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

Перелыгин Д.А.,

Менеджер по работе с партнерами и корпоративными заказчиками

Объект и каналы утечек (9 мес. 2008)

Источник: http://www.viruslist.com/ru/analysis?pubid=204007639

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

Нелегитимные коммуникации

Нелегитимные коммуникации

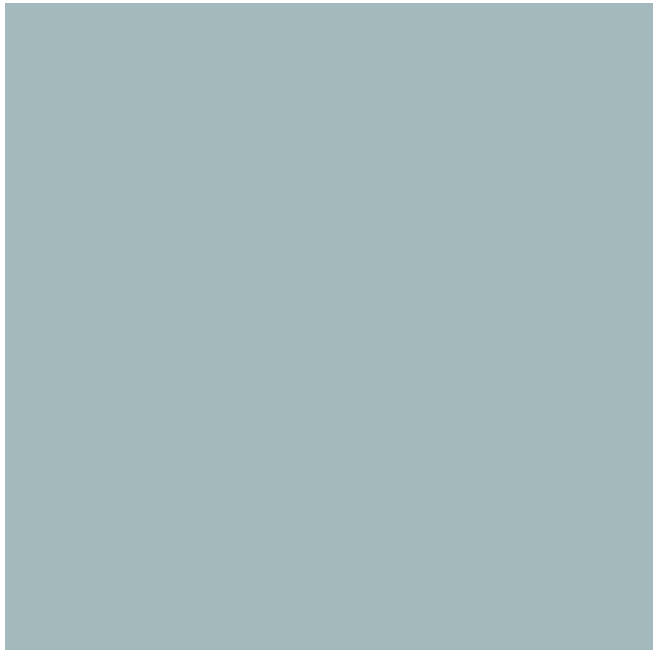
- HTTP PROXY 13,531
- SOCKS PROXY 57
- ANONYMUS WEB-PROXY 1,791
- MS INTERNET NET SHARING 3
- HTTP Tunneling 5
- HTTP (SSL) Tunneling 48
- HTTP OVER SSL (HTTPS) 1,502

