STONESOFT

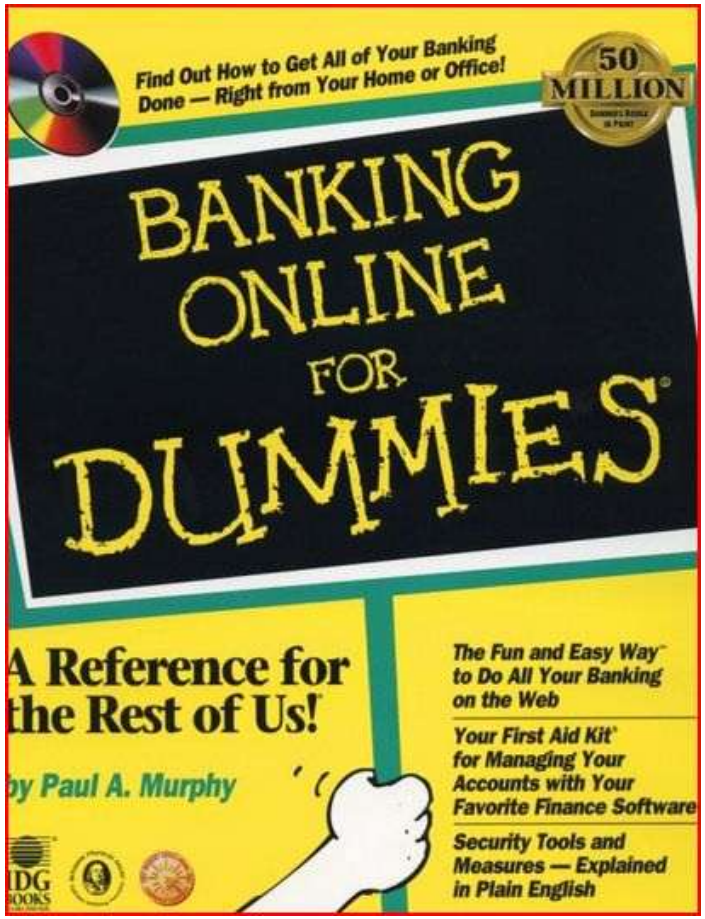
Защищенное ДБО

Миф или реальность?

Карагедян Карен, директор по продажам
Stonesoft в России, СНГ и странах Балтии

Содержание

- О компании Stonesoft
- ДБО: виды и тенденции развития
- Безопасность или удобство?
- Как защитить?
- Защита корпоративных клиентов
- Вопросы и ответы



Кратко о Stonesoft

Global Company

- Международная компания, занимающаяся безопасностью, создана в 1990 году
- Акции размещены на бирже в Helsinki, Финляндия (HEX)
- Головной офис в Helsinki, Финляндия

