Эссе по курсу "Защита информации"
Кафедра радиотехники, Московский физико-технический институт (ГУ МФТИ)
http://www.re.mipt.ru/infsec

Выполнил Вишницкий Р.О., 311 гр.

Введение в IPsec.
Introduction to IPsec.

Содержание

Введение

Ещё относительно недавно Интернет использовался в основном только для обработки информации по простым протоколам: электронная почта (SMTP,POP3), передача файлов (FTP,TFTP), удалённый доступ (SSH, Telnet) и т.д. В настоящее время, благодаря широкому распространению web-технологий, Internet все плотнее входит в нашу жизнь. В связи с этим неуклонно растет объем данных, передаваемых по сетям общего пользования. Для обеспечения безопасности взаимодействия посредством Internet разработано несколько протоколов прикладного уровня, однако совершенно ясно, что наличие средств защиты в протоколах TCP/IP-стека, как самых распространенных, позволит осуществлять информационный обмен между гораздо более широким спектром приложений и служб.

Архитектура

IP Security - это комплекс протоколов, касающихся способов шифрования, аутентификации и обеспечения защиты при транспортировке IP-пакетов; в его состав на данный момент входят около 20ти предложений по стандартам и 18ти RFC. Спецификация IP Security (известная ныне как IPsec) разрабатывается рабочей группой IP Security Protocol IETF. Основными функциями IP Security являются:

- Обеспечение конфиденциальности. Отправитель должен иметь возможность шифровать пакеты перед тем, как передавать их по сети.
- Обеспечение целостности. Получатель должен иметь возможность аутентифицировать стороны, учавствующие в процессе обмена информацией, и пакеты IPSec, посылаемые этими сторонами, дабы быть уверенным в том, что передаваемые данные не были изменены в пути.
- Обеспечение защиты от воспроизведения пакетов. Получатель должен иметь возможность обнаруживать и отбрасывать воспроизведенные пакеты, исключая таким образом проведение атак внедрения посредника.

В комплекс IP Security входят следующие протоколы и стандарты (перечислены основные, о которых пойдет речь в данной работе):

- Internet Key Exchange (IKE), обеспечивающий аутентификацию сторон, согласование параметов ассоциаций защиты (SA), а так же выбор ключей шифрования.
- Authentication Header (AH), обеспечивающий аутентификацию пакетов и выявление их воспроизведения.
- Encapsulating Security Payload (ESP) - обеспечивает конфиденциальность, аутентификацию источника и целостность данных, а также (опционально) сервис защиты от воспроизведения пакетов.
- Hashed Message Authentication Code (HMAC) - механизм аутентификации сообщений с использованием хэш функций.
- Data Encryption Standard (DES), 3DES – стандарты шифрования данных.

Взаимосвязи между протоколами представлены на рисунке 1:

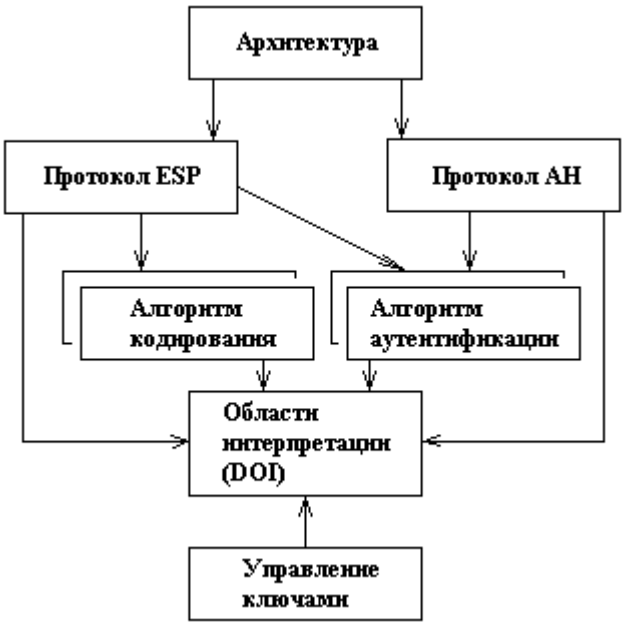

Рисунок 1. Архитектура IPsec

В сущности IPSec работает на третьем уровне модели OSI – сетевом, в результате чего защита передаваемых IP-пакетов становится прозрачной для сетевых приложений. В отличие от SSL (Secure Socket Layer), работающего на транспортном уровне, IPSec призван обеспечить низкоуровневую защиту.

