Протоколы защищенного канала. IPsec

БГА, РТФ
Кафедра ИБ

Зензин Александр Степанович, к.т.н.

Обзор

1. Технологии защищенного канала
2. Иерархия технологий защищенного канала
3. Распределение функций между протоколами IPsec
4. Безопасная ассоциация
5. Транспортный и туннельный режимы
6. Протокол AH
7. Протокол ESP
8. База данных SAD и SPD
9. Сети VPN на основе шифрования

Технологии защищенного канала

Известно, что задачу защиты данных можно разделить на две подзадачи: защиту данных внутри компьютера и защиту данных в процессе их передачи от одного компьютера в другой. Для обеспечения безопасности данных при их передаче по публичным сетям используются различные технологии защищенного канала.

Технология защищенного канала обеспечивает защиту трафика между двумя точками в открытой транспортной сети, например в Интернете, Защищенный канал подразумевает выполнение трех основных функций:

- взаимная аутентификация абонентов при установлении соединения, которая может быть выполнена, например, путем обмена паролями;
- защита передаваемых каналу сообщений от несанкционированного доступа, например, путем шифрования;
- подтверждение целостности поступающих по каналу сообщений, например, путем передачи одновременно с сообщением его дайджеста.

В зависимости от места расположения программного обеспечения защищенного канала различает две схемы его образования:

- схема с конечными узлами, взаимодействующими через публичную сеть (рис. 1, а);
- схема с оборудованием поставщика услуг публичной сети, расположенным на границе между частной и публичной сетями (рис. 1, б).

Технологии защищенного канала

В первом случае защищенный канал образуется программными средствами, установленными на двух удаленных компьютерах, принадлежащих двум разным локальным сетям одного предприятия и связанных между собой через публичную сеть. Преимуществом этого подхода является полная защищенность канала вдоль всего пути следования, а также возможность использования любых протоколов создания защищенных каналов, лишь бы на конечных точках канала поддерживался один и тот же протокол. Недостатки заключаются в избыточности и децентрализованности решения.

