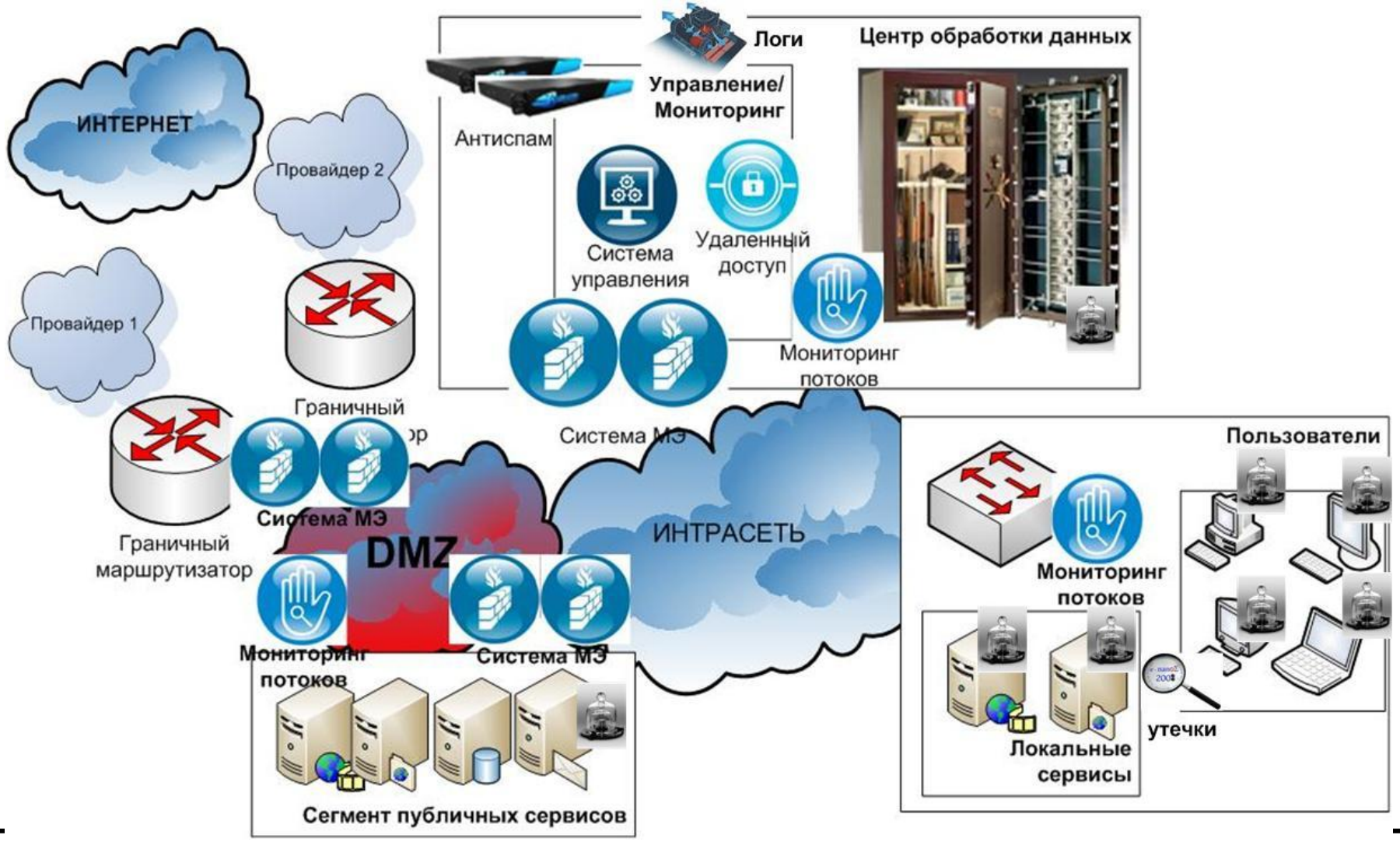
STONESOFT

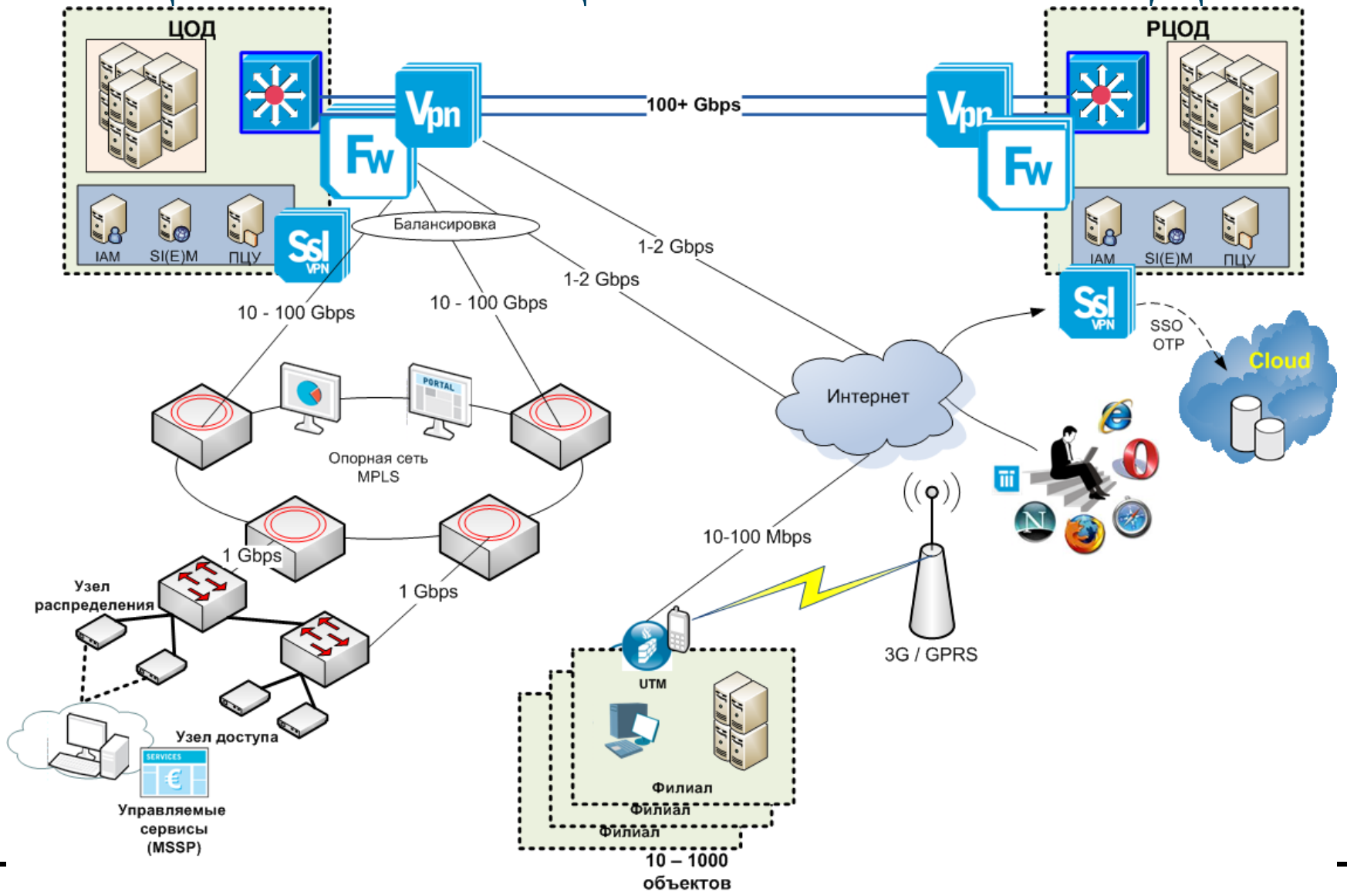
Современные подходы к защите высокоскоростных каналов и обеспечение связи с персональными устройствами

Дмитрий Ушаков
Семинар GlobalTrust
12.10.2011

Смещение акцентов - вчера



Смещение акцентов - сегодня



STONESOFT

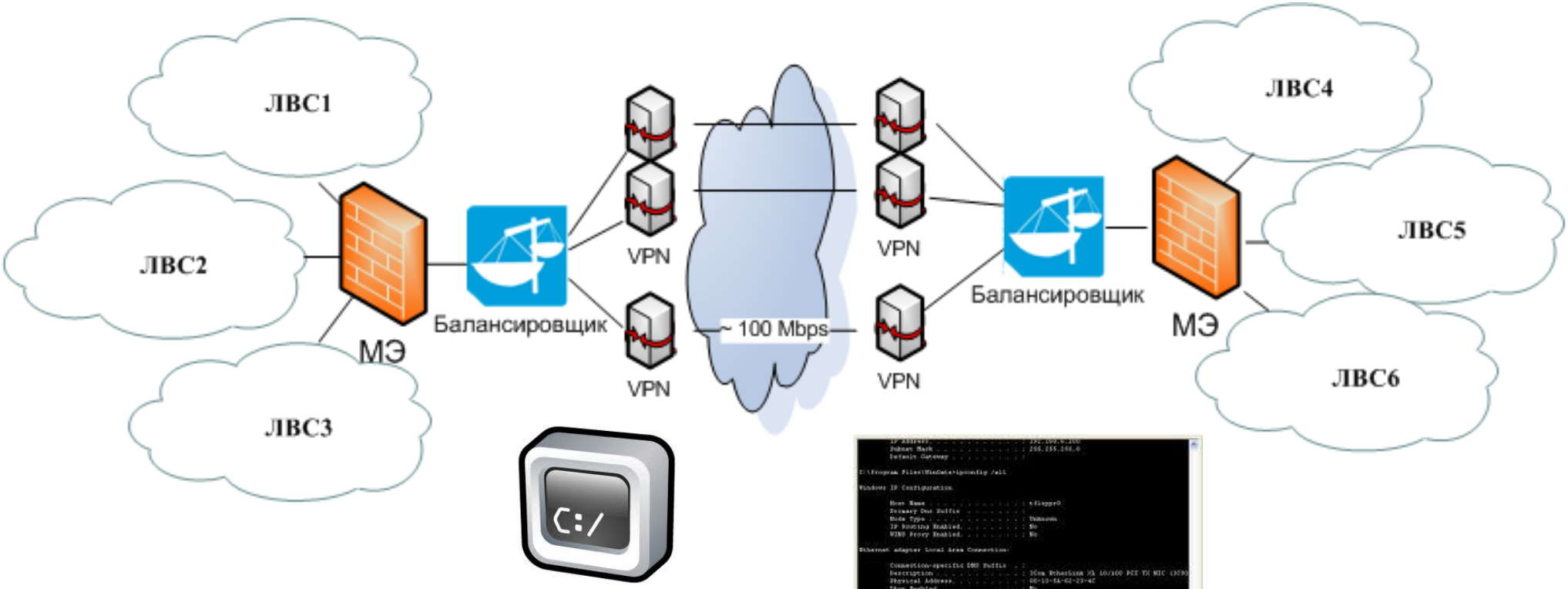
ТРУДНО НЕ ЗАМЕТИТЬ РАЗНИЦУ

Современное решение – это:

- Высокие скорости
- Отказоустойчивость во всем
- Распределенность
- Поддержка «облачных» сервисов
- Поддержка управляемых услуг безопасности
- «Реальная» защита
- Соответствие требованиям регуляторов

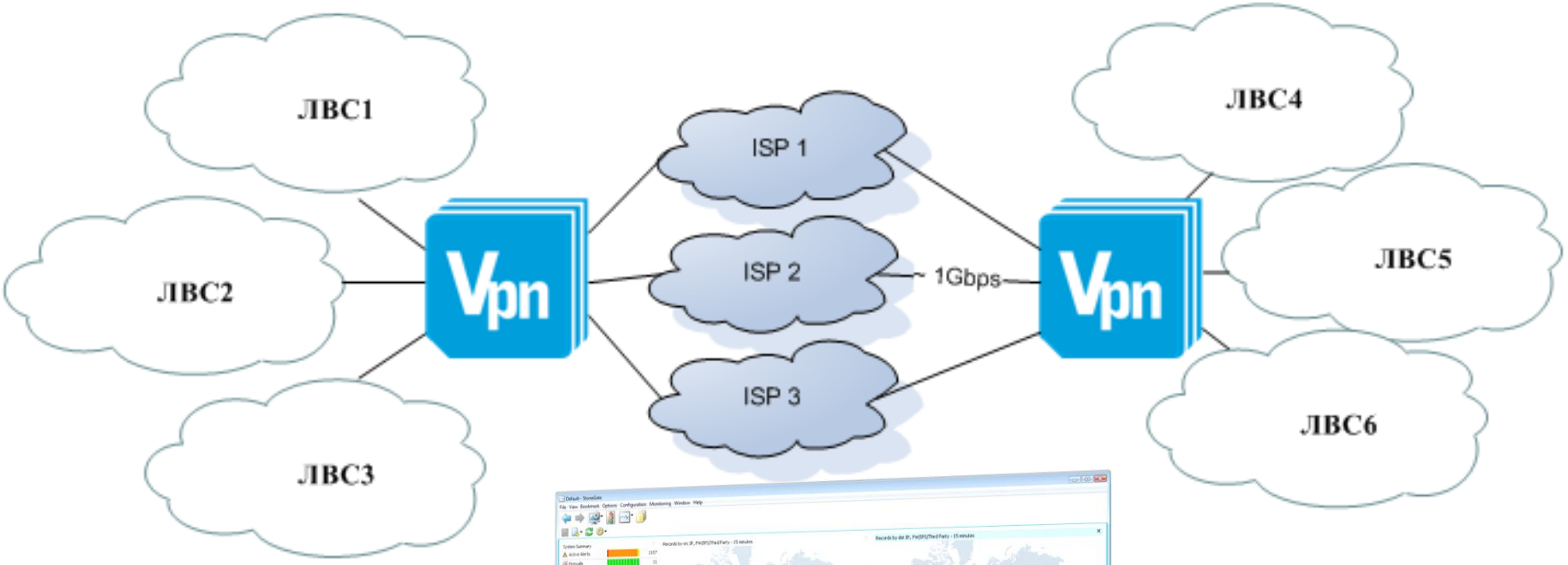
Задачи шифрования трафика

- Раньше



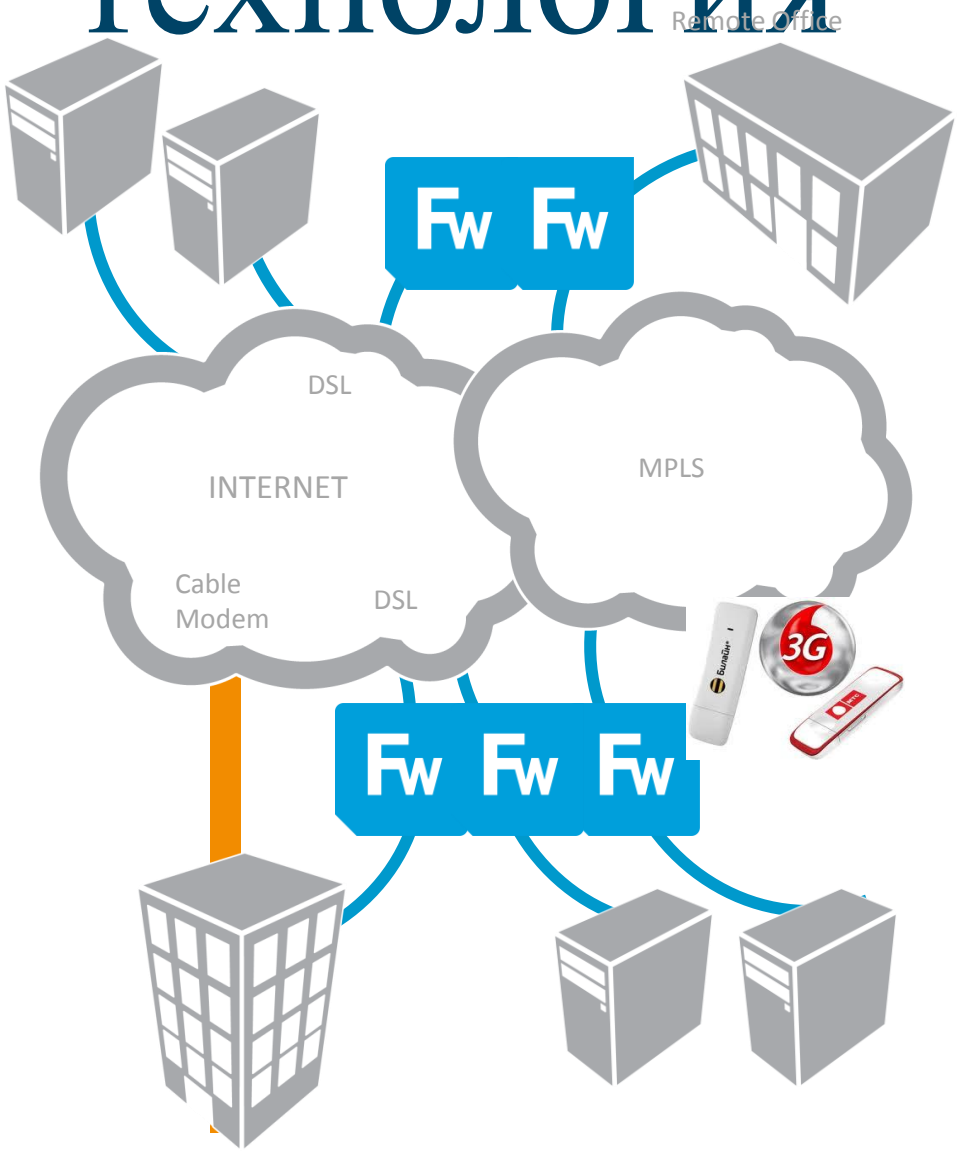
Задачи шифрования трафика

- Сейчас



Multi-Link™ технология

- Единственное на рынке решение, которое обеспечивает действительно отказоустойчивую связь одновременно через несколько провайдеров связи (например, Интернет).
- Обеспечения подключения каналов связи
  - Active/active/active/…. – до 16 каналов одновременно!
- Исключает дорогие решения на IGP/EGP протоколах (OSPF, BGP…)
- Безопасно и масштабируемо
  - Неограниченное количество и типы соединений
- Поддержка критических технологий встроенными(!) функциями QoS
  - Например, VoIP, video конференции

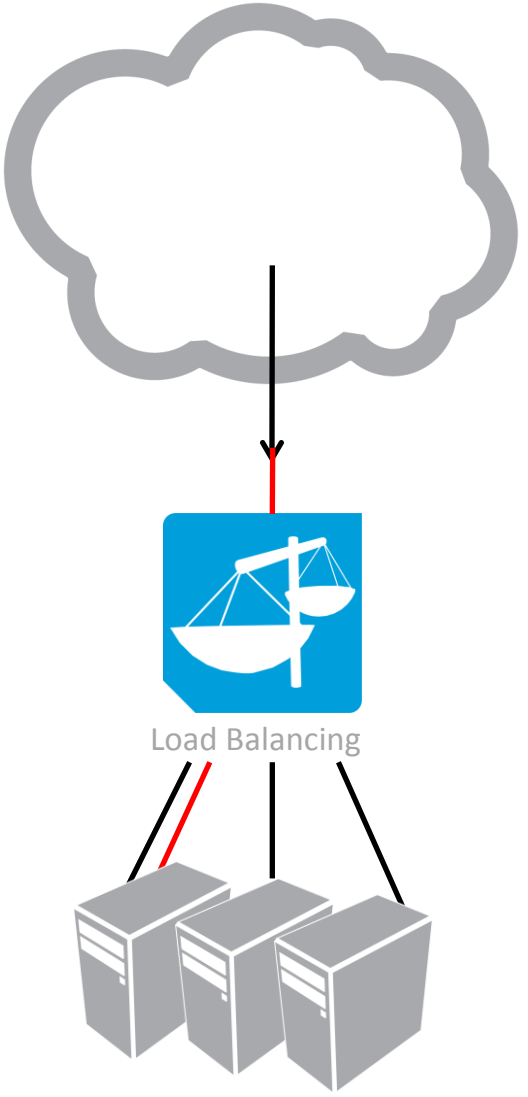


STONESOFT

- Достижение доступности **0,99999**

Динамическая балансировка нагрузки Server Load Balancing

- Исключает необходимость в дополнительном оборудовании
  - Не лимитированное количество серверов для балансировки
  - Точный мониторинг доступности и состояния
  - Оптимизация трафика
  - Автоматические корректирующие действия
  - Прозрачное управление серверами
- Автоматически распределяет трафик
  - Нет ограничений по количеству клиентских соединений
- Работает на всех платформах!

