TECHNICAL NOTES

Исследование осуществимости IPSec (в сотрудничестве с Метеослужбой Германии, МЕТЕОФРАНС, ГНМС и КНМИ):

Резюме и рекомендации

Отделение сетей и безопасности

Компьютерный отдел

Май 2003 г.

European Centre for Medium-Range Weather Forecasts
Europäisches Zentrum für mittelfristige Wettervorhersage
Centre européen pour les prévisions météorologiques à moyen terme

Европейский центр среднесрочных прогнозов погоды
Shinfield Park, Reading, Berkshire RG2 9AX, England

Информация в рамках данной публикации предоставляется с честными намерениями и полагается правдивой, но ЕЦСПП не принимает на себя никакой ответственности за ошибки, пропуски, а также потери и ущерб, которые могут возникнуть при ее использовании.

Содержание

Стр.

1 Введение

В 2002 г. ЕЦСПП и четыре государства-члена (Германия, Греция, Франция и Нидерланды) предприняли испытания IPSec с целью оценки осуществимости использования ВЧС, основанной на IPSec и предусматриваемой в качестве резерва для РСПМД для передачи тех данных, объем которых превышает возможности РСПМД.

Поскольку бóльшая часть сайтов РСПМД имеет доступ к Интернету, использование ВЧС, основанной на IPSec, в качестве дополнительного средства резервирования в случае отказа линии РСПМД и связанного с ней резерва в виде ISDN, поможет гарантировать непрерывность обслуживания.

РСПМД является специализированной сетью, целевым назначением созданной для передачи данных в реальном времени и оперативном режиме, но различные выделенные диапазоны частот имеют ограниченную пропускную способность. Интернет можно использовать в дополнение к РСПМД для передачи данных в тех случаях, когда возможности РСПМД недостаточны. Однако следует иметь в виду, что:

- Интернету не хватает концепции гарантированной производительности и QoS (качества обслуживания); он также подвержен различным атакам, включая атаки типа DoS (отказ в обслуживании).
- На Интернете время от времени случаются продолжительные отказы.

В данном документе сообщается о результатах испытаний IPSec, а также предоставляются руководящие принципы и рекомендации для создания безопасных соединений с использованием Интернета. Он разделен на четыре части:

Часть 1 - дается краткое введение в виртуальные частные сети и IPSec.
Часть 2 - описываются выполненные испытания IPSec.
Часть 3 - представлены результаты этих испытаний.
Часть 4 - приводятся подробные рекомендации.

2 Технический обзор

2.1 Определение IP-ВЧС

Виртуальная частная сеть – это группа из двух или более компьютерных систем "безопасно" соединенных с использованием сети передачи данных общего пользования. ВЧС может быть создана между отдельной машиной и частной сетью (удаленный пользователь-сайт), либо между частными сетями (сайт-сайт). Характеристики безопасности различаются от продукта к продукту, но большинство экспертов по безопасности согласно с тем, что ВЧС должна включать кодирование, строгую аутентификацию удаленных пользователей или хост-компьютеров, а также механизмы сокрытия и маскировки информации о топологии частной сети от лиц, которые потенциально могут организовать атаку на эту частную сеть, используя сети общего пользования.

2.2 Протокол IPSec

IPSec является протоколом сквозной безопасности: все функциональные характеристики и алгоритмы соединения ВЧС остаются в конечных точках, либо в шлюзовом интерфейсе, либо в конечном хост-компьютере.

Пользователи IP-сети, предоставляемой поставщиком услуг, не знают о существовании IP-ВЧС, поскольку технологии туннелирования обеспечивают передачу прикладных данных с помощью их упаковки. Адрес источника и адрес места назначения этих пакетов являются адресами IP конечных точек туннеля. Затем они маршрутизируются как любые обычные IP-пакеты по IP-сети общего пользования.

В прошлом было разработано несколько протоколов туннелирования IP. Однако на протяжении последних трех лет IPSec стал доминирующим протоколом туннелирования IP и в настоящее время является прекрасной технологией при осуществлении соединений сайт-сайт с применением сети общего пользования. IPSec изначально был разработан для обеспечения частных коммуникаций по IP-сетям общего пользования. Протокол поддерживает две основных функции обеспечения безопасности:

- аутентификация: обеспечение аутентичности и целостности всего IP-пакета;
- кодирование: обеспечение конфиденциальности полезной нагрузки.

С помощью IPSec возможно определить туннель между двумя шлюзовыми интерфейсами. Шлюзовой интерфейс, работающий с IPSec, как правило должен иметь маршрутизатор доступа или брандмауэр, на которых осуществляется IPSec-протокол. Шлюзовые интерфейсы IPSec располагаются между частной сетью пользователя и сетью общего пользования, предоставляемой поставщиком услуг.

IPSec-туннели создаются динамически и уничтожаются, когда не используются. Для создания IPSec-туннеля два шлюзовых интерфейса должны аутентифицировать друг друга и определить, какие алгоритмы и ключи безопасности они будут использовать для этого туннеля. Полный исходный IP-пакет кодируется и помещается между заголовками IPSec, используемыми для аутентификации и кодирования. Он становится полезной нагрузкой нового IP-пакета, для которого IP-адреса пункта отправления и пункта назначения являются IP-адресами, используемыми на сети общего пользования для шлюзовых интерфейсов IPSec. Этим обеспечивается логическое разделение потоков полезной нагрузки между ВЧС и IP-сетью общего пользования. Затем между оконечными точками туннеля используется традиционная IP-маршрутизация.

IPSec достигает этих целей, используя:

- два протокола обеспечения безопасности полезной нагрузки: аутентификационный заголовок (AH), который обеспечивает целостность данных, а также протокол платной нагрузки в оболочке безопасности (ESP), который обеспечивает целостность и секретность данных;
- протокол управления с ключом кодирования: обмен по ключу с помощью Интернета (IKE), который используется для согласования IPSec-соединений.

