NFL @ NYJ 1:00 PM	Tickets	FOX	711	725	125	123	
	TEN @ JAC 1:00 PM	Tickets	CBS	707		108		
	CAR @ STL 1:00 PM	Tickets	FOX	712	726	147	146	
	NY @ CLE 1:00 PM	Tickets	CBS	705	720	153	151	
	NE @ NYG 1:00 PM	Tickets	CBS	708	722	122	151	
	IND @ GB 1:00 PM	Tickets	FOX	713	724	114	126	
	CIN @ BUF 1:00 PM	Tickets	CBS	704	719	110	143	
	HOU @ SD 1:00 PM	Tickets	CBS	706	721	140	157	
	NY @ DEN 4:15 PM	Tickets	FOX	715	726	119	147	
	DET @ OAK 4:15 PM	Tickets	FOX	714	725	106	123	
	CIN @ SD 4:15 PM	Tickets	FOX	713	724	125	132	
	NYG @ OAK 8:15 PM	Tickets	NBC	83		122	126	Radio

Сайт распространяющий malware

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



Parameters Under Management		
IP Address Reputation	19,111,326	30.4% corpora
URL Reputation	160,003,098	99.9% of Servers Co
Product Vulnerability	39,983	
Protocol Signatures	3,261	25.1% Vul



Out Security Rules	Deployment Interval	Last D
Email: IronPort Anti-Spam	5 minutes	2009-01-
Email: VOF	5 minutes	2009-01-
Firewall: Protocol Violation	1 week	2009-01-
Anomaly Detection	1 week	2009-01-
	15 minutes	
	5 minutes	

Опытные аналитики

500 аналитиков

Европейские и азиатские
языки

1 Cisco Fellow

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

Мощные инструменты

Динамические обновления
Корреляция и исследование
данных

Оптимизированное утверждение
правил, приложения для
создания и публикации

Работа 24x7x365

5 центров, расположенных
по всему миру

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

Cisco SIO

Лучшие возможности по применению

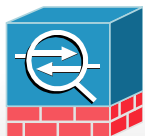
Быстрые механизмы сканирования и детальные политики



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.

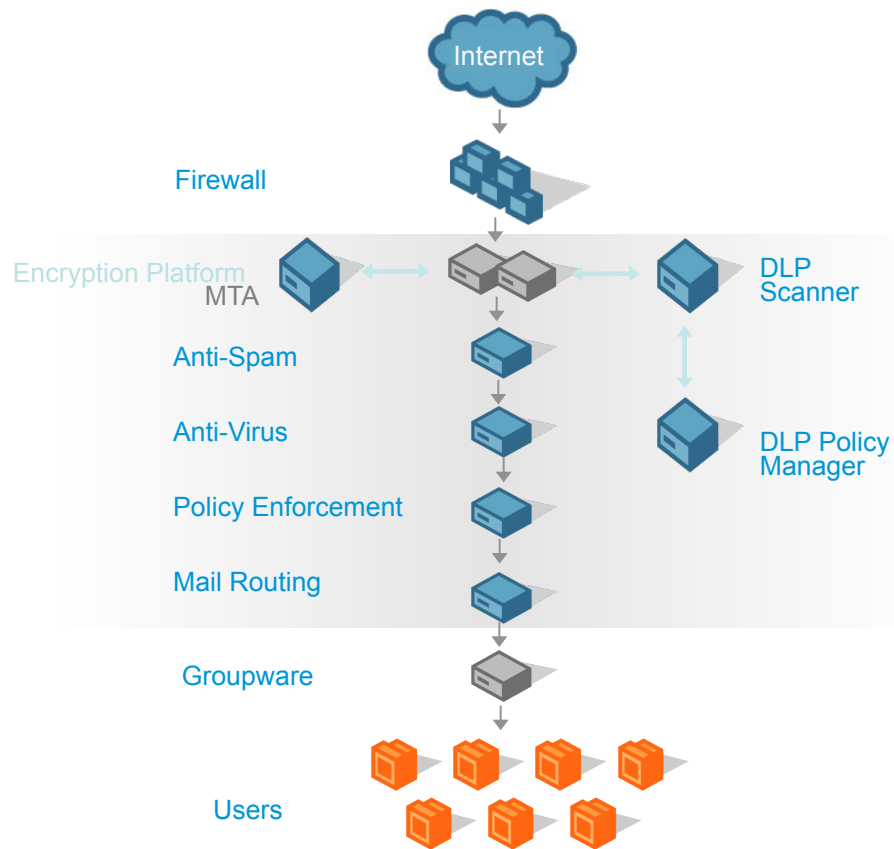
Cisco IronPort E-mail Security Appliances



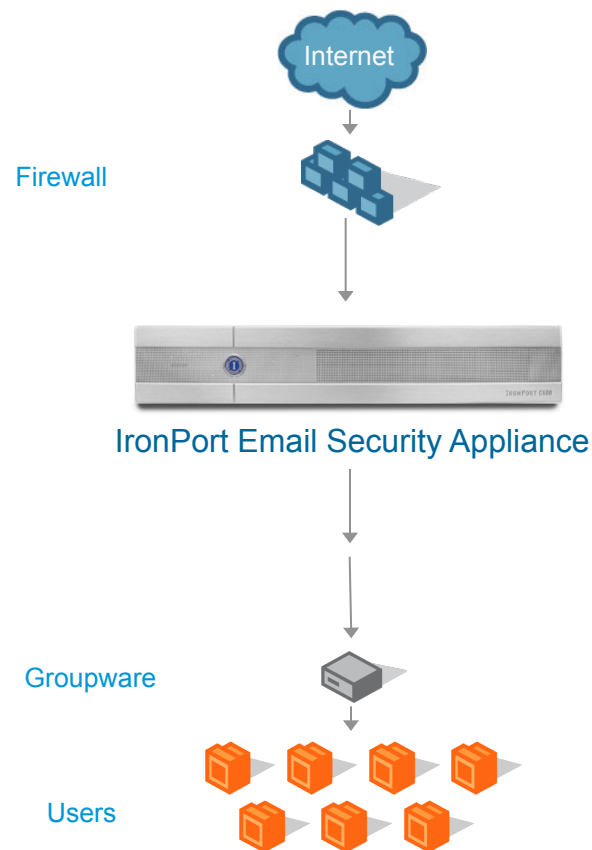
Cisco IronPort объединяет периметр сети

Для надежности, безопасности и снижения затрат на обслуживание

Перед IronPort



После IronPort

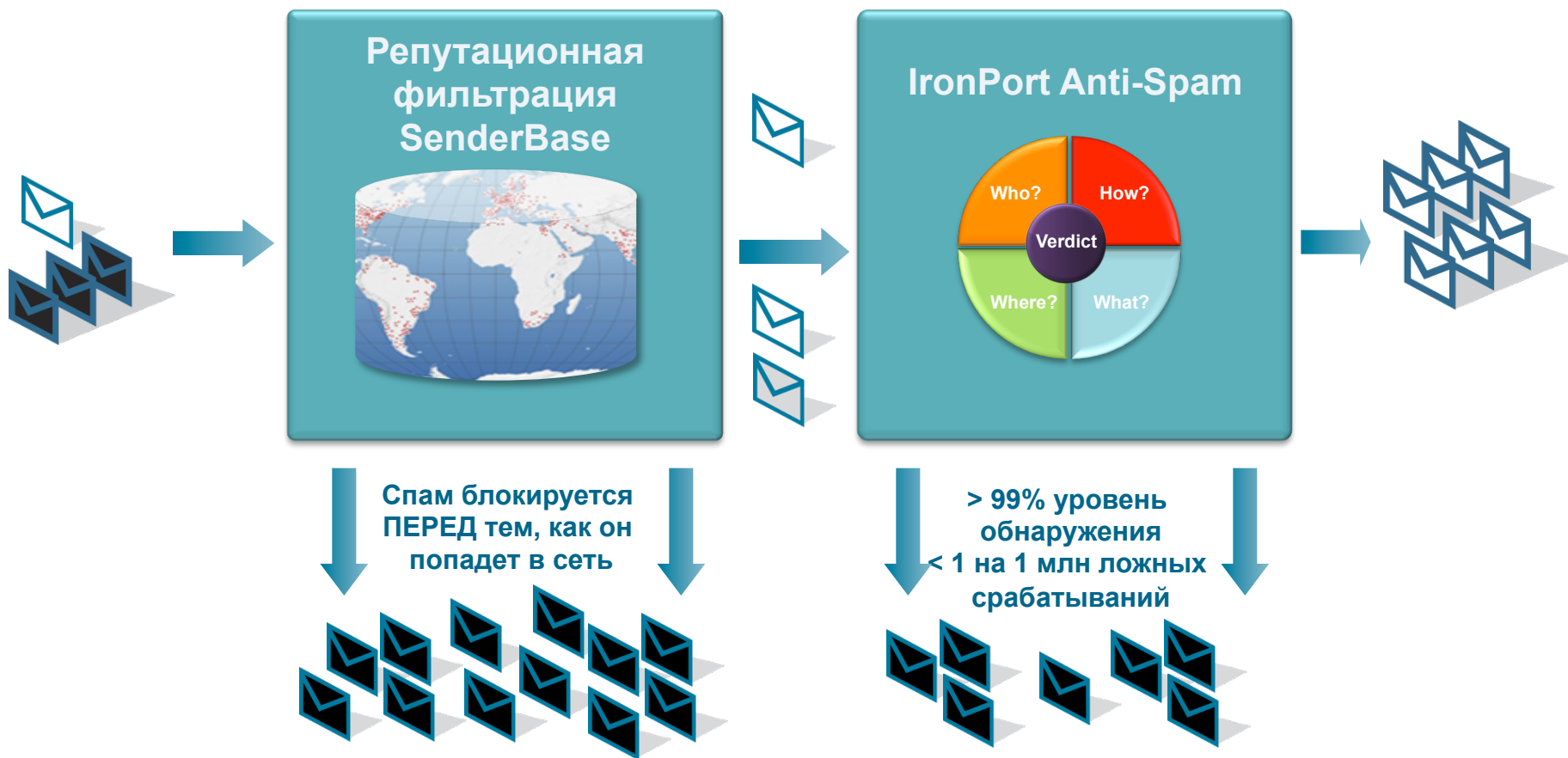


Email Security Architecture

Безопасность входящих, контроль исходящих



Антиспам – эшелонированная оборона



Репутационная фильтрация SenderBase

Предотвращение угроз в реальном времени



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



- ✓ Spam Botnets
- ✓ Spammer Networks

EMAIL REPUTATION

Кто?

- ✓ SMS Spam
- ✓ Attachment-based Spam

MESSAGE CONTENT

Что?

Verdict

WEB REPUTATION

Куда?

MESSAGE CONSTRUCTION

Как?

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

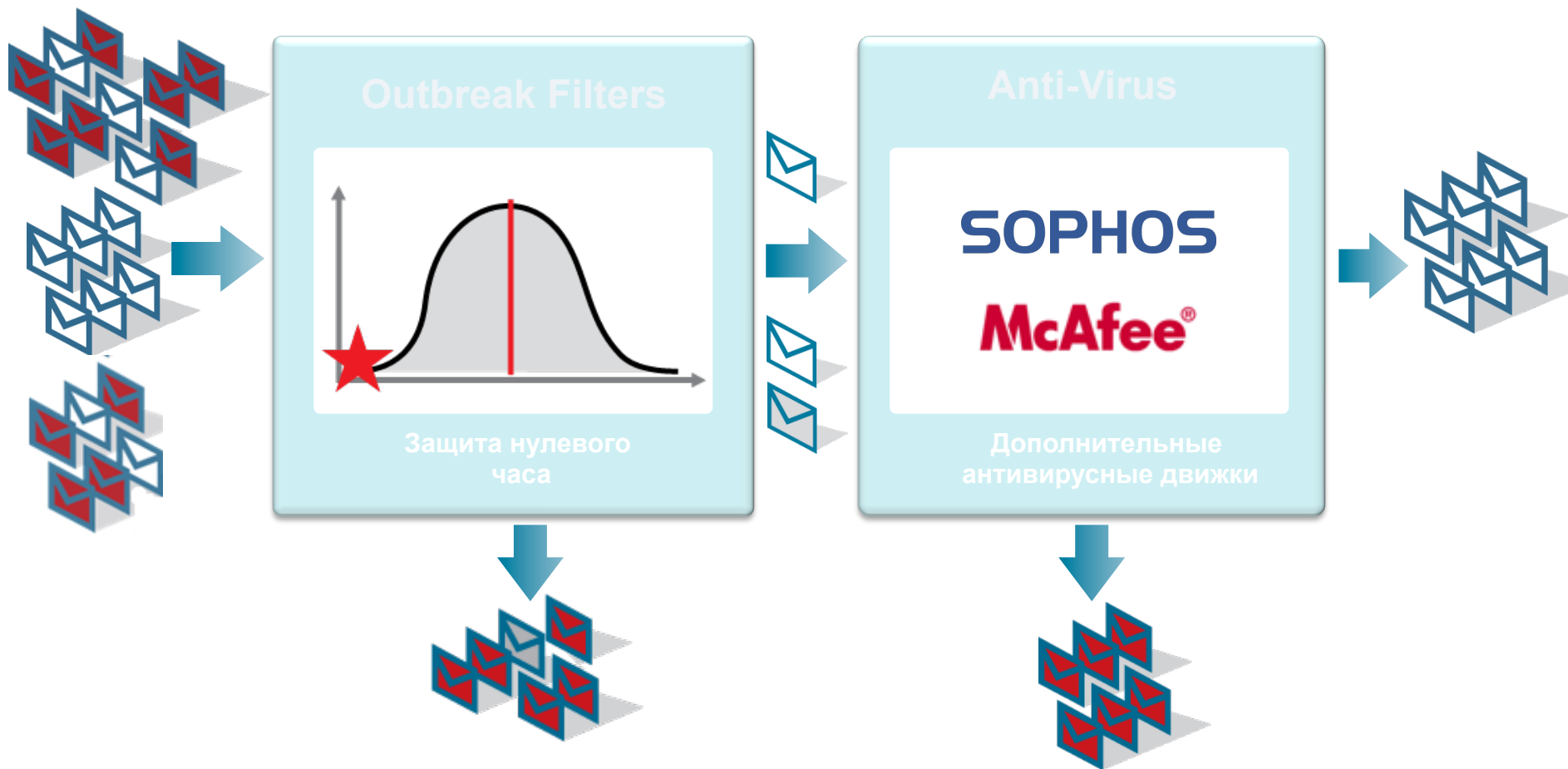
- ✓ Image Spam
- ✓ Spam created using Automation Tools