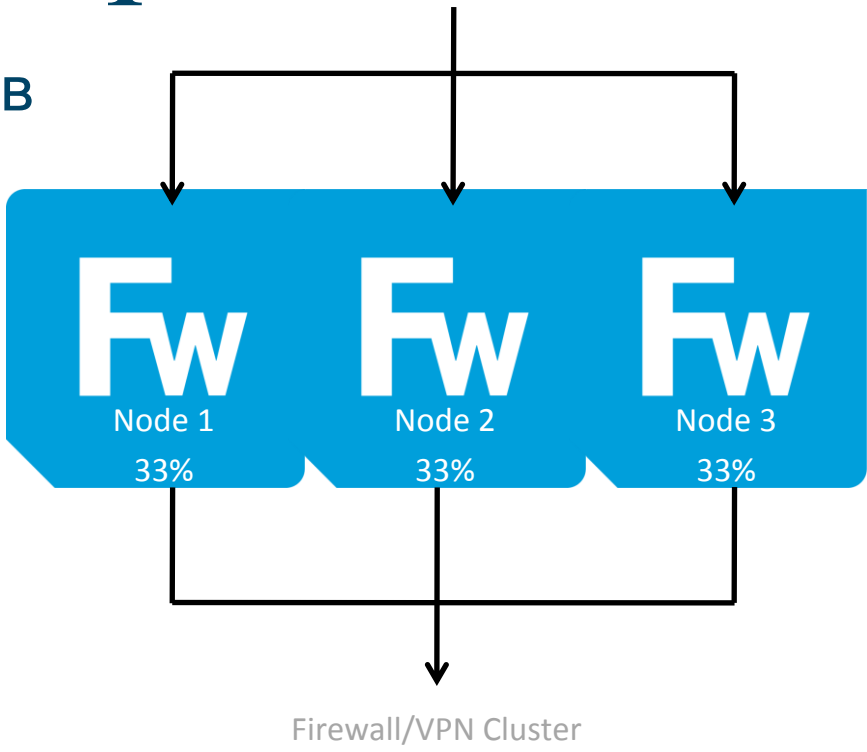


Современное решение – это:

- **Высокие скорости**
- **Отказоустойчивость во всем**
- Распределенность
- Поддержка «облачных» сервисов
- Поддержка управляемых услуг безопасности
- «Реальная» защита
- Соответствие требованиям регуляторов

Полноценная кластеризация

- Уникальный кластер до 16 устройств
- Достижение доступности 0,99999
- не требует переконфигураций сети
- Нет необходимости обслуживать
- Кластеры управляются как единое устройство
- Кластеризованный VPN – обеспечивает полноценную доступность
- Позволяет постепенно наращивать производительность
- Концепция «pay-as-you-grow» - разные модели в кластере

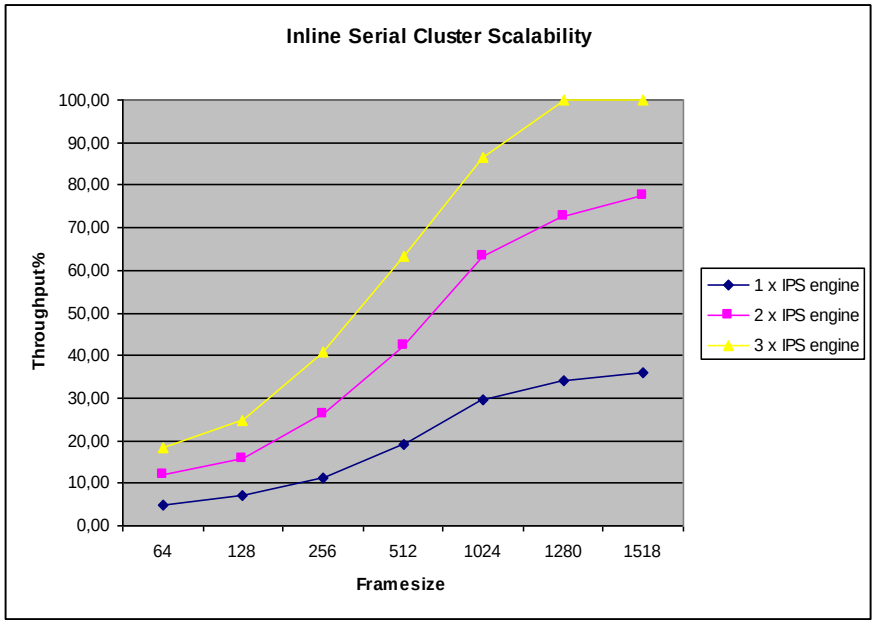


Патентованная технология «drop-in-clustering»

Нет необходимости идти на компромисс: высокий уровень безопасности или высокая скорость

Inline IPS кластеризация - нужно 30 Gb/s?

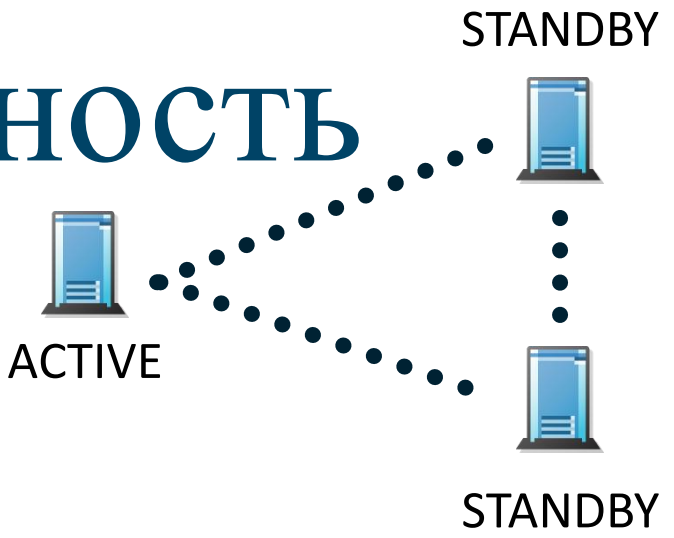
- **Кластеризация**:
  - Увеличивается скорость работы IPS
- Простое управление кластером = как одна IPS
- «Fault tolerance» для сервисов IPS (отказоустойчивость):
  - Hardware **bypass** (inline pair)
  - Software **bypass**
- IPS для датацентров – **до 15 Гб/с на узел**
- До **10 млн.** одновременных **соединений**

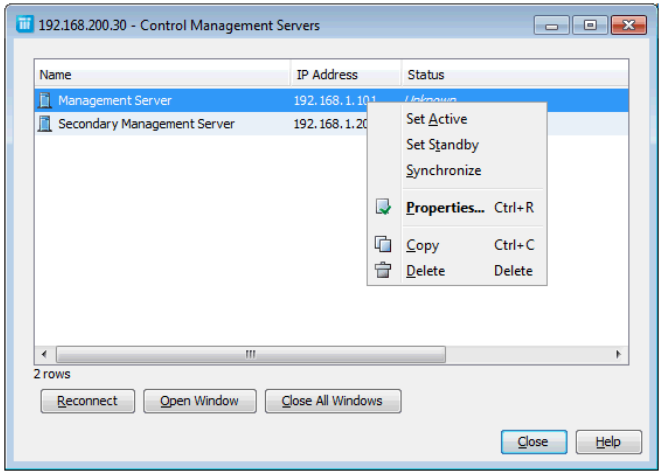


STONESOFT

SMC HA и производительность

- Инкрементальная репликация
- Операции из GUI
- Масштабируемость до тысяч устройств
- Скорость обработки событий до 100 тыс./сек.
- Эффективность передачи информации:
  - ~150 байт/событие
  - Обмен между сервером и клиентом
- Одновременные операции
- Распределение нагрузки

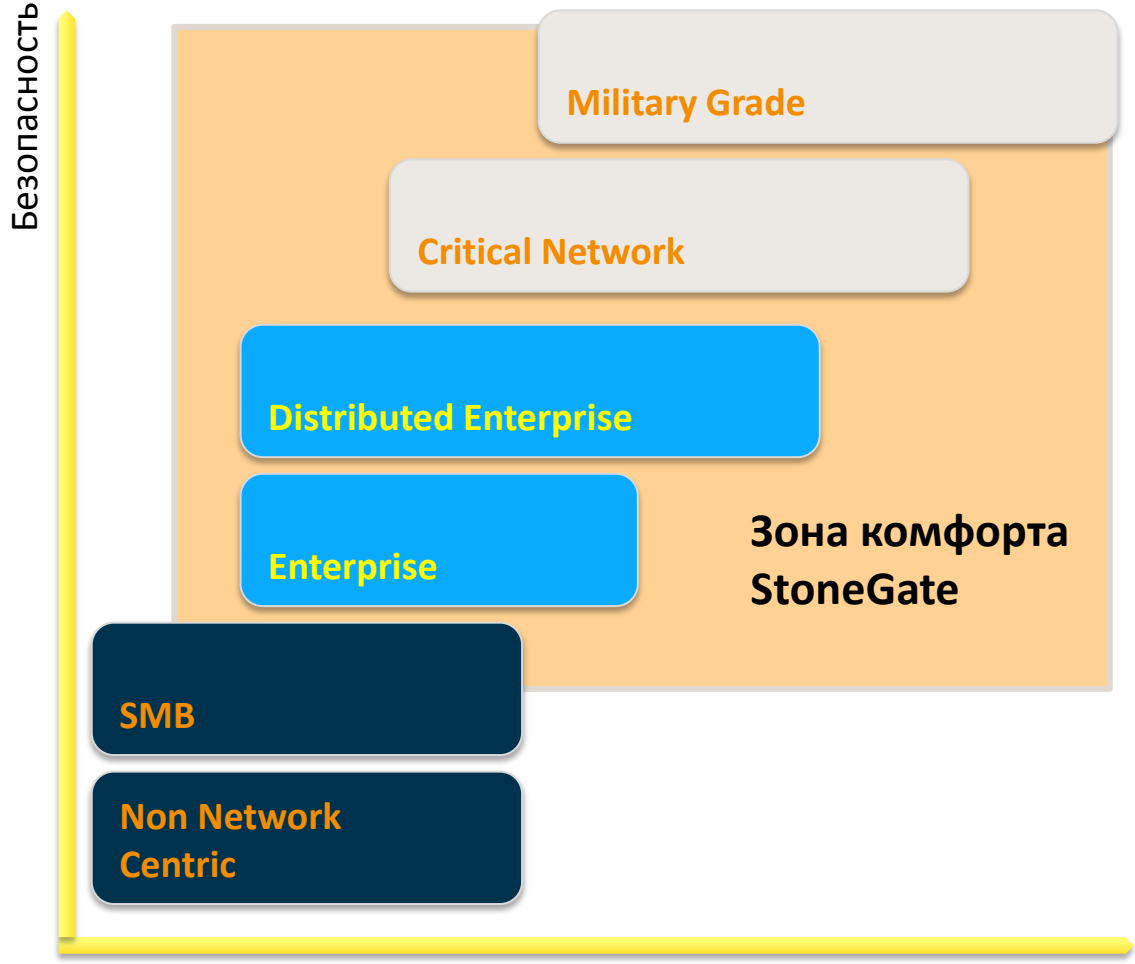




Современное решение – это:

- Высокие скорости
- Отказоустойчивость во всем
- **Распределенность**
- Поддержка «облачных» сервисов
- Поддержка управляемых услуг безопасности
- «Реальная» защита
- Соответствие требованиям регуляторов

Зона комфорта StoneGate



- Производительность во всем!
  - Управляемость
  - Развертываемость (TCO)

Типичные шаги реализации

- Покупка и логистика (никуда не деться)
- Затраты на внедрение
  - Первоначальная настройка
  - Дублирование конфигурации по устройствам
  - Отладка и тестирован
- Принятие
  докум
- За
  - Ин жка
  - Визуали ация текущего уровня защиты
  - Регламентное тестирование [соответствия]…

Ситуация становится необратимой, когда уже нельзя сказать: «Давайте все забудем!»