Рис. 1. Два подхода к образованию защищенного канала

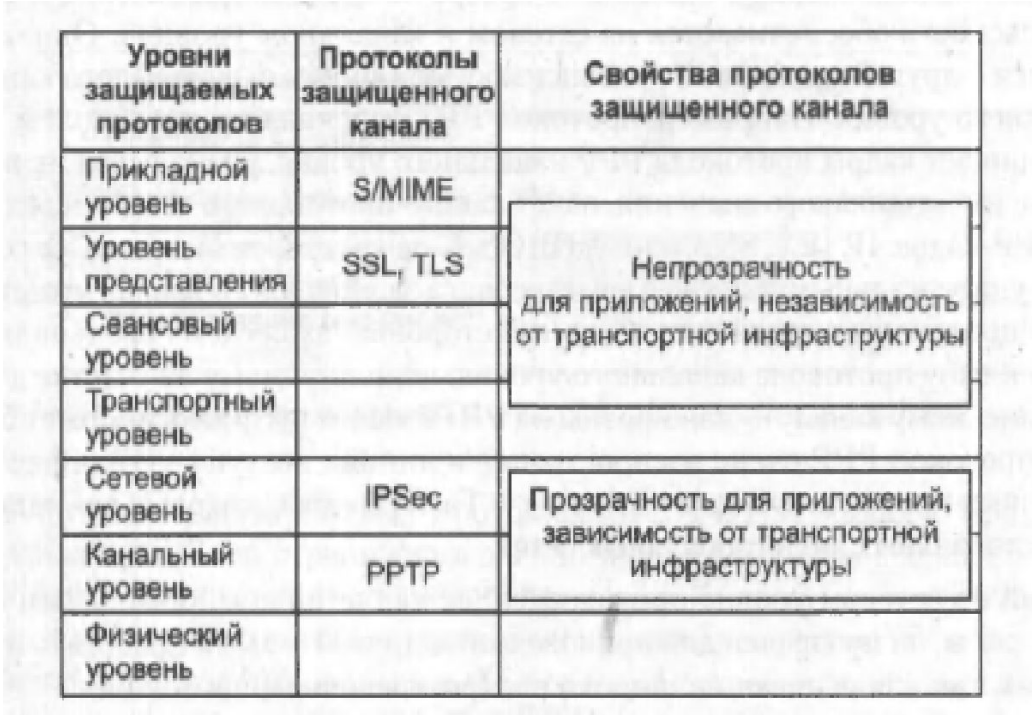
Технологии защищенного канала

Избыточность состоит в том, что вряд ли стоит создавать защищенный канал на всем пути следования данных: уязвимыми для злоумышленников обычно являются сети с коммутацией пакетов, а не каналы телефонной сети или выделенные каналы, через которые локальные сети подключены к территориальной сети. Поэтому защиту каналов доступа к публичной сети можно считать избыточной. Децентрализация заключается в том, что для каждого компьютера, которому требуется предоставить услуги защищенного канала, необходимо отдельно устанавливать, конфигурировать и администрировать программные средства защиты данных. Подключение каждого нового компьютера к защищенному каналу требует выполнять эти трудоемкие операции заново.

Во втором случае клиенты и серверы не участвуют в создании защищенного канала — он прокладывается только внутри публичной сети с коммутацией пакетов, например внутри Интернета. Так, канал может быть проложен между сервером удаленного доступа поставщика услуг публичной сети и пограничным маршрутизатором корпоративной сети. Это хорошо масштабируемое решение, управляемое централизовано администраторами как корпоративной сети, так и сети поставщика услуг. Для компьютеров корпоративной сети канал прозрачен — программное обеспечение этих конечных узлов остается без изменений. Такой гибкий подход позволяет легко образовывать новые каналы защищенного взаимодействия между компьютерами независимо от места их расположения. Реализация этого подхода сложнее — нужен стандартный протокол образования защищенного канала, требуется установка у всех поставщиков услуг программного обеспечения, поддерживающего такой протокол, необходима поддержка протокола производителями пограничного коммуникационного оборудования. Но остаются сомнения в надежности защиты: во-первых, незащищенными оказываются каналы доступа к публичной сети, во-вторых, потребитель услуг чувствует себя в полной зависимости от надежности поставщика услуг.

Иерархия технологий защищенного канала

Защищенный канал можно построить с помощью системных средств, реализованных на разных уровнях модели OSI (рис. 2).



Уровни защищаемых протоколов	Протоколы защищенного канала	Свойства протоколов защищенного канала
Прикладной уровень	S/MIME	Непрозрачность для приложений, независимость от транспортной инфраструктуры
Уровень представления	SSL, TLS	
Сеансовый уровень		
Транспортный уровень		
Сетевой уровень	IPSec	Прозрачность для приложений, зависимость от транспортной инфраструктуры
Канальный уровень	PPTP	
Физический уровень		

Рис. 2. Протоколы, формирующие защищенный канал на разных уровнях модели OSI

Если защита данных осуществляется средствами верхних уровней (прикладного, представления или сеансового), то такой способ защиты не зависит от технологий транспортировки данных (IP или IPX, Ethernet или ATM), что можно считать несомненным достоинством. В то же время приложения при этом становятся зависимыми от конкретного протокола защищенного канала, так как в них должны быть встроены явные вызовы функций этого протокола.

Иерархия технологий защищенного канала

Защищенный канал, реализованный на самом высоком (прикладном) уровне, защищает только вполне определенную сетевую службу, например файловую, гипертекстовую или почтовую. Так, протокол S/MIME защищает исключительно сообщения электронной почты. При таком подходе для каждой службы необходимо разрабатывать собственную защищенную версию протокола.

Популярный протокол SSL (Secure Socket Layer — слой защищенных сокетов) работает на уровне представления и создает защищенный канал, используя следующие технологии безопасности:

- взаимная аутентификация приложений на обоих концах защищенного канала выполняется путем обмена сертификатами (стандарт X.509);
- для контроля целостности передаваемых данных используются дайджесты;
- секретность обеспечивается шифрацией со средствами симметричных ключей сеанса.

Протокол SSL разработан компанией Netscape Communications для защиты данных, передаваемых между веб-сервером и веб-браузером, но он может быть использован и любыми другими приложениями. Работа протокола защищенного канала на уровне представления делает его более универсальным средством, чем протокол безопасности прикладного уровня. Однако для того чтобы приложение смогло воспользоваться протоколом уровня представления, в него по-прежнему приходится вносить исправления, хотя и не столь существенные, как в случае протокола прикладного уровня. Модификация приложения в данном случае сводится к встраиванию явных обращений к API соответствующего протокола безопасности.