Дополнительная информация о протоколе IPSec содержится в ссылках, перечень которых имеется в приложении B.

3 Испытания IPSec

Основными целями этих испытаний были:

- **Оценить осуществимость использования IPSec-туннелей для создания соединения сайт-сайт:**
  Хотя и было написано несколько документов, касающихся осуществления IPSec и различных связанных с этим вопросов, этот протокол стоило испытать, с тем чтобы детально его понять, оценить его сложность и осуществимость его реализации в контексте РСПМД.

- **Испытать возможности взаимодействия оборудования при применении IPSec:**
  Метеорологические центры, подсоединенные к РСПМД, могут уже иметь какое-то оборудование (маршрутизатор, брандмауэр и т.д.), которое способно поддерживать IPSec. Даже если возможность взаимодействия не будет сегодняшней проблемой, возможности взаимодействия различных устройств должны быть проверены.

- **Сформулировать глобальные рекомендации:**
  Владельцы сайтов РСПМД, которые рассматривают вопрос об осуществлении IPSec, могут использовать данный документ и его рекомендации в качестве отправной точки.

3.1 Настройка параметров IPSec

Поскольку испытание всех характеристик и возможностей IPSec неосуществимо, эти проверки были сконцентрированы на их части. Для каждого параметра IPSec были выбраны исходные варианты:

Туннельный режим в сравнении с транспортным

Как протокол AH, так и протокол ESP, функционируют в двух режимах: транспортный и туннельный. Каждый из этих режимов имеет собственное применение:

- туннельный режим обычно используется для кодирования полезной нагрузки между шлюзовыми интерфейсами, безопасность которых обеспечивает IPSec;
- транспортный режим используется между оконечными станциями, поддерживающими IPSec, либо между оконечной станцией и шлюзовым интерфейсом, если интерфейс рассматривается в качестве хост-компьютера.

Поскольку целью испытаний было исследование безопасности соединений сайт-сайт, то в рамках данного исследования *рассматривался "туннельный режим" IPSec* (см. рисунок 1 ниже).

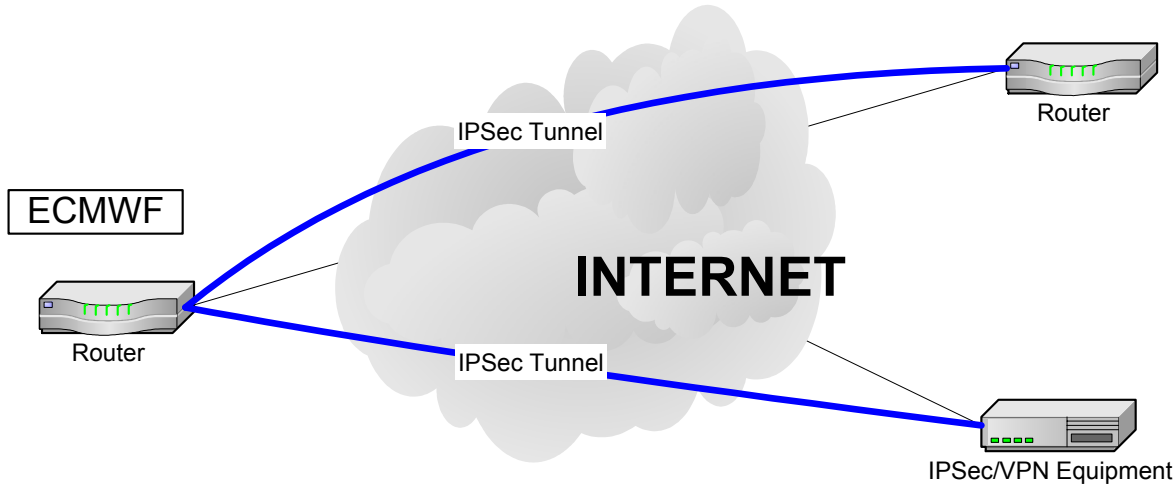

Рисунок 1 – Испытания "туннельного режима" IPSec

Обмен по ключу

Ключами туннеля IPSec можно управлять либо вручную, либо динамически. По причинам, связанным с универсальностью и управляемостью, в ходе испытаний *был использован протокол IKE для динамического управления ключами*.

Метод аутентификации устройств

Протокол IKE является очень гибким и поддерживает многочисленные методы аутентификации. Два равных по техническим возможностям узла должны согласовать общий метод аутентификации. Двумя основными протоколами аутентификации являются:

- **Предварительно согласованный ключ:**
  Один и тот же ключ конфигурируется в каждом IPSec-узле. IKE-узлы аутентифицируют друг друга с помощью подготовки и отсылки защищенных ключом случайных данных с использованием сконфигурированного, предварительно согласованного ключа. Если принимающий узел способен создать те же самые случайные данные, независимо используя собственный, предварительно согласованный ключ, ему становится известно, что оба узла должны обладать одним и тем же секретом, аутентифицируя, таким образом, другой узел.

- **Подпись по криптосхеме RSA (алгоритм Ривеста, Шамира, Адлемана):**
  В этом протоколе используется цифровая подпись, с помощью которой каждое устройство в цифровом виде подписывает комплект данных и посылает его другой стороне. В подписях RSA используется CA (основание сертификата), предназначенное для генерации единственного цифрового сертификата, который назначается каждому узлу для аутентификации. Цифровой сертификат аналогичен по функциям предварительно согласованному ключу, но обеспечивает гораздо более высокий уровень безопасности.

Предварительно согласованные ключи легко осуществить, но достаточно трудно приводить к масштабу, поскольку каждый узел IPSec должен быть сконфигурирован с предварительно согласованным ключом для каждого другого узла, с которым он будет устанавливать сеансы связи. Кроме того, предварительно согласованные ключи обеспечивают меньший уровень безопасности и в некоторых видах оборудования конфигурируются в формате свободного текста, например в маршрутизаторе Cisco.

Поэтому *были использованы подписи RSA с применением сертификатов x509 v.3*.

