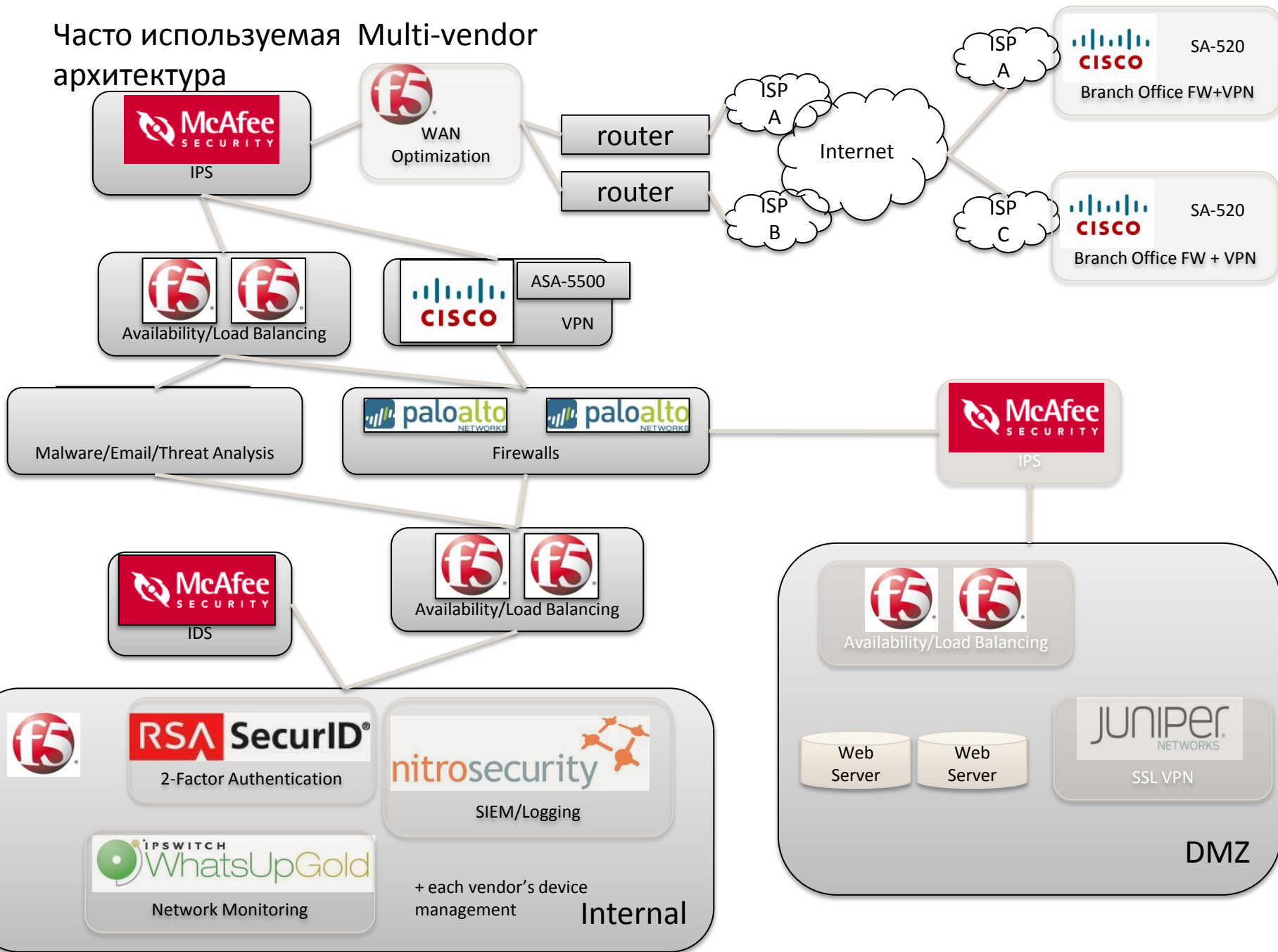


# Новые возможности бизнеса. Комплекс решений Stonesoft

# Часто используемая Multi-vendor архитектура

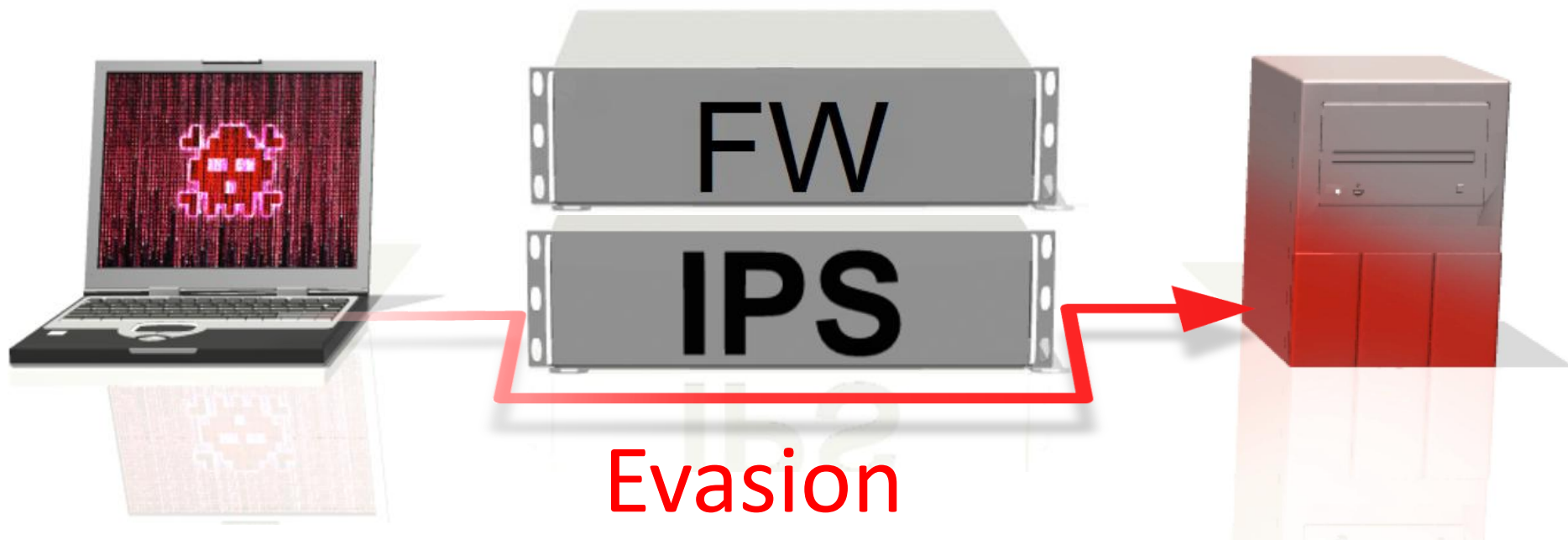


# Эффективность



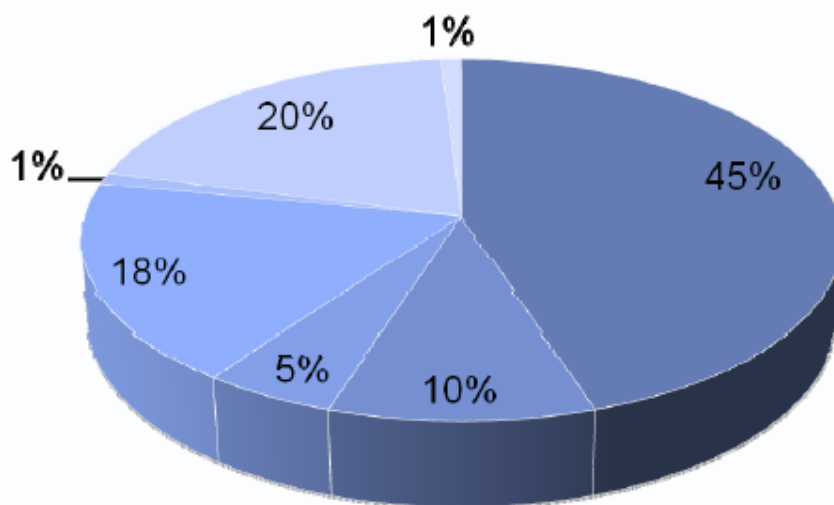
— это свойство системы выполнять поставленную цель в заданных условиях использования и с определенным качеством. Показатели эффективности характеризуют степень приспособленности системы к выполнению поставленных перед ней задач и являются обобщающими показателями оптимальности ее функционирования.

