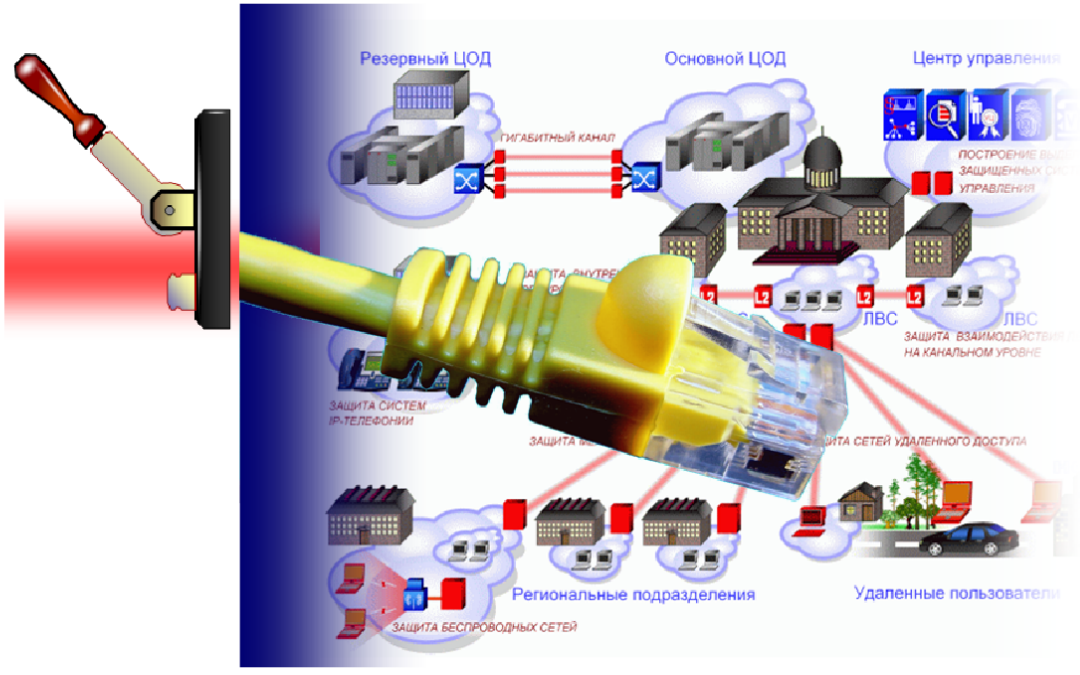
s·terra
csp

Методы построения высокопроизводительных систем защищенного взаимодействия на основе криптографических алгоритмов ГОСТ