Масштабируемость и управляемость

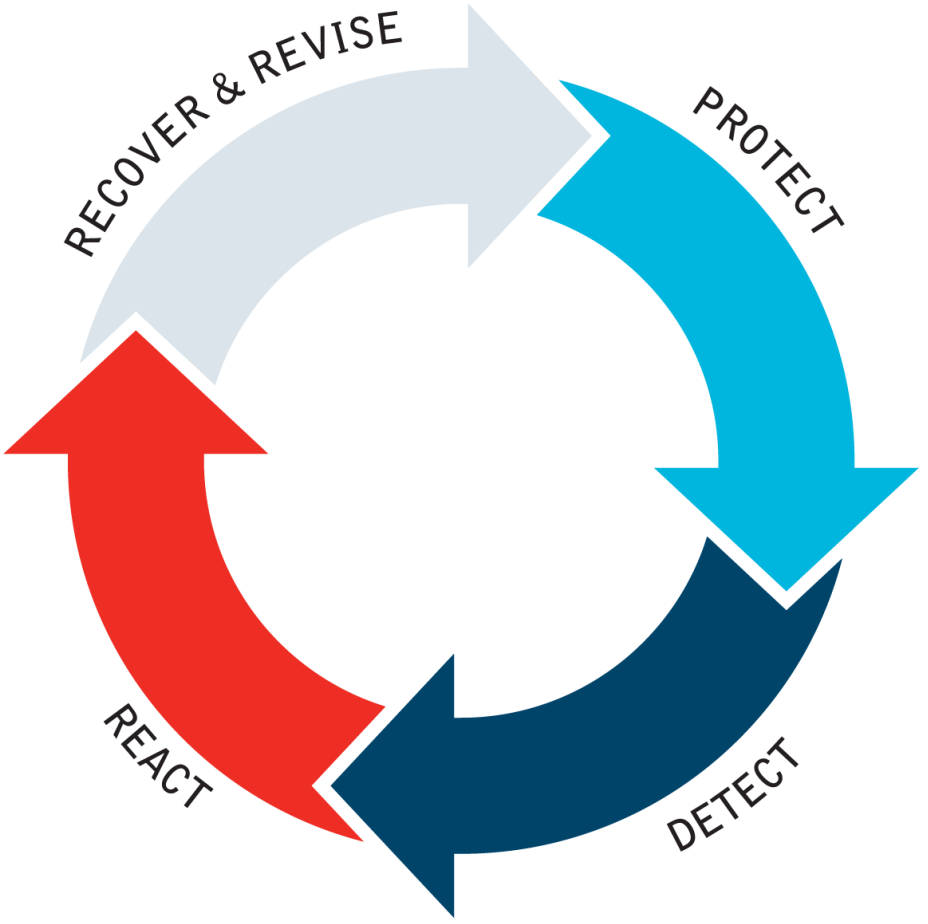
Situation Awareness

”More han 99% of firewall breaches are caused by misconfigurations rather than firewall flaws.”

Gartner

Процесс управления безопасностью

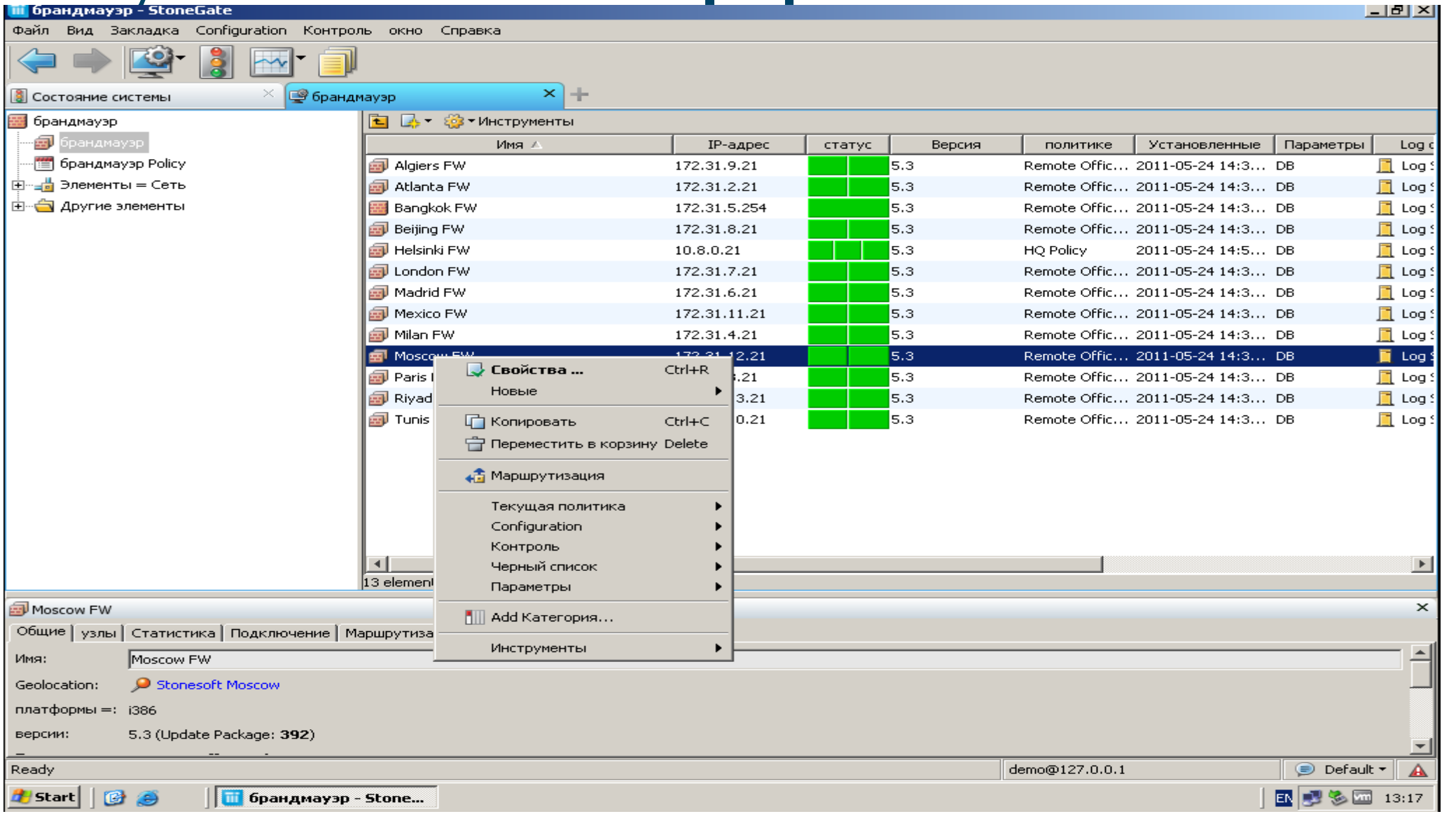
- **Идентификация** рисков
- **Защита** активов
- **Детектирование** взломов
- **Реакция на** инциденты
- **Восстановление** систем
- **Пересмотр** процессов и уровня защиты



ПРОАКТИВНАЯ СИСТЕМА УПРАВЛЕНИЯ НОВОГО ПОКОЛЕНИЯ

- Использование созданного элемента во всех конфигурациях
- Централизованное хранилище
- Наглядность управления сетью
- Оптимизация политик ИБ
- Глобальное администрирование
- Интерактивный мониторинг и оповещение администратора в режиме реального времени
- Мониторинг сторонних устройств
- SOC / SIEM интеграция
- Управление ПО, программно-аппаратными и виртуальными решениями из одной точки

Русский интерфейс!



STONESOFT

Востребованность Mass Security

STONESOFT

Решение «Mass Security»

1. **Plug n Play инсталляция:** новых МЭ в отдаленных точках.
2. **Применение политики:** мгновенное обновление политики безопасности в любой и каждой из точек – никаких задержек.
3. **Безопасная & отказоусточивая связность** посредством нескольких ISP/CSP соединений.
4. **Легкое управление** помогает **сделать более прозрачным IT** затраты, освободить ресурсы для выолнения ключевых бизнес-задач, вместо командировок.

Ключевые преимущества

Интуитивные операции

Создать один раз, использовать везде (за секунды)

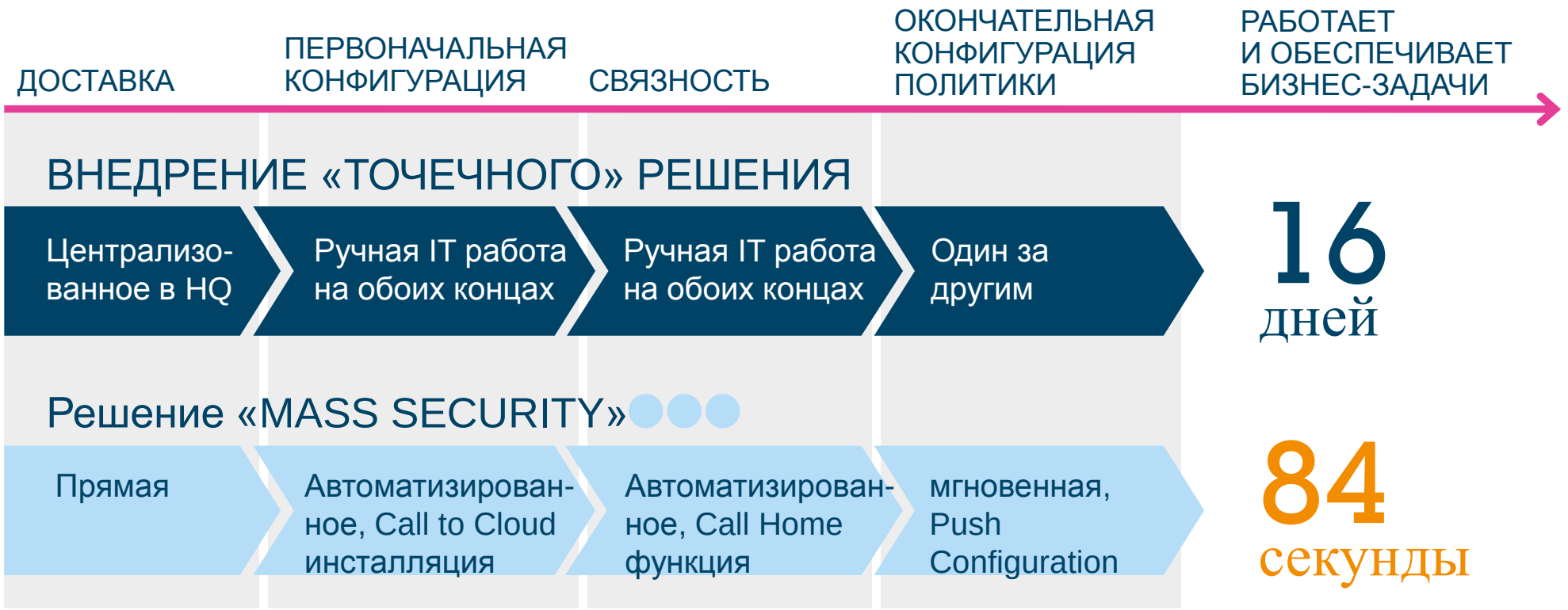
Нет нужды в локальном IT администраторе

Отказоустойчивый, защищенный от человеческих ошибок, всегда up-to-date

Быстрее

Почему это быстрее?