Туннелинг

- HAMACHI 4

Трояны

- SeeMe Backdoor 1
- Brontok.A 1

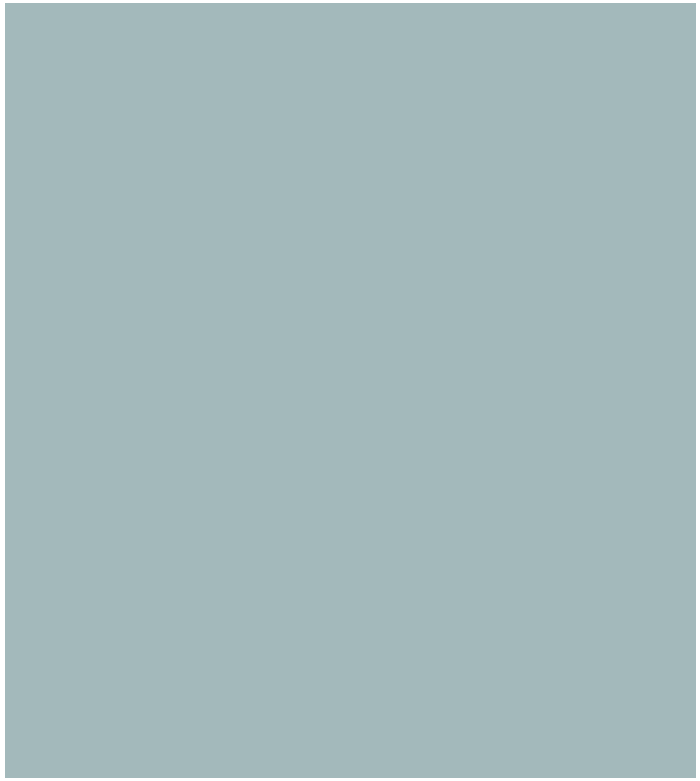


Нелегитимные коммуникации

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

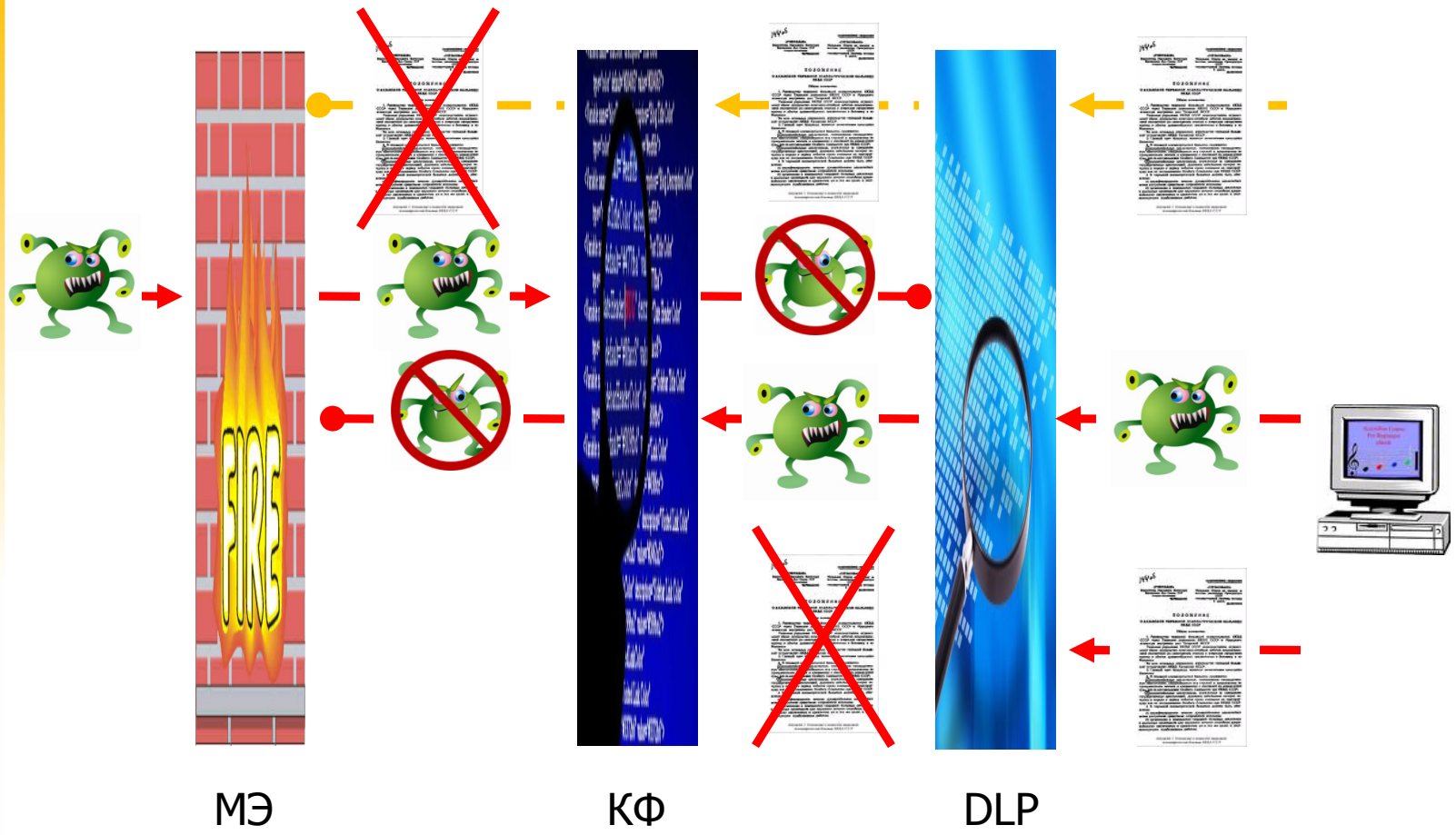
eSafe
PROACTIVE CONTENT SECURITY

Как это обычно происходит

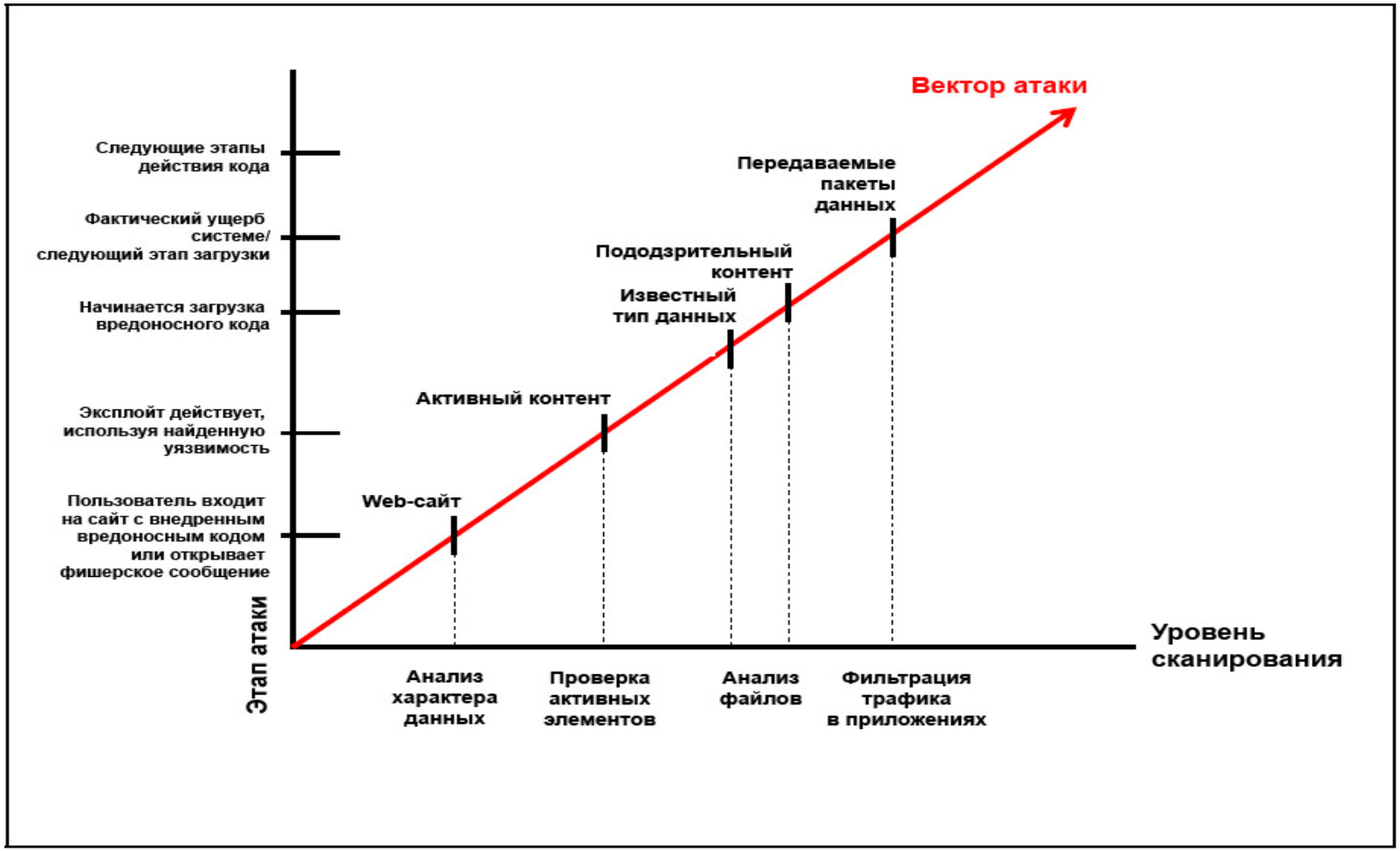
Aladdin
SECURITY SOLUTIONS

Как это может выглядеть

Системы безопасности (шлюз)