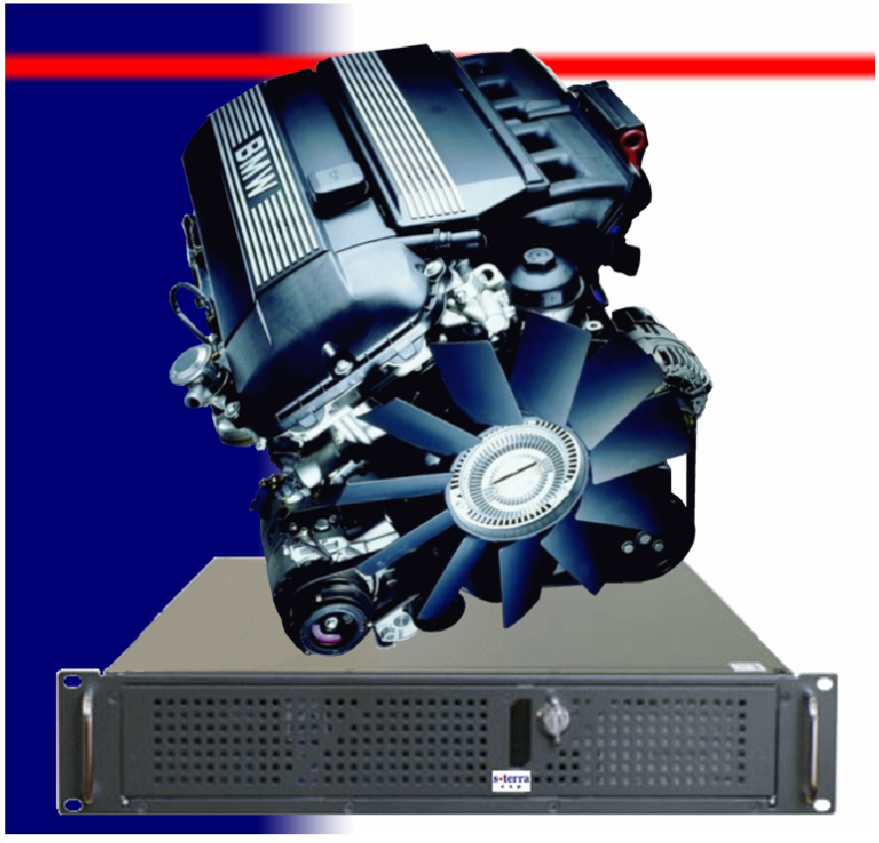
СТАНДАРТ СЕТЕВОЙ БЕЗОПАСНОСТИ ДЛЯ РОССИЙСКОГО БИЗНЕСА

Неограниченные возможности сетевой защиты



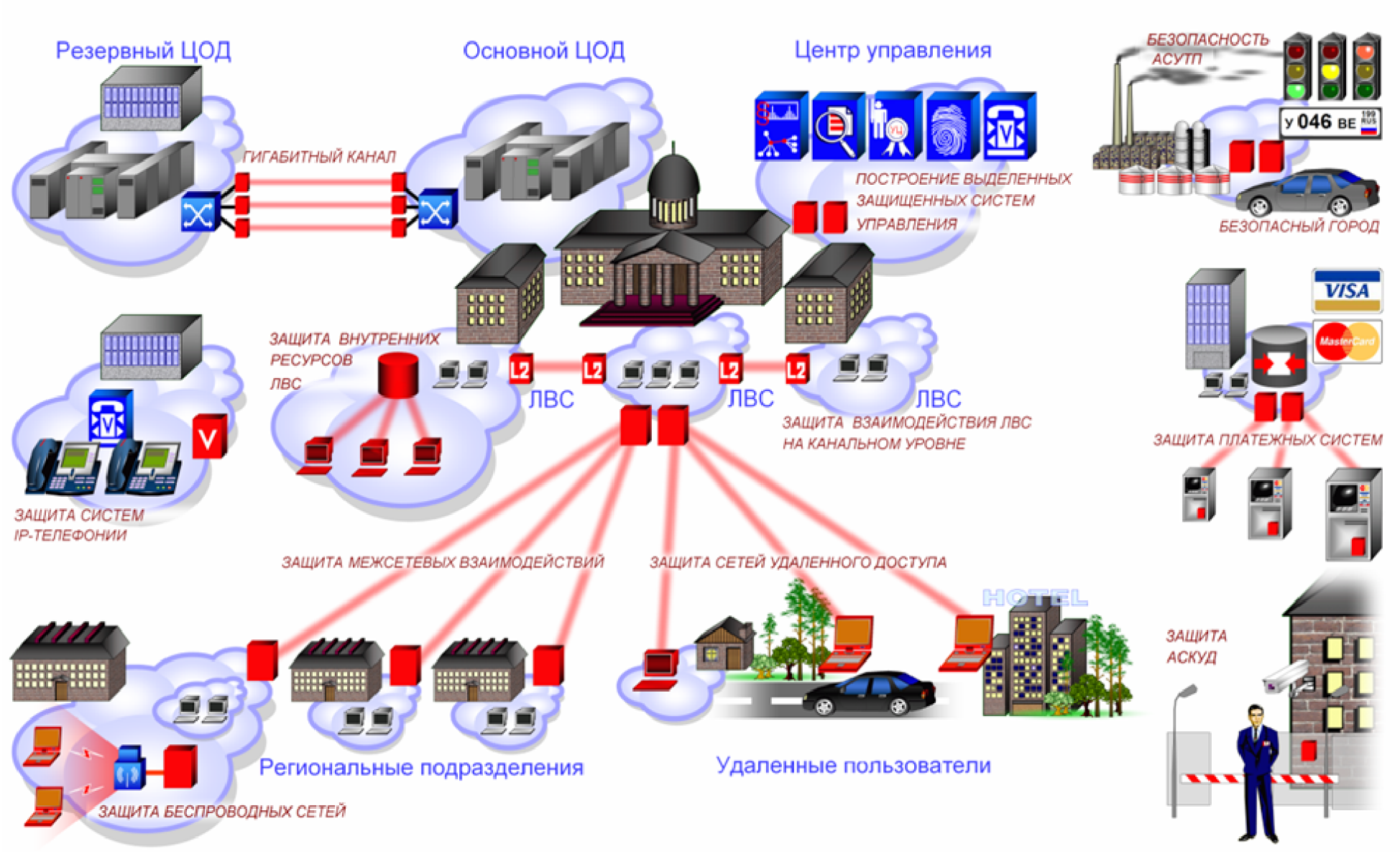
- Сетевая информационная безопасность: комплекс мер защиты от атак на основе коммуникационных протоколов
  - актуальна: сегодня все компьютеры работают в сети
  - универсальна: сетевая безопасность применима в любой сети, вне зависимости от специфики бизнес-процессов и приложений
  - обеспечивает полноту контроля: инспекции подвержен каждый пакет, обойти сетевой драйвер невозможно

Зачем производительность?



- Очень критична для криптографических приложений
- Существенно влияет на показатель цена/качество VPN-продукта
  - Рекордные показатели: скорость шифрования 3.5 Гбит/с
  - Февраль 2010
- Особое значение имеет для мультисервисных приложений

Где нужны высокопроизводительные решения



Преимущества стандартного дизайна

- Базовые стандарты IPsec:
  - RFC 2401-RFC 2412
- Расширения IKE:
  - DPD
  - NAT Traversal IPsec
  - IKE-CFG
  - XAUTH
- Криптоархитектура:
  - RFC 2628, 4357, MS CryptoAPI
  - ГОСТ 28147-89, DES, 3DES, AES
  - ГОСТ Р 34.10-94, 2001, RSA
  - ГОСТ Р 34.11-94, MD5, SHA-1
- Интеграция с PKI:
  - PKCS#7,10,12
  - X.509 v.3 (RSA, DSA, ГОСТ)
  - CRL
  - LDAP
- Мониторинг и аудит:
  - SNMP
  - Syslog

- Исчерпывающая аналитическая проработка архитектуры, безопасный дизайн протоколов защиты информации
- Совместимость
- Унифицированная функциональность
- Верификация кода продуктов, кросс-отладка
- «Смешанные» сценарии применения, включающие в периметр защиты отечественные и импортные продукты
- Документированное поведение продуктов

Функции безопасности IPsec

- Базовые стандарты IPsec:
  - RFC 2401-2406, 2410

- Конфиденциальность трафика, протокол ESP
  - стойкое шифрование IP-пакетов на любых доступных криптоалгоритмах
  - транспортный (клиент-сервер) и туннельный (клиент-сеть и сеть-сеть) режимы шифрования
    - в туннельном режиме обеспечивается сокрытие топологии сети
  - доступен режим контроля целостности блока данных
- Целостность трафика, протокол AH
  - обеспечивается целостность пакетов (включая IP-заголовок, защита от подмены IP-адресов)
  - обеспечивается не только целостность потока пакетов, невозможно «подмешать» не только «чужой», но даже ранее переданный «свой» трафик
- В совокупности именно эти протоколы обеспечивают криптографически стойкий контроль доступа (в сеть проникает только владелец секретного ключа) и, таким образом, изоляцию корпоративного информационного пространства в агрессивной внешней среде

