СПбГЭТУ «ЛЭТИ»
ПЕРВЫЙ ЭЛЕКТРОТЕХНИЧЕСКИЙ

Р.Р. Фаткиева

Основы построения защищенных компьютерных сетей

Виртуальные частные сети

СПбГЭТУ «ЛЭТИ», 2021 г.

5. ВИРТУАЛЬНЫЕ ЧАСТНЫ СЕТИ

5.1 Классификация виртуальных частных сетей

При подключении ЛВС к сети Internet возникает угроза несанкционированного доступа к ресурсам как самой сети, так и доступ к передаваемому сетевому трафику. Для реализации защиты ресурсов и данных используются виртуальные сети (Virtual Private Network).

Защищенной виртуальной частной сетью– называется объединение локальных сетей и компьютеров, с территориально удаленными сетями через открытую внешнюю среду передачи данных, обеспечивающую безопасность информационного потока за счет использования механизмов туннелирования.

Организация виртуальных защищенных сетей обладает рядом преимуществ:

- масштабируемость и поддержка удаленного доступа к ресурсам локальной сети (доступ мобильных пользователей к корпоративной сети через провайдеров Internet)
- сокращение расходов на информационный поток через открытую внешнюю среду, вследствие отказа от построения или аренды дорогих выделенных каналов связи.

На виртуальные частные сети накладываются следующие функции:

- аутентификация партнеров взаимодействия;
- обеспечение конфиденциальности, целостности и доступности передаваемого информационного потока;
- управление доступом;
- обнаружение вторжений.

Защита информационного потока в процессе передачи по сети Internet основана на построении защищенных виртуальных каналов связи, называемых туннелями VPN. При этом туннель представляет собой логическое соединение, позволяющее инкапсулировать данные одного протокола в пакеты другого. Пакет протокола более низкого уровня шифруется вместе с заголовком и помещается в поле данных пакета протокола более высокого или такого же уровня и передается по сети. Это позволяет сокрыть не только передаваемую информацию, но и сведения о

внутренней структуре сети - данные о количестве подсетей и узлов и их IP-адресах.

При получении пакета из него извлекают внутренний исходный пакет, расшифровывают и используют его восстановленный заголовок для дальнейшей передачи по внутренней сети.

Туннели VPN создаются для различных типов пользователей:

- ЛВС к ЛВС;
- отдельные удаленные или мобильные пользователи к ЛВС
- отдельные удаленные пользователи друг с другом.

Для создания виртуальной частной сети крупного предприятия используют VPN-шлюзы, VPN-серверы и VPN-клиенты:

- *VPN-клиент* – программный или программно-аппаратный комплекс, на базе персонального компьютера сетевое ПО которого выполняет шифрования и аутентификации трафика, используется для удаленного доступа к VPN;
- *VPN-сервер* – программный или программно-аппаратный комплекс, обеспечивающий поддержание множественных соединений с VPN-клиентами как локальных сетей, так и соединения с мобильными пользователями.
- *Шлюз безопасности VPN*-устройство, прозрачное для пользователей, выполняющее функции шифрования и аутентификации для многочисленных хостов, расположенных за ним. Адрес шлюза безопасности указывается как внешний адрес входящего туннелируемого пакета, а внутренний адрес пакета является адресом конкретного хоста позади шлюза. Реализуется как программно так и аппаратно (маршрутизатор или межсетевой экран), применяется для защиты локальных сетей предприятия.

Классификация сетей VPN:

По архитектуре технического решения:

- *внутрикорпоративные* –обеспечивают защищенное взаимодействие между подразделениями внутри предприятия, группы предприятий, объединенных корпоративными сетями связи, включая выделенные линии;

- *VPN удаленного доступа*–обеспечивает защищенный удаленный доступ к информационным ресурсам мобильным и/или удаленных сотрудников;
- *межкорпоративные VPN*– обеспечивают прямой защищенный обмен информацией со стратегическими партнерами.

По уровню модели OSI:

Для независимости и прозрачности от прикладных протоколов и приложений защищенные виртуальные сети создаются на одном из уровней модели OSI – канальном, сетевом или транспортном. При этом, чем ниже уровень, тем меньше набор реализуемых услуг безопасности и сложнее организация управления VPN. С повышением уровня увеличивается набор услуг безопасности, надежность контроля доступа и конфигурирование системы защиты, однако усиливается зависимость от используемых приложений и протоколов обмена. Защита информационного потока может одновременно выполняться на нескольких уровнях модели OSI, что ведет к увеличению криптостойкости. но снижается пропускная способность сети. В связи с этим защищенные виртуальные сети формируются, как правило, на одном уровне канальном, сетевом, транспортном, или сеансовом.

Канальному уровню соответствуют протоколы PPTP, L2F и L2TP, которые лучше всего подходят для защиты информационного потока при удаленном доступе к локальной сети. Так как в состав операционной системы Windows включена реализация протокола L2TP, то данный протокол получил наиболее широкое распространение для организации защищенного удаленного доступа. Однако формирование канала на описанном уровне имеет ряд недостатков: сложность конфигурирования и поддержки, плохая масштабируемость при необходимости иметь несколько туннелей с общими конечными точками.

Сетевому уровню соответствуют протоколы IPSec, SKIP, IKE. Лидером сетевого уровня является протокол IPSec, входящий в состав версии Internet-протокола – IPv6. Возможность использование протокола IPSec совместно с протоколом L2TP обеспечивает наиболее высокий уровень гибкости при защите виртуальных каналов. Преимущество такого подхода заключается в том, что протокол L2TP отличается независимостью от транспортного уровня,

что полезно в гетерогенных сетях, состоящих из IP-, IPX- и AppleTalk-сегментов.

Для управления криптографическими ключами широко используются протоколы:

- SKIP (Simple Key management for Internet Protocols)– прост в реализации, однако отсутствует поддержка переговоров по поводу алгоритмов шифрования, и если получатель, не сможет расшифровать пакет, то не может согласовать метод шифрования с противоположной стороной;
- IKE – (Internet Key Exchange) поддерживает согласование алгоритмов шифрования, выбран в качестве обязательного протокола для управления ключами в IPSec для IPv6.

Реализация сетей, организованных на канальном или сетевом уровне, заключается в открытии или закрытии канала для передачи трафика по аутентифицированному туннелю, что может вызвать проблему, если сеть на другом конце туннеля ненадежна.

Траспортный/Сеансовый уровень для реализации использует «посредников каналов»-ретрансляция трафика из защищенной сети в открытую для каждого сокета в отдельности на транспортном уровне. Данному уровню соответствуют протоколы:

- SSL/TLS (Secure Sockets Layer/ Transport Layer Security) – обеспечивает взаимную аутентификацию партнеров взаимодействия, конфиденциальность, подлинность и целостность информационных потоков, циркулирующих в канале;
- SOCKS-обеспечивает создание защищенных туннелей для каждого приложения и сеанса в отдельности.