Принципы работы

Целостность и конфиденциальность данных посредством IPsec обеспечивается за счет реализации механизмов аутентификации сторон и пакетов, а также шифрования, которые, в свою очередь, требуют предварительного согласования сторонами параметров информационного обмена – так называемого «контекста безопасности»- используемых криптографических алгоритмов, протоколов управления ключами и их параметров. Спецификация IPsec является алгоритмонезависимой, то есть предусматривает возможность использования сторонами нескольких протоколов и параметров аутентификации и шифрования, различных схем распределения ключей. Результатом согласования контекста безопасности является индекс параметров безопасности (Security Parameters Index, SPI), который представляет собой указатель на определенный элемент базы данных политики безопасности (SPD). На основании информации, содержащейся в SPD, для пакета данных может быть выбрано одно из трёх действий: отбросить пакет, обработать пакет без вмешательства IPSec или обработать пакет с помощью IPSec. В

последнем случае в SPD также содержится указатель на SA (Security Association), который необходимо использовать в процессе обмена данными (если он уже был создан) или указывает параметры, с которыми нужно создать новый SA.

В свою очередь Security Association (SA) – это согласованная политика или способ обработки данных, которыми обмениваются стороны. Два устройства с каждой стороны одной ассоциации защиты содержат данные о протоколах, алгоритмах и ключах, используемых в SA. Отдельно взятая ассоциация защиты используется для связи только в одном направлении, для двунаправленной связи их требуется две. Каждый SA реализует один режим и протокол, поэтому в случае, когда для анализа некоторого пакета требуется применить два протокола (например, AH и ESP, хотя этот случай и является очень редким), требуется создание двух различных SA.

Процесс функционирования IPsec в общем случае можно разбить на следующие шаги:

1. Инициация IPSec. Приложение, трафику которого требуется защита IPSec, начинает процесс обмена данными IKE-протокола.
2. Первая фаза IKE, в которой выполняется аутентификация сторон, и ведутся переговоры о параметрах ассоциаций защиты IKE, в результате чего создается защищенный канал для обмена параметрами защиты IPSec в ходе второй фазы IKE.
3. Вторая фаза IKE, по ходу которой ведутся переговоры о параметрах ассоциации защиты IPSec, создаются соответствующие SA для устройств обеих сторон.
4. Собственно передача данных, т.е. процесс обмена данными, основывающийся на параметрах IPSec и ключах, хранимых в SPD.
5. Завершение работы IPSec. SA IPSec завершают свою работу в результате либо их удаления, либо превышения лимита времени их существования.

В данной работе наиболее подробно будет рассматриваться именно шаг 4, процесс передачи данных. Ссылки на материалы по управлению ключами и протоколу IKE представлены в разделе «Литература».
Теперь перейдем к рассмотрению конкретных протоколов, обеспечивающих защиту трафика при передаче посредством IPsec.

Протокол AH

Протокол, Authentication Header (AH), используется только для аутентификации IP-трафика, но не для обеспечения конфиденциальности. То есть, используя данные этого протокола, мы можем убедиться, что содержимое пакета не изменилось в процессе передачи, и принять меры в случае, если эти изменения произошли (чаще всего – отбросить пакет). Формат заголовка AH представлен на рисунке 2:

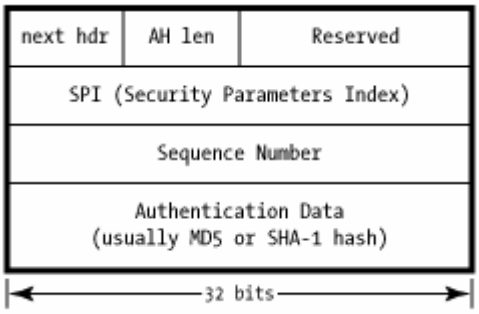

Рисунок 2. Формат AH заголовка

Ниже приведена расшифровка названчения каждого из его полей:

next hdr – идентифицирует протокол, данные которого находятся в следующим за заголовком поле полезной нагрузки
AH len – длина AH заголовка в 32-битных словах минус 2 (смысл вычитания 2х слов приведен в RFC 1883)

