



eSafe® - ТОТАЛЬНЫЙ КОНТРОЛЬ  
НА ШЛЮЗЕ В ИНТЕРНЕТ

**eSafe**  
**SmartSuite**



Максим Чирков

Сыктывкар, 18 марта 2011 г.

ЗАЧЕМ ВСЕ ЭТО НУЖНО?



ТАК ЛИ ЭТО ОПАСНО?

# Угрозы и риски ИБ

- Конфиденциальность
- Целостность
- Доступность

Риск = F (Угроза; Уязвимость; Ущерб)

Угрозы :

Конфиденциальности

- Утечка информации по каналам Интернет
  - Результат действий инсайдера
  - Результат действий вредоносного программного обеспечения

Целостности

- Удаленное управление и получение административных полномочий над атакуемым ресурсом

Доступности

- Нарушение процесса функционирования элементов сетевой инфраструктуры

# Уязвимости

- Возможные ошибки в топологии (пересечения производственной и офисной сетей организации)
- Возможные ошибки конфигурирования активного оборудования опорной сети и средств защиты (те же пересечения, но на другом уровне сетевой модели) производственной и офисной сетей организации)
- Ошибки в назначении прав
- Уязвимости используемого системного и прикладного программного обеспечения
- Умышленные нарушения политик информационной безопасности
  - предоставление несоответствующих полномочий
  - злоупотребления администраторов
  - использование несанкционированных программ туннелирования и удаленного управления
- Рассеянное внимание сотрудников, в рабочее время использующих запрещенные политиками безопасности:
  - не относящиеся к работе ресурсы Интернет (**социальные сети**, клиентов служб мгновенных сообщений (IM), P2P, Skype, потоковые аудио/видео и т. д.
- Рассеянное внимание сотрудников, вызванное разборкой нежелательной корреспонденции (спам)



# Нецелевое использование ресурсов

- Использованием корпоративной электронной почты сотрудниками
  - для ведения личной переписки
  - для регистрации в интернет магазинах, **социальных сетях**, различных форумах и т. д.
- Использованием Web-почты
- Посещением сотрудниками организации из внутренней сети Интернет-ресурсов ненадлежащего содержания (порно, наркотики, warez, **социальные сети** и т. д.)
- Использованием сотрудниками организации Интернет пейджеров (IM), клиентов файлообменных сетей (P2P), Skype, удаленного управления по неавторизованным туннелям

Как следствие – реализация угроз, упомянутых ранее:

- Заражение компьютеров spyware
  - участие компьютеров организации в бот сетях
  - попадание IP-адресов организации в RBL
  - утечки конфиденциальной и персональной информации по трудно контролируемым каналам

Пример – эпидемия заражений malware Confiker (Kido)



# Немного аналитики по итогам 2010 года\*)

## Основные типы инцидентов (отраженных)

- Атаки через Интернет
- Локальные инциденты
- Сетевые атаки
- Инциденты в электронной почте



## Из них инцидентов первого типа

- Атаки на браузеры - >500 миллионов в год
  - Непосредственное инфицирование
  - Трафик (Drive-By, Black SEO и т. д.)
- Атаки через P2P – от 2.5 до 10 миллионов в месяц  
В основном – самораспространяющиеся вредоносные программы (черви)



Огромное количество атак на популярные сервисы –



 \*) А.Гостев. Kaspersky Security Bulletin 2010. Развитие угроз в 2010 году

# Прогноз на 2011 год

## Используемые методы

- Эксплуатация уязвимостей системного и прикладного ПО
- Развитие Spyware 1.0 (Classic)
  - Похищение данных о банковских картах, финансовые мошенничества
  - Включение в состав бот-сетей (DDoS, спам etc.)
- Расширение списка атакуемых платформ:
  - 64 битная MS Windows
  - Android
- Расширение присутствия в социальных сетях

## Преследуемые цели

- Развитие нового вида malware, нацеленного на технологические сети (Stuxnet)

## Прогнозируемые тенденции

- Появление новых игроков на рынке malware
- Появление Spyware 2.0, ориентированного на похищение любых личных данных (Identity Theft)
- Перенаправление вектора атак в сторону корпоративных пользователей "в ущерб" домашним

Январь 2011 года – 68,956,183 зафиксированные атаки через браузеры



\*) А.Гостев. Kaspersky Security Bulletin 2010. Развитие угроз в 2010 году

# Реализация угроз

## Инфицирование

- Браузинг (веб серфинг, блуждание по сайтам etc.)
- Загрузка файлов (HTTP, FTP, FTP через HTTP, HTTPS, P2P, IM etc.)
- Электронная почта
- Найм на работу инсайдера либо вербовка прежде лояльного сотрудника