Прикладной уровень защищает только определенную сетевую службу, гипертекстовую, файловую, почтовую, удаленного доступа. Например, протокол SHTTP –дополнение по функциям защиты к протоколу передачи гипертекста http. Протоколы формирования защищенных виртуальных каналов на данном уровне непрозрачны для прикладных протоколов, для каждой службы требуется разработка соответствующей защищенной версии, однако достоинством данного подхода является независимость от среды передачи (IP, IPX, Ethernet, ATM).

По способу технической реализации:

- аппаратные;
- программные;
- интегрированные.

На сегодняшний день наибольшее распространение получили варианты построения VPN, представленные в Табл. 1. Нестандартные схемы построения VPN применяются в случае, если отсутствует необходимость взаимодействия с другими компьютерными системами.

Таблица 1

Вид	*Область применение*	*Используемые протоколы*	*Используемые криптосистемы/ алгоритмы аутентификации*	*Достоинства*	*Недостатки*
VPN на базе маршрутизаторов	Организация не использует межсетевой экран, используя маршрутизатор, совмещающий функции фильтрации трафика и шифрования	Канальный уровень модели OSI L2F, L2TP, Сетевой уровень модели OSI IPSec	DES, Triple Des, /PAP,CHAP, собственные	Возможность встраивание функций поддержки сетей VPN в маршрутизираторы, сокращает расходы и упрощает администрирование	-отрицательное влияние на выполнение функций маршрутизации при неправильной настройке; -уязвимость канала между получателем внутри локальной сети и маршрутизатором; -необходимость использования единого каналообразующего оборудования всеми участниками VPN канала
Программное обеспечение VPN для брандмауэров	Организация использует МЭ для обеспечения комплексной защиты предприятия, однако может пренебречь производительностью при передаче трафика	Канальный уровень модели OSI PPTP, L2F и L2TP Сетевой уровень модели OSI IPSec и SKIP Сеансовый уровень модели OSI SSL/TLS и SOCKS/	DES, RC4,FWZ1, CAST,IDEA,RSA /MD5, SHA-1,CBC DES, MAC	-контроль туннелируемого криптозащищенного трафика; -высокая эффективность администрированияVPN; -комплексная защита информационного потока; -отсутствие избыточности аппаратных платформ для средств сетевой защиты	-возможность снижение производительность брандмауэра за счет операций шифрования потока; -уязвимость канала между получателем внутри локальной сети и брандмауэром; -необходимость модернизации аппаратного обеспечения при повышении производительности серверных продуктов; -необходимость использования единого каналообразующего оборудования всеми участниками VPN канала

Вид	*Область применение*	*Используемые протоколы*	*Используемые криптосистемы/ алгоритмы аутентификации*	*Достоинства*	*Недостатки*
VPN на базе специализированного ПО	Организации необходимо обеспечить возможность подключения удаленных пользователей	Канальный уровень модели OSI PPTP, L2F, L2TP.	DES, 3-DES, CAST,IDEA собственные, ГОСТ /PAP,CHAP, собственные SSL	-масштабируемость, гибкость и мобильность; -низкая стоимость; -оперативное устранение ошибок	-администрирование VPN может потребовать отдельного приложения; -необходимость модернизации аппаратного обеспечения при повышении производительности серверных продуктов
VPN на базе программно-аппаратных средств	Организации необходима высокая производительность при передаче информационного потока.	Канальный уровень модели OSI PPTP, L2F и L2TP Сетевой уровень модели OSI IPSec и SKIP Сеансовый уровень модели OSI SSL/TLS и SOCKS/	DES, 3-DES, собственные, ГОСТ	-высокая производительность; -облегчение обслуживание и конфигурации в многофункциональных аппаратных устройствах; -возможность тонкой настройки для достижения наивысшей производительности в однофункциональных устройствах; -прозрачность для пользователя.	-повышение производительности одного приложения в ущерб другому в многофункциональных блоках; -необходимость отдельных инструментов администрирования и каталогов в однофункциональных устройствах; -трудности с модернизацией из-за высокой стоимости или ее невозможности; -уязвимость канала между получателем внутри локальной сети и аппаратным устройством шифрования трафика .

5.2 Туннелирование на канальном уровне

5.2.1 Протокол PPTP

PPTP (Point-to-Point Tunneling Protocol) — туннельный протокол типа точка-точка, позволяющий компьютеру устанавливать защищённое соединение с сервером за счёт создания специального туннеля в стандартной, незащищённой сети. Разработан он компаниями 3Com и Microsoft с целью предоставления безопасного удаленного доступа к корпоративным сетям через Интернет.

PPTP инкапсулирует кадры PPP в IP-пакеты для передачи по сети. Пакеты, циркулирующие в рамках сессии PPTP, имеют следующую структуру (Рис. 5.1):

- данные;
- заголовок кадра Ethernet;
- заголовок IP;
- заголовок GRE (протокол GRE, используется при инкапсуляции).

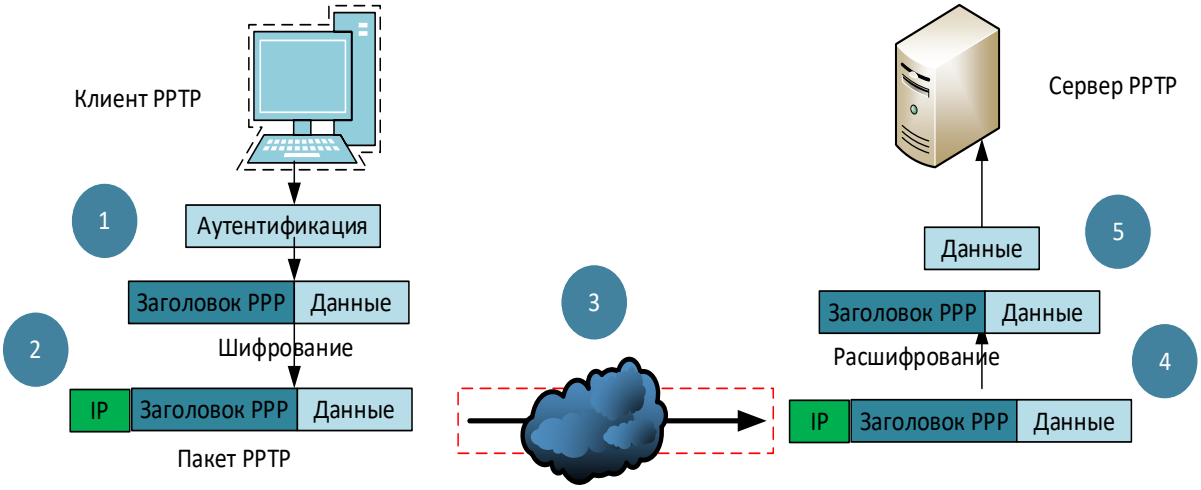

Рис. 5.1

PPTP использует канал с двумя соединениями. Первый канал сформированный по TCP соединению (порт 1723) необходим для управления GRE-соединением. Технология предусматривает аутентификацию удаленного пользователя по протоколу аутентификации PAP (аутентификатор передается в открытом виде) и CHAP (пароль шифруется на основе случайного числа, полученного от сервера). Второй канал устанавливает обычную PPP сессию используя протокола GRE.

