

# Конференция "FinSec: безопасность финансовых организаций"



**Москва, КВЦ “Сокольники”, 19 ноября 2009 г.**

# Платформа безопасности StoneGate включает в себя:

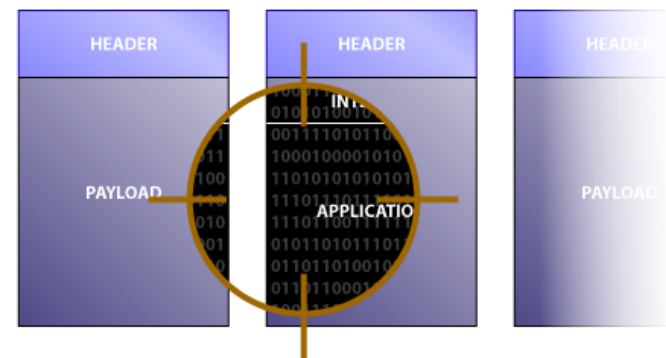
- **Межсетевой экран** с технологиями кластеризации **Multilink**, позволяющей организовать полностью отказоустойчивые подключения к любым сетям
- Уникальное **отказоустойчивое решение VPN** (с поддержкой российской криптографии на базе сертифицированного ФСБ ядра **Крипто Про**), позволяющее организовать отказоустойчивое подключение VPN клиента
- Уникальное **решение SSL VPN** с поддержкой NAC, SSO, 15 методов аутентификации клиента
- Система предотвращения сетевых вторжений **Stonegate IPS** - непревзойденная точность обнаружения и встроенная корреляция событий
- **Stonegate UTM** - универсальное решение по защите небольших офисов с возможностями антивируса, IPS и фильтрации контента
- **Virtual Firewall, Virtual IPS** – решение по защите виртуальных систем

# Сертификации продуктов StoneGate: мировые и российские

- **ФСТЭК (в настоящее время все продукты имеют сертификаты ФСТЭК на партии, сертификация производства по ФСТЭК – январь-февраль 2010 г.!)**
- Common Criteria Certification EAL 4+
- ICSA Labs Certified IPS
  - StoneGate IPS – единственный серийный продукт IPS, который выполнил последние сертификационные требования ICESA Labs
- ICESA Labs Certified Firewall
- VMware
  - VMware Technology Alliance Partner
  - VMware certified – StoneGate Virtual IPS & StoneGate Virtual Firewall/VPN
  - VMsafe technology partner
  - **Top 5 VMware virtual appliance – StoneGate Virtual IPS**
- RSA Secured
- VPN Consortium Certifications
  - IPsec VPN and SSL VPN



- Многоуровневый анализ потоков, патентованная технология Multilayer Inspection позволяют соединить в себе высочайший уровень безопасности как в прокси, и производительность как в потоковых системах.
- Расширенная поддержка приложений – специальные агенты анализируют работу потоков данных и выявляют аномалии работы протоколов и приложений
- Расширенная система оптимизации правил Политики безопасности, проверка их согласованности (в соответствии с требованиями РД и мировых стандартов), что значительно упрощает работу администратора и минимизирует число ошибок.
- Встроенная IPS для анализа потоков и блокировки атак
- Встроенные механизмы антивирусной защиты, защиты от вредоносного контента и контентной фильтрации
- SSL инспекция для защиты критичных серверов и рабочих станций
  - Защита от DoS атак,
  - Обеспечение защиты от утечек данных
  - Встроенные сертифицированные криптобиблиотеки для VPN и многое другое.



*“StoneGate Firewall/VPN и IPS предоставили нам большие возможности, которые в свою очередь позволили нам быть более проактивными в обеспечении безопасности и доступности нашей расширяющейся сети.”*