Иерархия технологий защищенного канала

Средства защищенного канала становятся **прозрачными для приложений** в тех случаях, когда безопасность обеспечивается на сетевом и канальном уровнях. Однако здесь мы сталкиваемся с другой проблемой — зависимостью сервиса защищенного канала от протокола нижнего уровня. Например, протокол PPTP, не являясь протоколом канального уровня, защищает кадры протокола PPP канального уровня, упаковывая их в IP-пакеты. При этом не имеет никакого значения, пакет какого протокола, в свою очередь, упакован в данном PPP-кадре: IP, IPX, SNA или NetBIOS. С одной стороны, это делает сервис PPTP достаточно универсальным, так как клиент сервиса защищенного канала может задействовать любые протоколы в своей сети. С другой стороны, такая схема предъявляет жесткие требования к типу протокола канального уровня, используемому на участке доступа клиента к защищенному каналу — для протокола PPTP таким протоколом может быть только PPP. Хотя протокол PPP очень распространен в линиях доступа, сегодня конкуренцию ему составляют протоколы Gigabit Ethernet и Fast Ethernet, которые все чаще работают не только в локальных, но и глобальных сетях.

Работающий на сетевом уровне протокол IPSec является компромиссным вариантом. С одной стороны, он прозрачен для приложений, с другой — может "работать практически во всех сетях, так как основан на широко распространенном протоколе IP и использует любую технологию канального уровня (PPP, Ethernet, ATM и т. д.).

Распределение функций между протоколами IPsec

Протокол IPSec называют в стандартах Интернета **системой**. Действительно, IPSec — это согласованный набор открытых стандартов, имеющий сегодня вполне очерченное ядро, которое в то же время может быть достаточно просто дополнено новыми функциями и протоколами.

Ядро IPSec составляют три протокола:

- AH (Authentication Header — заголовок аутентификации) — гарантирует целостность и аутентичность данных;
- ESP (Encapsulating Security Payload — инкапсуляция зашифрованных данных) — шифрует передаваемые данные, обеспечивая конфиденциальность, может также поддерживать аутентификацию и целостность данных;
- IKE (Internet Key Exchange — обмен ключами Интернета) — решает вспомогательную задачу автоматического предоставления конечным точкам защищенного канала секретных ключей, необходимых для работы протоколов аутентификации и шифрования данных.

Распределение функций между протоколами IPsec

Как видно из краткого описания функций, возможности протоколов AH и ESP частично перекрываются (рис. 3). В то время как AH отвечает только за обеспечение целостности и аутентификации данных, ESP может шифровать данные и, кроме того, выполнять функции протокола AH (хотя, как увидим позднее, аутентификация и целостность обеспечиваются им в несколько урезанном виде). ESP может поддерживать функции шифрования и аутентификации/целостности в любых комбинациях, то есть либо всю группу функций, либо только аутентификацию/целостность, либо только шифрование.

Разделение функций защиты между протоколами AH и ESP вызвано применяемой во многих странах практикой ограничения экспорта и/или импорта средств, обеспечивающих конфиденциальность данных путем шифрования.