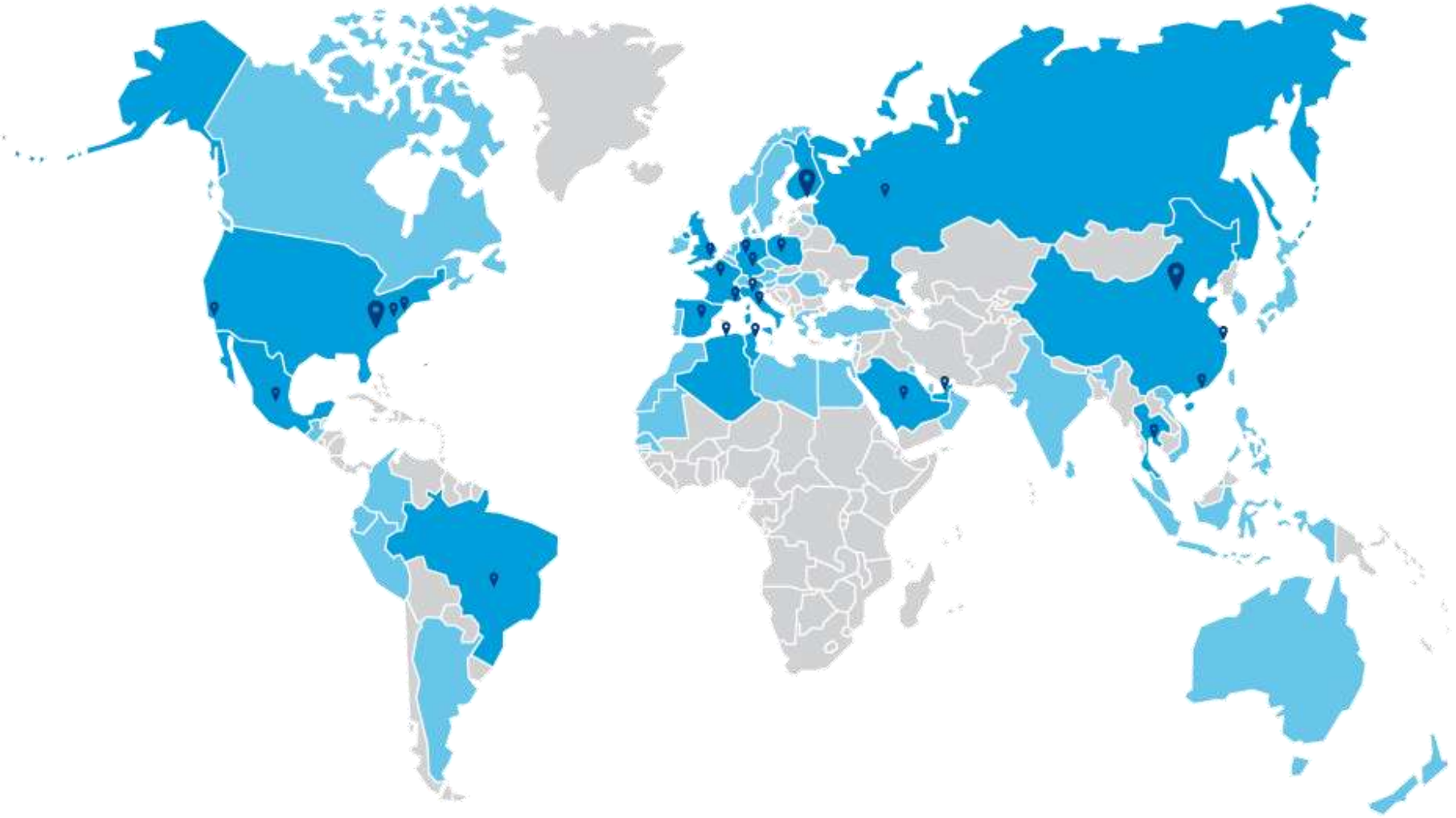
Customer Focus

- Офисы в USA, EMEA и Asia
- Поддержка 24/7
- Пользователи в более, чем 80 странах
- Фокусируется на организациях, нуждающихся во многофункциональных системах информационной безопасности, а также на непрерывности бизнеса

Innovation

- Инновационная фирма предоставляющая интегрированные системы информационной безопасности и непрерывности бизнеса
- R&D центры в Франции и Финляндии, Польше. Обладает большим количеством патентов в области безопасности (38 зарегистрированы и более 20 на рассмотрении)

