

eSafe v.7. Новая версия - новые возможности. Функциональность. Особенности использования для различных сегментов рынка.

eSafe[®]

*Перелыгин Д.А.,
Менеджер по работе с
партнерами и
корпоративными заказчиками*

Объект и каналы утечек (9 мес. 2008)

eSafe
PROACTIVE CONTENT SECURITY



Причины утечек (9 мес. 2008)



Выводы

- Большая часть утечек происходит неумышленно. Перекрыть возможности случайной утечки означает решить проблему на три четверти. Борьба же с инсайдерами-злоумышленниками – это в среднем менее приоритетная и более сложная задача. При ограниченности средств её следует решать во вторую очередь.
- Мобильные носители информации (ноутбуки, флэшки и т.п.) и Интернет – это два основных канала утечек. Как намеренных, так и случайных. “Мобильные” ненамеренные утечки достаточно легко перекрыть, введя обязательное шифрование данных.



Опыт выявления скрытых и неконтролируемых каналов утечки при использовании Интернет

Схема включения

eSafe
PROACTIVE CONTENT SECURITY

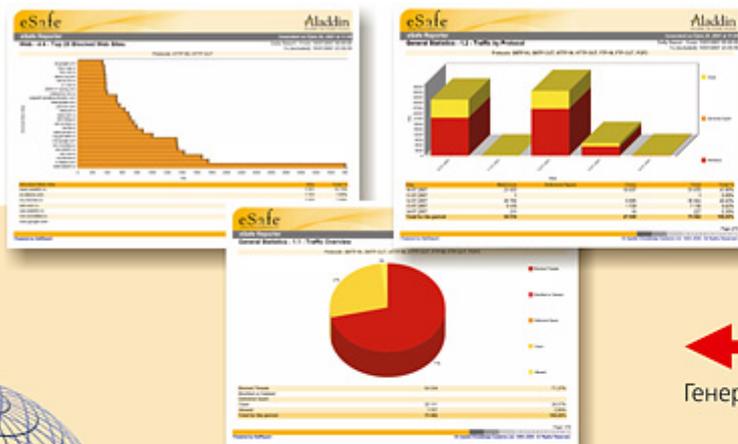


Схема работы



Нелегитимные коммуникации

Нелегитимные коммуникации

• HTTP PROXY	13,531
• SOCKS PROXY	57
• ANONYMUS WEB-PROXY	1,791
• MS INTERNET NET SHARING	3
• HTTP Tunneling	5
• HTTP (SSL) Tunneling	48
• HTTP OVER SSL (HTTPS)	1,502

Туннелинг

• HAMACHI	4
-----------	---

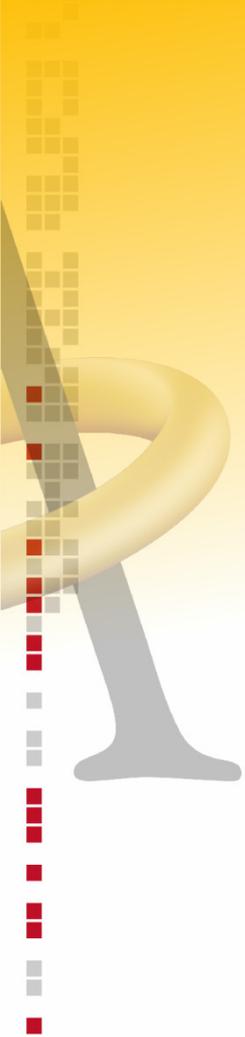
Трояны

• SeeMe Backdoor	1
• Brontok.A	1



Нелегитимные коммуникации

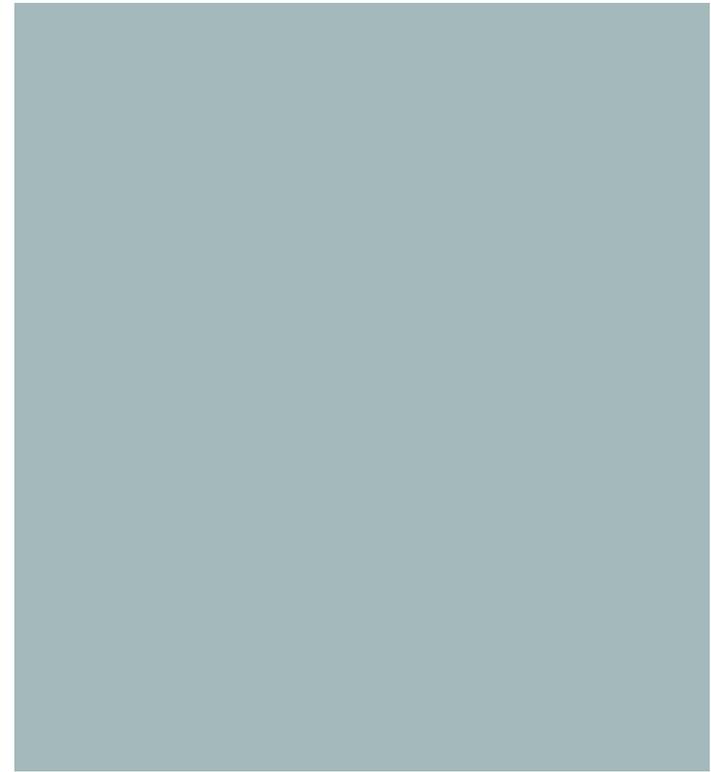
eSafe
PROACTIVE CONTENT SECURITY



Коммуникации шпионского ПО

Spyware

• QUADRO	38
• EROR GUARD	115
• ROGUE	112
• EASYSEARCH (BI)	4
• NEW.NET	13
• GATOR	195
• DIRECTWEBSEARCH	27
• VISICOM (BI)	4
• XXXTOOLBAR	256
• DEBORAH	1
• CMSINIT	1,392



Клиенты файлообменных сетей/IM

Файлообменные сети (P2P)