## Выполнение "полезной нагрузки"

- Распространение "инфекции" всеми возможными способами
- Похищение и передача похищенных данных
- Реализация деструктивных воздействий посредством программ удаленного управления
- Участие в различного рода атаках (DDoS), рассылке спама
- Передача конфиденциальной информации инсайдером по каналам Интернет



dreamstime.com

ПРЕДОТВРАЩЕНИЕ

**eSafe**

**SmartSuite**

ИНФИЦИРОВАНИЯ



# URL фильтр

## Браузинг (веб серфинг)

Ограничение доступа к несоответствующим, не продуктивным и потенциально опасным web-сайтам за счет использования

- Одной из лучших в отрасли база категорированных URL\*):
  - 80 категорий
  - Более 100 миллионов категорированных web-сайтов
- Динамической фильтрации
- Разрешенных, запрещенных, “серых” категорий
- Квотирования трафика (глобально и по категориям)
- Блокирования анонимайзеров
- Фильтрации по HTTPS



\*) eSafe v.8.6



**В ДОСТУПЕ ОТКАЗАНО!!!**

Вы обратились к ресурсу, запрещенному к использованию политикой информационной безопасности предприятия!

*The URL <http://porno.ru/> was blocked, it is in the Restricted Pornography category.*

# Обезвреживание вредоносного кода

Полная проверка HTTP, FTP, SMTP, POP3, HTTPS

- Два антивирусных мотора:
  - Aladdin:
    - Проактивный антивирус. Проактивное блокирование до 98% вредоносного кода “zero-hour”, включая троянов и червей
    - Сигнатурный антивирус, сертифицированный на 100% блокирование “диких” вирусов
  - Антивирус Касперского – KAV v8
- Защита от эксплойтов. Проактивное блокирование попыток эксплуатации уязвимостей в веб 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® - единственное на рынке решение, которое не использует технологию проксирования (но может работать как прокси)



# Фильтр приложений

Ключевые слова - **сигнатуры протоколов**

Блокирование попыток обхода URL фильтра

- Блокирование HTTP туннелинга и ряда методов, используемых анонимайзерами для обхода систем защиты
- Предотвращение туннелирования
- Запрет использования не доверенных сертификатов



Блокирование использования потенциально опасных веб приложений

- Клиентов программ файлообменных сетей (BitTorrent, DC++, **Skype** ...)
- Интернет-пейджеров или передачу файлов их средствами (ICQ/AOL, Google Talk, Yahoo!, MSN ...)
- Web 2.0 приложений (Adobe Connect, Google DOCs, Gmail/Hotmail Upload/Download Attachments ...)
- Социальных сетей (Facebook, Twetter, Odnoklassniki ... - выборочное блокирование потенциально опасных функций)
- Online игр (World of WarCraft, Second Life, Poker Stars ...)

**Злой умысел (инсайд) – только HR!!!**

БЛОКИРОВАНИЕ

**eSafe**

**SmartSuite**

“ПОЛЕЗНОЙ” НАГРУЗКИ

# Фильтр приложений

Ключевые слова - **сигнатуры протоколов**

Блокирование трафика шпионских программ (MDLP)

Блокирование каналов связи, которые невозможно контролировать средствами DLP (анти-инсайд)

- Блокирование трафика неавторизованного туннелирования
  - HTTP Tunneling
  - HTTP (SSL) Tunneling
  - HTTP OVER SSL (HTTPS)
  - TOR, HAMACHI etc.
- Блокирование трафика потенциально опасных веб приложений
  - Интернет-пейджеров (ICQ/AOL, Google Talk, Yahoo!, MSN ...)
  - Web 2.0 приложений (Adobe Connect, Google DOCs, Gmail/Hotmail Upload/Download Attachments ...)
  - Социальных сетей (Facebook, Tweeter, Odnoklassniki ... - выборочное блокирование потенциально опасных функций)
  - Облачных хранилищ (iDrive, DropBox ...)
- Блокирование программ удаленного управления



Symantec  
pcAnywhere

netviewer



# Data Leakage Prevention (DLP)

eSafe DLP – решение для прагматиков

Позволяет определить профили и привязать к ним соответствующие политики для мониторинга исходящего трафика

## Определение профиля

APPS DLP Alerts Updates

### DLP Profiles

Allows defining profiles for preventing data leakage in outgoing traffic. To do this, you must associate network entities based on users and groups taken from the LDAP server, with a specific DLP policy.

#### Profiles

Entity	Policy	Activation status
<input type="checkbox"/> ALL	Default	Always active

### Network Entities Handler

Allows you to view information on users/groups taken from the LDAP server (Objects | LDAP Configuration) and manually define new network entities, including: users, groups, IP addresses, IP address ranges, VLANs, hosts, and domains.