Программное обеспечение удаленного доступа, реализующее PPTP, может использовать любой стандарт криптографического закрытия передаваемых данных (RC4).

При прямом соединении хоста с сетью Internet удаленное соединение с сервером устанавливается помощью клиентской части сервиса удаленного доступа. В этом варианте на хосте должен быть установлен клиент RAS и драйвер PPTP, а на сервере удаленного доступа локальной сети – сервер RAS и драйвер PPTP, входящие в Server. Пакеты, передаваемые через это соединение, помимо заголовка канального уровня, содержат заголовок протокола IP, заголовок протокола TCP и управляющее сообщение PPTP в области данных пакета. Если удаленный хост не имеет поддержки PPTP, например создание защищенного канала между сервером удаленного доступа провайдера Internet и пограничным маршрутизатором сети, то в процессе

обмена управляющими сообщениями этот хост не участвует, а функции хоста возложены на сервер удаленного доступа провайдера Internet. В этом случае при обмене управляющими сообщениями PPTP использует порт 1723 TCP, а при передаче инкапсулированных пакетов PPP в заголовке IP устанавливается ID протокола, равный 47. Эти соглашения позволяют использовать технологию PPTP совместно с межсетевыми экранами.

5.2.2 Протокол L2TP

L2TP (Layer 2 Tunneling Protocol) - протокол туннелирования канального уровня. Объединяет протокол L2F (Layer 2 Forwarding), разработанный компанией Cisco, и протокол PPTP корпорации Microsoft. В отличие от PPTP, данный протокол характеризуется более высоким удобством в использовании, а также поддержкой разных сетевых протоколов, например, X.25. В соответствии с протоколом L2F для связи хоста с сервером могут применяться различные протоколы удаленного доступа – PPP, SLIP и другие, добавлена возможность работы с протоколами AH и ESP стека протоколов IPSec.

Протокол использует 2 канала для организации защищённого соединения: канал для передачи данных и канал для формирования управляющих воздействий (рис. 5.2)

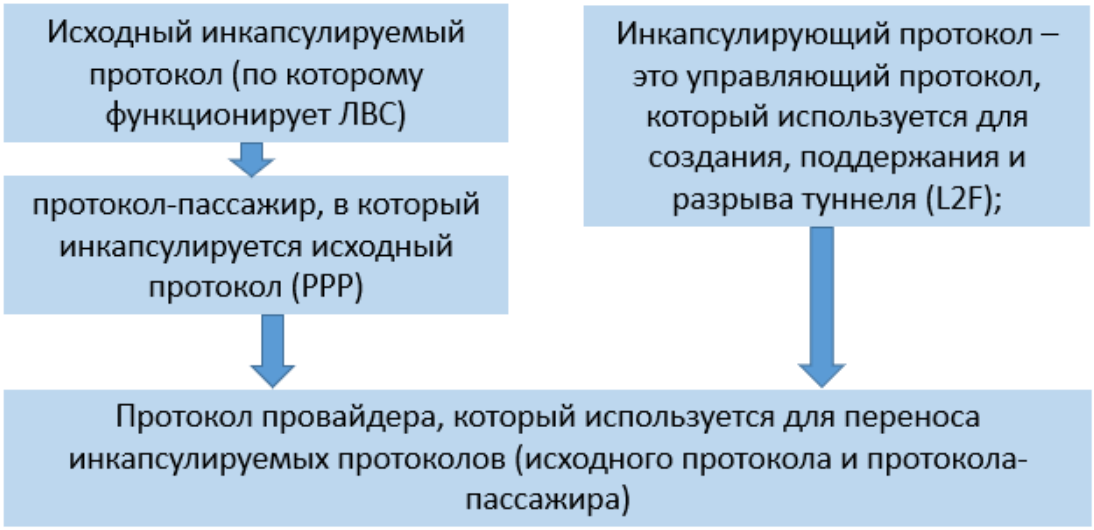

Рис. 5.2

Протокол L2TP начинает сборку пакета для передачи в туннель с того, что к полю информационных данных PPP добавляется сначала заголовок PPP,

а затем заголовок L2TP. Полученный таким образом пакет инкапсулируется протоколом UDP (порт 1701).

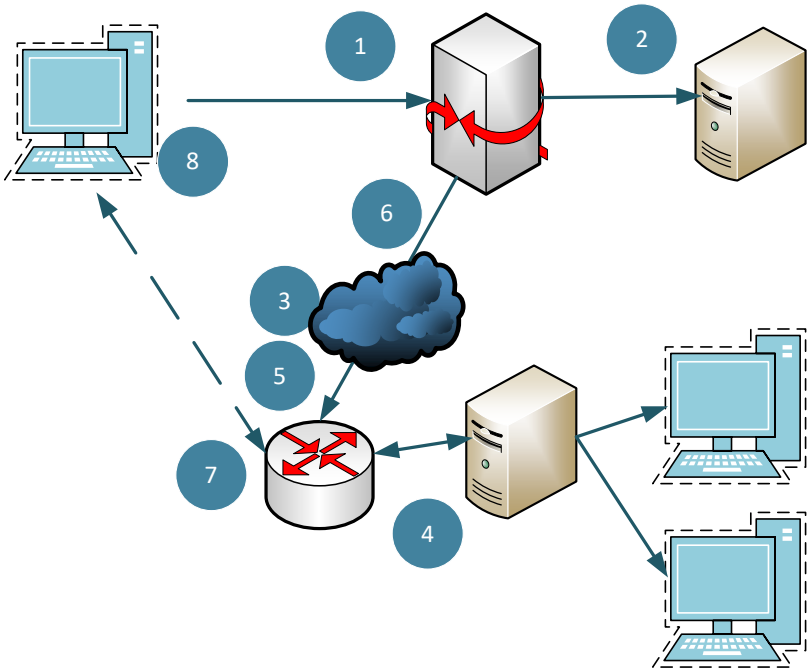

Рис. 5.3

Формирование управляющего канала по протоколу L2F выполняется в соответствии алгоритмом, представленным на Рис.5.3.