Reserverd – зарезервировано для будущих нужд, должно иметь нулевое значение
Security Parameters Index – 32-битный идентификатор параметров безопасности данного соединения в SPD
Sequence Number – монотонно увеличивающееся значение, служащее для того, чтобы исключить атаки воспроизведения пакетов.
Authentication Data – ICV (Integrity Check Value) - значение, вычисляемое по всему пакету, включая большинство полей стандартного IP-заголовка. Получатель вычисляет это же значение, и в случае, если значения совпадут, пакет считается аутентифицированным.

Об алгоритме вычисления последнего значения будет сказано чуть позже.
Существует два возможных варианта использования протокола AH: transport mode (транспортный режим) и tunnel mode (туннельный режим). Рассмотрим каждый из них подробнее.

Transport mode

Используется преимущественно для защиты end-to-end соединений между двумя пользователями. В этом режиме IP-пакет лишь слегка модифицируется – в него вставляется заголовок AH, между заголовком IP и полем полезной нагрузки:

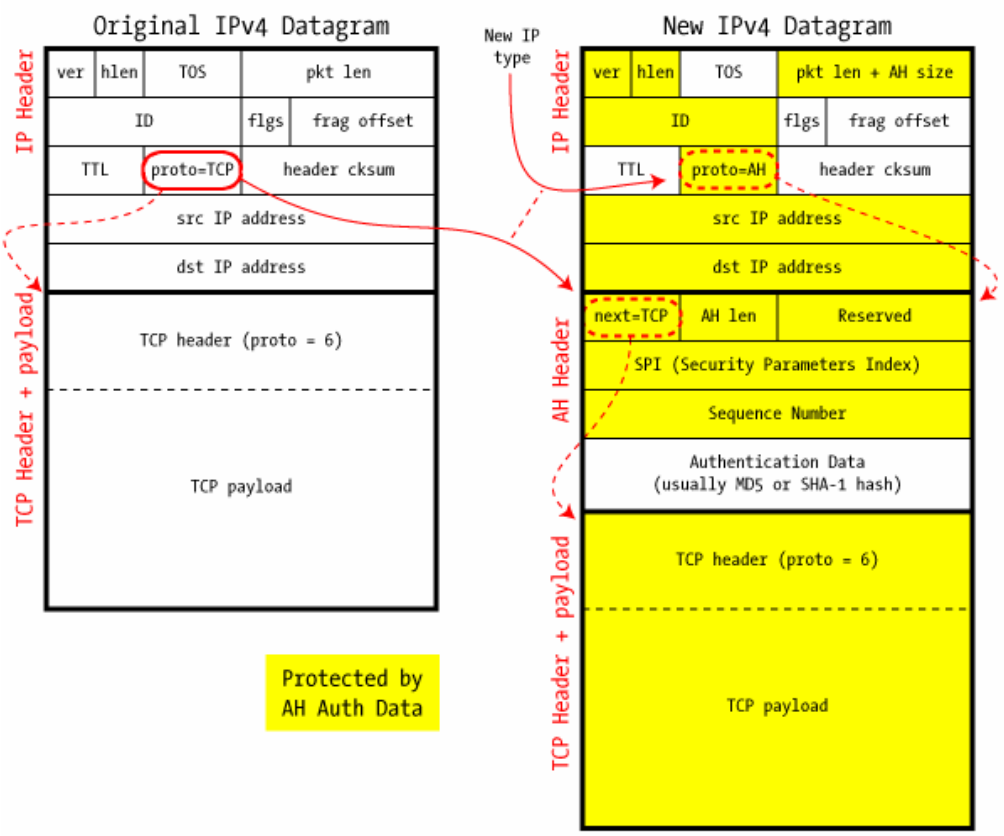

Рисунок 3. AH в транспортном режиме.

Помимо добавления в IP-пакет AH-заголовка изменяется так же значение поля protocol: в нем указывается идентификатор AH, а значение, хранившееся там ранее, перемещается в поле next hdr. В случае успешной аутентификации пакета происходит извлечение загаловка AH и обратная замена идентификатора протокола.
Как видно на рисунке 3, алгоритм вычисления ICV не затрагивает поля, которые могут быть санкционированно изменены по ходу следования пакета по сети (к примеру, поле TTL).