Требования к защите



eSafe
PROACTIVE CONTENT SECURITY

Как это реализовано в

… и других продуктах

Aladdin
SECURITY SOLUTIONS

eSafe
PROACTIVE CONTENT SECURITY

Уровень доступа к данным

I

URL фильтрация

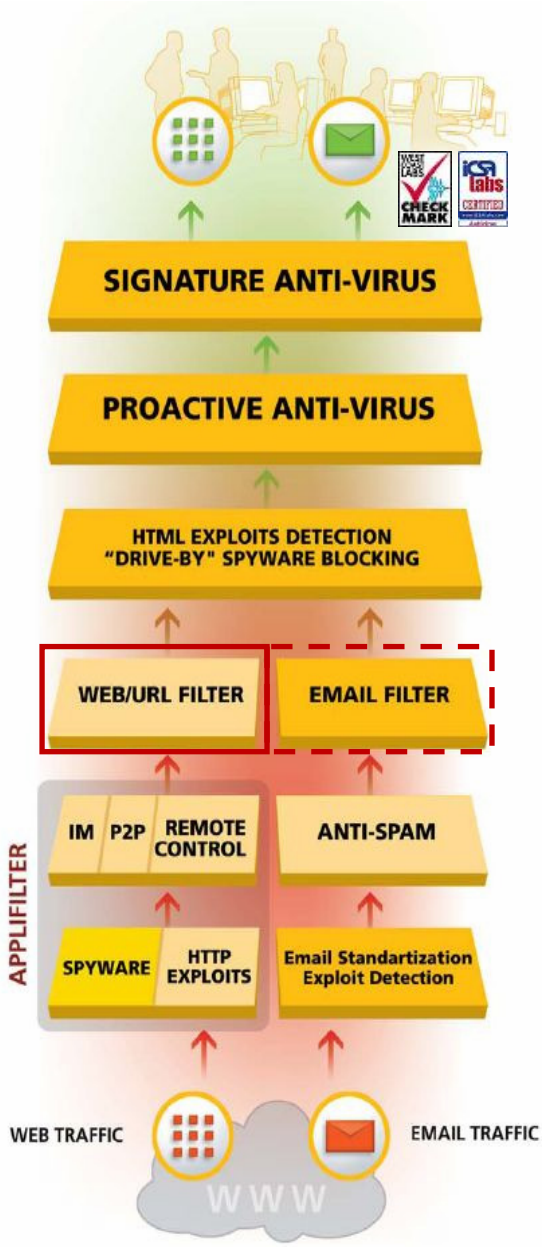
Aladdin
SECURITY SOLUTIONS

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

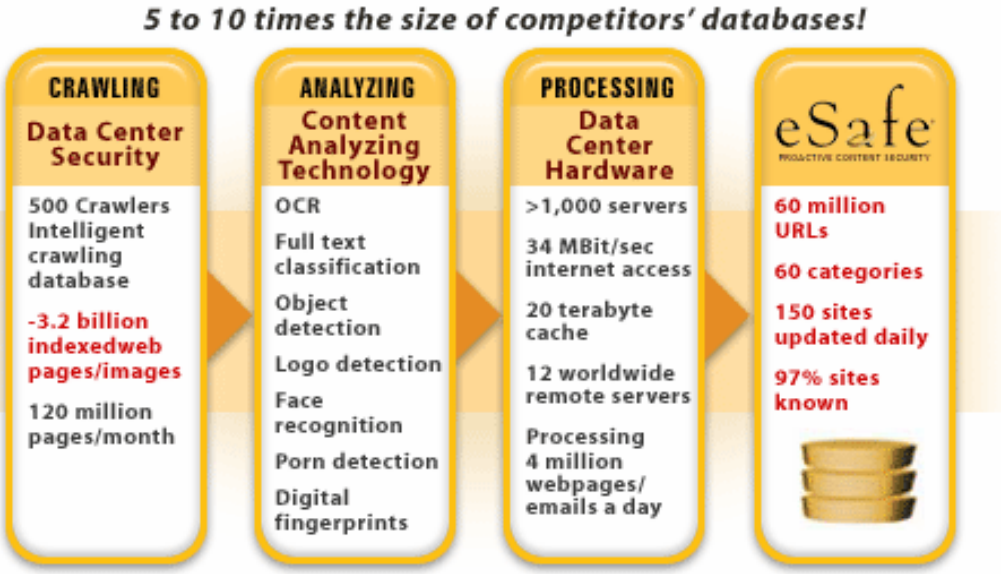
Возможность назначения политик:

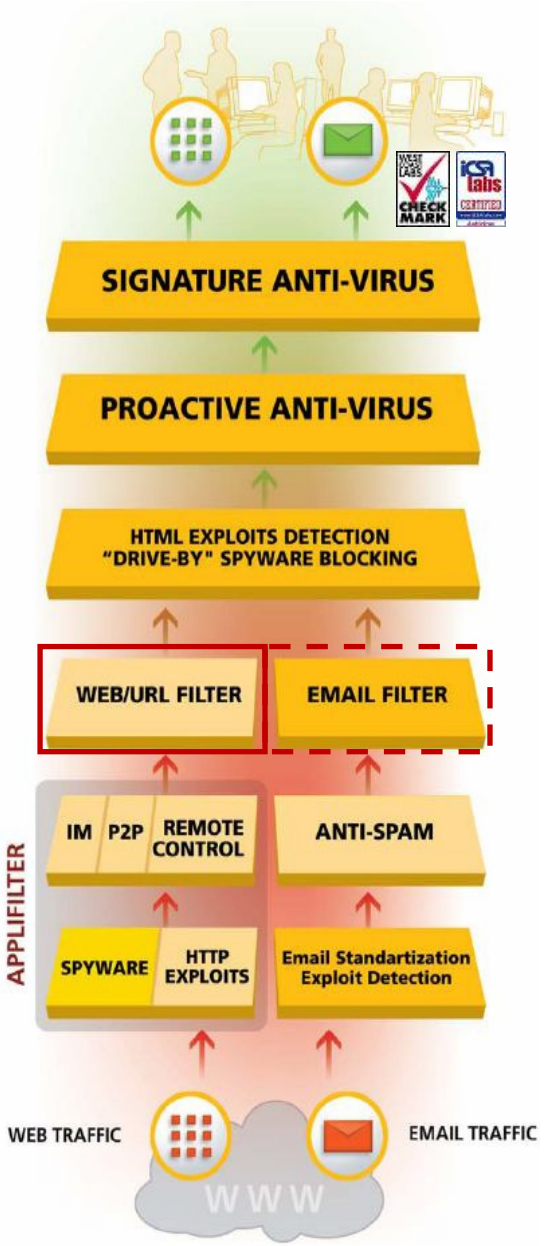
- В соответствии с бюджетом пользователя или его принадлежности к группе (LDAP/AD)
- По имени хоста или IP-адресу
- По принадлежности к подсети, диапазону IP-адресов или VLAN
- С использованием плагина к Microsoft ISA



eSafe® URL Filter

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





eSafe
PROACTIVE CONTENT SECURITY

Уровни анализа и передачи

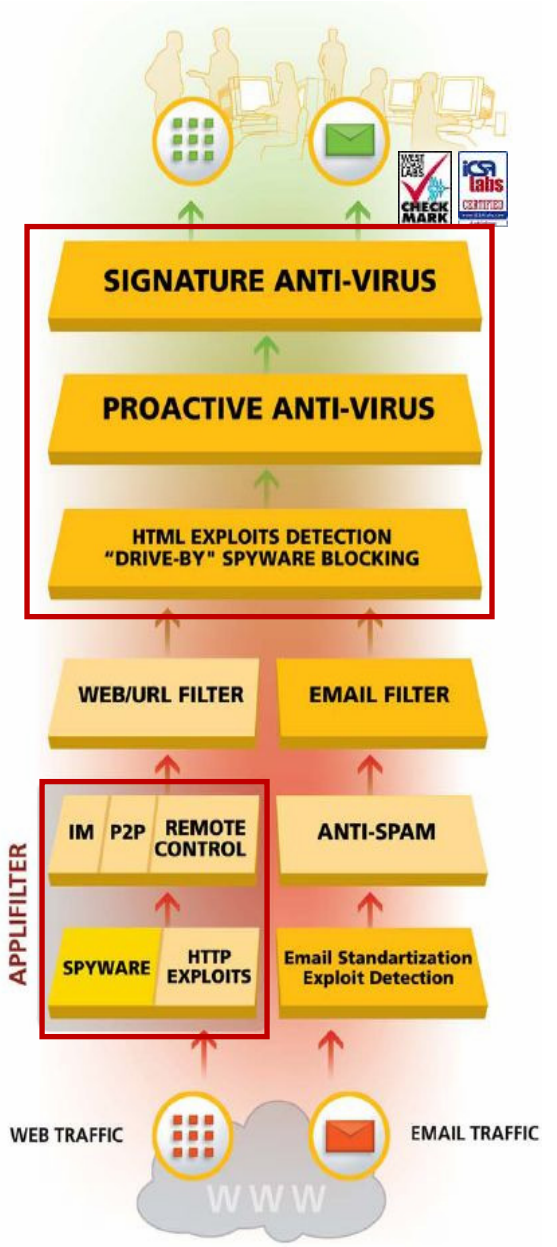
II,III

данных

Aladdin
SECURITY SOLUTIONS

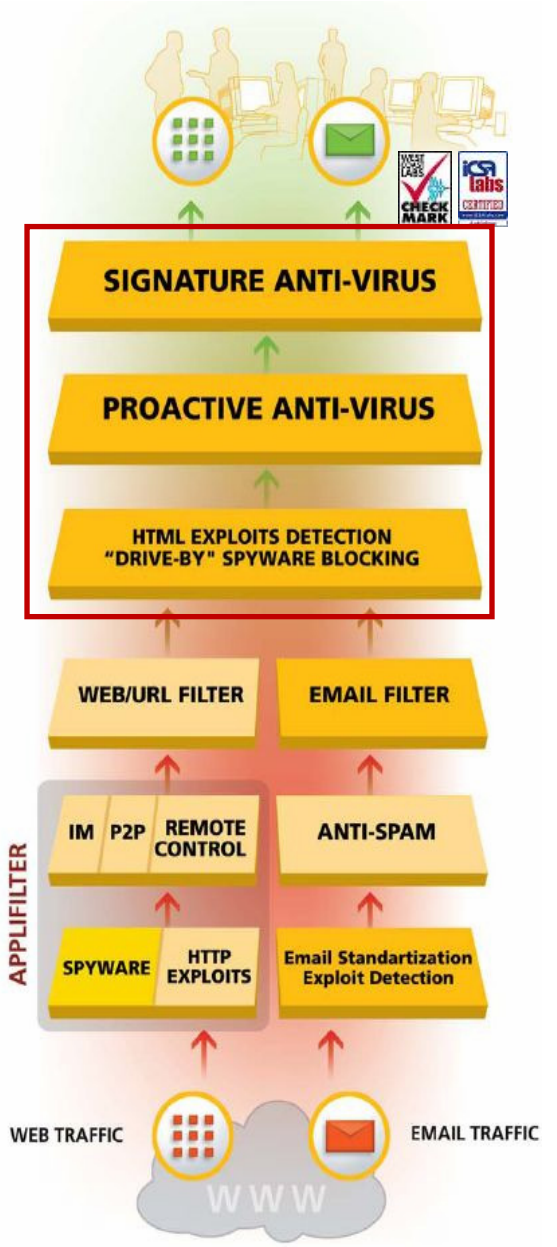
eSafe® WEB

- 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 предопределенных доверенных ActiveX объектов (опционально)
- Разрешение на выполнение только предустановленных доверенных ActiveX объектов