1. Удаленный хост устанавливает соединение с сервером RAS (Remote Access Service) провайдера по протоколу PPP, который осуществляет его аутентификацию на основе протокола CHAP, PAP и др.

2. В процессе аутентификации RAS провайдера обращается к серверу провайдера для поиска адрес пограничного маршрутизатора запрашиваемой ЛВС.

3. После получения адреса пограничного маршрутизатора локальной сети проверяется существование туннеля к этому пограничному маршрутизатору. Если туннель отсутствует, то он создается с использованием протокола UDP. На этом этапе генерируется псевдослучайный ключ и отправляет серверу удаленного доступа локальной сети сообщение об установлении новой сессии, включающее информацию для аутентификации. Сгенерированный псевдослучайный ключ используется для защиты пакетов сообщений от подмены.

4. На основе информации, полученной от сервера RAS провайдера, сервер ЛВС осуществляет аутентификацию пользователя (на основании ID пользователя, хэш-функции от пароля и случайной последовательности).

5 Корпоративный шлюз подтверждает возможность создание соединения.

6. Сервер RAS ЛВС создает виртуальный канал по протоколу для передачи.
7. Корпоративный шлюз согласовывает передачу данных по протоколу PPP/
8. После создания канала кадры протокола PPP передаются в обоих направлениях. На сервере RAS провайдера и ЛВС кадры PPP для передачи по Internet очищаются от стартовых и стоповых флагов, инкапсулируются по протоколу L2F в пакеты IP и отправляются. При приеме пакетов IP с инкапсулированными кадрами PPP в пограничных точках Internet серверы RAS провайдера и локальной сети выполняют обратную процедуру.

5.3 Туннелирование на сетевом уровне. Протокол IPSec

IPsec (IP Security) — согласованный набор открытых стандартов, имеющий ядро протоколов для обеспечения защиты данных, передаваемых по межсетевому протоколу IP. Позволяет обеспечить:

- аутентификацию отправителя, с использованием протоколов аутентификации IKE, основанного на алгоритме Диффи-Хелмана;
- конфиденциальность передаваемого трафика, за счет использования механизмов шифрования DES, 3DES;
- целостность данных с применением AH и HMAC;
- защиту от воспроизведения путем использования протокола AH.

Ядро IPSec составляют три протокола:

- AH (Authentication Header) гарантирует целостность и аутентичность данных за счет использования механизмов аутентификации.
- ESP (Encapsulating Security Payload) обеспечивает инкапсуляцию зашифрованных данных, обеспечивая конфиденциальность позволяет поддерживать аутентификацию и целостность данных;
- IKE (Internet Key Exchange) осуществляет обмен ключами и предоставляет конечным точкам защищенного канала секретные ключи,

необходимые для работы протоколов аутентификации и шифрования данных.

Существует несколько способов реализации IPSec:

-интеграция IPSec в конкретную реализацию IP (с изменением исходного кода IP на хосте, или шлюзе безопасности);

-bump-in-the-stack (BITS) реализация (между обычным IP и локальными сетевыми драйверами без доступа к исходному коду стека IP, удобен для встраивания в существующие системы, и реализации на хостах);

-использование внешнего криптопроцессора.

5.3.1 Протокол AH

Протоколы AH и ESP, могут применяться как по отдельности, так и в комбинации с друг другом, обеспечивая транспортный режим и режим туннелирования.

Протокол AH обеспечивает аутентификацию и целостность данных для пакетов IP, передаваемых между двумя системами. Формат заголовка AH показан в соответствии с Рис. 5.4 [1].

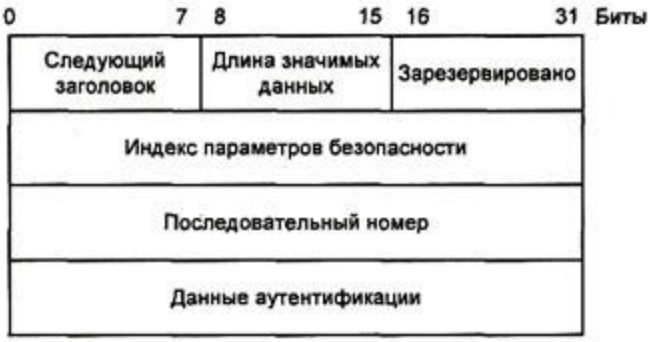

Рис. 5.4

- «следующий заголовок» (Next header) идентифицирует тип значимых данных за аутентификационным заголовком;

- поле «длина значимых данных» (Payload length) определяет длину заголовка AH;

- зарезервированное поле (содержит 0);

- «индекс параметров безопасности» (Security Parameters Index - SPI) - значение, которое в совокупности с адресом назначения и протоколом (AH) определяет ассоциацию безопасности SA;

- «последовательный номер» (Sequence number) - номер пакета;

-«данные аутентификации» (Authentication data) содержат значение контроля целостности (Integrity check value – ICV) и код аутентификации сообщения (Message Authentication Code - MAC) с ключом симметричного или асимметричного алгоритма или хэшфункции;

Рассмотрим алгоритм выполнения протокола AH (Рис.5.5):

1. Осуществляется хэш преобразование IP-заголовка и поля данных исходного пакета.

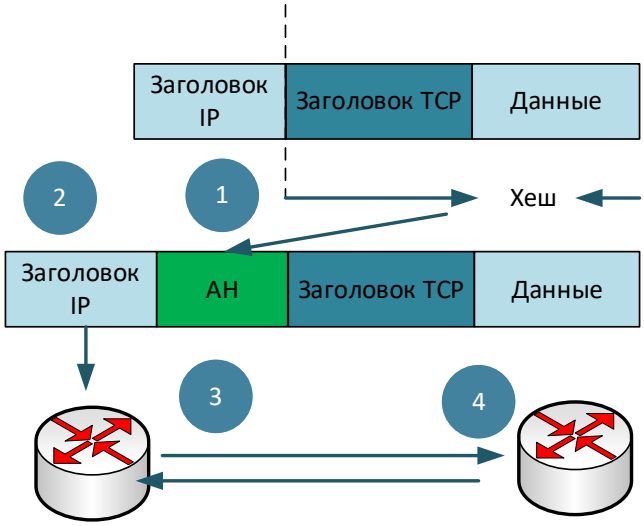

Рис. 5.5

2. Полученный хэш-код используется при построении нового заголовка AH, который подсоединяется к исходному пакету между заголовком и блоком данных.

3. Осуществляется передача пакета получателю.

4. Получатель вычисляет значение хэша для заголовка IP и данных, извлекает переданное значение хэш-кода из заголовка AH и сравнивает эти два значения. При совпадении пакет будет принят (при этом изменяемые поля (например, поля TTL) изменяются промежуточными сетевыми устройствами и не защищаются протоколом AH). Защита от воспроизведения пакетов, осуществляется путем присвоения порядкового номера пакета.