# Уверены, что защищены?



# Безопасность ДБО способов атак очень много

- Хакерские атаки на собственно систему ДБО (SQL injections..).
- Троянские программы - воровство паролей и криптографических ключей
- Трояны – перехват нажатий клавиатуры , снимки экрана при каждом нажатии, и др....
- Пресловутый универсальный троян Ibank
- Установка удаленного канала в рабочей станции
- Сбор данных в том числе остатки информации по работе с ДБО ( кеш , куки, файлы в папках temp ..... )
- Man in the middle ( работа через посредника) , Man in the



- Атака на ключевой контейнер - 45% (тенденция к снижению)
- Физическая кража носителя - 10%
- Атака на ключ в оперативной памяти - 5%
- Удаленное управление - 18% (тенденция к росту)
- Подмена документа - 1%
- Фишинг - 20%
- Атаки на канал - менее 1%

(1) На основании данных предоставленных производителями решений для ДБО и средств защиты

# Как противостоять?

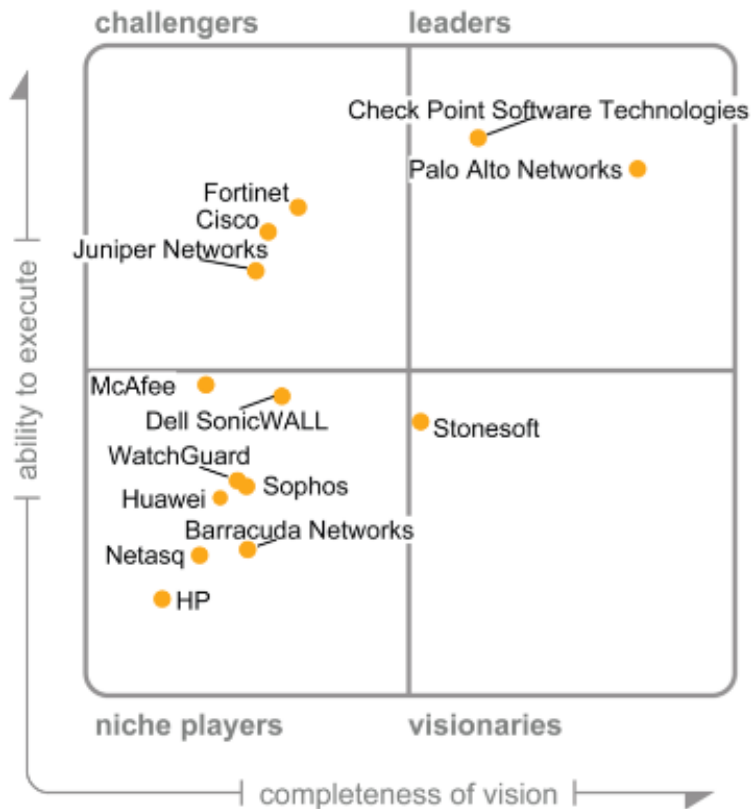
Требования  
безопасности  
( более 100  
пунктов)



Функционал  
(около 50  
пунктов)

# Безопасность можно измерить?

Figure 1. Magic Quadrant for Enterprise Network Firewalls



As of February 2013

Source: Gartner (February 2013)