Tunnel mode

Туннельный режим более близок по функциональности к знакомому широкой публике сервису виртуальных частных сетей (VPN), в нем исходные IP-пакеты полностью инкапсулируются в новые и передаются по сети. В месте назначения происходит обратный процесс. Полная инкапсуляция позволяет IP-адресам во вложенном пакете

отличатся от тех, которые будут указаны во внешнем, тем самым реализуя функции туннеля.

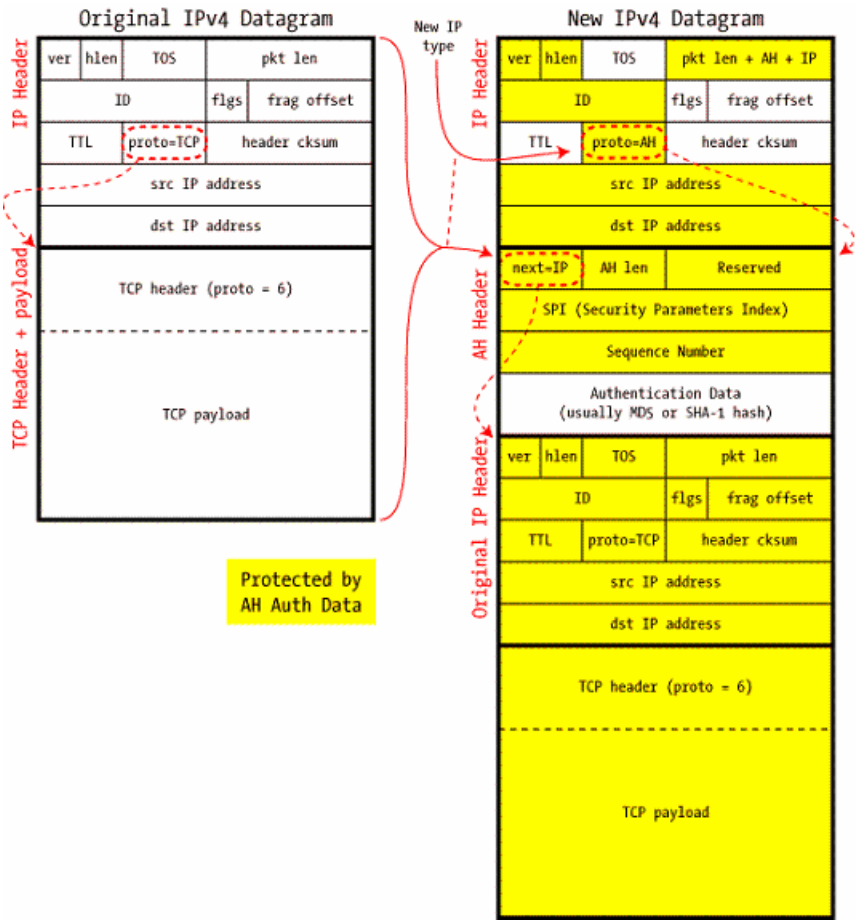

Рисунок 4. AH в туннельном режиме

Как можно видеть из рисунка 4, использование туннельного режима позволяет аутентифицировать все поля исходного IP-пакета: включая те, которые приходилось исключать при использовании транспортного режима.

Транспортный режим чаще всего используется для организации защищенных сеансов связи между двумя оконечными пользователями, в то время как туннельный режим применяется преимущественно для организации связи между маршрутизаторами, что позволяет реализовывать сервисы вирутальных частных сетей.