Email Security Architecture

Безопасность входящих, контроль исходящих



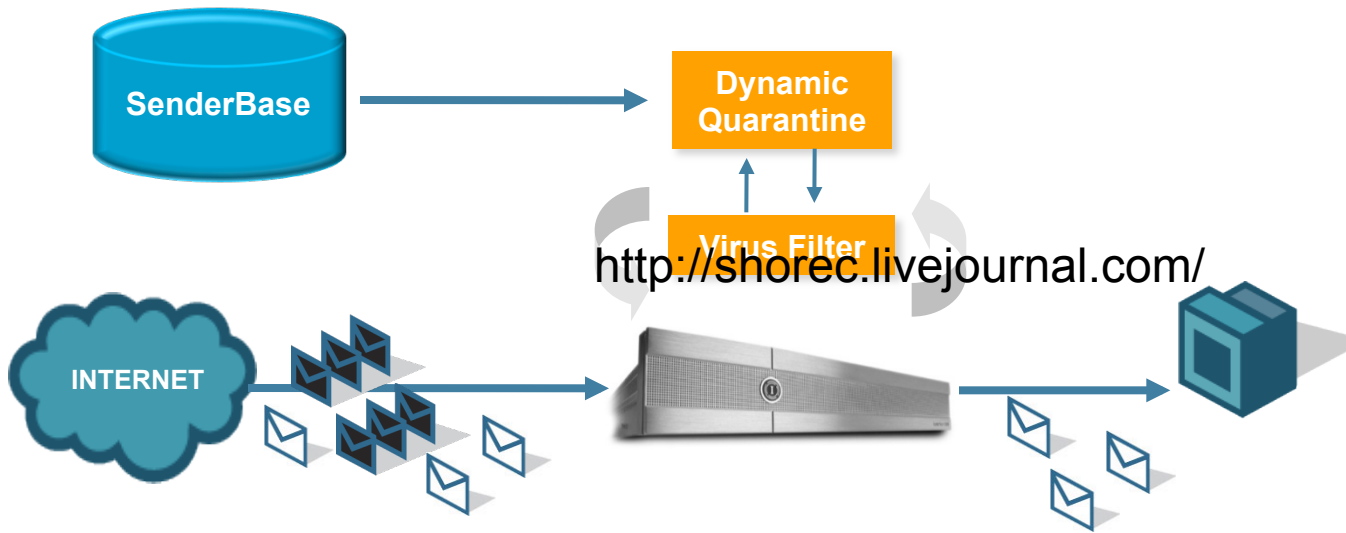
Эшелонированная антивирусная защита



Cisco IronPort Virus Outbreak Filters

Защита от malware нулевого дня

Virus Outbreak Filters в действии



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!”



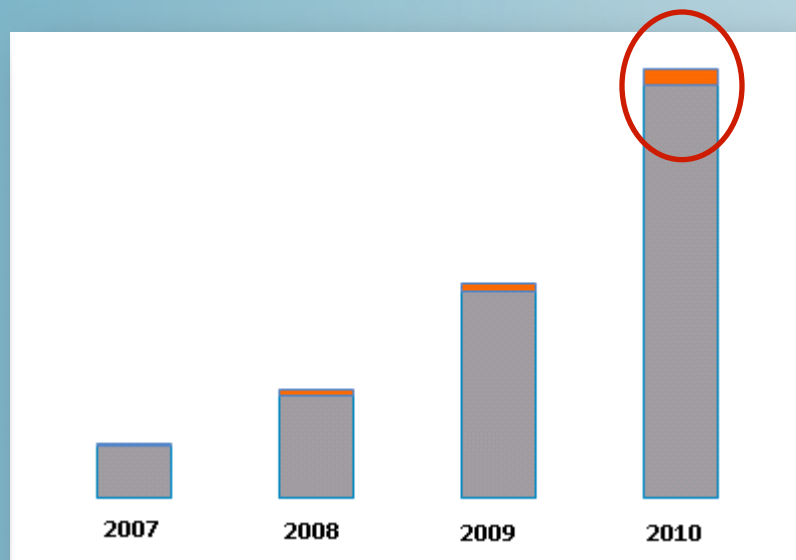
“Over 24,000 virus positive messages stopped in 9 months”



“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

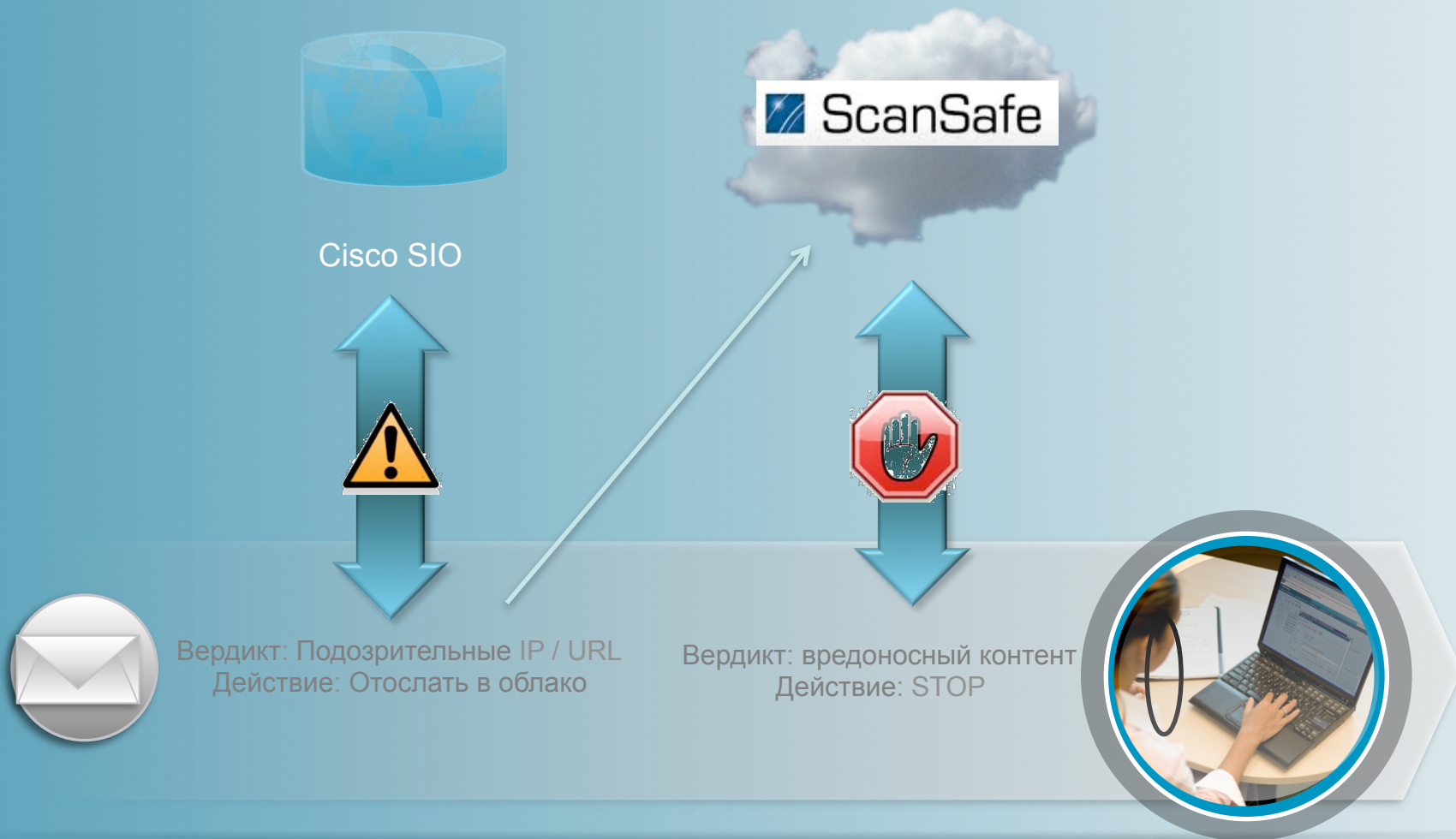
Outbreak фильтрация в действии



Delay

Перенаправление подозрительных URI

Outbreak фильтрация в действии



Redirect

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 ТОС/AV
 - Другие угрозы сканируются согласно рекомендуемому 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
- Использование predetermined categories/creation of their own
- Can be applied for specific users/specific conditions

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 <input type="text" value="1"/> <input type="button" value="v"/>
	<input checked="" type="checkbox"/>	Social Security Numbers <input type="text" value="1"/> <input type="button" value="v"/>
	<input checked="" type="checkbox"/>	ABA Routing Numbers <input type="text" value="1"/> <input type="button" value="v"/>
	<input checked="" type="checkbox"/>	CUSIPs <input type="text" value="1"/> <input type="button" value="v"/>

Data Loss Prevention

Всесторонние опции реагирования и отчетности

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

The screenshot displays a 'Quarantine' configuration window. On the left is a scrollable list of actions, and on the right is a detailed view of the 'Quarantine' action.

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:

Duplicate message

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

RSA – Рынок рынка и технологий



at&t



Microsoft®



CVS
CAREMARK

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

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

Всестороннее закрытие политиками

100+ Предопределенных политик для полного покрытия

Regulatory Compliance	
Add	Payment Card Industry Data Security Standard (PCI-DSS)
Add	PIPEDA (Personal Information Protection and Electronic Documents Act)
Add	FERPA (Family Educational Rights and Privacy Act) <i>Customization recommended.</i>
Add	GLBA (Gramm-Leach Bliley Act) <i>Customization recommended.</i>
Add	HIPAA (Health Insurance Portability and Accountability Act) <i>Customization recommended.</i>
Add	SOX (Sarbanes-Oxley)

Privacy Protection	
Add	ABA Routing Numbers
Add	Australia Bank Account Numbers
Add	Australia Business and Company Numbers
Add	Australia Medicare Card Numbers
Add	Australia Tax File Numbers
Add	Canada Drivers License Numbers
Add	Canada Social Insurance Numbers
Add	Contact Information
Add	Credit Card Numbers
Add	Custom Account Numbers <i>Customization recommended.</i>
Add	EU Debit Card Numbers
Add	France BIC Numbers

Add DLP Policy from Templates	
Display Settings: Expand All Categories Display Policy Descriptions	
▸ Regulatory Compliance	●
▸ US State Regulatory Compliance	
▸ Acceptable Use	
▸ Privacy Protection	●
▸ Intellectual Property Protection	
▸ Company Confidential	
▸ Custom Policy	●

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

Полный набор опций реагирования

Quarantine ▾

Enable Encryption
Encryption Profile: CRES Encryption ▾

Encrypted Message Subject: \$subject

Apply TLS if message encryption fails.

