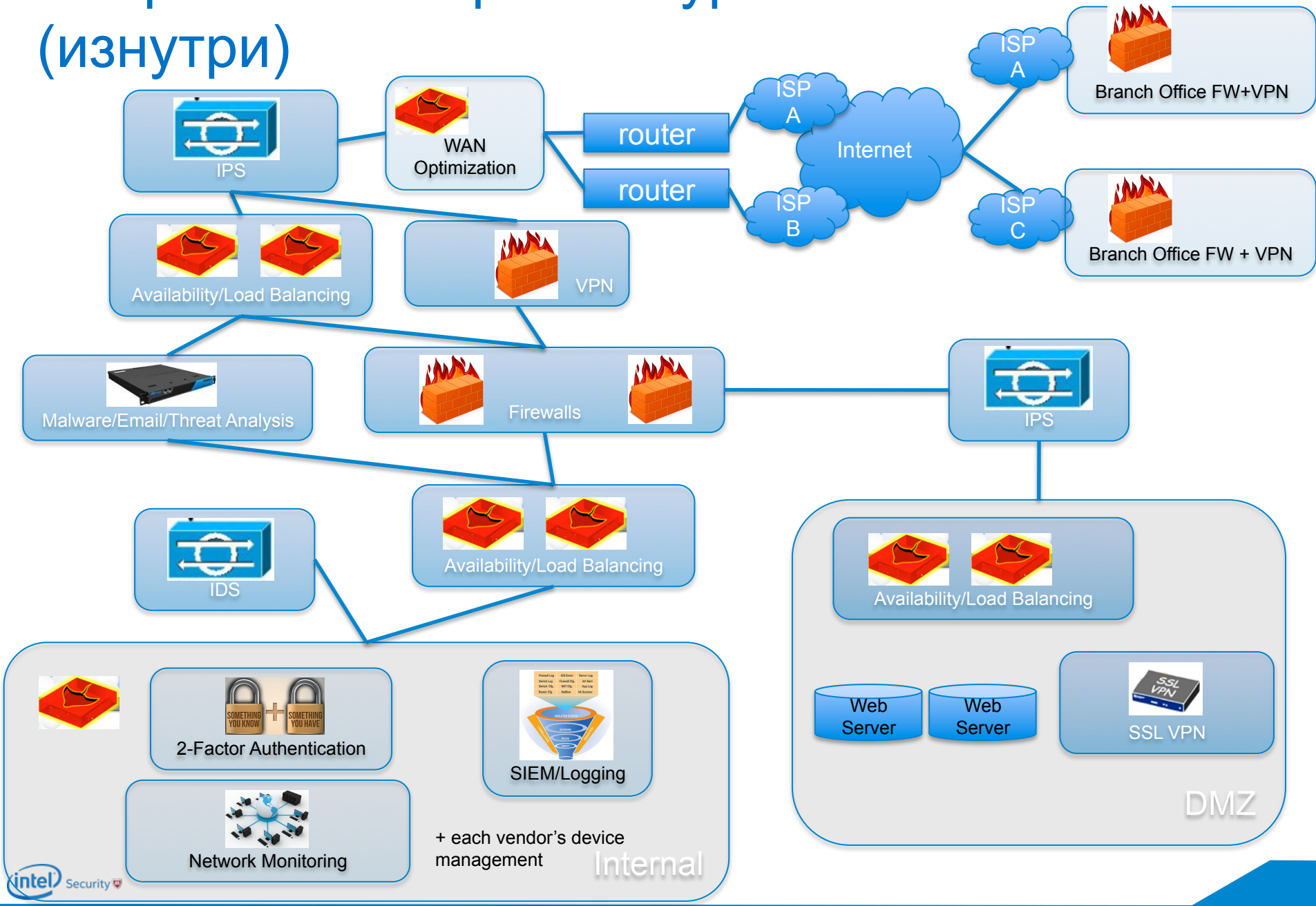
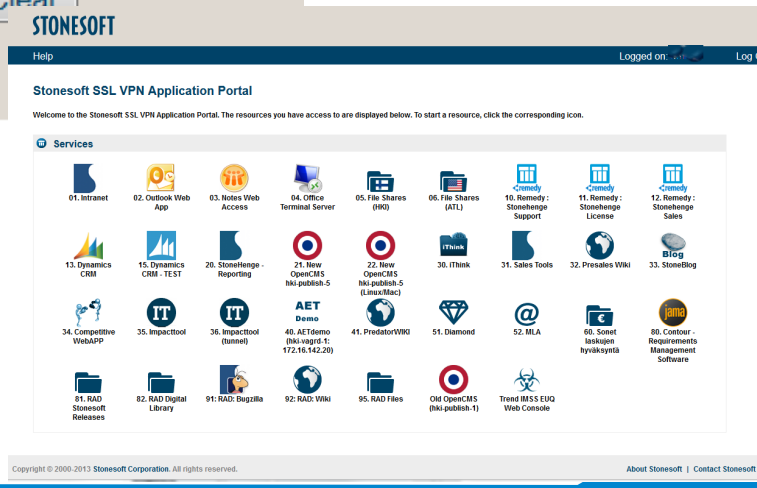
Защищенный удаленный доступ для разных платформ

Специфика и особенности

Современные архитектуры (изнутри)



Современные архитектуры снаружи



Тренды

1

Облака

Максимизация эффективности работы с минимальными затратами

2

Универсальный, безопасный доступ отовсюду

С любого устройства к любому приложению

3

Контекстная безопасность

Доступ, зависящий от состояния и задач клиента

4

Минимизация OPEX

Безопасность за разумные деньги

ОБЛАЧНЫЕ РЕШЕНИЯ

Миграция в облака

- Гарантированная гибкость
- Бизнес как сервис
- Минимизация OPEX

Безопасность доступа – это ПРОБЛЕМА

Когда нам нужен доступ?

- Частные лица
  - Интернет-банк
  - Интернет-порталы (госуслуги, билеты, …)
  - Электронная почта
- Корпоративные нужды
  - Работа сотрудников
  - Удаленное обслуживание оборудования
  - Предоставление доступа к своим сервисам для пользователей (например, электронная почта, корпоративные приложения и т.п.)
  - …

Риски удаленного доступа

- Риски относящиеся к воровству данных [аутентификации]
  - (по каналу связи) – информация может быть перехвачена
- Риски анонимности
  - Стойкие или «облегченные» методы аутентификации
    - Ограничения оборудования (нет возможности воткнуть USB токен с секретным ключом).
    - Сложно понять с чего вообще осуществляется доступ, и соответственно применить политику безопасности.
- Физический неконтролируемый доступ к удаленным компьютерам – можно установить шпионское ПО
  - Пользователь может быть доверенным а на устройстве может быть шпионское ПО.
- Доступ с неуправляемых удаленных устройств
  - Чувствительная информация может случайно остаться на чужом устройстве
  - Чувствительная информация может быть сохранена легитимным пользователем (и оставлена)

УНИВЕРСАЛЬНЫЙ БЕЗОПАСНЫЙ ДОСТУП

Удобство или Безопасность?

