STONESOFT

Формальная и реальная безопасность: как построить систему защиты для будущего?

Как построить высокоэффективную систему защиты с выполнением всех требований законодательства

Михаил Романов

Типичные проблемы

- Нет политики ИБ
- Нет модели угроз
- «Зоопарк» в сети
- Недостаточное финансирование
- Разное толкование требований регуляторов, а также изменения законодательства
- Малые сроки на внедрение, не смотря на неоднократный перенос сроков
- Унаследованные лоскутные решения
- Проприетарные протоколы
- Большое количество мобильных устройств

Типичные угрозы

- Вредоносное ПО (вирусы , фишинг и др..)
- Деятельность кибер-ОПГ (адресные целенаправленные атаки)
- Реакция регуляторов на нарушения законодательства по ПДн
- Размытый периметр безопасности
- Низкая культура ИБ у пользователей и контрагентов
- Ошибочные действия администраторов или саботаж
- Расходы на поездки в дальние филиалы на настройки или перенастройки
- Низкая доступность (отказоустойчивость) сервисов

Муки выбора, или в поисках баланса

- Злоумышленники или регуляторы: кто страшнее?
- Функциональность или сертификат?
- Недорого или работоспособно?
- Поставить “рядом”или интегрировать в инфраструктуру?
- Теперь есть персональный ответственный за защиту ПДн....!

Как сейчас строится защита?

- Рабочее место :
- СЗИ НСД (Secret Net, Accord, DallasLock…)
- Антивирус
- Персональный файрвол ? (чаще не ставят)
- Система HOST IPS (чаще обходятся антивирусом)
- Защита портов (Device Lock и др…)
- VPN client (часто с криптографией своей)
- Криптобиблиотеки (CSP)
- Ключи типа Aladdin (Рутокен) для хранения ключей
- различные «пробы», агенты от других систем …..

Как сейчас строится защита?

а еще :

- Firewall
- Antispam
- URL Filtering
- СЗИ НСД в сети ….
- Контроль принтеров – стали приспосабливать DLP
- Система аутентификации
- Каталог (AD. LDAP, метакаталог …..)
- HoneyPot (ставят только маньяки)
- Шифраторы Шлюзы (IPSEC и другие)

Нужны нормальные сертификаты

- Сертификат № 1774
- **Microsoft Windows Vista с Service Pack 1**. Задание по безопасности OEM_MS.Win_Vista_SP1.3Б. Версия 1.0, 2008", имеет **оценочный уровень доверия ОУД 1 (усиленный)**

- **Выписка из руководящего документа :**

ОУД1 применим, когда требуется некоторая уверенность в правильном функционировании, а угрозы безопасности не рассматривают как серьезные.

При оценке на этом уровне следует предоставить свидетельство, что ….. предоставляет приемлемую защиту против идентифицированных угроз.

Вы поняли, о чем этот сертификат?

Изменения в ФЗ "О персональных данных“: что изменилось в части технических требований?

Статья 19. Меры по обеспечению безопасности персональных данных при их обработке (в ред. ФЗ от 25.07.2011 N 261-ФЗ):

Пункт 2. Обеспечение безопасности ПДн достигается, в частности:

1) определением угроз безопасности ПДн при их обработке в ИСПДн;
2) применением организационных и технических мер по обеспечению безопасности ПДн при их обработке в ИСПДн, необходимых для выполнения требований к защите ПДн, исполнение которых обеспечивает установленные Правительством РФ **уровни защищенности ПДн**;
3) **применением прошедших в установленном порядке процедуру оценки соответствия** средств защиты информации;
4) **оценкой эффективности принимаемых мер** по обеспечению безопасности ПДн до ввода в эксплуатацию ИСПДн;
5) учетом машинных носителей персональных данных;
6) обнаружением фактов НСД к ПДн и принятием мер;
7) восстановлением ПДн, модифицированных или уничтоженных вследствие НСД;
8) установлением правил доступа к ПДн, обрабатываемым в ИСПДн, а также обеспечением регистрации и учета всех действий, совершаемых с ПДн;
9) контролем за принимаемыми мерами по обеспечению безопасности ПДн и уровня защищенности ИСПДн.

«Положение о методах и способах защиты информации в ИСПДн»

(Приказ директора ФСТЭК России от 05.02.10 № 58)

При взаимодействии ...с ...сетями международного информационного обмена (сетями связи общего пользования) ……**основными методами и способами защиты информации от НСД являются**:

- **межсетевое экранирование** с целью управления доступом, фильтрации сетевых пакетов и **трансляции сетевых адресов** для скрытия ИС;
- **обнаружение вторжений** в информационную систему, нарушающих или создающих предпосылки к нарушению установленных требований .....;
- **анализ защищенности** информационных систем, предполагающий применение специализированных программных средств (сканеров безопасности);
- защита информации **при ее передаче по каналам связи**;
- **использование смарт-карт**, электронных замков и др. носителей информации для **надежной идентификации и аутентификации** пользователей;
- использование средств **антивирусной защиты**;
- **централизованное управление системой защиты персональных данных** информационной системы.

Выполнение других стандартов и требований

Кроме закона о персональных данных есть требования других стандартов по ИБ:

- Стандарт Центрального Банка России
- СТР – К (построение систем, обрабатывающих конфиденциальную информацию и ДСП и др…)
- Отраслевые стандарты (КСИИ и др.)
- Требований международных стандартов (SoX, HIPAA, PCI DSS и др.)
- Требования нормативных документов ФСБ России
- Ведомственные документы

а что в будущем ?

- Стандартизация является трендом и в будущем требования различных регуляторов будут только расти
- Сращивание технологий (FW + IPS, AV + PFW…..)
- Более целенаправленные атаки и все больше целевых атак (коммерциализация хакерства)
- Больше сложных систем – больше цена эксплуатации и более высокая цена ошибки .
- Требуется все более короткое время на реагирование на инциденты
- Безопасность постепенно уходит в область сервисов предоставляемых профессиональными компаниями .
- Более сложные системы – должны стать более простыми в эксплуатации или они становятся бесполезными.

Возьмите все сразу

- Реальная защита
- Высокая производительность
- Отказоустойчивость до 0.99999
- Автоматическая балансировка нагрузки
- Наглядное централизованное управление
- Сертификация производства
- Широкая линейка устройств

ICSA labs CERTIFIED NETWORK IPS

ArcSight An HP Company CERTIFIED CEF COMPLIANT

ICSA labs CERTIFIED FIREWALL - CORPORATE

NSS Labs Security. Certified.

Common Criteria

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).