Целостность и достоверность данных

Целостность данных достигается за счет профиля сообщений (или идентификационной метки) для данных внутри пакетов IPSec. Профили сообщения рассчитываются с использованием хэш-функций. Все устройства, способные обрабатывать IPSec, должны поддерживать хэш-функции HMAC-MD5 и HMAC-SHA, как это установлено в RFC (запрос на комментарии) 2401. Поэтому другие, менее распространены в применяемые хэш-функции, не рассматривались. HMAC-MD5 и HMAC-SHA основаны на MD5 и SHA в сочетании с дополнительными характеристиками кодирования алгоритма HMAC. Это делается во избежание взлома самого профиля сообщения. MD5 создает 128-битный профиль сообщения, а SHA – 160-битный, поэтому SHA является более защищенной хэш-функцией, чем MD5. Однако использованные варианты HMAC-MD5 и HMAC-SHA были усечены до самых значимых 96 битов. Усечение имеет преимущества в смысле безопасности (меньше информации в профиле для тех, кто производит атаку) и недостатки (производящему атаку приходится предсказывать меньше битов). По нашему мнению, обе усеченные версии HMAC-MD5 и HMAC-SHA обеспечивают достаточную безопасность для удовлетворения наших требований.

В нашей среде, в которой производились испытания, *использовались как HMAC-MD5, так и HMAC-SHA; небольшое предпочтение отдавалось HMAC-SHA*

Кодирование данных

Конфиденциальность данных достигается в IPSec путем использования симметричных алгоритмов кодирования и ключей для проведения сеанса. Наиболее широко используемыми алгоритмами являются:

- ESP-NULL: никакого кодирования не применяется;
- DES (стандарт кодирования данных): обеспечивает кодирование с использованием 56-битного ключа;
- 3DES (стандарт тройного кодирования данных): обеспечивает кодирование с использованием 168-битного ключа;
- AES (стандарт усовершенствованного кодирования): обеспечивает кодирование с использованием ключей длиной 128, 192 и 256 битов.

В соответствии с RFC 2401 все устройства, работающие с IPSec, должны поддерживать по крайней мере алгоритмы ESP-NULL и DES. Однако из-за короткого ключа DES считается слабым алгоритмом кодирования, и поэтому некоторые продавцы не советуют его использовать, а другие отказываются его поддерживать (например, FreeS/Wan).

Поэтому для данного испытания *использовались везде, где это было возможно, NULL (без кодирования) и алгоритм кодирования 3DES*. DES использовался только тогда, когда 3DES не был доступен.

Международное применение ВЧС, защищенных IPSec, с использованием Интернета должно соответствовать законодательству каждой страны (кодирование, размер ключа и т.д.). Поэтому перед тем, как использовать кодирование, каждому владельцу сайта следует получить информацию о национальной политике в этом отношении.

Обмен ключами сеанса

Протокол Диффи-Хеллмана (DH) является протоколом шифрования с открытым ключом. Он позволяет двум сторонам установить известный только им секрет. DH используется в рамках IKE для создания двустороннего секрета, который используется в качестве ключа для сеанса.

Наиболее распространенными группами DH являются:

- группа 1: используется 768-битный открытый ключ для создания двустороннего секрета;
- группа 2: используется 1024-битный открытый ключ для создания двустороннего секрета.

Для нашего испытания *была использована группа 2 DH*, поскольку она обеспечивает более высокую степень безопасности и не создает какой-либо перегрузки для устройств, работающих с IPSec.

3.2 Лабораторные испытания

С целью проверки выбранных параметров настроек характеристик IPSec, а также до выполнения любых внешних испытаний (через Интернет), в ЕЦСПП была создана структура для проведения некоторых предварительных экспериментов. Цель этих испытаний – ознакомиться с процессами конфигурации IPSec и подготовки сертификатов.

На рисунке 2 приводится конфигурация структуры, созданной для испытаний.

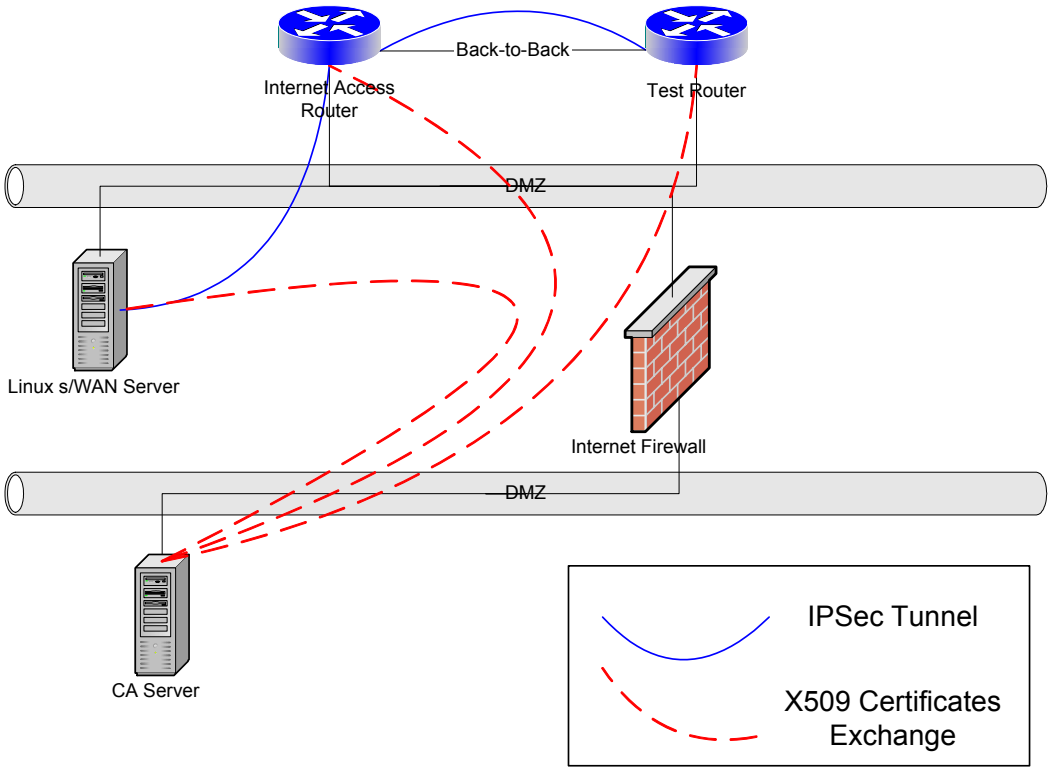

Рисунок 2 – Сетевая конфигурация структуры для осуществления испытаний

С этой настройкой мы получили возможность проделать следующее:

- испытать три различных метода аутентификации: предварительно согласованные ключи, открытое кодирование (RSA_ENCR) и открытые ключи с подписью на основании сертификации (RSA_SIG);
- испытать процесс создания и использования сертификатов X509;
- выполнить базовую конфигурацию IPSec: создать туннели с выбранными параметрами IKE/IPSec;
- испытать осуществление IPSec в домене общего пользования: FeeS/WAN;
- проверить взаимодействия между несколькими устройствами на уровне IPSec.

Структура для испытаний была также использована в ходе испытаний на Интернете для воспроизведения проблем с целью их исправления.

3.3 Испытания на Интернете

На рисунке 3 показана общая схема испытаний IPSec, выполненных на Интернете общего пользования. Их целью было создание безопасных соединений между ЕЦСПП и государствами-членами, а также их использование для передачи данных. Примеры конфигурации можно найти в приложении A.

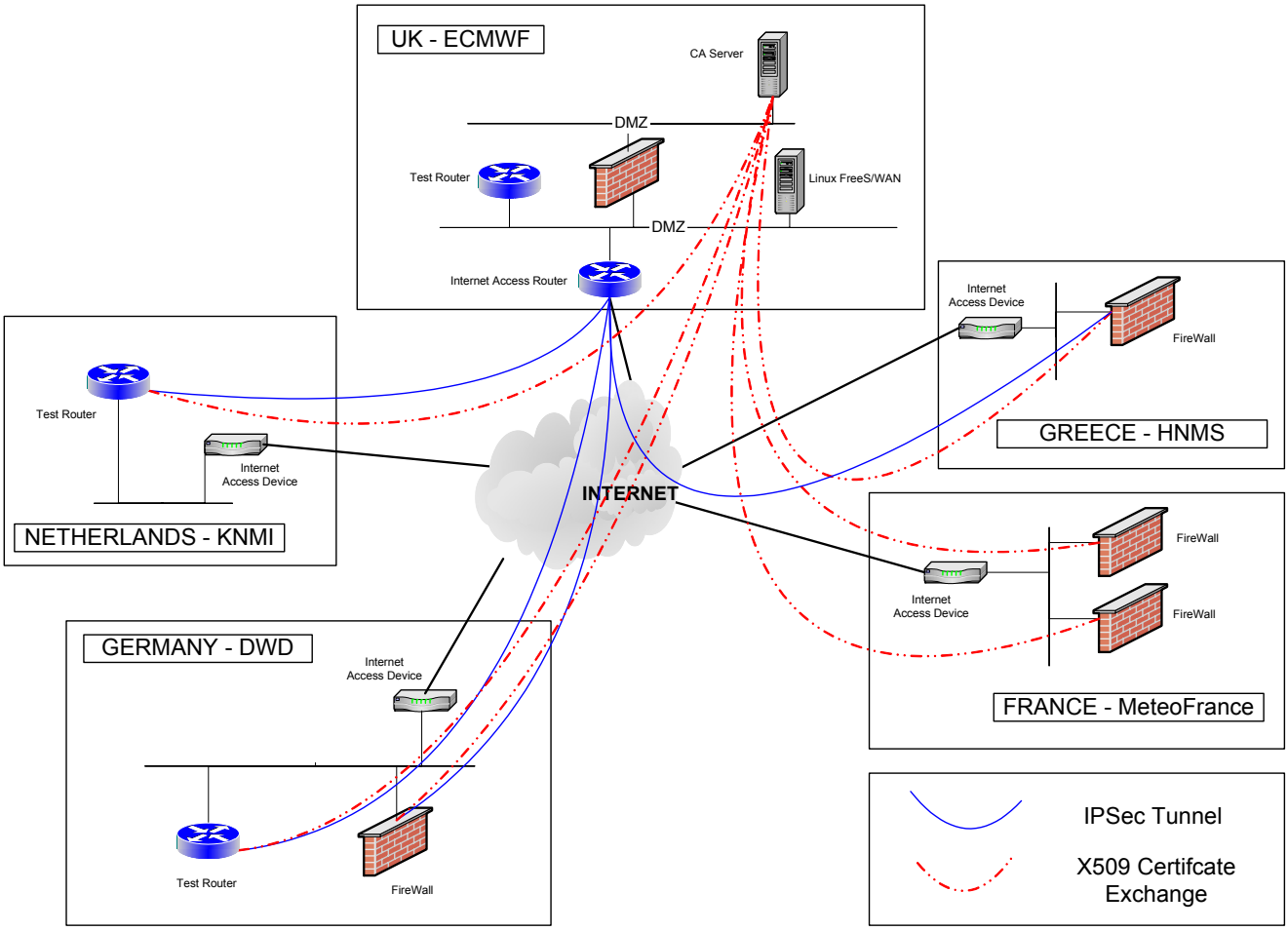

Рисунок 3 – Конфигурация сети для испытаний на Интернете

4 Результаты испытаний

В следующих разделах кратко описываются четыре испытания, проведенных совместно с государствами-членами, а также выдвигаются на первый план некоторые аспекты полученного опыта.

