Лекция №20. ЗАЩИТА НА СЕТЕВОМ УРОВНЕ – ПРОТОКОЛ IPSEC.

Оглавление

[1. Архитектура средств безопасности IPSec 2](#_Toc509156291)

[2. Защита передаваемых данных с помощью протоколов АН и ESP 7](#_Toc509156292)

[2.1. Протокол аутентифицирующего заголовка AH 7](#_Toc509156293)

[2.2. Протокол инкапсулирующей защиты ESP 9](#_Toc509156294)

[2.3. Алгоритмы аутентификации и шифрования в IPSec 13](#_Toc509156295)

[3. Протокол управления криптоключами IKE 15](#_Toc509156296)

[3.1. Установление безопасной ассоциации SA. 15](#_Toc509156297)

[4. Особенности реализации средств IPSec 19](#_Toc509156298)

Радикальное устранение уязвимостей компьютерных сетей возможно при создании системы защиты не для отдельных классов приложений, а для сети в целом. Применительно к IP-сетям это означает, что системы защиты должны действовать на сетевом уровне модели OSI.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Модель OSI** | | | | |
| **Уровень (layer)** | | **Тип данных** | **Функции** | **Примеры** |
| **Host layers** | 7. Прикладной (application) | Данные | Доступ к сетевым службам | HTTP, FTP, SMTP, RDP, SNMP, DHCP |
| 6.Представительский представления) (presentation) | Представление и шифрование данных | ASCII, EBCDIC |
| 5. Сеансовый (session) | Управление сеансом связи | RPC, PAP |
| 4. Транспортный (transport) | Сегменты (segment)/ Дейтаграммы (datagram) | Прямая связь между конечными пунктами и надёжность | TCP, UDP, SCTP, PORTS |
| **Media layers** | 3. Сетевой (network) | Пакеты (packet) | Определение маршрута и логическая адресация | IPv4, IPv6, **IPsec**, AppleTalk |
| 2. Канальный (data link) | Биты (bit)/ Кадры (frame) | Физическая адресация | PPP, IEEE 802.22, Ethernet, DSL, ARP, L2TP, Network Cards |
| 1. Физический (physical) | Биты (bit) | Работа со средой передачи, сигналами и двоичными данными | USB, кабель ("витая пара", коаксиальный, оптоволоконный), радиоканал |

Преимущество такого выбора заключается в том очевидном факте, что в IP-сетях именно сетевой уровень отличается наибольшей гомогенностью: независимо от вышележащих протоколов, физической среды передачи и технологии канального уровня транспортировка данных по сети не может быть произведена в обход протокола IP. Поэтому реализация защиты сети на третьем уровне автоматически гарантирует как минимум такую же степень защиты всех сетевых приложений, причем без какой-либо модификации последних.

При формировании защищенных виртуальных каналов на сетевом уровне модели ОSI достигается оптимальное соотношение между прозрачностью и качеством защиты. Размещение средств защиты на сетевом уровне делает их прозрачными для приложений, так как между сетевым уровнем и приложением функционирует реализация протокола транспортного уровня. Для пользователей процедуры защиты оказываются столь же прозрачными, как и сам протокол IP. На сетевом уровне существует возможность достаточно полной реализации функций защиты трафика и управления ключами, поскольку именно на сетевом уровне выполняется маршрутизация пакетов сообщений.

*Стек протоколов IPSec* (*Internet Рrotocol Security*) используется для аутентификации участников обмена, туннелирования трафика и шифрования IP-пакетов. Основное назначение протокола IPSec – обеспечение безопасной передачи данных по сетям IP. Поскольку архитектура IPSec обеспечивает его совместимость с протоколом IPv4, ее поддержку достаточно обеспечить на обоих концах соединения; промежуточные сетевые узлы могут вообще ничего «не знать» об IPSec. Протокол IРSес может защищать трафик как текущей версии протокола IРv4, применяемой сегодня в Интернете, так и версии IРv6, которая постепенно внедряется в Интернет.

# Архитектура средств безопасности IPSec

Основное назначение протоколов IPSec – обеспечение безопасной передачи данных по сетям IP. Применение IPSec гарантирует:

* + - целостность передаваемых данных, то есть данные при передаче не искажены, не потеряны и не продублированы;
    - аутентичность отправителя, то есть данные переданы именно тем отправителем, который доказал, что он тот, за кого себя выдает;
    - конфиденциальность передаваемых данных, то есть данные передаются в форме, предотвращающей их несанкционированный просмотр.

Следует отметить, что обычно в понятие безопасности данных включают еще одно требование – доступность данных, что в рассматриваемом контексте можно интерпретировать как гарантию их доставки. Протоколы IPSec не решают данную задачу, оставляя ее протоколу транспортного уровня TCP. Стек протоколов IPSec обеспечивает защиту информации на сетевом уровне, что делает эту защиту невидимой для работающих приложений.

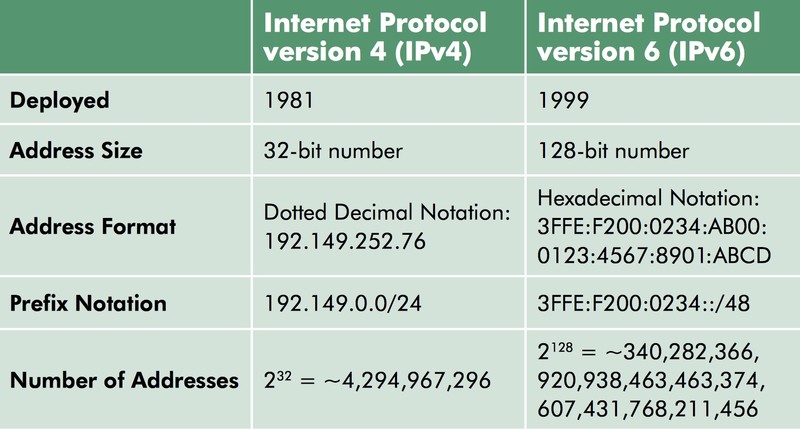
Фундаментальной единицей коммуникации в IP-сетях является IP-пакет. Структура IP-пакета показана на рис. 1. IP-пакет содержит S-адрес источника и D-адрес получателя сообщения, транспортный заголовок, информацию о типе данных, переносимых в этом пакете, и сами данные.

***Рис. 1. Структура IP-пакета***

Пользователь воспринимает сеть как надежно защищенную среду только в том случае, если он уверен, что его партнер по обмену – именно тот, за кого он себя выдает (аутентификация сторон), что передаваемые пакеты не просматриваются посторонними лицами (конфиденциальность связи) и что получаемые данные не подверглись изменению в процессе передачи (целостность данных).

Для того чтобы обеспечить аутентификацию, конфиденциальность и целостность передаваемых данных стек протоколов IPSec построен на базе ряда стандартизованных криптографических технологий:

* + - обмены ключами согласно алгоритму Диффи–Хеллмана для распределения секретных ключей между пользователями в открытой сети;
    - криптография открытых ключей для подписывания обменов Диффи–Хеллмана, чтобы гарантировать подлинность двух сторон и избежать атак типа «человек в середине»;
    - цифровые сертификаты для подтверждения подлинности открытых ключей;
    - блочные симметричные алгоритмы шифрования данных;
    - алгоритмы аутентификации сообщений на базе функций хэширования.

Протокол IРSес определяет стандартные способы защиты информационного обмена на сетевом уровне модели ОSI для IР-сети, являющейся основным видом открытых сетей. Данный протокол входит в состав новой версии протокола IР (IРv6) и применим также к его текущей версии (IРv4). Для протокола IРv4 поддержка IРSес является желательной, а для IРv6 – обязательной.

Протокол IРSес представляет собой систему открытых стандартов, которая имеет четко очерченное ядро и которую можно дополнять новыми протоколами, алгоритмами и функциями. Стандартизованными функциями IРSес-защиты могут пользоваться протоколы более высоких уровней, в частности управляющие протоколы, протоколы конфигурирования, а также протоколы маршрутизации.

Основными задачами установления и поддержания защищенного канала являются следующие:

* + - аутентификация пользователей или компьютеров при инициации защищенного канала;
    - шифрование и аутентификация передаваемых данных между конечными точками защищенного канала;
    - обеспечение конечных точек канала секретными ключами, необходимыми для работы протоколов аутентификации и шифрования данных.

Для решения перечисленных задач система IРSес использует комплекс средств безопасности информационного обмена.

Большинство реализаций протокола IPSec имеют следующие компоненты:

* + - основной протокол IPSec. Этот компонент реализует протокол инкапсулирующей защиты ESP и протокол аутентифицирующего заголовка AH. Он обрабатывает заголовки, взаимодействует с базами данных SPD и SAD для определения политики безопасности, применяемой к пакету;
    - протокол управления обменом ключевой информации IKE (Internet Key Exchange). IKE обычно представляется как процесс пользовательского уровня, за исключением реализаций, встроенных в операционную систему;
    - базу данных политик безопасности SPD (Security Policy Database). Это один из важнейших компонентов, поскольку он определяет политику безопасности, применяемую к пакету. SPD используется основным протоколом IPSec при обработке входящих и исходящих пакетов;
    - базу данных безопасных ассоциаций SAD (Security Association Database). База данных SAD хранит список безопасных ассоциаций SA (Security Association) для обработки входящей и исходящей информации. Исходящие SA используются для защиты исходящих пакетов, а входящие SA – для обработки пакетов с заголовками IPSec. База данных SAD заполняется SA вручную или с помощью протокола управления ключами IKE;
    - управление политикой безопасности и безопасными ассоциациями SA. Это приложения, которые управляют политикой безопасности и SA.

Основной протокол IPSec (реализующий ESP и AH) тесно взаимодействует с транспортным и сетевым уровнями стека протоколов TCP/IP. Фактически протокол IPSec является частью сетевого уровня. Основной модуль протокола IPSec обеспечивает два интерфейса: входной и выходной. Входной интерфейс используется входящими пакетами, а выходной – исходящими. Реализация IPSec не должна зависеть от интерфейса между транспортным и сетевым уровнями стека протоколов TCP/IP.