Group User IP address IP address range VLAN Host Domain

Filter: default

Groups	Members	Member of
<ul style="list-style-type: none"><li>Accounting</li><li>Admin</li><li>All</li><li>Developments</li><li>Finance</li><li>IT</li><li>Manager</li><li>QA</li></ul>		

Search:

Reload DB Select Close Help

# Data Leakage Prevention

## Определение политики

PPs DLP Alerts Updates

### DLP Policies

Allows defining to which file and traffic types the DLP policy applies, and which dictionaries will be used to search for content.

Policy name: Default  
Description: Default DLP Policy

Monitor | Dictionaries | Actions

Allows defining to which files and traffic types the DLP policy applies.

Enabled for all outgoing traffic  
 Enabled for file types selected below  
 Disabled for file types selected below

Description	Extensions
<input checked="" type="checkbox"/> Adobe	fla,flv,swf*.pdf,pmd,psb,psd,pdd,ai,prc,as,jsfl,ppj,indl
<input type="checkbox"/> Archives	a,ar,cpio,shar,LBR,tar,bz2,f,gz,lz,lzma,lzo,rz,sfark,7z,
<input checked="" type="checkbox"/> Excel Files	xls,xlsx,xlam,xlsb,xlsm,xltm,xltx,csv,dif,iqy,slk,xla,xlb,
<input type="checkbox"/> Images	abr,ani,art,arw,bmp,cnv,cr2,craw,crw,cur,cvx,dcr,dcx
<input type="checkbox"/> Internet	asp,aspx,atom,axd,axl,cgi,cls,crt,css,css1,dcd,dtd,hte
<input type="checkbox"/> Media files	asf,wma,avi,mp3,mp2,mpa,mid,midi,rmi,aif,aifc,aiff,au,
<input type="checkbox"/> Office 2007 Files	accdb,accde,accdr,accdt,bdr,docm,docx,dotm,dotx,gf-
<input type="checkbox"/> Office Any Files	ans,asa,contact,dict,dif,doc,docx,etl,frm,ldf,log,m13,n
<input type="checkbox"/> Office Core Files	doc,docx,rtf,xls,xlsx,csv,dif,iqy,slk,xla,xlb,xlc,xld,xlk,>
<input checked="" type="checkbox"/> PowerPoint Files	pot,pps,ppsx,ppt,pwz,thmx,potm,potx,ppsm,pptm,ppt
<input checked="" type="checkbox"/> Source code files	c,cpp,h,java,hpp,inc,pas,dcr,mak,dsw
<input checked="" type="checkbox"/> Word Files	doc,docx,rtf,dotm,dot,dotx,dotm

Apply to:  Mail  Web  FTP

**Типы файлов**

PPs DLP Alerts Updates

### DLP Policies

Allows defining to which file and traffic types the DLP policy applies, and which dictionaries will be used to search for content.

Policy name: Default  
Description: Default DLP Policy

Monitor | Dictionaries | Actions

Select which dictionaries will be used:

Dictionary Name: Description:

- \*Any outgoing file
- Canada SIN
- Confidential Information
- Credit Card
- email Addresses
- English Gambling Words
- English Profanity Words
- English Racism Words
- Financial Information
- GLBA
- Hacker Research
- IP Addresses
- Job Search
- Login credentials
- Mail Addresses
- PCI-DSS
- Postal Codes
- Sox
- UK NDNo
- US SSN

**Словари**

PPs DLP Alerts Updates

### DLP Policies

Allows defining to which file and traffic types the DLP policy applies, and which dictionaries will be used to search for content.

Policy name: Default  
Description: Default DLP Policy

Monitor | Dictionaries | Actions

Select the actions eSafe will take if the selected dictionaries match the data:

- Report
- Block
- Archive to repository
- Notify sender
- Forward file by email

Define email recipients for forwarded files (CSV format):

**Действие**

# Data Leakage Prevention

## Определение нового словаря

DLP Dictionaries

Define dictionaries and select which rules will be used.

Dictionaries

- \*Any outgoing file
- Canada SIN
- Confidential Information
- Credit Card
- email Addresses
- English Gambling Words
- English Profanity Words
- English Racism Words
- Financial Information
- GLBA
- Hacker Research
- IP Addresses
- Job Search
- Login credentials
- Mail Addresses
- NW**
- PCI-DSS
- Postal Codes
- Sox
- UK NIINo
- US SSN

Name: NW  
Description: Nuclear weapon, Nop Secret

**Новый словарь**

DLP Dictionaries

Define rules by creating expressions, assigning a weight to the rule, and defining in which section of the file the rule will apply.

Name	Section...	Weight	Variant...	Required
Nuclear ...	ANY	1	0	1

**Новое правило**

Containing dictionaries: NW

**Edit rule**

Rules are created by defining expressions, that consist of a filter, threshold, selecting the expression type, and defining the distance between the characters.