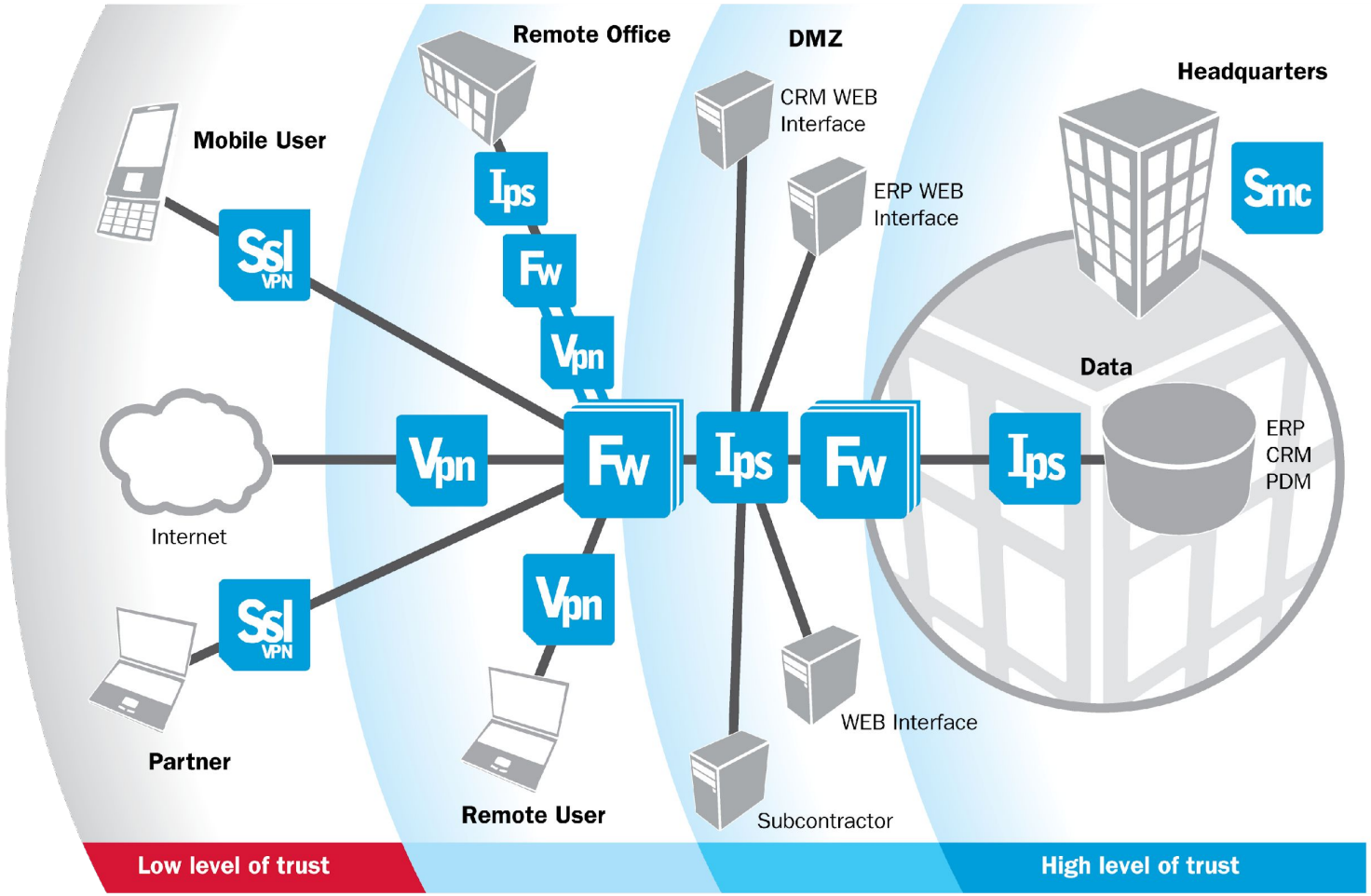
Защита персональных данных

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			+	+	+	

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

Комплексный подход



STONESOFT

Требования по 58 приказу

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

Обеспечение безопасности

- Защита периметра с управлением приложениями!
- Защита 10G каналов по ГОСТ !
- Обеспечение непрерывности бизнеса (полная отказоустойчивость)
- Гибкая защита критичных бизнес-приложений с анализом контента
- Защита распределенных офисов – простое управление 1000+ устройствами из одного центра !
- Эффективное управление инцидентами
- Защита от новейших угроз (в т.ч. AET)
- Безопасный удаленный доступ (мобильный офис)
- Мощная система аутентификации с системой аудита