# Сколько теряем?

Ежегодные потери  
= €200-250К



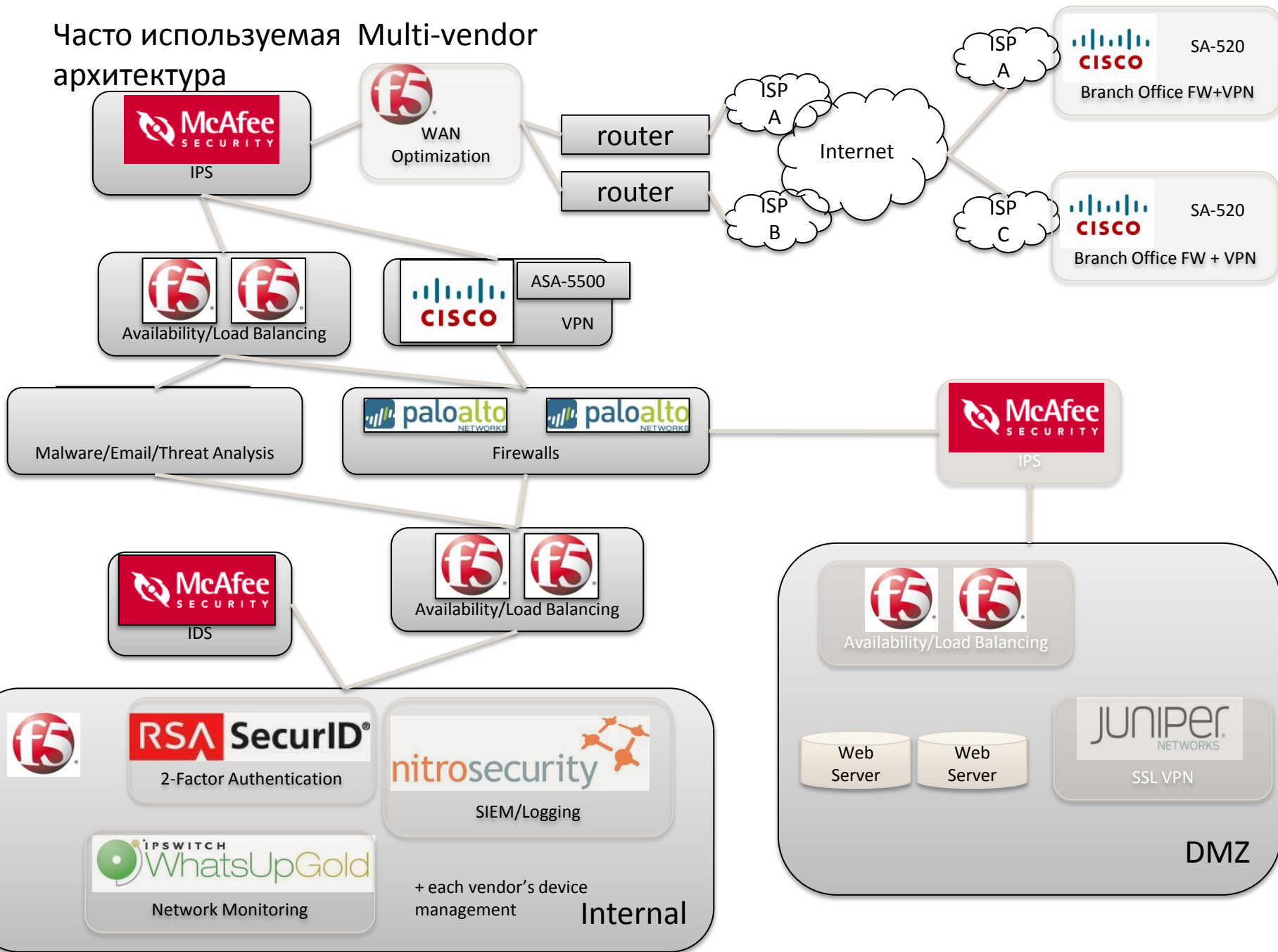
Потери за 3 года=  
€600-800К



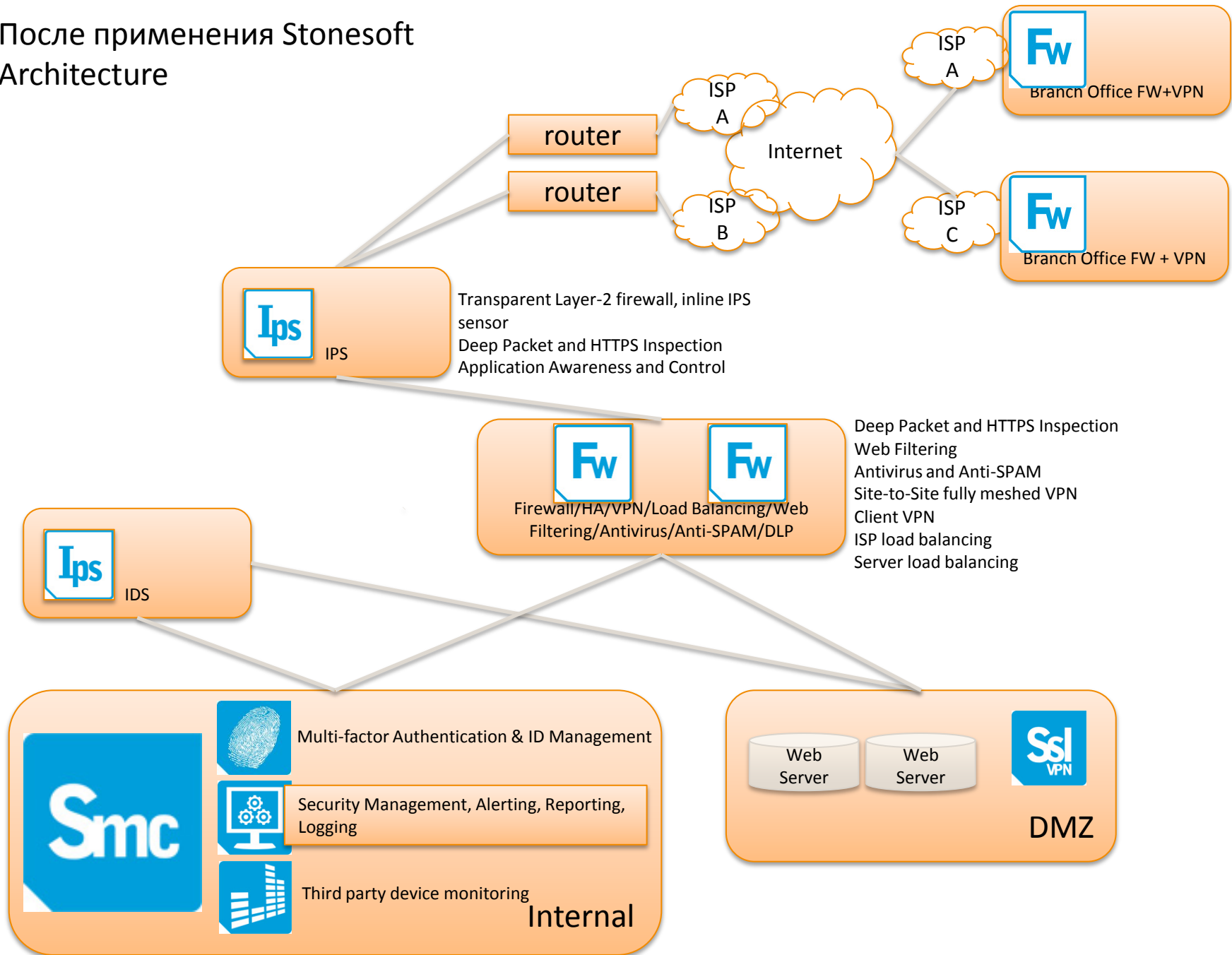
- Расходы на расследование
- Расходы на возмещение
- Расходы на восстановление работоспособности
- Потери репутации

## Сколько сможем сберечь?

# Часто используемая Multi-vendor архитектура




# После применения Stonesoft Architecture



# Самый низкий TCO на рынке

- Проактивный контроль = сильно снижает расходы администрирования
- Always-on технологии подключения = уменьшает расходы на оборудование, инфраструктуру и связь ( коммуникации )
- Множество встроенных просто настраиваемых механизмов защиты

	Stonesoft Capability	Cost Saving
Rules & Policy Management	Proactive Control →	Up to 50%
Remote Device Management	Proactive Control →	Up to 75%
Communications Costs, BGP, MPLS	Multi-Link Communication →	Eliminates Cost
High Availability, Load Balancing, Seamless Failover	Drop-in Active Clustering →	Eliminates hardware
Auditing & Compliance Reporting	Interactive Reporting →	Up to 25%



# Остановимся на сетевой составляющей безопасности

КАК СОВМЕСТИТЬ БЕЗОПАСНОСТЬ И  
ЭФФЕКТИВНОСТЬ

---

# Комплексная сетевая защита мобильного банкинга

- Защита собственно ресурса мобильного банкинга от новейших атак
- Строгая, двухфакторная аутентификация и авторизация
- Контроль удаленного устройства при подключении (безопасно оно или нет ?)
- Шифрование передаваемой информации (сертифицированные средства?)
- Исключение возможности «захвата» удаленного устройства в момент доступа.
- Удаление следов сеанса работы на удаленном устройстве ( чтобы исключить воровство данных)
- Динамическая блокировка устройства в случае несанкционированной активности во время сеанса

...