Протокол управления ключами IKE

- Базовые стандарты IPsec:
  - RFC 2401-RFC 2412
- Расширения IKE:
  - DPD
  - NAT Traversal IPsec
  - IKE-CFG
  - XAUTH

Internet Key Exchange, IKE

управление аутентификацией партнеров по взаимодействию, согласование политик защиты и выработка ключевого материала для протоколов AH и ESP

IP Security Architecture, IPsec

Authentication Header, AH	Encapsulated Secure Payload, ESP
обеспечение целостности IP-пакетов	шифрование содержимого IP-пакетов

- Базовые функции:
  - взаимная аутентификация взаимодействующих объектов
    - широкий спектр алгоритмов аутентификации (симметричный ключ, сертификаты X.509, токены, системы двухфакторной аутентификации с одноразовым паролем)
  - защита сведений о взаимодействующих объектах (identity protection)
  - защита ключевой информации
    - выработка сессионного ключевого материала, защита мастер-ключей путем обработки при их использовании малого объема трафика
    - защита сессионных ключей (perfect forward secrecy)
    - замена сессионных ключей при передаче заданного объема трафика или по истечении заданного времени жизни сессионного ключа
    - продукты CSP VPN также поддерживают режим «прозрачной» замены сессионных ключей с тем, чтобы пересинхронизация ключей не вносила возмущений в процесс защиты трафика

Протокол управления ключами IKE (продолжение)

- Базовые стандарты IPsec:
  - RFC 2401-RFC 2412
- Расширения IKE:
  - DPD
  - NAT Traversal IPsec
  - IKE-CFG
  - XAUTH

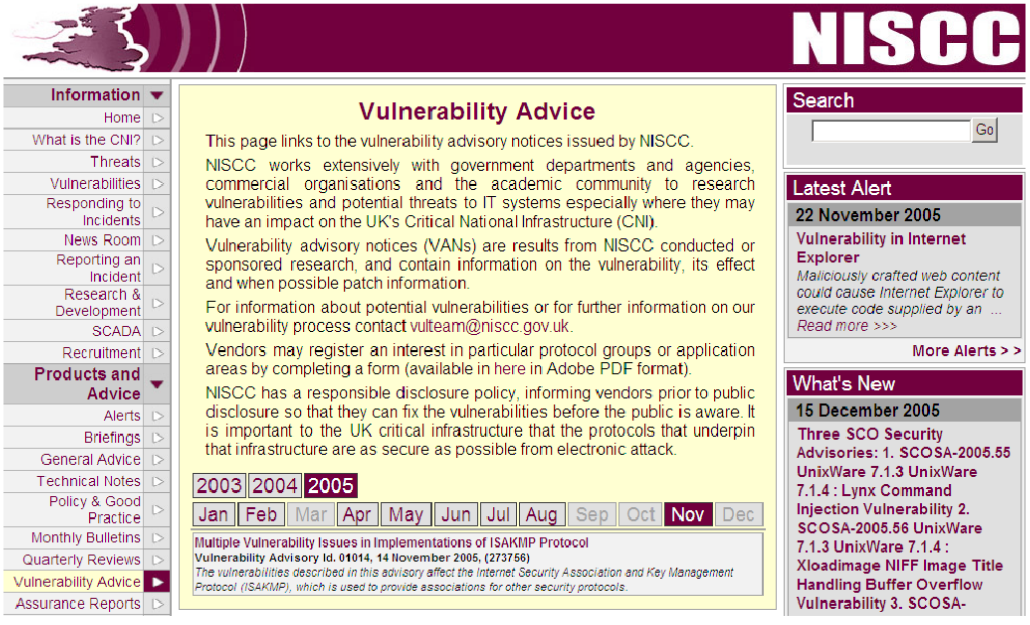
- Базовые функции:
  - согласование политик безопасности
    - партнеры по взаимодействию могут поддерживать каждый свое множество вариантов политики безопасности, приемлемый для обоих вариант будет автоматически выбран в процессе начального диалога
    - это важно для обеспечения совместимости и для переходных процессов, например, при замене политики безопасности в масштабах большой сети
  - автоматическое детектирование наличия NAT на пути передачи защищенного трафика, инициализация режима прозрачной передачи трафика AH/ESP через NAT-шлюзы
  - конфигурирование IP-адресов VPN-клиентов «внутри» VPN
    - клиент удаленного доступа получает адрес из внутреннего пространства корпоративной сети; далее к нему применимы все правила для «внутренних» пользователей
  - обнаружение отказа партнера по взаимодействию и автоматическое переключение на резервный шлюз (dead peer detection protocol)
- Резюме: IKE- наиболее мощный, гибкий (и расширяемый) из современных криптографических протоколов

Контроль качества и кросс-отладка

ВНИМАНИЕ!