Алгоритмы аутентификации

В заголовке AH содержится значение ICV, которое может рассчитываться на основе стандартных криптографических алгоритмов хэширования MD5 или SHA-1. Вместо реализации алгоритмов непосредственного вычисления контрольных сумм, в этом случае применяется метод вычисления Hashed Message Authentication Code (HMAC), включающий в себя использование секретных ключей, дабы предотвратить возможность атаки с пересчетом ICV. Детальное описание HMAC можно найти в источниках, указанных в разделе «Литература». Здесь же приведем лишь краткую схему расчета кода аутентификации:

Для расчета HMAC требуется хэш-функция (обозначим её как H) и секретный ключ K. Предположим, что H является хэш-функцией, где данные хэшируются с помощью процедуры, последовательно применяемой к последовательности блоков данных. Обозначим за B длину таких блоков в байтах, а длину блоков, полученных в результате хэширования - как L. Далее введем вспомогательные, «магические» значения

ipad = байт 0x36, повторённый B раз

opad = байт 0x5C, повторённый B раз

Для вычисления HMAC от пользовательских данных, обозначенных как 'text', необходимо выполнить следующую операцию:

ICV = H (K XOR opad, H (K XOR ipad, text))

Эта схема вычисления ICV представлена на рисунке:

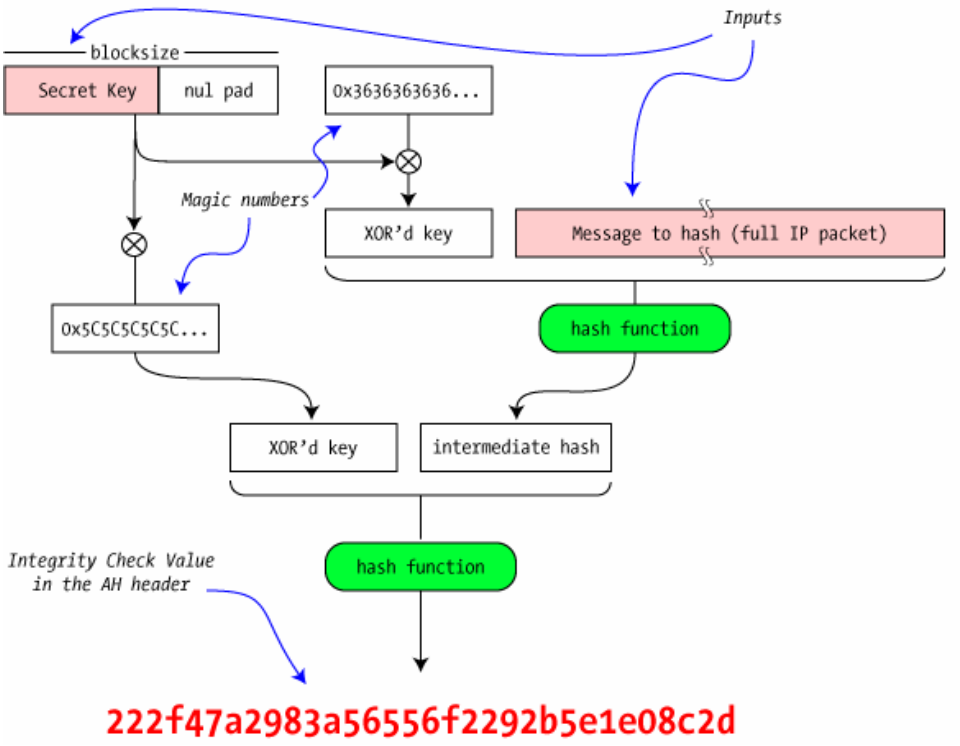

Рисунок 5. HMAC

Стоит упомянуть, что IPsec не предполагает использование фиксированных алгоритмов, требуется лишь их согласованность с обеих сторон, участвующих в обмене информацией. Поэтому сохраняется возможность для использования других функций аутентификации.

Протокол ESP

ESP (Encapsulating Security Payload) – протокол, использующий алгоритмы шифрования для сохранения конфиденциальности передаваемой информации, а потому несколько более сложный. В стандартных реализациях ESP для шифрования данных используется алгоритм DES. Длина ключа, используемого в данном алгоритме, составляет 56 бит, поэтому он не является достаточно устойчивым по сегодняшним стандартам. Ввиду этого обстоятельства большинство производителей в своих имплементациях уже перешли на 3DES,а некоторые и на AES.