# Компоненты платформы StoneGate



## StoneGate SMC :

- унифицированная система управления и мониторинга
- анализ и обработка событий безопасности, в.т.ч. от устройств третьих производителей



## StoneGate Firewall/VPN :

- Межсетевой экран с технологиями кластеризации и Multilink (отказоустойчивые подключения к любым сетям);
- Высокоотказоустойчивое решение VPN Crypto Pro + отказоустойчивое подключение клиента;
- Антивирусный шлюз + веб-фильтрация;



## StoneGate IPS :

- Высокая точность обнаружения вторжений и надежная защита от атак
- Корреляция событий;



## Уникальное решение StoneGate SSL VPN:

- Поддержка NAC, SSO
- 15 методов аутентификации клиента;



## Сервер аутентификации **Authentication server**

Кроме того: Virtual Firewall, IPS, SSL VPN – защита в виртуальной среде

# StoneGate SSL VPN

- **Безопасный доступ с любых устройств**
  - Встроенная двух факторная аутентификация
  - Интеграция с любыми каталогами и др. ( AD, LDAP, Oracle)
  - Поддержка single sign-on & ID federation
- **Интегрированное управление угрозами**
  - Только доверенные соединения .
  - Анализ целостности и безопасности устройства
  - Удаление «следов» работы пользователя.
- **Гранулированное и гибкое управление доступом**
  - Авторизация на уровне приложений
  - Концепция least privileges – только то что разрешено





---

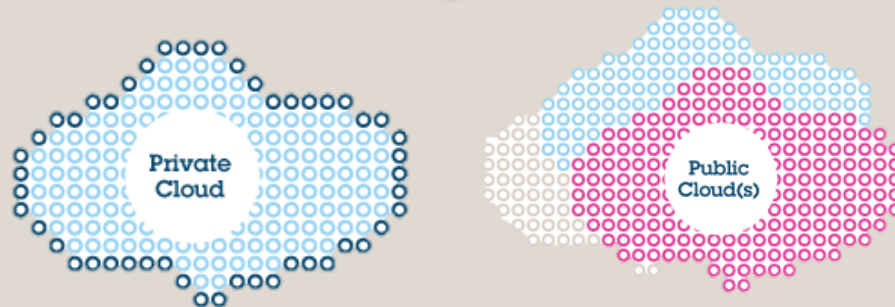
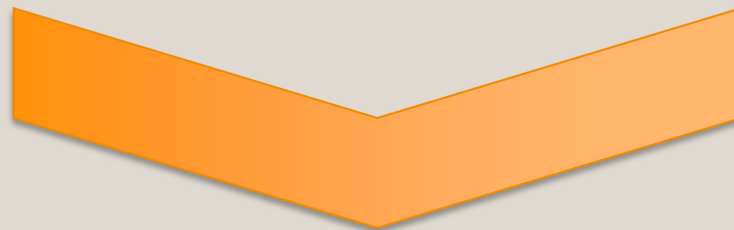
# Создан для людей

- Стратегия управления доступом, основанная на поведении > **удобство использования гарантировано технологией**
- Гибкие критерии доступа > **вы сами выбираете условия в каждой ситуации**
- Динамическая безопасность > **вы сами контролируете приложения, в зависимости от заданных критериев**



# Универсальный удаленный доступ – почему?

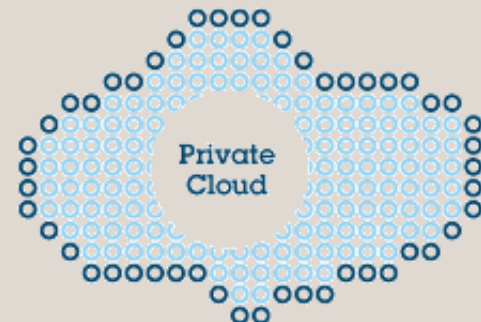
- Любое устройство отовсюду и в любое время – дает свободу
- Не нужно привыкать к новому ПО – дает простоту
- Single Sign On для приложений и ресурсов – повышает производительность труда



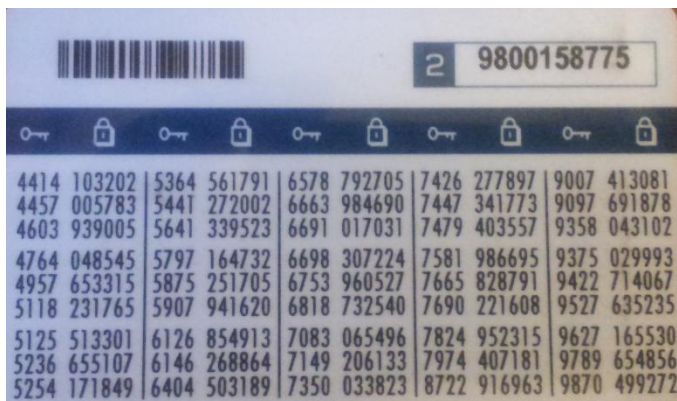
---

# Соответствие политикам ИБ?

- Оценка всего профиля, а не только проверка прав!
- Доверие всей ситуации, а не только пользователю!
- Комплексный подход