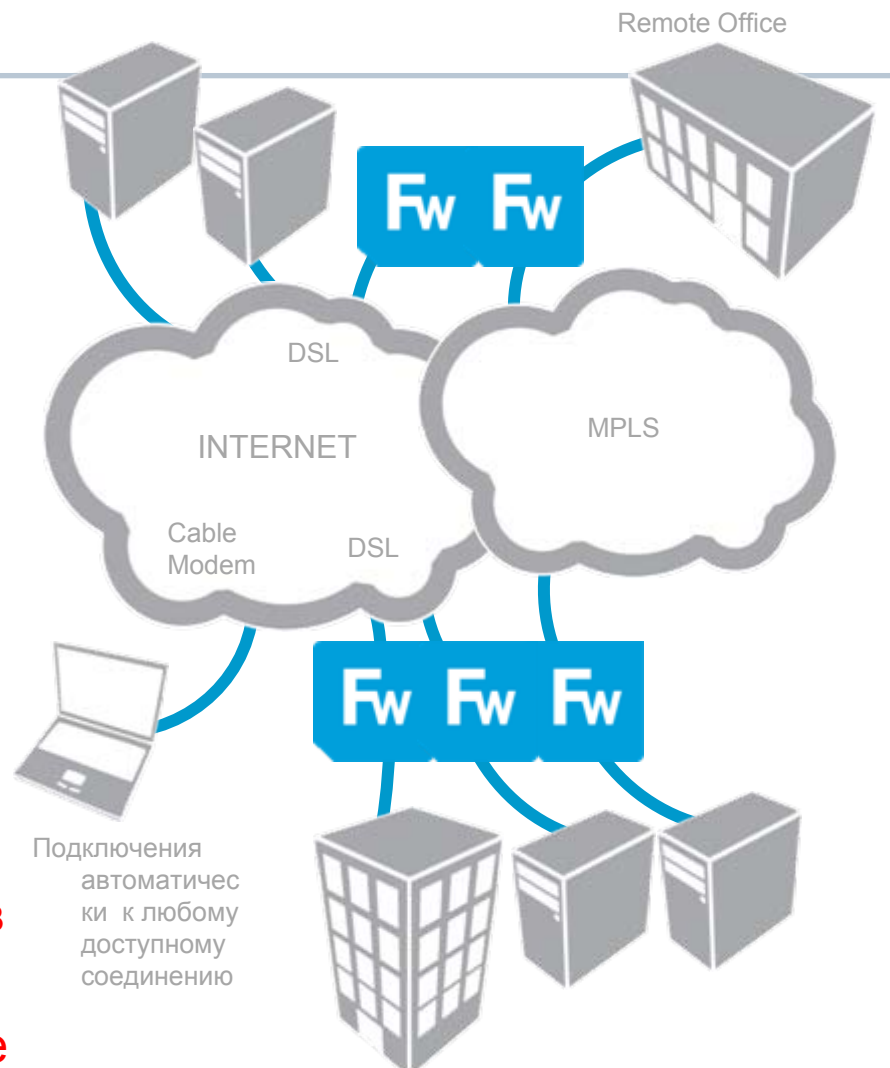
*- Hovman Javdan – Network and Security Administrator  
– Canadian MedicAlert*