Stonesoft: Global Innovator



Этапы развития Stonesoft

2010
- **AET**
- Federated ID , Authentication

2009
- **Управление событиями любых устройств**
- SSL инспекция

2008
- Виртуальный аплайнс для VMware

2004
- Интегрированный StoneGate Management Center

2002
- виртуальный Firewall/VPN для **IBM ® zSeries®**

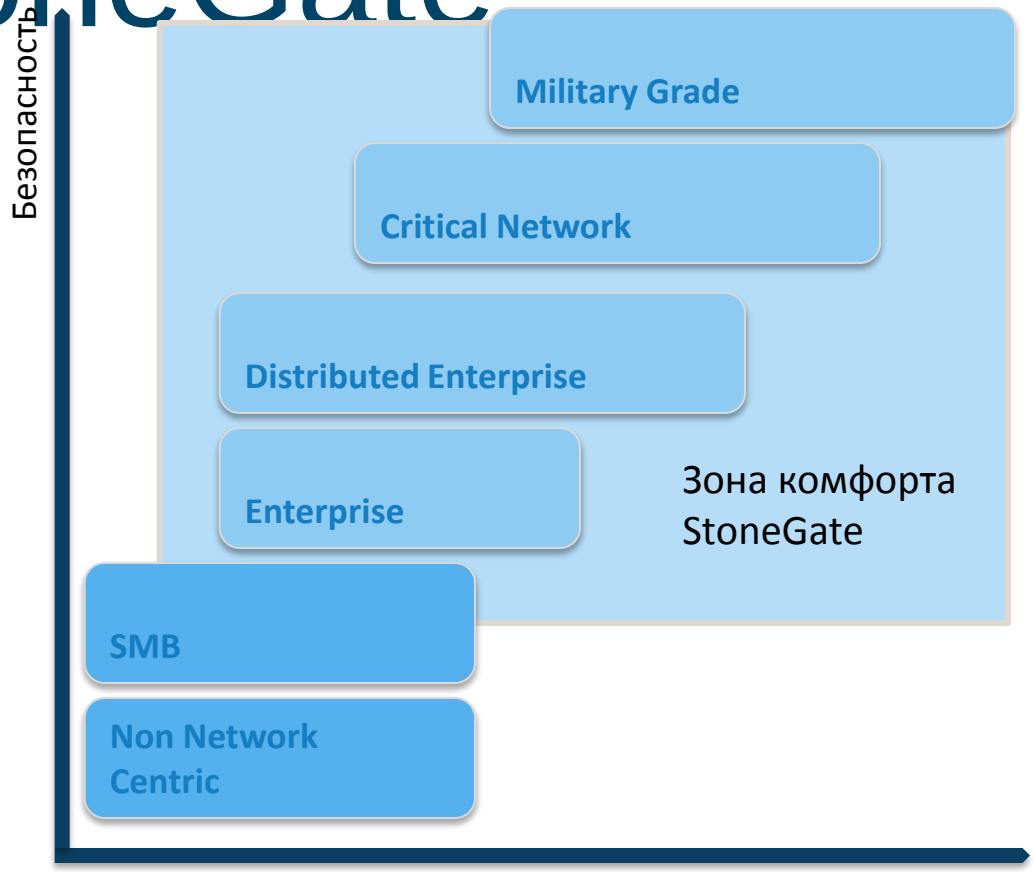
2001
- StoneGate™ **High-Availability Firewall/VPN**

1999
- StoneBeat™ High Availability становится **лидером рынка**

1994
- Выход продукта StoneBeat **для телекоммуникационных компаний и банков**

1990 ⟹ **2011**

Зона комфорта StoneGate



•Военные ведомства
•Государственные структуры

•Финансовые организации
•Производство (нефть , газ, промышленность…)
•Здравоохранение

•Телекоммуникации
•Сервисы и сети продаж
•Образование

Где безопасность не опция

Защита ДБО – это необходимо?

- Мобильный банк
- Интернет-банк
- Телефонный банк
- Киоск самообслуживания
- Банкомат

- Новые технологии доступа:
  - WiFi, WiMAX, 3G, LTE…
- Новые мобильные устройства:
  - планшеты, нетбуки,смартфоны, коммуникаторы...
- Новые угрозы безопасности:
  - Специфические атаки на банк-клиент и т.п.
  - Вирусы, трояны (malware),
  - Имперсонализация, кража данных с устройств
- Периметр защиты «размыт»
  - Ad-hoc Mobility (SMS, IM) → Structured Mobility (DB) → Optimized Mobility, попытки перехода в «облака» …

Атаки хакеров

Кто скрывается за кражей данных?