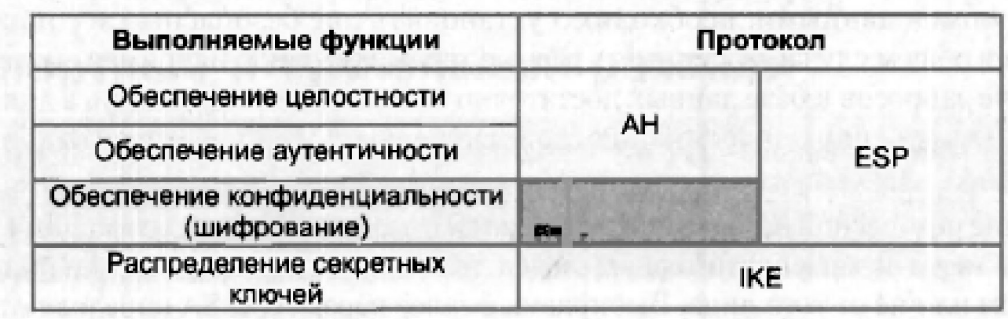


Рис. 3. Распределение функций между протоколами IPsec

Каждый из этих протоколов может использоваться как самостоятельно, так и одновременно с другим, так что в тех случаях, когда шифрование из-за действующих ограничений применять нельзя, систему можно поставлять только с протоколом AH. Естественно, подобная защита данных во многих случаях оказывается недостаточной. Принимающая сторона получает лишь возможность проверить, что данные были отправлены именно тем узлом, от которого они ожидаются, и дошли в том виде, в котором были отправлены. Однако от несанкционированного просмотра данных на пути их следования по сети протокол AH защитить не может, так как не шифрует их. Для шифрования данных необходим протокол ESP.

Безопасная ассоциация

Для того чтобы протоколы AH и ESP могли выполнять свою работу по защите передаваемых данных, протокол IKE устанавливает между двумя конечными точками логическое соединение (рис. 4), которое в стандартах IPSec носит название **безопасной ассоциации** (Security Association, SA).

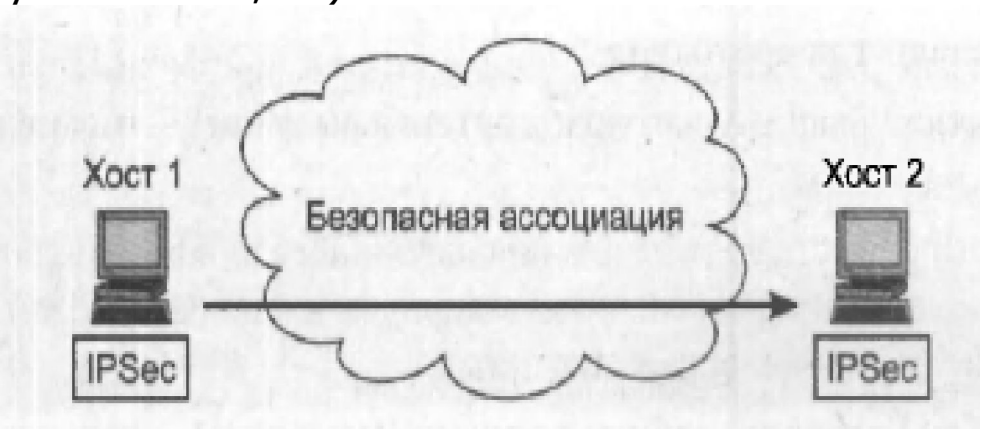


Рис. 4. Безопасная ассоциация

Стандарты IPSec позволяют конечным точкам защищенного канала использовать как одну безопасную ассоциацию для передачи трафика всех взаимодействующих через этот канал хостов, так и создавать для этой цели произвольное число безопасных ассоциаций, например, по одной на каждое TCP-соединение. Это дает возможность выбирать нужную степень детализации защиты — от одной общей ассоциации для трафика множества конечных узлов до индивидуально настроенных ассоциаций для защиты каждого приложения.

Безопасная ассоциация

Безопасная ассоциация в протоколе IPSec представляет собой однонаправленное (симплексное) логическое соединение, поэтому если требуется обеспечить безопасный двусторонний обмен данными, необходимо установить две безопасные ассоциации. Эти ассоциации в общем случае могут иметь разные характеристики, например, в одну сторону при передаче запросов к базе данных достаточно только аутентификации, а для ответных данных, несущих денную информацию, дополнительно нужно обеспечить конфиденциальность.

Установление безопасной ассоциации начинается с взаимной аутентификации сторон, потому что все меры безопасности теряют смысл, если данные передаются или принимаются не тем лицом или не от того лица. Выбираемые далее параметры SA определяют, какой из двух протоколов, AH или ESP, будет применяться для защиты данных, какие функции будет выполнять протокол (например, можно выполнять только аутентификацию и проверку целостности или, кроме того, еще и обеспечивать конфиденциальность). Очень важными параметрами безопасной ассоциации являются также секретные ключи, используемые в работе протоколов AH и ESP.

Протокол IPSec допускает как автоматическое, так и ручное установление безопасной ассоциации. При ручном способе администратор конфигурирует конечные узлы так, чтобы они поддерживали согласованные параметры ассоциации, включая секретные ключи. При автоматической процедуре установления SA протоколы IKE, работающие по разные стороны канала, выбирают параметры в ходе переговорного процесса.