**Проходит сертификацию  
на контроль НДС и для  
применения в АС до  
класса 1В и в ИСПДн до К1**

**ВКЛ.**

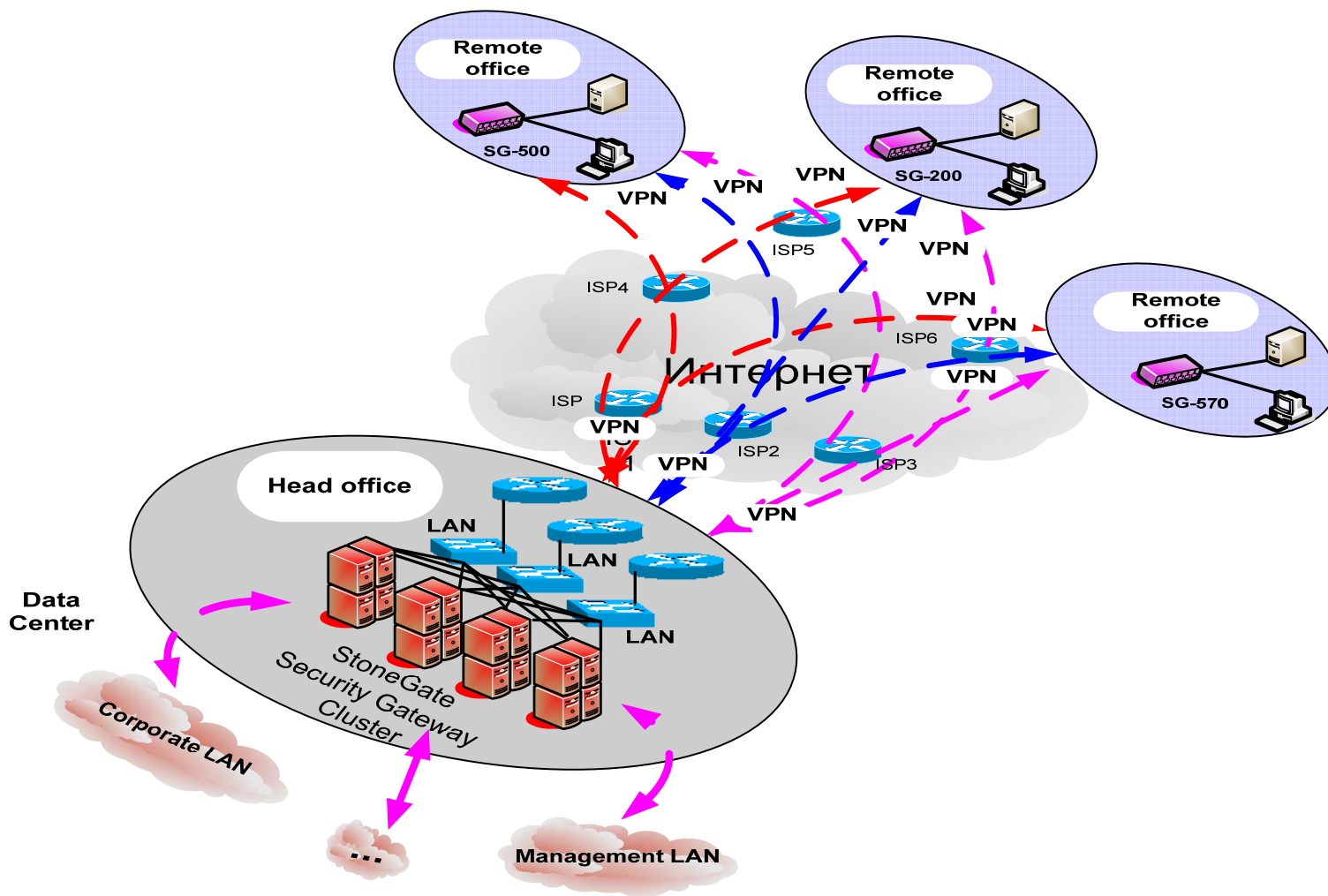
# Технология Multi-Link VPN

- Единственное на российском рынке решение, которое обеспечивает действительно отказоустойчивую связь через несколько провайдеров.
- Легкость подключения каналов связи
  - Режим Active/active, без дополнительного оборудования и сложных протоколов взаимодействия (BGP)
- Поддержка критических технологий
  - VoIP, SIP, video конференции
  - Используются сертифицированные криптографические решения;
  - Технологии QoS, Load Balancing, Multilink, приоритезация потоков обеспечивают непрерывность потоков информации
  - Обеспечение безопасности в качестве распределенного межсетевых экранов вместе с VPN клиентом



Достижение доступности **0,99999**

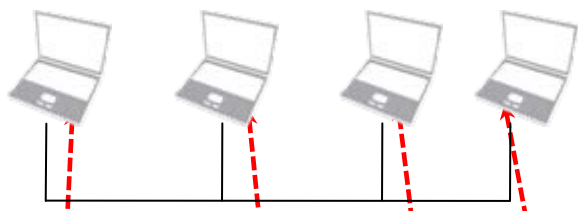
# Организация отказоустойчивых VPN



# Единое управление StoneGate Management Center

## Традиционное управление

FW Mgmt    IPS Mgmt    Incidents    Events



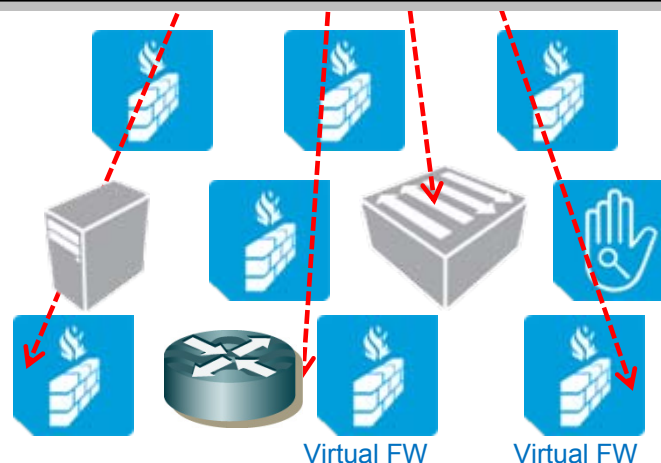
В рамках одного окошка – отдельные консоли, трудоемкие ручные операции и апдейты, наследуемые ошибки администраторов, медленное реагирование на инциденты