Опубликован тест уязвимостей протокола IKE:

http://www.niscc.gov.uk/niscc/vulnAdv-en.html



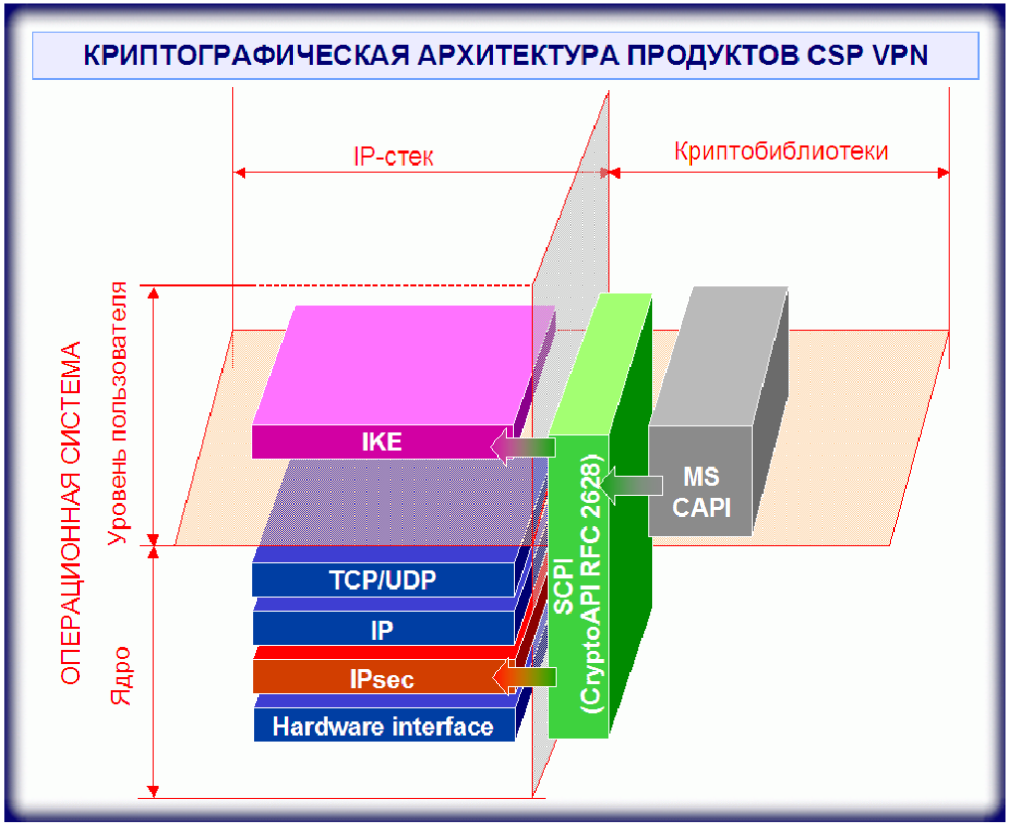
- 14 ноября 2005 года опубликован первый публичный тест уязвимостей протокола IKE
- Компания «С-Терра СиЭсПи» в феврале 2006 года, первой в России, провела этот тест на своих продуктах, устранила все найденные неполадки (5-7 замечаний по 5000 тестов) и объявляет, что версии 2.1 продуктов CSP VPN устойчива по отношению к данной версии теста
- Качество реализации IKE/IPsec проверяется также в тестах совместимости с продуктами Cisco Systems, которые являются неотъемлемой частью выходного тестирования каждой версии линейки продуктов CSP VPN

Управление уровнем загрузки шлюзов

- Поскольку криптографические приложения потребляют очень много вычислительной мощности, они перегружают вычислительную систему, замедляют ее отклик на управляющие воздействия и подвержены одной из самых трудных для отражения атак – атаки отказа в обслуживании (**Denial of Service attack, DoS**)
- В продуктах **CSP VPN** администратор безопасности может устанавливать предельный уровень загрузки процессора, который доступен задачам шифрования трафика
- Ограничение порога потребляемой мощности обеспечивает доступность шлюза для администрирования при любом уровне нагрузки и повышает устойчивость шлюза к **DoS**-атаке

Криптографическая архитектура

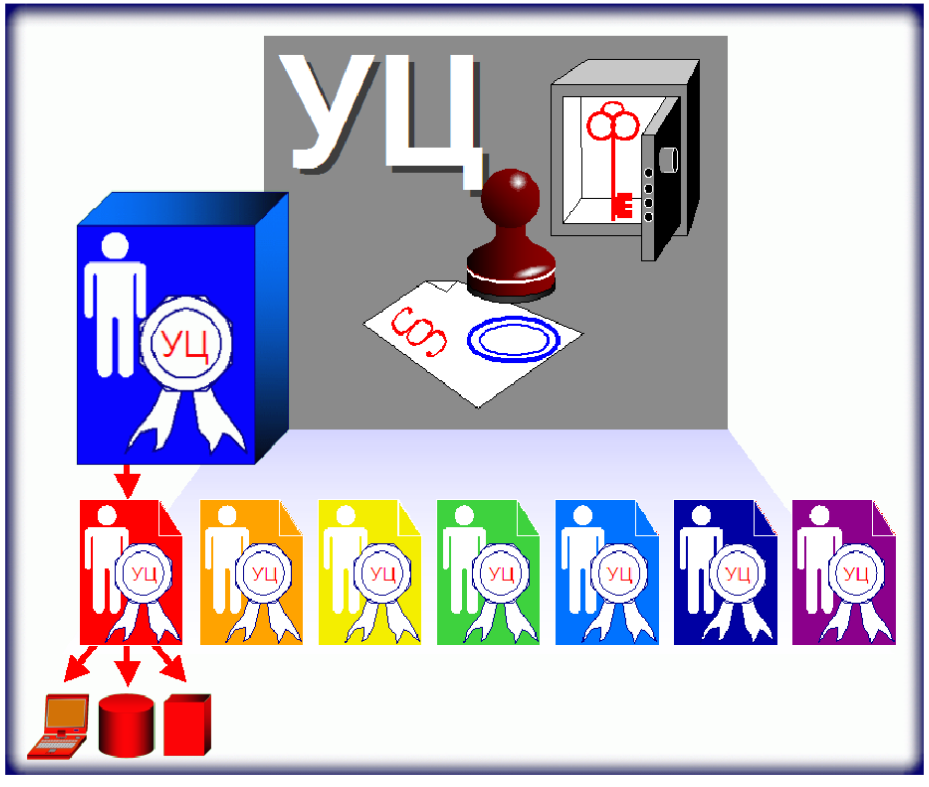
- Криптоархитектура:
  - RFC 2628, 4357, MS CryptoAPI
  - ГОСТ 28147-89, DES, 3DES, AES
  - ГОСТ Р 34.10-94, 2001, RSA
  - ГОСТ Р 34.11-94, MD5, SHA-1