• GNUTELLA	5
• BITTORRENT	29,497
• DC++	6
• EDONKEY 2000	13,995
• WAREZ	1
• WINMX	36
• SKYPE	530

Передача файлов в IM

• GOOGLE TALK	160
• ICQ/AOL	4

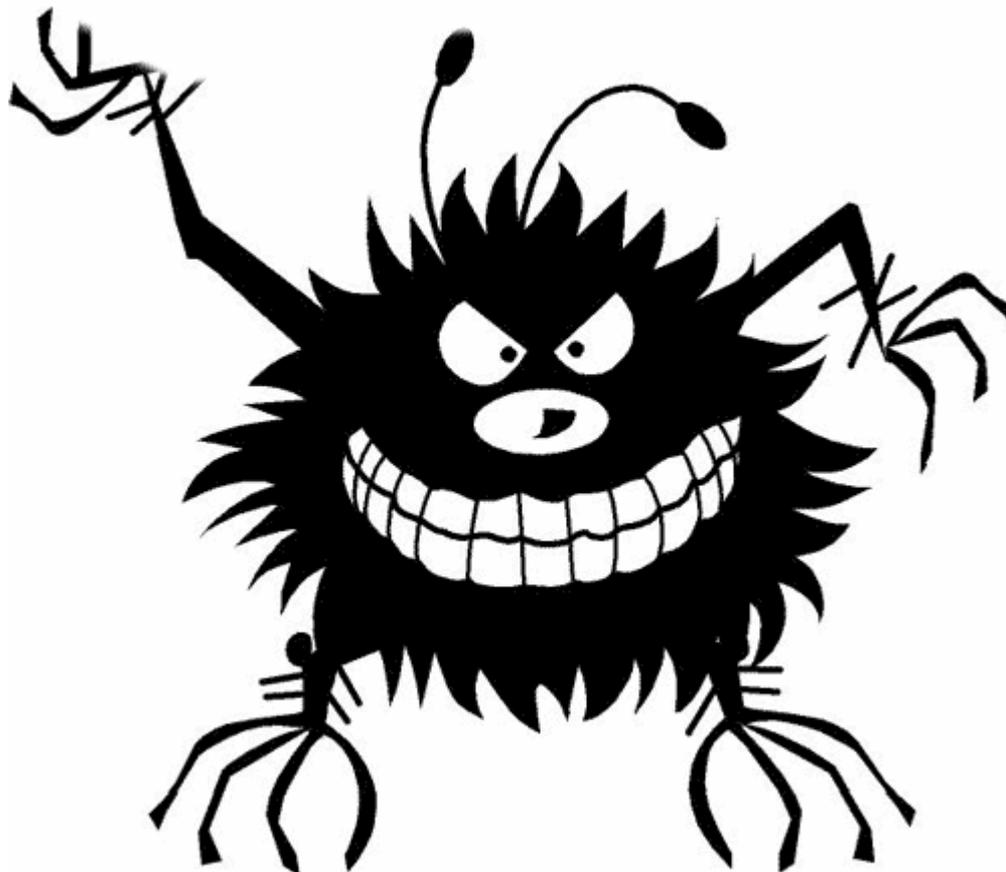
Удаленное управление

REMOTE CONTROL

- LOGMELN 4
- CITRIX 2
- RDP 5
- RADMIN 1



Как это обычно происходит

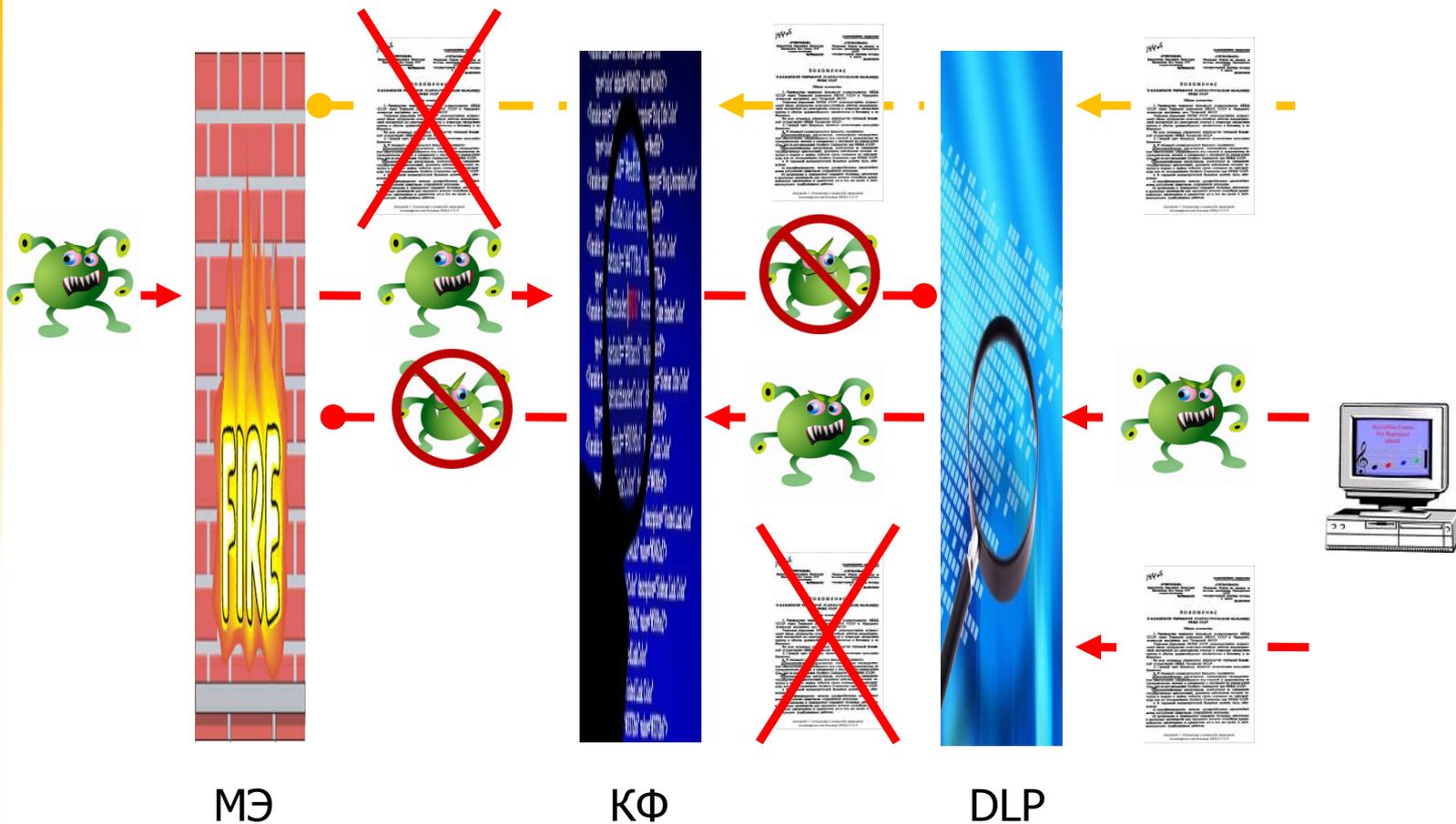


Как это может выглядеть

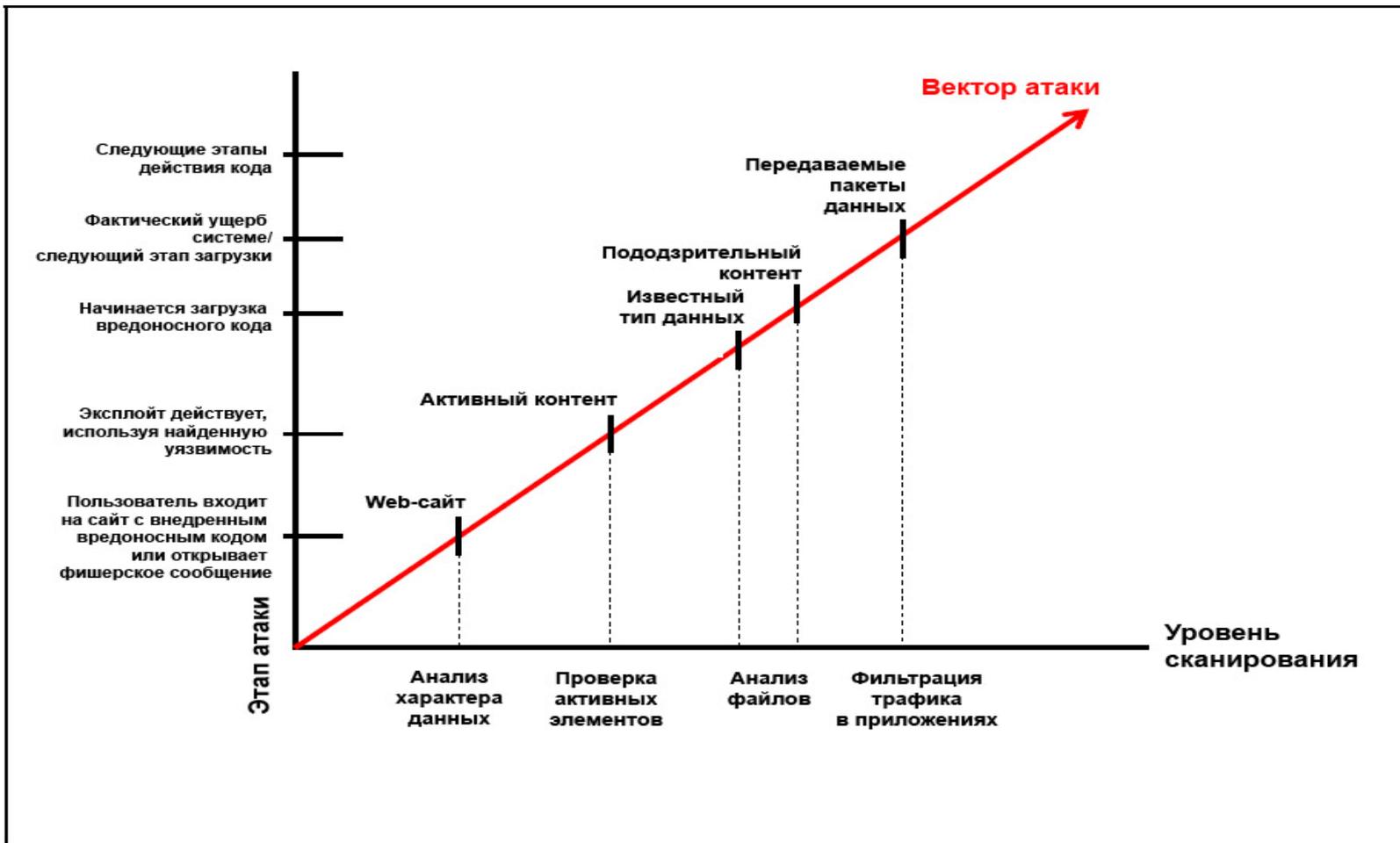


eSafe
PROACTIVE CONTENT SECURITY

Системы безопасности (шлюз)