Безопасная ассоциация

Для каждой задачи, решаемой протоколами AH и ESP, предлагается несколько схем аутентификации и шифрования (рис. 5). Это делает протокол IPSec очень гибким средством. Заметим, что выбор дайджест-функции для решения задач целостности и аутентификации никак не влияет на выбор функции шифрования, обеспечивающей конфиденциальность данных.

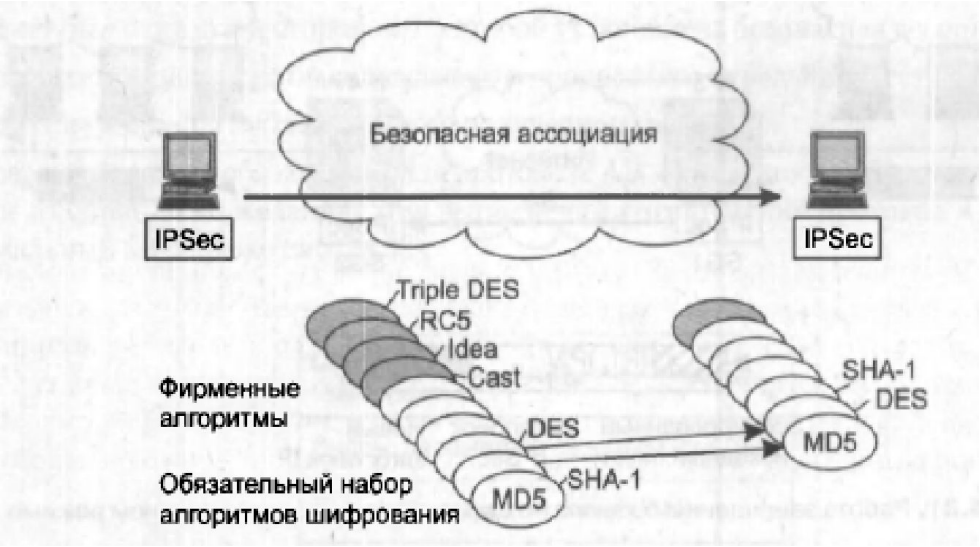


Рис. 5. Согласование параметров в протоколе ESP

Для обеспечения совместимости в стандартной версии IPsec определен некоторый обязательный «инструментальный» набор, в частности для аутентификации данных всегда может быть использована одна из стандартных дайджест-функций MD5 либо SHA-1, а в число алгоритмов шифрования непременно входит DES. При этом производители продуктов, в которых используется IPSec, вольны расширять протокол путем включения других алгоритмов аутентификации и симметричного шифрования, что они с успехом и делают. Например, многие реализации IPSec поддерживают популярный алгоритм шифрования Triple DES, а также сравнительно новые алгоритмы: Blowfish, Cast, CDMF, Idea, RC5.

Транспортный и туннельный режимы

Протоколы AH и ESP могут защищать данные в двух режимах: транспортном и туннельном. В **транспортном режиме** передача IP-пакета через сеть выполняется с помощью оригинального заголовка этого пакета, а в **туннельном режиме** исходный пакет помещается в новый IP-пакет, и передача данных по сети выполняется на основании заголовка нового IP-пакета.

Применение того или иного режима зависит от требований, предъявляемых к защите данных, а также от роли, которую играет в сети узел, завершающий защищенный канал. Так, узел может быть хостом (конечным узлом) или шлюзом (промежуточным узлом). Соответственно, имеются три схемы применения протокола IPSec:

- хост-хост;
- шлюз-шлюз;
- хост-шлюз.

В **схеме хост-хост** защищенный канал, или, что в данном контексте одно и то же, безопасная ассоциация, устанавливается между двумя конечными узлами сети (рис. 4). Тогда протокол IPSec работает на конечных узлах и защищает данные, передаваемые от хоста 1 к хосту 2. Для схемы хост-хост чаще всего используется транспортный режим защиты.

В соответствии со **схемой шлюз-шлюз** защищенный канал устанавливается между двумя промежуточными узлами, так называемыми **шлюзами безопасности** (Security Gateway, SG), на каждом из которых работает протокол IPSec (рис. 6).