4.1 Испытание № 1: Составление сертификата и аутентификация устройств

Цель этого испытания – посмотреть, каким образом различные устройства пройдут процесс составления и использования сертификата X509 для аутентификации устройств. Если бы здесь возникли проблемы с устройствами, использующими сертификаты X509, то ранее согласованные ключи были бы сконфигурированы вручную. На большей части проверенных устройств было с успехом выполнено составление и использование сертификатов для аутентификации[1].

Основные проблемы, которые встретились в ходе этого испытания, были связаны с тем фактом, что в устройствах используются различные методы составления сертификата (главным образом URL и загрузка типа "out-of-band"), а также различные форматы сертификатов.

[1] Оборудование CheckPoint FW1: было проверено только составление сертификата. FW1 требует контрольного листа передачи (CRL) для начала процесса IPSec. Использование CRL не включались в испытания. Это будет сделано на будущей стадии.

4.2 Испытание № 2: Целостность данных

Цель данного испытания – создать основные соединения IPSec с использованием алгоритма HMAC (SHA и MD5) для проверки целостности данных. При согласовании IKE использовался сертификат X509, загруженный из сервера CA. За исключением FreeS/WAN, который не осуществляет протокол AH, все проверенные устройства смогли создать IPSec-тоннели с использованием алгоритма HMAC с протоколами AH и ESP.

4.3 Испытание № 3: Кодирование данных

Это испытание является продолжением испытания № 2; при нем было добавлено кодирование 3DES. Когда кодирование 3DES недоступно, использовалось кодирование DES. Эти испытания были успешно выполнены. Однако важно учесть, что возможность кодирования 3DES/DES зависит от аппаратного обеспечения и версий программного обеспечения.

4.4 Испытание № 4: Проверки характеристик функционирования

С целью оценки воздействий IPSec-туннелирования на ЦП была предпринята группа испытаний с применением FTP. Было выполнено несколько FTP-испытаний, как с созданием туннелей IPSec, так и без этого. Конфигурация, приведенная ниже (рисунок 4), использовалась для проведения FTP-испытаний; маршрутизатор B представляет собой исходный удаленный маршрутизатор, который гарантирует государствам-членам подключение к Интернету в обоих направлениях.

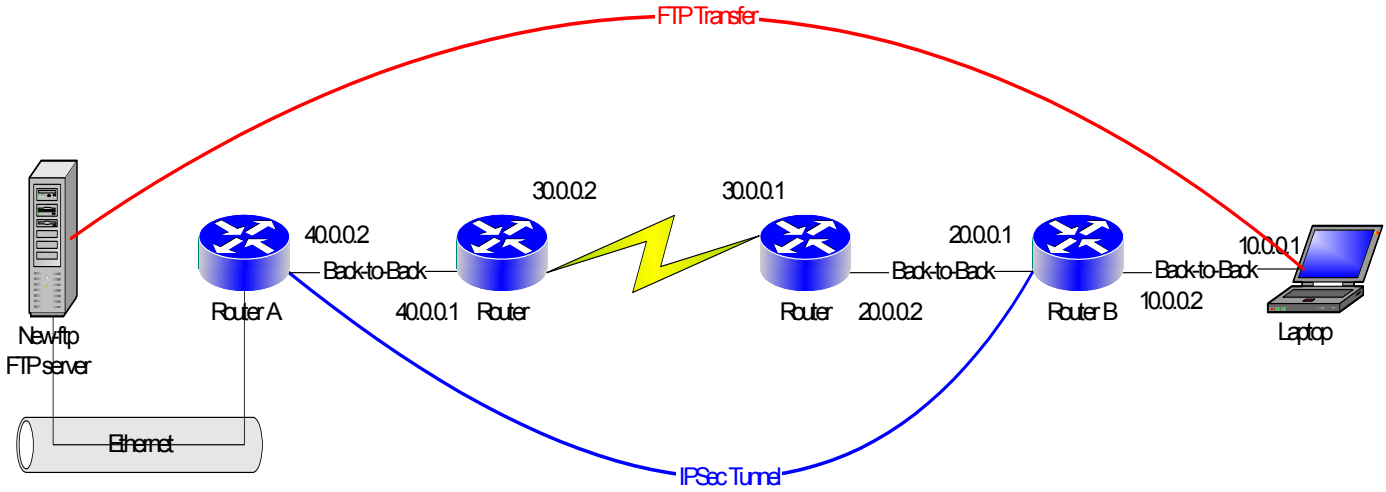

Рисунок 4 – Настройка при лабораторных испытаниях с применением FTP

Испытания также проводились на Интернете между ЕЦСПП и брандмауэром Cisco PIX, имеющимся в Метеослужбе Германии.

Основные заключения, полученные в ходе этих проверок характеристик функционирования:

- протокол IPSec оказывает значительное воздействие на загрузку ЦП конкретного устройства;
- кодированные туннели потребляют больше ресурсов ЦП, чем некодированные;
- алгоритм HMAC-MD5 слегка меньше расходует ресурсы ЦП, чем алгоритм HMAC-SHA;
- протокол ESP для целостности данных расходует ресурсы ЦП так же, как протокол AH;
- небольшой маршрутизатор с возможностями IPSec (такой как Cisco 1605) не подходит для IPSec-туннелирования, когда скорость подключения к Интернету выше 128 кб/с.

5 Рекомендации

Нижеследующие рекомендации основаны на результатах испытаний, описанных в разделе 3. Эти рекомендации могли бы помочь владельцам сайтов установить безопасные отсоединения с использованием IPSec на Интернете общего доступа.

5.1 Аутентификация устройств

Использование сертификатов X509 для аутентификации устройств рекомендуется по следующим причинам:

- это самый безопасный метод;
- это самый масштабируемый метод.

Более того, рекомендуется генерация 1024-битных ключей RSA и использование группы 2 DH (алгоритм кодирования).

5.2 Целостность данных

Для аутентификации пакетов могут быть использованы как протокол AH, так и ESP. Однако:

- испытания показали, что ESP расходует столько же ресурсов ЦП, как и AH;
- только протокол ESP может обеспечить кодирование пакетов (см. раздел 4.3).