- 74% - внешние источники
- 20% - инсайдеры
- 32% - «так наз[illegible]аемые» бизнес-партнеры
- 39% - комбинация участников

91% всех компрометаций связаны с работой ОПГ

Как происходят кражи?

- 67% способствовали значительные ошибки
- [illegible]4% способствовала хакерская [illegible]ктивность
- [illegible]пользовали malware
- [illegible]мели в составе [illegible]вление привилегиями
- [illegible]ошли путем физических

STONESOFT

"2009 Data Breach Investigations Report", Verizon Business

Больше пользователей -выше

Атаки на ДБО

- Наиболее часто атакуют клиента чтобы у него украсть ключевой контейнер или пароль (до 45 % всех атак)
- Фишинг до 20 %
- Удаленное управление (…) 17 – 19 %
- Физическая кража носителей и физический доступ (до 9 %)
- Атака на СКЗИ и ключ в оперативной памяти- 5%
- Подмена документов в оперативной памяти – 1 %
- Атака на канал - 1 %

Многообразие систем защиты

- Логин, пароль, ключевые файлы
- шифрование канала связи (SSL)
- Аутентификация и авторизация транзакций по сертификатам ,
- challenge процедуры (вопрос – ответ);
- пароли по СМС;
- использование Transaction Authorisation Numbers (TAN)
- Сетевая защита (WAF, IPS, FW, AV ….)
- «антифрод»

А на деле бывает и так ☺

Типичная защита ДБО

- Клиентское средство не защищено никак – есть только рекомендации на сайте ….
- Браузер подключается к сайту (в общем то это часть ДБО) используя SSL соединение. Клиент аутентифицируется по сертификату с флешки (в лучшем случае)
- ДБО защищено Firewall в котором закрыты все порты кроме 80 и 443 (ну или назначенного).
- Иногда используется система типа «Антифрод» за которую отвечает департамент IT в лучшем случае…

Проблемы со стороны банка

- Банк не знает кто подключился – только аутентификация клиента говорит что это вроде он .
- Если есть подозрительные транзакции - они ставятся на холд – что неудобно для клиента .
- В случае кражи ключа у клиента трудно сразу это понять и заблокировать – в результате списание средств…
- Нет согласия между подразделением ИБ управляющих сетевыми средствами безопасности и другими – которые следят за транзакциями …

Проблемы со стороны банка

- Все усугубляется DDoS атаками на WEB-ресурсы - а они должны быть доступными
- а также и другие атаки на ресурсы позволяющие например использовать SQL инъекции и другие атаки….
- Последние исследования в области обхода систем предотвращения вторжений показывают, что средства защиты могут не видеть атак и не ставить виртуальные патчи, так требуемые стандартом PCI DSS.