- Архитектура IKE/IPsec не накладывает ограничений на применение криптоалгоритмов
- В продукты линейки CSP VPN встраивает криптобиблиотеки третьих производителей
  - поддерживаются российские криптографические стандарты а также, для целей тестирования и совместимости с импортными продуктами, – западные криптоалгоритмы
  - в настоящее время продукты CSP VPN поставляются с криптобиблиотеками компаний «Крипто-Про» и «Сигнал-КОМ»

Инфраструктуры открытых ключей

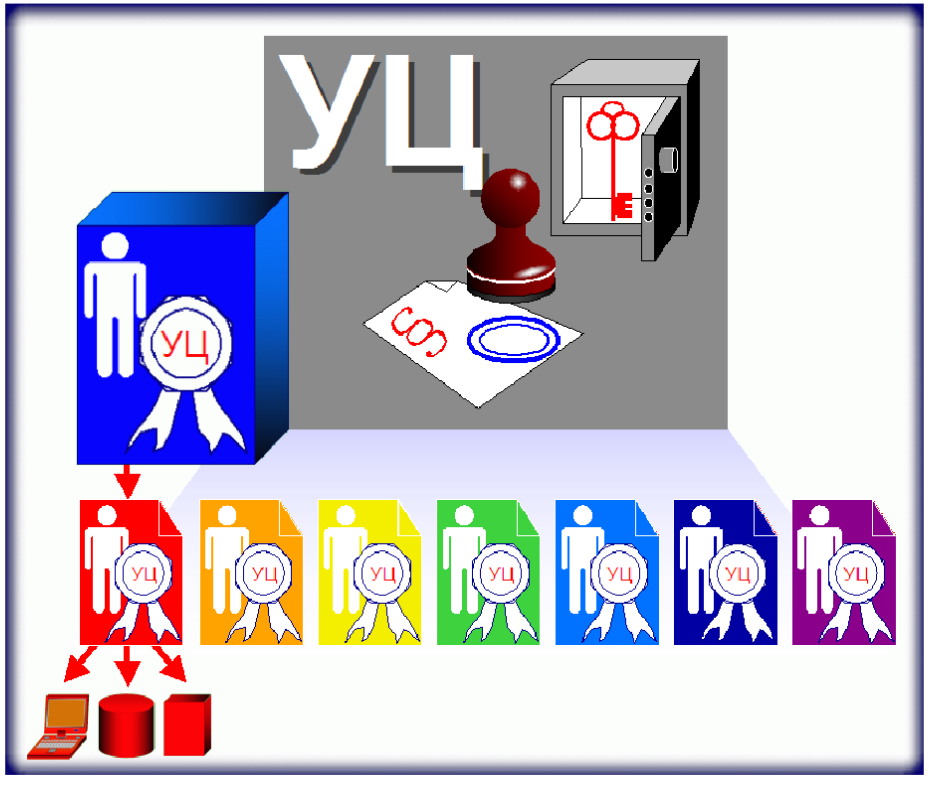
- Интеграция с PKI:
  - PKCS#7,10,12
  - X.509 v.3 (RSA, DSA, ГОСТ)
  - CRL
  - LDAP



- **Управление криптографическими ключами в крупной системе (число объектов свыше 20-50) наиболее эффективно только с применением инфраструктуры открытых ключей (PKI)**
- **PKI обеспечивает:**
  - идентификацию ключей
  - генерацию ключевых пар в централизованном и децентрализованном режимах, удостоверение ключей (выдачу ключевых документов – сертификатов X.509)
  - распространение сертификатов
  - проверку подлинности ключевой информации
  - отзыв компрометированных или вышедших из эксплуатации ключей

Инфраструктуры открытых ключей (продолжение)

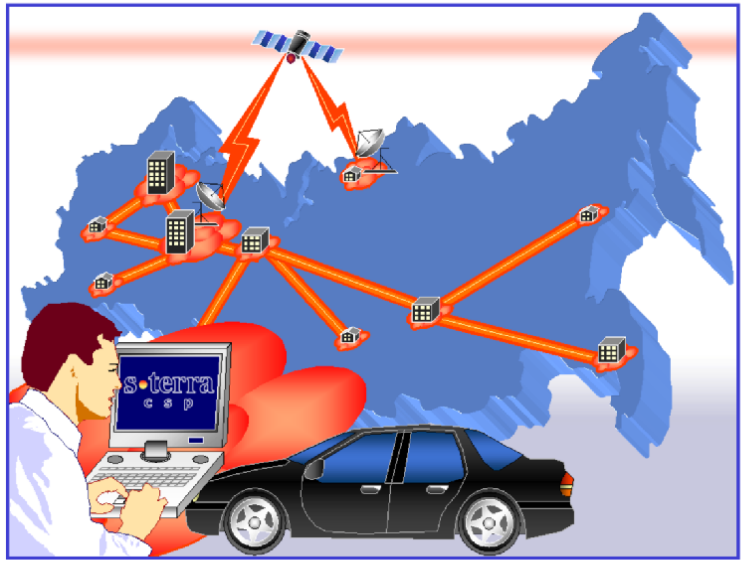
- Интеграция с **PKI**:
  - **PKCS#7,10,12**
  - **X.509 v.3 (RSA, DSA, ГОСТ)**
  - **CRL**
  - **LDAP**