Поэтому в целях упрощения для аутентификации пакетов рекомендуется использование ESP HMAC. Можно также использовать либо ESP-HMAC-MD5, либо ESP-HMAC-SHA.

5.3 Кодирование данных

В связи с характером данных (метеорологические) кодирование не рекомендуется как обязательное. Поскольку кодирование данных является крупным потребителем ресурсов ЦП, аутентификация пакетов обеспечивает достаточный уровень безопасности. Поэтому рекомендуется использование ESP NULL. Это означает, что ESP будет применяться для пакета без кодирования.
Если понадобится кодирование данных, рекомендуется осуществление ESP-3DES, поскольку этот метод обеспечивает более высокую степень безопасности, чем DES.

5.4 Оборудование, способное работать с IPSec

В свете предыдущих рекомендаций (разделы 4-1–4-3) при выборе устройства, способного использовать IPSec для осуществления ВЧС, следует предусмотреть следующее:

- для обеспечения масштабирования устройство должно быть способным поддерживать IKE и поддерживать стандарт сертификата X509;
- важно, чтобы устройство поддерживало метод кодирования ESP_NULL;
- если предусматривается кодирование данных, то оборудование должно быть способно применять 3DES. Более того, следует принять во внимание, что AES может вскоре стать фактическим стандартом кодирования. Поэтому желательно наличие оборудования, которое также имеет возможности AES, чтобы предусмотреть удовлетворение будущих потребностей;
- для сайтов с высокоскоростным подсоединением к Интернету рекомендуется специализированное устройство, поддерживающее ВЧС с IPSec, с картой кодирования (карта-акселератор), поскольку она значительно снижает нагрузку на ЦП при использовании протокола IPSec.

В качестве последнего замечания: испытания показали, что проще конфигурировать оборудование, имеющее возможности IPSec, чем осуществлять решение проблемы на основе использования домена общего пользования. Тем не менее осуществление открытого источника, FeeS/WAN, может быть рассмотрено с учетом того, что FeeS/WAN осуществляет кодирование 3DES по определению (см. http://www.freeswan.org for further details).

5.5 Проектирование сети

Проектируя осуществление IPSec, следует учесть ряд руководящих принципов. Шлюзовой интерфейс ВЧС должен быть всегда в ДМЗ и никогда внутри "частной" сети. Это означает, что устройство для ВЧС должно быть где-то между брандмауэром и внешней сетью (Интернет); весь поток данных между устройством для ВЧС и частной внутренней сетью должен проходить через брандмауэр, см. рисунок 5. Поскольку устройство для ВЧС располагается в ДМЗ, важно сконфигурировать брандмауэр таким образом, чтобы позволить потоку данных, защищенных IPSec, проходить в брандмауэр и из него. В нижеследующей таблице показаны протоколы IP и номера портов TCP/UDP, которые позволяют применение IPSec на брандмауэре:

Протокол/порт	**Комментарий:**
IP протокол 50	Протокол ESP
Протокол 51 IP	Протокол AH
UDP 500	Согласование IKE
UDP/TCP 10000	Туннелирование NAT

Для реализации IPSec не обязательно использовать специализированное устройство, обеспечивающее работу с IPSec. Осуществимо объединение технического решения для IPSec и возможностей брандмауэра или IPSec и возможностей доступа к Интернету или всех трех возможностей в едином устройстве.

На нижеследующей схеме (рисунок 5) показана топология, по которой специализированное устройство с возможностями ВЧС/IPSec используется с дополнение к маршрутизатору доступа к Интернету и брандмауэру.

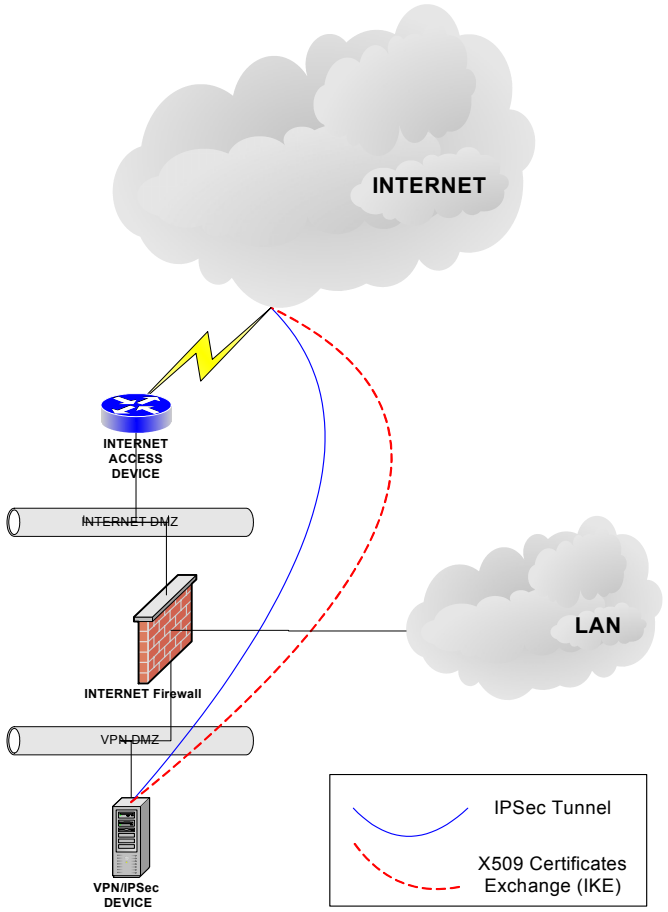

Рисунок 5 – Сетевая схема ВЧС с использованием специализированного устройства для ВЧС

6 Выражение благодарности

Нижеперечисленные лица внесли свой вклад в исследование, а также в создание данного документа:

Inge Essid, Метеослужба Германии

Ilona Glaser, Метеослужба Германии

Erwan Favennec, МЕТЕОФРАНС

Georgios Konstandinidis, ГНМС

Frits van de Peppel, КНМИ

Freerk Feunekes, КНМИ

Camine Rizzo, ЕЦСПП

Ahmed Benallegue, ЕЦСПП

Matteo dell'Acqua, ЕЦСПП

Ricardo Correa, ЕЦСПП

Tony Bakker, ЕЦСПП

Pam Prior, ЕЦСПП

Приложение A – Руководящие принципы и примеры конфигурации

A.1 Выходные и конфигурационные файлы для маршрутизатора Cisco и PIX

Cisco IOS: руководящие принципы составления сертификата

При запросе сертификата от маршрутизатора Cisco рассмотреть основные аспекты:

1 – Конфигурировать имя хост-компьютера маршрутизатора и имя домена: использовать общие команды конфигурации "hostname" и "ip domain-name".