Policy Quarantine: Policy ▾

Message Modifications

Автоматическое реагирование

Encrypt, quarantine, deliver, or drop

Add disclaimer, modify subject

Copy or notify

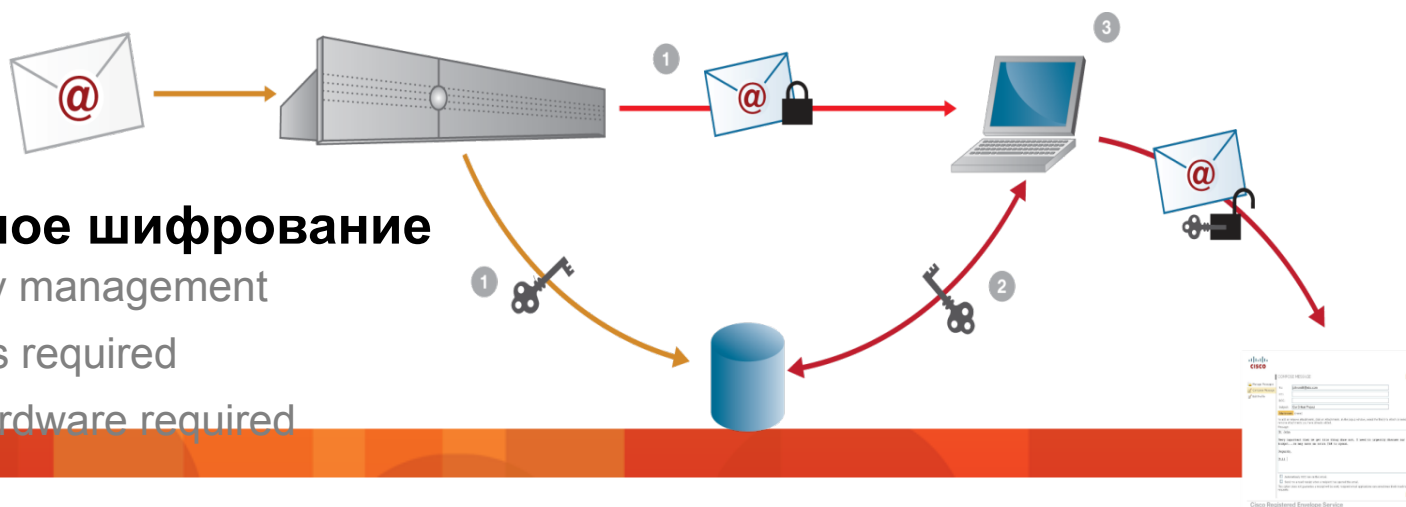
Guaranteed secure delivery

Встроенное шифрование

Hosted key management

No plug-ins required

No new hardware required



Email Security Architecture

Безопасность входящих, контроль исходящих



Препятствия к внедрению

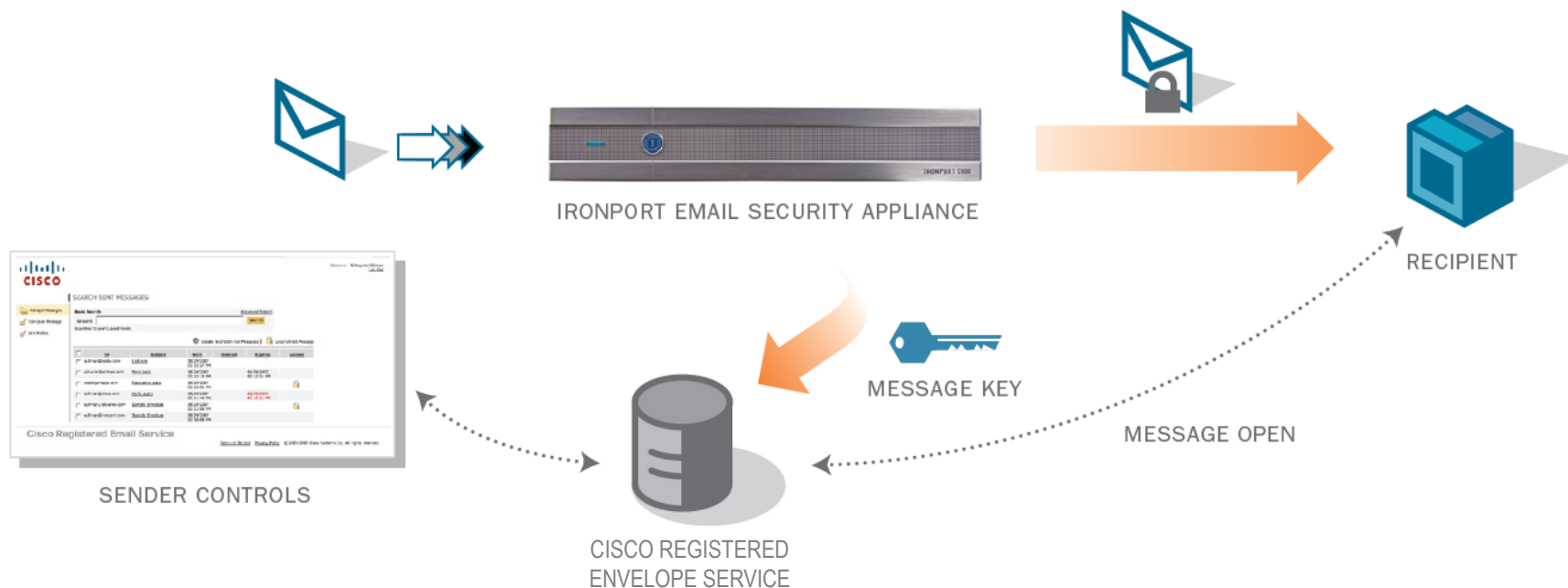
Почему шифрование email еще не внедрено везде?

- **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**
 - Требуется уже настроенная система криптографических связей
 - Отправка/получение ограниченным набором клиентов с плагинами



Шифрование Cisco IronPort Email

Просто для отправителя. . .



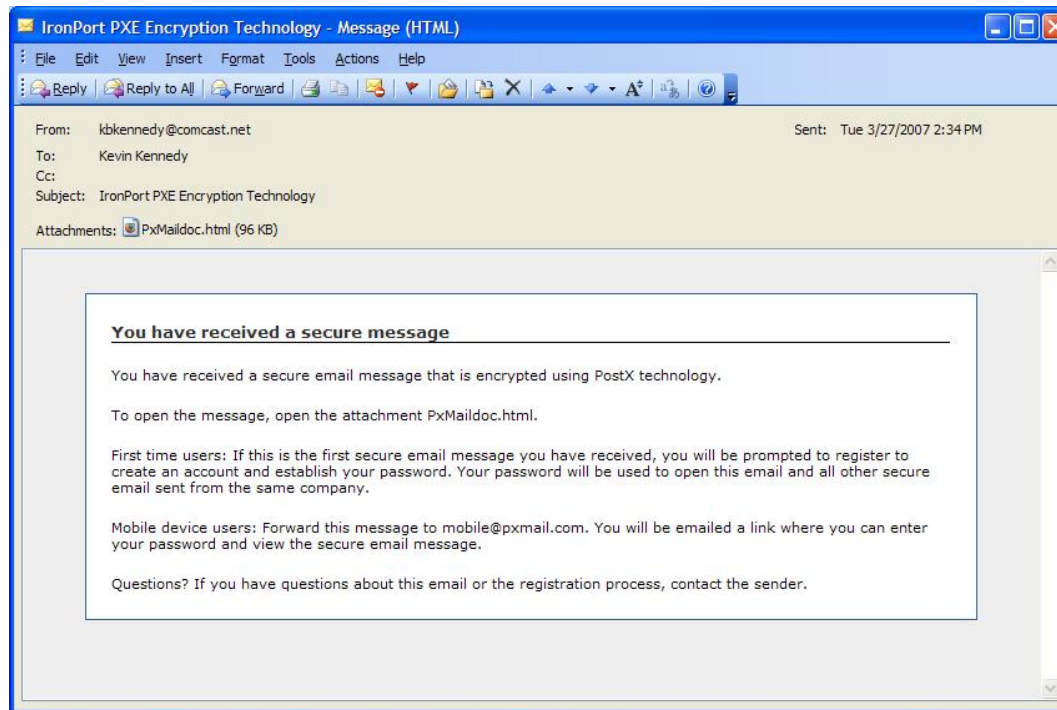
- Автоматическое управление ключами
- Не требуется дополнительное ПО
- Прозрачная отправка на любой email

Шифрование Email Cisco IronPort

Получение сообщения

1

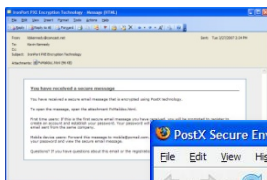
Получите почту, кликните для открытия присоединенного файла



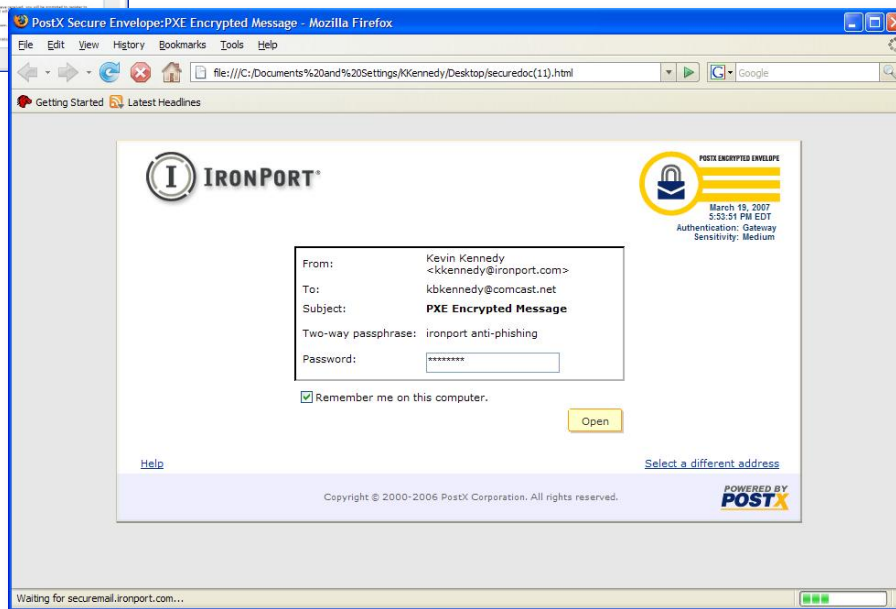
Шифрование Email Cisco IronPort

Получение сообщения

1 Получайте почту



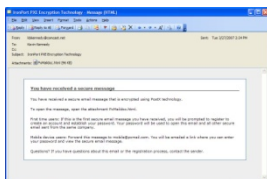
2 Введите пароль



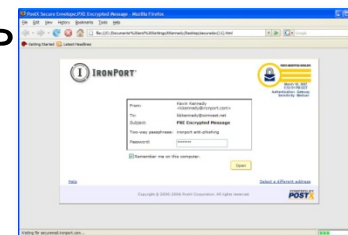
Шифрование Email Cisco IronPort

Получение сообщения

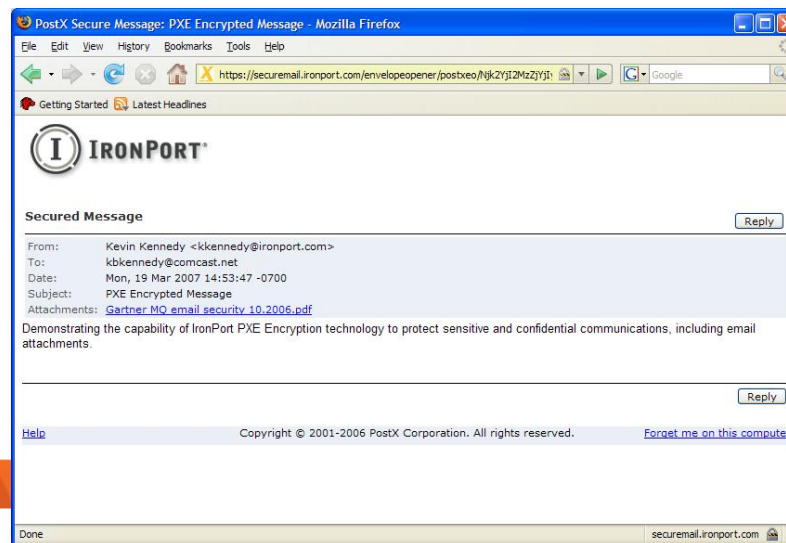
1 Получите письмо



2 Введите пароль



3 Просмотрите защищенное сообщение



Решение ограничений других продуктов шифрования Email

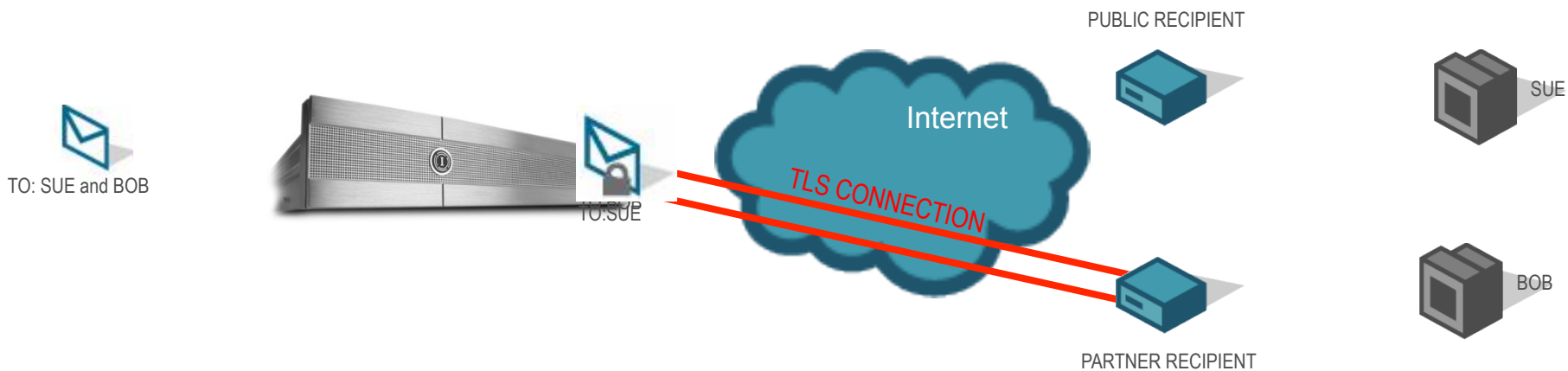
- **Простота использования -- решено**
 - Сложные плагины и вмешательство в работу пользователей
 - Public Key и Identity ManagementНет клиентского ПО, нет сертификатов
- **Простота внедрения -- решено**
 - Поддержка плагинов
 - Public Key и инфраструктура Identity ManagementIronPort Hosted Key Service
- **Универсальность -- решено**
 - Требуется уже настроенная система криптографических связей
 - Отправка/получение ограниченным набором клиентов с плагинамиОтправка-получение с любой платформы



Гарантированная безопасная доставка

Шифрование почты по назначению

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



Email Security Architecture

Безопасность входящих, контроль исходящих



Cisco IronPort Email Security Manager

Просмотр 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,
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

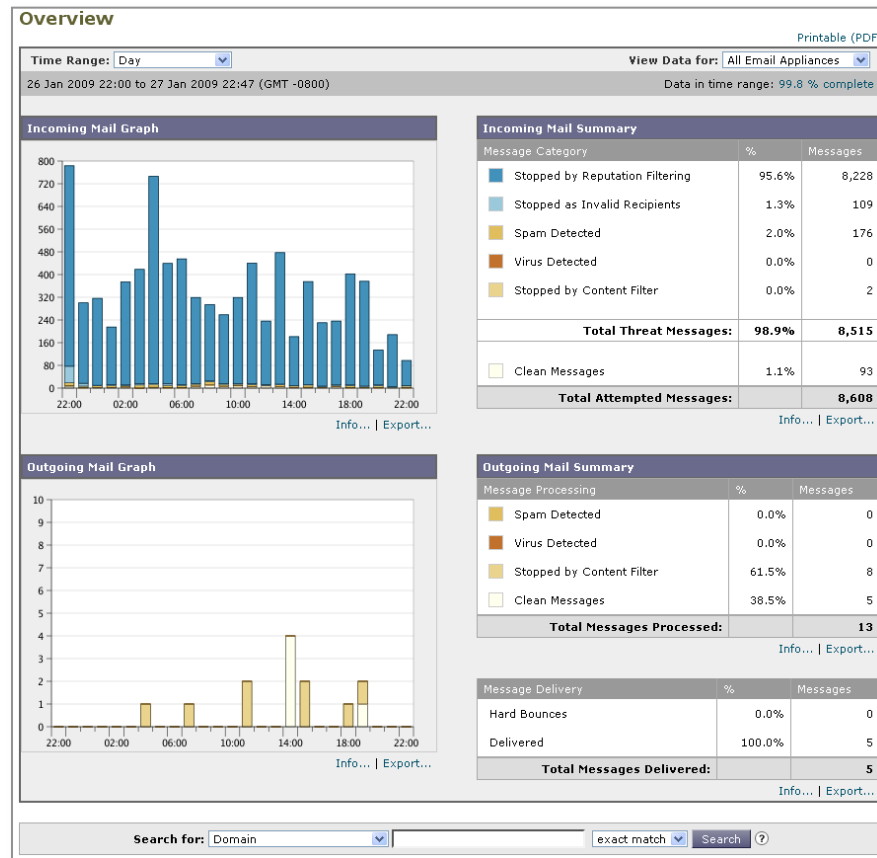
“IronPort Email Security Manager работает в качестве простой, гибкой панели всех настроек устройства.” – PC Magazine

Всесторонний просмотр

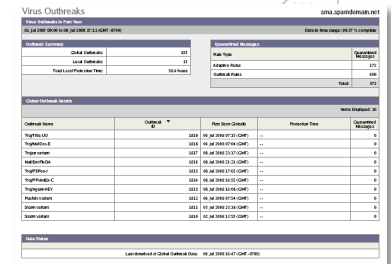
Система унифицированного репортинга

Объединенные отчеты

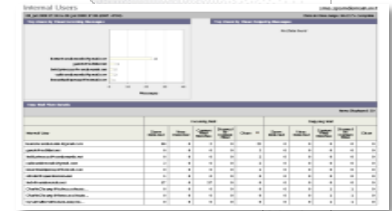
- Простой просмотр в организации
- Трафик реального времени Email и угроз
- Иерархические исполняемые отчеты



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 гарантии
соответствия

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:	End Date:	Time:
	01/26/2009	22:00	and	01/27/2009 22:52 (GMT -0800)
▼ Advanced				
Sender IP Address:				
	<input type="radio"/> Search rejected connections only <input checked="" type="radio"/> Search messages			
Message Event:	<i>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.</i>			
	<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

Скоро...