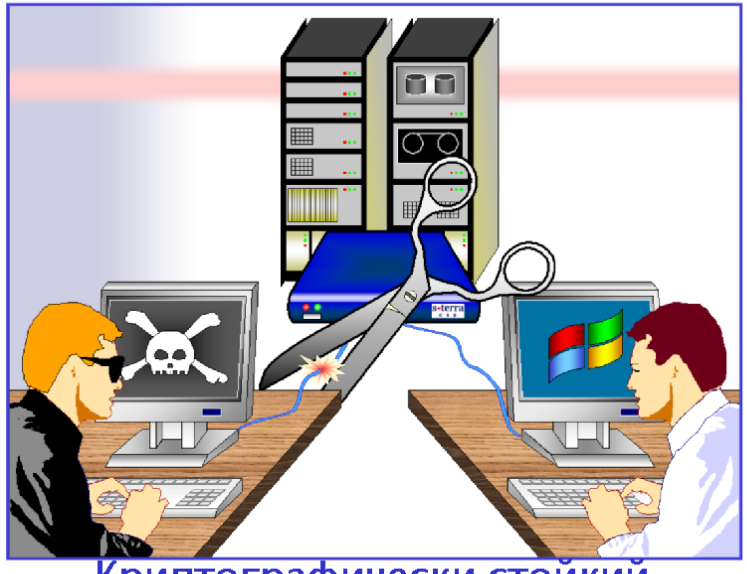


- Продукты **CSP VPN** поддерживают:
  - генерацию запросов на сертификаты и распространение ключевых документов в форматах **PKCS#7, 10, 12** (индустриальные стандарты **RSA**)
  - работу с сертификатами **X.509**
  - работу с контейнерами «Крипто-Про» и «Сигнал-КОМ»
  - распространение сертификатов через службы каталогов **LDAP**
    - **очень полезна также функциональность протокола IKE, который сам «умеет» передавать сертификаты и информацию для их проверки (certificate validation chain) – это позволяет реализовать распространение сертификатов между партнерами по взаимодействию напрямую, без службы каталога – это снижает издержки на обработку трафика**
  - списки отзыва сертификатов (**CRL**)
- Продукты **CSP VPN** совместимы с удостоверяющими центрами:
  - УЦ **Microsoft**, УЦ «Крипто-Про»
  - **Notary-Pro** («Сигнал-КОМ»)
  - **CCERT** («Валидата»)
  - **Keon** (**RSA**, СКЗИ «Крипто-Про»)

Концепция и реализация

Изоляция корпоративного информационного пространства

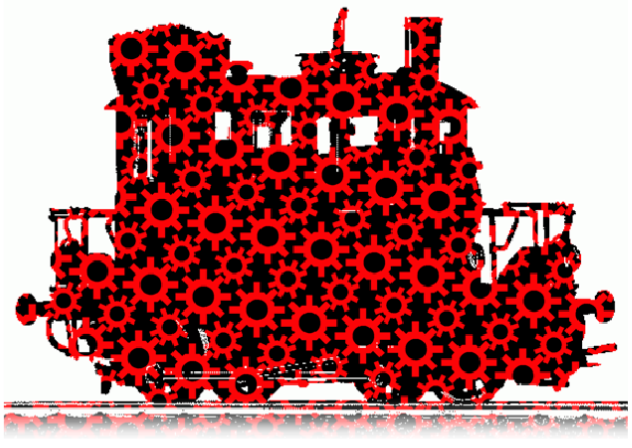




Криптографически стойкий контроль доступа

- Базовая технология: фундаментальная архитектура сетевой защиты **IPsec**
- Механизмы безопасности **IPsec:**
  - конфиденциальность и целостность информации
    - каждый пакет шифруется при помощи стойких криптоалгоритмов
    - ключевая информация надежно защищена за счет использования временных сеансовых ключей с ограниченным временем жизни
  - целостность информации обеспечивается для данных, для заголовков IP-пакетов и для потока пакетов
  - поддерживается много механизмов аутентификации
    - для отдельного пользователя можно реализовать него индивидуальную политику
  - криптографически стойкий контроль доступа
    - в сеть может проникнуть только владелец секретного ключа
    - это обеспечивает полную изоляцию корпоративного информационного пространства

Легитимность IPSec VPN решений



- Устройство VPN – это коммуникационная среда со встроенным СКЗИ или это СКЗИ?
- Центр ФСБ России отвечает на этот вопрос однозначно:
  - VPN – это средство криптографической защиты
  - Основания для такого взгляда:
    - стойкость сервиса VPN существенно зависит от структуры и корректности реализации криптографического протокола
    - криптографический протокол в целом характеризуется параметрами криптографической стойкости
- Состав сертификатов VPN-продукта:
  - ФСБ России:
    - СКЗИ
  - ФСТЭК России:
    - НДВ