Требования к защите



Как это реализовано в

eSafe®

... и других продуктах

Уровень доступа к данным

I

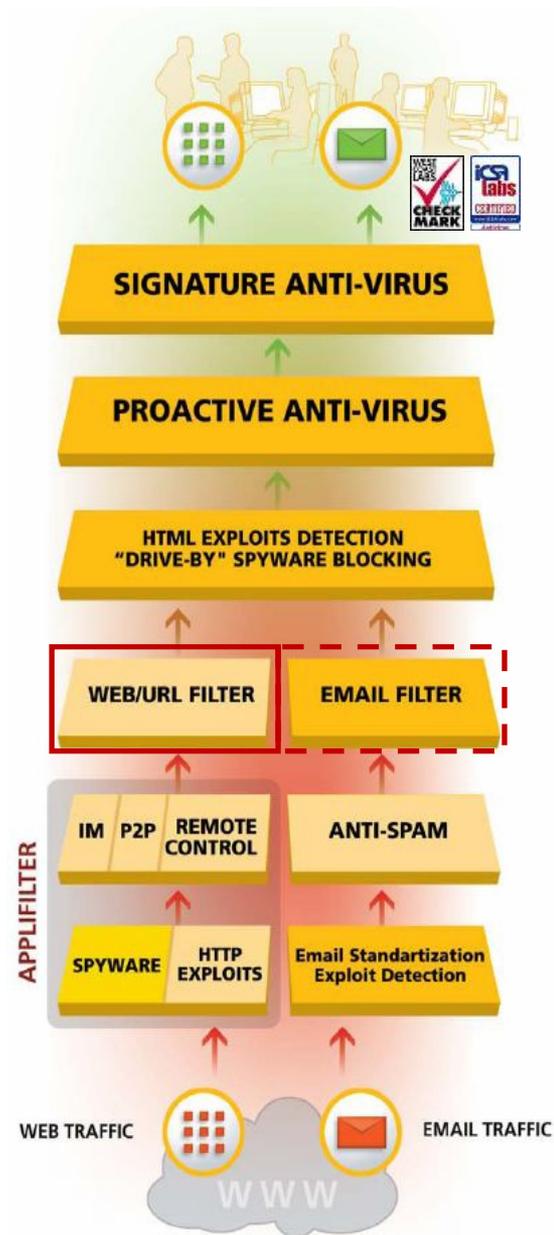
URL фильтрация

eSafe® URL Filter

- 95 миллионов сайтов, 3 миллиарда проиндексированных страниц
- 68 категории сайтов
- 150,000 новых страниц каждый день
- Обновление сайтов/страниц каждые 1-6 недель
- Подробные отчеты

Возможность назначения политик:

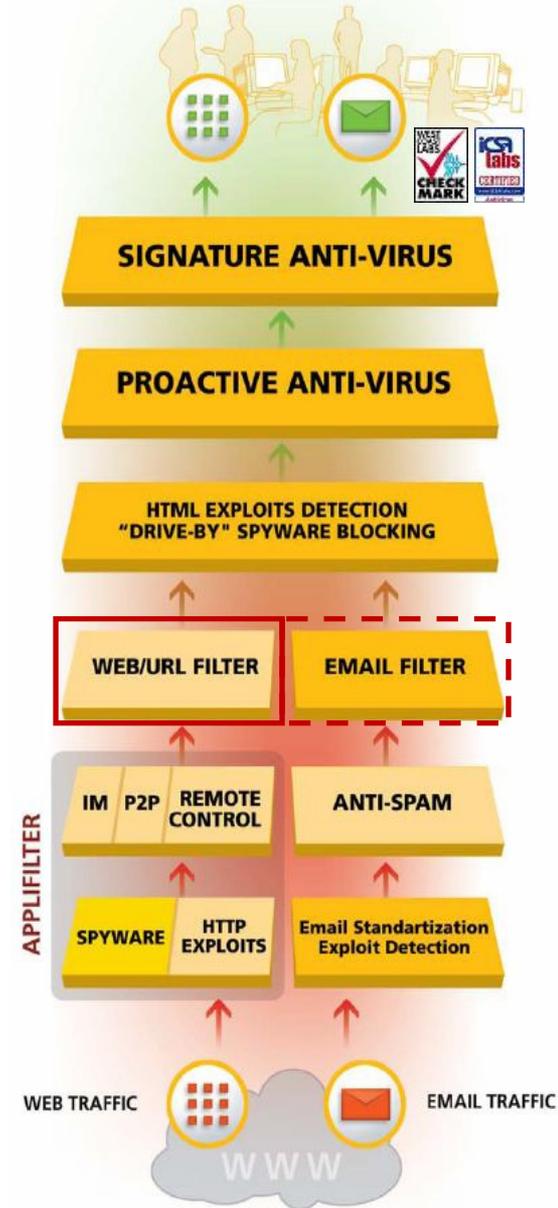
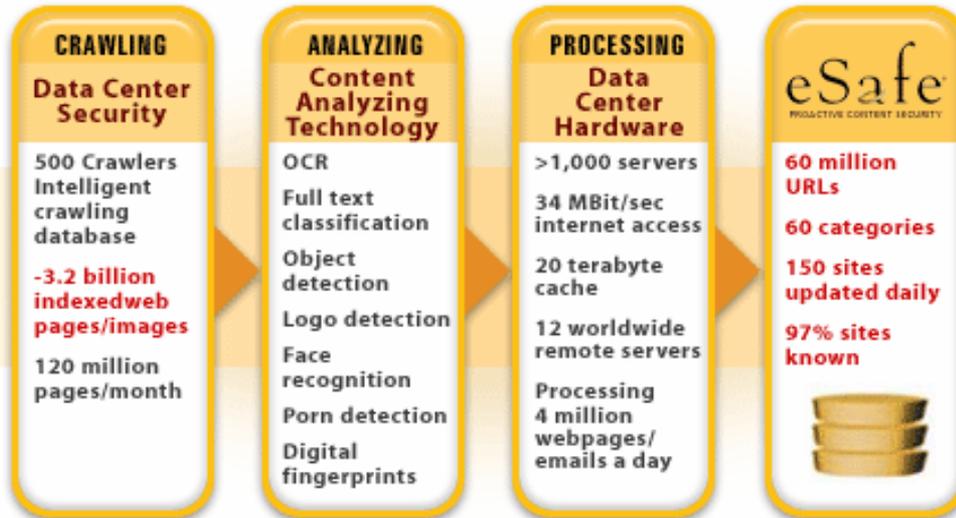
- В соответствии с бюджетом пользователя или его принадлежности к группе (LDAP/AD)
- По имени хоста или IP-адресу
- По принадлежности к подсети, диапазону IP-адресов или VLAN
- С использованием плагина к Microsoft ISA



eSafe® URL Filter

- По результатам аутентификации с использованием утилиты eSLogin
- Любой профиль может быть гибко настроен по времени доступа к Интернет

5 to 10 times the size of competitors' databases!