2 – Установить время и дату маршрутизатора: обеспечить, чтобы часовой пояс маршрутизатора, время и дата были аккуратно сконфигурированы с помощью команды "set clock". Часы должны быть установлены до начала конфигурации пары ключей RSA и составления сертификата, поскольку ключи и сертификаты зависят от времени.

3 – Пара ключей RSA должна быть сгенерирована с использованием длины 1024 бита: с применением команды "crypto key generate rsa" сгенерировать пару ключей RSA длиной 1024.

4 – Установить CA и сконфигурировать его параметры:
- установить CA: команда – "crypto ca identity <CA identity>"
- сконфигурировать параметры: "enrolment url <CA server URL> и "crl optinal"
- аутентифицировать CA: "ca authenticate <CA identity>.

5 – Запросить сертификат X509: запрашивая сертификат X509, отвечать "no", если вы хотите включить:
- серийный номер маршрутизатора
- адрес IP в имя объекта

Cisco IOS: результаты составления сертификата

Нижеследующее является результатом составления сертификата, выполненного на маршрутизаторе Cisco:

```
! The first step is to generate the RSA key
Cisco-Test(config)#crypto key generate rsa
The name for the keys will be: mys-cisco.domain.top
Choose the size of the key modulus in the range of 360 to 2048 for your
General Purpose Keys. Choosing a key modulus greater than 512 may take
a few minutes.

How many bits in the modulus [512]: 1024
Generating RSA keys ...
[OK]

! The second step is to identify the CA server
Cisco-Test(config)#ca iden
Cisco-Test(config)#crypto ca identity my-test
Cisco-Test(ca-identity)# enrollment url http://myca.domain.top/cgi-bin/openscep
Cisco-Test(ca-identity)# crl optional
Cisco-Test(ca-identity)#exit
Cisco-Test(config)#crypto ca authenticate my-test
Certificate has the following attributes:
Fingerprint: 8395FE5B C08238A7 FA6BFD76 727E84A7
% Do you accept this certificate? [yes/no]: yes

! The third step is to request a certificate from the CA server
Cisco-Test(config)#crypto ca enrol my-test
%
% Start certificate enrollment ..
% Create a challenge password. You will need to verbally provide this
  password to the CA Administrator in order to revoke your certificate.
  For security reasons your password will not be saved in the configuration.
  Please make a note of it.

Password:
Re-enter password:

% The subject name in the certificate will be: my-cisco.domain.top
% Include the router serial number in the subject name? [yes/no]: no
% Include an IP address in the subject name? [yes/no]: no
Request certificate from CA? [yes/no]: yes
% Certificate request sent to Certificate Authority
% The certificate request fingerprint will be displayed.
% The 'show crypto ca certificate' command will also show the fingerprint.

Cisco-Test(config)#exit
```

```
Cisco-Test#
! Once the 3 steps are completed, two certificates are available in the router: the CA certificate and the router's certificate
Cisco-Test#show crypto ca certificates
CA Certificate
  Status: Available
  Certificate Serial Number: 01
  Key Usage: General Purpose
    EA =<16> ca-email@domain.top
     CN = Org
     O = Org
     L = Place
     ST = county
     C = Country
  Validity Date:
    start date: 08:51:38 GMT Apr 9 2002
    end   date: 08:51:38 GMT Apr 8 2012

Certificate
  Status: Available
  Certificate Serial Number: 3F
  Key Usage: General Purpose
  Subject Name
    Name: my-test.domain.top
  Validity Date:
    start date: 15:56:14 GMT Jun 12 2002
    end   date: 15:56:14 GMT Jun 13 2007
```

Cisco IOS: пример конфигурация IPSec

Нижеследующее является примером конфигурации туннеля ESP-HMAC-SHA ESP-NULL IPSec:

```
hostname Cisco
!
! The time zone must be accurate, as the certificates are time sensitive
clock timezone GMT 0
!
! The following lines describe the CA server name and IP address
ip host myca.domain.top 191.168.1.1
ip domain-name domain.top
!
! CA identity command specifies the local name of the CA server
crypto ca identity my-test
 enrollment url http://myca.domain.top/cgi-bin/openscep
 crl optional
!
! The following lines are the certificates available in the router
crypto ca certificate chain my-test
 certificate 36
  30820338 308202A1 A0030201 02020136 300D0609 2A864886 F70D0101 04050030
  ****
  B49B0FEF 07921B58 B9BD54B2 0713AE83 B6BA3CB4 B8D30EA8 95005EEA
  quit
 certificate ca 01
  30820379 308202E2 A0030201 02020101 300D0609 2A864886 F70D0101 04050030
  ****
  9A81DB7F 902EE833 800B9487 9634907E 9333BE95 88900068 7889AB95 51
  quit
!
! The isakmp (ike) policy parameters are used when the router tries to establish the IKE tunnel
crypto isakmp policy 100
 group 2
!
crypto isakmp policy 200
 encr 3des
 group 2
!
! "transform-set" command defines which kind of IPSec tunnelit  is possible to establish
crypto ipsec transform-set MoreSecure esp-sha-hmac esp-null
!
! A crypto-map links a set of IPSec parameters with the remote IPSec gateway
crypto map IOS_IOS 10 ipsec-isakmp
 description To Cisco-Test internal router
 set peer 10.0.0.1
 set transform-set MoreSecure
 match address 151
!
! Finally, a crypto-map that will be used to establish IPSec tunnels is applied to the physical interface
interface FastEthernet4/0
 ip address 10.0.0.2 255.0.0.0
 crypto map IOS_IOS
!
! The mirror ACL will trigger the IPSec tunnel establishment
access-list 151 permit ip host 192.168.1.2 host 192.168.2.1 log
end
```