- Концепция BYOD
- «Эргономика» удаленной работы
- «Интернет вещей»

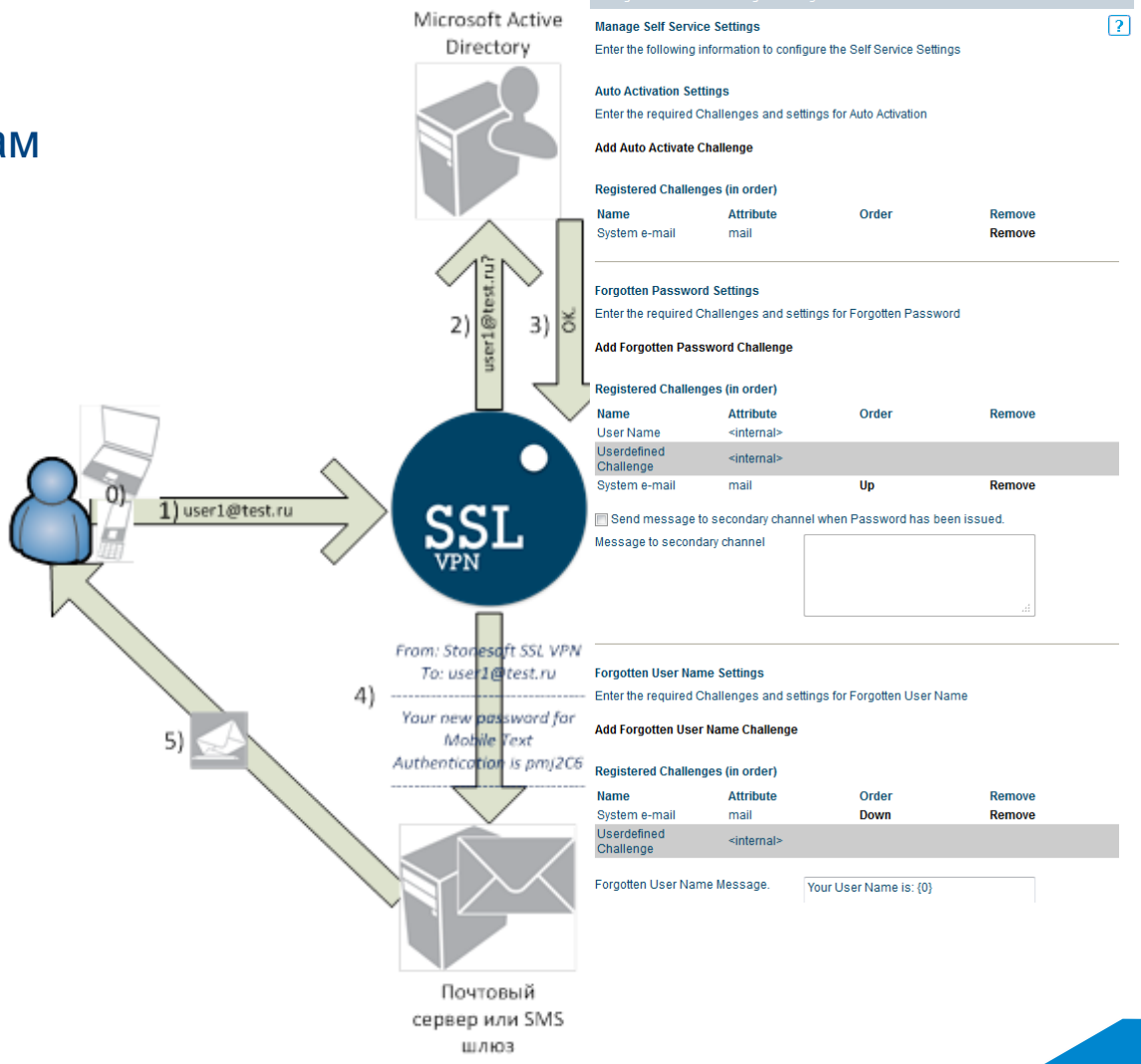
Сценарии доступа

Примеры и технологии

Портал самообслуживания как вариант «безопасного» provisioning-а и снижения труда («ошибок») администратора

Цель:

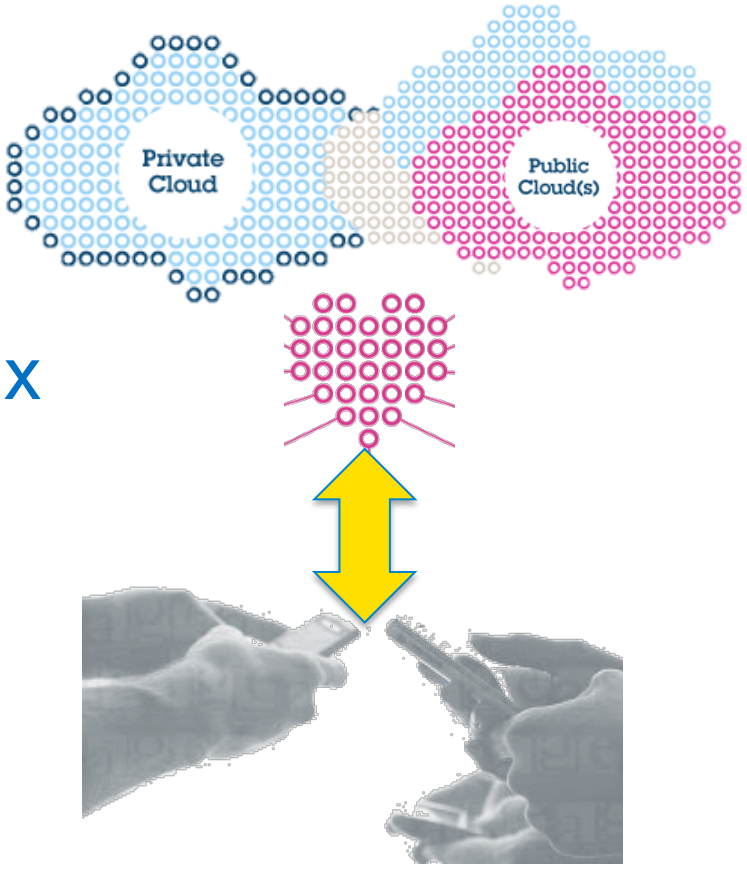
- Безопасный доступ к ресурсам (SSL)
- Надежная аутентификация (OTP, MobileID)
- Контроль доступа, определение типа устройств
- Множественные критерии разграничения прав
- Почти «нулевые» затраты IT-ресурсов