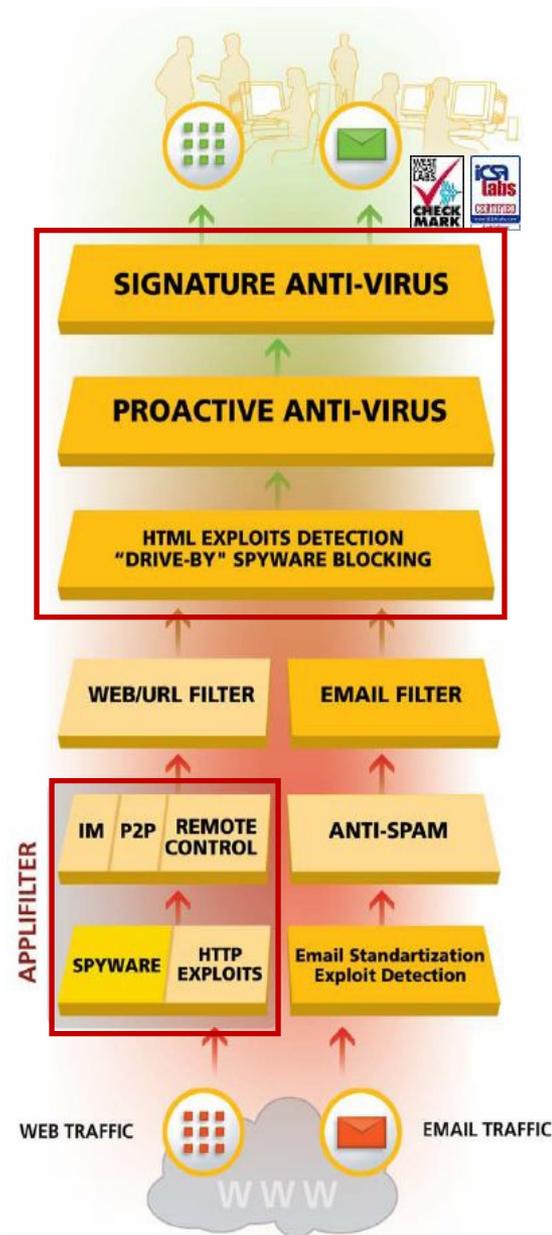
Уровни анализа и передачи

II, III

данных

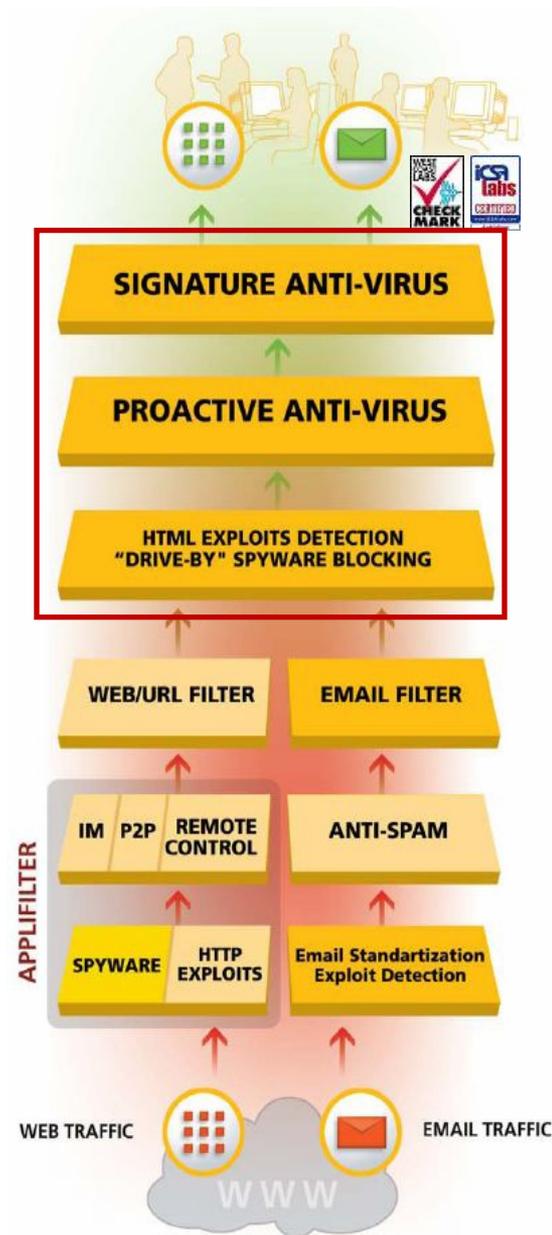
eSafe® WEB

- Проактивный антивирус. Проактивное блокирование до 98% вредоносного кода "zero-hour", включая Троянов и червей
- Сигнатурный антивирус, сертифицированный и на 100% блокирование "диких" вирусов
- Защита от эксплойтов. Проактивное блокирование попыток эксплуатации уязвимостей в web трафике
- Блокирование эксплойтов в HTTP протоколе
- Проверка 100% HTML на наличие вредоносных скриптов, эксплойтов, других видов вредоносного кода в веб страницах, веб-почте, в теле email



eSafe® WEB

- Удаление вредоносных и подозрительных скриптов (SmartScript Filtering™)
- Блокирование скриптовых вирусов и эксплойтов
- Блокирование известных HTML и HTTP эксплойтов (XploitStopper™)
- Удаление (опционально) ActiveX тэгов
- Разрешение выполнения только predetermined доверенных ActiveX объектов (опционально)
- Разрешение на выполнение только предустановленных доверенных ActiveX объектов

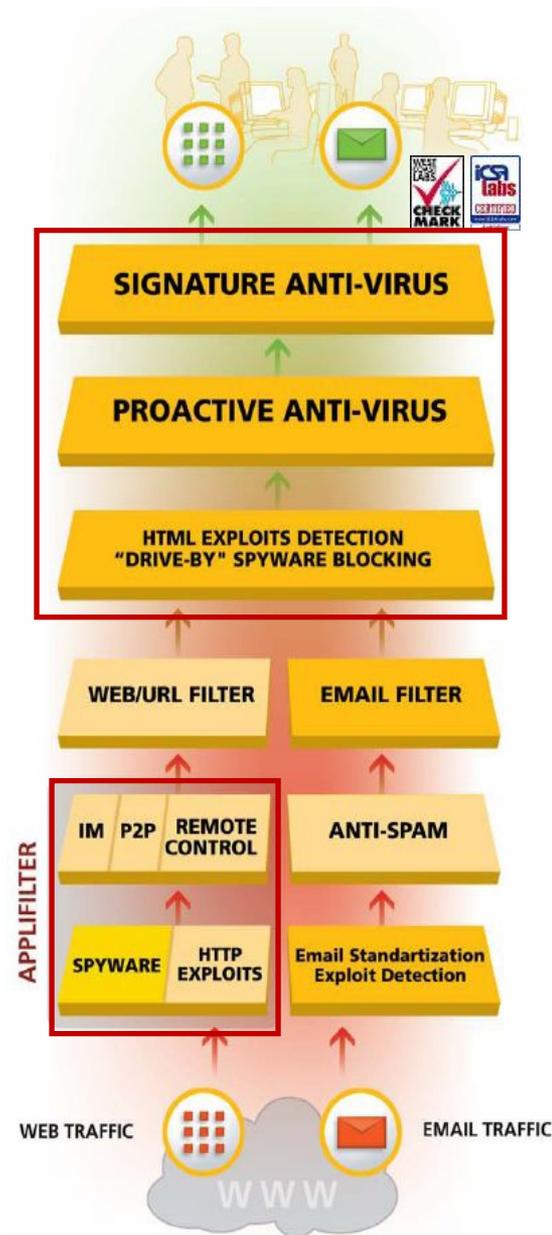


eSafe® WEB

- Опциональное удаление Java апплетов
- Опциональное удаление cookies
- Опциональное блокирование HTML страниц, содержащих predetermined слова
- Опциональное инспектирование контента SSL Web страниц

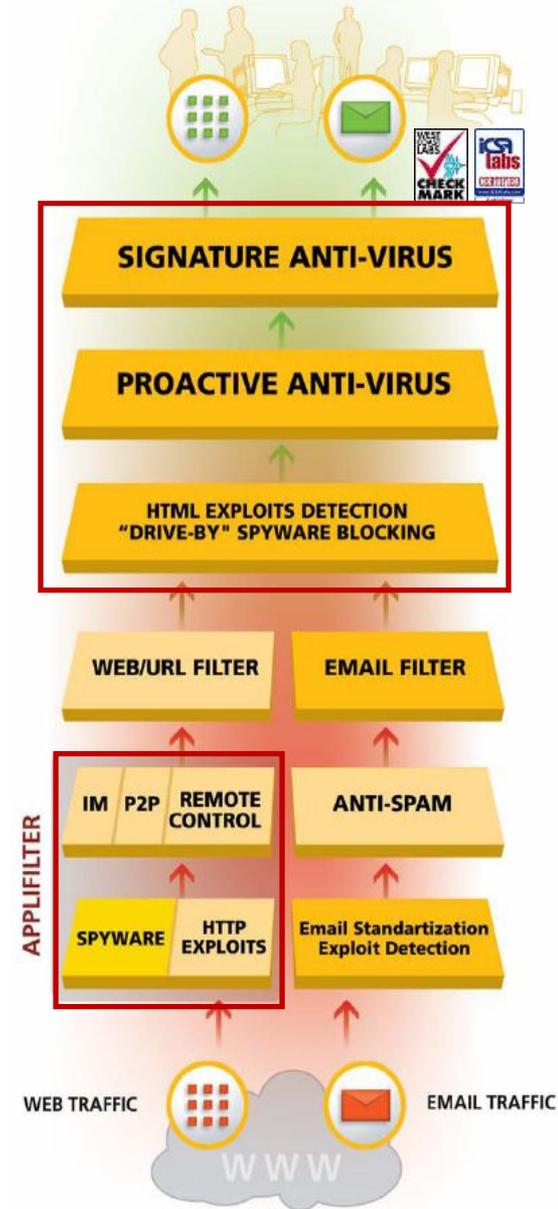
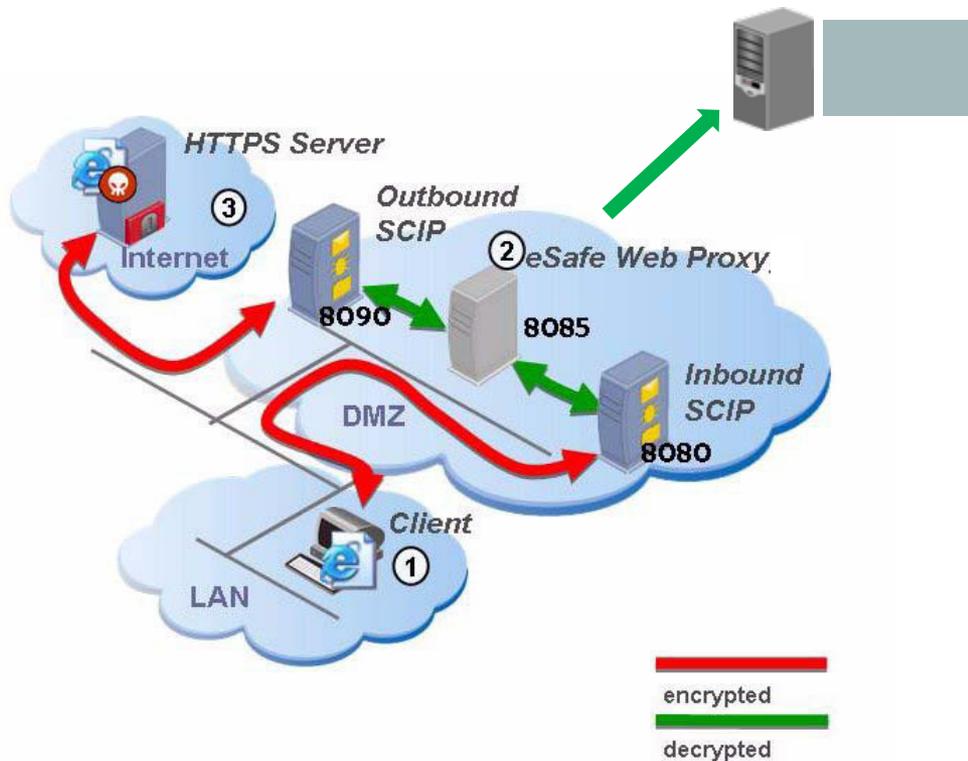
Четыре уровня блокирования Spyware:

- Блокирование на уровне доступа
- Блокирование навязанной рекламы и предотвращение "drive by" Spyware
- Блокирование Spyware по сигнатурам
- Блокирование коммуникаций Spyware
- Многое другое ...



eSafe® WEB SSL

- Дополнение функциональности eSafe® WEB возможностью прозрачной проверки зашифрованного трафика (HTTPS, SSL, TLS)



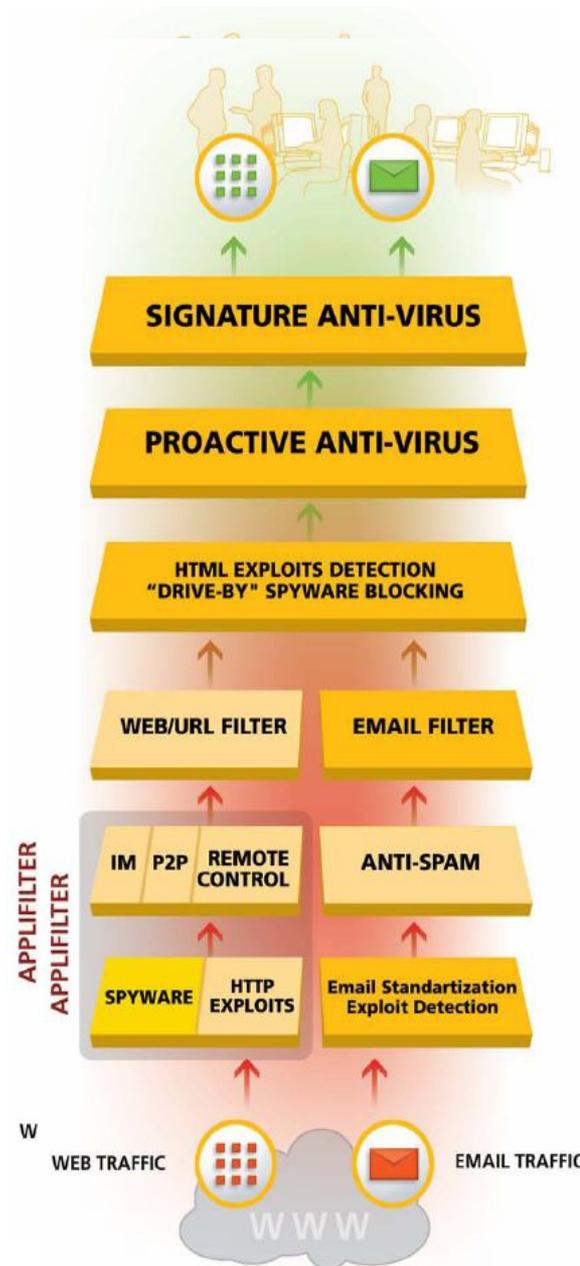
Уровень передачи данных

IV

Фильтр приложений

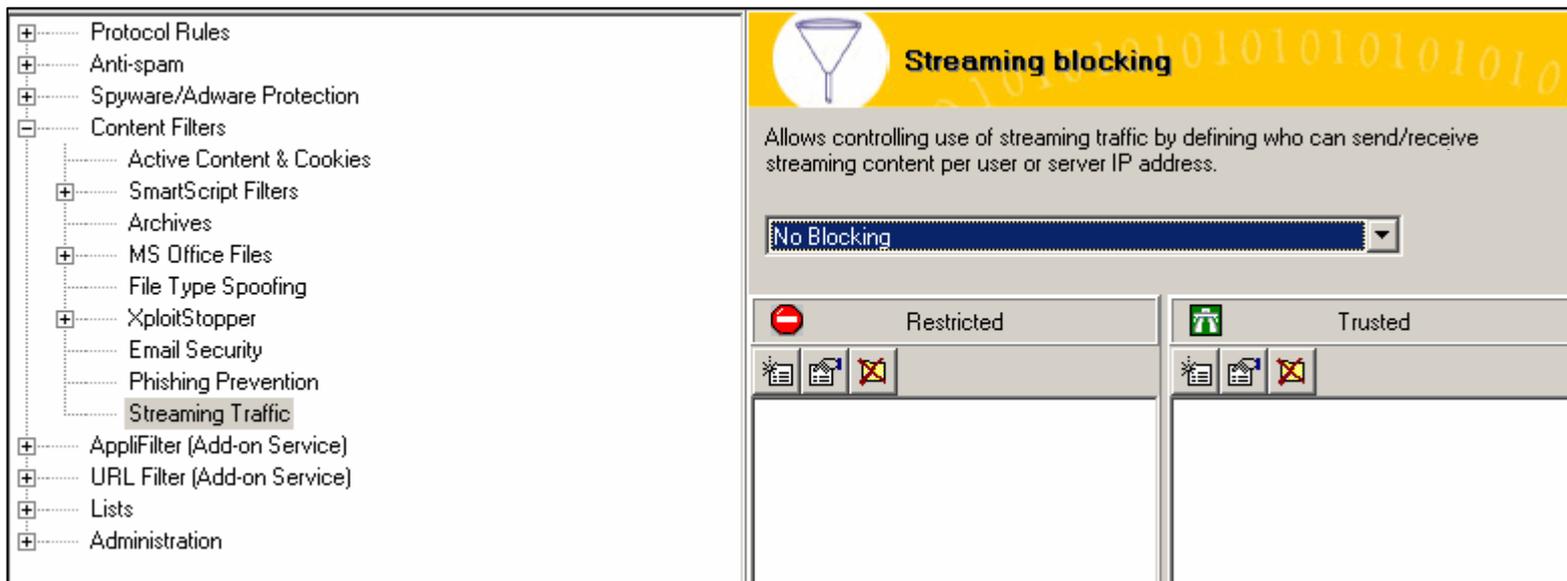
eSafe® Application Filter

- Блокирование вредоносного кода уровня шлюза (CodeRed, Nimda, MS Blaster и т. д.)
- Блокирование клиентов файлообменных сетей (P2P), **Skype**
- Блокирование Интернет-пейджеров
- **Блокирование коммуникаций Spyware/adware приложений**
- **Блокирование неавторизованного туннелирования**
 - HTTP Tunneling
 - HTTP (SSL) Tunneling
 - HTTP OVER SSL (HTTPS)
 - TOR, HAMACHI etc.
- **Блокирование 100% анонимных прокси**



eSafe® Application Filter

- Блокирование потоковых видео/аудио с возможностью создания черных и белых списков ресурсов



The screenshot displays the eSafe Application Filter configuration window. On the left is a tree view of filter categories, with 'Streaming Traffic' selected. The main panel is titled 'Streaming blocking' and contains a description: 'Allows controlling use of streaming traffic by defining who can send/receive streaming content per user or server IP address.' Below the description is a dropdown menu set to 'No Blocking'. At the bottom, there are two columns: 'Restricted' (with a red prohibition sign icon) and 'Trusted' (with a green house icon). Each column has a header bar with icons for adding, editing, and deleting items, and a large empty area below for listing resources.