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

STONESOFT

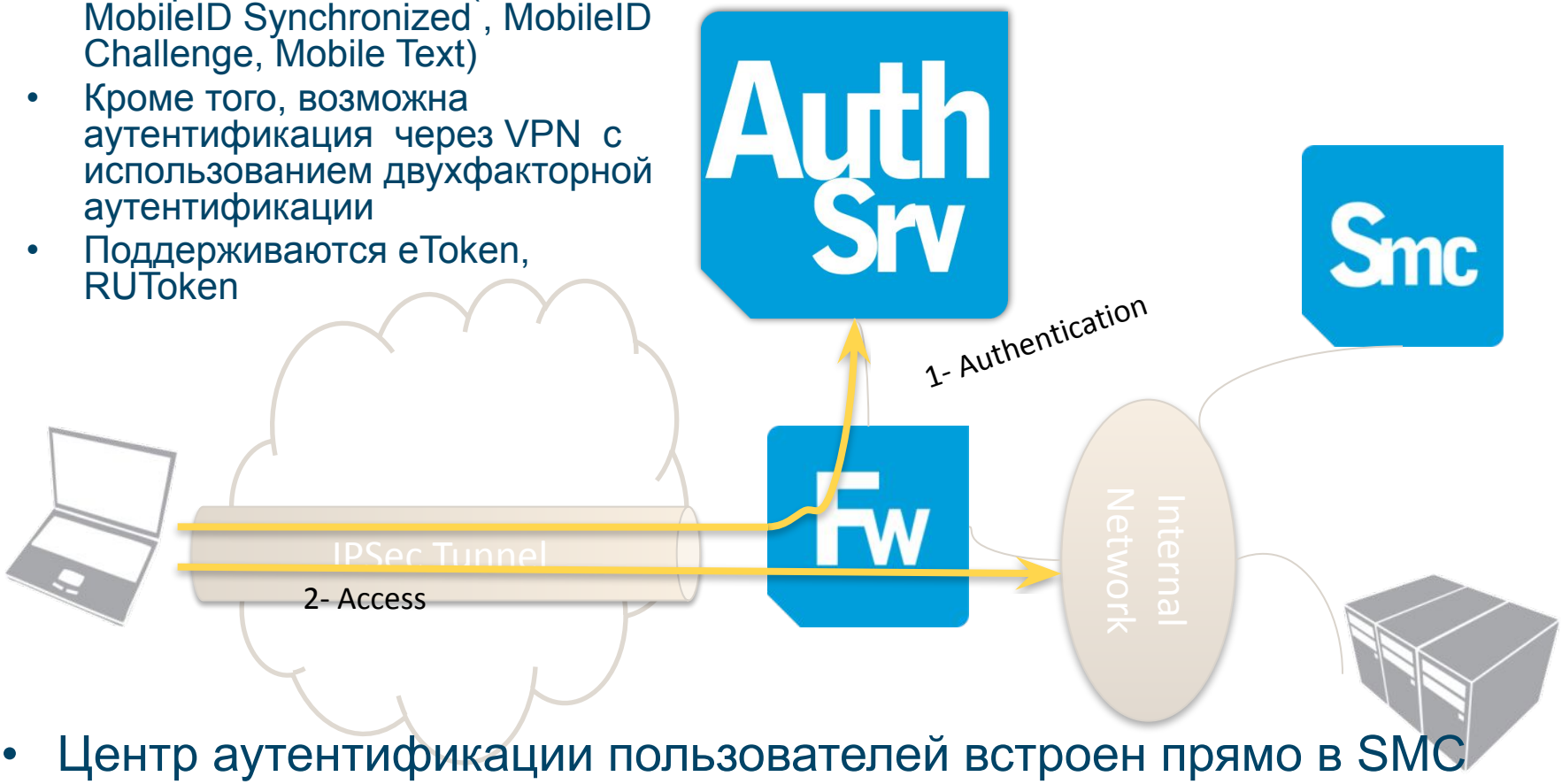
Требования по хранению логов

- Большинство требований стандартов и ведомственных документов требует хранить лог информацию для разбора в дальнейшем инцидентов безопасности и случаев несанкционированного доступа.
- SMC совместно с LOG Server может использоваться именно для этих целей
- Надежное хранилище – масштабируемое и простое в эксплуатации
- Сохранение и управление лог информацией, собираемых со сторонних устройств …

Требования	Длительность хранения
SOX	7 лет
PCI	1 год
EU DR Directive	2 года
Basel II	7 лет
HIPAA	6/7 лет
СТО БР	5-7 лет
Ведомственные	3 года

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



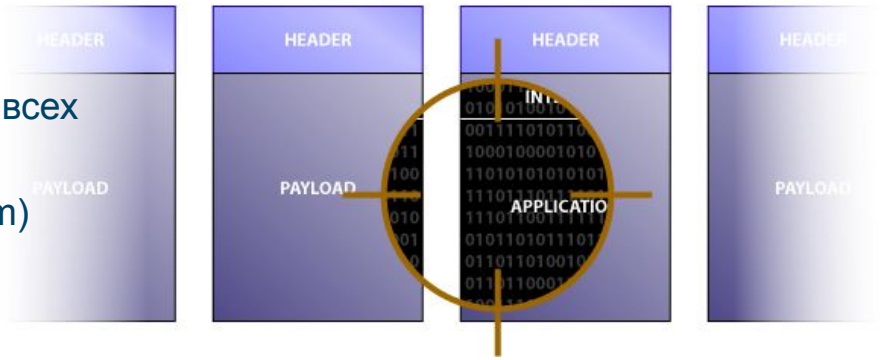
- Центр аутентификации пользователей встроен прямо в SMC

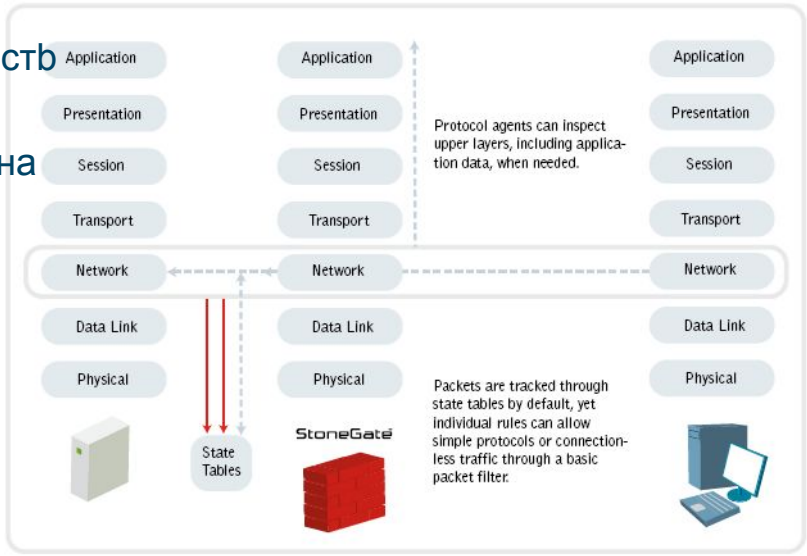
Next Gen Firewall

- Multi-Layer Inspection ™
- Прокси для приложений, stateful inspection технология, определение приложений, анализ на всех уровнях и др.
- UTM возможности (AV, IPS, Web Filtering, AntiSpam)
- Поддержка критических технологий
  - VoIP, video конференции и др.

  Технологии QOS , Load Balancing , Multilink приоретезация потоков, обеспечение непрерывность потоков информации

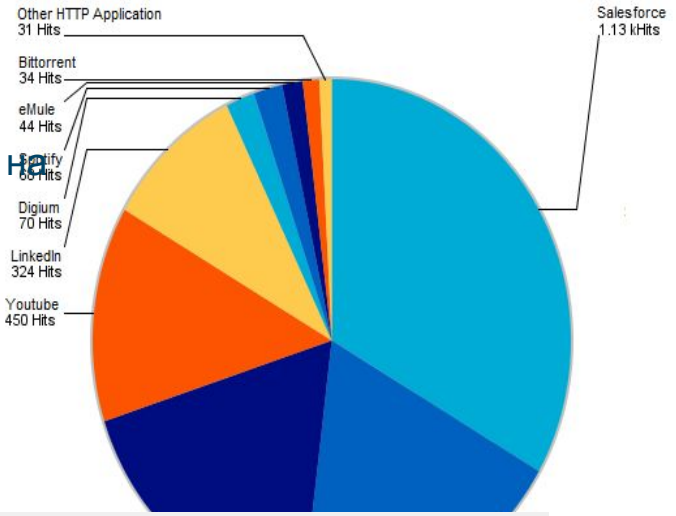
  Работа в качеств распределенного межсетевого экрана вместе с VPN клиентом
- SSL инспекция в обоих направлениях
- Обеспечение динамической идентификации пользователей
- Анализ контента





Идентификация приложений

- Теперь можно динамически определять, какое приложение работает в сети, и разрешать или обеспечивать заданную полосу пропускания данному приложению. Хосты можно описывать как URL ссылки …..
- Приложения независимо от протоколов ….
- Принятие решения о доступе может также осуществляться на основе учетных записей, названий служб и приложений
- А также с учетом времени аутентификации, расписания работы хоста и др. Для остальных сотрудников можно, например, разрешить использование Интернет, но не загружая основную полосу пропускания .