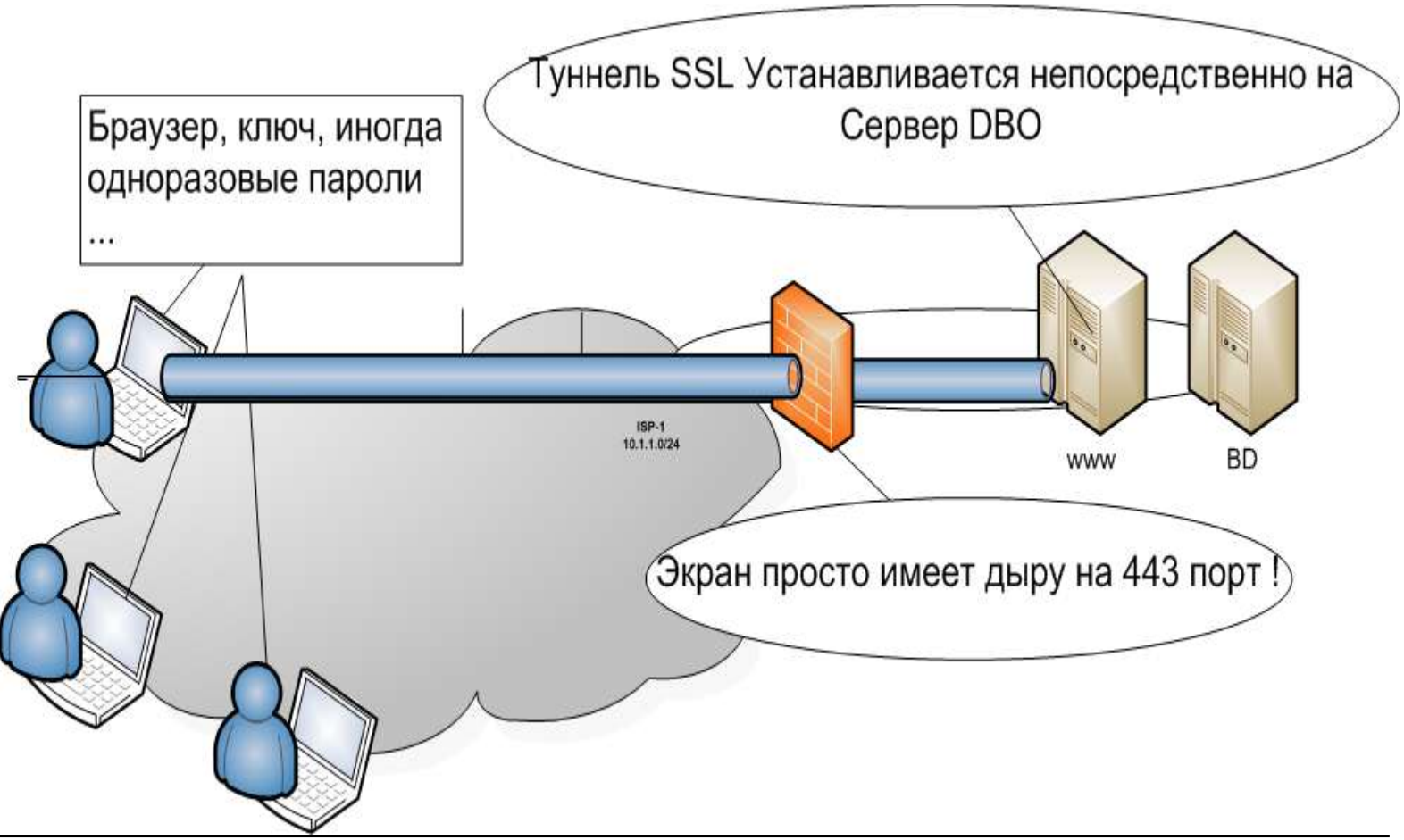
Как противостоять?

Требования безопасности (более 100 пунктов)

Функционал (около 50 пунктов)