Сертификация продуктов CSP VPN

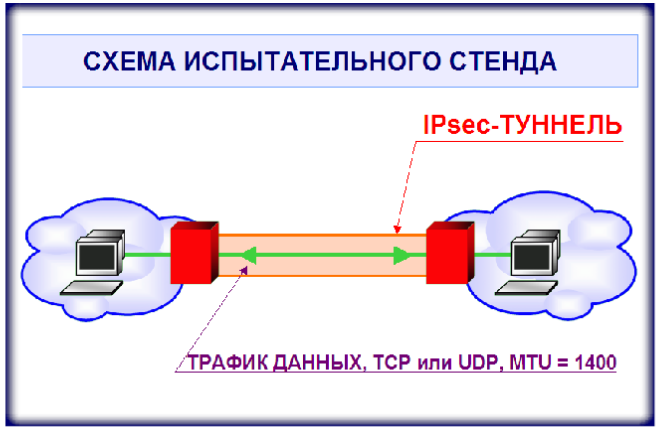
- **CSP VPN версия 3.1**
  - ФСБ России
    - Сертификат СКЗИ КС1, КС2 на продукт CSP VPN Gate (в т.ч. в исполнении CSP VPN Client)
      - распространяется на аппаратную платформу «Модуль Сетевой Модернизированный».
  - ФСТЭК России
    - ГОСТ 15408, ОУД 3+
    - РД НДВ 3й уровень контроля
    - Рекомендация для защиты конфиденциальной информации в АС до класса 1Г включительно и в ИСПДн до класса К1 включительно
    - Сертификация в качестве межсетевых экранов по 3 классу защищенности от НСД; защита информации в ИСПДн до 1 класса включительно

Измерение производительности

Источник: BMW

- **Производительность является критически важным показателем для шлюзов безопасности**
  - запас производительности позволяет использовать сеть без потери пропускной способности
  - высокопроизводительное устройство вносит минимальную задержку при обработке трафика, что критически важно для поддержания высокого качества сетевого обслуживания (QoS)
- **Практически во всех измерениях производительности VPN-шлюзов данные приводятся для IP-пакетов размером 1,5 кбайт, в то время как для коротких пакетов производительность по потоку падает в 4-5 раз**
  - поэтому номинальная производительность шлюзов должна быть в несколько раз ниже пиковой производительности

Рекордная производительность

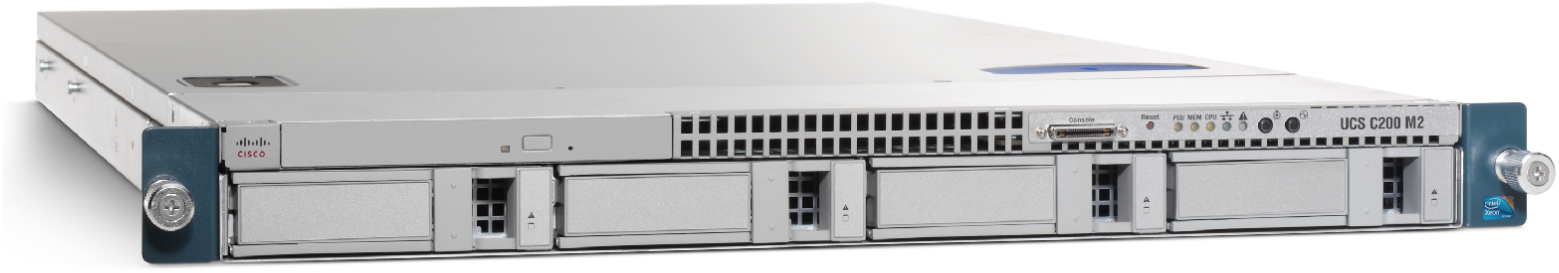


Наименование изделия	IPsec ESP / ГОСТ 28147	IPsec ESP / ГОСТ 28147 и IPsec AH / ГОСТ Р 34.11
CSP VPN Gate 100	18 Mbps	8 Mbps
CSP VPN Gate 1000	43 Mbps	18 Mbps
NME-RVPN (MCM)	95 Mbps	37 Mbps
CSP VPN Gate 3000	200-400 Mbps	50-110 Mbps
CSP VPN Gate 7000	500Mbps - 1Gbps	100-160 Mbps

- **Продукты CSP VPN Gate оптимизированы по производительности при реализации протоколов IPsec с использованием российских криптографических стандартов**
  - см. дополнительно *http://www.s-terra.com/CSP/RU/products/performance.htm*
- **На независимых испытаниях производительности продукты CSP VPN показывали на различных платформах рекордные производительности шифрования трафика**
  - *независимый источник: http://www.ot.ru/pr20050412.html*

Пример решения: VPN шлюз на Cisco UCS C-200

- Решение CSP VPN Gate на платформе Cisco UCS C-200 представляет собой VPN-шлюз, реализующий международные стандарты безопасности в сетях TCP/IP (IPSec) с применением российской криптографии.