5.3.2 Протокол ESP

ESP (Encapsulating Security Protocol) - инкапсулирующий протокол безопасности, который обеспечивает целостность и конфиденциальность. ESP является протоколом защиты, обеспечивающим конфиденциальность (DES, 3DES), аутентификацию источника и целостность данных (SHA и MD5), защиту от воспроизведения. Протокол ESP поддерживает все функции протокола AH

при этом функции аутентификации и криптографического закрытия могут быть задействованы либо вместе, либо отдельно друг от друга. О том, что пакет является пакетом ESP, говорит значение в поле протокола заголовка IP, равное 50, а для пакета AH - равное 51.

При выполнении шифрования без аутентификации появляется возможность использования механизма трансляции сетевых адресов NAT, поскольку в этом случае адреса в заголовках IP-пакетов можно модифицировать [2].

ESP не обязательно предоставляет все сервисы, но либо конфиденциальность, либо аутентификация должны быть задействованы. Рассмотрим заголовок протокола (Рис. 5.6): поля «индекс параметров безопасности (SPI)», «порядковый номер» и «аутентификационные данные» (последнее присутствует только при включенной аутентификации) имеют тот же смысл, что и для AH. ESP аутентифицирует лишь зашифрованную часть пакета (плюс два первых поля заголовка).

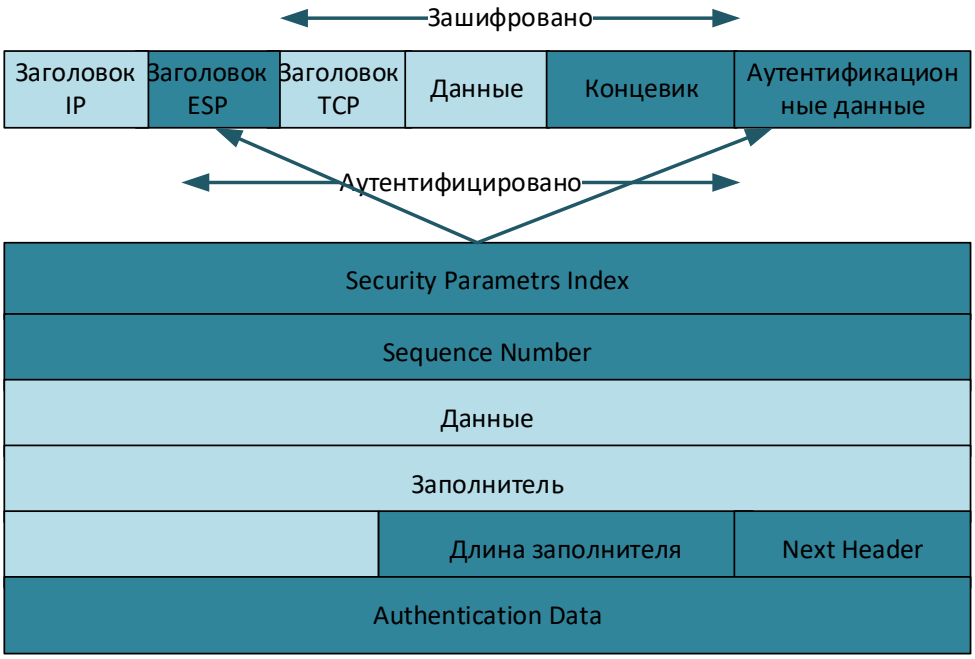

Рис. 5.6

Для обеспечения шифрования необходимо:

1. Скопировать содержимое пакета (заголовок TCP, данные и контрольную суммы) в буфер обмена.

2. Остаток дополнить байтами, с тем чтобы номер был прижат к границе 32-битного слова, а размер буфера удовлетворял требованиям алгоритма шифрования.
3. Осуществить криптографическое преобразование содержимого буфера.
4. Дополнить сообщение полями «индекс параметров безопасности (SPI)» и «порядковый номер» с соответствующими значениями.
5. Полученное на ш 5 сообщение аутентифицировать и поместить в поле «Аутентификационные данные».
6. В полученное сообщение поместить заголовки старого пакета (IP) и конечное содержимое буфера.

Если в ESP включены и шифрование, и аутентификация, то аутентифицируется зашифрованный пакет. Для входящих пакетов действия выполняются в обратном порядке, т. е. сначала производится аутентификация. Это позволяет не тратить ресурсы на расшифровку поддельных пакетов, что в какой-то степени защищает от атак на доступность.

Набор сервисов, обеспечиваемых протоколом ESP, зависит от параметров, которые выбираются при создании ассоциации защиты IPSec. Заголовок ESP вставляется в пакет после заголовка IP перед заголовком протокола высшего уровня (в транспортном режиме) или перед инкапсулированным заголовком IP (в туннельном режиме).

Шифрование охватывает только поле данные, а заголовок IP не защищается. Сервис ESP HMAC не может использоваться самостоятельно, а должен быть объединен с протоколом шифрования ESP.

Для выбора между AH и ESP необходимо выяснить, передаются ли данные из идентифицированного источника без нарушения целостности и требуется ли обеспечение конфиденциальности данных, если эти требования не нарушаются, то в этом случае достаточно протокола AH. В случае необходимость сохранить данные, используйте ESP.

5.3.3 Туннельный и транспортный режимы IPSec

В режиме транспорта ESP заголовок находится между оригинальным IP заголовком и заголовком TCP или UDP (Рис. 5.7), при этом шифруется только полезный груз IP, а исходный заголовок IP остается нетронутым.

Особенностью этого режима видимость истинных адресов отправителя и получателя.