SINGLE SIGN-ON в SSL

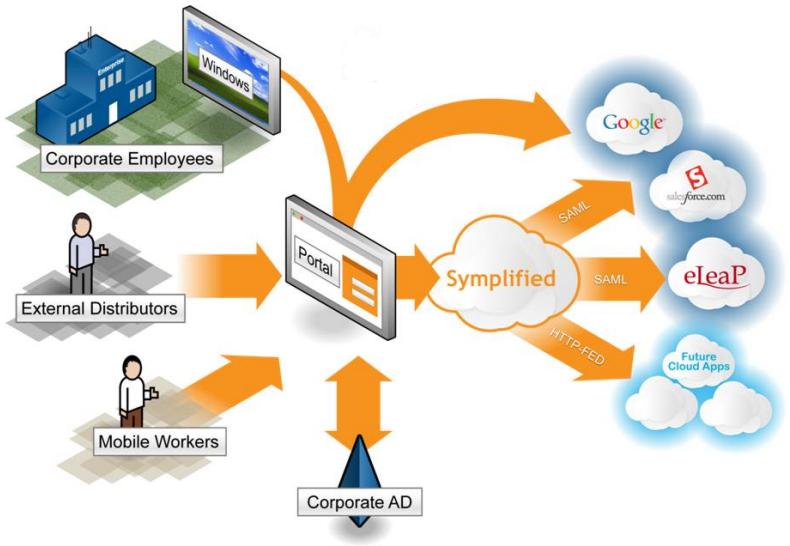
- Разные SSO методы
- SSO для унаследованных

  и веб-приложений
- Разные SSO домены

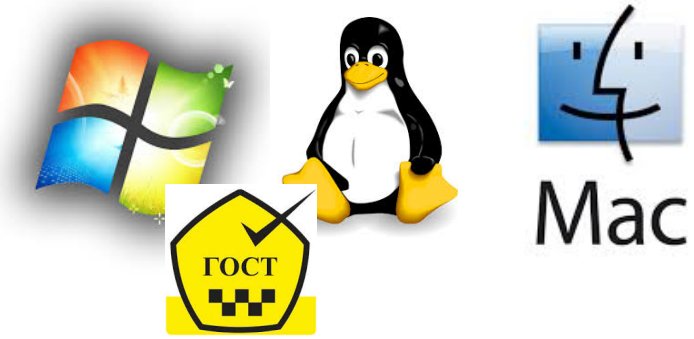


Federated Authentication

- Доступ к облачным сервисам, сохраняя полное управление данными аутентификации
- Разделение процесса аутентификации и доступа/SSO
- Позволяет установить отношения доверия
- Поддержка SAML и ADFS



Авторизация



- Гибкая стратегия авторизация с множественными критериями
- Условный доступ
- Повторное сканирование
- Удаление следов

Безопасность хоста

Наличие Key logger?
Проверка антивируса, других программ

Проверка патчей OS, антивируса

безопасность браузера

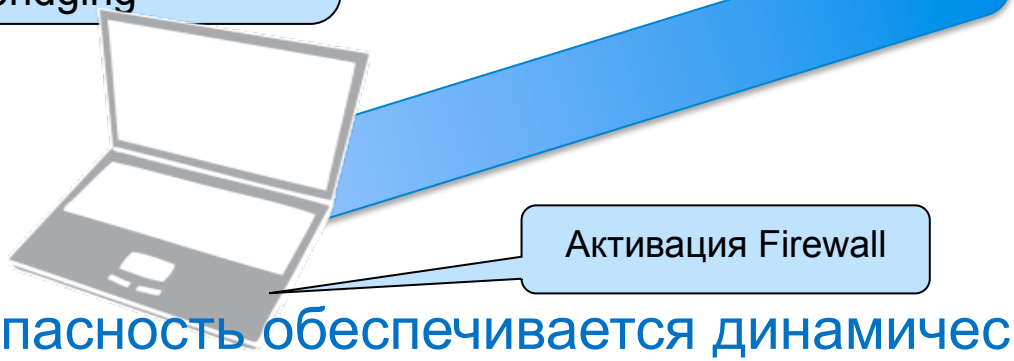
Проверки отсутствия IP-forwarding & network bridging

Проверки специфичных файлов/процессов /сервисов/ портов/приложений, ключей реестра

Проверка наличия Firewall
Анализ серийных номеров, запущеных процессов

Real time проверки подключаемого устройства

Определяет уровень безопасности устройства и дает нужные права доступа



SSL VPN Gateway

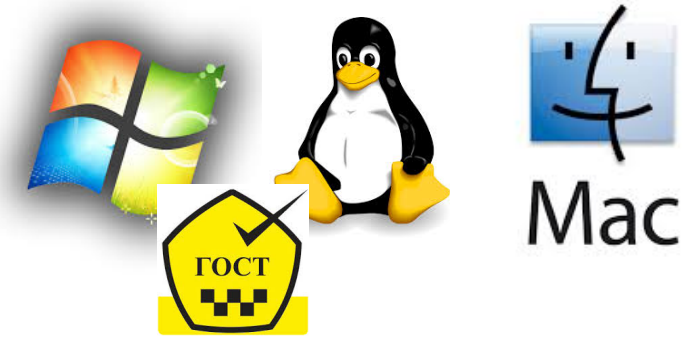
Активация Firewall

Сервера приложений

APP server
Citrix
Oracle Db
File share
Lotus
MS Exchange
SSH Server
Web portal

Безопасность обеспечивается динамически

Контроль окружения



Add Access Rule - Assessment

Select Type

An assessment access rule uses client data requirements, matched with the result of a client scan, to control access to resources protected by the rule. The client data requirements can be custom-defined or specified in a plug-in.

Upload Plug-in

If the plug-in you want to use is not available in the drop-down list box below, click Upload Plug-in to upload it and make it available for selection.

Upload Plug-in...