Пример: обеспечение связности между HQ и 500 удаленными сайтами



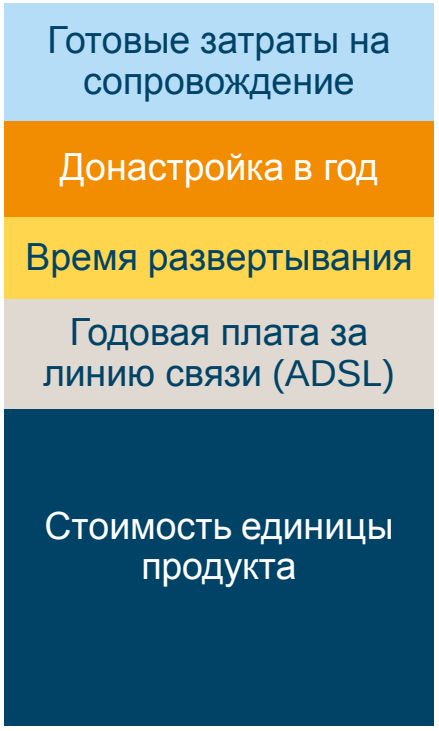
STONESOFT

Дешевле

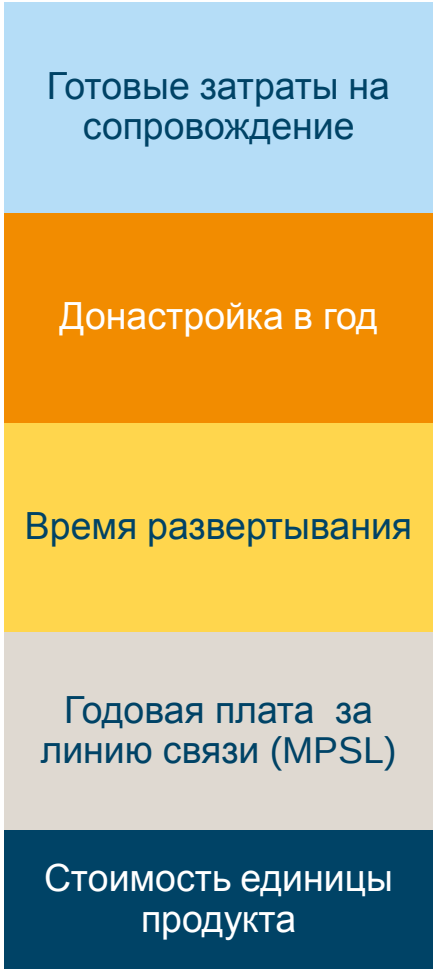
Почему это дешевле?

Пример: 500 сайтов
TCO после 3-х лет

- Время/стоимость на сайт
- 15 новых сайтов в год



Решение MASS SECURITY
Профиль затрат



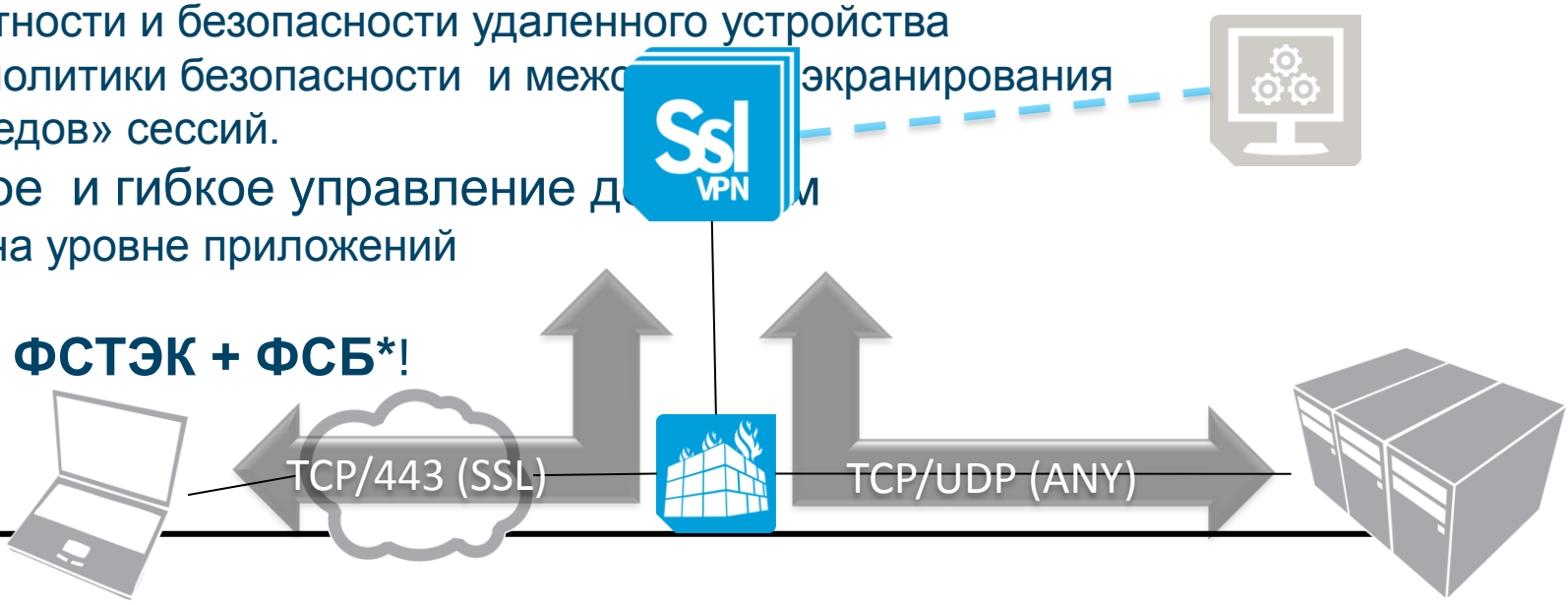
Точечное решение
Профиль затрат

Современное решение – это:

- Высокие скорости
- Отказоустойчивость во всем
- Распределенность
- **Поддержка «облачных» сервисов**
- **Поддержка управляемых услуг безопасности**
- «Реальная» защита
- Соответствие требованиям регуляторов

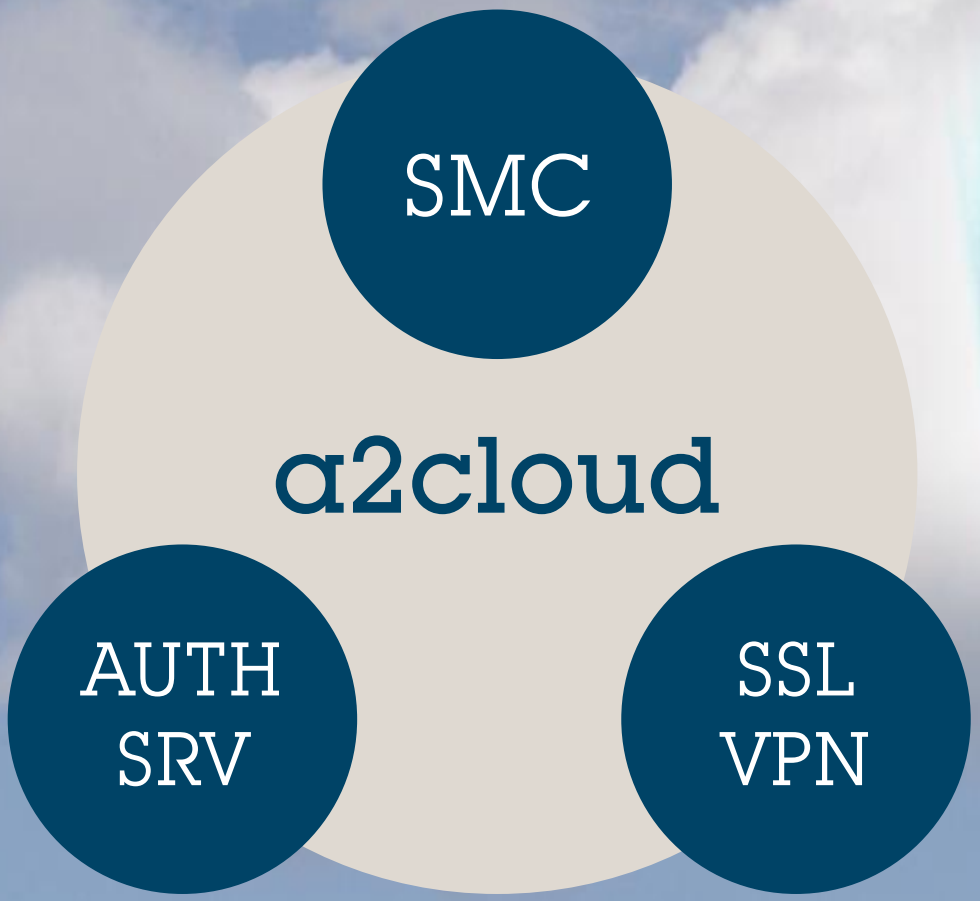
Первое в России сертифицированное решение StoneGate SSL VPN

- Безопасный доступ из любой точки, в любое время с любых устройств (нужен только TCP/443!)
- 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
  - Только доверенные соединения
  - Анализ целостности и безопасности удаленного устройства
  - Применение политики безопасности и межсетевого экранирования
  - Удаление «следов» сессий.
- Гранулированное и гибкое управление доступом
  - Авторизация на уровне приложений
- **Сертификация ФСТЭК + ФСБ***!