IPv4 Access | IPv6 Access | IPv4 Inspection | IPv4 NAT | IPv6 NAT

ID	Source	Destination	Service	Action	QoS Class
13.1.1	Workstation Administrators	RAD, Marketing, Presales, Sales	Remote Desktop	Allow	
13.1.2	Any network	www.stonesoft.com	HTTP, HTTPS	Allow	
13.1.3	Presales, Sales	www.facebook.com	Facebook	Allow	Low Priority
13.1.4	RAD	Any network	Spotify	Discard	
13.1.5	Internal Zone	Any network	HTTP_BrightCloud-Adult-and-Pornography, HTTP_BrightCloud-Gambling, HTTP_BrightCloud-Games	Discard	
Discard all					

STONESOFT

Управление большими конфигурациями

1. **Plug & Play инсталляция** новых экранов в удаленных офисах
2. **Policy Push:** немедленное распространение апдейтов на все инсталлированные устройства – без задержек.
3. **Secure & redundant connectivity** через множество ISP/CSP соединений.
4. **Простое управление** помогает **упростить и ускорить IT функции,** минимизируя количество администраторов и освобождая ресурсы для выполнения ключевых задач вместо командировок на места.

Дешевле

Почему это дешевле ?

Пример : 500 сайтов
TCO через 3 года

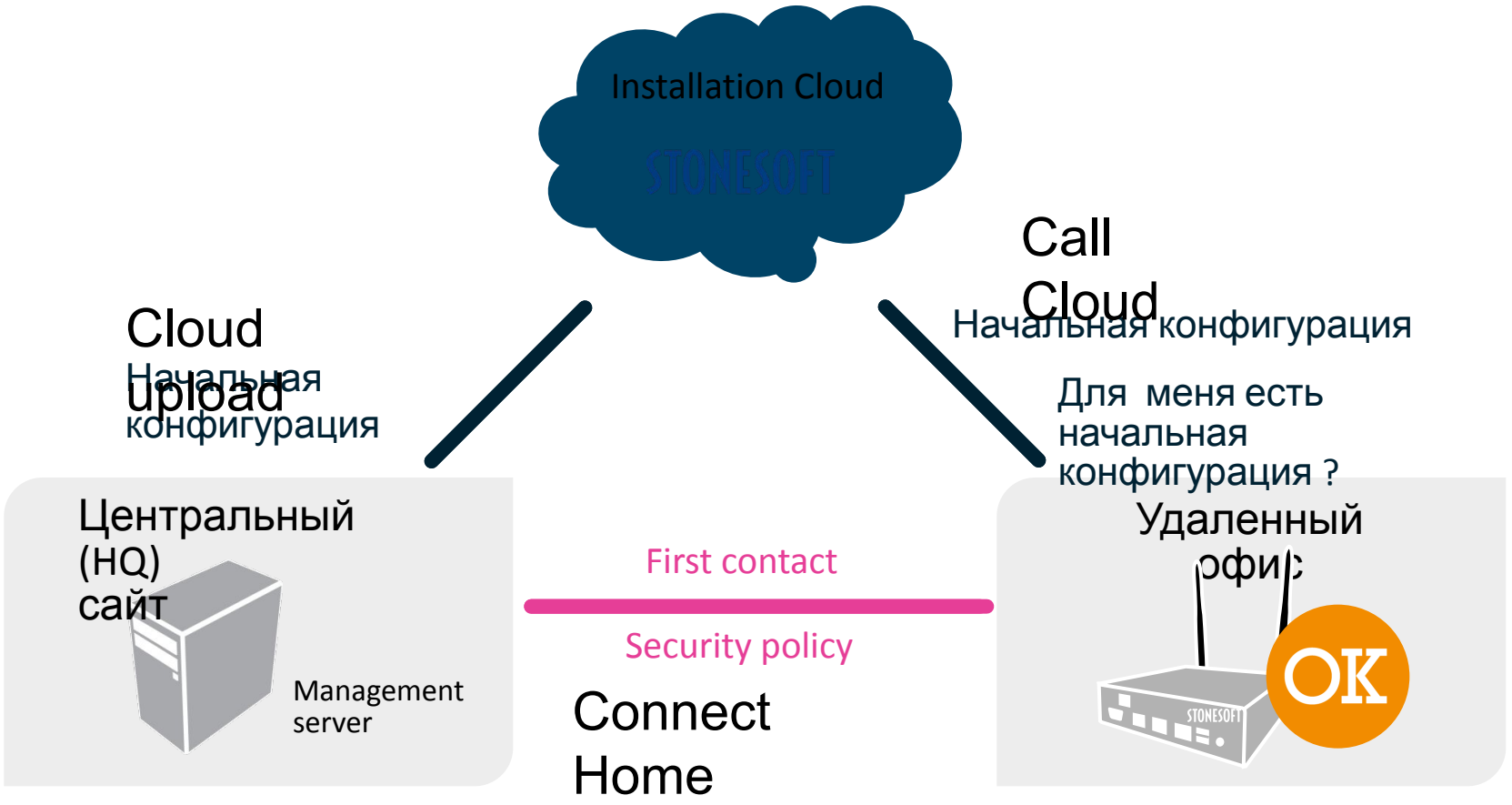
- Время/цена на сайт
- 15 новых сайтов в год