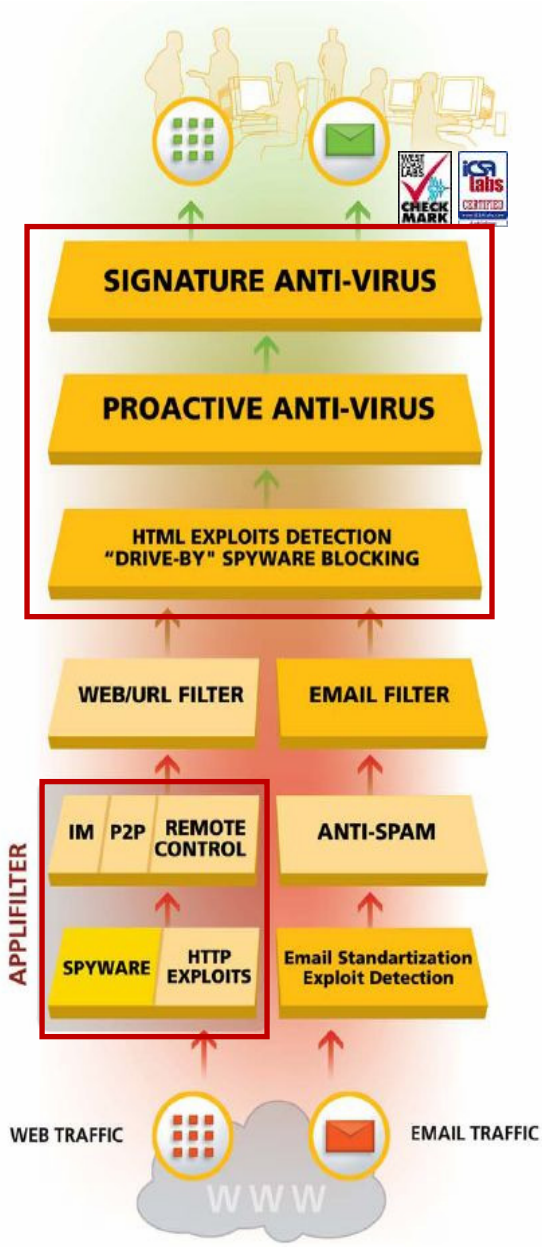


eSafe® WEB

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

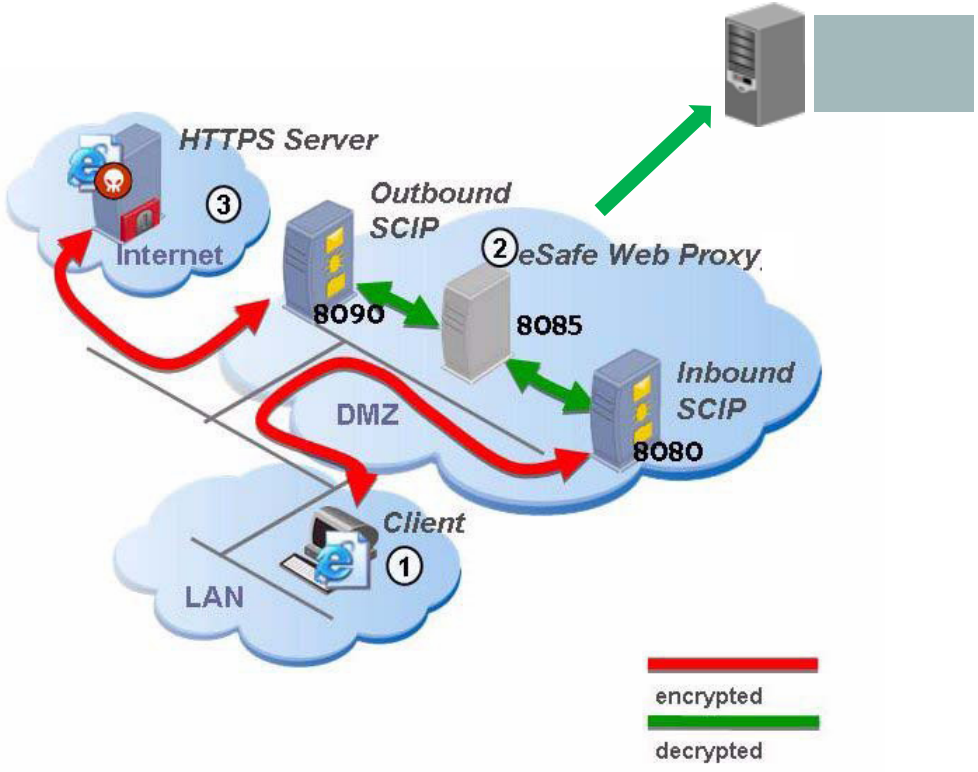
Четыре уровня блокирования Spyware:

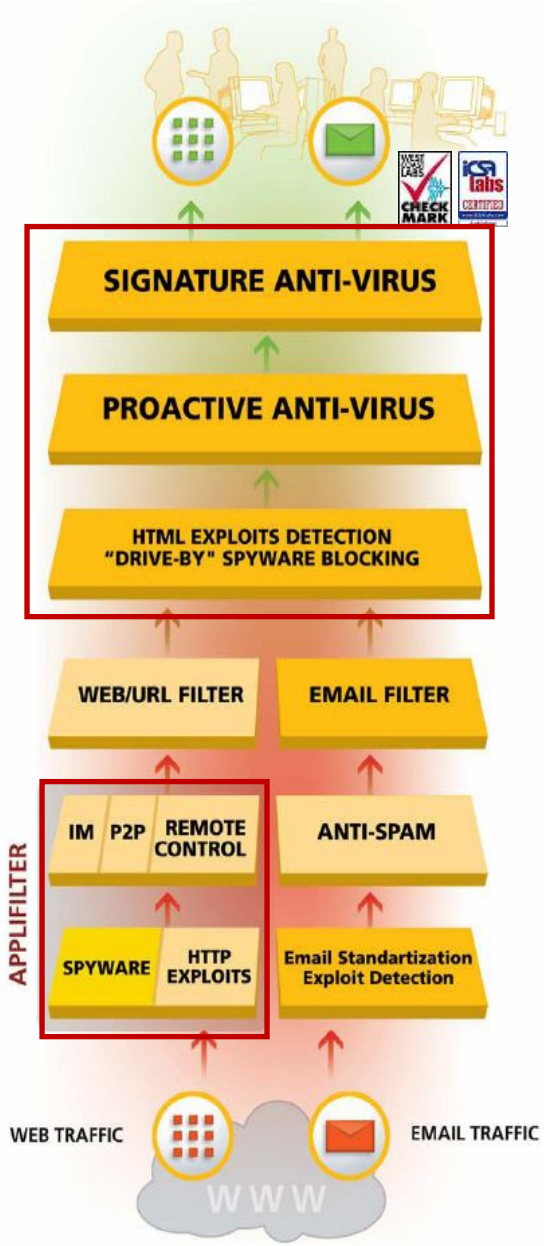
- Блокирование на уровне доступа
- Блокирование навязанной рекламы и предотвращение “drive by” Spyware
- Блокирование Spyware по сигнатурам
- Блокирование коммуникаций Spyware
- Многое другое …