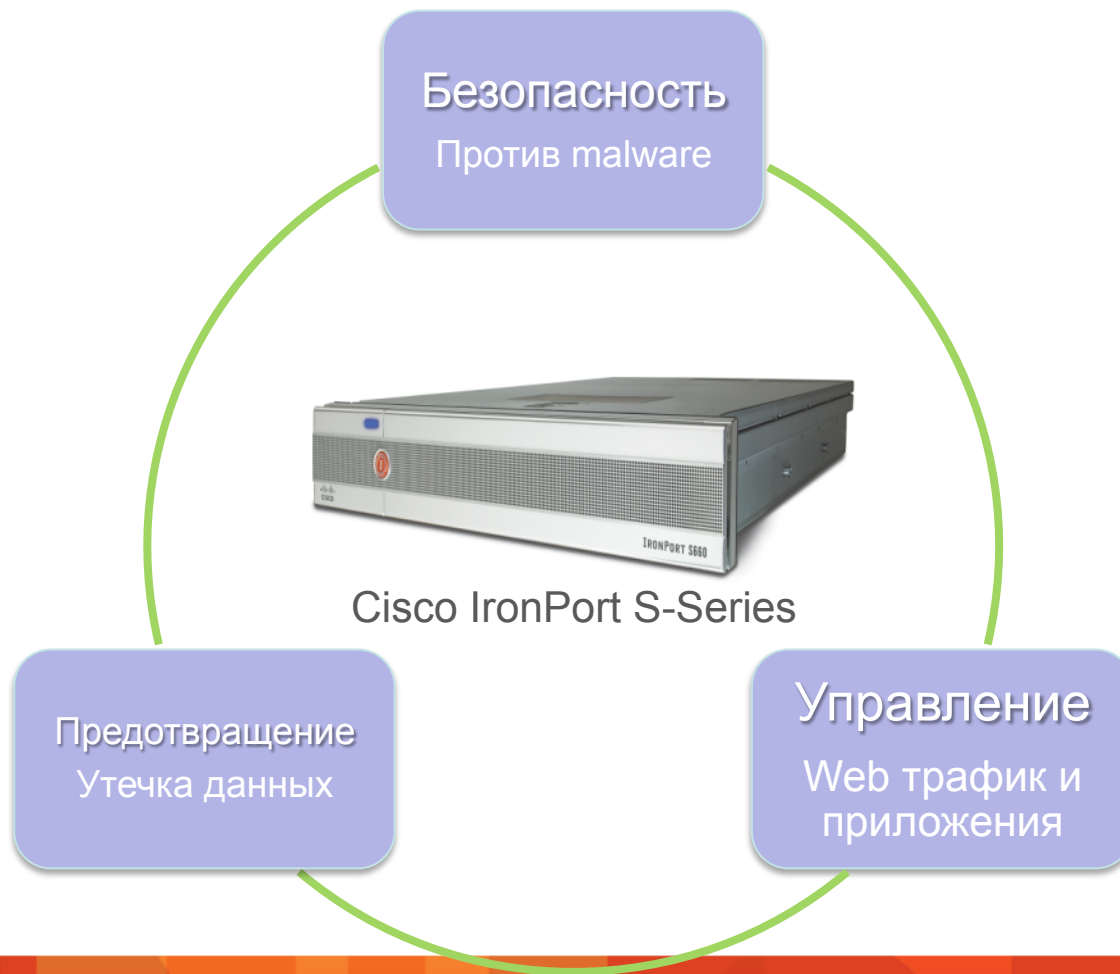
- Outbreak Filters
- Делегированное администрирование
- Поддержка «сильных» паролей
- SMTP Call Ahead

Cisco IronPort Web Security Appliances



Cisco IronPort Secure Web Gateway

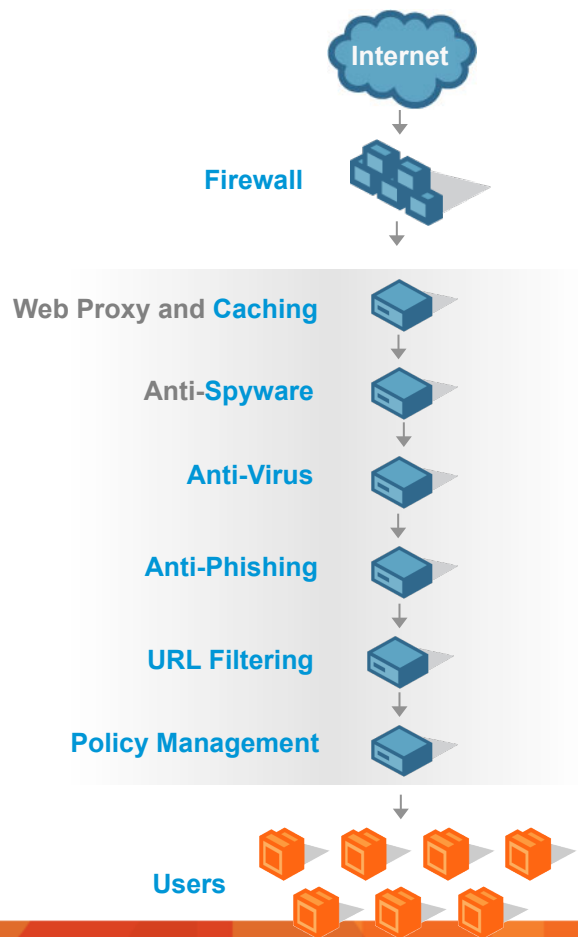
Решение бизнес-проблем



Шлюз Web-безопасности следующего поколения

Объединение увеличивает эффективность работы

Перед Cisco IronPort



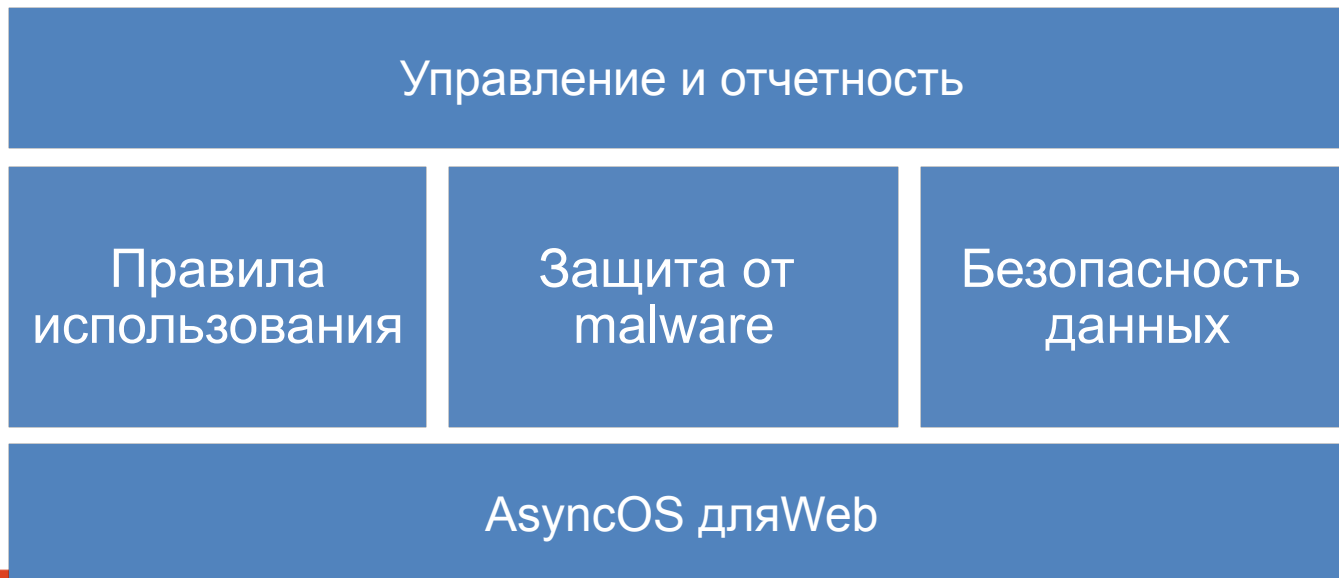
После Cisco IronPort



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 предлагает оптимальное TCO



Правила использования

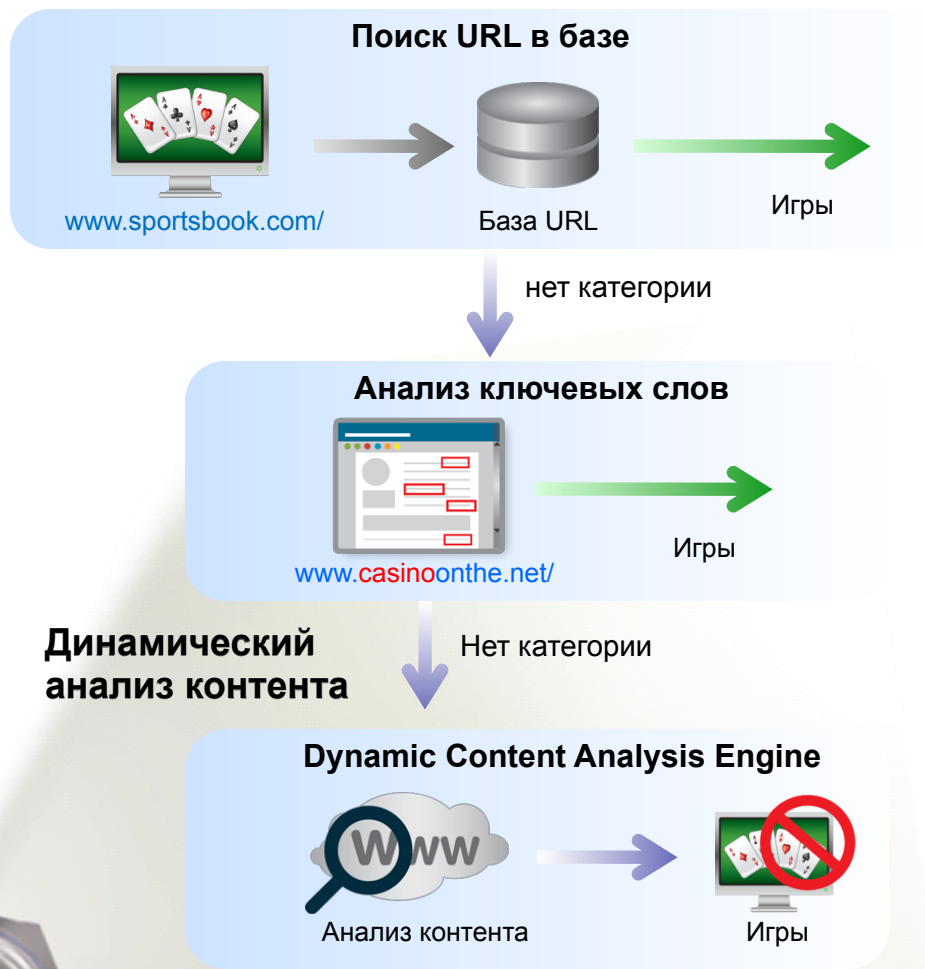
Просмотр и управление Web-трафиком и Web-приложениями



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

Представляем технологию Cisco IronPort Web Usage Controls

Луч света в темном Web

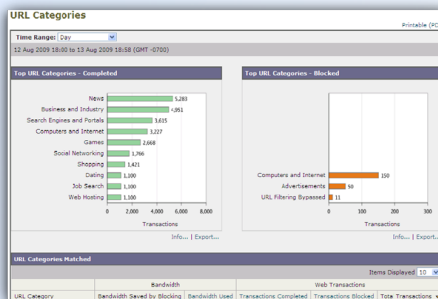
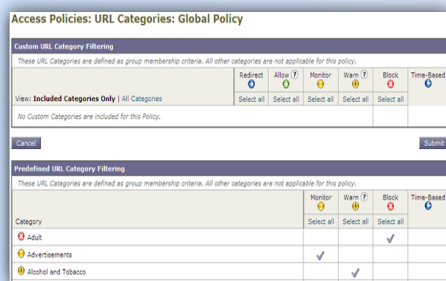


- Одна из самых эффективных баз URL
 - 65 категорий
 - Обновления каждые 5 минут
 - Использует Cisco SIO
- Динамический анализ контента позволяет определить 90% of «темного» Web



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

Collaboration



Software as a Service



Tunneled Applications

`ftp://ftp.funet.fi/pub/`



HTTP

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

Офисный
работник



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

Точный контроль над использованием Web

Новые приложения: Facebook

Access Policies: Applications Visibility and Control: Global Policy

Default Actions for Application Types	
Application Types	Default Action for Type
Facebook	🟡 Monitor
Instant Messaging	🟡 Monitor
Media	🟡 Monitor Bandwidth Limit: No Bandwidth Limit
P2P / File Sharing	🟡 Monitor
Presentation / Conferencing	🟡 Monitor
Social Networking	🟡 Monitor

Edit Applications Settings

Browse Application Types Applications Info

To identify some applications, inspection of HTTPS content may be required. For best efficacy, enable the HTTPS Proxy, then select the option that enables decryption for application visibility and control (see Security Services > HTTPS Proxy).