STONESOFT

MASS SECURITY SOLUTION

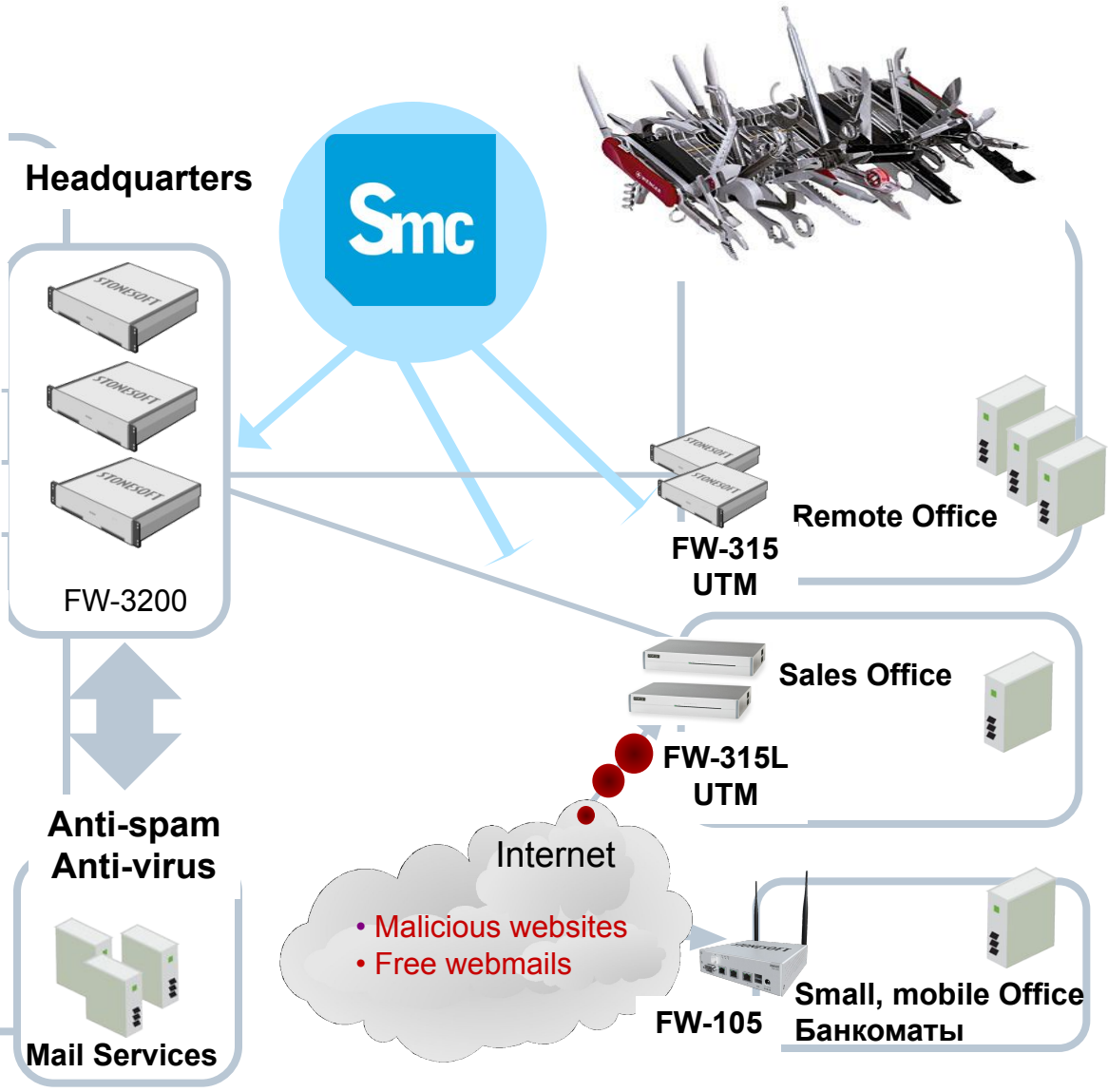
Обычное решение Профиль стоимости

Как это работает



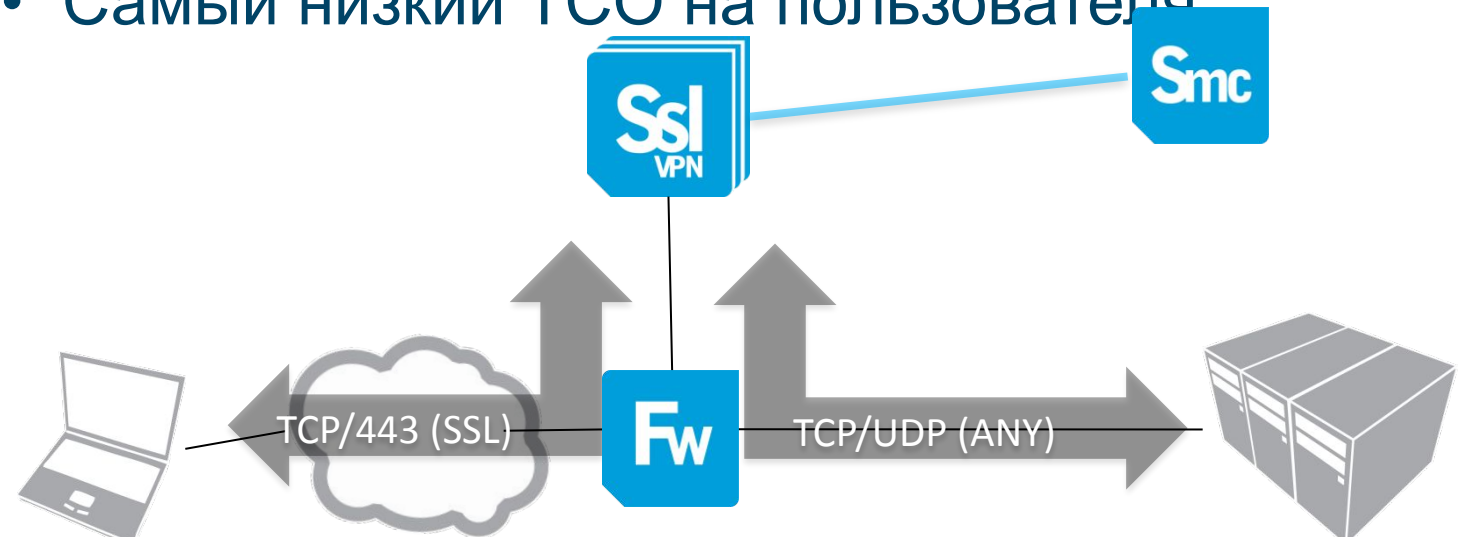
StoneGate UTM для удаленных офисов

- 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**



Безопасный удаленный доступ

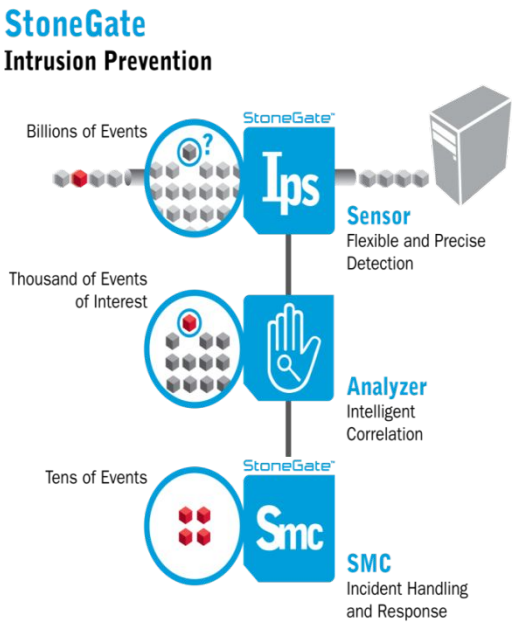
- Отказоустойчивый шлюз
- Бесклиентская технология
- Самый низкий TCO на пользователя



Если организации нужно, чтобы сотрудники имели доступ к своим приложениям с ноутбуков, чужих компьютеров, IPAD, Android и др. без опасений компрометации корпоративных данных..

