THALES

Защита Данных Филиальной Сети

Сергей Кузнецов,

Regional Director Sales, Russia and CIS, Thales CPL

Содержание

- Выводы
- Зачем защищать Филиальную Сеть? Возможные варианты защиты
- Как защищать? Примеры из жизни
- Почему Thales, или а как же импортозамещение?
- Q&A

- * В презентации использованы примеры международных заказчиков, так как для РФ не принято разглашать инифформацию о решениях по защите инфраструктуры.

Выводы

- Каналы связи требуют защиты, то есть, шифрования
- Оптические каналы также требуют защиты
- IPSec – проверенная временем технология, но далеко не оптимальна
- VPN имеет право на жизнь, но требует дополнительной защиты доступа – MFA
- На рынке представлены решения, более современные, чем стандартные VPN IPSec. Нужно уметь понимать отличия.
- На рынке представлены как современные международные решения AES, так и аналогичные решения Российского производства с поддержкой алгоритмов ГОСТ.

Зачем защищать оптику?

Вы знаете что это такое?

Так называемая «прищепка» или пассивное устройство для считывания инифформации с оптических каналов связи без нарушения структуры.
Ориентирововчная цена – 300 Долларов США.

Это больше не удел секретных служб... Все доступно для заказа в Интернете

Альтернатива IPSec есть

	IPSec	HSE
Производительность	Средняя • Высокие потери (overhead) • Высокие задержки • Плохо подходят для высокоскоростных каналов (> 1Gbps)	Высокая • Предсказуемая скорость • Полная полоса канала • Отсутствие задержки • Любые скорости 1/10/100Gbps
Применимость	Высокая • Применимы для L2 и L3 топологий	Высокая • Любые топологии L2 • Не зависит от производителей каналообразующего оборудования
Масштабируемость	Средняя • Высокие потери (package overhead) • Высокие задержки • Сложность настройки/поддержки • Плохо подходят для (> 1Gbps)	Высокая • Настроил и забыл • Поддержка сотен виртуальных каналов внутри линка. • Поддержка любых топологий
Безопасность	Средняя • Средняя/низкая защита • Использует ГСЧ • Нет защиты ключа шифрования • Нет разделения прав доступа	Высокая • Выделенное устройство • Корень доверия (как HSM) • Управление сертификатами на базе PKI • Аппаратный ГСЧ • Международные/ГОСТ сертификации
Крипто-стойкость	Низкая • Предопределенные алгоритмы • Нет возможности обновления	Высокая • Широкий набор алгоритмов • Возможность кастомного алгоритма (ГОСТ) • Обновление в полях • Поддержка Кватновых ГСЧ

Альтернатива IPSec есть

	IPSec	HSE
Производительность	Средняя • **Высокие потери (overhead)** • **Высокие задержки** • Плохо подходят для высокоскоростных каналов (> 1Gbps)	Высокая • Предсказуемая скорость • **Полная полоса канала** • **Отсутствие задержки** • Любые скорости **1/10/100Gbps**
Применимость	Высокая • Применимы для L2 **и L3 топологий**	Высокая • **Любые топологии L2** • Не зависит от производителей каналообразующего оборудования
Масштабируемость	Средняя • Высокие потери (package overhead) • Высокие задержки • **Сложность настройки/поддержки** • Плохо подходят для (> 1Gbps)	Высокая • **Настроил и забыл** • Поддержка сотен виртуальных каналов внутри линка. • **Поддержка любых топологий**
Безопасность	Средняя • Средняя/низкая защита • Использует ГСЧ • **Нет защиты ключа шифрования** • **Нет разделения прав доступа**	Высокая • Выделенное устройство • **Корень доверия (как HSM)** • Управление сертификатами на базе PKI • **Аппаратный ГСЧ** • **Международные/ГОСТ сертификации**
Крипто-стойкость	Низкая • Предопределенные алгоритмы • Нет возможности обновления	Высокая • Широкий набор алгоритмов • **Возможность кастомного алгоритма (ГОСТ)** • Обновление в полях • **Поддержка Кватновых ГСЧ**