Транспортный и туннельный режимы

Защищенный обмен данными может происходить между любыми двумя конечными узлами, подключенными к сетям, которые расположены позади шлюзов безопасности. От конечных узлов поддержка протокола IPSec не требуется, они передают свой трафик в незащищенном виде через заслуживающие доверие внутренние сети предприятий. Трафик, направляемый в общедоступную сеть, проходит через шлюз безопасности, который и обеспечивает его защиту с помощью протокола IPSec. Шлюзам доступен только туннельный режим работы.

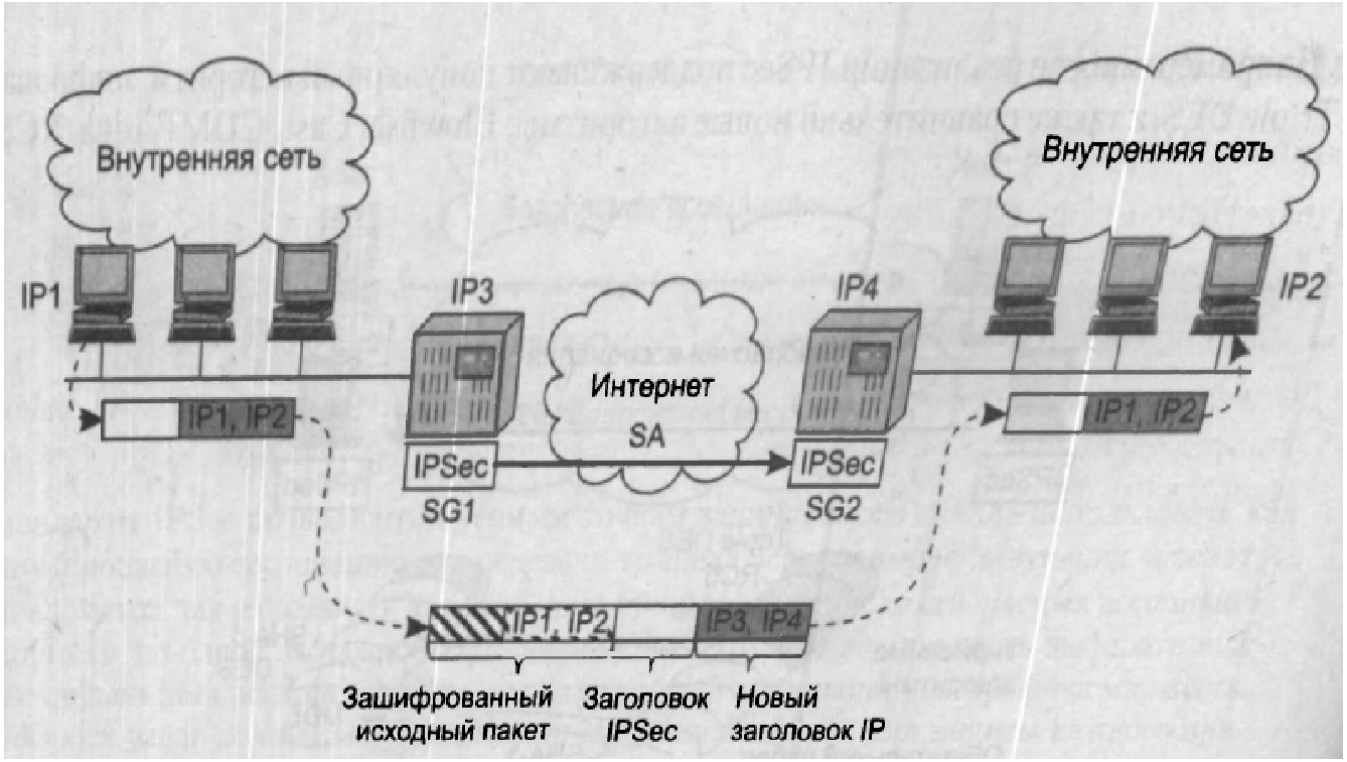


Рис. 6. Работа защищенного канала по схеме шлюз-шлюз в туннельном режиме

Транспортный и туннельный режимы

На рис. 6 пользователь компьютера с адресом IP1 посылает пакет по адресу IP2, используя туннельный режим протокола IPSec. Шлюз SG1 зашифровывает пакет целиком, вместе с заголовком, и снабжает его новым заголовком IP, в котором в качестве адреса отправителя указывает свой адрес — IP3, а в качестве адреса получателя — адрес IP4 шлюза SG2. Вся передача данных по составной IP-сети выполняется на основании заголовка внешнего пакета, а внутренний пакет становится при этом полем данных для внешнего пакета. На шлюзе SG2 протокол IPSec извлекает инкапсулированный пакет и расшифровывает его, приводя к исходному виду.