eSafe® WEB SSL

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





eSafe
PROACTIVE CONTENT SECURITY

Уровень передачи данных

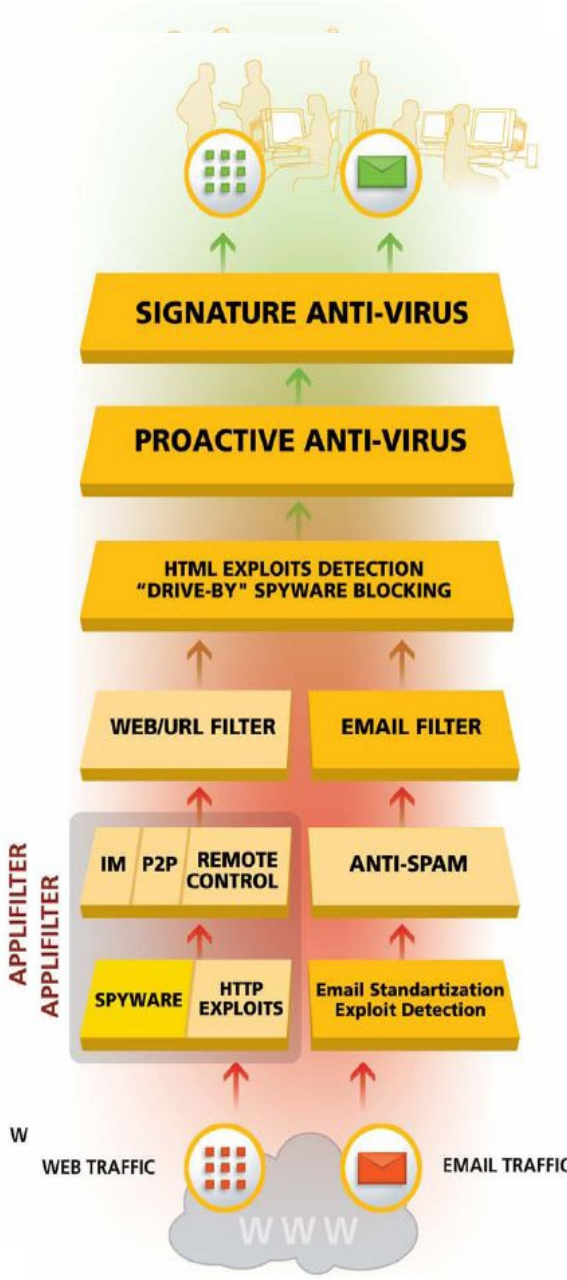
IV

Фильтр приложений

Aladdin
SECURITY SOLUTIONS

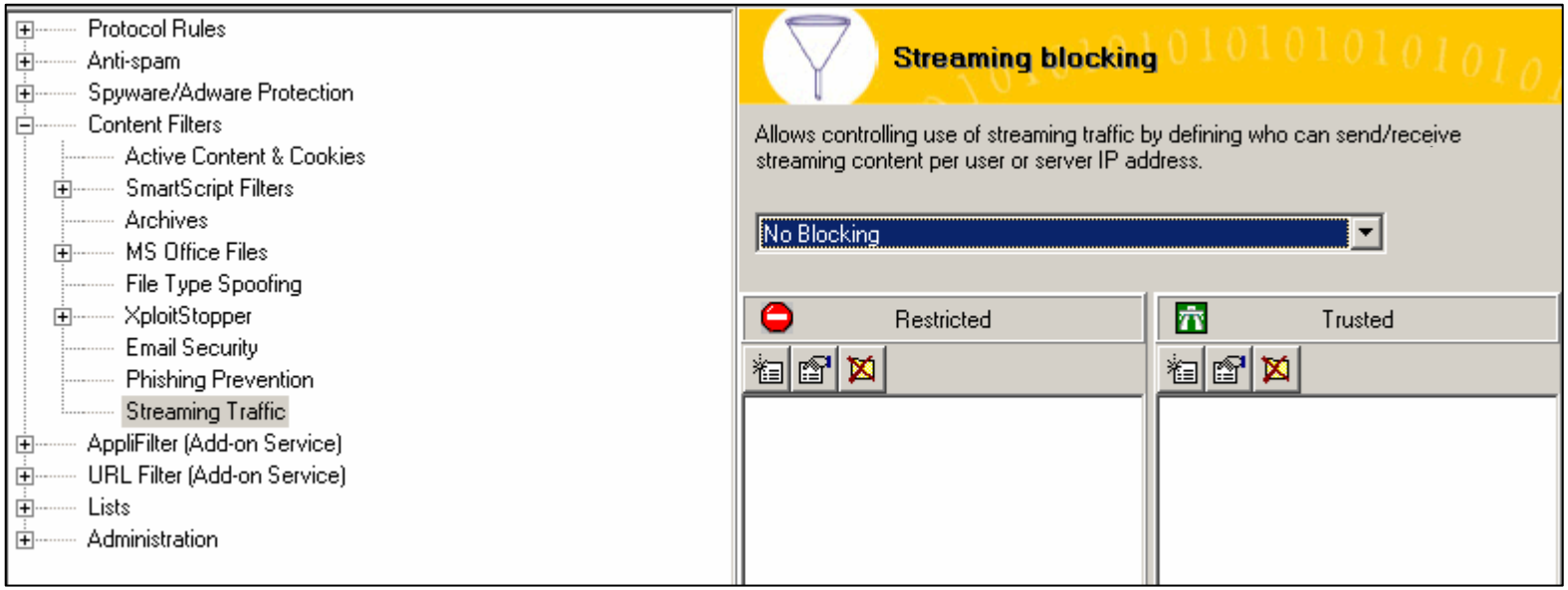
eSafe® Application Filter

- 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



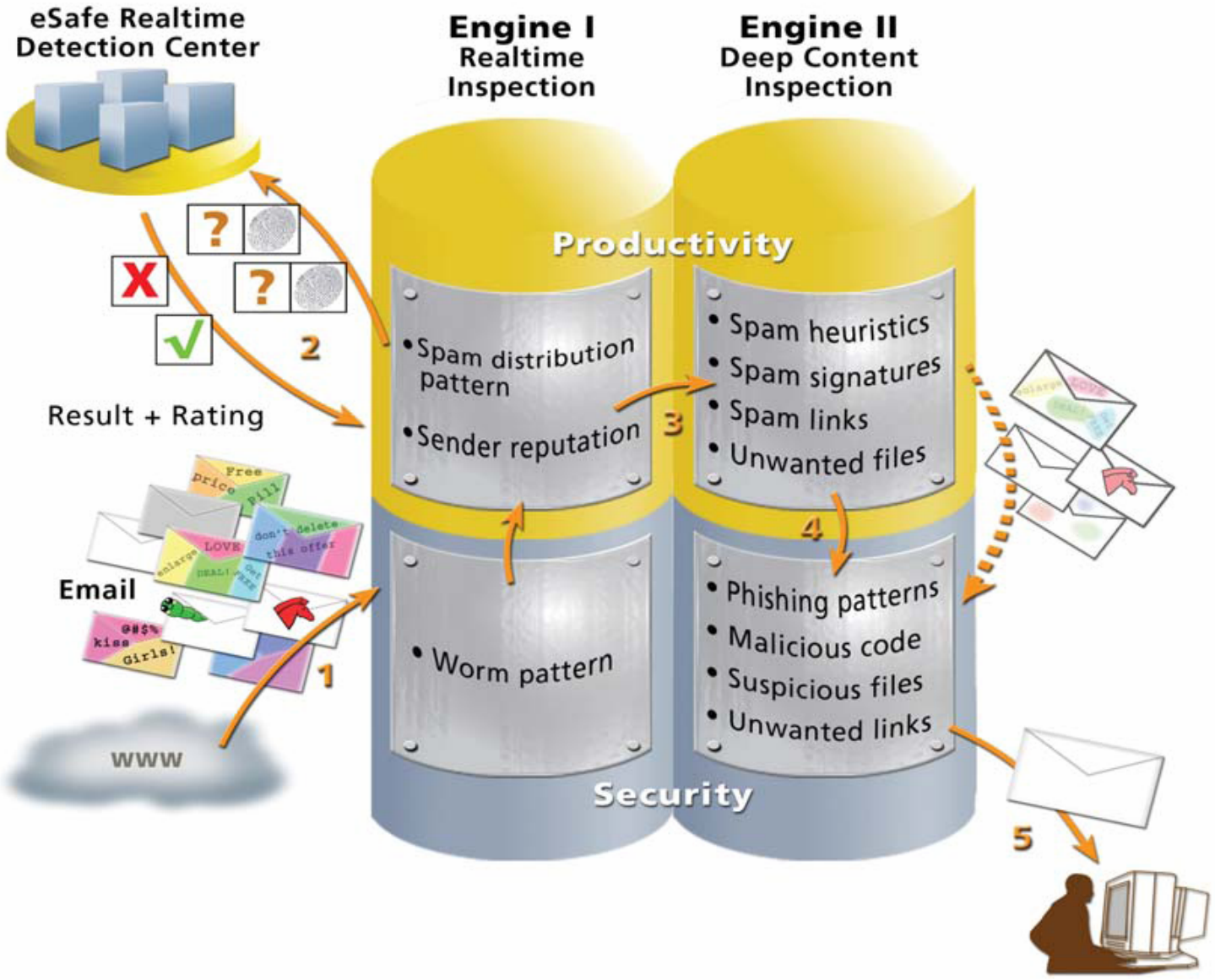
eSafe
PROACTIVE CONTENT SECURITY

Самое время спросить о Web в

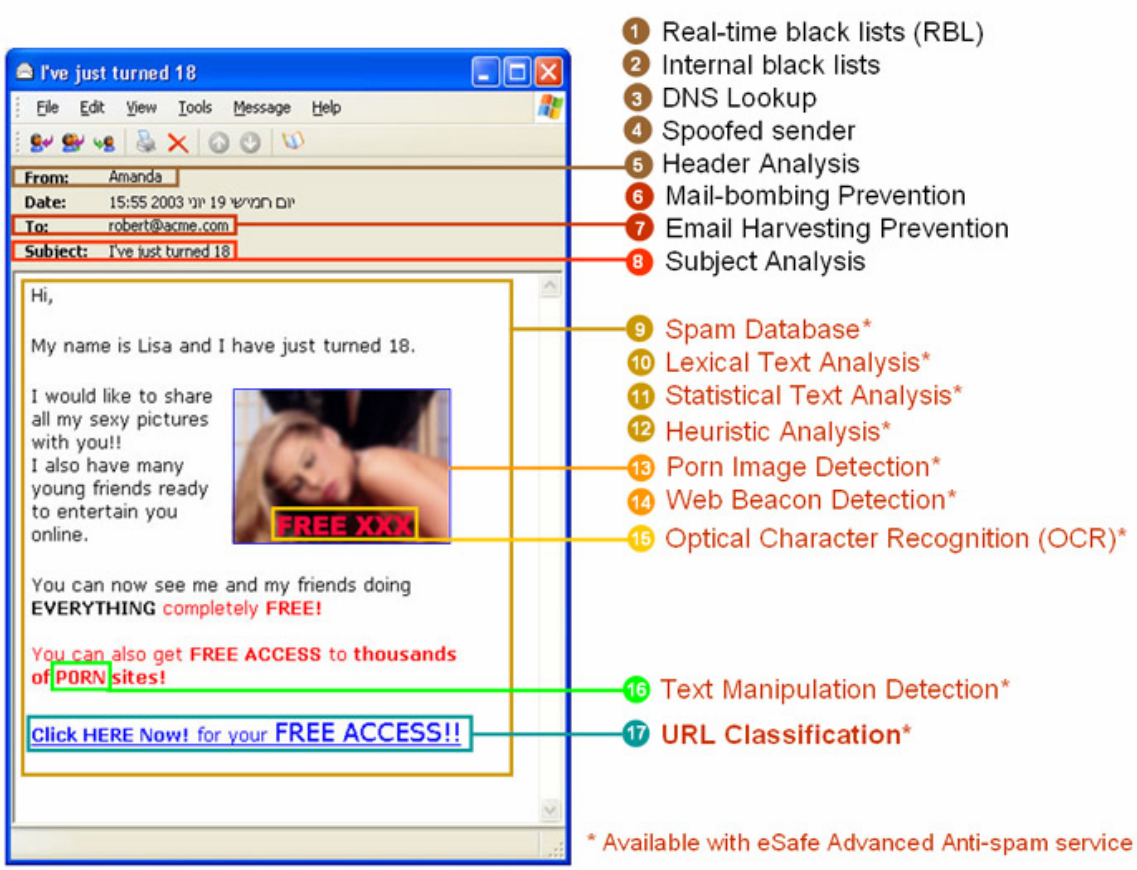
… и других продуктах

Aladdin
SECURITY SOLUTIONS

eSafe® Mail


eSafe Realtime Detection Center
Engine I Realtime Inspection
Engine II Deep Content Inspection
Productivity
Spam distribution pattern
Sender reputation
Spam heuristics
Spam signatures
Spam links
Unwanted files
Result + Rating
2
3
4
Email
1
Worm pattern
Phishing patterns
Malicious code
Suspicious files
Unwanted links
www
Security
5