Cisco PIX: пример конфигурации

Нижеследующее является примером конфигурации туннеля ESP-HMAC-SHA ESP-NULL IPSec для Cisco PIX:

```
PIX Version 6.2(1)
hostname pix
domain-name domain.top
!
****
!
! The following ACL will be used to trigger the IPSec tunnel establishment
access-list 101 permit ip host 192.168.3.1 host 192.168.1.2

! IPSec protocol must be enabled in the device
sysopt connection permit-ipsec
no sysopt route dnat

! "transform-set" command defines which kind of IPSec tunnel it will be possible to establish
crypto ipsec transform-set MoreSecure2 esp-null esp-sha-hmac

! A crypto map defines the IPSec parameters, which will be negotiated during the IPSec tunnel establishment
crypto map ECMWF_MSS 50 ipsec-isakmp
crypto map ECMWF_MSS 50 match address 101
crypto map ECMWF_MSS 50 set peer 192.168.4.1
crypto map ECMWF_MSS 50 set transform-set MoreSecure
crypto map ECMWF_MSS interface outside

! The isakmp (ike) policy parameters are used when the device tries to establish the IKE tunnel
isakmp enable outside
isakmp policy 10 authentication rsa-sig
isakmp policy 10 encryption des
isakmp policy 10 hash sha
isakmp policy 10 group 2
isakmp policy 10 lifetime 86400

ca identity myca.domain.top 192.168.1.19:/cgi-bin/openscep
ca configure myca.domain.top ca 1 1 crloptional
```

A.2 Пример конфигурации FreeS/WAN

Конфигурационный файл FreeS/WAN (ipsec.conf) для примера конфигурации ESP-HMAC-SHA ESP-3DES:

```
# /etc/ipsec.conf - FreeS/WAN IPsec configuration file

# More elaborate and more varied sample configurations can be found
# in FreeS/WAN's doc/examples file, and in the HTML documentation.

# basic configuration
config setup
        # THIS SETTING MUST BE CORRECT or almost nothing will work;
        # %defaultroute is okay for most simple cases.
        interfaces=%defaultroute
        # Debug-logging controls:  "none" for (almost) none, "all" for lots.
        klipsdebug=none
        plutodebug=all
        # Use auto= parameters in conn descriptions to control startup actions.
        plutoload=%search
        plutostart=%search
        # Close down old connection when new one using same ID shows up.
        uniqueids=yes

# defaults for subsequent connection descriptions
conn %default
        # How persistent to be in (re)keying negotiations (0 means very).
        keyingtries=2
        # RSA authentication with keys from DNS.
        # authby=secret
        authby=rsasig
        #
        # use x509 certificates
        #
        leftrsasigkey=%cert
        rightrsasigkey=%cert
        #
        #freeswan security gateway
        left=192.168.1.20
        leftsubnet=192.168.1.20/32
        leftid=@host.domain.top
        #
        keyexchange=ike
```

```
# the following is the IPSec configuration towards the "cisco" router

conn rw1
  right=192.168.5.2
  rightid=@host.otherdomain.top
  rightsubnet=10.0.0.0/8
  ikelifetime=3600
  keylife=3600
  pfs=no
  auto=start
  esp=3des-sha-96
```

Приложение B – Ссылки

- A cryptographic Evaluation of IPSec – Niels Ferguson and Bruce Scheier – Counterpass Internet Security, Inc. (Криптографическая оценка IPSec)
- Applied Cryptography – Bruce Schneier – Wiley (Прикладная криптография)
- Cisco Secure VPN – Andre G. Mason – Cisco Press (Безопасная ВЧС Cisco)
- FreeS/WAN: http://www.freeswan.org
- IPSec Protocol: http://www.ietf.org/html.charters/ipces-charter.htnl (Протокол IPSec)
- IPSec RFCs – http://www.ietf.org/rfc.html
- IPSec Securing VPNs – Carlton R. Davis – RSA Press (Обеспечение безопасности ВЧС с помощью IPSec)
- VPN Consortium: http://www.vpnc.org (консорциум ВЧС)

Приложение C - Список сокращений

3DES	Стандарт тройного кодирования данных
AES	Стандарт усовершенствованного кодирования
AH	Аутентификационный заголовок
CA	Основание сертификат
CRL	Контрольный лист передачи
DER	Признанные правила кодирования
DES	Стандарт кодирования данных
DH	Ключевое соглашение Диффи-Хеллмана
DWD	Метеослужба Германии
ECMWF – ЕЦСПП	Европейский центр среднесрочных прогнозов погоды
ESP	Платная нагрузка в оболочке безопасности
HMAC	Код аутентификации сообщения с контрольной суммой
HNMS	Греческая национальная метеорологическая служба
IKE	Обмен по ключу с помощью Интернета
IPSec	Протокол безопасности IP
KNMI – КНМИ	Королевский нидерландский метеорологический институт
MD5	Профиль сообщения 5
NAT	Сетевой перевод адресов
PEM	Почта с повышенной секретностью
PKI	Общественная ключевая инфраструктура
QoS	Качество обслуживания
RFC	Запрос на комментарии
RMDCN – РСПМД	Региональная сеть передачи метеорологических данных
RSA	Алгоритм Ривеста, Шамира, Адлемана
SHA	Алгоритм безопасности с контрольной суммой