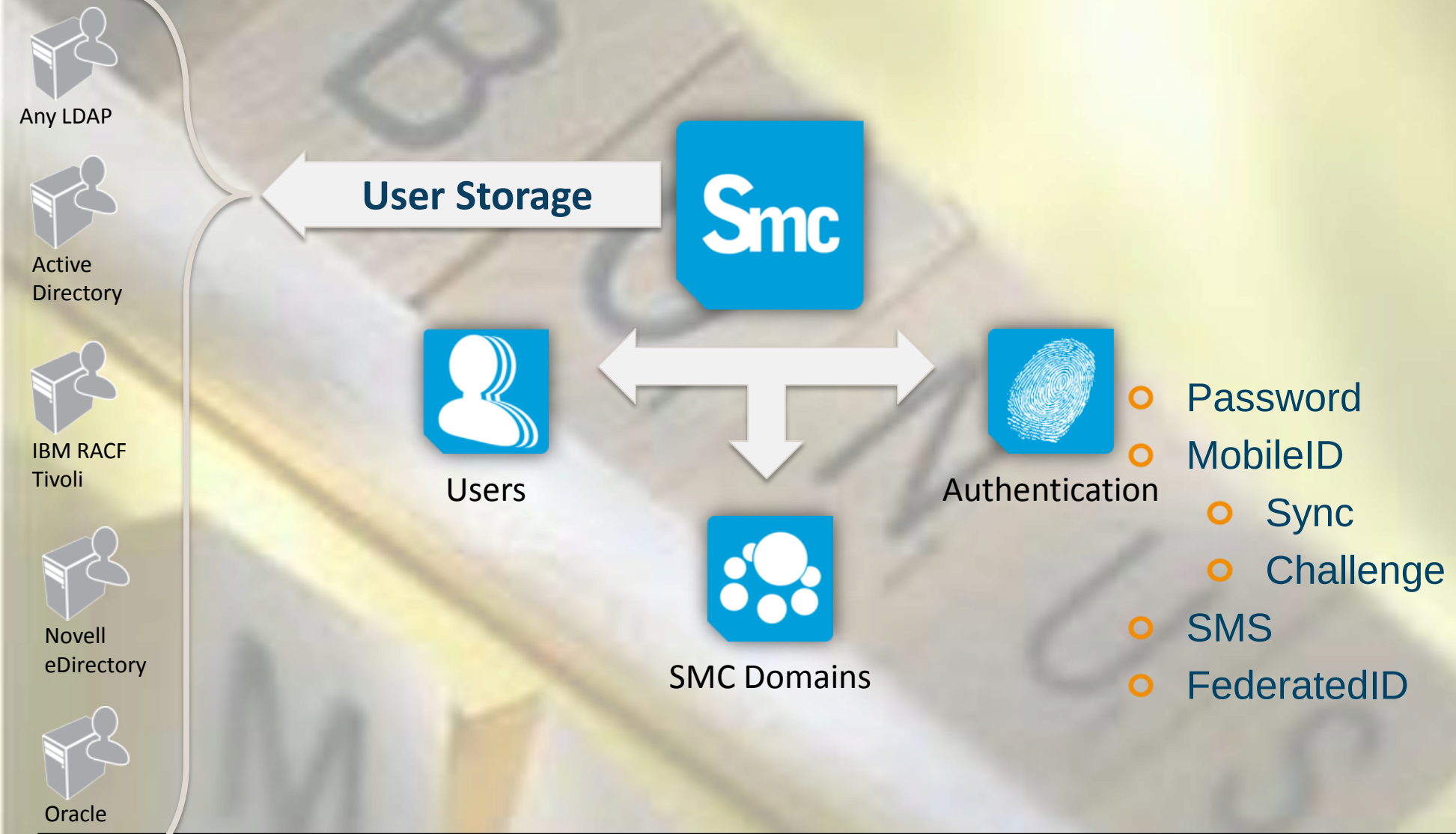


STONESOFT

Комбинация технологий

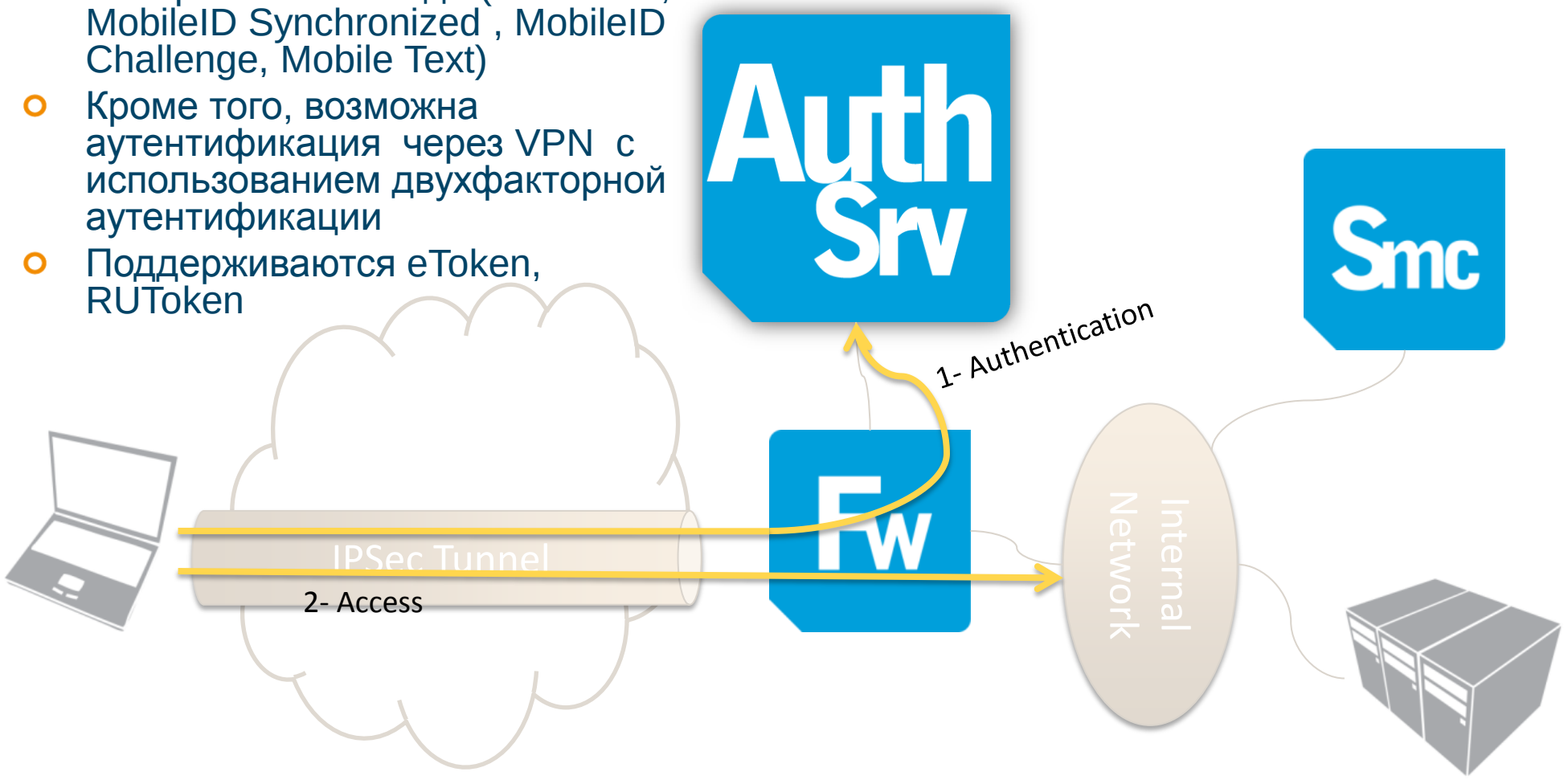


Центр аутентификации встроен в SMC



Разные сценарии аутентификации

- 4 встроенных метода (Password, MobileID Synchronized , MobileID Challenge, Mobile Text)
- Кроме того, возможна аутентификация через VPN с использованием двухфакторной аутентификации
- Поддерживаются eToken, RUToken



Пример:

ДОСТУП К ПУБЛИЧНОМУ ОБЛАКУ (АУТ-ЦИЯ «ДОМА»)

Проблемы

- Доступ к веб-сервисам без потери контроля над аутентификацией
- Ограничить распространение данных пользователей через Интернет
- Обеспечить интероперабельность системы аутентификации

Требования

- Не изменять приложения
- Усилить методы аутентификации (не простой логин/пароль)
- Доступ к разным веб-сервисам без ограничений
- Использовать интегрированную аутентификацию

выгоды

- Полный контроль над процессом аут-ции
- Доступ к частным и публичным сервисам с помощью SSO (single sign-on)
- Доступ к CRM, почте и др. приложениям с помощью методов интегрированной аутентификации

Пример:

ЧАСТНОЕ ОБЛАКО И ДОСТУП СОТРУДНИКОВ/ПАРТНЕРОВ

Проблемы

- Сохранить сильную аутентификацию без ущерба для usability и эргономики
- Оценка соответствия подключающегося клиента
- Разрешать/запрещать соединения в зависимости от контекста

Требования

- Сократить расходы на токены
- Улучшить usability
- Проверять не только данные аут-ции, но и *контекст соединения*, состояние антивируса, наличие патчей ОС и пр.

Выгоды от решения

- Безопасные подключения с проверкой соответствия политике безопасности
- Легкая, эргономичная аутентификация

Пример:

ПРОВАЙДЕР УСЛУГ АУТЕНТИФИКАЦИИ

Проблемы

- Предоставление данных в разных форматах разным пользователям
- Независимость от клиентских систем и приложений
- Предложить несколько методов аутентификации без использования новых устройств пользователями

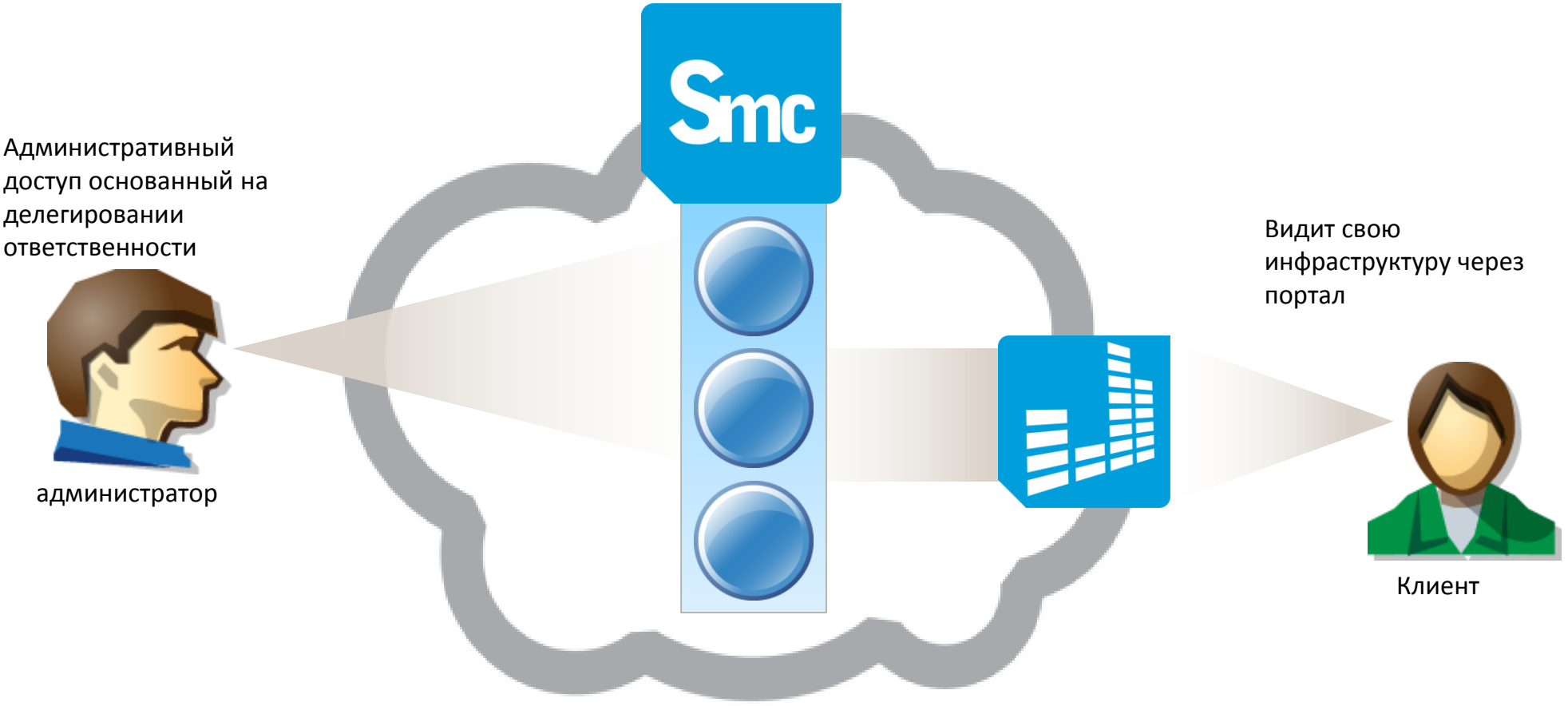
Требования

- Быть в курсе событий, журналы, статистика, аудит
- Поддержка стандартов интегрированной аутентификации
- Дешевые токены
- Стойкая аутентификация