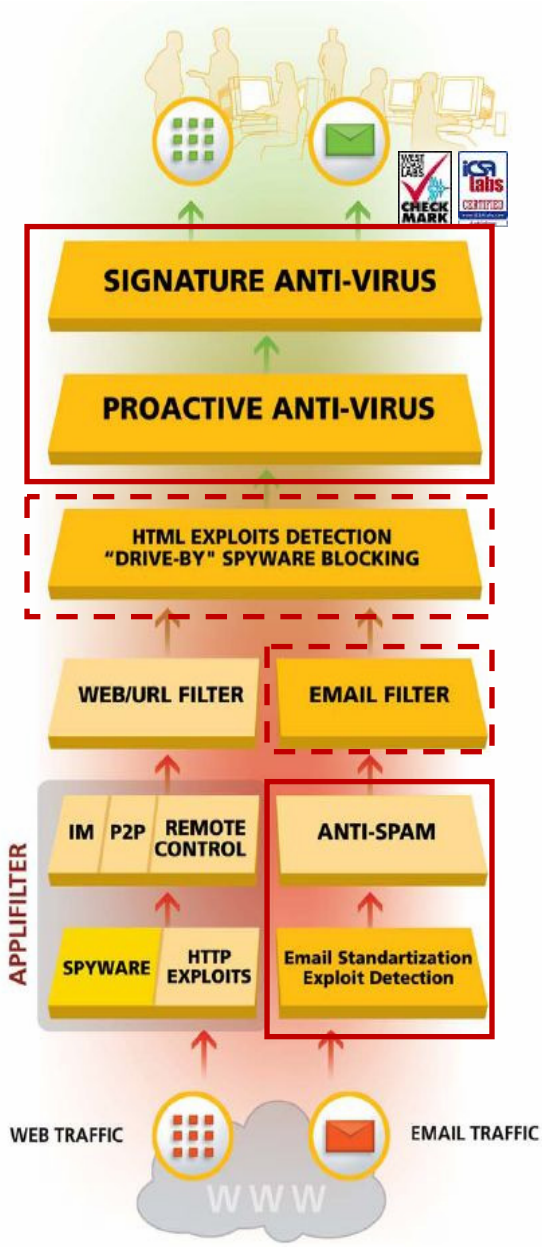
eSafe® Mail Content Filter



- Spam Phishing
- Spam Fingerprint
- Spam Fuzzy Fingerprint

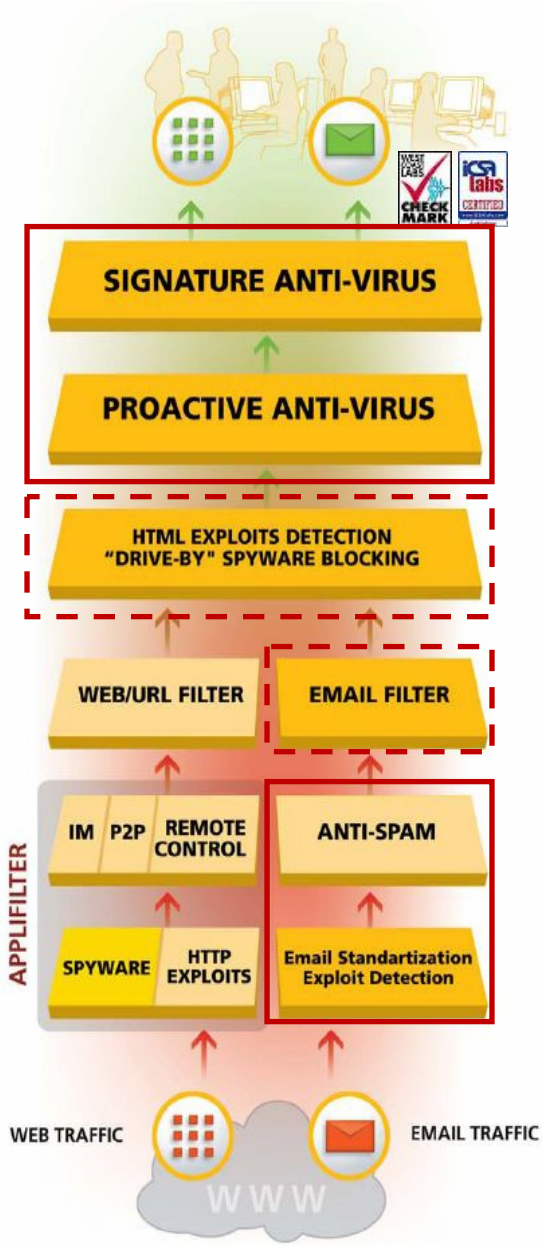
eSafe® Mail CSE

- 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

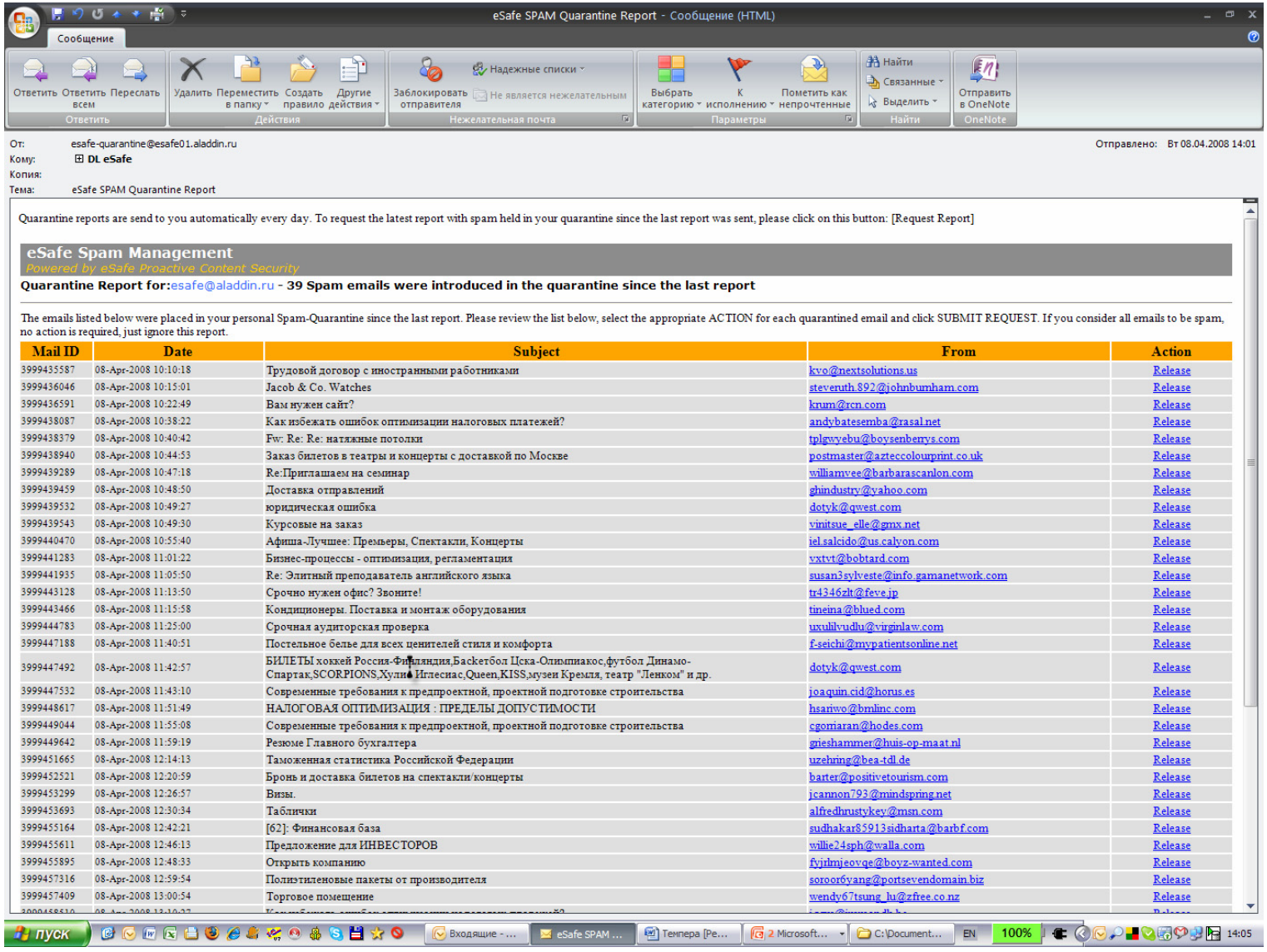


eSafe® Mail CSE

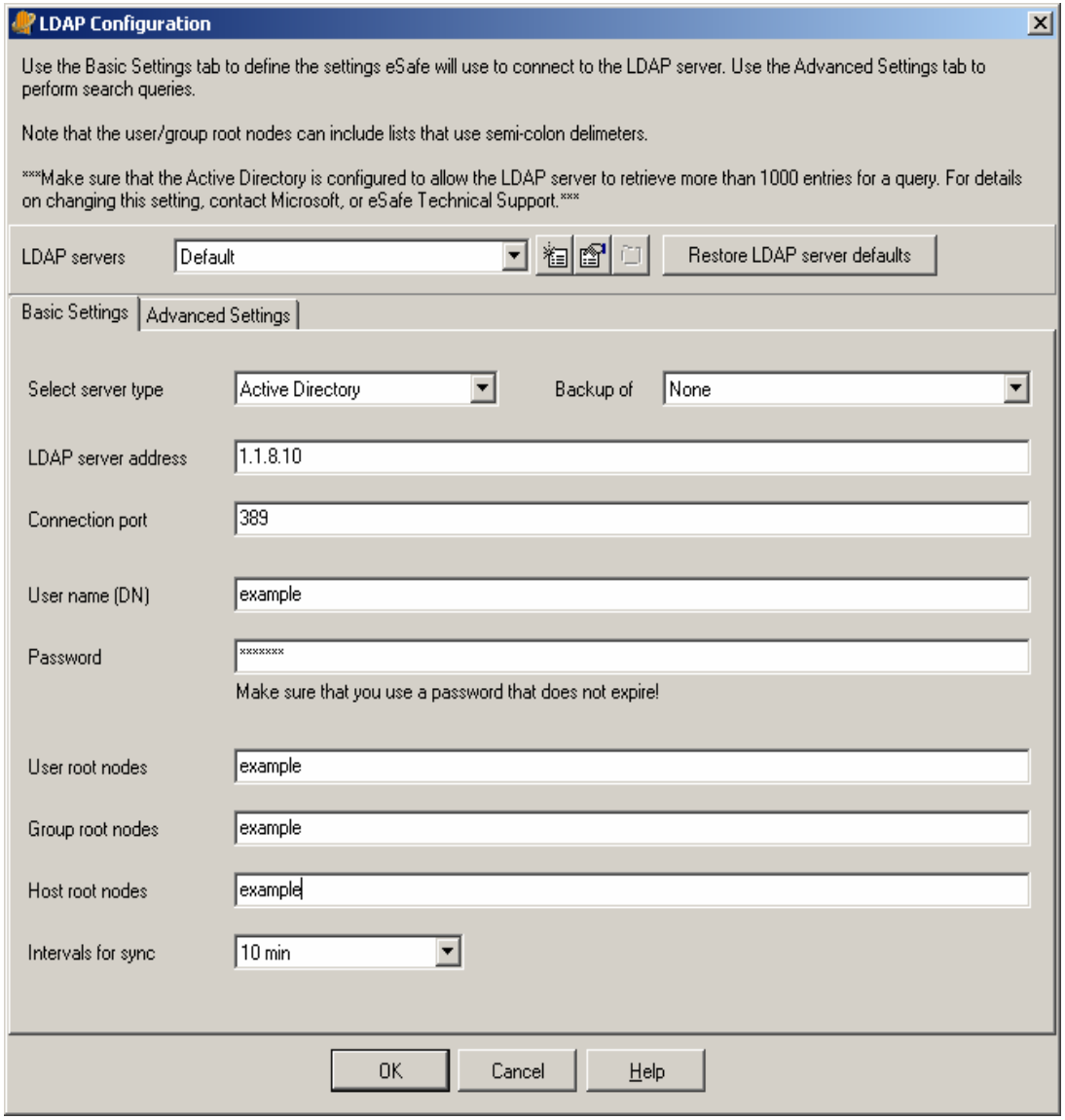
- Встроенные механизмы защиты от DoS, relaying, email spoofing, email attachment spoofing и т. д.
- Возможность автоматической отправки копии email на указанные адреса
- Возможность автоматической переадресации email на указанные адреса
- Возможность определения политик и ограничений для обработки почты 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