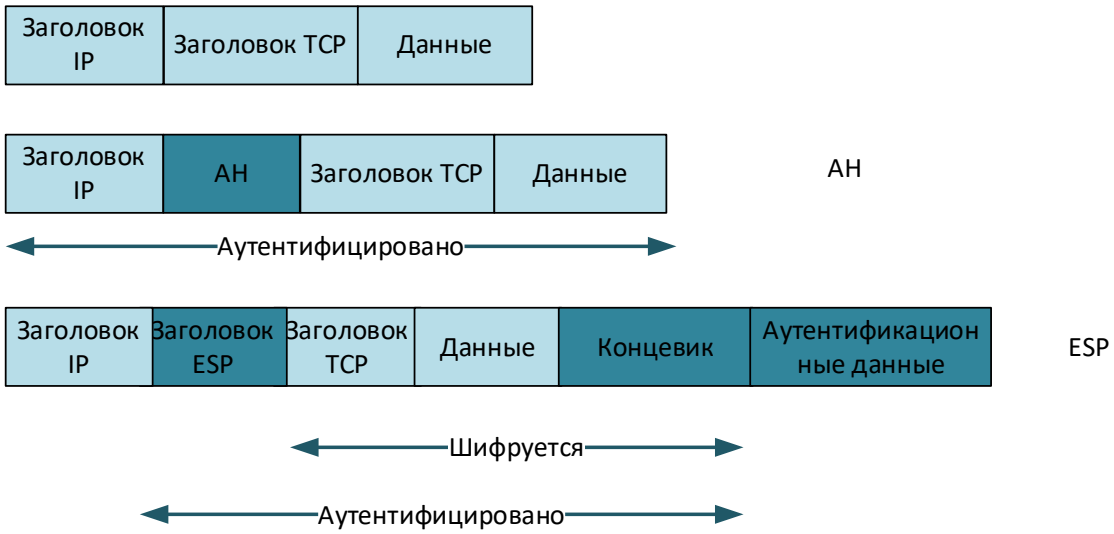

Рис. 5.7

Передача заголовка IP в открытом виде в транспортном режиме позволяет нарушителю в определенной мере выполнить анализ потока данных (количество переданных пакетов, IP- адреса).

В режиме туннеля заголовок ESP размещается между новым IP заголовком и полностью зашифрованным оригинальным IP пакетом (Рис 5.8).

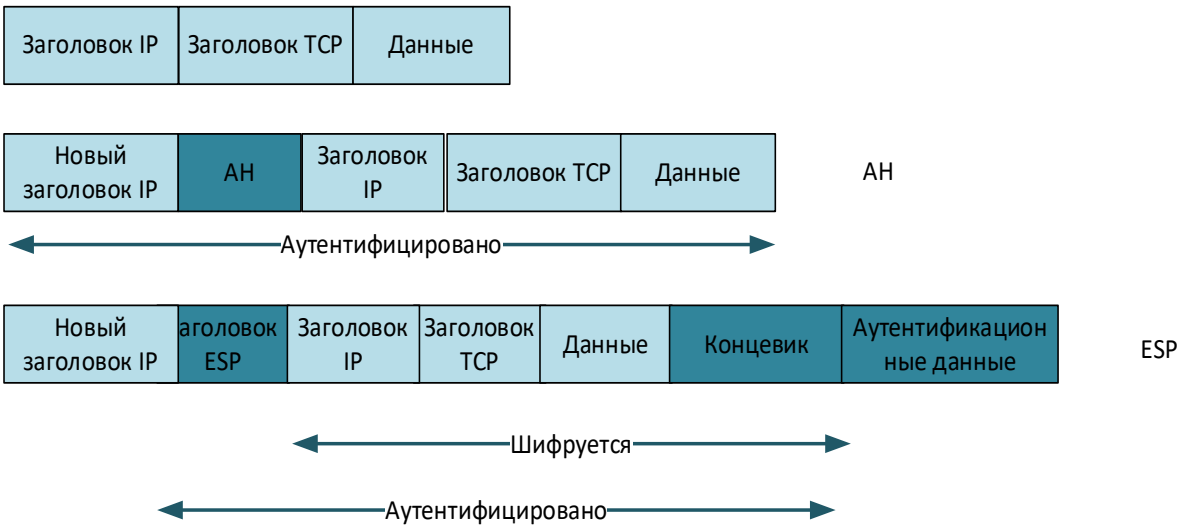

Рис. 5.8

Туннельный режим позволяет сетевому устройству выступать в роли шлюза IPSec или прокси-сервера, выполняющего шифрование для хостов, размещенных за маршрутизатором (или МСЭ).

Маршрутизатор источника зашифровывает пакет полученный от хоста вместе с исходным IP-заголовком, для обеспечения возможности

маршрутизации полученного пакета, шлюз снабжает его новым IP-заголовком и только после этого отправляет его по туннелю IPSec (Рис. 5.9).

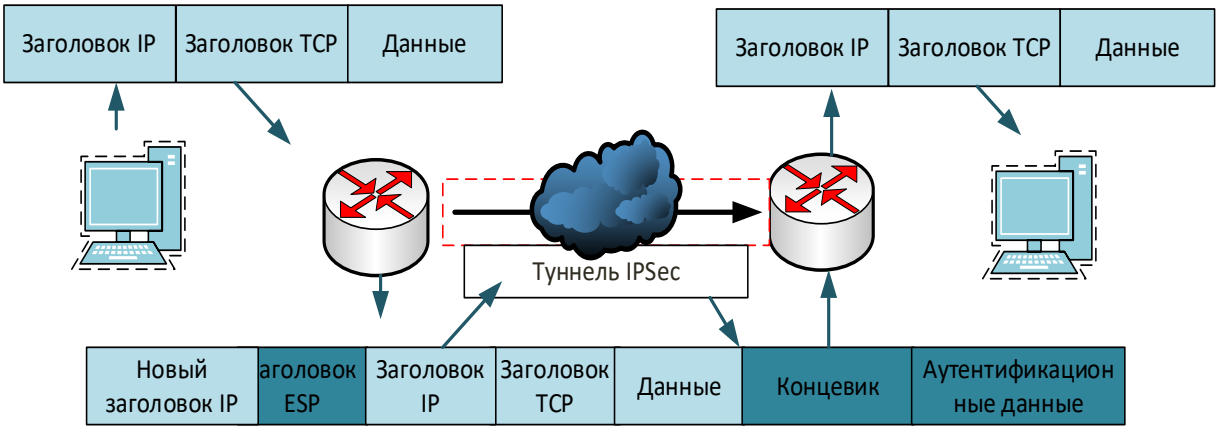

Рис. 5.9

Маршрутизатор адресата (или МСЭ) расшифровывает полученный пакет IPSec, извлекает исходную дейтаграмму IP и передает ее системе адресата. Главное преимущество туннельного режима заключается в том, что не требуется модифицировать конечные системы, чтобы обеспечить им возможность использования IPSec. Туннельный режим также не позволяет противнику анализировать поток данных, путем сокрытия истинных источника и адресата проходящих через туннель пакетов).

5.3.4 Протокол управления криптоключами IKE

Применение различных режимов передачи данных, а также согласование ключей криптографического закрытия требует предварительной координации набора применяемых алгоритмов и их параметров, поддерживаемых сторонами обмена. Поэтому до установления туннеля передачи данных сторон необходимо согласовать общий контекст безопасности (Security Association, SA), с формированием инфраструктуры, включающий алгоритмы шифрования, ключи и применяемые политики безопасности. В качестве такой инфраструктуры в IPSec выступает протоколы IKE (Internet KeyExchange), которые решают задачи:

- аутентификации сторон, согласования алгоритмов шифрования и характеристик ключей;
- создание, обмен и управление ключевой информации соединения (в том числе возможность их частой смены);

- управление параметрами соединения и защитой от некоторых типов атак.