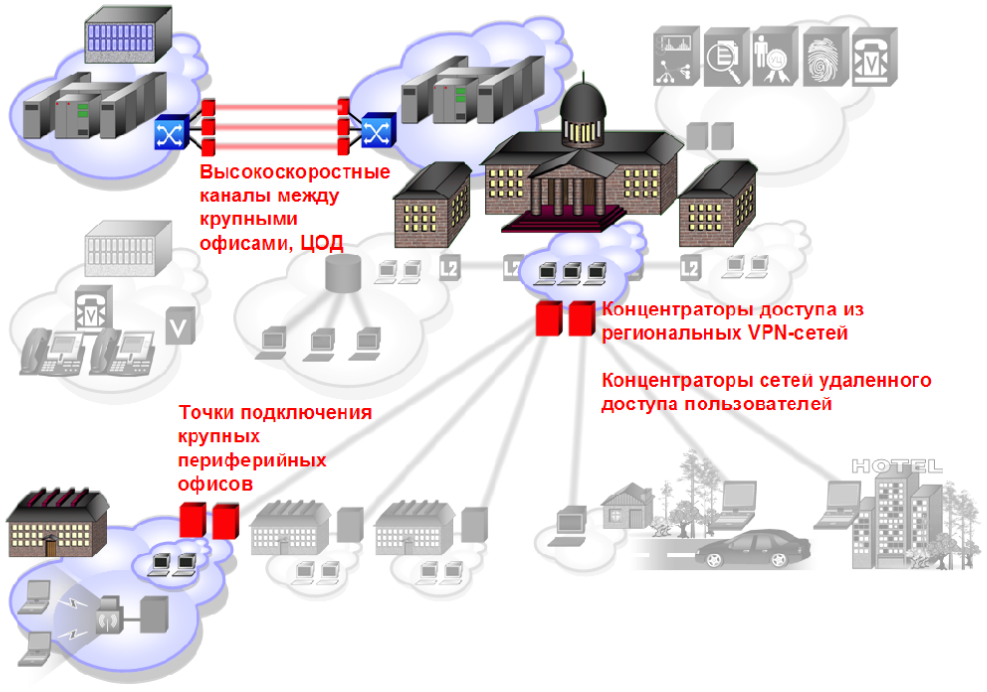


- Производительность решения в зависимости от аппаратной платформы:*

G-3000-S-9100-2-CP	800 Мбит/с
G-3000-S-9101-2-CP	1520 Мбит/с
G-3000-S-9102-2-CP	1700 Мбит/с
G-7000-S-9103-2-CP	2480 Мбит/с
G-7000-S-9104-6-RED-CP	3100 Мбит/с

* цены на CSP VPN Gate на платформе Cisco UCS C-200 M2
см. на сайте www.s-terra.com/CSP/RU/products/documents/S_Terra_price_Gate.pdf

Механизмы обеспечения надежной работы сети



Для обеспечения надежного функционирования сети в решении CSP VPN применяются следующие механизмы:

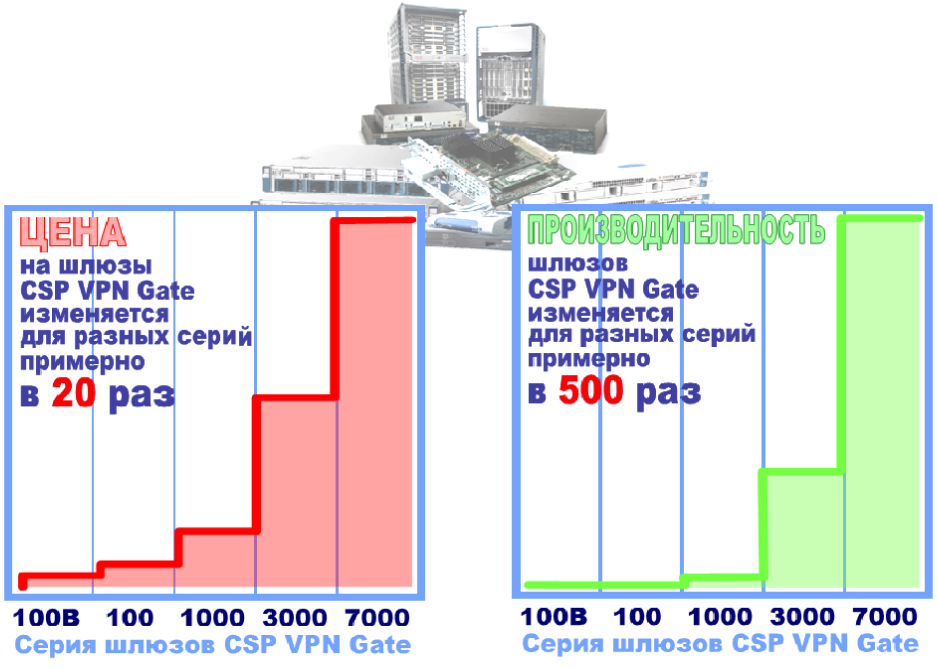
- Пакетное резервирование шлюзов безопасности (по схеме N+1 с выравниванием нагрузки)
  - протокол DPD
  - протокол VRRP
  - протокол RRI
  - протокол Etherchannel в сочетании с защитой канального уровня на основе продукта CSP L2VPN Gate
- Динамическая маршрутизация, GRE

Решение для субгигабитного канала

- **Оптимизированная производительность продуктов CSP VPN Gate позволяет использовать эти устройства в качестве конструктивных блоков для защиты субгигабитного канала связи**
- **Узел защиты каналов связи построенный на основе нескольких шлюзов безопасности с производительностью до 3 Гбит/с впервые был испытан в 2005 году компанией Микротест**
  - первое в России испытание VPN для гигабитного канала на основе российских криптографических стандартов
  - *независимый источник:* ***http://www.microtest.ru/solutions/systems_informbezopasnost/sterra_3gb.html***
- **В ближайших планах построение решения для 10 Гбит/с**

Заключение

Линейка CSP VPN: рекордная производительность и масштабируемость



- CSP VPN Gate:
  - системообразующий продукт в продуктовой линейке,
  - поставляется на ряде стандартных аппаратных платформ (масштабируемых в соответствии с требованиями заказчика) и
  - обладает единым набором технических характеристик в составе всей линейки шлюзов безопасности
- Производительности шлюзов безопасности CSP VPN Gate от младших серий к старшим различаются в 100 раз, цены на них – почти в 40 раз
- Масштабируемость мощности и цены платформ позволяет «дозировать» производительность строго по потребности заказчика и в реальных проектах (где, как правило, доминируют низкоскоростные каналы), снизить суммарную стоимость решения на 30-50% по сравнению с конкурентными предложениями

КОНТАКТЫ

e-mail: sales@s-terra.com
web: http://www.s-terra.com/

Тел.: +7 (499) 940 9001
+7 (495) 726 9891
Факс: +7 (499) 720 6928

Вопросы?

Обращайтесь к нам!

s·terra
csp
Cisco Solution Technology Integrator