Схема хост-шлюз часто применяется при удаленном доступе. В этом случае защищенный канал прокладывается между удаленным хостом, на котором работает протокол IPSec, и шлюзом, защищающим трафик для всех хостов, входящих во внутреннюю сеть предприятия. Эту схему можно усложнить, создав параллельно еще один защищенный канал — между удаленным хостом и каким-либо хостом, принадлежащим внутренней сети, защищаемой шлюзом (рис. 7). Такое комбинированное использование двух безопасных ассоциаций позволяет надежно защитить трафик и во внутренней сети.

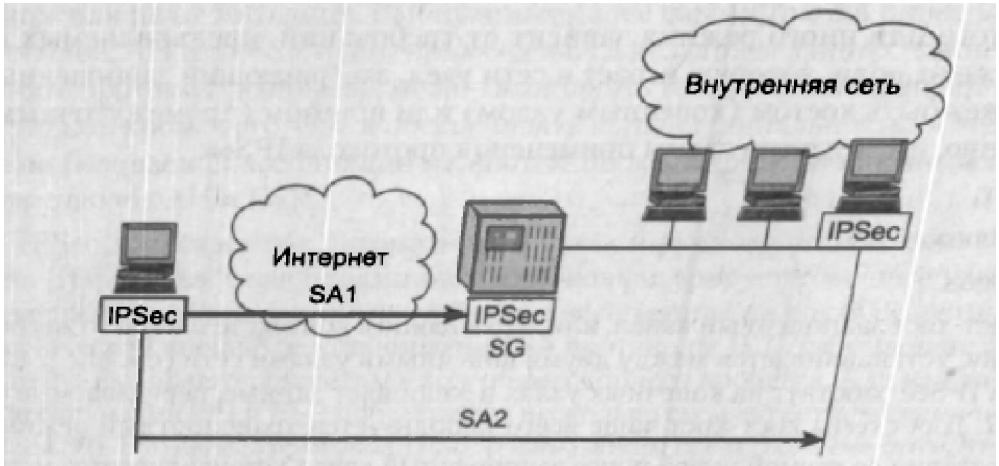


Рис 7. Схема защищенного канала хост-шлюз

Протокол AH

Протокол AH позволяет приемной стороне убедиться, что:

- пакет был отправлен стороной, с которой установлена безопасная ассоциация;
- содержимое пакета не было искажено в процессе его передачи по сети;
- пакет не является дубликатом уже полученного пакета.

Две первые функции обязательны для протокола AH, а последняя выбирается при установлении ассоциации по желанию. Для выполнения этих функций протокол AH использует специальный заголовок (рис. 8).

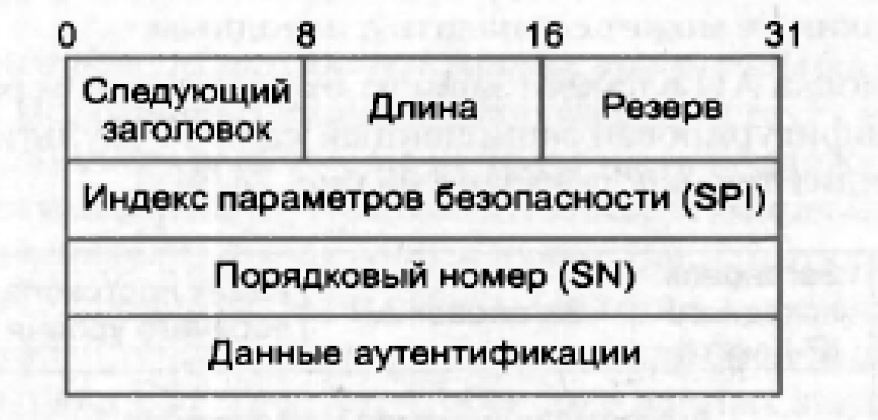


Рис. 8. Структура заголовка протокола AH

В поле *следующего заголовка* (next header) указывается код протокола более высокого уровня, то есть протокола, сообщение которого размещено в поле данных IP-пакета. Скорее всего, им будет один из протоколов транспортного уровня (TCP или UDP) или протокол ICMP, но может встретиться и протокол ESP, если он используется в комбинации с AH.