Базы данных SPD и SAD существенно влияют на эффективность работы IPSec. Выбор структуры данных для хранения SPD и SAD является критическим моментом, от которого зависит производительность IPSec. Особенности реализации SPD и SAD зависят от требований производительности и совместимости системы.

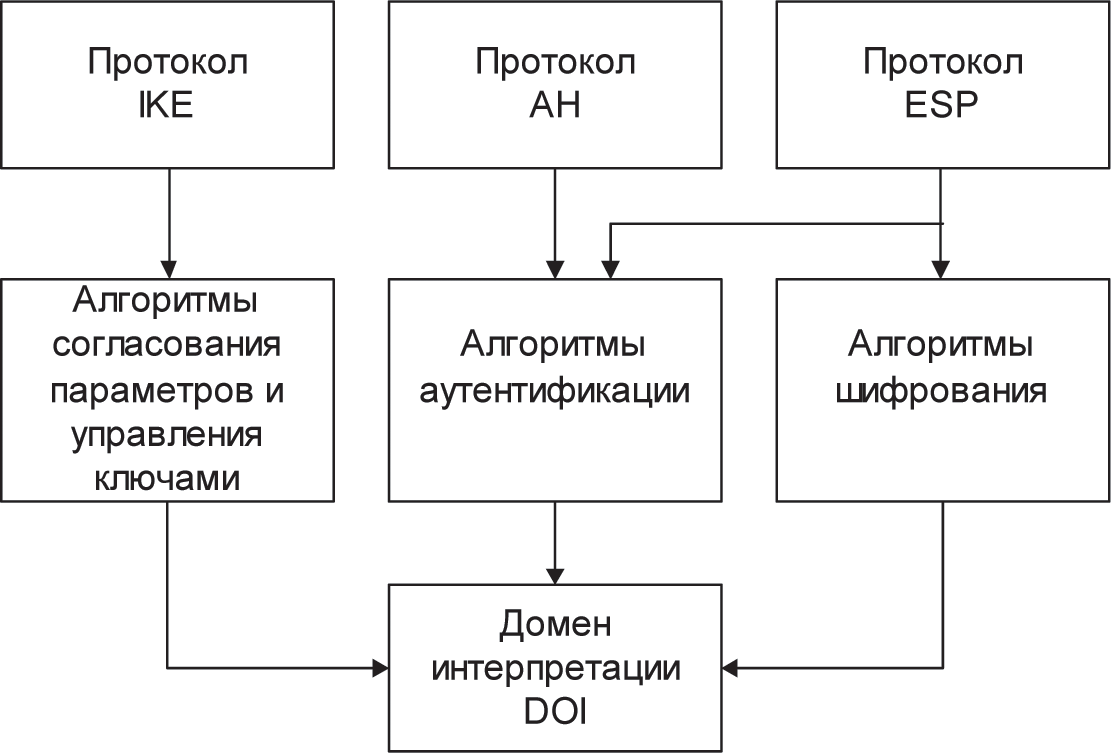
Все протоколы, входящие в IPSec, можно разделить на две группы:

* + - протоколы, непосредственно производящие обработку передаваемых данных (для обеспечения их защиты);
    - протоколы, позволяющие автоматически согласовать параметры защищенных соединений, необходимые для протоколов первой группы.

**Ядро IPSec составляют три протокола:**

1. протокол аутентифицирующего заголовка AH (Authentication Header),
2. протокол инкапсулирующей защиты ESP (Encapsulating Security Payload),
3. протокол согласования параметров виртуального канала и управления ключами IKE (Internet Key Exchange).

Архитектура средств безопасности IРSес представлена на рис. 2.



***Рис. 2. Архитектура стека протоколов IPSec***

На *верхнем уровне* расположены следующие протоколы:

* + - протокол согласования параметров виртуального канала и управления ключами IКЕ, определяющий способ инициализации защищенного канала, включая согласование используемых алгоритмов криптозащиты, а также процедуры обмена и управления секретными ключами в рамках защищенного соединения;
    - протокол аутентифицирующего заголовка АН, обеспечивающий аутентификацию источника данных, проверку их целостности и подлинности после приема, а также защиту от навязывания повторных сообщений;
    - протокол инкапсулирующей защиты содержимого ЕSР, обеспечивающий криптографическое закрытие, аутентификацию и целостность передаваемых данных, а также защиту от навязывания повторных сообщений.

Разделение функций защиты между двумя протоколами AH и ESP обусловлено применяемой во многих странах практикой ограничения экспорта и/или импорта средств, обеспечивающих конфиденциальность данных путем шифрования. Каждый из протоколов AH и ESP может использоваться как самостоятельно, так и совместно с другим. Из краткого перечисления функций протоколов AH и ESP видно, что возможности этих протоколов частично перекрываются.

Протокол AH отвечает только за обеспечение целостности и аутентификации данных, в то время как протокол ESP является более мощным, поскольку может шифровать данные, а кроме того, способен выполнять функции протокола AH (хотя, как увидим позднее, аутентификация и целостность обеспечиваются им в несколько урезанном виде).

Протокол ESP может поддерживать функции шифрования и аутентификации/обеспечения целостности в любых комбинациях, то есть либо и ту и другую группу функций, либо только аутентификацию/обеспечение целостности, либо только шифрование.

Для шифрования данных в IPSec (протокол ESP) может быть применен практически любой симметричный алгоритм шифрования с секретными ключами. Для обеспечения целостности и аутентификации данных (протоколы АН и ESP) используется один из приемов шифрования – шифрование с помощью односторонней функции (One-way Function), называемой также дайджест-функцией (Digest Function).

Протоколы IКЕ, АН и ЕSР взаимодействуют следующим образом.

Сначала с помощью протокола IКЕ между двумя точками устанавливается логическое соединение, которое в стандартах IРSес получило название «безопасная ассоциация SА». При установлении этого логического соединения выполняется аутентификация конечных точек канала, а также выбираются параметры защиты данных, например, алгоритм шифрования, сессионный секретный ключ и т. п.

Затем в рамках установленной безопасной ассоциации SА начинает работать протокол АН или ЕSР, с помощью которого и выполняется требуемая защита передаваемых данных с использованием выбранных параметров.

*Средний уровень* архитектуры IРSес образуют алгоритмы согласования параметров и управления ключами, применяемые в протоколе IKE, а также алгоритмы аутентификации и шифрования, используемые в протоколах аутентифицирующего заголовка АН и инкапсулирующей защиты содержимого ЕSР.

Следует отметить, что протоколы защиты виртуального канала верхнего уровня архитектуры IРSес (АН и ЕSР) не зависят от конкретных криптографических алгоритмов. За счет возможности использования большого количества разнообразных алгоритмов аутентификации и шифрования IРSес обеспечивает высокую степень гибкости организации защиты сети. Гибкость IРSес состоит в том, что для каждой задачи предлагается несколько способов ее решения. Выбранные методы для одной задачи обычно не зависят от методов реализации других задач. Например, выбор для шифрования алгоритма DЕS не влияет на выбор функции вычисления дайджеста, используемого для аутентификации данных.

*Нижний уровень* архитектуры IPSec образует так называемый домен интерпретации DOI. Необходимость применения домена интерпретации DOI обусловлена следующими причинами. Протоколы АН и ESP имеют модульную структуру, допуская применение пользователями по их согласованному выбору различных криптографических алгоритмов шифрования и аутентификации. Поэтому необходим модуль, который мог бы обеспечить совместную работу всех применяемых и вновь включаемых протоколов и алгоритмов. Именно такие функции возложены на домен интерпретации DOI. Домен интерпретации DOI в качестве базы данных хранит сведения об используемых в IPSec протоколах и алгоритмах, их параметрах, протокольных идентификаторах и т. п. По существу, домен интерпретации DOI выполняет роль фундамента в архитектуре IPSec. Для того чтобы использовать алгоритмы, соответствующие национальным стандартам в качестве алгоритмов аутентификации и шифрования в протоколах АН и ESP, необходимо зарегистрировать эти алгоритмы в домене интерпретации DOI.

Для того чтобы протоколы AH и ESP могли выполнять свою работу по защите передаваемых данных, между конечными узлами необходимо установить безопасную ассоциацию SA. Цель SA – обеспечить достоверную идентификацию каждого конечного узла (данный процесс называется взаимной аутентификацией конечных узлов) и установить согласованные параметры защищенного соединения. Для установления безопасной ассоциации SA между двумя конечными точками используется протокол ISAKMP (Internet Security Association and Key Management Protocol), входящий в состав протокола согласования параметров виртуального канала и управления ключами IКЕ.

Установление SA начинается со взаимной аутентификации сторон. Выбираемые далее параметры SA определяют, какой из двух протоколов, AH или ESP, применяется для защиты данных, какие функции выполняет протокол защиты: например, только аутентификацию и проверку целостности или, кроме того, и защиту конфиденциальности данных. Важным параметром безопасной ассоциации SA является так называемый ключевой материал, то есть секретные криптографические ключи, используемые в работе протоколов AH и ESP. В целях безопасности IPSec никогда не пересылает ключи по сети; пересылаются данные, необходимые каждому конечному узлу, чтобы локально генерировать ключ.

Параметры безопасной ассоциации должны устраивать обе конечные точки защищенного канала. Поэтому при использовании автоматической процедуры установления SA протоколы IKE, работающие по разные стороны канала, выбирают параметры на основе взаимного согласования. Для каждой задачи, решаемой протоколами AH и ESP, предлагается несколько схем аутентификации и шифрования. Все это делает IPSec очень гибким средством защиты передаваемых данных.

Безопасная ассоциация SA представляет собой в IPSec однонаправленное логическое соединение, поэтому при двустороннем обмене данными необходимо установить две ассоциации SA. После того как между конечными узлами согласованы параметры шифрования, хэш-алгоритм и методы аутентификации, эти узлы создают одно соединение SA для входящих пакетов данных и другое – для исходящих.

Протоколы AH или ESP функционируют уже в рамках установленного логического соединения SA, с его помощью и осуществляется требуемая защита передаваемых данных с использованием выбранных параметров.