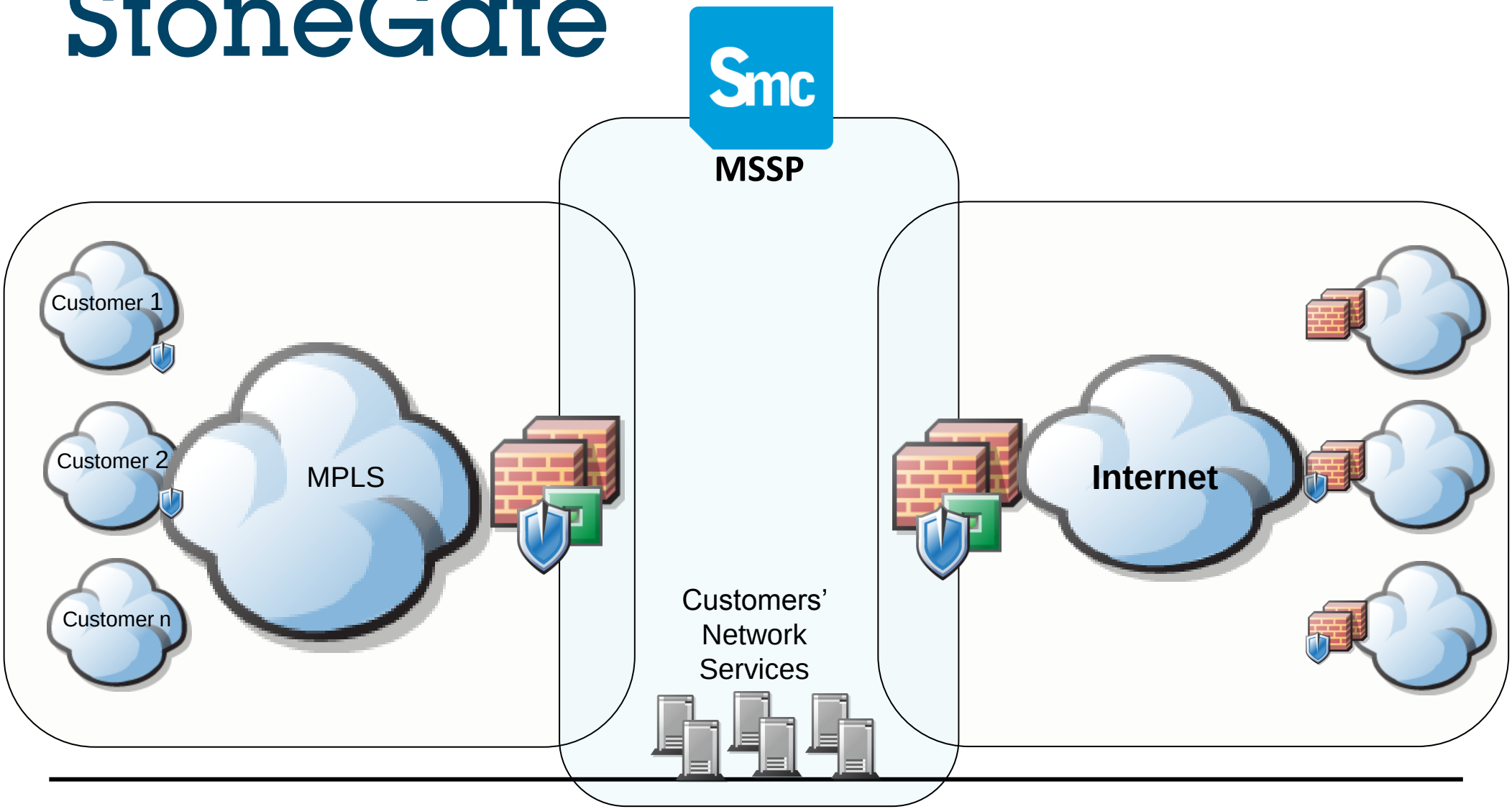
Выгоды от решения

- Сильные методы аутентификации
- Соответствие требованиям стандартов
- Поддержка Federated ID
- Бесплатные программные токены и аутентификация через sms

Готовое решение по предоставлению **MSSP** услуг



Предоставление сервисов с помощью платформы StoneGate



Современное решение – это:

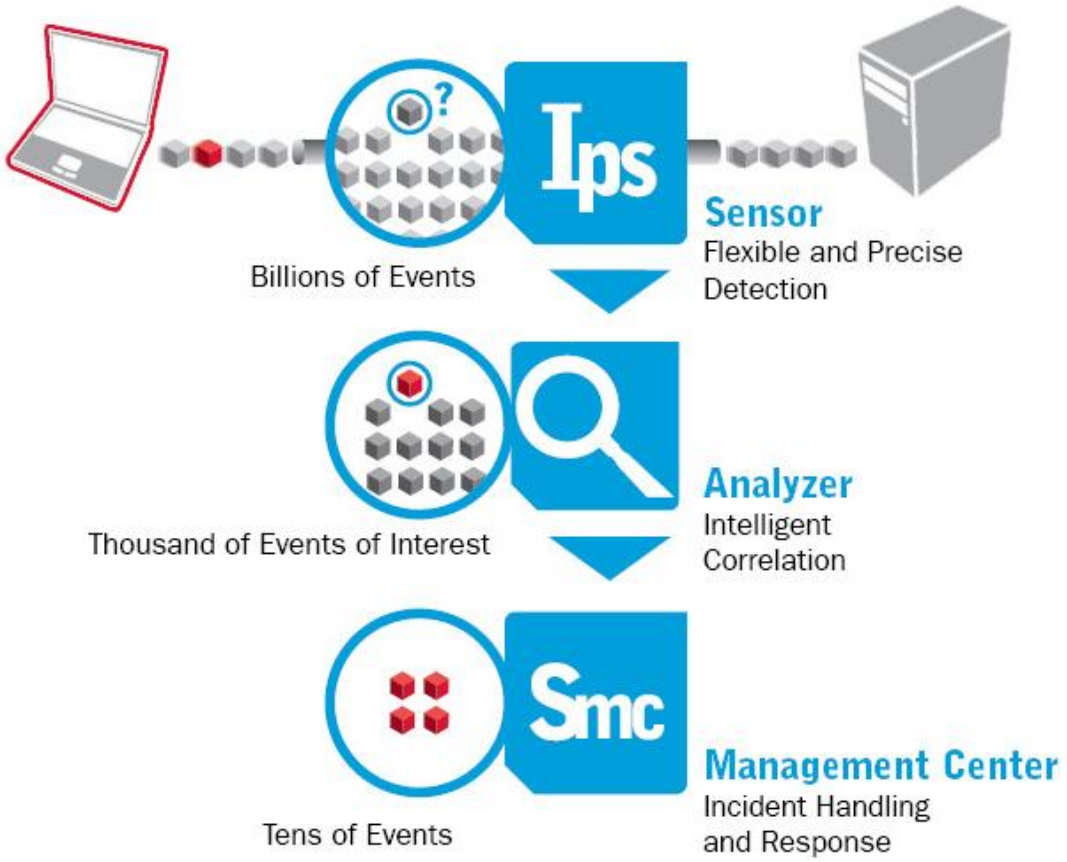
- Высокие скорости
- Отказоустойчивость во всем
- Распределенность
- Поддержка «облачных» сервисов
- Поддержка управляемых услуг безопасности
- **«Реальная» защита**
- Соответствие требованиям регуляторов

StoneGate UTM для удаленных офисов

- antispyware? YES
- antiadware? YES
- antiphishing? YES
- antivirus? YES
- antispam? YES
- URL Filtering with DB? YES
- web content inspection? YES
- HTTP inspection YES
- VoIP Security YES
- QoS YES
- HTTPS (SSL) inspection YES
- IPS (AET ready) YES
- Multilink VPN YES
- Application Identification YES
- **и многое др., чего нет в традиционных UTM**

STONESOFT

Безопасность от StoneGate



Идентификация

- **Пользователей**
- **Приложений**

Защита от угроз

- Buffer overflow, DoS/DDoS
- Worm, Trojan, Backdoor
- Port Scan, P2P & VoIP attack
- Protocol, Application & Statistical anomaly