StoneGate NextGen IPS

Challenge	Solution
Next Generation Security	✔ Закрывает уязвимости ✔ Имела защиту от червя Conficker за два года до его появления ✔ NSS Labs IPS report поставил на #1 по TCO ✔ Zero-day protection (с помощью регулярных выражений) ✔ Множество методов детектирования ✔ SSL инспекция ✔ Полная инспекция IPv6 ✔ Гибридный режим, защита от AET
Performance	✔ Сильно снижает количество ложных срабатываний ✔ Кластеризация



Gartner ICSA labs CERTIFIED NETWORK IPS

VMWARE CERTIFIED VIRTUAL APPLIANCE

NSS approved IPS

Тестирование NSS и ICSA LABS

NSS: Одни из лучших по соотношению цена – качество!

IPS-3205: "At only $38 per Protected-Megabit, the Stonesoft 3205 is an excellent value purchase for enterprises looking to protect DMZs and datacenters. “

IPS-1205: "At only $84 per Protected-Megabit, the Stonesoft 1205 provides the best price per Mbps-protected in the sub-gigabit category and is an excellent value purchase.“

Практически не требует времени на установку, конфигурирование и настройку.

100% защита от evasion техник.

В последнем **тесте ICSA LAB** StoneGate IPS - единственная, которая не выдала ложных срабатываний и показала лучший результат по обнаружению атак.
У ближайшего конкурента Sourcefire были ложные срабатывания.

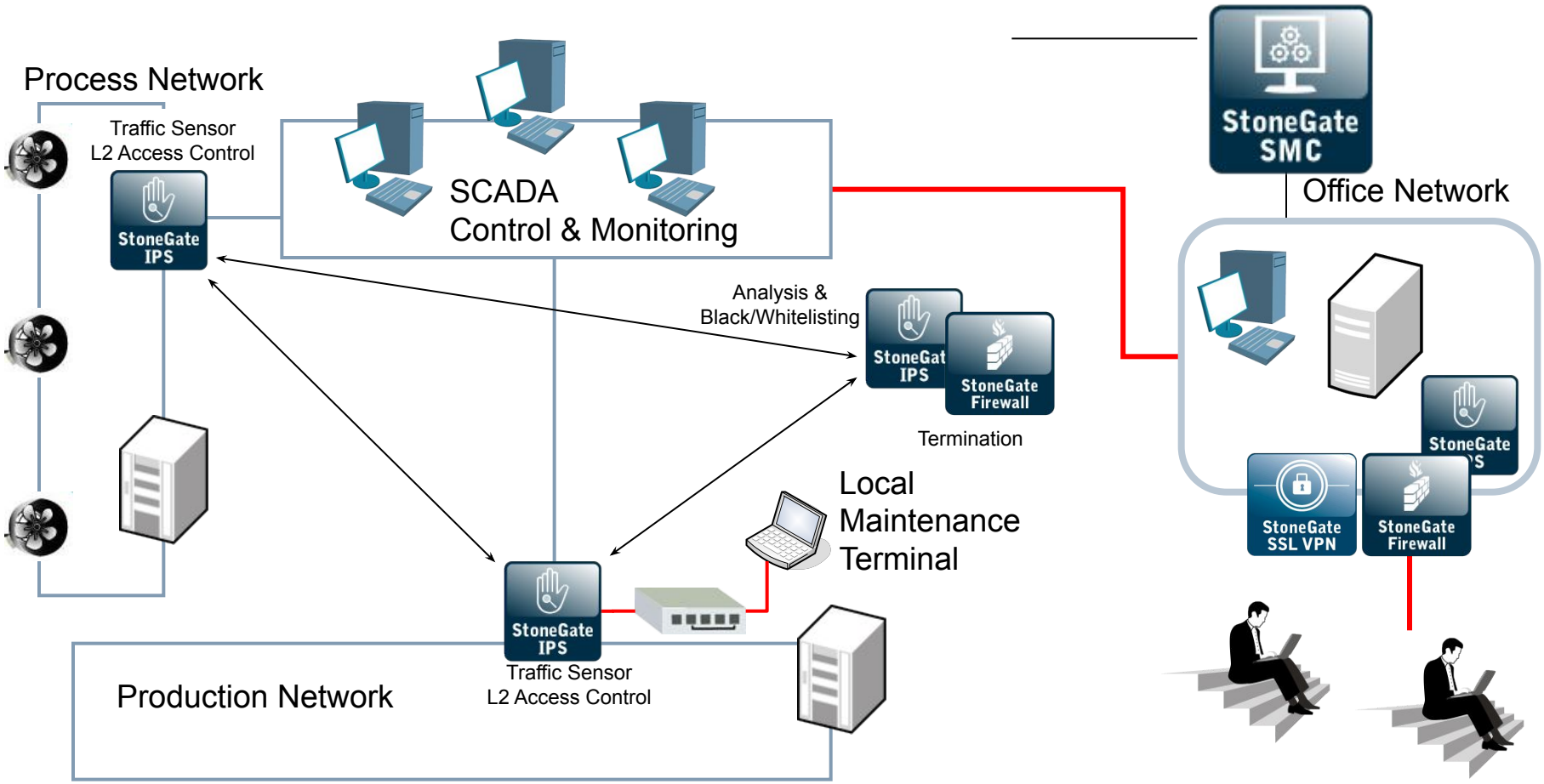
Developer	Product	Q1 Initial Test Run	Q1 Final Test Run
Fortinet	FortiGate-310B	65.6%	81.3%
Sourcefire	3D4500*	59.4%	90.6%
Stonesoft	IPS-1205	78.1%	90.6%
TippingPoint	660N**	71.9%	84.4%
TippingPoint	TP330**	71.9%	84.4%