# Защита передаваемых данных с помощью протоколов АН и ESP

Протокол аутентифицирующего заголовка АН и протокол инкапсулирующей защиты содержимого ЕSР могут работать в туннельном или транспортном режимах. Для выполнения своих задач по обеспечению безопасной передачи данных протоколы AH и ESP включают в обрабатываемые ими пакеты дополнительную служебную информацию, оформляя ее в виде заголовков. Ниже мы рассмотрим подробнее содержимое заголовков AH и ESP и связанную с ними функциональность.

## Протокол аутентифицирующего заголовка AH

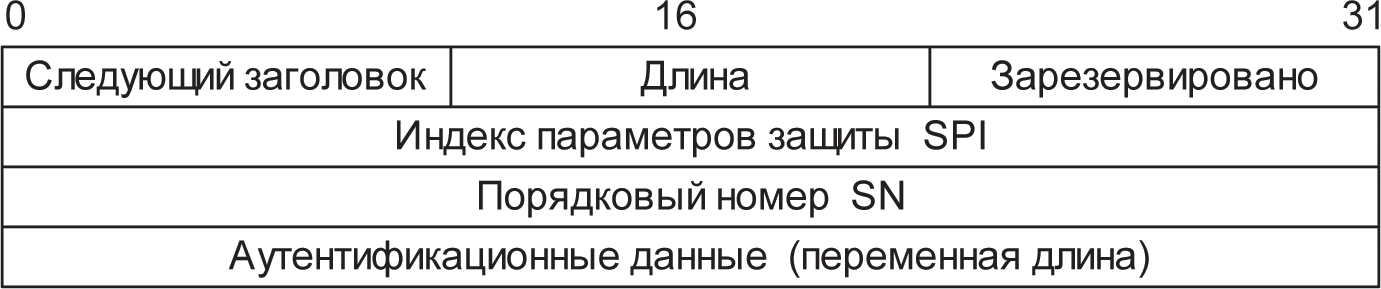
Протокол аутентифицирующего заголовка AH обеспечивает проверку аутентичности и целостности IР-пакетов, а также защиту от воспроизведения ранее посланных IР-пакетов.

Протокол AH позволяет приемной стороне убедиться в следующем:

* пакет был отправлен именно той стороной, с которой установлена данная ассоциация;
* содержимое пакета не подверглось искажениям в процессе передачи его по сети;
* пакет не является дубликатом некоторого пакета, полученного ранее.

Протокол АН полностью защищает от подлога и искажения содержимого IР-пакетов, включая данные протоколов более высоких уровней. Полнота защиты полей IР-заголовков зависит от используемого режима работы – туннельного или транспортного.

Однако протокол AH не обеспечивает конфиденциальности передаваемых данных, то есть он не предназначен для их шифрования. Данные могут быть прочитаны промежуточными узлами, но не могут быть изменены. Целостность и аутентичность данных обеспечиваются добавлением аутентифицирующего заголовка (AH) перед заголовком IP и заголовком транспортного уровня (TCP/UDP). Формат заголовка AH показан на рис. 3.

***Рис. 3. Формат заголовка AH***

Заголовок AH включает в себя следующие поля:

* + *следующий заголовок (Next Header)* – однобайтовое поле, содержащее код протокола следующего заголовка, вложенного в IРSес-пакет, например код протокола TCP или ESP, чей заголовок следует за AH;
* *длина (Рауlоаd Lеn)* – указывает длину заголовка AH в 32-битных словах;
* *индекс параметров защиты SPI (Security Parameters Index)* – представляет собой 32-разрядную метку безопасной ассоциации SА, содержащей все параметры туннеля IРSес, включая типы криптографических алгоритмов и ключи шифрования. На основании индекса SPI пакет будет правильно отнесен к одной из существующих ассоциаций в приемном шлюзе (или хосте). Если же активной ассоциации, на которую указывает метка SPI, не существует, то пакет просто отбрасывается;
* *порядковый номер SN (Sequence Number)* – беззнаковое 32-битное число, увеличиваемое на единицу после передачи каждого защищенного по протоколу АН IР-пакета. Обеспечивает защиту от ложного воспроизведения ранее посланных IР-пакетов. При формировании каждого защищенного сеанса информационного обмена в рамках туннеля IРSес взаимодействующие стороны делают свои счетчики нулевыми, а потом согласованным образом увеличивают их. Получатель проверяет это поле с целью удостовериться, что пакета с таким номером принято еще не было. Если же такой пакет уже был, он не принимается;
* *аутентификационные данные (Authentication Data)* – поле переменной длины, содержащее информацию, используемую для аутентификации пакета и называемую МАС-кодом (Меssаgе Аuthеntication Соdе). Это поле называют также цифровой подписью, дайджестом или кодом проверки целостности IСV (Integritу Сhесk Vаluе) пакета. Содержимое поля Аuthеntication Dаtа вычисляется с помощью одного из двух обязательно поддерживаемых протоколом АН алгоритмов, НМАС-МD5 и НМАС-SНА1, основанных на применении

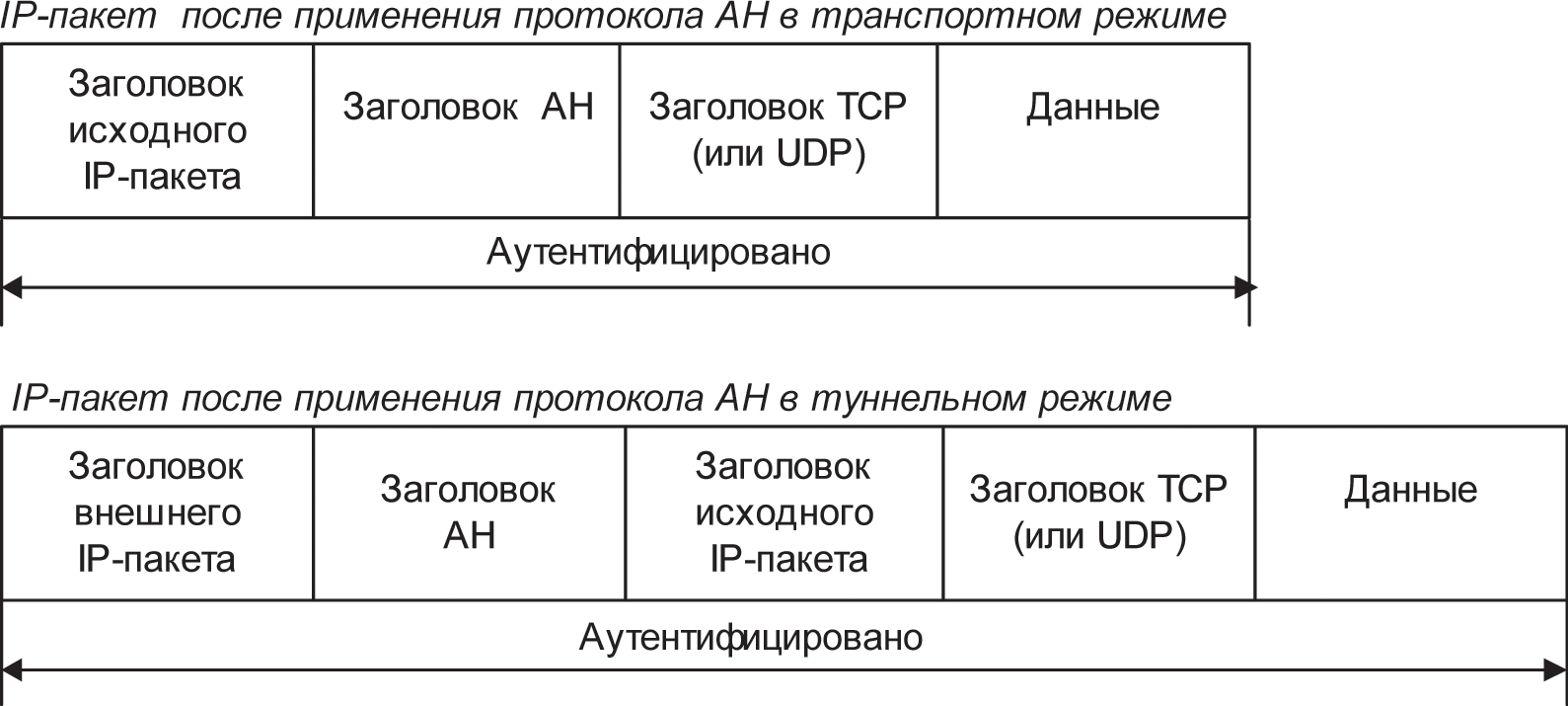
односторонних хэш-функций с секретными ключами. Длина дайджеста зависит от выбранного алгоритма, так что это поле имеет в общем случае переменный размер. Наиболее часто используемый алгоритм НМАС-МD5 порождает 16-байтный дайджест.

Протокол AH защищает весь IP-пакет, за исключением некоторых полей в IP-заголовке, таких как время жизни (TTL) и тип службы (Type of Service), которые могут меняться в процессе передачи пакета в сети. Заметим, что протокол AH обеспечивает защиту от изменений IP-адресов в заголовке пакета. Протокол аутентификации AH создает своеобразный конверт, обеспечивающий аутентификацию источника данных, их целостность и защиту от навязывания повторных сообщений.

Протокол AH может быть использован в двух режимах:

* + туннельном;
  + транспортном.

Местоположение заголовка AH в пакете зависит от того, в каком режиме – транспортном или туннельном – сконфигурирован защищенный канал. На рис. 4 показано расположение AH-заголовка относительно IP-заголовка в обоих режимах.

***Рис. 4. IР-пакет после применения протокола АН в транспортном и туннельном режимах***

В *транспортном режиме* заголовок исходного IP-пакета становится внешним заголовком, за ним следует заголовок AH, а затем все данные защищаемого пакета (то есть пакет протокола верхнего уровня). Протокол AH защищает весь полученный таким образом пакет, включая заголовок IP и собственно сам заголовок AH. Таким образом, любое изменение данных в пакете или заголовков будет обнаружено. Следует также заметить, что в этом режиме данные пакета отсылаются открытыми, то есть мы защищаем данные пакета от изменений, но не можем защитить их от просмотра. В частности, не удается скрыть IР-адреса источника и назначения от возможного просмотра посторонними лицами, поскольку эти поля всегда присутствуют в незашифрованном виде и соответствуют действительным адресам хостов.