Select Plug-in or Custom

If you want to use a plug-in to define the required client data in the access rule, selec
plug-in below. If you want to custom-define the client data requirements, select Custo

None selected

- None selected
- Generic anti-virus (2.1)
- Security Center Health (1.0)
- Sygate On-Demand (1.0)
- MAC Address Authorization (1.1)
- Security Center (1.4)

< P

Add Access Rule - Assessment

Select Criteria

Select type of information applicable for the client data you will specify requirements for, and define whether the access rule will be used to allow or to deny access.

Display Name

Operating System: Windows

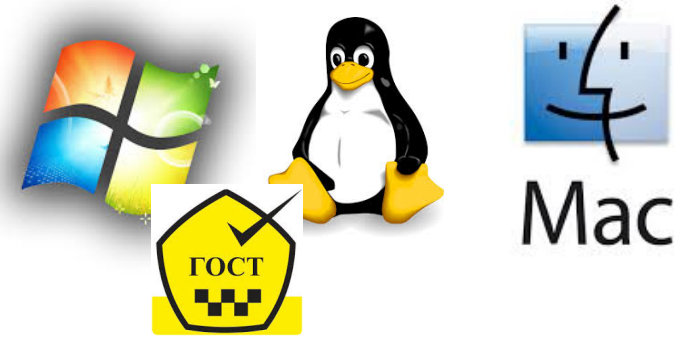
Information Type: File information

- File information
- Directory information
- Registry Key information
- Registry Sub Key information
- Process information
- Windows user information
- Windows domain information
- Network interface information
- TCP port information
- UDP port information

Deny access

< Previous **Next >**

Повторное сканирование



Manage Assessment

General Settings | Advanced Settings | Plug-ins

Client Scan Overview

Use the general settings to configure the client scan performed when accessing a resource protected by an assessment access rule. Note that you need to add an assessment access rule before these settings can take effect.

Real Time Scan

Use the real time scan option to run a client scan at a specified interval during the user session.

☑ Enable real time scan

Interval 120 sec

Client Scan Path

Add client scan paths used by the assessment access rules. A client scan path defines the information that will be scanned during the client scan.

Add Client Scan Path...

Operating System	Type	Path

Windows

☐ Enable collection of Windows information

☐ Enable collection of process information

☑ Enable collection of network information

Mac OS X

Linux

Save

Add Client Scan Path

General Settings

Select type and enter a client scan path. Note when specifying a path to a directory containing many files and sub-directories, it may take quite some to process the information.

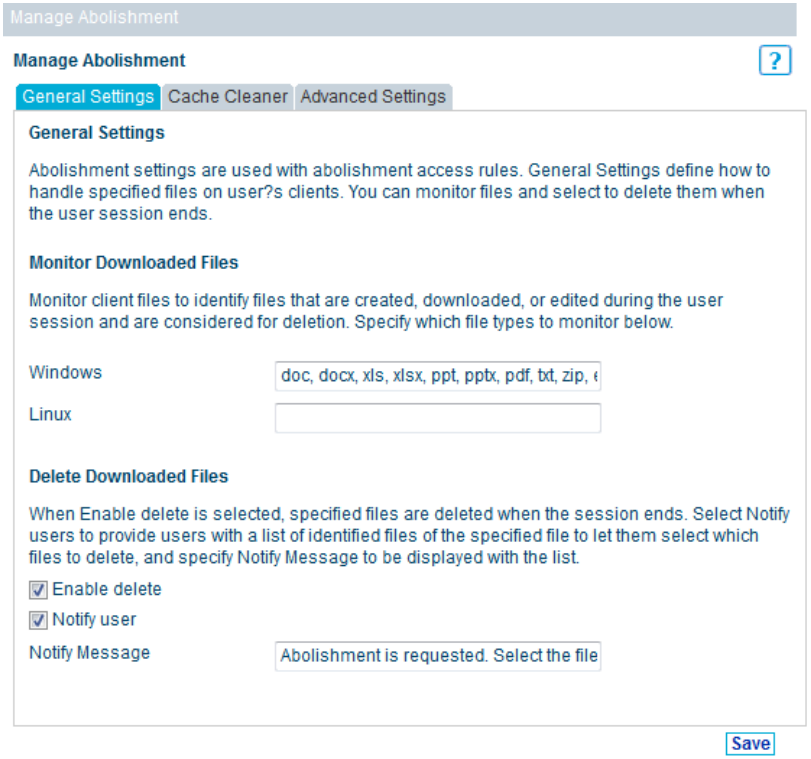
Operating System: Mac OS X

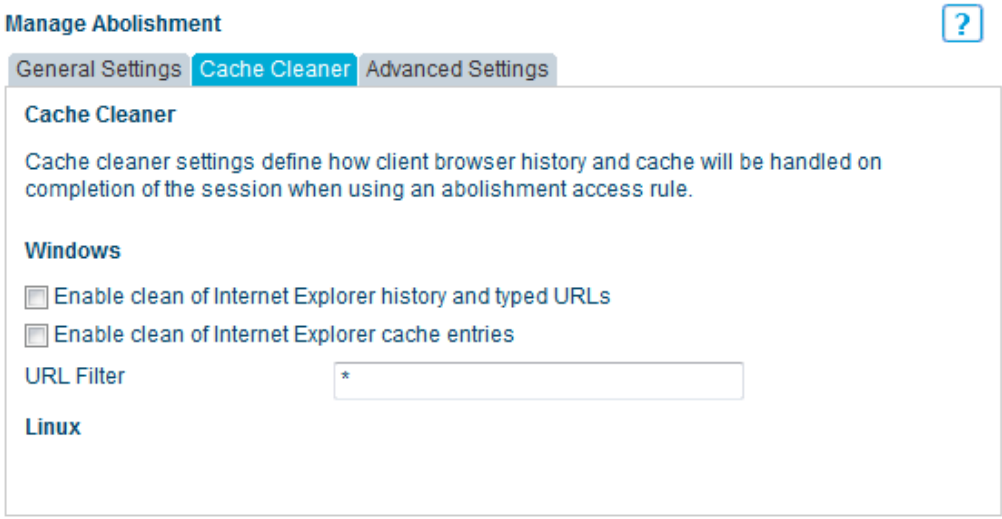
Type: File (File / Directory)