Пара слов об AET

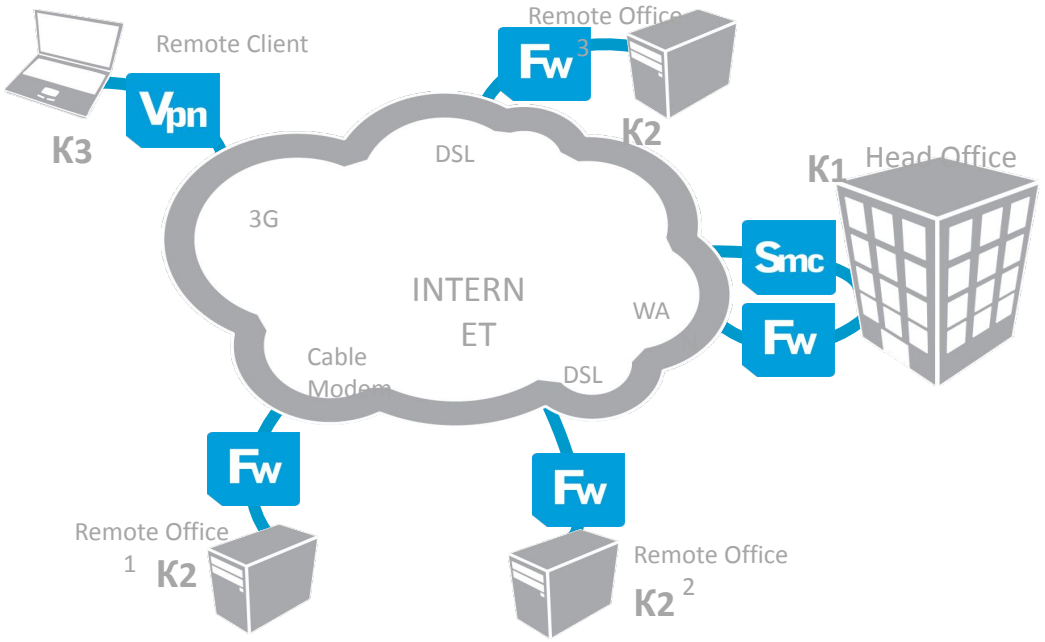
Status of official Vendor information delivered to CERT
Dated: 23.September 2011

Vendor	23 evasions http://www.cert.fi/en/reports/2010/vulnerability385726.html	124 evasions http://www.cert.fi/en/reports/2011/vulnerability487536.html
Cisco	Vendor information: Investigation started. No remediation reported.	No vendor information
Paloalto	No vendor information	No vendor information
Sourcefire	No vendor information	No vendor information
Checkpoint	Vendor information: Not vulnerable	Vendor information: Not vulnerable
Top layer	Vendor information: Investigation started. No remediation reported.	Vendor information: Not vulnerable
McAfee	No vendor information	No vendor information
Juniper	No vendor information	No vendor information
Fortinet	No vendor information	No vendor information
HP/Tipping Point	Vendor information: Not vulnerable	No vendor information

Защита SCADA сетей



Обеспечение отказоустойчивых VPN

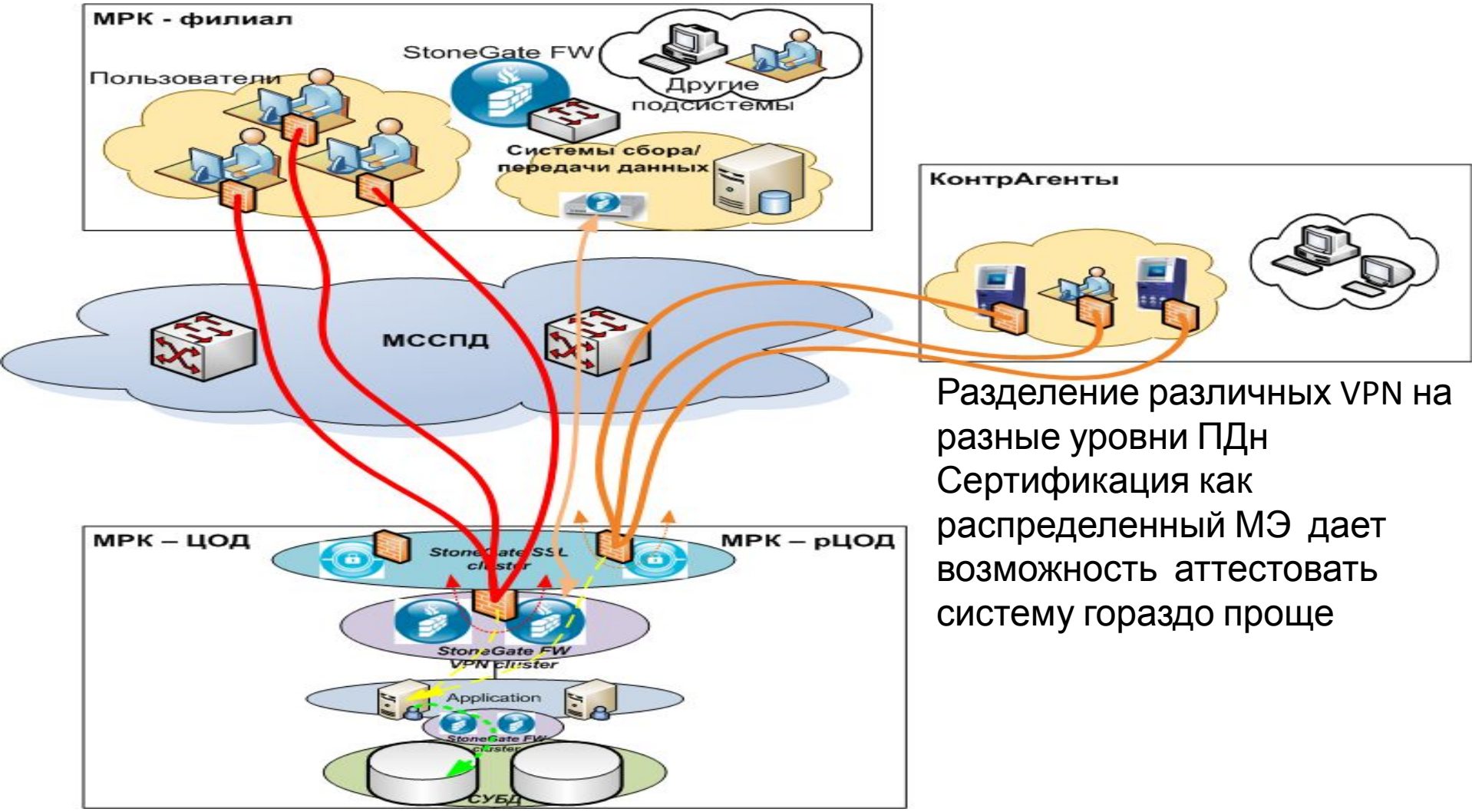


Единственное на рынке решение, позволяющее агрегировать VPN туннели.