Details

Name: Nuclear weapon File section: ANY

Weight: 1  Variant weight/Counted

Required

Expressions

Filter: None Threshold

Type: Unicode Regular Expressions Must be X characters apart: 0

Expression	Weight	Counted	Required	Case sensitive
Nuclear Bomb	1	1	0	0
Ядерная бомба	1	1	0	1

OK Cancel

ЗАЩИТА  
**eSafe**  
SmartSuite

ЭЛЕКТРОННОЙ ПОЧТЫ

# Предотвращение инфицирования (eMail)

Полная проверка HTTP, SMTP, POP3, HTTPS

- Два антивирусных мотора:
  - Aladdin:
    - Проактивный антивирус. Проактивное блокирование до 98% вредоносного кода “zero-hour”, включая троянов и червей
    - Сигнатурный антивирус, сертифицированный на 100% блокирование “диких” вирусов
  - Антивирус Касперского – KAV v8
- Защита от эксплойтов. Проактивное блокирование попыток эксплуатации уязвимостей в веб 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



# Подавление нежелательных рассылок

## Антиспам v.8.6 – замена мотора

The screenshot shows the configuration interface for 'Advanced Anti-Spam Engines'. The left sidebar contains a tree view with categories like Protocol Rules, Anti-spam, DNS Lookup, Spyware/Adware Protection, Content Filters, and Email Settings. The main content area is titled 'Advanced Anti-Spam Engines' and contains the following text: 'The Real-time Reputation Engine checks the reputation of email for spam by checking the email properties and content in real-time against a global data center, that uses spam bots and sensors installed around the globe that detect spam outbreaks as they emerge.' Below this text are two checked checkboxes: 'Spam realtime reputation engine' and 'Use IP reputation engine'. A red box highlights the 'Use IP reputation engine' checkbox and the text below it: 'The IP Reputation Engine checks the reputation of the email sender IP address against global databases in real-time. If the IP address is a known spamming address, eSafe will reject the connection at an early stage of the SMTP handshake without accepting or quarantining the email.'

v. 8.6

The screenshot shows the configuration interface for 'Anti-spam Configuration'. The top navigation bar includes 'APPS', 'DLP', 'Alerts', and 'Updates'. The main content area is titled 'Anti-spam Configuration' and contains the text: 'Select methods eSafe will use to identify and block spam.' Below this text are two checked checkboxes: 'Spam realtime reputation engine' and 'Spam content analysis engine'. A red box highlights the 'Spam content analysis engine' section, which contains a list of checked options: 'Smart signature matching', 'Text analysis', 'Flow control', 'Bayesian classification', 'Phishing', 'Fuzzy Finger Print', 'Meta-heuristics', 'URL categories', 'Known spam URLs', 'Structure analysis', and 'Finger Print'. A 'List' link is visible next to 'URL categories'.

v. 8.5

# Ложные срабатывания и карантин

Сообщение

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

Отправлено: Вт 08:04 2008 14:01

Quarantine reports are send 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 Interactive Content Security