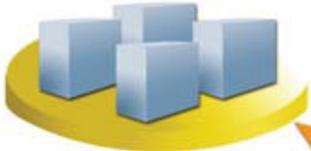
Самое время спросить о Web в

eSafe®

... и других продуктах

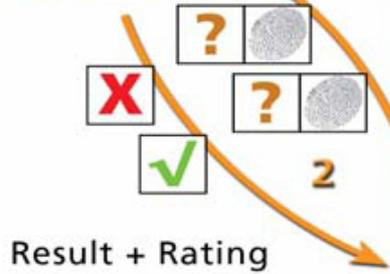
eSafe® Mail

eSafe Realtime
Detection Center



Engine I
Realtime
Inspection

Engine II
Deep Content
Inspection



Email



WWW

Productivity

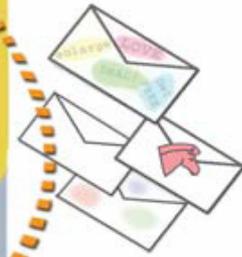
- Spam distribution pattern
- Sender reputation

- Spam heuristics
- Spam signatures
- Spam links
- Unwanted files

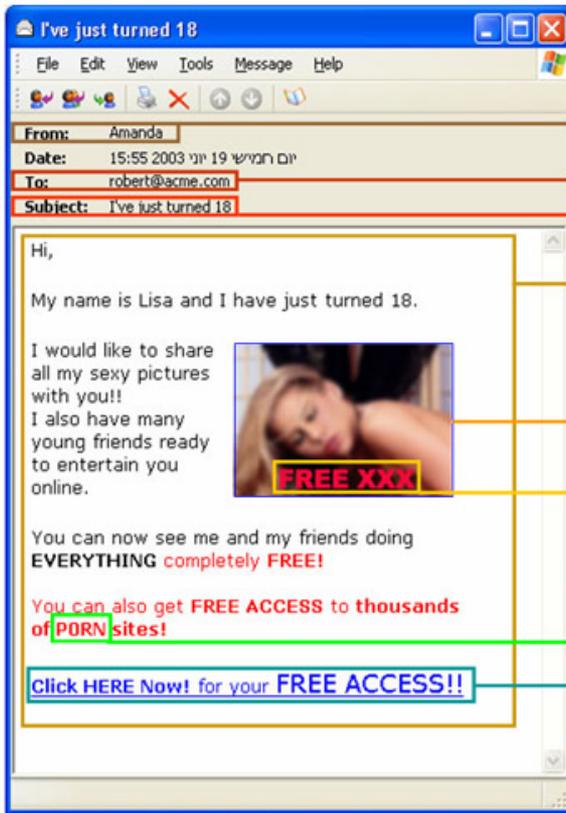
- Worm pattern

- Phishing patterns
- Malicious code
- Suspicious files
- Unwanted links

Security



eSafe® Mail Content Filter



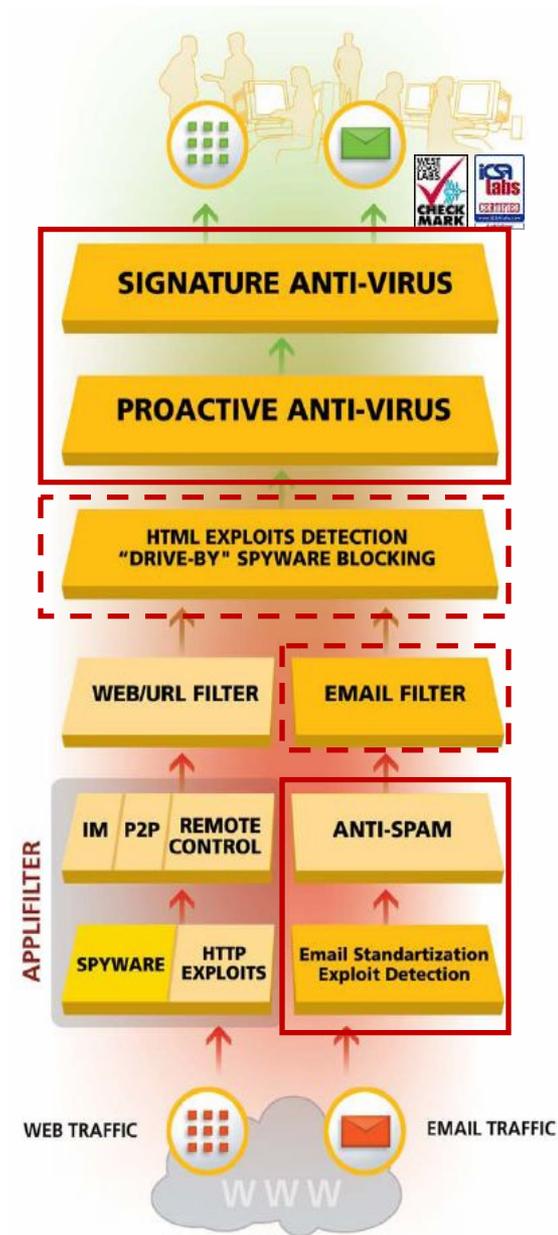
- 1 Real-time black lists (RBL)
- 2 Internal black lists
- 3 DNS Lookup
- 4 Spoofed sender
- 5 Header Analysis
- 6 Mail-bombing Prevention
- 7 Email Harvesting Prevention
- 8 Subject Analysis
- 9 Spam Database*
- 10 Lexical Text Analysis*
- 11 Statistical Text Analysis*
- 12 Heuristic Analysis*
- 13 Porn Image Detection*
- 14 Web Beacon Detection*
- 15 Optical Character Recognition (OCR)*
- 16 Text Manipulation Detection*
- 17 URL Classification*

* Available with eSafe Advanced Anti-spam service

- Spam Phishing
- Spam Fingerprint
- Spam Fuzzy Fingerprint

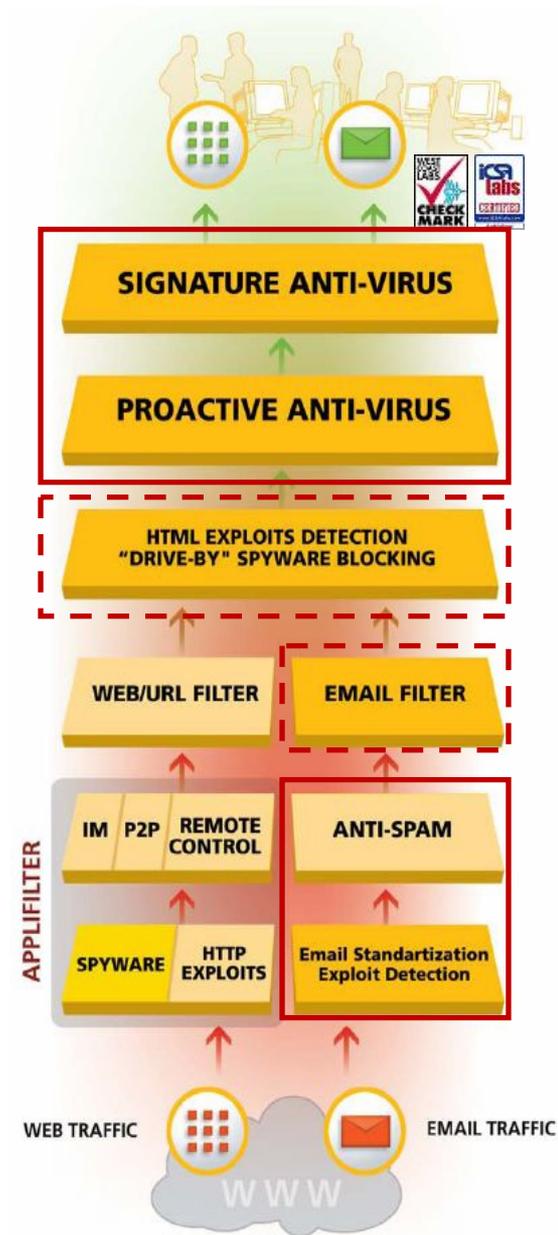
eSafe® Mail CSE

- Блокирование 100% известных “диких” вирусов сигнатурным антивирусом eSafe. Блокирование неизвестных вирусов и другого вредоносного кода (ActiveX, Java) проактивным антивирусом eSafe.
- Обнаружение и блокирование эксплойтов.
- Эффективное подавление спама (до 99,9%) практически без ложных срабатываний
- Блокирование cookies от недоверенных источников и всех email
- Удаление макросов и внедренных документов (MS Office, например), полученных из недоверенных источников



eSafe® Mail CSE

- Встроенные механизмы защиты от DoS, relaying, email spoofing, email attachment spoofing и т. д.
- Возможность автоматической отправки копии email на указанные адреса
- Возможность автоматической переадресации email на указанные адреса
- Возможность определения политик и ограничений для обработки почты на уровне групп и пользователей LDAP/AD
- Проверка валидности бюджета пользователя или его email (интеграция с LDAP/AD) и отказ в приеме email в случае невалидности



eSafe® Quarantine Report

Сообщение

От: esafe-quarantine@esafe01.aladdin.ru
 Кому: DL eSafe
 Копия:
 Тема: eSafe SPAM Quarantine Report

Отправлено: Вт 08.04.2008 14:01

Quarantine reports are sent to you automatically every day. To request the latest report with spam held in your quarantine since the last report was sent, please click on this button: [Request Report]

eSafe Spam Management
 Powered by eSafe Proactive Content Security

Quarantine Report for: esafe@aladdin.ru - 39 Spam emails were introduced in the quarantine since the last report

The emails listed below were placed in your personal Spam-Quarantine since the last report. Please review the list below, select the appropriate ACTION for each quarantined email and click SUBMIT REQUEST. If you consider all emails to be spam, no action is required, just ignore this report.