Сертификация ФСБ по классам КС1 – КС3!

Возможность включения USB модема прямо в устройство МЭ

Обеспечение разноуровневых VPN



Разделение различных VPN на разные уровни ПДн
Сертификация как распределенный МЭ дает возможность аттестовать систему гораздо проще

STONESOFT

Выбираем лучшее :

Переписка на ispdn.ru:

Скажу Вам по секрету, что в продуктах ViPNet тоже есть механизм обнаружения вторжений (IDS), но почему-то его никто целенаправленно в этих целях не использует …. Для справки: согласно документации ViPNet противостоит аж целым 6 атакам !!! При этом стоимость шлюза ViPNet порядка 46 000 руб.

Про UserGate было официальное письме с вопросом - "Как настроить UG, чтобы были реализованы все требования 58 приказа?" И был технический ответ с настройками тех "особых" пунктов, которые отсутствуют в UG, но при таком подходе могут быть настроены.
Итог - UG можно использовать и в К1 (4 НДВ, 4 МЭ).
Стоимость этого решения 32 000 руб.

Стоимость решения StoneGate Firewall 315L порядка 52 000 рублей … При этом, Вы получаете 100 Мб межсетевой экран, который может посредством лицензионного апгрейда стать 1 Гб файрволом!

Почувствуйте разницу: в базовую лицензию включены все технологии (опционально предлагается только подписка на антивирус и URL фильтрацию!) При этом Вы получаете российский VPN, централизованное управление и многое др.

Выводы:

Решение на StoneGate оказываются часто .. **дешевле**, и при этом:

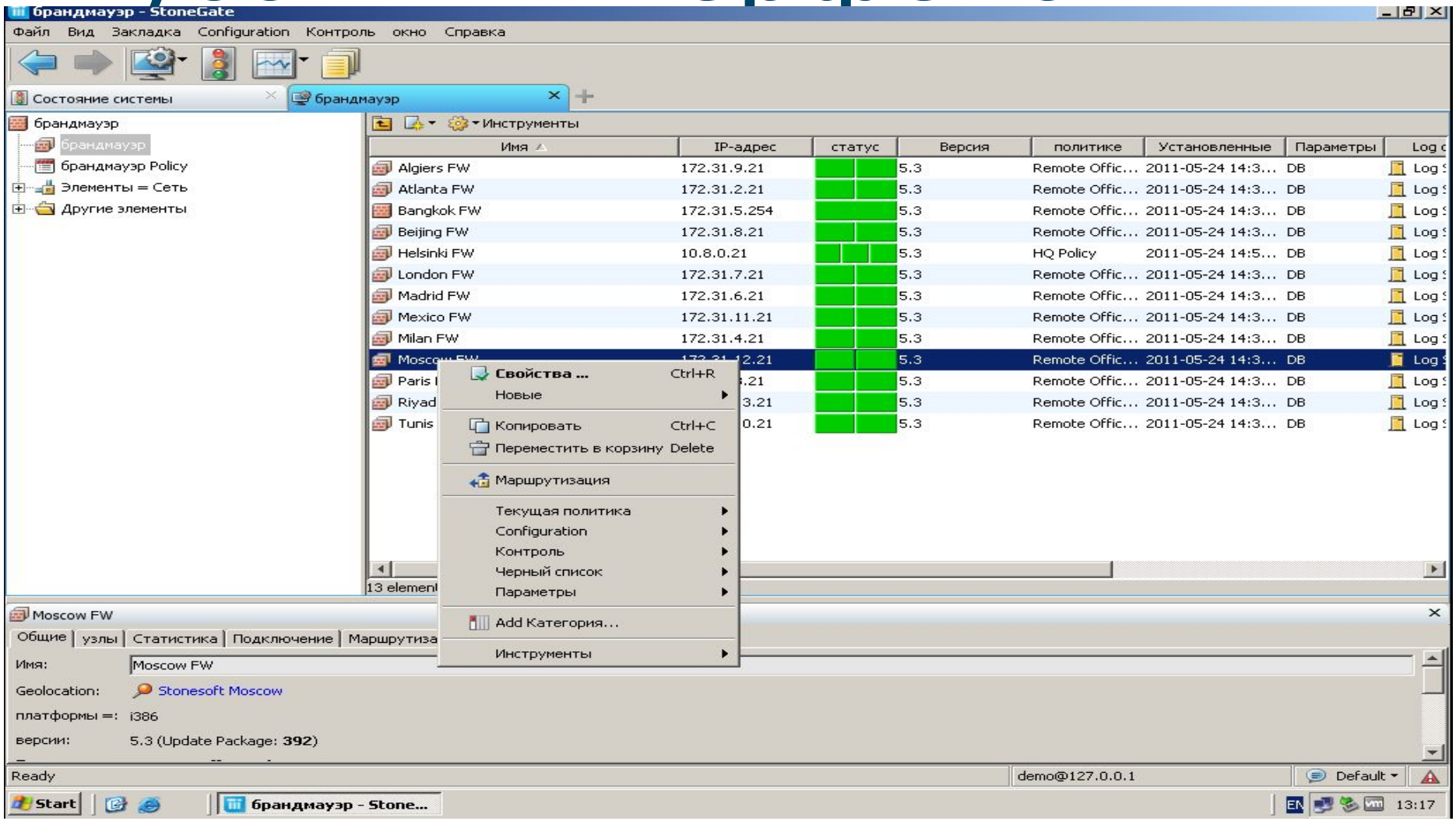
- Функциональность UTM или NGFW…
- Проще развертывание и управляемость
- Отказоустойчивость любого элемента и кластеризация в режиме балансировки нагрузки
- Использование одновременно множества каналов связи (доступность), поддержка QoS и др.
- Интегрируемость в инфраструктуру
- Хорошая техническая поддержка
- Автоматические безопасные обновления
- Совместимость с другими решениями
- Нужные сертификаты

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%**

Русский интерфейс!



STONESOFT

Мы делаем безопасность проще .

Хотите узнать больше о сертифицированных продуктах ?

www.newinfosec.ru

Официальный партнер в России !

www.antievasion.com
узнайте об атаках и способах обмана

www.stonesoft.com