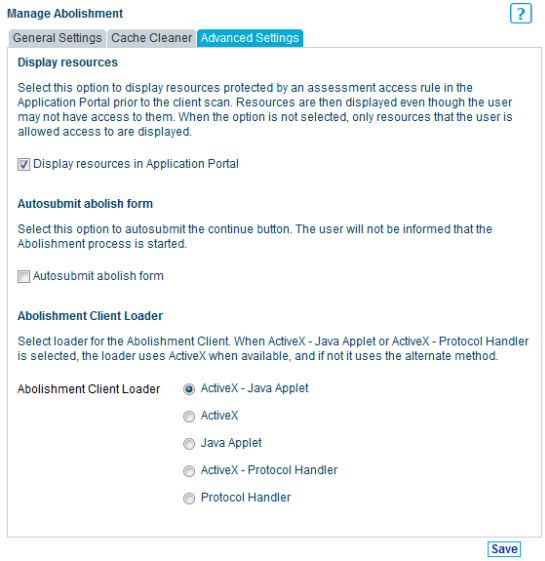
Path

< Previous Add

Удаление следов доступа







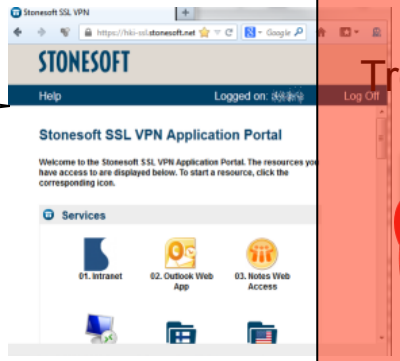
Полная… изоляция для приложений

Рабочее место клиента

Активация агента
(это может быть выполнено до начала сессии)

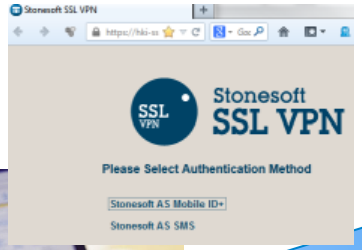
2. Авторизация с автоматическим пер[illegible]

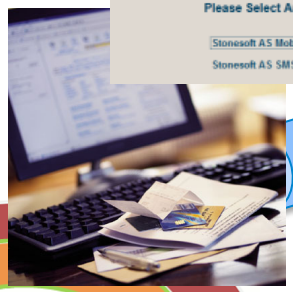
Аутентификация и авторизация на вход в банк (оформление меняется под Заказчика)

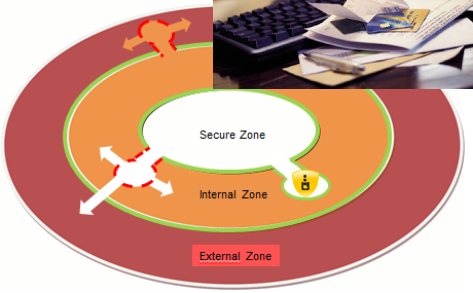


Пользователь «как обычно» работает с сайтом.

1. Доступ на сайт (через SSL)

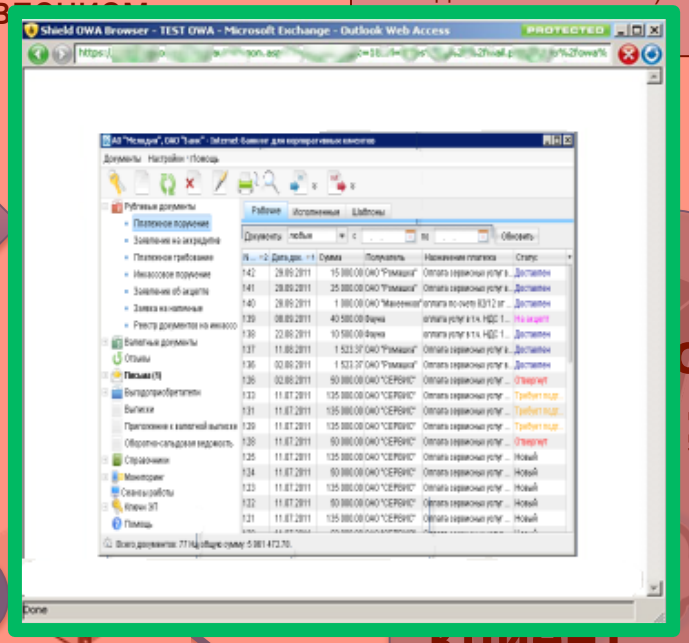






Trojans

Keyloggers



StoneGate SSL VPN

Spyware

MitB

Интернет-банк

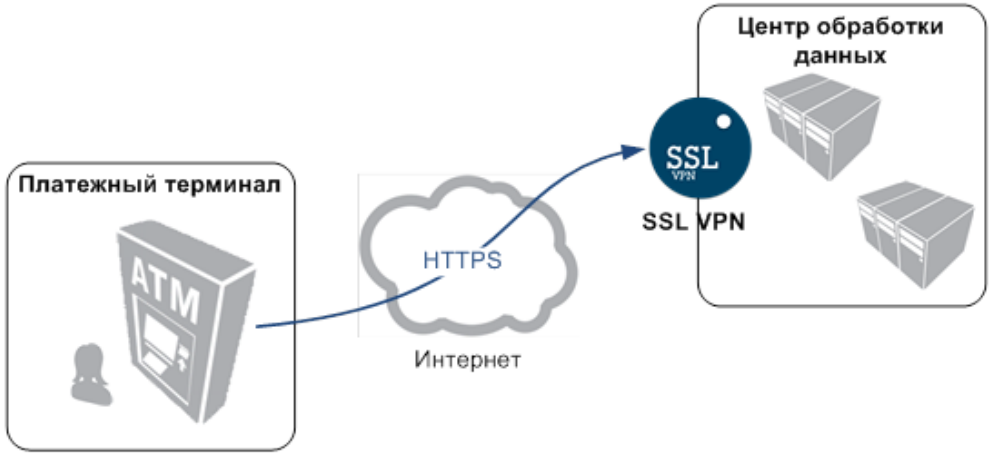
Загрузка и активация модуля безопасности