Основным отличием ESP от AH является тот факт, что ESP инкапсулирует зашифрованные данные, то есть включает в себя и заголовок, и концевик. Основной функцией ESP является защита трафика от несанкционированного просмотра, в то время как защита от изменения посредством аутентификации является опциональной. Однако ESP аутентифицирует только полезную нагрузку и ESP загаловок, в то время как AH аутентифицирует и большинство полей в стандартном IP-заголовке. На рисунке представлены два формата ESP-пакета с различными опциями: без аутентификации и с аутентификацией трафика

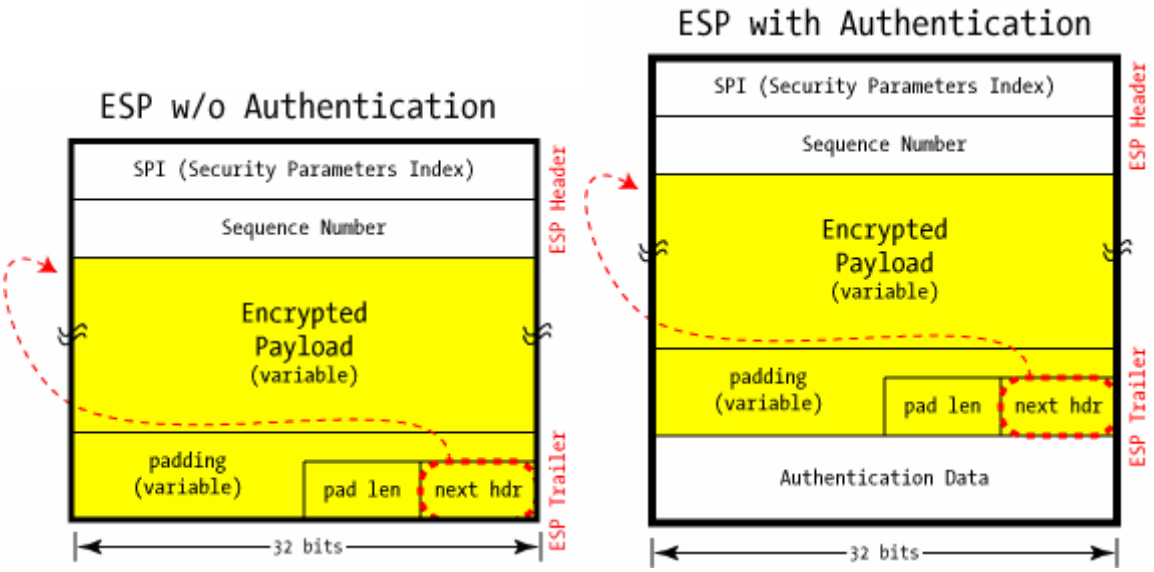

Рисунок 6 ESP

Поля SPI и Sequense Number, next hdr имеют значение, аналогичное соответствующим полям AH.
Encrypted Payload – зашифрованные данные протоколов верхних уровней (TCP, UDP и т.д.)
padding – поле, служащее для выравнивания длины блоков данных
pad len – длина поля padding

ESP, так же, как и AH, может работать как в туннельном, так и в транспортном режиме. Рассмотрим оба режима функционирования ESP в отдельности:

Transport mode

Функционирование ESP в транспортном режиме в целом аналогично транспортному режиму AH, с той лишь разницей, что данные шифруются, и к ним, в случае необходимоскти, добавляется концевик:

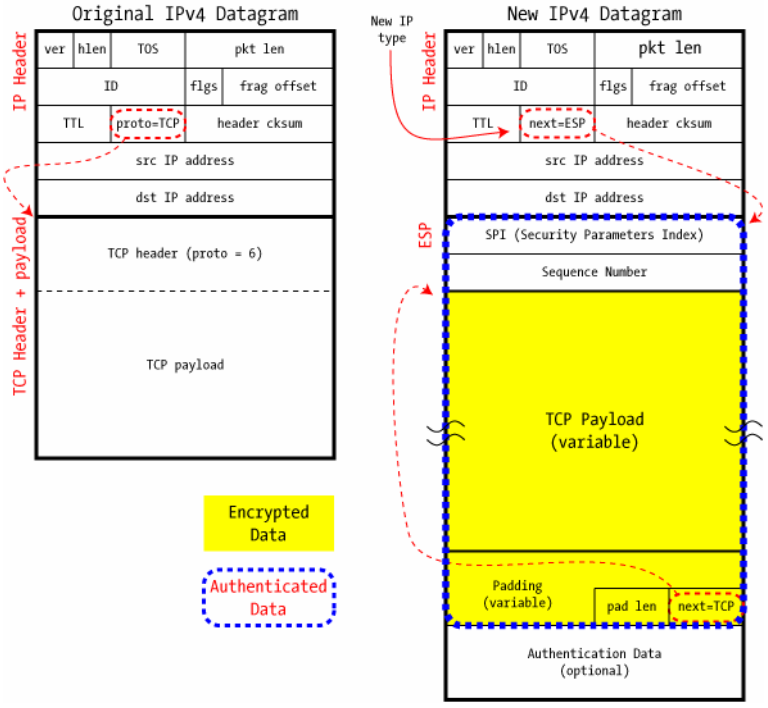

Рисунок 7. ESP transport mode

Tunnel mode

Аналогично туннельному режиму в AH:

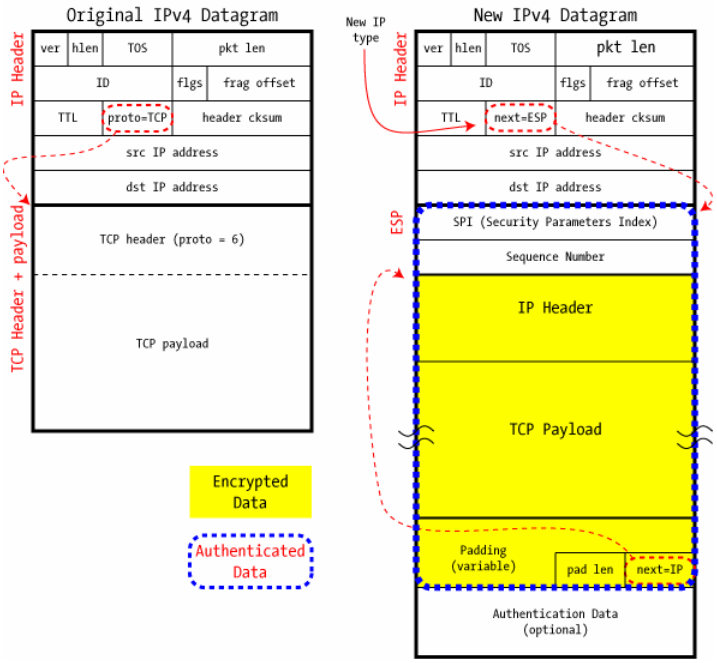

Рисунок 8. ESP tunnel mode

Еще одно отличие режимов в ESP и AH заключается в том, что в AH сторонний наблюдатель всегда может сказать, какой режим используется: если next hdr = IP – туннельный, в других случаях – транспортный. В ESP сторонний наблюдатель не может выяснить режим обработки покетов, поскольку next hdr принадлежит к числу шифруемых полей.

Заключение

После рассмотрения всех используемых в IPsec протоколов можно сделать вывод, что ESP в туннельном режиме с аутентификацией реализует наиболее высокую степень защиты от всех несанкционированных воздействий извне. Этот режим наиболее подходит для создания виртуальных частных сетей.
Вышеописанные средства защиты IPsec реализованы, к примеру, в маршрутизаторах Cisco, брандмауэрах PIX Firewall, клиентах и концентраторах Cisco VPN и многих других устройствах и программных средствах.

Литература

- IPsec-Википедия: http://ru.wikipedia.org/wiki/IPSec#column-one
- TCP/IP guide, IPsec overview and standarts: http://www.tcpipguide.com
- http://www.ietf.org/rfc.html
  - RFC 2104 HMAC: Keyed-Hashing for Message Authentication
  - RFC 2403 The Use of HMAC-MD5-96 within ESP and AH
  - RFC 2404 The Use of HMAC-SHA-1-96 within ESP and AH
  - RFC 2407 The Internet IP Security Domain of Interpretation for ISAKMP
  - RFC 2408 Internet Security Association and Key Management Protocol (ISAKMP)
  - RFC 4301 Security Architecture for the Internet Protocol
  - RFC 4302 IP Authentication Header
  - RFC 4303 IP Encapsulating Security Payload (ESP)
  - RFC 4306 Internet Key Exchange (IKEv2) Protocol