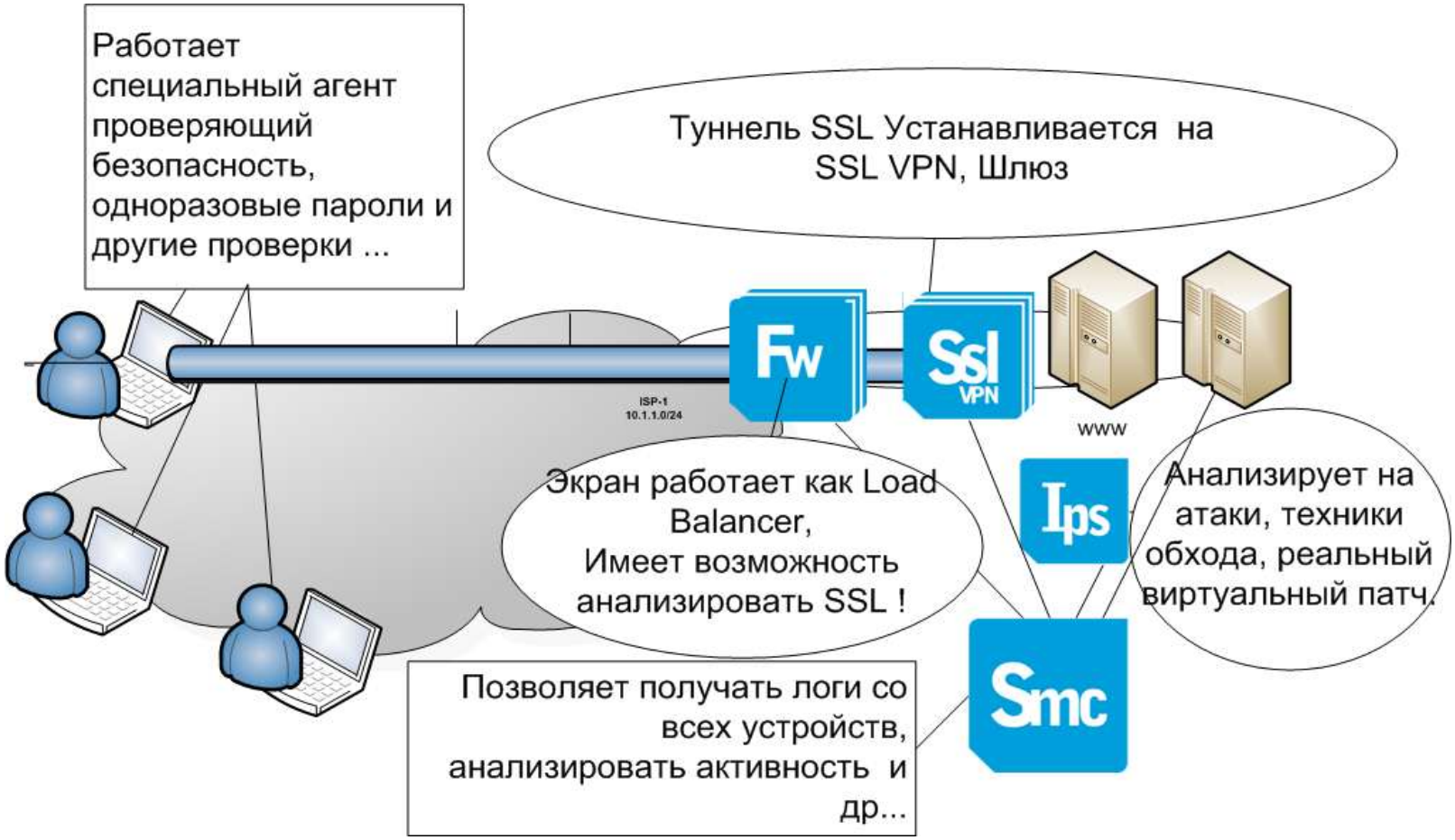
Риски могут быть снижены

Типичная система защиты



Риски могут быть снижены

Схема с системами безопасности



Комплексная защита

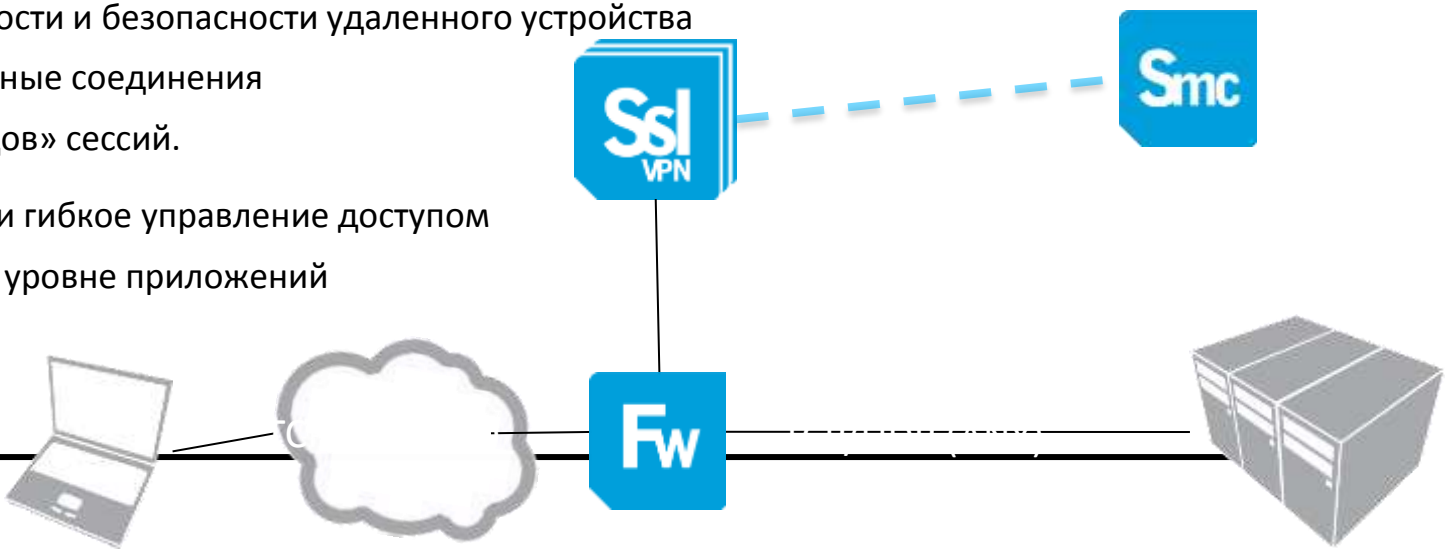
- Часто признаком атаки является нестандартная транзакция при например подключении через Yota…
- Другая непонятная сетевая активность
- Использование другого компьютера вкупе с выходом из неожиданной сети и другое ….
- Усложнение действий злоумышленнику – одноразовые пароли как дополнение к обычным мерам, а также например одновременно SMS информирование о транзакциях …..
- Упрощение картины – когда все события можно проанализировать в одном месте совместно с другими данными

Комплексная защита

- Предлагаемое решение перекрывает не только множество атак , но и например заодно и выполнение требований PCI DSS.
- Позволяет в том числе и передавать данные в нужном структурированном виде (нормализованном) в системы корреляции событий (типа Arcsight и др…)
- Значительно затрудняет атакующему жизнь, а также не увеличивает стоимость вложений например в системы одноразовых паролей, а также например в SSO и др.

Первое в РФ сертифицированное решение StoneGate SSL VPN

- Безопасный доступ из любой точки, в любое время с любых устройств
- Аутентификация в соответствии с вашими требованиями
  - Встроенная двух факторная аутентификация (более 15 видов – в комплекте)
  - Интеграция с любыми аутентификациоными сервисами
  - Поддержка single sign-on & ID federation
- Интегрированное управление угрозами
  - Применение политик безопасности и межсетевого экранирования
  - Анализ целостности и безопасности удаленного устройства
  - Только доверенные соединения
  - Удаление «следов» сессий.
- Гранулированное и гибкое управление доступом
  - Авторизация на уровне приложений



STONESOFT

Сколько теряем?

Ежегодные потери
= €100-140К

Потери за 3 года=
€300-420К

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

Сколько стоит проект?

Банки нуждаются в надежных решениях

- Снижение рисков потерь
- Соответствие PCI DSS
- Соответствие СТО БР ИББ
- Поддержка непрерывности бизнеса
- Дополнительная защита дл особых клиентов

Защищенное ДБО

Безопасный удаленный доступ

Предотвращение вторжений

Виртуальные сети

Защита периметра

Управление событиями
и инцидентами

STONESOFT

Вопросы?

Карагедян Карен
Директор по продажам Stonesoft
в России, СНГ и странах Балтии