Applications	Settings
Facebook	🔴 3 Block 🟡 12 Monitor Edit all...
Instant Messaging	🟡 4 Monitor Edit all...
Media	🟡 11 Monitor

Edit Facebook Controls



Детальный контроль Facebook

Set action for application Facebook General

Use Setting from Type (Monitor)

Monitor

Block Posting Text

Block Like/Tag

Block Installation of Third Party Applications

Block

Cancel

Set action for application Facebook Photos

Use Setting from Type (Monitor)

Monitor

Block File Upload

Block Posting Text

Block Like/Tag

Block

Cancel Apply

- 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

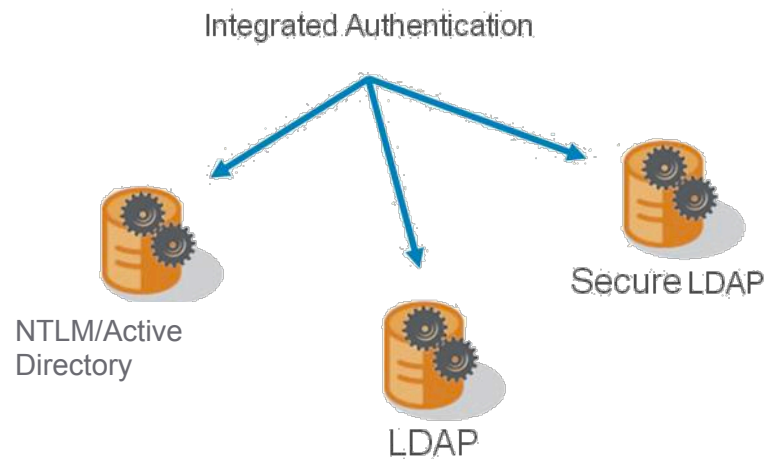
Интегрированная идентификация и аутентификация

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

Access Policies

Policies						
Order	Group	Applications	URL Categories	Objects	Web Reputation and Anti-Malware Filtering	Delete
1	Sales Policy Identity: Sales	Block: FTP over HTTP Allow: HTTP, HTTPS, Native FTP Allow: Ports 20, 21,....	Redirect: 0 Allow: 0 Monitor: 36 Warn: 0 Block: 14 Used: 3	Block: Object Types HTTP/HTTPS Object Max Size: None FTP Object Max Size: None	(global policy)	
2	Technical Groups Policy Identity: Engineering	(global policy)	(global policy)	(global policy)	(global policy)	
	Global Policy Identity: All	Allow: FTP over HTTP, HTTP, ... Allow: Ports 8080, 21,....	Allow: 0 Monitor: 37	HTTP/HTTPS Object Max Size: None FTP Object Max Size: None	(enabled)	



Define Acceptable Use and Data Security Policies
using Rich Identity Constructs

Правила использования

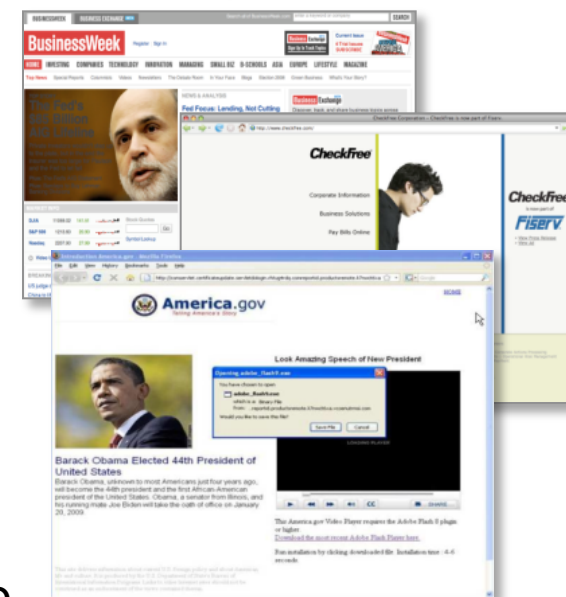
Просмотр и управление Web-трафиком и Web-приложениями



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

Многоуровневая защита от Malware

Защита от современных угроз



- 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

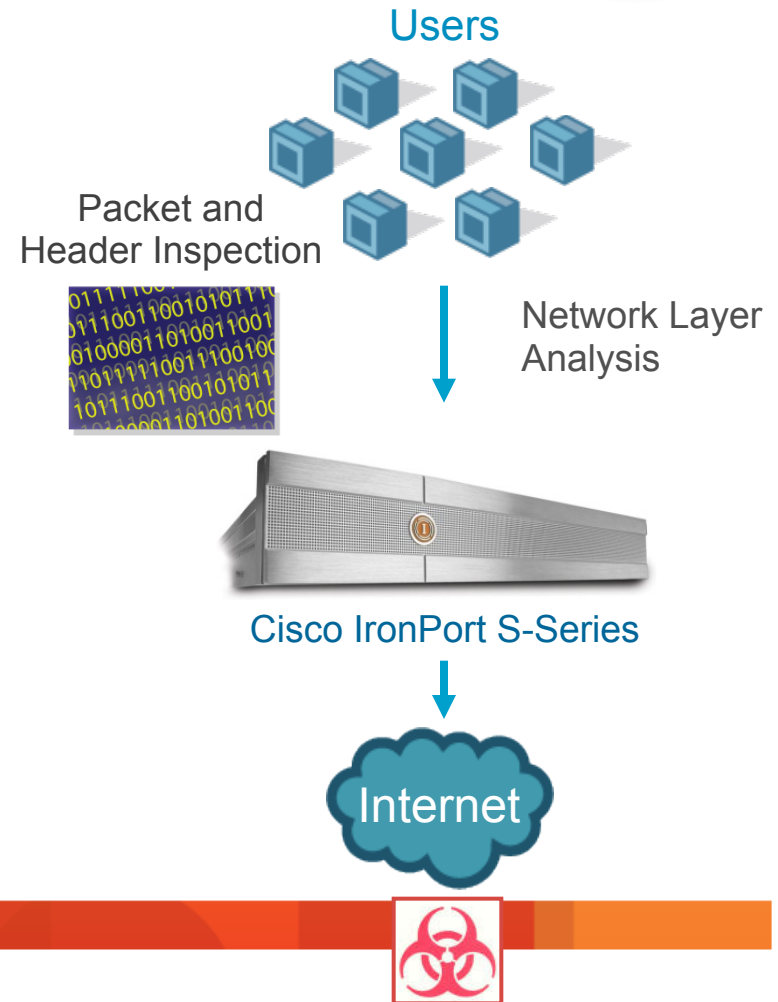
Обнаружение malware, которое не использует порт 80

Блокирует трафик ботнетов

- Мощные данные анти-malware

Автоматически обновляемые правила

Генерирование правил в реальном времени с помощью механизма “Dynamic Discovery”





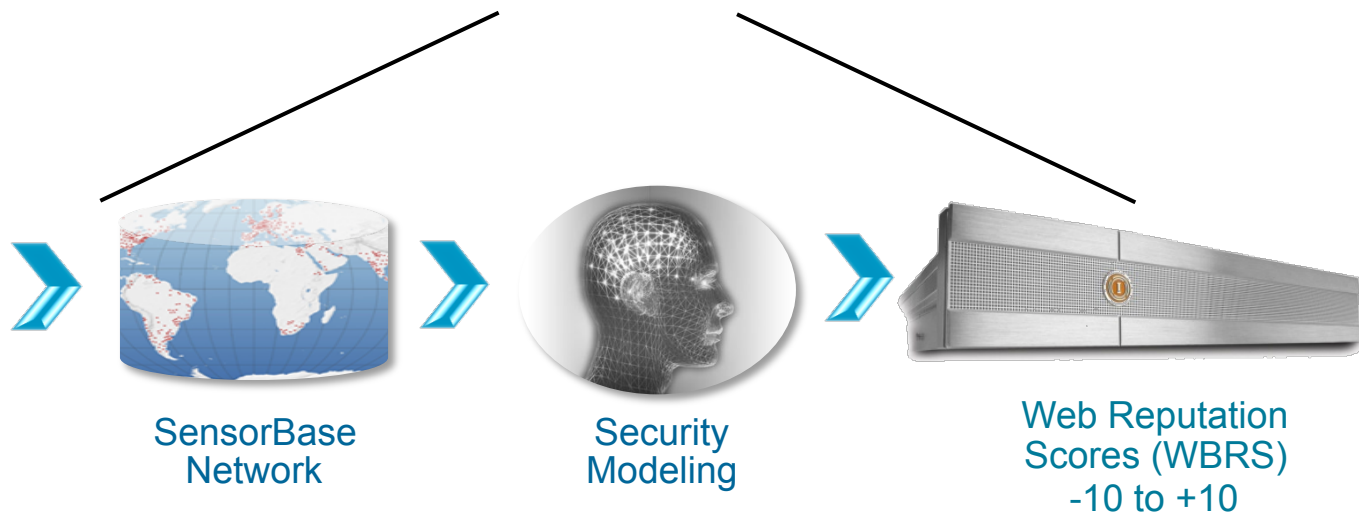
Фильтры web-репутации

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

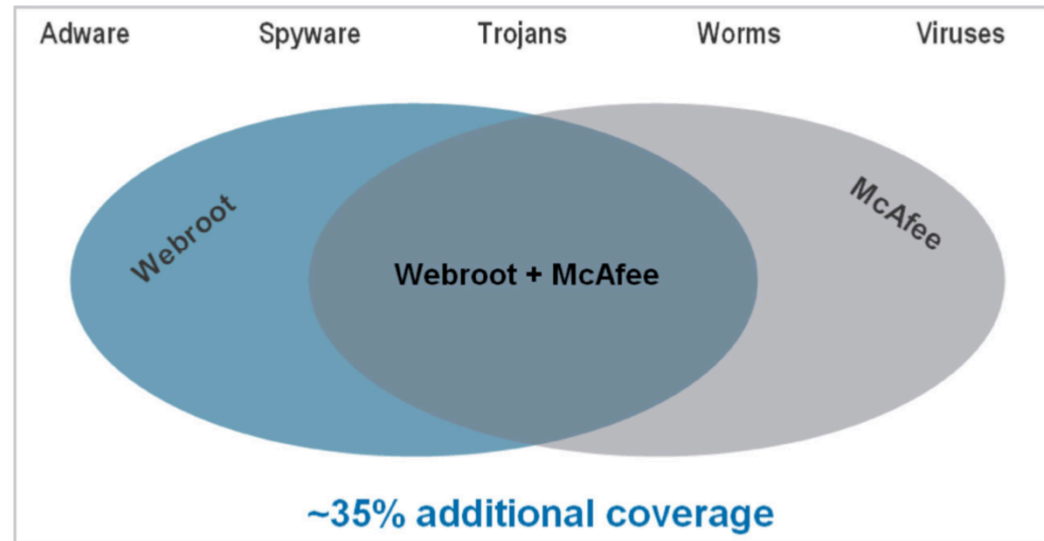
Cisco Security Intelligence Operations



Механизм IronPort DVS

Dynamic Vectoring and Streaming

- Ускоренное сигнатурное сканирование
 - Параллельное сканирование
 - Потокное 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»