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

The email 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
3999435281	08-Apr-2008 10:10:18	Трудовой договор с иностранцами работниками	kyv@nestsoft.com.ua	Release
3999436048	08-Apr-2008 10:15:01	Jacob & Co. Watches	stevenmh597@comcast.com	Release
3999436591	08-Apr-2008 10:22:49	Ваш любимый сайт?	knem@rsm.com	Release
3999436887	08-Apr-2008 10:38:22	Как избежать ошибок оптимизации налоговых платежей?	andrbatemba@ruralnet	Release
3999438479	08-Apr-2008 10:40:42	Рв. Ре. Ре. матюжные потопки	mlpnyevs@boxenberry.com	Release
3999438960	08-Apr-2008 10:44:55	Заказ билетов в театры и концерты с доставкой по Москве	postmaster@accessgroup.co.uk	Release
3999439289	08-Apr-2008 10:47:38	Re: Приглашения на семинар	wilamox@habacast.com.com	Release
3999439459	08-Apr-2008 10:48:50	Доставка отправлений	ghin@att.net	Release
3999439552	08-Apr-2008 10:49:27	юридическая ошибка	dotyk@yandex.com	Release
3999439549	08-Apr-2008 10:49:30	Курсовые на заказ	vkitov_e@pkn.net	Release
3999440479	08-Apr-2008 10:55:40	Афиша-Лучшие: Презенты, Спектакли, Концерты	telalalido@usa.cable.com	Release
3999441283	08-Apr-2008 11:01:22	Бизнес-процессы - оптимизация, регламентация	yatro@holstark.com	Release
3999441933	08-Apr-2008 11:05:50	Re: Элитный преподаватель английского языка	susan19@verste@info.gamanetwork.com	Release
3999443128	08-Apr-2008 11:13:10	Срочно нужен офис? Закажите!	td1246@fvee.jp	Release
3999443468	08-Apr-2008 11:15:58	Кондиционеры. Доставка и монтаж оборудования	tiorema@bmail.com	Release
3999444783	08-Apr-2008 11:25:00	Срочная аудиторская проверка	smid@yudu@virginia.com	Release
3999447188	08-Apr-2008 11:40:51	Постановка белья для всех посетителей спальни и комфорта	f.seich@mp-patientonline.net	Release
3999447492	08-Apr-2008 11:42:57	БИЛЕТЫ хоккей России-Филадельфия,Баскетбол ЦСКА-Оптимизация,футбол Динамо-Спартак,SCORPIONS,Худож.Ниласас,Queen,KISS,Музеи Кремля, театр "Лешкин" и др.	dotyk@yandex.com	Release
3999447532	08-Apr-2008 11:43:10	Сопровождающие требования к предпроектной, проектной подготовке строительства	janapn.cid@homa.ru	Release
3999448617	08-Apr-2008 11:51:49	НАЛОГОВАЯ ОПТИМИЗАЦИЯ - ПРЕДЕЛЫ ДОПУСТИМОСТИ	huanxy@hmlinc.com	Release
3999449044	08-Apr-2008 11:55:08	Сопровождающие требования к предпроектной, проектной подготовке строительства	sgomaran@hodes.com	Release
3999449642	08-Apr-2008 11:59:19	Рекоменд. Главного бухгалтера	greshammon@huc-op.mta.ru	Release
3999451865	08-Apr-2008 12:14:15	Ташкентская статистика Российской Федерации	uzabing@bea.td.de	Release
3999452521	08-Apr-2008 12:20:39	Бронь и доставка билетов на спектакли/концерты	hater@post.russian.com	Release
3999453299	08-Apr-2008 12:26:57	Визы	lcannon191@mim3spring.net	Release
3999451897	08-Apr-2008 12:30:34	Таблицы	alfre@untybes@rsm.com	Release
3999455164	08-Apr-2008 12:42:21	(S7) Финансовая база	subhakar1213@shanta@bathf.com	Release
3999455811	08-Apr-2008 12:46:13	Предложения для ИНВЕСТИТОРОВ	wilne14@ic@yalla.com	Release
3999455895	08-Apr-2008 12:48:33	Отправить электронно	lunty@orange@bryce-wanted.com	Release
3999457318	08-Apr-2008 12:59:54	Полностью новые пакеты от производителя	seorsedyang@postevrindemam.biz	Release
3999457499	08-Apr-2008 13:00:54	Торговые предложения	wandy67@ang_bu@china.co.za	Release

пуск | eSafe SPAM | 100%

УПРАВЛЕНИЕ И МОНИТОРИНГ



ПОДГОТОВКА ОТЧЕТОВ

# eSafe® Security Center (dashboard)



# eSafe® Security Center (real time report)

The screenshot displays the eSafe Security Center interface in demo mode. The top navigation bar includes tabs for Web, Mail, APPs, System, Quarantine, and DLP. The main content area shows a report titled "All Violations" for the period of 03.02.2011. The report is a table with columns for Date, Time, Machine name, Method, Event, Subject, Size, Source, Sender, Recipients, User, Profile, Policy, Details, and ID. The table lists numerous spam-tagged messages with subjects such as "Hil :) You have a few second fo...", "samsung blackjack specs", "Funny Animals 5...", "Cheap watches and accessories...", "Stand up and be happy!", "Sexual", "Exquisite Replica", "Causing an erection", "Federal Tax Rap for Girls Gone...", "Italian tourist catches in on Cruise...", "Viagra cures", "Missing Pig Found In Back Of St...", "Purosubatweiny Phil predicts earl...", "Authentic leather shoes at rock...", "Keep traction", "Get all your necessary ED pills a...", "Re:", "Chopard and Hermes Watches", "Stimulation", "Professor Allegedly Shows Expi...", "Jacob & Co. Watches", "Washington woman who registe...", "Lowest price worldwide", "Get cheaper Gals today at onlin...", "Professor Allegedly Shows Expi...", "Mich. farm has maze cut into cor...", "Think of your future", "China seeks profit from panda poo", "Professor Allegedly Shows Expi...", "Respective Libidos", "No Impotence", "Our shop on-line health is the m...", "Wisdom in relations", "replica Watches! roles, patek ph...", "Authentic leather shoes at rock...", "Authentic leather shoes at rock...", "Watches", "FruityLoops Studio 8 101, Edition", "Luxury shoes at affordable prices", "Sabafactory sexual intercourse", "fashionable replica watches", "\$69.95 Price for Viagra (Sildenafil)", "Forget about world crisis", "Erectile", "Forget about world crisis", "Replica Watches", "Buy a knock off, and you will be...", "Marry fortune!", "Your doctor", "An overview of pumps, pills", "Save on Generic Meds! Xanax #...", and "Coin Forgeries Scammed Ancient...".