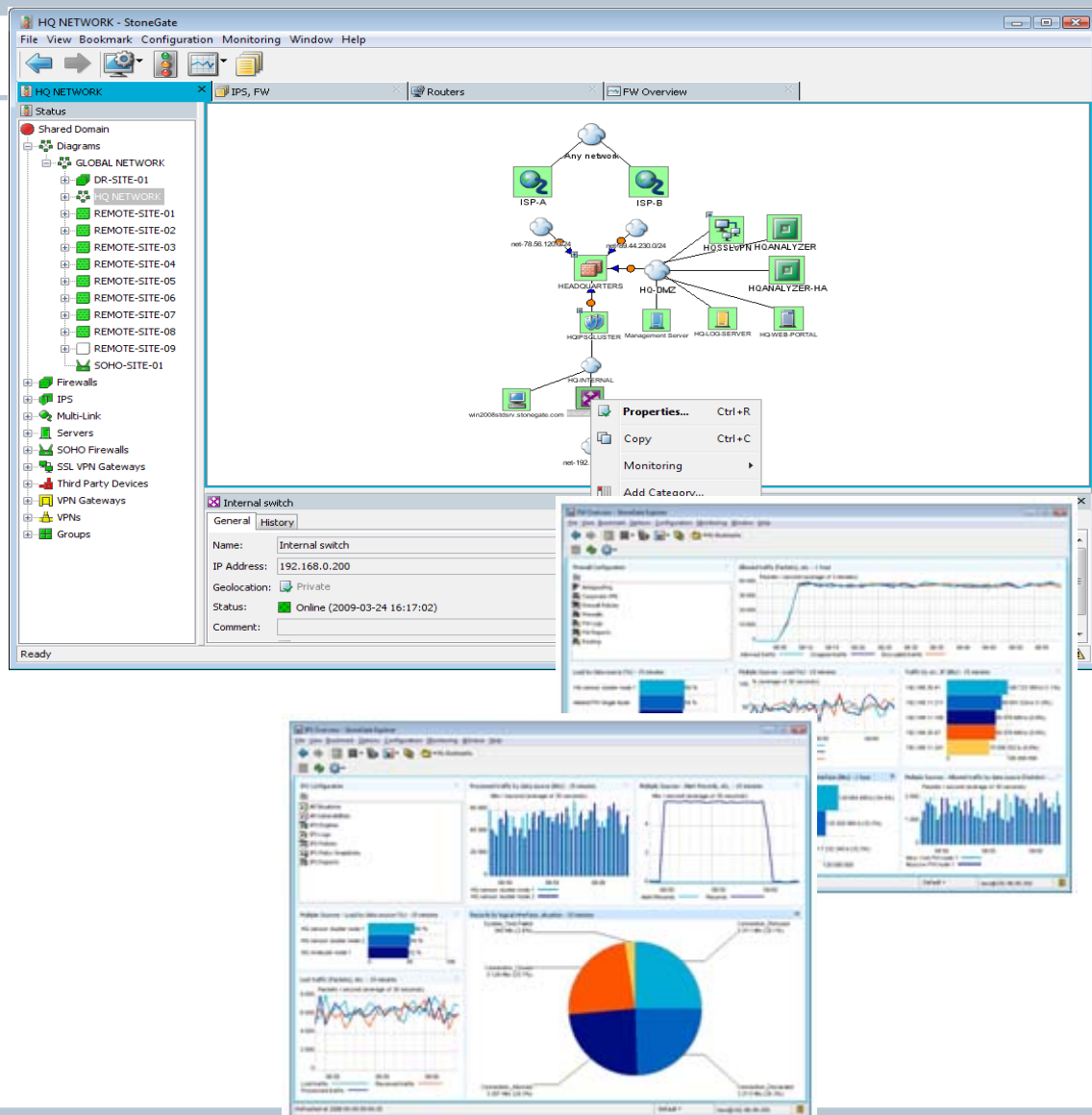
## One-step Management



Единая консоль управления: один раз созданный объект используется везде, автоматическое применение политики /правил Real-time быстрое реагирование на угрозы, управление событиями ИБ и оборудованием, в т.ч. сторонних производителей!



- Первая платформа для проактивного управления сетевой безопасностью в физической и виртуальной среде, в том числе событиями, генерируемыми оборудованием и ПО других производителей
- Real-time мониторинг, корреляция событий ИБ, журналирование и отчеты
- Управление сотнями устройств – коммутаторы, маршрутизаторы, устройства безопасности
- Быстрое управление инцидентами безопасности



# Централизованное хранилище логов

- Созданная однажды конфигурация используется везде
- Общие элементы в базе данных
- Сохраняет все конфигурации – от политики до настроек операционной системы
- Использование одних и тех же компонент везде => меньше ошибок администрирования
- Всегда активная система управления (Always-on management)
  - Встроенная функция восстановления после катастроф
  - Настраиваемые роли, права и действия
  - Одновременное администрирование
- Домены пользователей
  - Исключает администрирование большого количества систем в отдельности
  - **LOG server** – сбор и централизованное хранение логов с различных устройств (Cisco, Symantec, OS Windows, Unix и многих др.), управления логами, отчеты в соответствии с требованиями стандартов и т.п.!