В *туннельном режиме* в качестве заголовка внешнего IP-пакета создается новый заголовок IP. IP-адреса посылающей и принимающей сторон могут отличаться от адресов в заголовке исходного IP-пакета. В защищенном IР-пакете внутренний (первоначальный) IР-заголовок содержит целевой адрес пакета, а внешний IР-заголовок – адрес конца туннеля. За новым заголовком внешнего IP-пакета следует заголовок AH, а затем весь исходный пакет (заголовок IP и сами данные). Как и в случае транспортного режима, протокол AH защищает весь созданный пакет (два заголовка IP, заголовок AH и данные), что также позволяет обнаружить любые изменения в пакете. Как и в транспортном режиме, сам пакет не защищен от просмотра.

Независимо от режима работы протокол АН предоставляет меры защиты от атак, направленных на нарушение целостности и подлинности пакетов сообщений. С помощью этого протокола аутентифицируется каждый пакет, что делает программы, пытающиеся перехватить управление сеансом, неэффективными. Протокол АН обеспечивает аутентификацию не только содержимого, но и заголовков IР-пакетов. Однако следует иметь в виду, что аутентификация по протоколу АН не допускает манипулирования основными полями IР-заголовка во время прохождения пакета. По этой причине данный протокол нельзя применять в среде, где используется механизм трансляции сетевых адресов NАТ (Nеtwork Аddress Тrаnslation), поскольку для его работы необходимо манипулирование IР-заголовками.

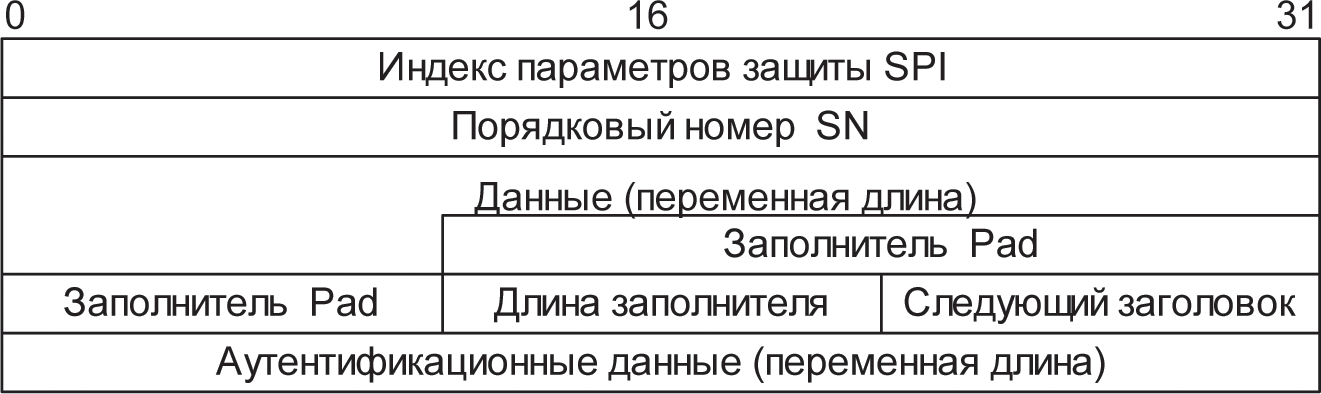
Протокол AH может применяться в одиночку и в комбинации с протоколом ESP или даже с пакетом, который уже содержит AH-заголовок (вложенное применение).

## Протокол инкапсулирующей защиты ESP

Протокол инкапсулирующей защиты содержимого ESP обеспечивает конфиденциальность, аутентичность, целостность и защиту от повторов для пакетов данных. Следует отметить, что конфиденциальность данных протокол ESP обеспечивает всегда, а целостность и аутентичность являются для него опциональными требованиями. Конфиденциальность данных обеспечивается путем шифрования содержимого отдельных пакетов. Целостность и аутентичность данных обеспечиваются на основе вычисления дайджеста.

Из приведенного перечня функций по защите информационного обмена видно, что функциональность протокола ЕSР шире, чем протокола АН. Протокол ЕSР поддерживает все функции протокола АН по защите зашифрованных потоков данных от подлога, воспроизведения и случайного искажения, а также обеспечивает конфиденциальность данных.

В протоколе ЕSР функции аутентификации и криптографического закрытия могут быть задействованы либо вместе, либо отдельно друг от друга. При выполнении шифрования без аутентификации появляется возможность использования механизма трансляции сетевых адресов NАТ, поскольку в этом случае адреса в заголовках IР-пакетов можно модифицировать [4].

Для решения своих задач протокол ESP использует заголовок формата, приведенного на рис. 5.

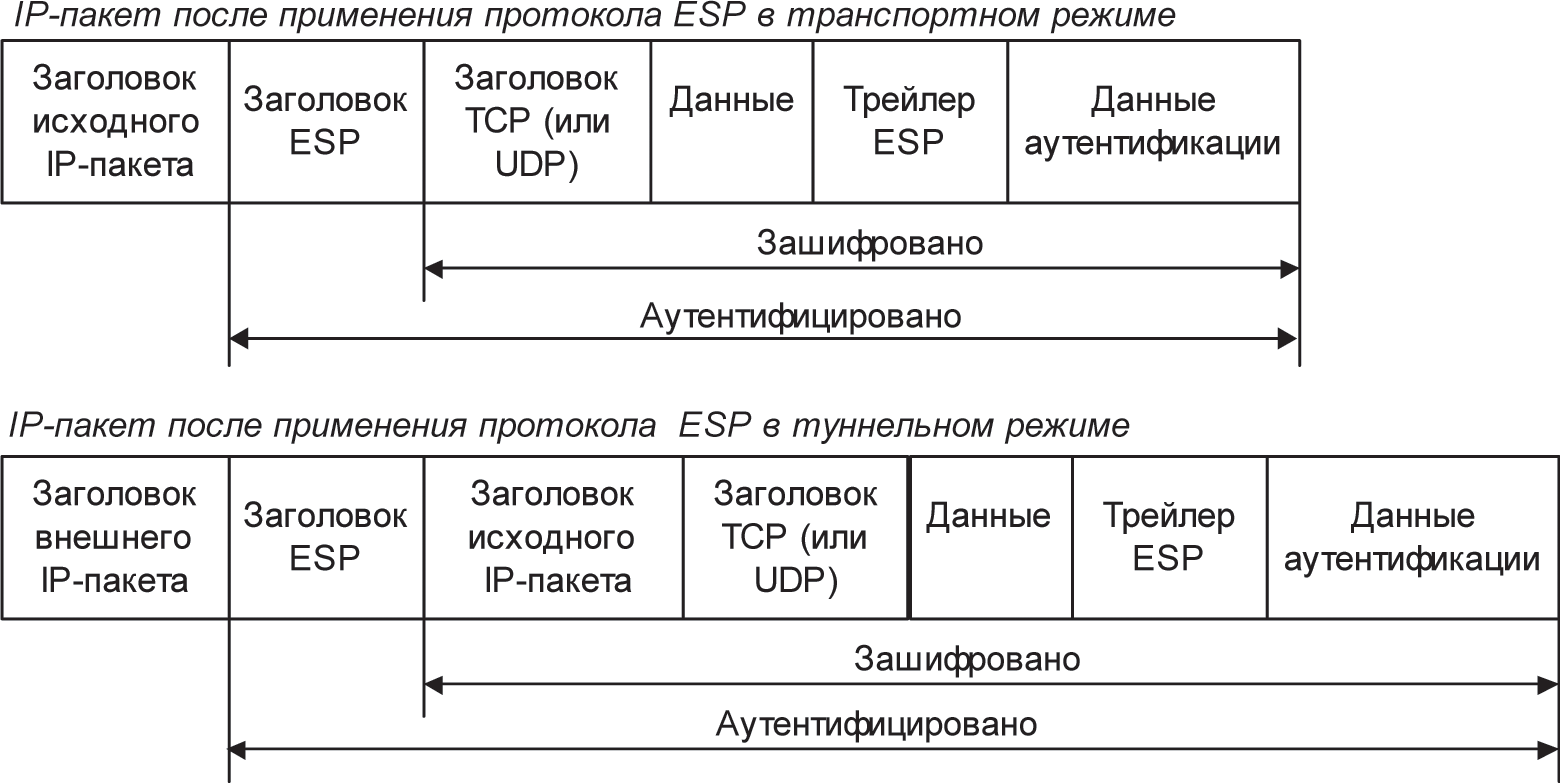
***Рис. 5. Формат заголовка ESP***

Заголовок ESP содержит следующие поля:

* + *индекс параметров защиты SPI (Security Parameters Index)* – используется совместно с адресом получателя и протоколом защиты (AH или ESP). Указывает соответствующее соглашение SA. Получатель использует это значение для определения соглашения о защите, с которым идентифицируется данный пакет;
  + *порядковый номер SN* (*Sequence Number*) – обеспечивает защиту от повторов для SA. Представляет собой 32-битное число, первоначально равное 1 и увеличивающееся с шагом 1. Оно не повторяется циклически и указывает номер пакета, отсылаемого по данному соглашению. Получатель проверяет это поле с целью удостовериться, что пакета с таким номером принято еще не было. Если же такой пакет уже был, он не принимается;
  + *данные* (*Payload Data*);
  + *заполнитель* (*Padding*) – дописывается от 0 до 255 байт для 32-битного выравнивания с размером блока шифра;
  + *длина заполнителя* (*Padding Length*) – указывает длину поля заполнителя в байтах;
  + *следующий заголовок* (*Next Header*) – указывает природу передаваемых данных (например, TCP или UDP);
  + *аутентификационные данные* (*Authentication Data*) – содержит код проверки целостности ICV и код аутентичности сообщения, используемые для проверки подлинности отправителя и целостности сообщения. Значение ICV вычисляется для заголовка ESP, передаваемых данных и концевой метки ESP. Поле Аuthentication Data помещается в заголовок ЕSР только при включенной аутентификации.