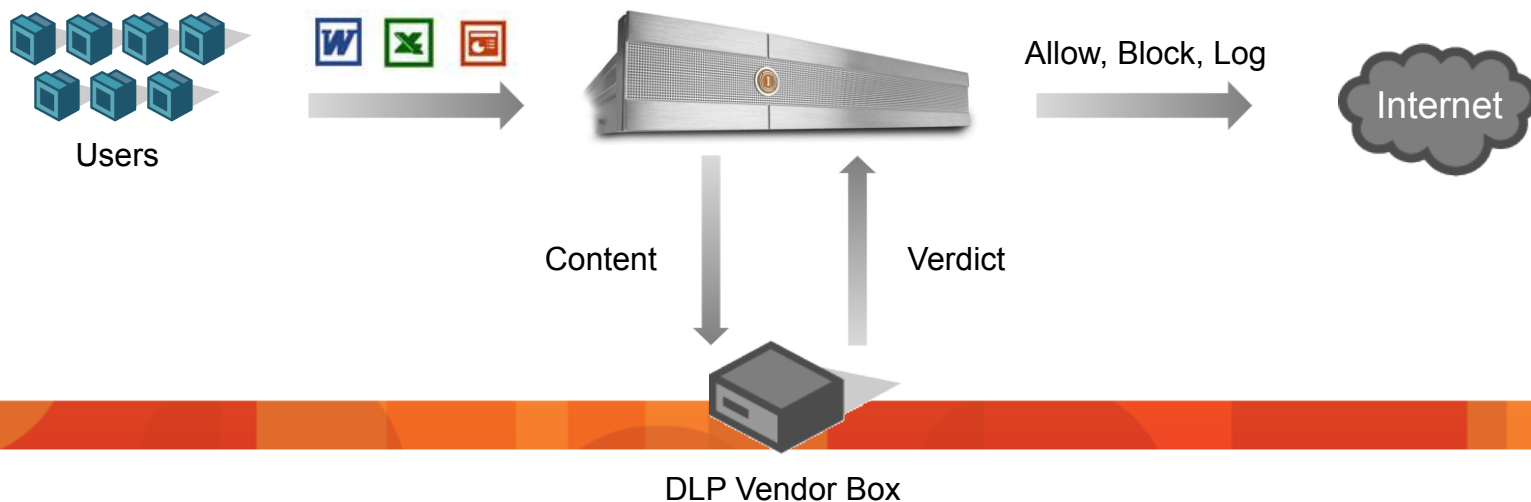
Простой подход к безопасности данных

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

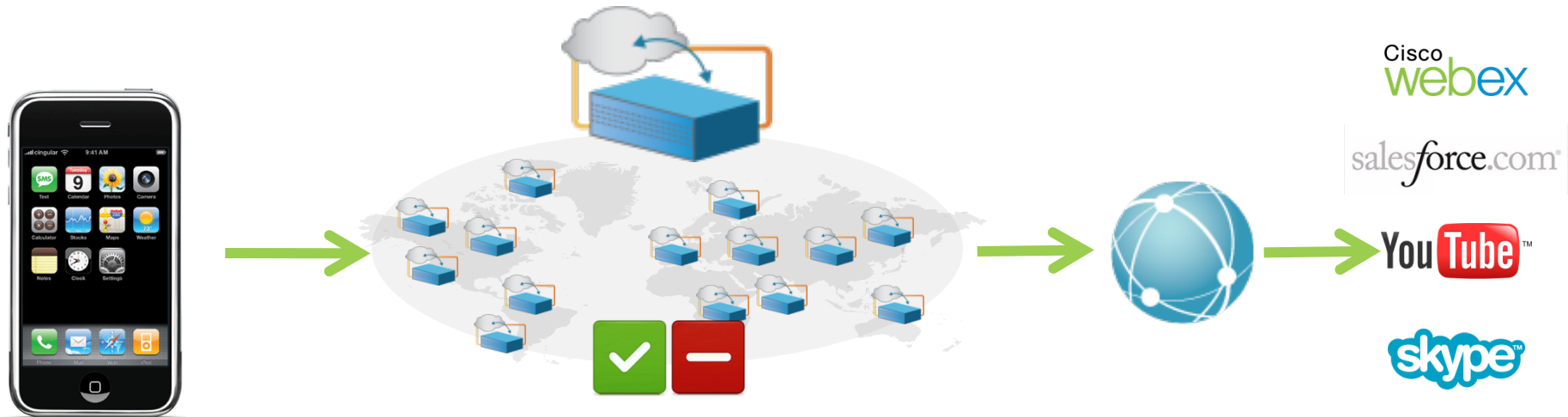
Расширенная безопасность off-box

- 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

Malware

Mobile User Security

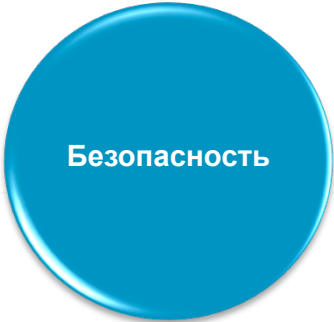
Безопасный доступ к Web в Borderless Network

- 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 устройства на WSA
но в будущем...

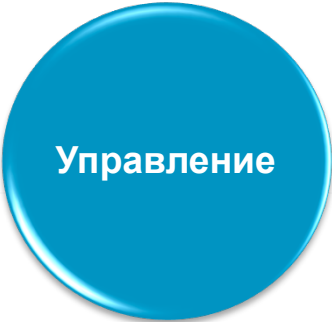


Cisco Secure Web Gateway

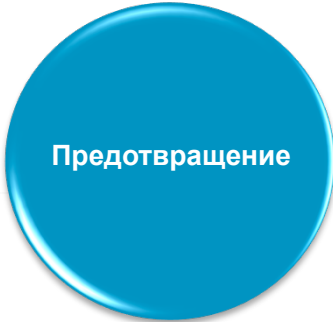
Самое высокопроизводительное решение в индустрии



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

1-1,000 users



ROBO

Cisco IronPort S360

1,000-10,000 users



Regional HQ / Mid-Market

Cisco IronPort S660

10,000-30,000 users



Corporate HQ

Market Segment

Управление безопасностью Web Security Management Appliance (M-серия)



Централизованное управление

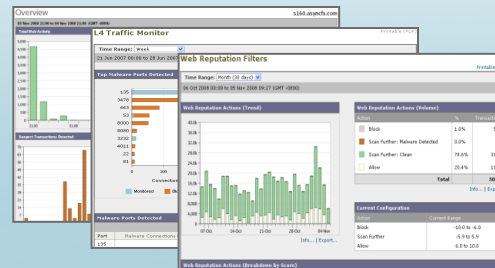


Централизованное
управление
политиками



Делегированное
администрирование

Централизованный репортинг



Глубокий
просмотр угроз

Широкие возможности
по расследованию

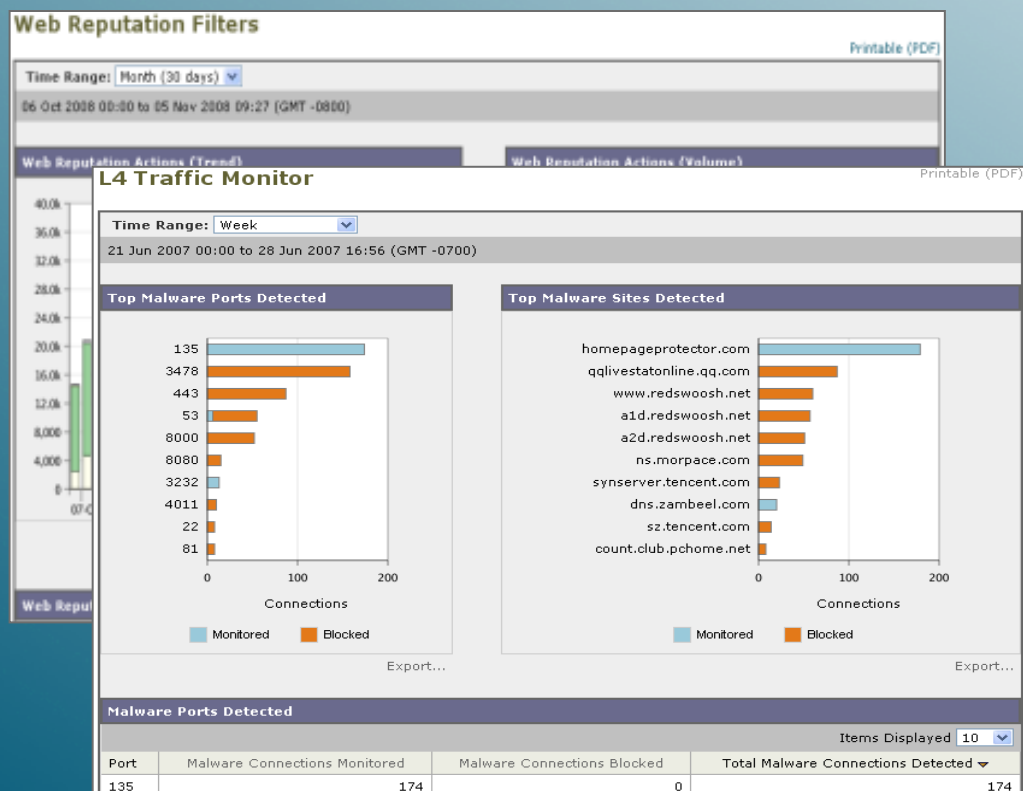
Просмотр
Приложений, угроз и
пользователей

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

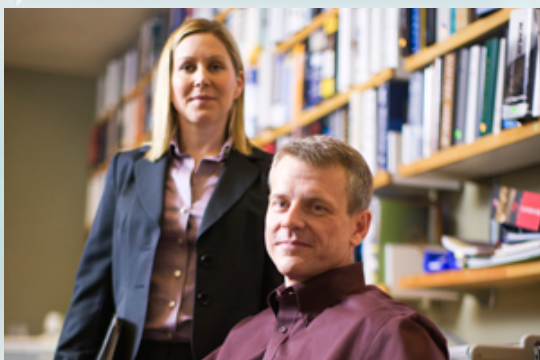
Измерить производительность

Анализ угроз

План на будущее

Отчеты для разных целевых групп

HR и юристы



- Расследования
- Измерения
- Производительность
- Применение политик

Безопасность



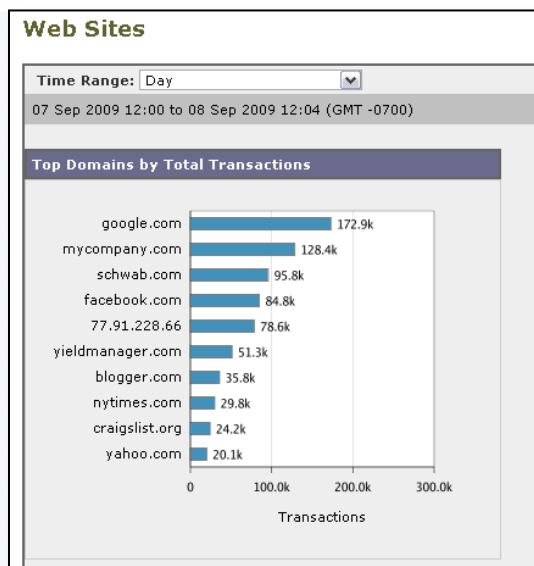
- Анализ угроз
- Расследования
- Управление политиками безопасности

Network Operations



- Управление полосой пропускания
- Планирование мощностей

Иерархия от высокоуровневых отчетов до отдельных транзакций



DETAILS: WBRs: -7, User community identified malicious behavior on domain or URI.

9 http://www.foxnews.com/story/0,2933,550140,00.html?loomia_ow=t0:s0:a16:g2:r3:c0.174555:
CONTENT TYPE: Text/HTML URL CATEGORY: News
DESTINATION IP: 101.211.501.631 HOST: wsa02-sfo
DETAILS: WBRs: -2 Malware - Adware. User community identified malicious behavior on domain or URI.

▶ PAGE ASSETS: 239

10 <http://www.foxnews.com/slideshow/entertainment/2009/09/06/rule-of-law-worship>

Высокий уровень:

- Приложения
- Узлы
- Пользователи
- Категории

Детальные:

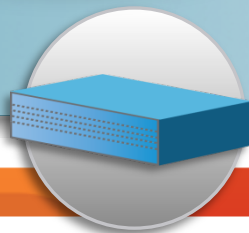
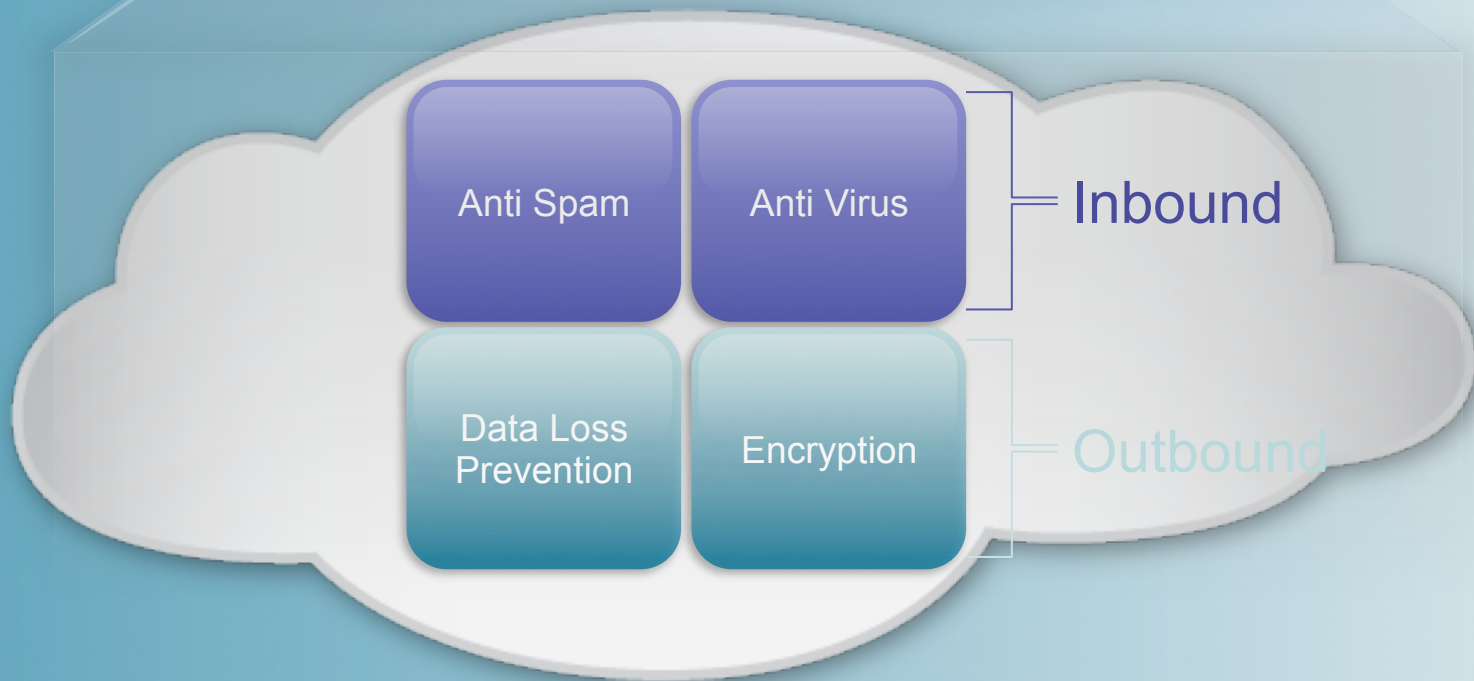
Детальная информация о каждой транзакции