4. Загрузка защищенного приложения/браузера

- Обеспечивается изоляция приложения и высокий уровень безопасности

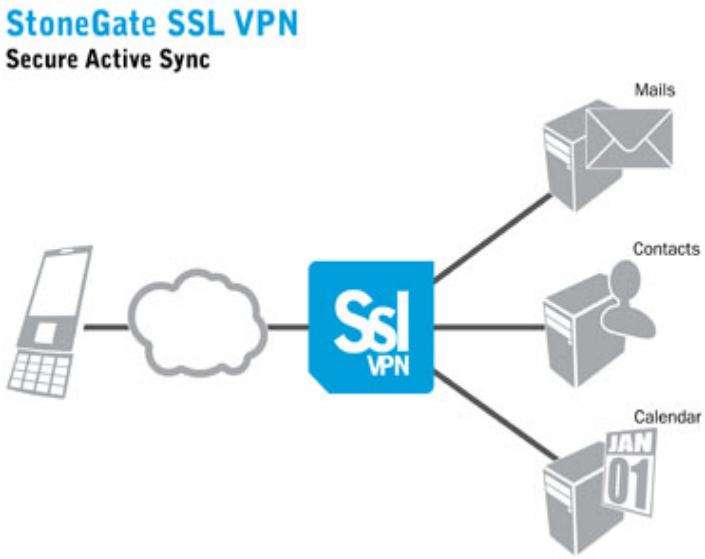
Защита терминалов / банкоматов

- Автоматизированная работа
- Надежная аутентификация
- Прозрачный доступ



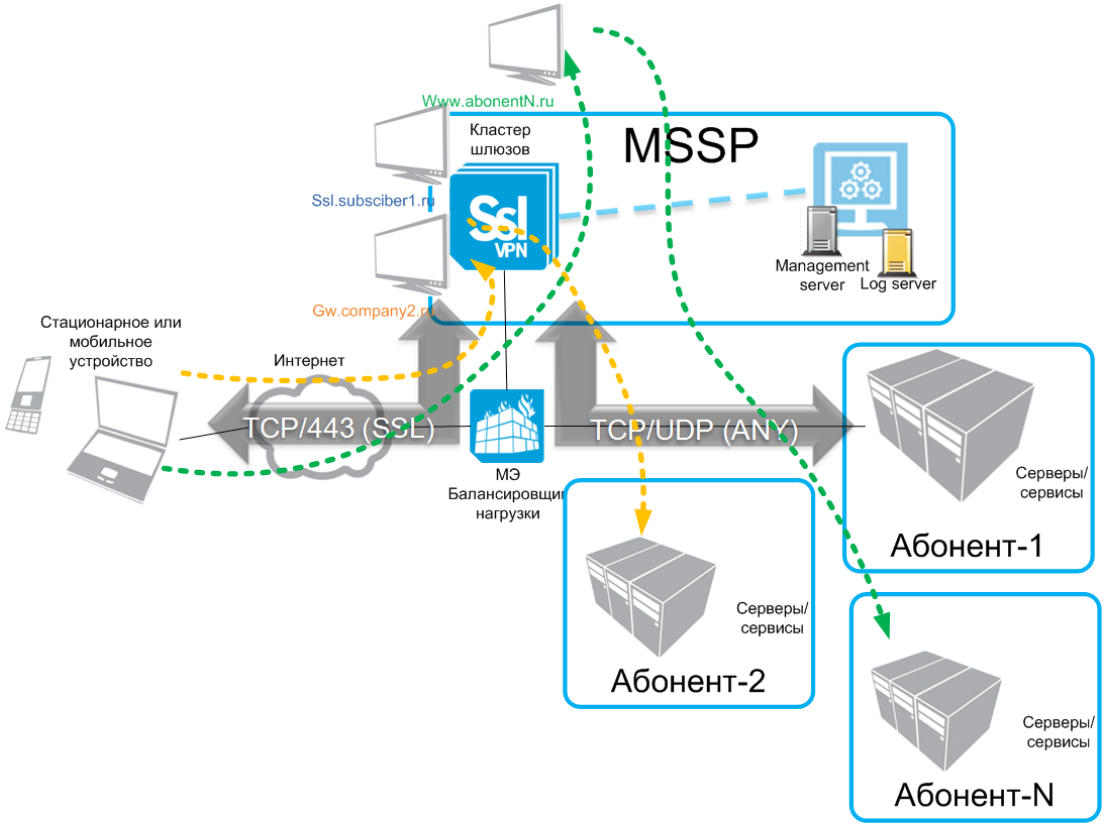
Безопасность мобильной почты

- StoneGate SSL – Active Sync Proxy;
- Снимает SSL с Exchange сервера;
- Аутентификация на шлюзе;
- не надо делать «дыру» в межсетевом экране до сервера почты;
- DeviceID locking = блокировка по идентификатору устройства;
- SSO для доступа Exchange;
- Возможность работы в том числе с мобильных устройств и даже по ГОСТу!



Защита удаленного доступа в распределенной организации / у сервис провайдера

- Поддержка разных платформ
- Разделение порталов на одном устройстве
- Различные сценарии доступа

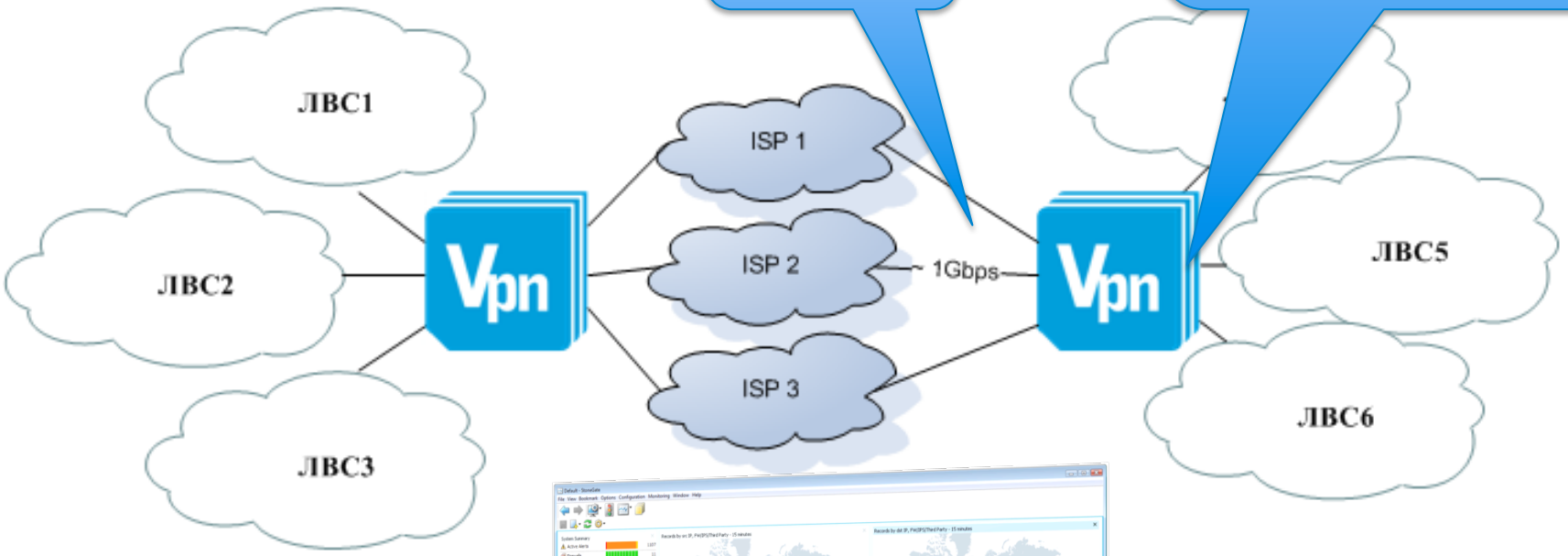


StoneGate SSL VPN

- Безопасный доступ с разных 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