Нетрудно заметить, что некоторые поля заголовка ESP аналогичны полям заголовка AH: Next Header, SPI, SN, Authentication Data. Но имеются и два дополнительных поля – заполнитель (Padding) и длина заполнителя (Pad Length). Заполнитель может понадобиться в трех случаях. Во-первых, для нормальной работы некоторых алгоритмов шифрования необходимо, чтобы шифруемый текст содержал кратное число блоков определенного размера. Во-вторых, формат заголовка ESP требует, чтобы поле данных заканчивалось на границе четырех байтов. И наконец, заполнитель можно использовать для сокрытия действительного размера пакета в целях обеспечения так называемой частичной конфиденциальности трафика. Правда, протокол ESP ограничивает возможности маскировки 255 байтами заполнителя; это сделано для того, чтобы из-за большого объема избыточных данных не слишком снижалась полезная пропускная способность канала связи. Как видно по рис. 9.5, заголовок делится на две части, разделяемые полем данных (полезная нагрузка – Payload Data). Первая часть, которая далее будет обозначаться как заголовок ESP, образуется двумя полями, SPI и SN, и размещается перед полем данных. Остальные служебные поля протокола ESP расположены в конце пакета. Непосредственно за полем данных следует так называемый трейлер, в который входят заполнитель (Padding), длина заполнителя (Pad Length), а также указатель на протокол следующего уровня (Next Header). Завершает пакет поле контроля целостности (Authentication Data). В том случае, когда при установлении безопасной ассоциации принято решение не использовать возможностей ESP по обеспечению целостности, это поле отсутствует.

Программное обеспечение перечисленных протоколов (утилиты шифрования, цифровой подписи и прочее) может функционировать на серверах или компьютерах конечных пользователей. Однако чаще его устанавливают на маршрутизаторах или специальных устройствах, которые в архитектуре IPSec именуются шлюзами безопасности (Security Gateway).

Различают два режима использования протокола ESP – транспортный и туннельный. На рис. 6 показано расположение ESPзаголовка в туннельном и транспортном режимах.

***Рис. 6. IР-пакет после применения протокола ЕSР в транспортном и туннельном режимах***

В *транспортном режиме* зашифрованные данные транспортируются непосредственно между хостами. В транспортном режиме протокола ESP заголовок исходного IP-пакета остается внешним.

Заголовок ESP помещается в передаваемый пакет между заголовками протоколов третьего (IP) и четвертого (например, TCP) уровней. Заметим, что поля протокола ESP следуют после стандартного IP-заголовка, а это означает, что такой пакет может маршрутизироваться в сети с помощью обычного оборудования, поддерживающего IP.

Шифрованию подвергаются только данные исходного IP-пакета (пакет верхнего уровня) и заключительная часть ESP-заголовка (ESP trailer). В этом режиме ESP не шифрует заголовок IP-пакета, иначе маршрутизатор не сможет прочитать поля заголовка и корректно осуществить продвижение пакета между сетями. В число шифруемых полей не попали также поля SPI и SN, которые должны передаваться в открытом виде, для того чтобы прибывший пакет можно было отнести к определенной ассоциации SA и защититься от ложного воспроизведения пакета.

В отличие от протокола AH, контроль целостности и аутентичности данных в протоколе ESP не распространяется на заголовок исходного пакета, и по этой причине имеет смысл применять оба протокола совместно – ESP для шифрования, а AH для контроля целостности.

Таким образом, адресная информация (IP-адреса отсылающей и принимающей сторон) видна при пересылке пакета по сети, и несанкционированное изменение этих IP-адресов не будет замечено.

В *туннельном режиме* основная роль отводится шлюзам безопасности, поскольку предполагается, что клиентские станции (или серверы) могут не поддерживать IPSec и отправляют в сеть обычный IP-трафик. Перед тем как достичь каналов глобальной сети, каждый исходный IP-пакет сначала попадает в шлюз, который помещает этот пакет целиком в «оболочку» IPSec, зашифровывая его содержимое вместе с исходным IP-заголовком. Чтобы обеспечить возможность маршрутизации получившегося пакета, шлюз снабжает его новым IP-заголовком и только после этого отправляет в сеть. Шлюз, находящийся на противоположном конце соединения, расшифровывает этот пакет и передает его на оконечное устройство в первоначальном виде. Описанная процедура называется *туннелированием*.

По рис. 6 видно, что в туннельном режиме в качестве внешнего заголовка создается новый заголовок IP. Весь исходный IP-пакет (и данные, и заголовок IP) и заключительная часть заголовка ESP (трейлер ESP) шифруются. Поэтому адресная информация исходного IP-пакета недоступна для просмотра. Заголовок внешнего IP-пакета протоколом ESP не защищается.

Туннелирование позволяет распространить действие средств защиты на сетевой уровень модели OSI и, в частности, скрыть истинные адреса источника и получателя. При этом уменьшается риск атак, основанных на детальном анализе трафика.

Сравнивая протоколы ESP и AH, можно заметить, что они дублируют функциональность друг друга в области обеспечения аутентификации данных. Главным отличием протокола AH от ESP в данном вопросе является то, что протокол AH обеспечивает аутентификацию всего пакета (и IP-заголовка, и самих данных), в то время как протокол ESP аутентифицирует только данные из пакета (см. рис. 6). При шифровании в протоколе ESP используется симметричный секретный ключ, то есть передаваемые данные зашифровываются и расшифровываются с помощью одного и того же ключа. Для протокола ЕSР также определен перечень обязательных алгоритмов шифрования – это DES, МD5 и SНА-1.

При аутентификации данных протокол ESP использует те же алгоритмы HMAC, что и протокол AH (использующие MD5 или SHA-1 в качестве функции хэширования). Однако способы применения различаются (см. рис. 6):

* + в транспортном режиме протокол ESP аутентифицирует только данные из пакета, не затрагивая IP-заголовка (протокол AH в том же режиме защищает и данные, и оба заголовка);
  + в туннельном режиме аутентификация в ESP-протоколе применяется к данным пакета и исходному IP-заголовку, но не затрагивает нового IP-заголовка (протокол AH в туннельном режиме аутентифицирует данные, AH-заголовок и оба IP-заголовка).

Протокол ESP может применяться отдельно или совместно с протоколом AH. При совместном использовании протоколы АН и ЕSР могут комбинироваться разными способами. Если используется транспортный режим, то аналогично тому, как в рамках ЕSР аутентификация идет следом за шифрованием, протокол АН должен применяться после протокола ЕSР. В туннельном режиме протоколы АН и ЕSР применяются к разным вложенным пакетам и, кроме того, допускается многократная вложенность туннелей с различными начальными и/или конечными точками.

## Алгоритмы аутентификации и шифрования в IPSec

Стек протоколов IPSec представляет собой согласованный набор открытых стандартов, имеющий вполне определенное ядро, и в то же время он может быть достаточно просто дополнен новыми протоколами, алгоритмами и функциями. Благодаря модульной структуре протоколы АН и ESP допускают применение пользователями по их согласованному выбору различных криптографических алгоритмов аутентификации и шифрования. Для шифрования данных в IPSec (протокол ESP) может быть применен практически любой симметричный алгоритм шифрования, использующий секретные ключи.

Для обеспечения целостности и аутентификации данных (протоколы АН и ESP) используется один из приемов шифрования – шифрование с помощью односторонней функции (One-way Function), называемой также хэш-функцией (Hash Function) или дайджест-функцией (Digest Function). Эта функция, примененная к шифруемым данным, дает в результате дайджест-значение, состоящее из фиксированного небольшого числа байтов. Дайджест передается в IP-пакете вместе с исходным сообщением. Получатель, зная, какая односторонняя функция шифрования была применена для составления дайджеста, заново вычисляет его, используя исходное сообщение. Если значения полученного и вычисленного дайджестов совпадают, это значит, что содержимое пакета во время передачи не было подвергнуто никаким изменениям. Знание дайджеста не дает возможности восстановить исходное сообщение и поэтому не может быть использовано для защиты конфиденциальности, но зато оно позволяет проверить целостность данных.

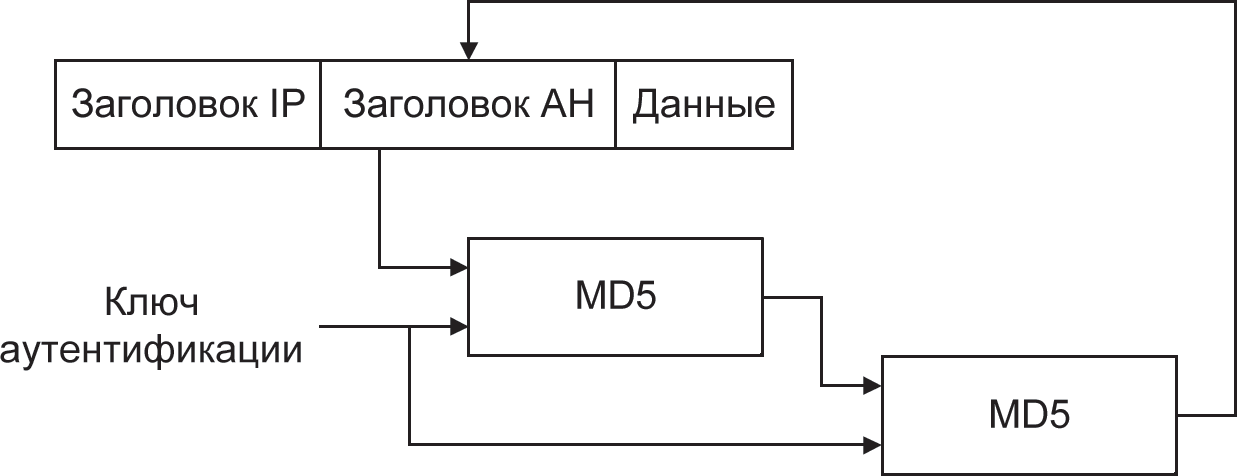
Дайджест является своего рода контрольной суммой для исходного сообщения. В отличие от традиционной контрольной суммы, при вычислении дайджеста используется секретный ключ. Если для получения дайджеста применялась односторонняя функция с параметром (в качестве которого выступает секретный ключ), известным только отправителю и получателю, любая модификация исходного сообщения будет немедленно обнаружена.