# Аутентификацию можно упорядочить ?

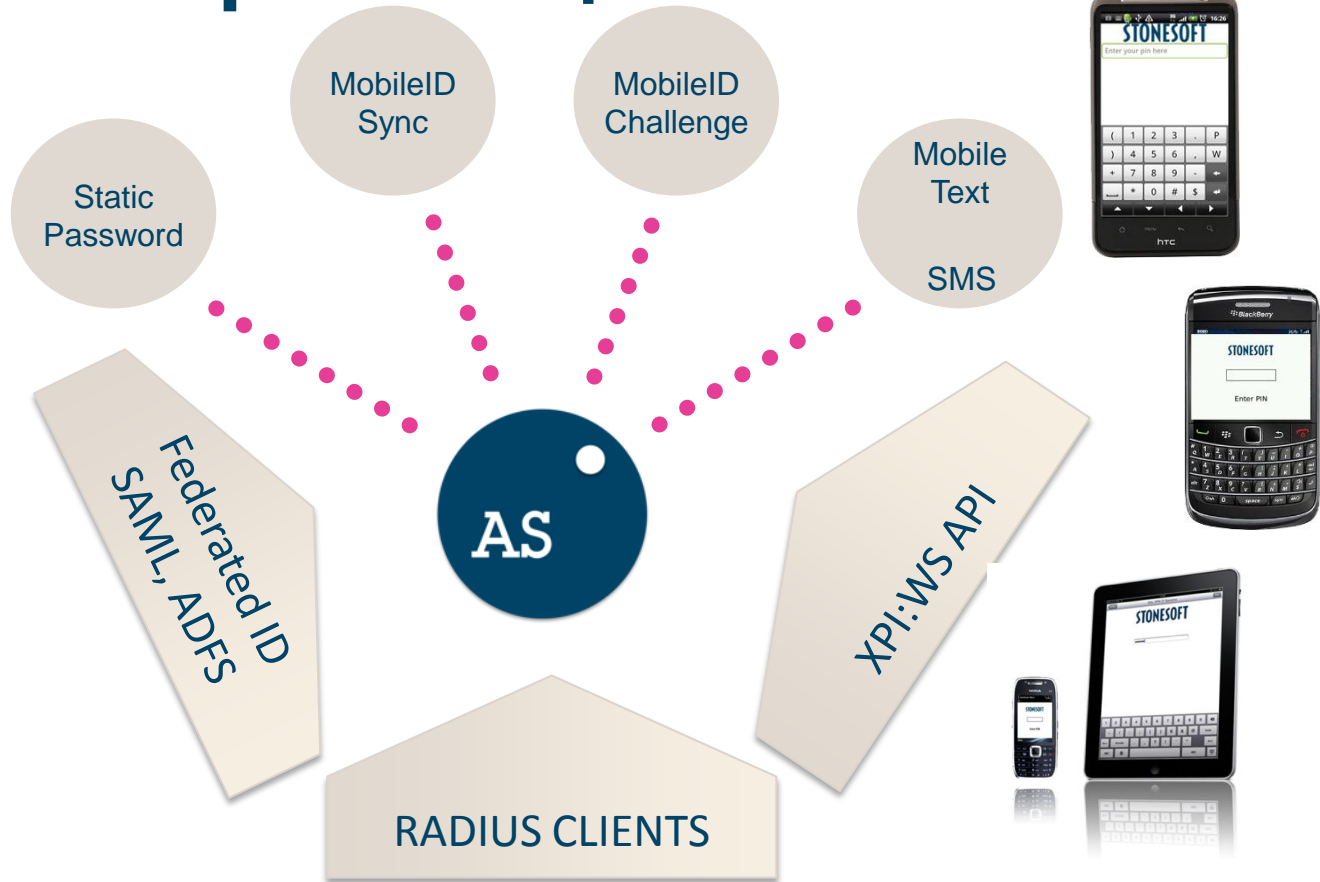
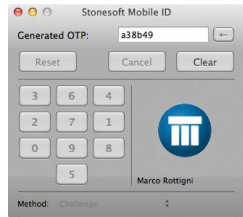