Cisco Cloud Email

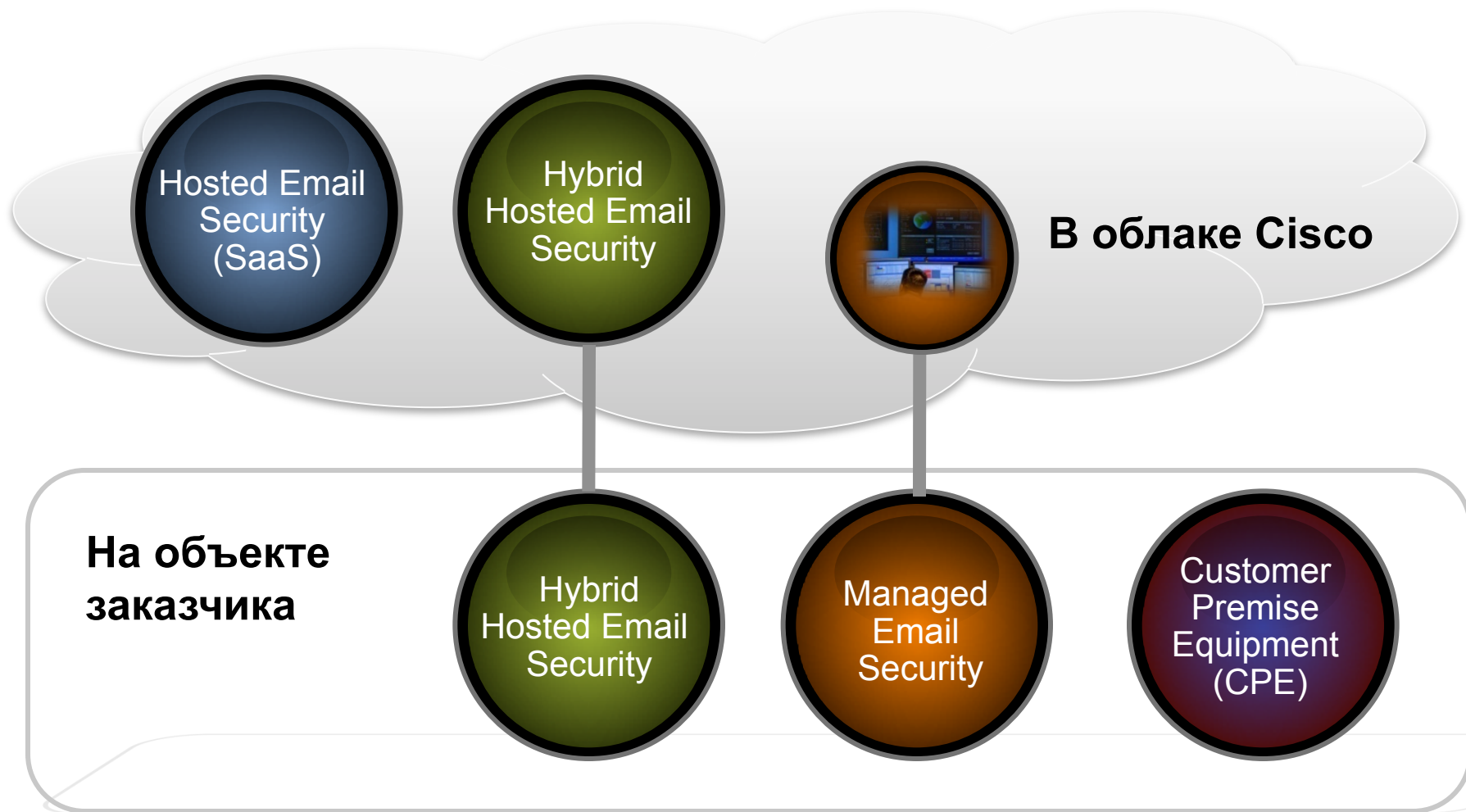


Архитектура решения IronPort ESA

В едином устройстве



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

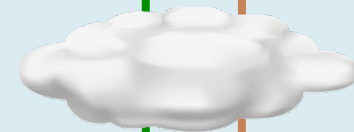
- Очистка входящей почты – в облаке Cisco
- Обработка исходящей почты, в т.ч. и DLP – у заказчика
- Конфиденциальная информация не покидает сети заказчика
- Единый интерфейс мониторинга

1: Очистка в облаке от спама и вирусов

1



2



2. Доставка проверенной почты



3

Применение политик DLP, интеграция с AD



Co-Managed

Мы администрируем, Вы контролируете

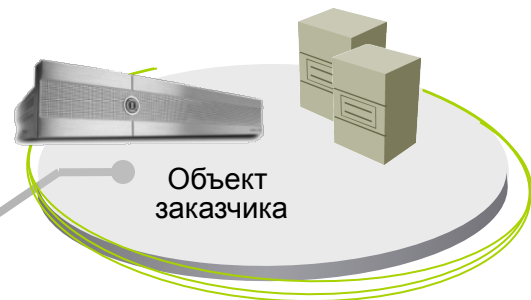
Заказчик



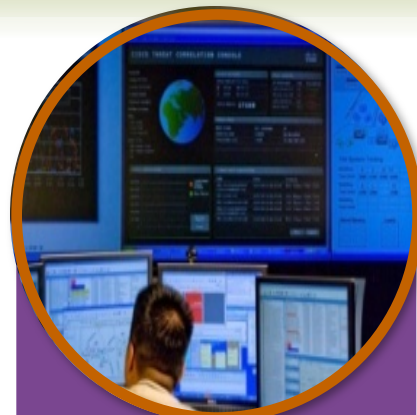
Отслеживание сообщений | Кейсы | Отчеты



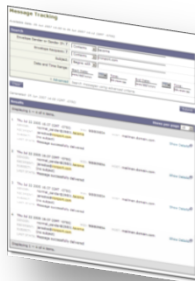
Отчеты



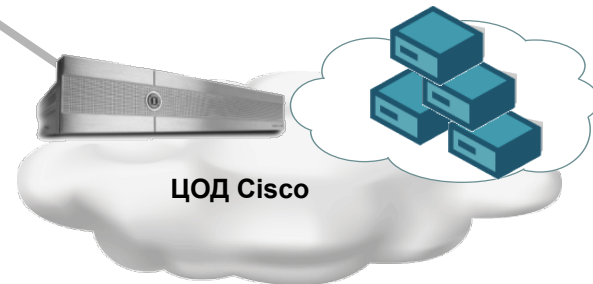
Разделяемый доступ



Cisco



Обслуживание



Мониторинг работоспособности | Обновления | Настройки

ScanSafe Web Security



Кто такой ScanSafe?



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



Security product
of the year 2008



Microsoft
GOLD CERTIFIED
Partner



2007 SIIA
//CODiE//
WINNER

Customers



Shell



Disney



BACARDI



ROTHSCHILD



Standard
Chartered



LOUIS VUITTON



IKEA



QUINTILES
TRANSNATIONAL

Partners



orange Business
Services



at&t

Google™

Sprint

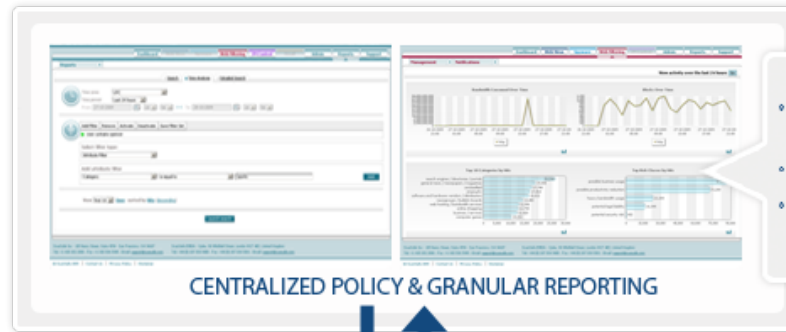


TELUS®

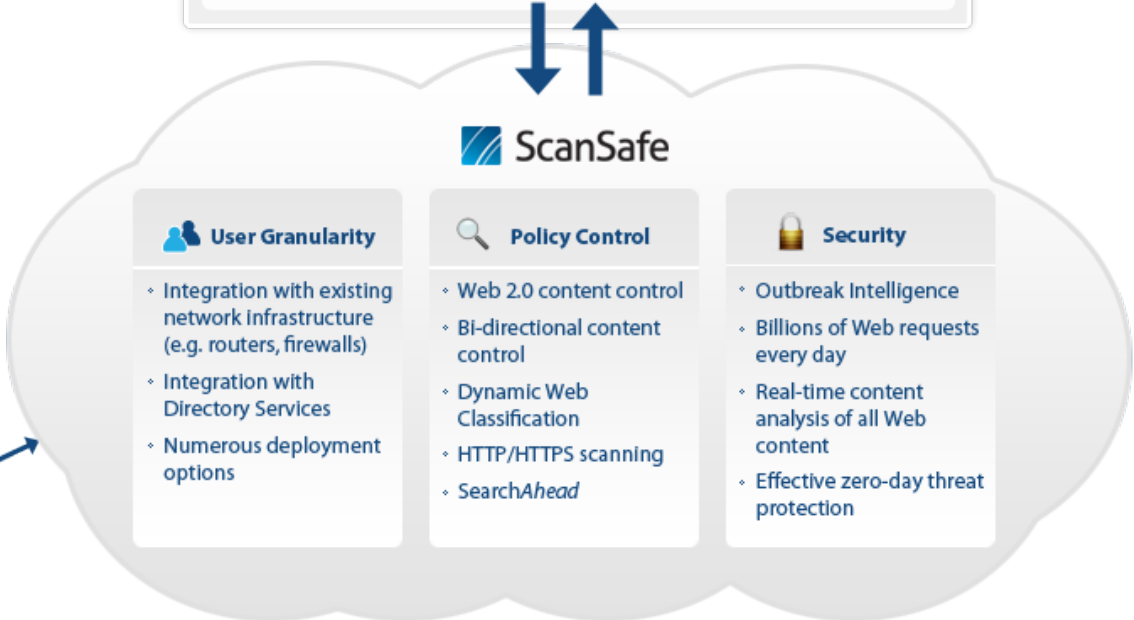


NEC

Обзор решения



- Flexible reporting with over 75 attributes
- Deep, drill down visibility
- Overview, trending and forensic data



User Granularity

- Integration with existing network infrastructure (e.g. routers, firewalls)
- Integration with Directory Services
- Numerous deployment options

Policy Control

- Web 2.0 content control
- BI-directional content control
- Dynamic Web Classification
- HTTP/HTTPS scanning
- SearchAhead

Security

- Outbreak Intelligence
- Billions of Web requests every day
- Real-time content analysis of all Web content
- Effective zero-day threat protection



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



ЦОДы Cisco ScanSafe

Надежность

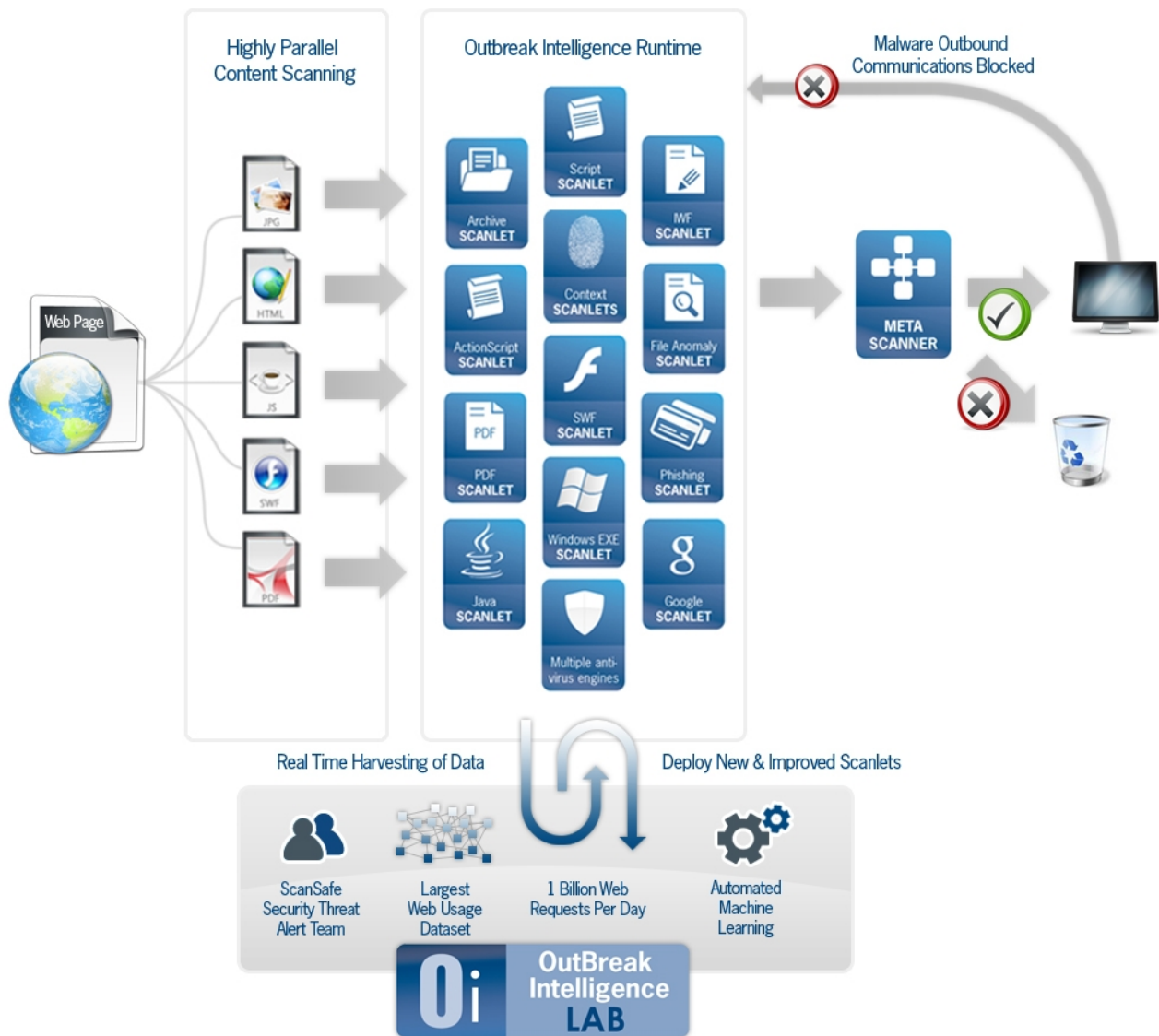
- 18ЦОДов
- 100% доступность сервиса за всю историю
- SLA по непрерывности и эффективности работы

Масштабируемость

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



Архитектура защиты от Web-угроз



- Статистика за 2009г.:
 - 28М уникальных JavaScript в день
 - 560К 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 *SearchAhead*
 - Классификация и уведомление пользователя



Как трафик попадает в облако

Опция 1 – при помощи имеющейся инфраструктуры заказчика

С изменениями настроек браузера:

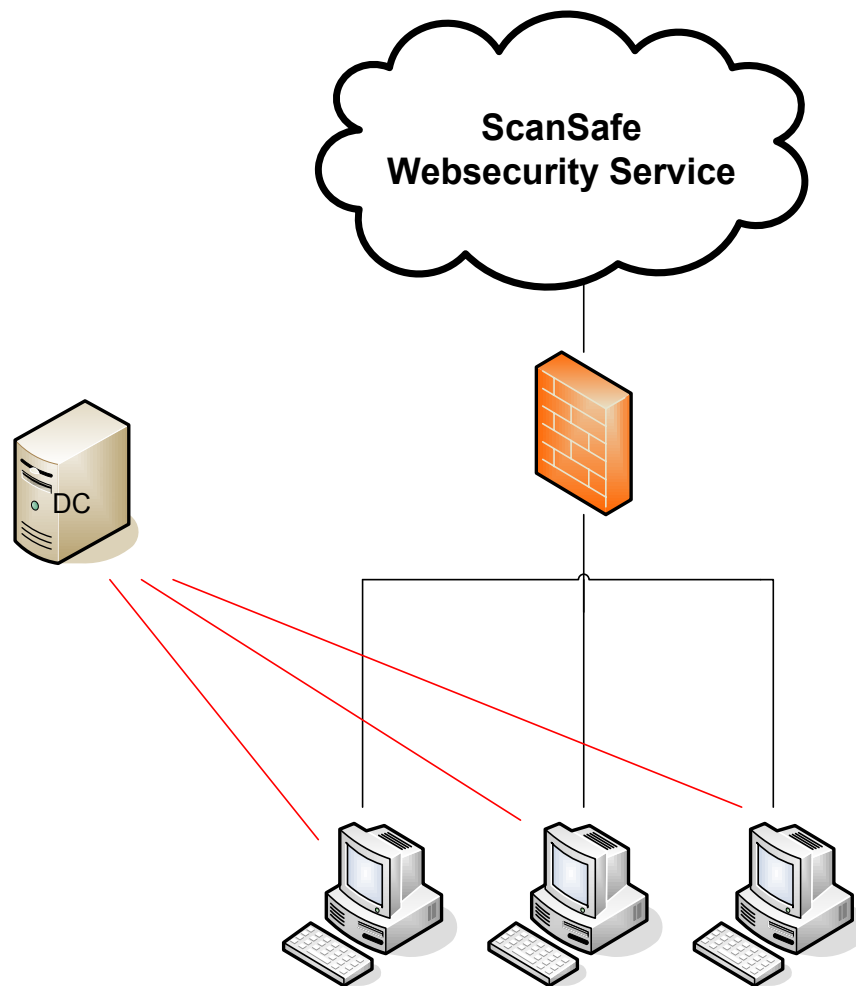
- Настройки Proxy загружаются на компьютеры из AD (GPO / PAC file) или по DHCP
- МСЭ блокирует исходящий HTTP трафик на все адреса кроме ScanSafe

Без изменения настроек браузера:

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

Опционально – User/Group Granularity:

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

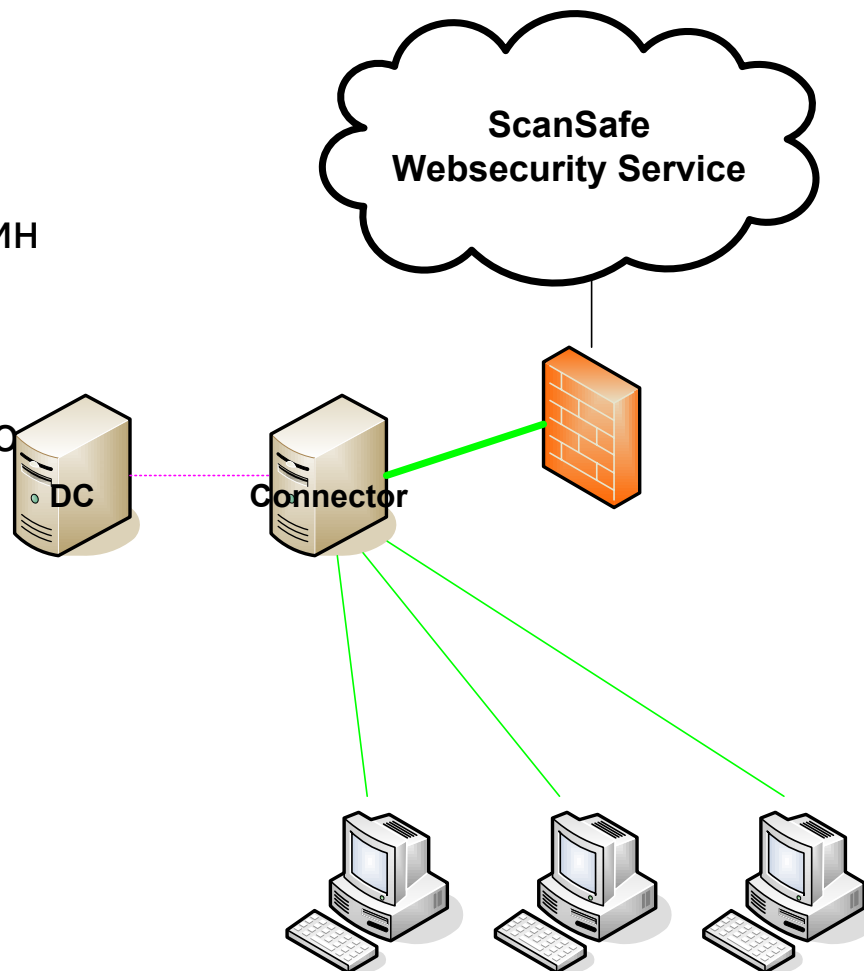


Как трафик попадает в облако

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



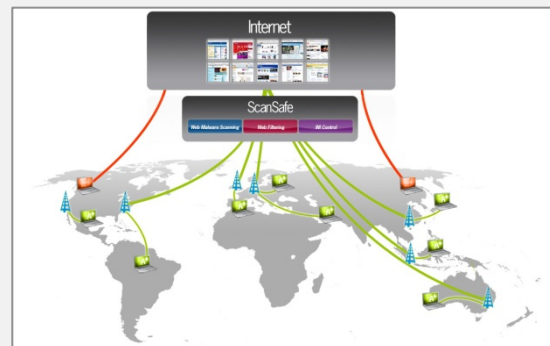
Как трафик попадает в облако

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

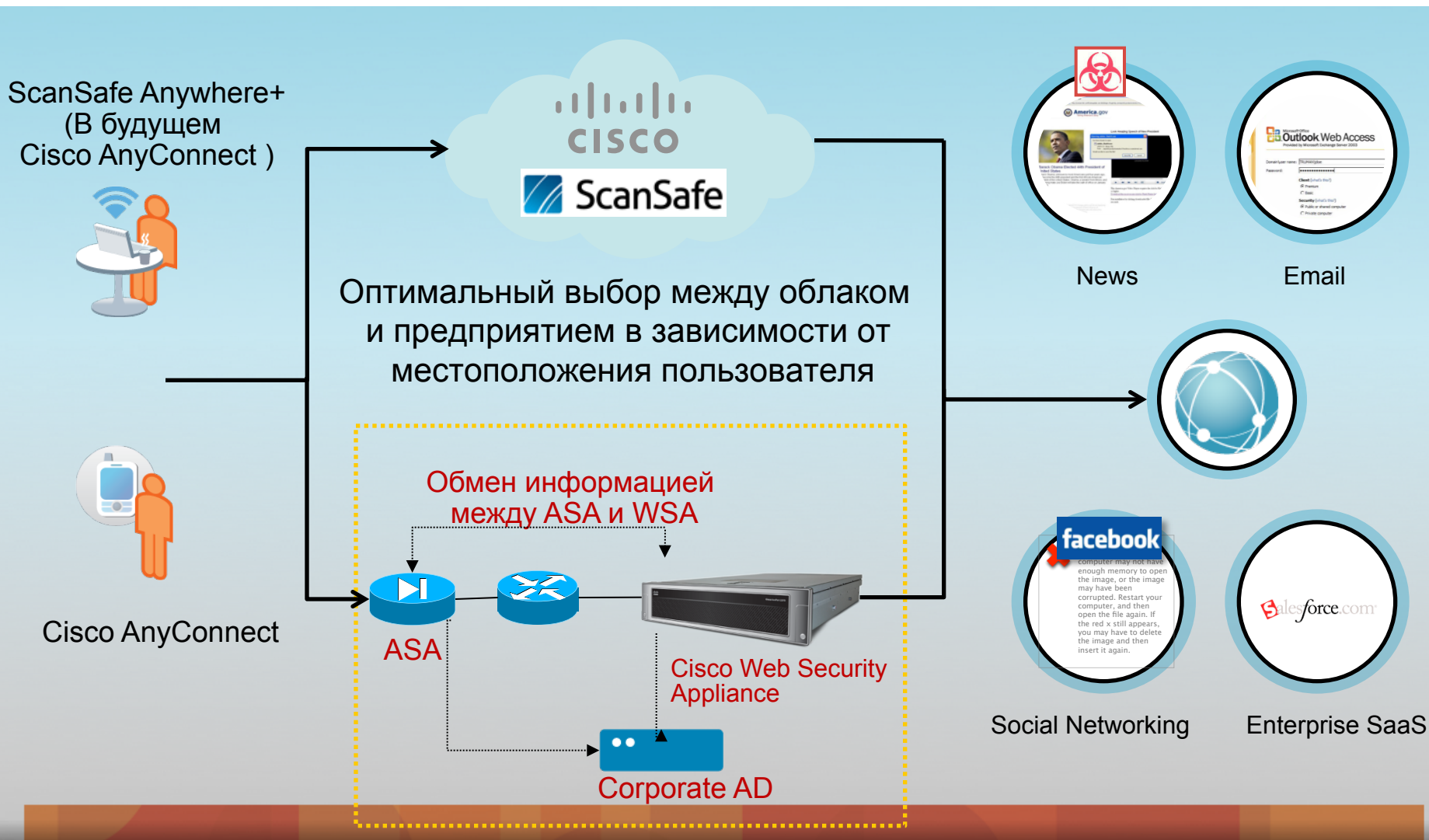
Факт: Мобильные пользователи только 17% времени в Интернет проводят в корпоративном VPN. **Как контролировать оставшиеся 83%?**



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

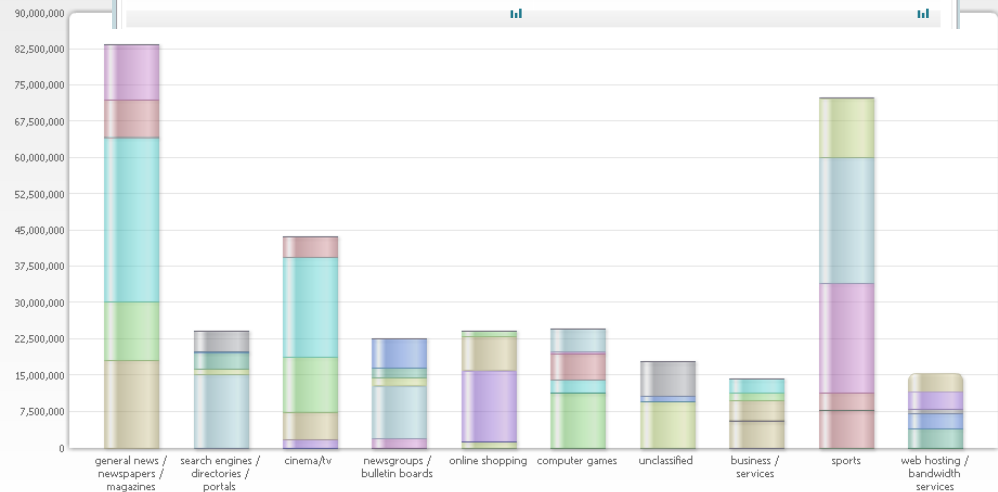
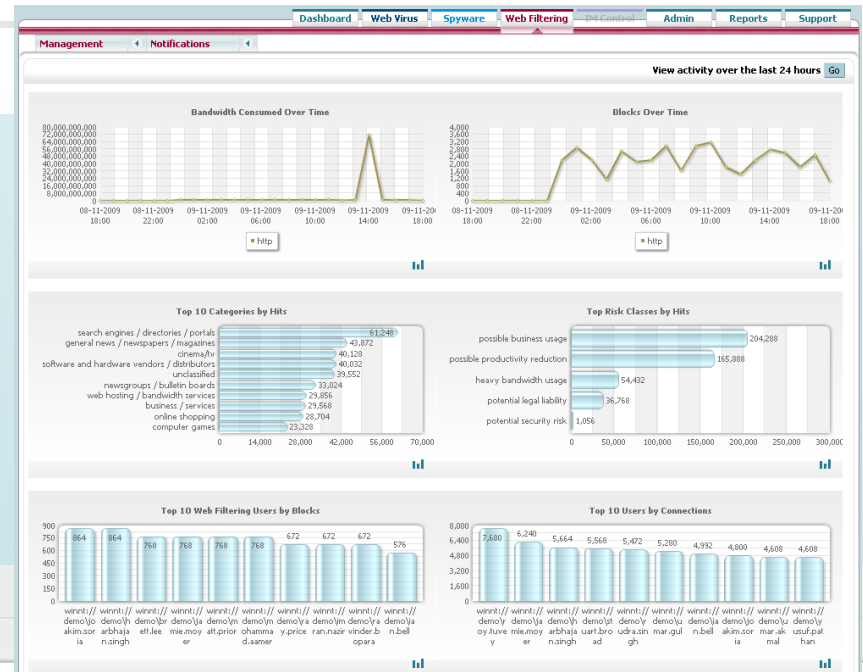
- Установки HTTP прокси не меняются.
- Идентификация Single Sign On с помощью LDAP и AD синхронизации.
- Пользователи настраиваются на ScanCenter Web Portal. Отчеты (Доступ по пользователям, группам и т.д. ...)
- ISR работает независимо от других сервисов безопасности (IOS FW, IPS, VPN)



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 Analyzer

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 Reputation 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:	<input type="text"/>
Submit Key	





THE INDUSTRY LEADING
CISCO IRONPORT C650
EMAIL SECURITY APPLIANCE

TRY BEFORE YOU BUY

Sign up today to
evaluate the
Cisco IronPort email
security solution
FREE.



© 2008 Cisco Systems, Inc.

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*