Наглядное сравнение Layer 2 vs Layer 3

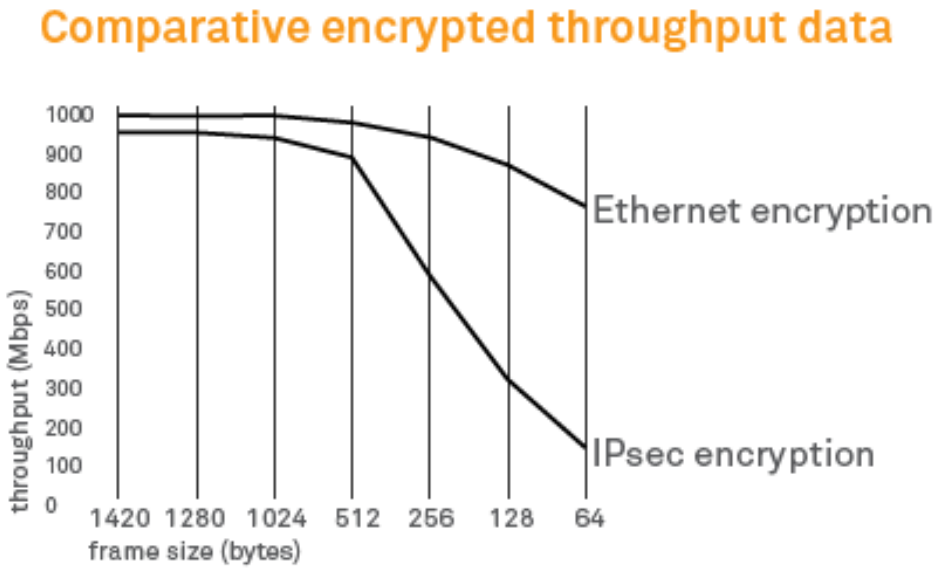
Layer 2 шифрование происходит на уровне Ethernet фрэймов

- Оптимизировано для шифрования на 2-м уровне (OSI)
- Латентность измеряется в микросекундах
- Гарантированная производительность до 100Gbps

Layer 3 шифрование на уровне IP пакетов layer (IPSec)

- Латентность в миллисекундах
- До 50% потеря эффективной полосы пропускания

Maximum throughput with zero protocol overhead



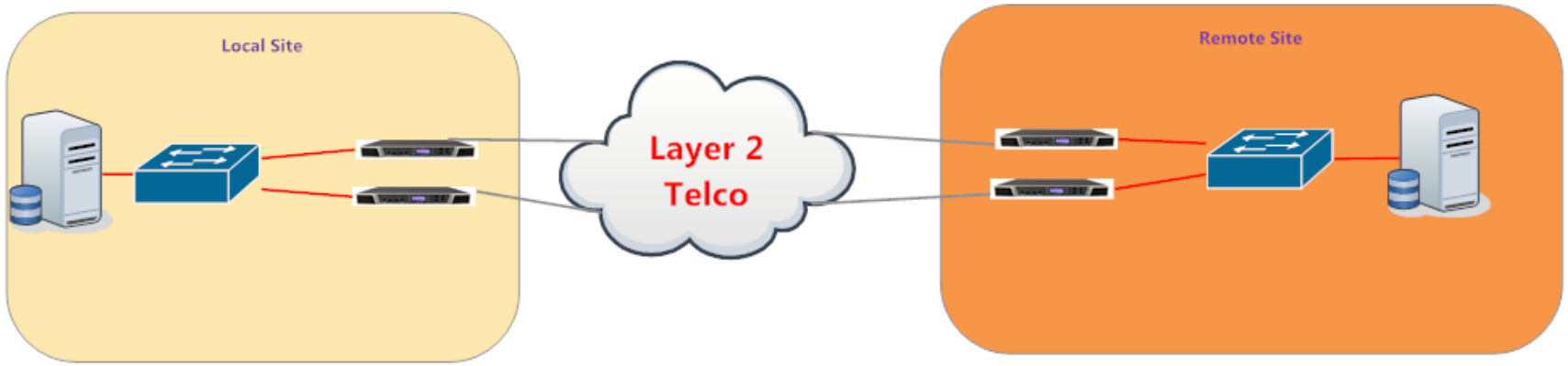
Пример 1 из жизни – Банк на Ближнем Востоке