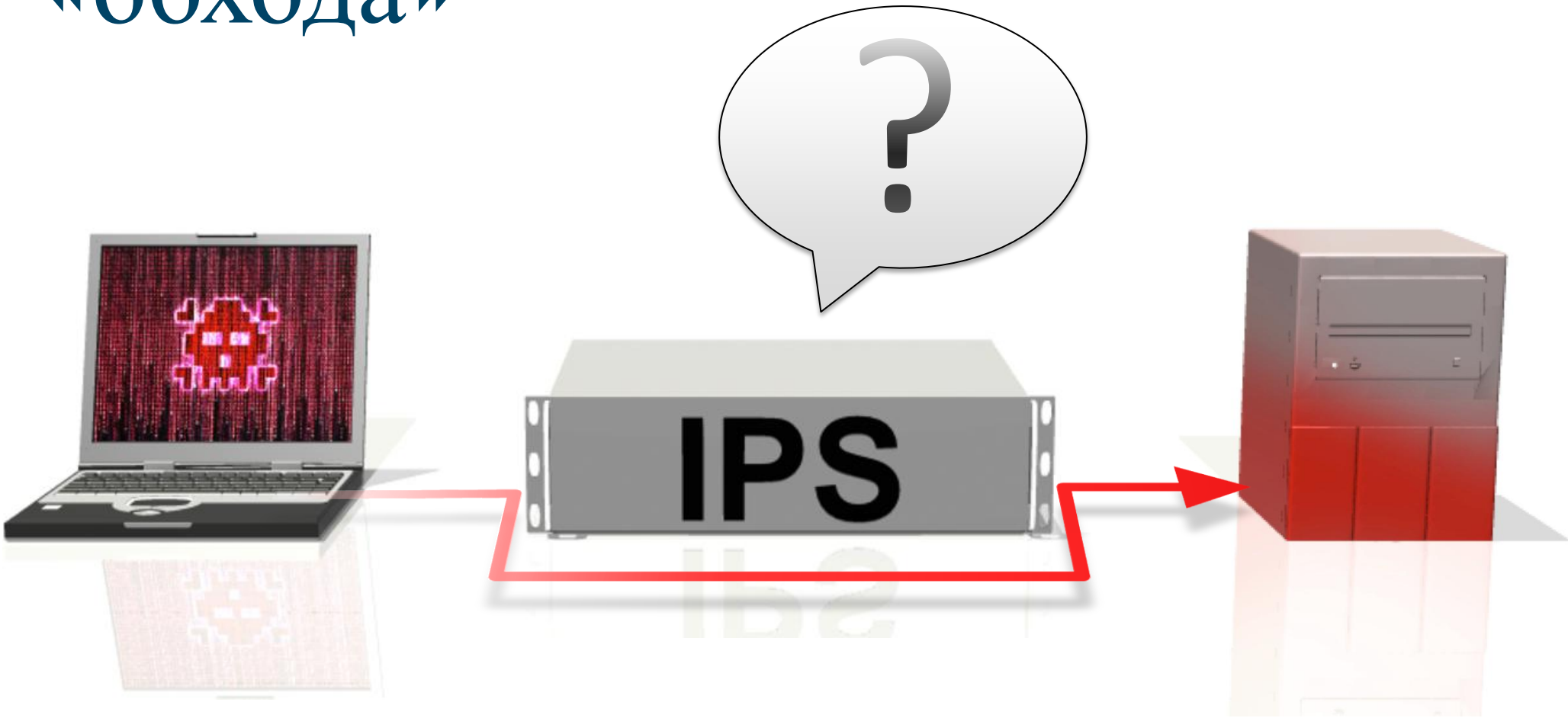
Защита от обхода!

- **Защита от традиционных и динамических техник обхода (АЕТ)**

Насколько «традиционные» решения эффективны?

Нет, если они не защищают от техник обхода (АЕТ)

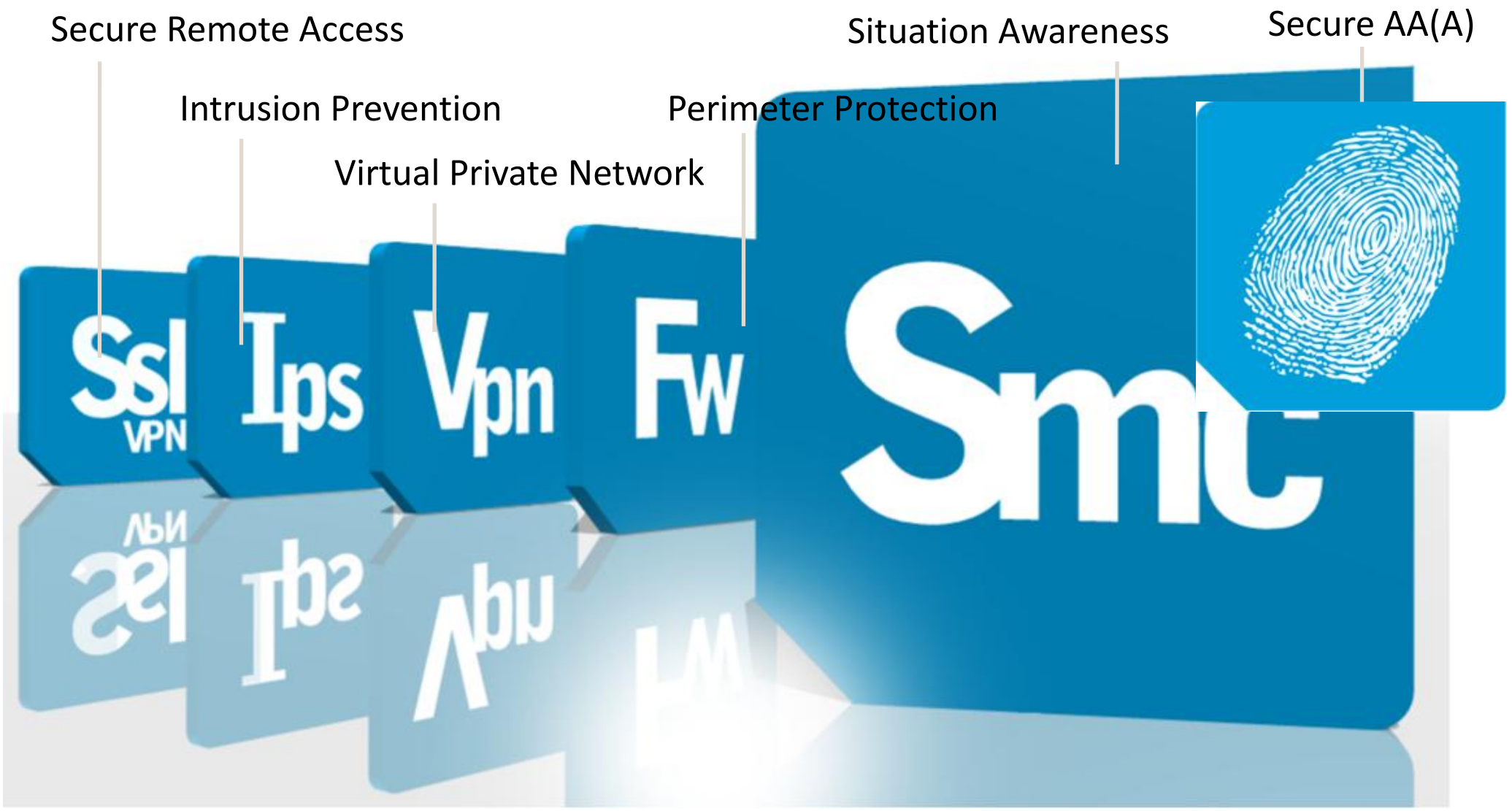
Базовый принцип техники «обхода»



Современное решение – это:

- Высокие скорости
- Отказоустойчивость во всем
- Распределенность
- Поддержка «облачных» сервисов
- Поддержка управляемых услуг безопасности
- «Реальная» защита
- **Соответствие требованиям регуляторов (всех)**

Портфолио StoneSoft



Сертифицированные и проверенные на практике

Сертификации производства по ФСТЭК:

- Межсетевой экран StoneGate сертифицирован по 2 классу для МЭ, 1 класс ПДн, 1Г, 4 класс НДВ
  - в составе МЭ сертифицированы по ТУ встроенные антивирус, механизм инспекции трафика Deep Inspection и др.
  - в составе МЭ сертифицирован VPN клиент как часть распределенного МЭ
- StoneGate IPS сертифицирована как прозрачный МЭ 3 класса, а также по ТУ как IPS, 1 класс ПДн, 1Г, 4 класс НДВ.
  - По ТУ сертифицированы механизмы предотвращения вторжений, анализ аномалий, виртуальный патч и др.,
- Шлюз защиты удаленного доступа StoneGate SSL* – 3 класс МЭ, 1класс ПДн, 4 класс НДВ.
  - В составе сертифицирована система многофакторной аутентификации!

В составе каждого средства защиты как компонент сертифицирован центр управления! А также сертифицирована версия продуктов для виртуальной среды!

Особенности сертификации ФСБ

- Сертифицируются решения SSL VPN и IPSEC VPN (с VPN клиентом)
- Классы защиты **КС1 – КС3!**
- SSL VPN – 9 исполнений!
- IPSec VPN - 11 исполнений!

(поддержка МАРШ, различные операционные системы)

SSL VPN поддерживает работу на клиентском компьютере – Crypto Pro, ValiData.

Тестируется совместимость: Signal-Com, VipNet (TLS).

Защита персональных данных

Требования	Компоненты решения StoneGate					
	SG FW	SG IPS	SG SSL VPN	SG VPN	SG VPN client	Management
Управление доступом	+	+	+			+
Регистрация и учет	+	+	+			+
Обеспечение целостности	+		+	+	+	
Межсетевое экранирование	+	+	+		+	
Обнаружение вторжений	+	+				
Антивирусная защита	+					
Анализ защищенности			+			
Криптографическая защита			+	+	+	

Защита персональных данных

Требования	Компоненты решения StoneGate					
	SG FW	SG IPS	SG SSL VPN	SG VPN	SG VPN client	Management
Двухфакторная аутентификация			+	+	+	+
Управление инцидентами						+
Восстановление и отказоустойчивость	+	+	+	+	+	+
Централизованный мониторинг всей инфраструктуры и сбор событий с любых устройств						+
Управление и оптимизация информационных потоков	+	+	+	+		
Защита от DoS/DDoS	+	+				
Защита от Malware	+	+				
Контентная фильтрация	+	+				
Обеспечение защиты от утечек		+				

«Положение о методах и способах защиты информации в ИСПДн»
(Приказ директора ФСТЭК России от 05.02.10 № 58)

Межсетевое экранирование	**StoneGate Firewall, IPS , VPN Client , SSL Access agent.**
Система антивирусной защиты	**Firewall (UTM)**
Защита информации по каналам	**SSL VPN, IPSEC VPN**
обнаружение вторжений (IPS)	**IPS, Firewall**
анализ защищенности	**Сторонними приложениями**
идентификация и аутентификация	**SSL VPN , Authentication Server**
Система Аудита и журналирования	**SMC**
Защита рабочей станции	**Stonesoft Security Suite (скоро) или сторонние приложения и средства**

STONESOFT

Выполнение требований стандарта Payment Card Industry (PCI)

Пункты требований
1.x.x – полноценное межсетевое экранирование
2.2. – отключение ненужных сервисов и др.
4.1. – защита с помощью шифрования в канале связи
6.1 – технология Virtual Patching
6.2 – управление уязвимостями
6.6 – функциональность Web Application Firewall
8.2 – идентификация всех пользователей и ресурсов
10.3.1 идентификация пользователей
10.6 – управление логами
11.4 – полноценная IDS / IPS

Причины выбора Stonesoft

	Возможности Stonesoft	Экономия
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%**

Самый низкий TCO

- Управление следующего поколения **(NGM)=** уменьшение затрат на администрирование
- Доступность и масштабируемость следующего поколения **(NGA&S)=** уменьшение затрат на оборудование,
инфраструктуру и коммуникациии
- Разница между понятиям «**Built-in**» (встроенный) и «**bolt-on**» (притянутый)

StoneGate можно включать!

- А еще

Мир становится сложнее.

Мы делаем Безопасность

Легкой

STONESOFT

Secure Information Flow