Mail ID	Date	Subject	From	Action
3999435587	08-Apr-2008 10:10:18	Трудовой договор с иностранными работниками	kvo@nextsolutions.us	Release
3999436046	08-Apr-2008 10:15:01	Jacob & Co. Watches	steveruth.892@johnbumham.com	Release
3999436591	08-Apr-2008 10:22:49	Вам нужен сайт?	kruan@rcn.com	Release
3999438087	08-Apr-2008 10:38:22	Как избежать ошибок оптимизации налоговых платежей?	andybatesemba@rasal.net	Release
3999438379	08-Apr-2008 10:40:42	Fw: Re: Re: натяжные потолки	tplgwyebu@boysenberys.com	Release
3999438940	08-Apr-2008 10:44:53	Заказ билетов в театры и концерты с доставкой по Москве	postmaster@arteccolourprint.co.uk	Release
3999439289	08-Apr-2008 10:47:18	Re: Приглашаем на семинар	williamvee@barbarascanlon.com	Release
3999439459	08-Apr-2008 10:48:50	Доставка отправлений	ghindustry@yahoo.com	Release
3999439532	08-Apr-2008 10:49:27	юридическая ошибка	dotyk@qwest.com	Release
3999439543	08-Apr-2008 10:49:30	Курсовые на заказ	vinitsue_elle@gmx.net	Release
3999440470	08-Apr-2008 10:55:40	Афиша-Лучшее: Премьеры, Спектакли, Концерты	iel.salcido@us.calvyn.com	Release
3999441283	08-Apr-2008 11:01:22	Бизнес-процессы - оптимизация, регламентация	vxtvt@bobtard.com	Release
3999441935	08-Apr-2008 11:05:50	Re: Элитный преподаватель английского языка	susan3ylveste@info.gamanetwork.com	Release
3999443128	08-Apr-2008 11:13:50	Срочно нужен офис? Звоните!	tr4346zt@feve.jp	Release
3999443466	08-Apr-2008 11:15:58	Кондиционеры. Поставка и монтаж оборудования	tineina@blued.com	Release
3999444783	08-Apr-2008 11:25:00	Срочная аудиторская проверка	uxulivudhu@virginlaw.com	Release
3999447188	08-Apr-2008 11:40:51	Постельное белье для всех ценителей стиля и комфорта	f-seichi@mypatientsonline.net	Release
3999447492	08-Apr-2008 11:42:57	БИЛЕТЫ хоккей России-Финляндия, Баскетбол Цска-Олимпиакос, футбол Динамо-Спартак, SCORPIONS, Хуллс Иглсиса, Queen, KISS, музеи Кремля, театр "Ленком" и др.	dotyk@qwest.com	Release
3999447532	08-Apr-2008 11:43:10	Современные требования к предпроектной, проектной подготовке строительства	joaquin.cid@honus.es	Release
3999448617	08-Apr-2008 11:51:49	НАЛОГОВАЯ ОПТИМИЗАЦИЯ : ПРЕДЕЛЫ ДОПУСТИМОСТИ	hsarivo@bmlinc.com	Release
3999449044	08-Apr-2008 11:55:08	Современные требования к предпроектной, проектной подготовке строительства	cgomarian@hodes.com	Release
3999449642	08-Apr-2008 11:59:19	Резюме Главного бухгалтера	gieshammer@huis-op-maat.nl	Release
3999451665	08-Apr-2008 12:14:13	Таможенная статистика Российской Федерации	uzehring@bea-tdl.de	Release
3999452521	08-Apr-2008 12:20:59	Бронь и доставка билетов на спектакли/концерты	barter@positivetourism.com	Release
3999453299	08-Apr-2008 12:26:57	Визы.	jcannon793@mindspring.net	Release
3999453693	08-Apr-2008 12:30:34	Таблички	alfredhrustkey@msn.com	Release
3999455164	08-Apr-2008 12:42:21	[62]: Финансовая база	sudhakar85913sidharta@barbf.com	Release
3999455611	08-Apr-2008 12:46:13	Предложение для ИНВЕСТОРОВ	willie24sph@walla.com	Release
3999455895	08-Apr-2008 12:48:33	Открыть компанию	fyrimjeovqe@boyz-wanted.com	Release
3999457316	08-Apr-2008 12:59:54	Пользительные пакеты от производителя	sorooryang@portsevendomain.biz	Release
3999457409	08-Apr-2008 13:00:54	Торговое помещение	wendy67tsung_hu@zfree.co.nz	Release

eSafe® и Multiple LDAP

LDAP Configuration

Use the Basic Settings tab to define the settings eSafe will use to connect to the LDAP server. Use the Advanced Settings tab to perform search queries.

Note that the user/group root nodes can include lists that use semi-colon delimiters.

****Make sure that the Active Directory is configured to allow the LDAP server to retrieve more than 1000 entries for a query. For details on changing this setting, contact Microsoft, or eSafe Technical Support.****

LDAP servers: Default [Icons] Restore LDAP server defaults

Basic Settings | Advanced Settings

Select server type: Active Directory Backup of: None

LDAP server address: 1.1.8.10

Connection port: 389

User name (DN): example

Password: *****
Make sure that you use a password that does not expire!

User root nodes: example

Group root nodes: example

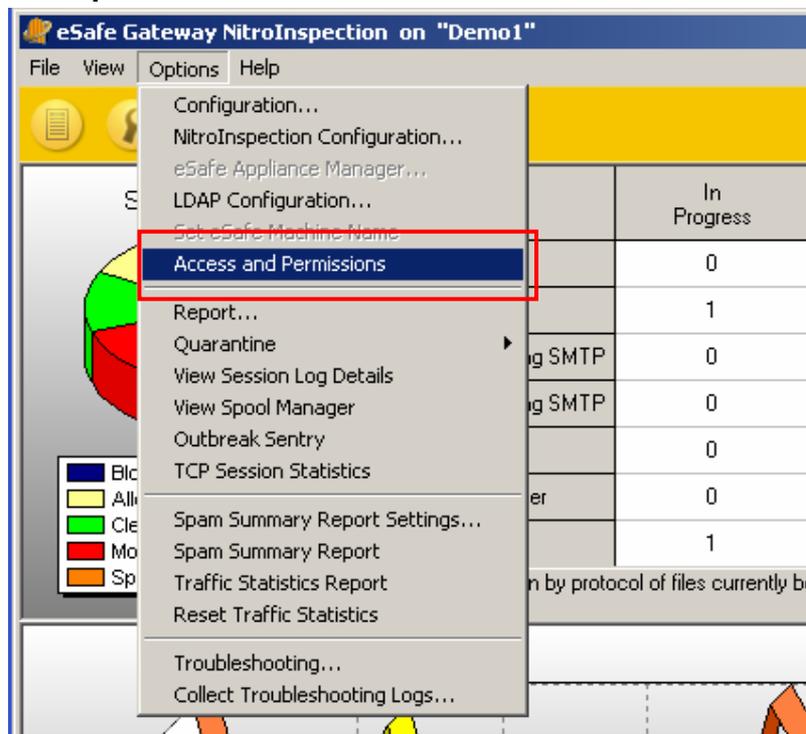
Host root nodes: example

Intervals for sync: 10 min

OK Cancel Help

eSafe® Ролевое управление

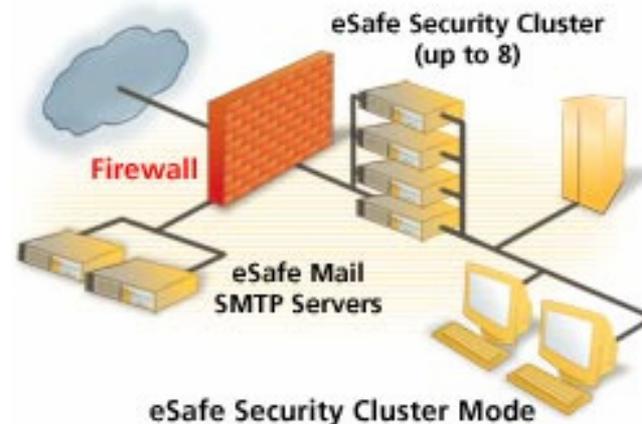
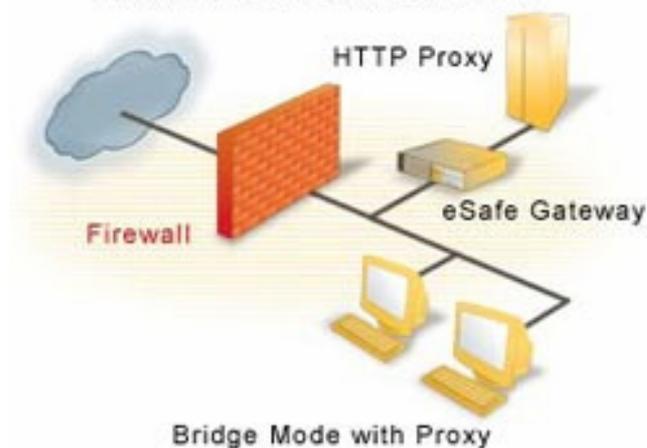
- Реализация доступа к консоли управления с уровнем привилегий в зависимости от роли:
 - Администратор
 - Только чтение (режим мониторинга)
 - Управление карантинном и работа с отчетами
 - URL Filter Helpdesk



eSafe® Схемы включения

- Прозрачный мост
- Маршрутизатор
- Маршрутизатор с подключением по PBR (Policy Based Routing)
- Forwarding proxy
- Full Proxy
- Отказоустойчивые схемы с балансировкой нагрузки
- Экзотические схемы