В целях обеспечения совместимости продуктов разных производителей рабочая группа IЕТF определила базовый набор поддерживаемых функций и алгоритмов, который должен быть однотипно реализован во всех продуктах, поддерживающих IРSес. На сегодня определены два алгоритма аутентификации и семь алгоритмов шифрования.

Для протоколов АН и ЕSР зарегистрированы два алгоритма аутентификации – НМАС-МD5 и НМАС-SНА-1. Алгоритм HMAC (Keyed-Hashing for Message Authentication Code) определяется стандартом RFC 2104. Функции MD5 (Message Digest version 5, стандарт RFC 1321) и SHA-1 (Secure Hash Algorithm version 1, стандарт FIPS 180-1) являются функциями хэширования. Алгоритмы НМАС-МD5

и НМАС-SНА-1 являются алгоритмами аутентификации с общим секретным ключом. Секретный ключ имеет длину 128 бит в случае MD5 и 160 бит в случае SHA-1.

Если секретный ключ известен только передающей и принимающей сторонам, это обеспечит аутентификацию источника данных, а также целостность пакетов, пересылаемых между двумя сторонами. Для обеспечения совместимости оборудования и программного обеспечения на начальной стадии реализации протокола IРSес один из зарегистрированных алгоритмов аутентификации принято использовать по умолчанию. В качестве такого алгоритма определен алгоритм НМАС-МD5.

Структура алгоритма HMAC показана на рис. 7. Принцип действия алгоритма HMAC заключается в двукратной обработке пакета функцией хэширования, управляемой ключом аутентификации (например, функцией хэширования MD5).

***Рис. 7. Структура HMAC-алгоритма***

Как видно по рис. 7, оба раза в обрабатываемые данные включается секретный ключ, который обеспечивает аутентификацию передаваемой информации. Полученная контрольная сумма помещается в заголовок протокола AH. Проверка аутентификации на другой стороне осуществляется путем повторного вычисления контрольной суммы для пришедшего пакета с использованием такого же ключа и сравнения полученного результата с присланным.

HMAC – это алгоритм аутентификации с секретным ключом. Целостность данных и аутентификация их источника, обеспечиваемые им, зависят от масштаба распространения секретного ключа. Если ключ HMAC известен только передающей и принимающей сторонам, это обеспечит и аутентификацию источника данных, и целостность пакетов данных, пересылаемых между двумя сторонами. Ключи для HMAC генерируются посредством процедуры ISAKMP/Oakley.

Алгоритм HMAC реализует симметричную схему аутентификации, используя параметр проверки целостности пакета ICV (Integrity Check Value). По сути, он представляет собой цифровую подпись, помещаемую в поле аутентификации и позволяющую отправителю подписать результат предварительного хэширования содержательной части пакета ESP.

Анализ содержимого этого поля дает возможность получателю идентифицировать источник данных и убедиться в том, что они не были изменены в процессе передачи. Если для протокола ESP функции аутентификации являются факультативными, то для протокола AH процесс аутентификации является обязательным.

Для протокола ЕSР зарегистрировано несколько алгоритмов шифрования. Чаще всего в качестве алгоритмов шифрования для ESP применяются DES (Data Encryption Standard), 3-DES (тройной DES) и новый стандарт шифрования AES (Advanced Encryption Standard). Для обеспечения IPSec-совместимости по умолчанию в качестве алгоритма шифрования стандартом предусмотрен симметричный метод DES-CBC (Cipher Block Chaining) с явно заданным вектором инициализации IV и с 56-разрядным ключом. Алгоритм AES повсюду встраивается в стандарт IPSec как альтернатива DES и 3-DES.

Выбор алгоритма шифрования целиком зависит от разработчика. Возможность выбора алгоритма шифрования предоставляет пользователю дополнительное преимущество: ведь злоумышленник должен не только вскрыть шифр, но и определить, какой именно шифр ему надо вскрывать. Вместе с необходимостью подбора ключей это еще более уменьшает шансы злоумышленника своевременно расшифровать данные пользователя.

IРSес может работать совместно с протоколом L2ТР, который выполняют только туннелирование, но не обеспечивают шифрования и аутентификации данных. Эти протоколы создают через Интернет туннель для пакетов любых протоколов, упаковывая их в пакеты IР. Когда трафик с помощью L2ТР оказывается упакованным в пакеты IР, то дальше для его защиты можно использовать IРSес. В результате комбинирование IРSес с протоколами туннелирования типа L2F/L2ТР позволяет решить задачу защиты данных для протоколов, отличных от IР.

Алгоритмическая независимость протоколов АН и ЕSР требует предварительного согласования взаимодействующими сторонами набора применяемых алгоритмов и их параметров.

# Протокол управления криптоключами IKE

Протоколы ESP и AH позволяют реализовать важнейшие атрибуты защищенной передачи – конфиденциальность связи, аутентификацию сторон и целостность данных. Однако их функции теряют всякую ценность в отсутствие мощной поддерживающей инфраструктуры, которая обеспечивала бы распределение ключей и согласование протоколов между участниками обмена.

Роль такой инфраструктуры в IPSec выполняет группа протоколов *IKE* (*Internet KeyExchange*)*.* Это название пришло в 1998 году на смену более раннему – ISAKMP/Oakley, которое непосредственно указывало на происхождение средств управления ключами в составе IPSec. Протокол *ISAKMP* (*Internet Security Association and Key Management Protocol*)*,* описанный в документе RFC 2408, позволяет согласовывать алгоритмы и математические структуры (так называемые мультипликативные группы, определенные на конечном поле) для процедуры обмена ключами Диффи–Хеллмана, а также процессов аутентификации. Протокол Oakley, описанный в RFC 2412, основан на алгоритме Диффи–Хеллмана и служит для организации непосредственного обмена ключами.

Протоколы IKE решают три задачи:

* + - осуществляют аутентификацию взаимодействующих сторон, согласовывают алгоритмы шифрования и характеристики ключей, которые будут использоваться в защищенном сеансе обмена информацией;
    - обеспечивают создание ключевой информации соединения и управление ею, непосредственный обмен ключами (в том числе возможность их частой смены);
    - управляют параметрами соединения и защитой от некоторых типов атак, контролируют выполнение всех достигнутых соглашений.

Разработчики IPSec начали свою деятельность с решения последней из перечисленных задач. В результате на свет появилась *концепция защищенных виртуальных соединений* или *безопасных ассоциаций SA* (*Security Associations*)*.*

## Установление безопасной ассоциации SA.

Основой функционирования IPSec являются защищенные виртуальные соединения, или безопасные ассоциации SA. Для того чтобы протоколы АН и ЕSР могли выполнять свою работу по защите передаваемых данных, между двумя конечными точками должна быть сформирована ассоциация SA. Безопасная ассоциация SA представляет собой соглашение о защите обмена данными между двумя взаимодействующими партнерами.

Установление безопасной ассоциации SA должно начинаться со взаимной аутентификации сторон, потому что меры безопасности теряют всякий смысл, если данные передаются или принимаются неавторизованными пользователями. Процедуры установления безопасной ассоциации SA оправданы лишь в том случае, если у каждой из сторон имеется полная уверенность в том, что ее партнер – именно тот, за кого он себя выдает.

Для выполнения аутентификации сторон в IКЕ применяются два основных способа.

Первый способ основан на использовании разделяемого секрета. Перед инициализацией IРSес-устройств, образующих безопасные ассоциации, в их базу данных помещается предварительно распределенный разделяемый секрет. Цифровая подпись на основе односторонней функции, например, МD5, использующей в качестве аргумента этот предварительно распределенный секрет, доказывает аутентичность противоположной стороны.

Второй способ основан на использовании технологии цифровой подписи и цифровых сертификатов стандарта Х.509: каждая из сторон подписывает свой цифровой сертификат своим закрытым ключом и передает эти данные противоположной стороне. Если подписанный сертификат расшифровывается открытым ключом отправителя, то это удостоверяет тот факт, что отправитель, предоставивший данные, действительно обладает ответной частью данного открытого ключа – соответствующим закрытым ключом.

Однако следует отметить, что для удостоверения аутентичности стороны нужно еще убедиться в аутентичности самого сертификата, и для этого сертификат должен быть подписан не только его владельцем, но и некоторой третьей стороной, выдавшей сертификат и вызывающей доверие. В архитектуре IPSec эта третья сторона именуется органом сертификации CA (Certification Authority).

После проведения взаимной аутентификации взаимодействующие стороны могут непосредственно перейти к согласованию параметров защищенного канала. Выбираемые параметры безопасной ассоциации SA определяют протокол, используемый для обеспечения безопасности передачи данных; алгоритм аутентификации протокола AH и его ключи; алгоритм шифрования, используемый протоколом ESP, и его ключи; наличие или отсутствие криптографической синхронизации; способы защиты сеанса обмена; частоту смены ключей и ряд других параметров. Важным параметром безопасной ассоциации SA является так называемый криптографический материал, то есть секретные ключи, используемые в работе протоколов AH и ESP. Сервисы безопасности, предлагаемые IPSec, используют для формирования криптографических ключей разделяемые секреты.

Параметры безопасной ассоциации SA должны устраивать обе конечные точки защищенного канала. Поэтому при использовании автоматической процедуры установления SA протоколы IKE, работающие по разные стороны канала, выбирают параметры в ходе переговорного процесса. Безопасная ассоциация SA представляет собой в IPSec однонаправленное логическое соединение, поэтому при двустороннем обмене данными необходимо установить две ассоциации SA. В рамках одной ассоциации SА может работать только один из протоколов защиты данных – либо АН, либо ЕSР, но не оба вместе.