- SAN поверх Ethernet между двумя площадками
- «Транспорт» предоставлялся местным провайдером

Зачем требовалось шифрование

- Передача важных финансовых данных через публичную сеть
- Был инцидент с утечкой данных клиентов банка
- Риск «прослушки» канала
- проблемы в конфигурации оборудования провайдера (сетевые проблемы и настройки безопасности)

Пример 1: Среда реализации проекта



Технические особенности

- Сеть провайдера с техническими проблемами
- Требовалась минимальная латентность для сети хранения данных
- Существующее IPSec решение не подошло по причине проблем с производительностью

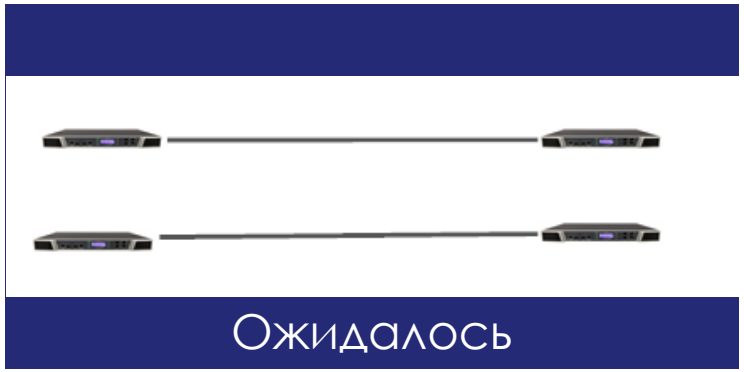
Пример 1: Как развивался проект?

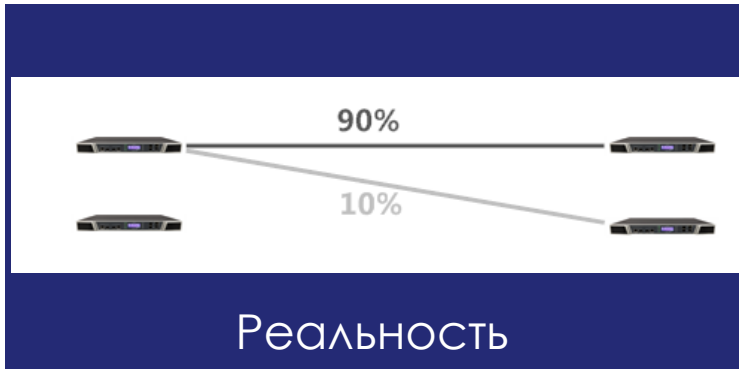
Заказчик заплатил за «пилот»

- 4 * CN6010 были установлены на одном из запасных каналов
- Thales обеспечил развертывание и тренинг на месте
- Устройства работали 6 месяцев

Вызовы

- Сеть провайдера оказалась не Point-to-Point!
- Потребовалось включить механизм управление групповыми ключами для адаптации к сетевым особенностям





- ***Простая задача для HSE но сложная для конкурентов!***

Пример 1: Реализация

POC был признан успешным

- Не возникло проблем при сбое питания
- Шифраторы соответствовали требованиям заказчика по латентности и производительности
- Поставка 8 устройств 1G CN6010
- Все взаимодействие через все каналы сейчас зашифровано
- Был привлечен PS для развертывания и обучения

Пример 1: Адаптация & Масштабируемость

Поддержка изоляции трафика разных владельцев

- Криптографическая изоляция (VLAN)

Подходит для многоадресного трафика

Гибкость в возможностях обслуживания и апгрейда

- Дизайн FPGA vs ASIC
- Обновление на месте
- Легкий вывод на рынок новой функциональности с обновлениями прошивки

Пример 2 – Проблемная область

- Австрийский поставщик электричества и газа
- Промышленная сеть управления SCADA

Зачем нужно шифрование

- Объекты компании считаются «критической инфраструктурой»
- Безопасность и прозрачность жизненно важны для бизнеса
- Факторы риска – «врезка» в каналы и манипуляция данными
- Stuxnet заставил переосмыслить требования безопасности
- Стандарты безопасности становятся законами
- Закон ЕС о кибербезопасности распространяется на промышленные системы

Пример 2 – Описание среды

Техническая среда

- SCADA системы генерируют большой объем данных и отправляют в центр управления
- Сеть объединяет точки добычи газа
- Городские и региональные WAN

Вызовы

- Существующие SCADA устройства в сети работают на 2-м сетевом уровне
- VPN или IPSec не подходят

Пример 2 – Что дальше?