10.8.1.13 - eSafe Security Center (Demo mode) v. 8.6.006.0  
Logged in user: Admin System Administrator  
Access permissions: System Administrator  
4Eye Login  
Period: 03.02.2011  
Report: All Violations  
Equals  
Date Time Machine name Method Event Subject Size Source Sender Recipients User Profile Policy Details ID  
2015-04-00:04:50 danny-net8 In Spam tagged Hil :) You have a few second fo... 2116 10.50... FJTLGH... QNFDP... QNFDP... Msg #1... 8127570  
2015-04-00:04:50 danny-net8 In Spam tagged samsung blackjack specs 1139 10.50... FJTLGH... QNFDP... QNFDP... Msg #1... 8127569  
2015-04-00:04:50 danny-net8 In Spam tagged Funny Animals 5... 3074 10.50... FJTLGH... QNFDP... QNFDP... Msg #1... 00:04:50  
2015-04-00:04:50 danny-net8 In Spam tagged Cheap watches and accessories... 1892 10.50... FJTLGH... QNFDP... QNFDP... Msg #1... 8127567  
2015-04-00:04:50 danny-net8 In Spam tagged Stand up and be happy! 1006 10.50... FJTLGH... QNFDP... QNFDP... Msg #1... 8127566  
2015-04-00:04:51 danny-net8 In Spam tagged Sexual 2220 10.50... FJTLGH... QNFDP... QNFDP... Subject... 8127583  
2015-04-00:04:51 danny-net8 In Spam tagged Exquisite Replica 2650 10.50... FJTLGH... QNFDP... QNFDP... Msg #1... 8127571  
2015-04-00:04:51 danny-net8 In Spam tagged Causing an erection 2600 10.50... FJTLGH... QNFDP... QNFDP... Msg #1... 8127578  
2015-04-00:04:51 danny-net8 In Spam tagged Federal Tax Rap for Girls Gone ... 3087 10.50... FJTLGH... QNFDP... QNFDP... Msg #1... 8127576  
2015-04-00:04:51 danny-net8 In Spam tagged Italian tourist catches in on Cruise... 3109 10.50... FJTLGH... QNFDP... QNFDP... Msg #1... 8127582  
2015-04-00:22:06 danny-net8 In Spam tagged Viagra cures 2485 10.50... FJTLGH... QNFDP... QNFDP... Subject... 8137791  
2015-04-00:22:06 danny-net8 In Spam tagged Missing Pig Found In Back Of St... 3192 10.50... FJTLGH... QNFDP... QNFDP... Msg #1... 8140981  
2015-04-00:22:06 danny-net8 In Spam tagged Purosubatweiny Phil predicts earl... 3150 10.50... FJTLGH... QNFDP... QNFDP... Body C... 8137793  
2015-04-00:22:06 danny-net8 In Spam tagged Authentic leather shoes at rock... 2149 10.50... FJTLGH... QNFDP... QNFDP... Msg #1... 8140980  
2015-04-00:22:06 danny-net8 In Spam tagged Keep traction 2114 10.50... FJTLGH... QNFDP... QNFDP... Msg #1... 8140982  
2015-04-00:22:06 danny-net8 In Spam tagged Get all your necessary ED pills a... 2480 10.50... FJTLGH... QNFDP... QNFDP... Msg #1... 8140979  
2015-04-00:22:06 danny-net8 In Spam tagged Re: 5227 10.50... FJTLGH... QNFDP... QNFDP... Msg #1... 8137792  
2015-04-00:22:07 danny-net8 In Spam tagged Chopard and Hermes Watches 2931 10.50... FJTLGH... QNFDP... QNFDP... Msg #1... 8140985  
2015-04-00:22:07 danny-net8 In Spam tagged Professor Allegedly Shows Expi... 3162 10.50... FJTLGH... QNFDP... QNFDP... Msg #1... 8140984  
2015-04-00:22:07 danny-net8 In Spam tagged Jacob & Co. Watches 1861 10.50... FJTLGH... QNFDP... QNFDP... Msg #1... 8140983  
2015-04-00:22:08 danny-net8 In Spam tagged Washington woman who registe... 3210 10.50... FJTLGH... QNFDP... QNFDP... Msg #1... 8140987  
2015-04-00:40:17 danny-net8 In Spam tagged Lowest price worldwide 2275 10.50... FJTLGH... QNFDP... QNFDP... Msg #1... 8152111  
2015-04-00:40:19 danny-net8 In Spam tagged Get cheaper Gals today at onlin... 2751 10.50... FJTLGH... QNFDP... QNFDP... Body #... 8152120  
2015-04-00:40:19 danny-net8 In Spam tagged Professor Allegedly Shows Expi... 6288 10.50... FJTLGH... QNFDP... QNFDP... Msg #... 8152121  