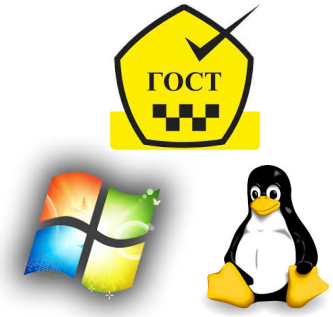
Задачи шифрования трафика в (между) ЦОД

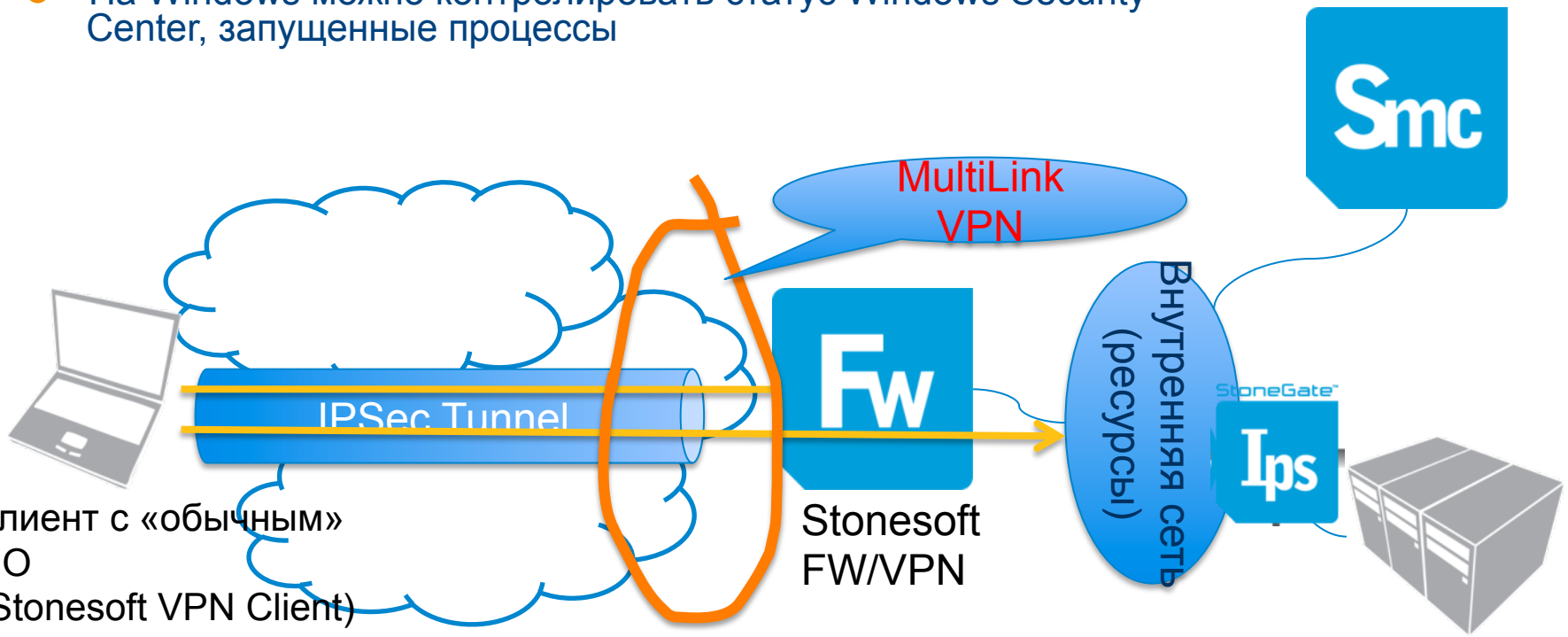
Современный подход



Проброс произвольного трафика

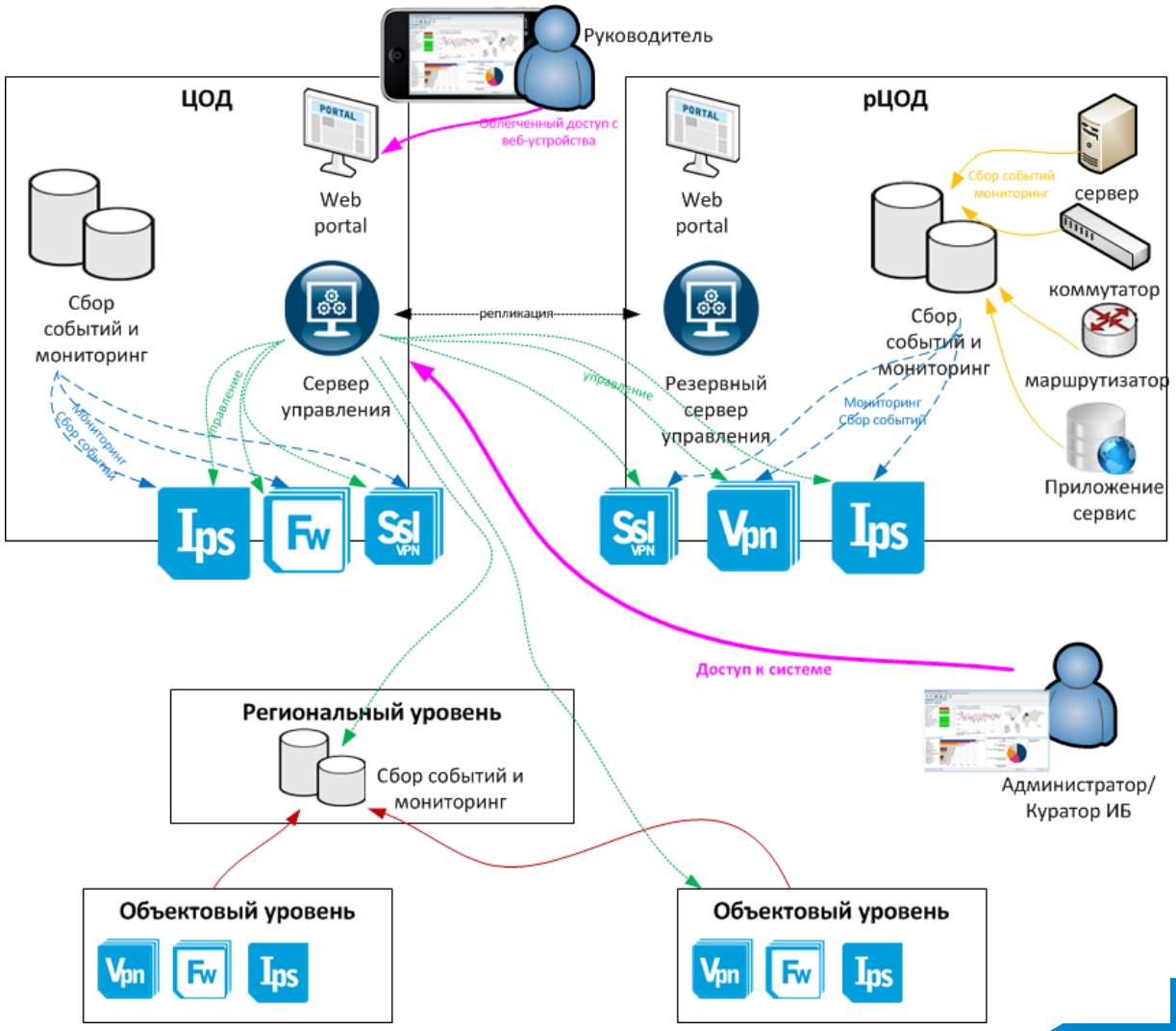
- Необходимость наличия предустановленного спец.ПО на клиенте
- Доступ «в сеть» (тогда как для SSL – доступ «к приложению»)
- Аутентификация в т.ч. по токенам (OTP может быть тоже)
- Поддержка **MultiLink**, NAT/PAT
- Туннелирует все, любое приложение
- На Windows можно контролировать статус Windows Security Center, запущенные процессы