В работе протоколов IPsec можно выделить пять этапов [3] (Рис 5.10):

1. Создание на хосте политики безопасности (какой трафик подлежит шифрованию, какие функции и алгоритмы применяются).

2. Первая фаза IKE — организация безопасного канала между сторонами:

2.1 аутентификация и защита идентификационной информации хостов;

2.2 проверка соответствий политик безопасности хостов;

2.3 получение ключевой последовательности по алгоритму Диффи-Хеллмана;

2.4 формирование безопасного канала для второй фазы IKE.

3. Вторая фаза IKE- создание IPsec-туннеля:

3.1 Согласование параметров передачи данных;

3.2 установление канала передачи данных;

В случае необходимости периодически осуществляется пересмотр IPsec SA, и выполняется дополнительный обмен Диффи-Хеллмана.

4. Обмен информацией между узлами через IPsec-туннель.

5. Прекращение действия текущих IPsec SA (при удалении или истечении времени жизни.

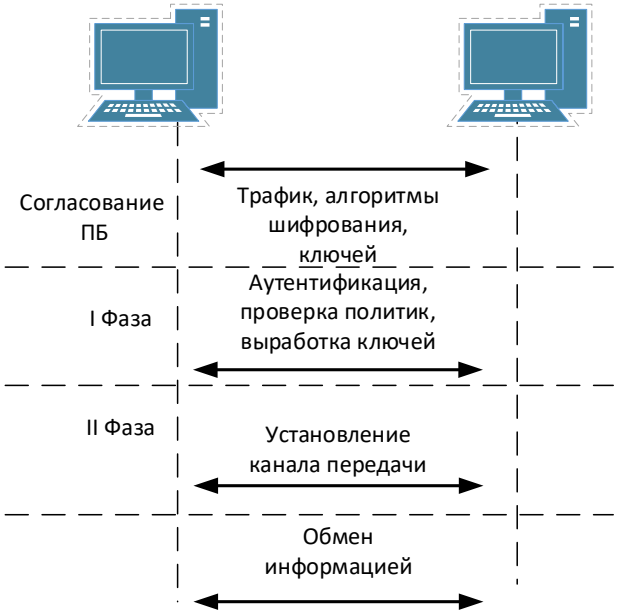

Рис. 5.10

Процесс создания новых SA может происходить и до завершения действия текущих, если требуется непрерывная передача данных.

Первая фаза IKE. Согласования IKE. На этом этапе формируется предложение (IKE Proposal) того, какими методами осуществляется защита данных. Для этого VPN-точка обращается к IPsec- модулю, который формирует и отправляет список предложений (Рис 5.11, п. 1.1). Поля спискам предложений включают в себя:

- идентификаторы конечных узлов;
- методы аутентификации;
- методы распределения ключевой информации, наиболее часто используется алгоритм Диффи-Хеллмана;
- вид сети (локальная и удаленная сеть/хост)
- режим VPN-туннеля (режим туннеля или транспорта).

Переговоры могут вестись как об установлении нового IPsec соединения, так и об установлении нового IKE соединения. В случае IPsec защищаемыми данными является тот трафик, что отправлен через VPN-туннель, а в случае IKE защищаемые данные – данные самих согласований IKE. IPsec- модуль получивший предложение, выбирает из него наиболее подходящее и указывает его в ответе (IKE Response).

Первая фаза IKE. Согласование защиты IKE (ISAKMP Tunnel). Во время первой фазы согласования защиты IKE, VPN-точки аутентифицируют друг друга (Рис 5.11, п. 1.2). Для аутентификации используются хэш алгоритм: MD5, SHA-1, SHA-2K, RSA. К методам распределения ключевой информации IKE можно отнести использование:

- *ручного режима* (ключи аутентификации, шифрования, параметры задаются вручную на обоих точках VPN подключения);
- общих ключей (общий ключ для криптографической защиты заранее введен на обоих точках VPN соединения);
- сертификатов.

Первая фаза IKE может проходить в одном из двух режимов:

- Основной режим (описан выше)
- Агрессивный режим (в первом сообщении помещается практически вся нужная информация для установления IKE: открытый ключ

Диффи-Хеллмана для синхронизации пакетов, подтверждаемое другим участником, идентификатор пакета. Получатель посылает в ответ все, что надо для завершения обмена. Первому узлу требуется только подтвердить соединение) [4].

Фаза завершается созданием безопасного канала для второй фазы IKE.