2015-04-00:40:19 danny-net8 In Spam tagged Mich. farm has maze cut into cor... 3068 10.50... FJTLGH... QNFDP... QNFDP... Msg #... 8152124  
2015-04-00:40:19 danny-net8 In Spam tagged Think of your future 989 10.50... FJTLGH... QNFDP... QNFDP... Msg #... 8152122  
2015-04-00:40:19 danny-net8 In Spam tagged China seeks profit from panda poo 3076 10.50... FJTLGH... QNFDP... QNFDP... Msg #... 8152123  
2015-04-00:40:19 danny-net8 In Spam tagged Professor Allegedly Shows Expi... 6286 10.50... FJTLGH... QNFDP... QNFDP... Msg #... 8152125  
2015-04-00:40:20 danny-net8 In Spam tagged Respective Libidos 2410 10.50... FJTLGH... QNFDP... QNFDP... Msg #... 8152130  
2015-04-00:40:20 danny-net8 In Spam tagged No Impotence 2333 10.50... FJTLGH... QNFDP... QNFDP... Msg #... 8152129  
2015-04-00:40:20 danny-net8 In Spam tagged Our shop on-line health is the m... 2642 10.50... FJTLGH... QNFDP... QNFDP... Msg #... 8152135  
2015-04-00:40:20 danny-net8 In Spam tagged Wisdom in relations 995 10.50... FJTLGH... QNFDP... QNFDP... Msg #... 8152131  
2015-04-00:40:20 danny-net8 In Spam tagged replica Watches! roles, patek ph... 1047 10.50... FJTLGH... QNFDP... QNFDP... Msg #... 8152126  
2015-04-00:40:20 danny-net8 In Spam tagged Authentic leather shoes at rock... 2124 10.50... FJTLGH... QNFDP... QNFDP... Msg #... 8152132  
2015-04-00:40:20 danny-net8 In Spam tagged Authentic leather shoes at rock ... 2638 10.50... FJTLGH... QNFDP... QNFDP... Msg #... 8152134  
2015-04-00:40:20 danny-net8 In Spam tagged Watches 2605 10.50... FJTLGH... QNFDP... QNFDP... Msg #... 8152133  
2015-04-00:40:20 danny-net8 In Spam tagged FruityLoops Studio 8 101, Edition 2077 10.50... FJTLGH... QNFDP... QNFDP... Msg #... 8152127  
2015-04-00:40:20 danny-net8 In Spam tagged Luxury shoes at affordable prices 2468 10.50... FJTLGH... QNFDP... QNFDP... Msg #... 8152128  
2015-04-00:40:21 danny-net8 In Spam tagged Sabafactory sexual intercourse 2903 10.50... FJTLGH... QNFDP... QNFDP... Subject... 8152137  
2015-04-00:40:21 danny-net8 In Spam tagged fashionable replica watches 1115 10.50... FJTLGH... QNFDP... QNFDP... Msg #... 8152136  
2015-04-00:40:22 danny-net8 In Spam tagged \$69.95 Price for Viagra (Sildenafil) 1153 10.50... FJTLGH... QNFDP... QNFDP... Subject... 8152139  
2015-04-00:40:22 danny-net8 In Spam tagged Forget about world crisis 983 10.50... FJTLGH... QNFDP... QNFDP... Msg #... 8152144  
2015-04-00:40:22 danny-net8 In Spam tagged Erectile 2898 10.50... FJTLGH... QNFDP... QNFDP... Msg #... 8152143  
2015-04-00:40:22 danny-net8 In Spam tagged Forget about world crisis 972 10.50... FJTLGH... QNFDP... QNFDP... Msg #... 8152138  
2015-04-00:40:22 danny-net8 In Spam tagged Replica Watches 2933 10.50... FJTLGH... QNFDP... QNFDP... Msg #... 8152141  
2015-04-00:40:22 danny-net8 In Spam tagged Buy a knock off, and you will be ... 2053 10.50... FJTLGH... QNFDP... QNFDP... Msg #... 8152142  
2015-04-00:40:22 danny-net8 In Spam tagged Marry fortune! 984 10.50... FJTLGH... QNFDP... QNFDP... Msg #... 8152140  
2015-04-00:40:23 danny-net8 In Spam tagged Your doctor 2626 10.50... FJTLGH... QNFDP... QNFDP... Body #... 8152148  
2015-04-00:40:23 danny-net8 In Spam tagged An overview of pumps, pills 2039 10.50... FJTLGH... QNFDP... QNFDP... Msg #... 8152149  
2015-04-00:40:23 danny-net8 In Spam tagged Save on Generic Meds! Xanax # ... 1523 10.50... FJTLGH... QNFDP... QNFDP... Subject... 8152145  
2015-04-00:40:23 danny-net8 In Spam tagged Coin Forgeries Scammed Ancient... 3020 10.50... FJTLGH... QNFDP... QNFDP... Msg #... 8152147  
Page 1 / 2 Page length: 2000 Showing lines #1 - 2000 of 3597 lines to show.