Система IPSec допускает применение ручного и автоматического способов установления безопасной ассоциации.

## Базы данных SAD и SPD

В каждом узле, поддерживающем IPSec, используются базы данных двух типов:

* + - база данных безопасных ассоциаций SAD (Security Associations Database);
    - база данных политики безопасности SPD (Security Policy Database).

При установлении безопасной ассоциации SA две вступающие в обмен стороны принимают ряд соглашений, регламентирующих процесс передачи потока данных между ними. Соглашения представляются в виде набора параметров. Для безопасной ассоциации SA такими параметрами являются, в частности, тип и режим работы протокола защиты (AH или ESP), методы шифрования, секретные ключи, значение текущего номера пакета в ассоциации и другая информация.

Наборы текущих параметров, определяющих все активные ассоциации, хранятся 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.

Кроме базы данных безопасных ассоциаций SAD, в архитектуре IPSec существует еще один компонент – база данных политики безопасности SPD, которая задает соответствие между IP-пакетами и установленными для них правилами обработки. При обработке пакетов базы данных SPD используются совместно с базами данных SAD. База данных политики безопасности SРD представляет собой упорядоченный набор правил, каждое из которых включает совокупность селекторов и допустимых политик безопасности. Селекторы служат для отбора пакетов, а политики безопасности задают требуемую обработку. Такая база данных формируется и поддерживается на каждом узле, где установлено программное обеспечение IPSec.

Политика безопасности предусматривает три возможных варианта обработки IР-пакета:

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

Каждый узел IPSec должен поддерживать две базы SPD: одну – для исходящего трафика, а другую – для входящего, так как может требоваться разная защита в разных направлениях.

Использование баз SPD и SAD для управления процессом защиты трафика позволяет достаточно гибко сочетать механизм безопасных ассоциаций, который предусматривает установление логического соединения, с дейтаграммным характером трафика протокола IP. Соответствующая настройка базы SDP позволяет выбирать нужную степень детализации защиты – от применения одной общей ассоциации для трафика большого количества конечных узлов до защиты каждого отдельного приложения с помощью индивидуально настроенной ассоциации.

## Согласование параметров защищенных каналов и распределение криптографических ключей.

При построении защищенных виртуальных сетей VPN важную роль играют функции согласования параметров защищенных туннелей и распределения криптографических ключей. Эти функции должны реализовываться при формировании каждого криптозащищенного канала. Применяемые в VPN криптографические ключи можно разделить по длительности использования на следующие типы:

* + - основные ключи, которые применяются в течение относительно долгого периода времени (от недели до нескольких месяцев);
    - временные ключи, каждый из которых генерируется для криптозащиты информации в рамках одного защищенного канала.

Основные ключи обеспечивают аутентификацию сторон, а также криптозащиту распределяемых временных ключей. Основные ключи должны распределяться заблаговременно до формирования защищенных виртуальных соединений. Наиболее высокая эффективность распределения основных криптографических ключей достигается при использовании асимметричных криптосистем, когда распределению подлежат только открытые ключи.

Временные (сеансовые) ключи, действующие в рамках одного криптозащищенного туннеля, распределяются по сети с помощью основных ключей. Одним из наиболее популярных алгоритмов формирования сеансового ключа на основе распределенных или передаваемых друг другу открытых ключей является алгоритм Диффи–Хеллмана. Поскольку для шифрования передаваемых данных используются симметричные криптосистемы, сеансовые ключи, как правило, являются симметричными ключами шифрования.

После аутентификации сторон и безопасного распределения временных ключей, а также согласования параметров защищенного туннеля криптозащита трафика в рамках этого туннеля осуществляется на основе распределенных временных ключей.

Существуют два основных способа построения защищенного виртуального туннеля между двумя узлами компьютерной сети:

* + - формирование защищенного канала для каждого соединения, устанавливаемого каким-либо программным приложением;
    - формирование общего защищенного канала между сетевыми узлами и создание в рамках этого канала отдельных защищенных соединений.

Формирование защищенного виртуального канала для каждого соединения включает следующие этапы:

* + - выдачу запроса одной из сторон и достижение соглашения на создание защищенного виртуального канала;
    - аутентификацию сторон, выполняемую с помощью ранее распределенных основных ключей шифрования или назначенных паролей;
    - распределение временных ключей и согласование параметров защищенного канала.

Обычно второй и третий этапы совмещаются друг с другом, и аутентификация выполняется совместно с распределением временных ключей.

При формировании между двумя сетевыми узлами общего защищенного канала, в рамках которого затем создаются отдельные защищенные соединения, перечисленные этапы выполняются как при установлении защищенного канала, так и при создании каждого защищенного соединения.

В начале формирования общего защищенного канала распределяется главный сеансовый ключ симметричного шифрования. Это распределение осуществляется с помощью основных ключей взаимодействующих сторон. Распределение же временных ключей для каждого создаваемого защищенного соединения выполняется на основе главного сеансового ключа. Независимо от числа защищенных соединений, создаваемых в рамках одного защищенного туннеля, основные ключи используются только один раз – при распределении главного сеансового ключа.

Способ формирования общего защищенного канала и создания затем на его основе отдельных защищенных соединений характеризуется более высокой сложностью реализации. Однако в этом случае снижается уязвимость закрытых основных ключей, служащих для распределения главного сеансового ключа, и может быть обеспечено более эффективное расходование компьютерных ресурсов, затрачиваемых на генерацию временных ключей.

Процесс установления защищенного соединения в протоколе IKE разбит на две фазы. Во время *первой фазы* происходит аутентификация участников, стороны договариваются о том, как они будут защищать обмен информацией во второй фазе, и происходит выработка ключевого материала для защиты обменов во второй фазе.

Во *второй фазе* участники договариваются о параметрах защищенного соединения (какие алгоритмы и в каком порядке использовать, параметры этих алгоритмов и т. п.) и обмениваются ключевой информацией (хотя это действие опционально). Все обмены второй фазы и часть обменов первой фазы передаются в зашифрованном виде (о том, как и чем шифровать, стороны договариваются в первой фазе).

# Особенности реализации средств IPSec

Протоколы AH или ESP могут защищать передаваемые данные в двух режимах:

* + - туннельном, при котором IР-пакеты защищаются целиком, включая их заголовки;
    - транспортном, обеспечивающем защиту только содержимого IР-пакетов.

Основным режимом является туннельный. В туннельном режиме исходный пакет помещается в новый IР-пакет, и передача данных по сети выполняется на основании заголовка нового IР-пакета.

При работе в этом режиме каждый обычный IР-пакет помещается целиком в криптозащищенном виде в конверт IРSес, а тот, в свою очередь, инкапсулируется в другой защищенный IР-пакет. Туннельный режим обычно реализуют на специально выделенных шлюзах безопасности, в роли которых могут выступать маршрутизаторы или межсетевые экраны. Между такими шлюзами и формируются защищенные туннели IРSес.

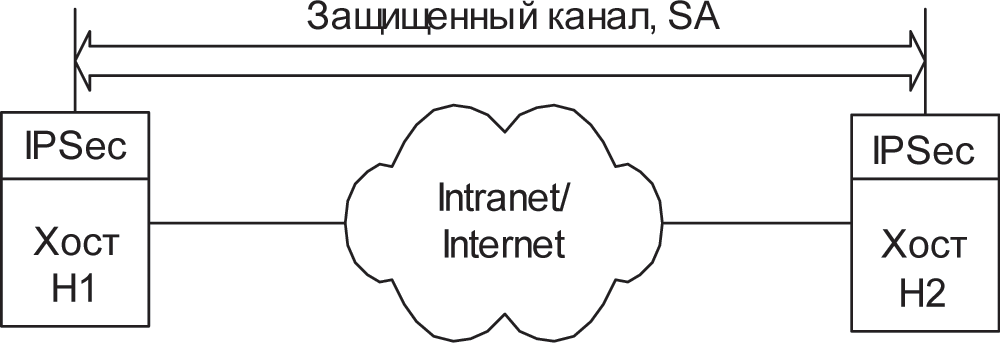
После приема на другой стороне туннеля защищенные IР-пакеты распаковываются и полученные исходные IР-пакеты передаются компьютерам приемной локальной сети по стандартным правилам. В транспортном режиме передача IР-пакета через сеть выполняется с помощью исходного заголовка этого пакета. В конверт IРSес в криптозащищенном виде помещается только содержимое исходного IР-пакета, и к полученному конверту добавляется исходный IР-заголовок. Транспортный режим быстрее туннельного и разработан для применения на оконечных системах. Данный режим может использоваться для поддержки удаленных и мобильных пользователей, а также для защиты информационных потоков внутри локальных сетей.