SAMPLE DEPLOYMENT MODES



eSafe® для Enterprise

- Масштабируемость. Возможность построения отказоустойчивых систем с балансировкой нагрузки
- eSafe® Hellgate XG-300 Appliance. Мощная двухпроцессорная аппаратная платформа.
- Более мощные аппаратные платформы. VACD

eSafe® HG-200 Appliance



eSafe® XG-300 Appliance

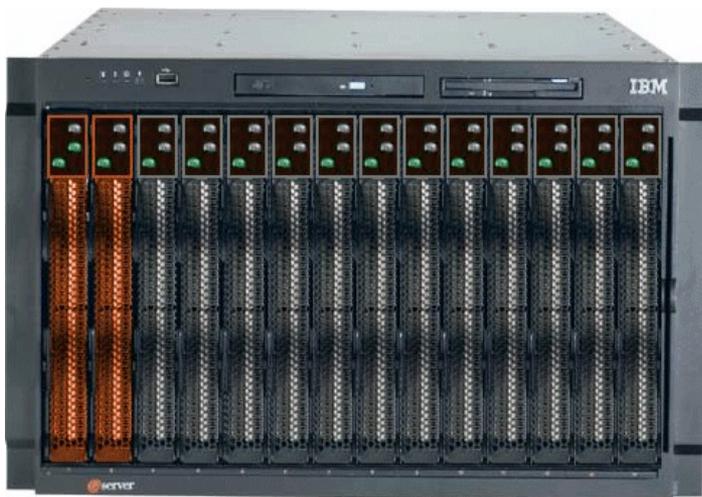


eSafe® VACD



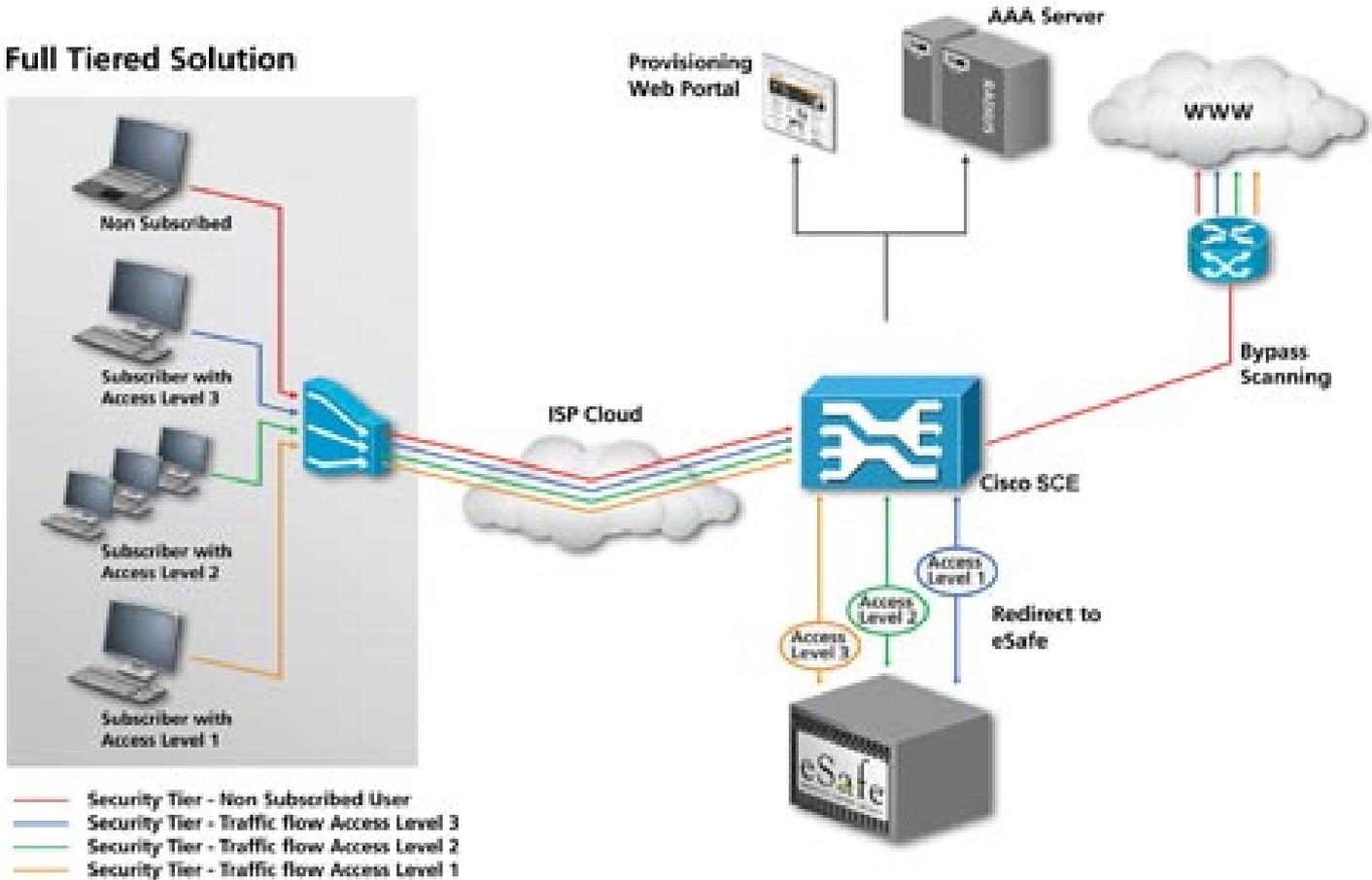
eSafe® для ISP

- Оптимизирован для выполнения на мощных аппаратных платформах (например IBM BladeCenter)
- Обеспечивает неограниченную пропускную способность при низкой стоимости владения
- Обеспечивает платформу для предоставления востребованной услуги очистки Интернет-трафика



Законченное решение

Full Tiered Solution



This Diagram shows a sample ISP environment with integrated provisioning services using Cisco Platform

Сертификат ФСТЭК

eSafe
PROACTIVE CONTENT SECURITY

СИСТЕМА СЕРТИФИКАЦИИ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ



ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ
№ РОСС RU.0001.01БИ00

СЕРТИФИКАТ СООТВЕТСТВИЯ № 1590

Выдан 7 апреля 2008 г.
Действителен до 7 апреля 2011 г.

Настоящий сертификат удостоверяет, что программный комплекс «Проактивная система контент-безопасности eSafe 6», децимальный номер 46538383.50 1400 001-06, разработанный и произведенный ЗАО «АЛАДДИН Р.Д.» в соответствии с техническими условиями 46538383.501400.001-06ТУ, функционирующий под управлением операционных систем Linux Red Hat, Windows NT/2000/2003/XP, является программным средством защиты информации, соответствует требованиям технических условий и может использоваться для создания автоматизированных систем до класса защищенности ИГ включительно в соответствии с требованиями руководящего документа «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации» (Гостехкомиссия России, 1992).

Сертификат выдан на основании результатов сертификационных испытаний, проведенных испытательной лабораторией ЗАО «Документальные системы» (аттестат аккредитации от 24.05.2006 № СЗИ RU.304.Б07.022) – техническое заключение от 27.02.2008, и экспертного заключения органа по сертификации Ассоциации ЕВРААС (аттестат аккредитации от 18.07.2003 № СЗИ RU.1225.А93.008) от 31.03.2008.

Заявитель: ЗАО «АЛАДДИН Р.Д.»
Адрес: 129226, г. Москва, ул. Докукина, д. 16
Телефон: (495) 223-0001

Контроль маркирования знаками соответствия сертифицированной продукции и инспекционный контроль ее соответствия требованиям указанных в настоящем сертификате руководящего документа и технических условий осуществляется испытательной лабораторией ЗАО «Документальные системы».



ЗАМЕСТИТЕЛЬ ДИРЕКТОРА ФСТЭК РОССИИ

А.Гапонов

Настоящий сертификат внесён в Государственный реестр сертифицированных средств защиты информации
7 апреля 2008 г.

Спасибо за Внимание!

eSafe®

*Перелыгин Д.А.,
Менеджер по работе с
партнерами и
корпоративными заказчиками*

eToken@aladdin.ru

eSafe@aladdin.ru