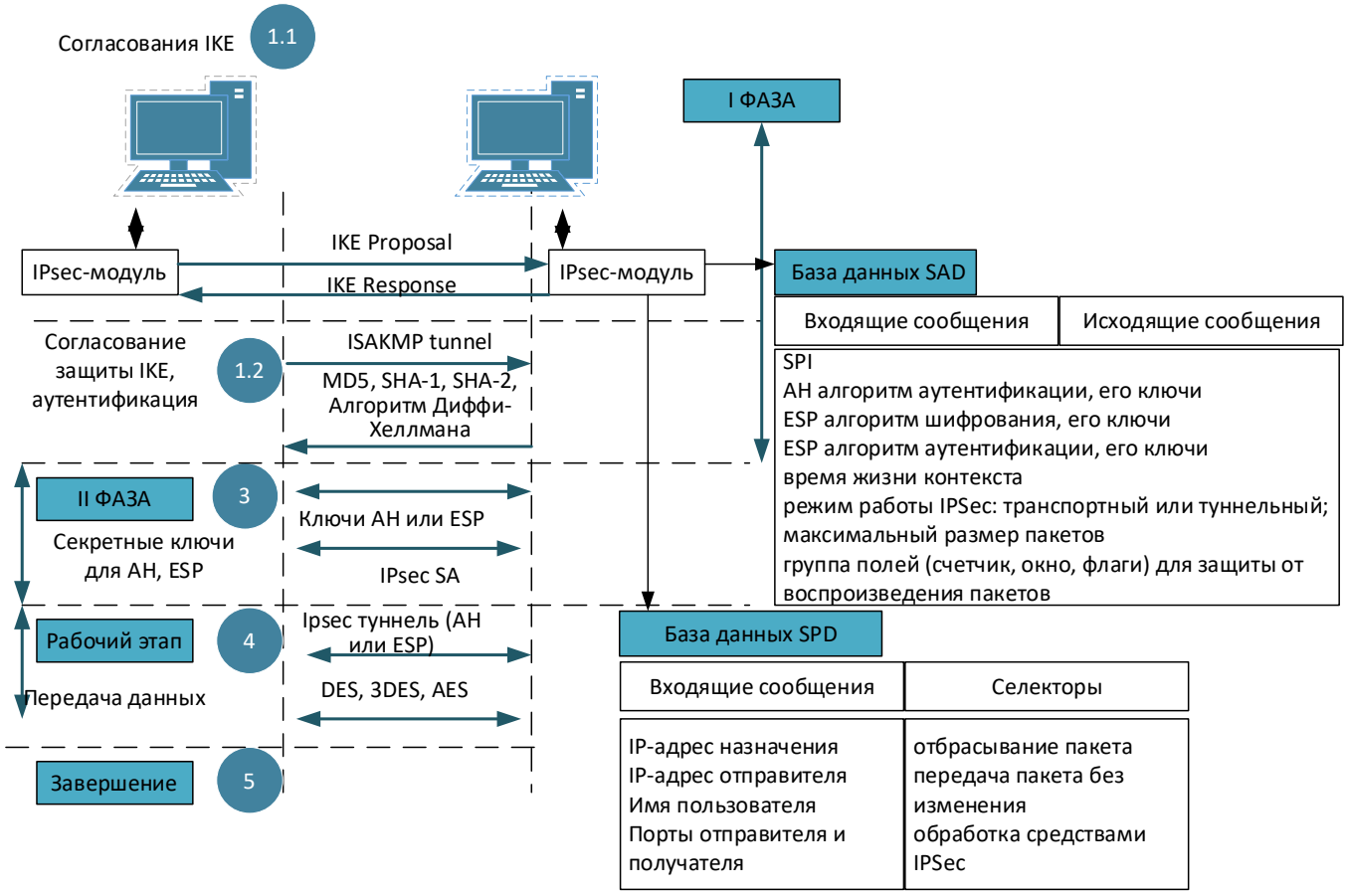

Рис. 5.11

Вторая фаза IKE функционируют в быстром режиме после создания безопасного канала. Она согласует общую политику IPsec, в том числе формирует общие секретные ключи для алгоритмов протоколов IPsec (AH или ESP), устанавливает IPsec SA. Осуществляет пересмотр текущей IPsec SA и выбор новой, если время жизни SA истекает (используя алгоритм Диффи-Хеллмана из первой фазы).

Рабочий этап. После создания IPsec SA начинается обмен информацией между узлами через IPsec-туннель, используются протоколы и параметры, установленные в SA. Эти параметры и протоколы для каждой сессии на обоих оконечных узлах защищенного канала в виде баз данных безопасных

ассоциаций SAD. Каждый узел IPSec поддерживает две базы SAD: одну для исходящих ассоциаций, а другую для входящих сообщений.

Элементы SAD содержат следующие поля:

- индекс параметров безопасности (Security Parameter Index, SPI, поскольку могут существовать несколько контекстов с одинаковыми IP-адресами и протоколами);
- используемый в протоколе AH алгоритм аутентификации, его ключи и т.п.;
- используемый в протоколе ESP алгоритм шифрования, его ключи, начальный вектор и т.п.;
- используемый в протоколе ESP алгоритм аутентификации, его ключи и т.п.;
- время жизни контекста;
- режим работы IPSec: транспортный или туннельный;
- максимальный размер пакетов;
- группа полей (счетчик, окно, флаги) для защиты от воспроизведения пакетов;

База данных политики безопасности SPD задает соответствие между IP-пакетами и установленными для них правилами обработки (за счет использования упорядоченного набора правил, каждое из которых включает совокупность селекторов и допустимых политик безопасности. Селекторы служат для отбора пакетов, а политики безопасности задают требуемую обработку). Предусмотрено три возможных варианта обработки IP-пакета:

- отбрасывание пакета;
- передача пакета без изменения;
- обработка средствами IPSec.

Для этого при поступлении пакета на IPsec-модуль при дальнейшей передаче по туннелю. IPsec-модуль определяет, связан ли пакет с SA, если да то определяется режим: туннельный или транспортный. В транспортном режиме AH-заголовок располагается после заголовка протокола IP и перед заголовками протоколов верхнего уровня (TCP или UDP). В режиме туннелирования весь исходный IP-пакет с заголовком AH, инкапсулируется

заголовком IP-протокола, добавляется служебная информация и пакет отправляется по туннелю.

После получения пакета, приёмный IPsec-модуль ищет соответствующее защищённое виртуальное соединение в базе SAD, используя IP-адрес получателя, протокол безопасности и индекс SPI. Если соответствующее SA не найдено, пакет уничтожается. К найденному защищённому виртуальное соединению (SA) аутентифицируется и вычисляется контрольная сумма, при совпадении пришедший пакет считается действительным и принимается для дальнейшей IP-обработки. Если проверка дала отрицательный результат, то принятый пакет уничтожается.

Работа за NAT реализована отдельной спецификацией. На уровне IKE конечные устройства обмениваются друг с другом информацией о поддержке, NAT Traversal и версией поддерживаемой спецификации (если оба устройства имеют такую поддержку). Если необходимо использование NAT, согласование IKE перемещаются с порта UDP 500 на порт 4500 (поскольку некоторые IPsec-модули некорректно обрабатывают IKE сессию на 500 порту при использовании NAT, а также особенности ESP протокола, к не применимо понятия TCP/UDP порта, что делает невозможным подключение через NAT более одного клиента к одному шлюзу). Для решения данной проблемы пакет ESP запаковывается в UDP дейтаграмму и посылается на порт 4500, тот же самый, который использует IKE при включенном NAT Traversal.

В настоящее время существуют 2 версии протокола IKE о различиях каждой версии можно посмотреть здесь [6].

Защищённые протоколы значительно повышают безопасность сети, но при этом необходимо понимать базовые принципы реализации этих протоколов и ограничения в их применении. Защищённый сетевой протокол позволяет контролировать подлинность агентов, целостность и конфиденциальность данных, но не убережёт от уязвимостей в клиентских и серверных приложениях и от вредоносного программного обеспечения. Поэтому необходимо понимать, что только комплексный подход к обеспечению защиты информации, где защищённые протоколы – только одно из используемых средств защиты, обеспечит приемлемый уровень рисков.

СПИСОК ЛИТЕРАТУРЫ

1. Методическое пособие по IPSec. Электронный ресурс http://dfe.petrsu.ru/koi/posob/security/
2. Лекция №20. Защита на сетевом уровне. Электронный ресурс https://yztm.ru/lekc2/l20/
3. Национальная библиотека им. Н. Э. Баумана. IPSec. Электронный ресурс. https://ru.bmstu.wiki/IPsec_(IP_Security)
4. Википедия. IPSec. Электронный ресурс https://ru.wikipedia.org/wiki/IPsec
5. IPSec (Internet Protocol Security). Электронный ресурс https://networklessons.com/cisco/ccie-routing-switching/ipsec-internet-protocol-security