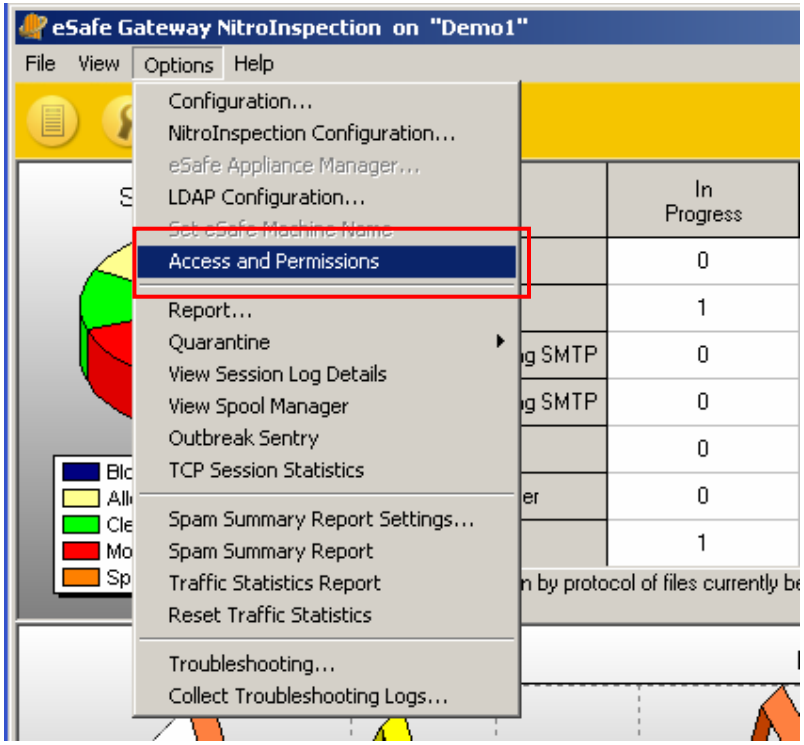


eSafe® и Multiple LDAP



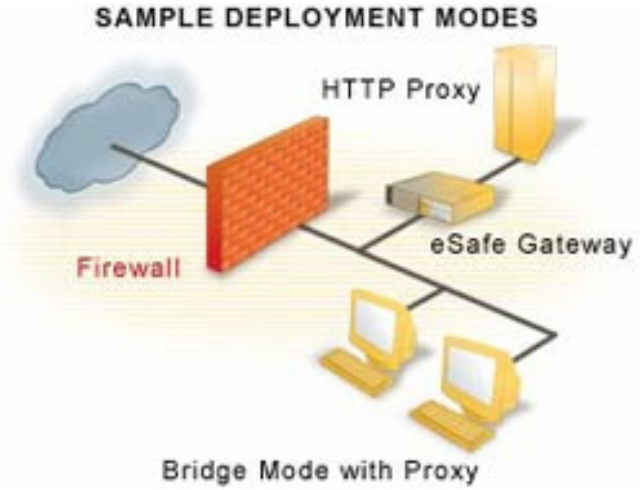
eSafe® Ролевое управление

- Реализация доступа к консоли управления с уровнем привилегий в зависимости от роли:
  - Администратор
  - Только чтение (режим мониторинга)
  - Управление карантином 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



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

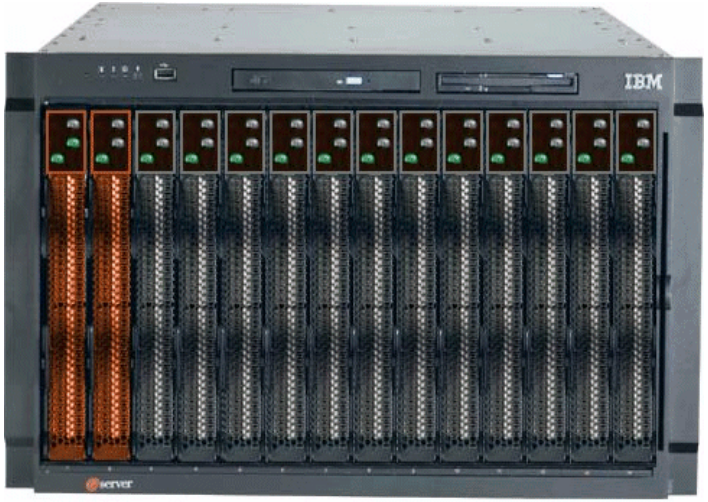
eSafe® HG-200 Appliance

eSafe® XG-300 Appliance

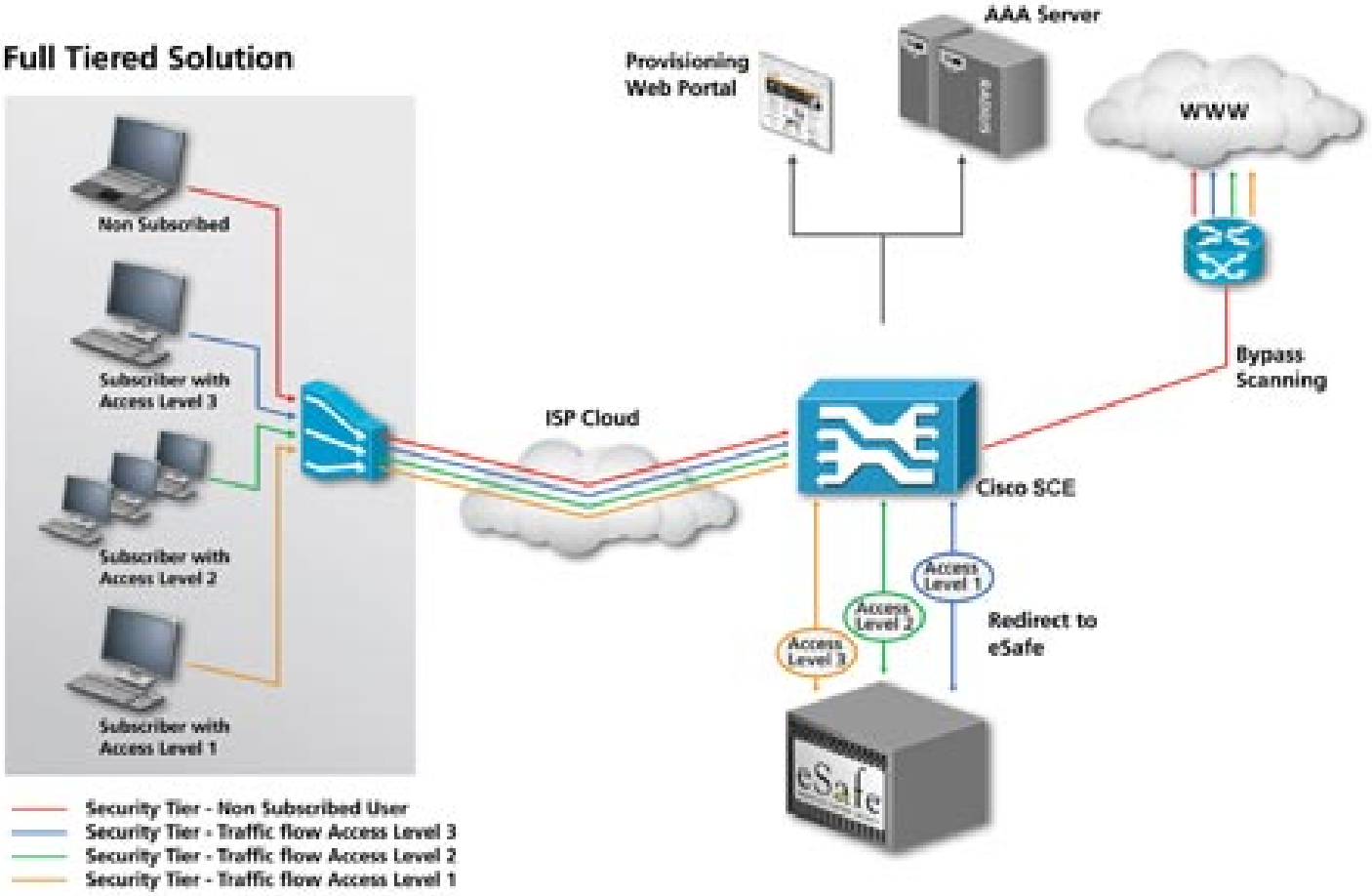
eSafe® VACD

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



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

Сертификат ФСТЭК

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 производимый 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 **1Г** 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 внесен в Государственный реестр сертифицированных средств защиты информации
7 апреля 2008 г.

Спасибо за Внимание!

Перелыгин Д.А.,

Менеджер по работе с партнерами и корпоративными заказчиками

eToken@aladdin.ru

eSafe@aladdin.ru