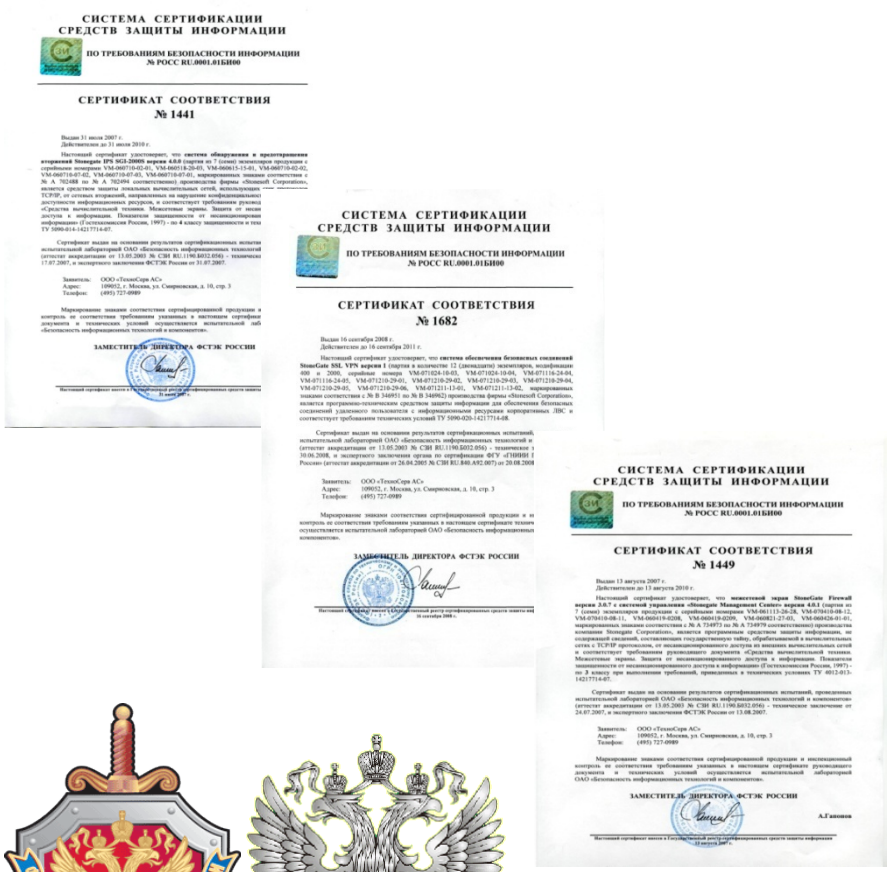




Пример сложной системы

- Можно комбинировать системы между собой и с другими компонентами
- От этого безопасность повышается




СИСТЕМА СЕРТИФИКАЦИИ
СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ
ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ
№ РОСС RU.0001.01БИ00
СЕРТИФИКАТ СООТВЕТСТВИЯ
№ 1441
ЗАМЕСТИТЕЛЬ ДИРЕКТОРА ФСТЭК РОССИИ
СИСТЕМА СЕРТИФИКАЦИИ
СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ
ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ
№ РОСС RU.0001.01БИ00
СЕРТИФИКАТ СООТВЕТСТВИЯ
№ 1682
ЗАМЕСТИТЕЛЬ ДИРЕКТОРА ФСТЭК РОССИИ
СИСТЕМА СЕРТИФИКАЦИИ
СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ
ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ
№ РОСС RU.0001.01БИ00
СЕРТИФИКАТ СООТВЕТСТВИЯ
№ 1449
ЗАМЕСТИТЕЛЬ ДИРЕКТОРА ФСТЭК РОССИИ

Сертифицированная платформа безопасности StoneGate для построения защищенных систем

Что где работает (вместо резюме)

ОС/механизм	Шифрование	Аут-ция	Авторизация	Удаление следов	Тип доступа
Win8	+ ГОСТ	+ (серт., OTP, токен)	М.б.проблемы	-	Веб, туннель
Win7	+ ГОСТ	+ (серт., OTP, токен)	+ (полный набор)	+ (зависит от версии IE)	Веб, туннель
WinXP	+ ГОСТ	+ (серт., OTP, токен)	+ (полный набор)	+ (зависит от версии IE)	Веб, туннель
*nix	+ ГОСТ	+ (серт., OTP, токен)	+ (файлы, директории), КС ГОСТ	-	Веб, туннель
MacOS	- (не ГОСТ)	+ (не ГОСТ серт., OTP, токен)	+ (файлы, директории)	-	Веб, туннель
iOS	+ ГОСТ	+ (серт., OTP, токен)	-	-	Веб или спец.ПО
Android	- (не ГОСТ)	+ (не ГОСТ серт., OTP, токен)	-	-	веб