## Основные схемы применения IPSec

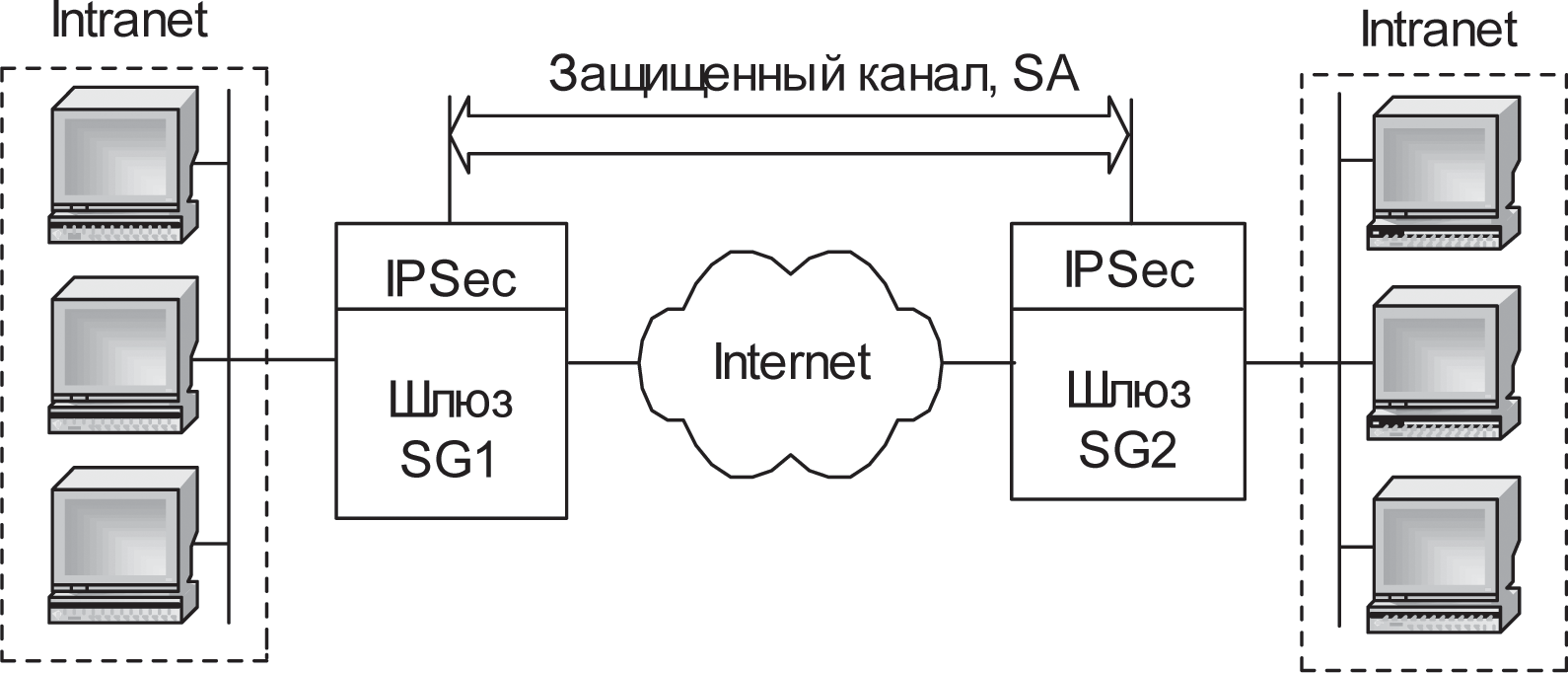
Применение туннельного или транспортного режима зависит от требований, предъявляемых к защите данных, а также от роли узла, в котором работает IРSес. Узлом, завершающим защищенный канал, может быть *хост* (конечный узел) или *шлюз* (промежуточный узел). Соответственно, различают три основные схемы применения IPSec: хост–хост, шлюз–шлюз и хост–шлюз.

В первой схеме защищенный канал, или, что в данном контексте одно и то же, безопасная ассоциация, устанавливается между двумя конечными узлами сети, то есть хостами Н1 и Н2 (рис. 8). Протокол IPSec в этом случае работает на конечном узле и защищает данные, поступающие на него. Для хостов, поддерживающих IРSес, разрешается использовать как транспортный режим, так и туннельный.

В соответствии со второй схемой защищенный канал устанавливается между двумя промежуточными узлами, называемыми шлюзами безопасности SG1 и SG2, на каждом из которых работает протокол IPSec (рис. 9).



***Рис. 8. Схема хост–хост***

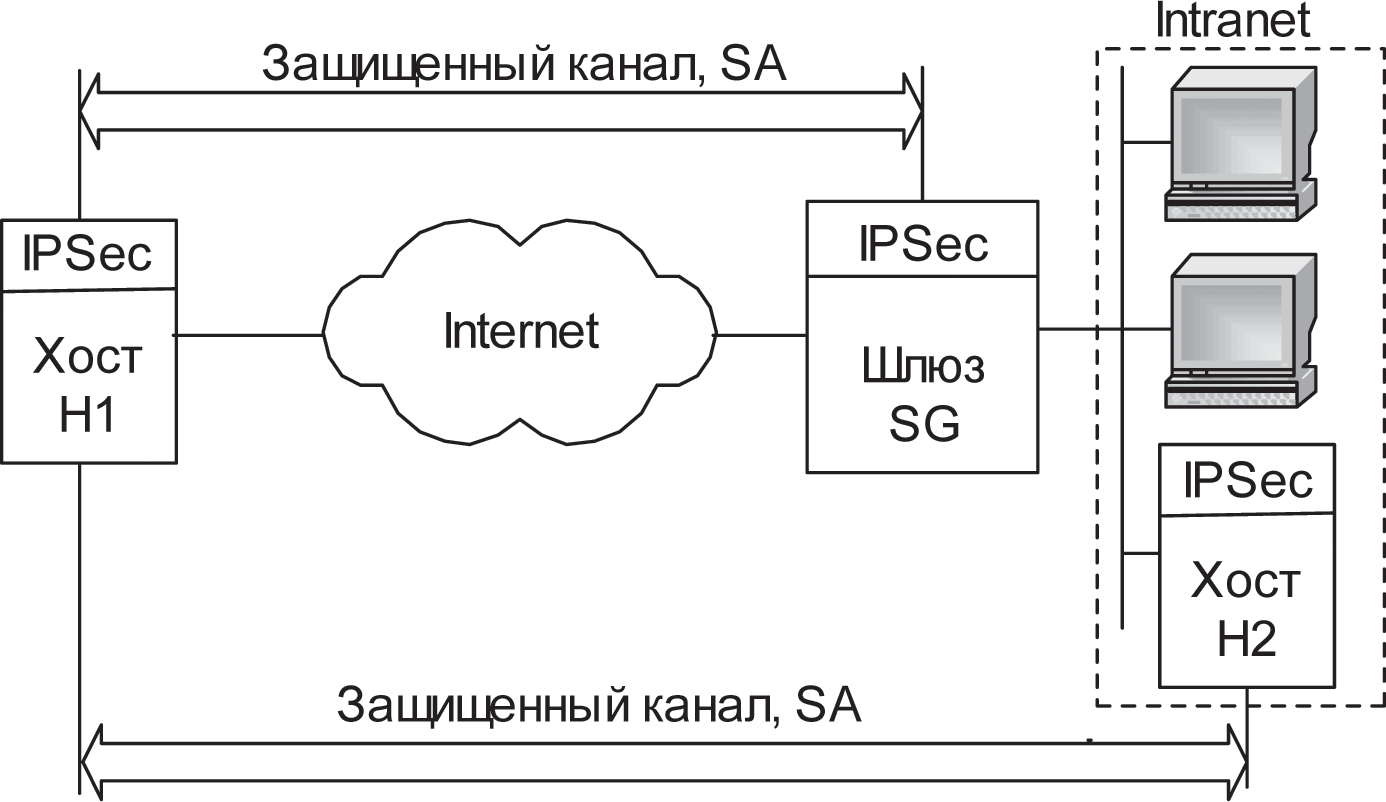


***Рис. 9. Схема шлюз–шлюз***

Шлюз безопасности представляет собой сетевое устройство, подключаемое к двум сетям, которое выполняет функции шифрования и аутентификации для хостов, расположенных позади него. Шлюз безопасности VPN может быть реализован в виде отдельного программного продукта, отдельного аппаратного устройства, а также в виде маршрутизатора или межсетевого экрана, дополненного функциями VPN.

Защищенный обмен данными может происходить между любыми двумя конечными узлами, подключенными к сетям, которые расположены позади шлюзов безопасности. При защищенном удаленном доступе часто применяется схема хост–шлюз (рис. 10).

Здесь защищенный канал организуется между удаленным хостом Н1, на котором работает IPSec, и шлюзом SG, защищающим трафик для всех хостов, входящих в сеть Intranet предприятия. Удаленный хост может использовать при отправке пакетов шлюзу как транспортный, так и туннельный режим, шлюз же отправляет пакеты хосту только в туннельном режиме.

***Рис. 10. Схема хост–шлюз, дополненная каналом хост–хост***

Эту схему можно модифицировать, создав параллельно еще один защищенный канал – между удаленным хостом Н1 и каким-либо хостом Н2, принадлежащим внутренней сети, защищаемой шлюзом. Такое комбинированное использование двух SA позволяет надежно защитить трафик и во внутренней сети.

Рассмотренные схемы построения защищенных каналов на базе IPSec широко применяются при создании разнообразных виртуальных защищенных сетей VPN. На базе IPSec успешно реализуются виртуальные защищенные сети любой архитектуры, включая VPN с удаленным доступом (Remote Access VPN), внутрикорпоративные VPN (Intranet VPN) и межкорпоративные VPN (Extranet VPN).

## Преимущества средств безопасности IPSec

Система стандартов IPSec вобрала в себя прогрессивные методики и достижения в области сетевой безопасности, завоевала признание специалистов как надежная и легко интегрируемая система безопасности для IP-сетей. Система IРSес прочно занимает лидирующие позиции в наборе стандартов для создания VPN. Этому способствует ее открытое построение, способное включать все новые достижения в области криптографии. IPsec позволяет защитить сеть от большинства сетевых атак, «сбрасывая» чужие пакеты еще до того, как они достигнут уровня IP на принимающем компьютере. В защищаемый компьютер или сеть могут войти только пакеты от зарегистрированных партнеров по взаимодействию.

IPsec обеспечивает:

* + - аутентификацию – доказательство отправки пакетов вашим партнером по взаимодействию, то есть обладателем разделяемого секрета;
    - целостность – невозможность изменения данных в пакете;
    - конфиденциальность – невозможность раскрытия передаваемых данных;
    - надежное управление ключами – протокол IKE вычисляет разделяемый секрет, известный только получателю и отправителю пакета;
    - туннелирование – полную маскировку топологии локальной сети предприятия.

Работа в рамках стандартов IPSec обеспечивает полную защиту информационного потока данных от отправителя до получателя, закрывая трафик для наблюдателей на промежуточных узлах сети. VPN-решения на основе стека протоколов IPSec обеспечивают построение виртуальных защищенных сетей, их безопасную эксплуатацию и интеграцию с открытыми коммуникационными системами.

## Оборудование для создания IPSec каналов.

Многофункциональные устройства обеспечения безопасности Cisco ASA (Adaptive Security Appliance) с сервисами FirePOWER.