CPU: 96% Memory: 46% HD: 267/976Gb

nyck | Dashboard | Microsoft... | 10.8.1.13... | Security... | Kasan... | dashboard... | 15:39

# eSafe<sup>®</sup> Reporter

- Содержит 240 predefined report forms:
  - Reports in real time
  - Detailed reports
  - Analytical reports
  - Individual reports
- Report formats: HTML, PDF, XLS
- Report generation and email distribution according to schedule



СЦЕНАРИИ УСТАНОВКИ

**eSafe**

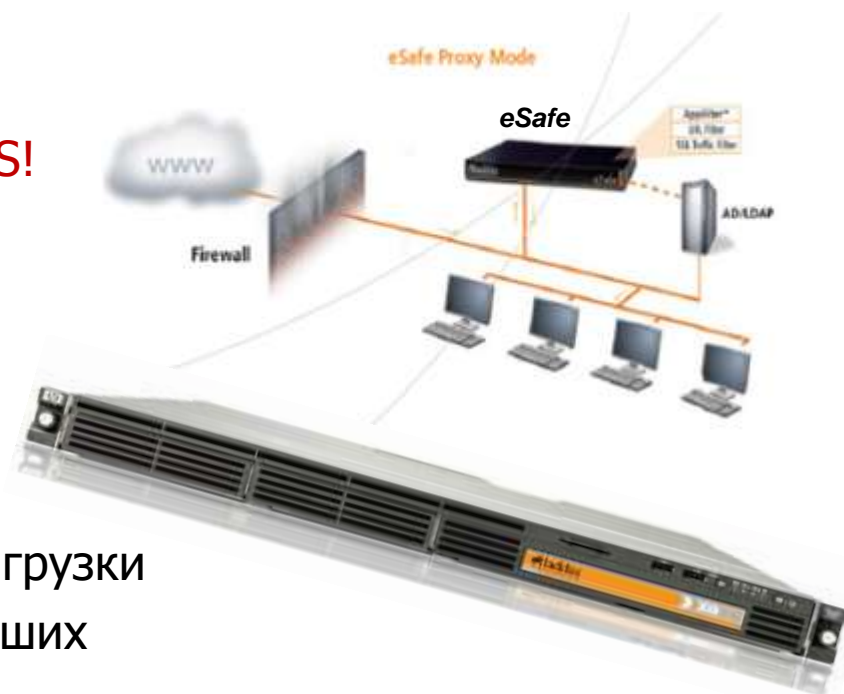
**SmartSuite**

ПРОИЗВОДИТЕЛЬНОСТЬ

МАСШТАБИРУЕМОСТЬ

# Впишемся в любую инфраструктуру !!!

- Поддерживаемые сценарии
  - Inline, Мост, Маршрутизатор,
  - !Прозрачное сканирование HTTP/HTTPS!  
Прокси (FWD, Full)
- Используемые платформы
  - Virtual appliance (VACD)
  - VMWare
  - Специальные аппаратные серверы
- Отказоустойчивость и балансировка нагрузки
  - Кластеры с использованием простейших концентраторов или коммутаторов
  - Кластеры с использованием балансировщиков нагрузки 3<sup>их</sup> изготовителей
  - Кластеры с использованием by-pass карт (штатная компонента каждого сервера)



# Конкурирующие решения

## На корпоративном сегменте

- Blue Coat Systems
- Cisco Systems
- McAfee (SC+)
- Websense

## На сегменте решений операторского класса

- Blue Coat Systems
- AdaptiveMobile
- McAfee (SC+)
- Zscaler
- Optenet
- Websense

# Тестирование решений

- Один вендор
  - Техническое задание
  - Согласованная методика тестирования
  - Протокол тестирования
  - Принятие решения
- Конкурентное тестирование
  - Техническое задание
  - Согласованная методика конкурентного тестирования
  - Вендорский контроль за процессом тестирования
  - Принятие решения



Спасибо за внимание!

**eSafe**  
**SmartSuite**

The logo for SmartSuite features the word "SmartSuite" in a bold, black, sans-serif font. The letter "a" in "Smart" is highlighted in red and has a small sunburst graphic above it. A thin vertical line extends downwards from the bottom of the red "a", ending in a small circle.

Максим Чирков

[dealer@aladdin-rd.ru](mailto:dealer@aladdin-rd.ru)

[www.aladdin-rd.ru](http://www.aladdin-rd.ru)