# Надежная аутентификация через SSL

- 6 включенных методов
- Поддержка до 15 внешних методов
- Возможность комбинирования методов аутентификации



# Интеграция сервисов аутентификации



# Полная... ИЗОЛЯЦИЯ

## 2. Авторизация с автоматическим переносом сессии

Аутентификация и авторизация на вход в банк (оформление меняется под Заказчика)



Пользователь «как обычно» работает с сайтом.

## 1. Доступ на сайт (через SSL)



Загрузка и активация модуля безопасности



## 4. Загрузка защищенного приложения/браузера

Рабочее место клиента

Активация агента (или модуля) быть выполнено до начала

Trojans

Keyloggers

Spyware

MitB Интернет-банк

---

# Удаление следов доступа

- Удаляет историю страниц браузера
- Прозрачный (автоматический) режим или интерактивный
- Удаляет временные (temporary) файлы
- Полностью настраиваются

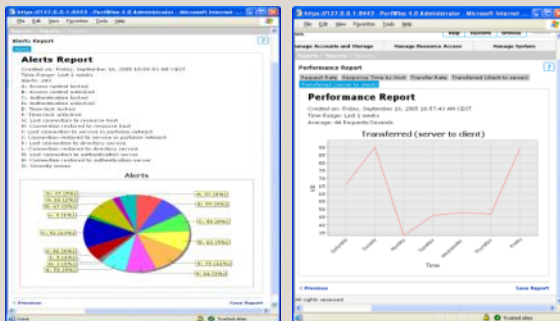




# Управление журналами, отчеты, оповещения и аудит

На устройстве

С помощью SMC



This composite image illustrates the management interface. On the left, a tree view shows 'SSL VPN Gateways' with a context menu open over 'HQSVPN', listing options like 'Properties...', 'New', 'Copy', 'Delete', and 'Monitoring'. In the center, a 'Data Options: Configuration Monitoring' window displays a detailed log table with columns for 'Auth. Method', 'Address...', 'Auth. User', and 'Information Message'. The table lists various authentication events such as 'User authenticated', 'RADIUS client makes access', and 'User entered wrong PIN'. On the right, a 'StoneGate' monitoring window shows several charts: 'Successful Authentications by User' (a pie chart), 'Failed Authentications by User' (a pie chart), 'Authentication Method Usage' (a pie chart), and 'Authentication Methods over Time' (a line graph).



# «Приятные мелочи»

# Технологическое партнерство



Security collaboration



Solution partners



# ПРОВЕРЕННЫЕ РЕШЕНИЯ...

# Сертификации



ФСТЭК  
ФСБ



Подтверждение  
эффективности  
решений  
StoneSoft



---

# Сертификация ФСТЭК и ФСБ

- SSL VPN сертифицирован ФСТЭК России:
- Шлюз защиты удаленного доступа StoneGate SSL\*  
—  
3 класс МЭ (распределенный), 4 класс НДВ и для применения ИСПДн 1 класса и АС до 1Г вкл.
- В составе сертифицирована система многофакторной аутентификации
- и ФСБ России:
  - Классы КС1 – КС2!
  - Поддерживаются криптопровайдеры (прописаны в сертификатах): Криптопро, Валидата ;
  - Встречная работа VipNet CSP, Signal Com

# Цифры и факты

- Компания основана в 1990
- Более 20 лет опыта решений по корпоративной безопасности
- Акции котируются на бирже с 1999 (NASDAQ OMX: SFT1V)
- Штаб-квартира в Хельсинки, Финляндия и в Атланте, США
- Региональные офисы в 18 странах на 4 континентах
- R&D в 3 странах Европы: Финляндия, Франция, Польша
- # 1 Европейский вендор по инф. безопасности
- Внедрения в 100 странах, на 5 континентах
- Более 4500 заказчиков
- Индекс удовлетворенности заказчиков 95%.
- С июня 2013 является частью McAfee Group



# Спасибо!

**Леонид Дмитришен**  
**+7 905 719 49 12**  
**leonid.dmitrishen@stonesoft.com**  
**+7 495 787 99 36**