Поставщик SCADA решений рекомендовал Thales HSE

- Был организован «Пилот»
- Проект успешно вредрен

"Мы были уверенны в продукте и производителе с самого начала .

Соотношение цена-качество соответствовало ожиданиям, реализация теста прошла гладко, и поддержка была очень профессиональной »."

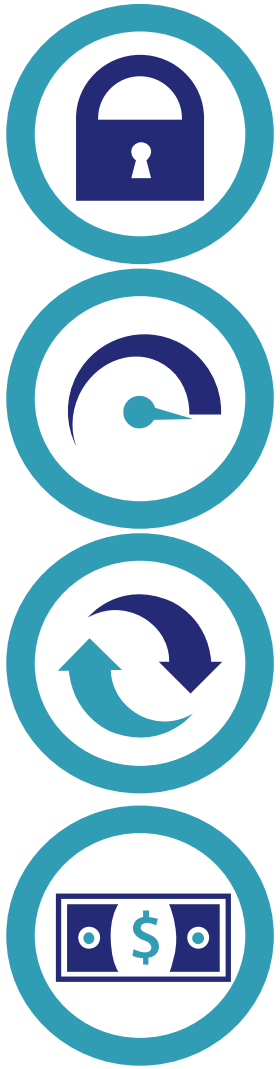
Michael * – Глава системной поддержки**

- Решения SCADA – полный аналог отечественных систем АСУТП

THALES
Building a future we can all trust

Почему Thales, а как же импортозамещение?

SafeNet HSE - #1



Безопасность и надежность

- Сертификация FIPS 140-2 L3, CC, NATO, UC APL
- Настоящее шифрование точка-точка с аутентификацией
- Управление ключами на стороне клиента

Максимальная производительность

- Режимы с нулевыми накладными издержками (доступна полная ширина канала)
- Латентность - микросекунды

Гибко, Масштабируемо и Просто

- Управление в стиле “Установил и забыл”
- Обслуживается и обновляется на месте
- Очень высокие показатели безотказной работы

А вы можете позволить себе не шифровать?

- Готовность платформы для будущих изменений
- Бюджетные модели
- Управление производительностью через лицензию

THALES

HSE – устройства на любой вкус, цвет, бюджет

CV1000

- Усиленный виртуальный апплаенс
- Интеграция с KeySecure
- Поддержка Transport Independent Mode
- **Идеально для Software Defined Networks (SDN) и коммуникации Сервер-Сервер**

CN4000 Series

- 10 Mbps-1 Gbps Ethernet Шифратор
- Сертифицированное, бюджетное и высокопроизводительное устройство
- **Идеальный форм-фактор для удаленных небольших офисов**

CN6000 Series

- 1 Gbps-40 Gbps Ethernet Шифратор
- Сертифицирован по всем основным «западным» стандартам безопасности
- Устанавливается в стойку, отказоустойчивое исполнение
- **Идеально для частных сетей и взаимодействия между офисами и DC**

CN9000 Series

- Коммерческий 100Gbps encryptors
- Единственный «мультипоинт» 100G шифратор
- Полностью совместим со всей остальной линейкой продуктов
- **Разработан для дата-центров «НОВОГО ПОКОЛЕНИЯ» и опорных сетей**

THALES

СИС Крипто ВСШ «Палиндром»

- Высокоскоростной шифратор L2 для распределенных сетей Ethernet
- Сделан в России на общей с Thales и адаптированной для «СИС крипто» аппаратной платформе
- Встроенное ПО отечественной разработки с алгоритмом шифрования ГОСТ Р 34.12-2015 «Кузнечик»
- Скорость передачи данных 10 Гбит/с
- Нулевые потери пакетов, минимальная вносимая сетевая задержка, низкие накладные расходы пропускной способности
- Оптимальный выбор для сплошного шифрования трафика между ЦОДами

CIS Crypto

THALES

THALES

Спасибо!

sergey.kuznetsov@thalesgroup.com