Протокол AH

В поле *длины полезной нагрузки* (payload length) содержится длина заголовка AH.

Индекс параметров безопасности (Security Parameters Index, SPI) служит для связи пакета с предусмотренной для него безопасной ассоциацией. Немного позже мы обсудим его более подробно.

Поле *порядкового номера* (Sequence Number, SN) указывает на порядковый номер пакета и применяется для защиты от его ложного воспроизведения (когда третья сторона пытается повторно использовать перехваченные защищенные пакеты, отправленные реально аутен-тифицированным отправителем). Отправляющая сторона последовательно увеличивает значение этого поля в каждом новом пакете, передаваемом в рамках данной ассоциации, так что приход дубликата обнаружится принимающей стороной (если, конечно, в рамках ассоциации будет активирована функция защиты от ложного воспроизведения). Однако в любом случае в функции протокола AH не входит восстановление утерянных и упорядочивание прибывающих пакетов — он просто отбрасывает пакет, когда обнаруживает, что аналогичный пакет уже получен. Чтобы сократить требуемую для работы протокола буферную память, используется механизм скользящего окна — на предмет дублирования проверяются только те пакеты, чей номер находится в пределах окна. Окно обычно выбирается размером в 32 или 64 пакета.

Протокол AH

Поле *данных аутентификации* (authentication data), которое содержит так называемое **значение проверки целостности** (Integrity Check Value, ICV), служит для аутентификации и проверки целостности пакета. Это значение является дайджестом, вычисляемым с помощью одной из двух обязательно поддерживаемых протоколом AH односторонних функций шифрования MD5 или SAH-1, но может использоваться и любая другая функция, о которой стороны договорились в ходе установления ассоциации. При вычислении дайджеста пакета в качестве параметра ОФШ выступает симметричный секретный ключ, который был задан для данной ассоциации вручную или автоматически с помощью протокола IKE. Так как длина дайджеста зависит от выбранной ОФШ, это поле имеет в общем случае переменный размер.

Протокол AH старается охватить при вычислении дайджеста как можно большее число полей исходного IP-пакета, но некоторые из них в процессе передачи пакета по сети меняются непредсказуемым образом, поэтому не могут быть включены в аутентифицируемую часть пакета. Например, целостность значения поля времени жизни (TTL) в приемной точке канала оценить нельзя, так как оно уменьшается на единицу каждым промежуточным маршрутизатором и никак не может совпадать с исходным.

Протокол AH

Местоположение заголовка AH в пакете зависит от того, в каком режиме — транспортном или туннельном — сконфигурирован защищенный канал. Результирующий пакет в транспортном режиме выглядит так, как показано на рис. 9.

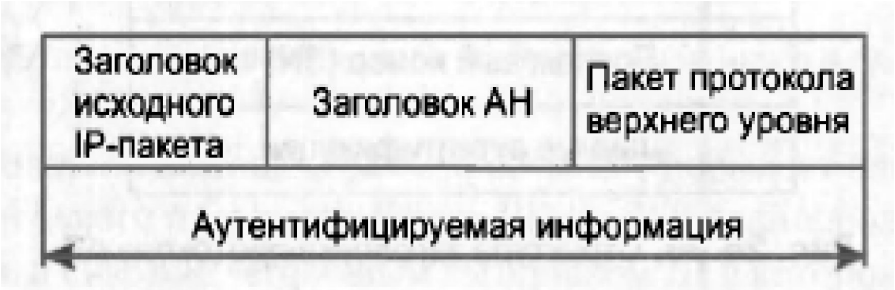


Рис. 9. Структура IP-пакета, обработанного протоколом AH в транспортном режиме

При использовании туннельного режима, когда шлюз IPSec принимает проходящий через него транзитом исходящий пакет и создает для него внешний IP-пакет, протокол AH защищает все поля исходного пакета, а также неизменяемые поля нового заголовка внешнего пакета (рис. 10).

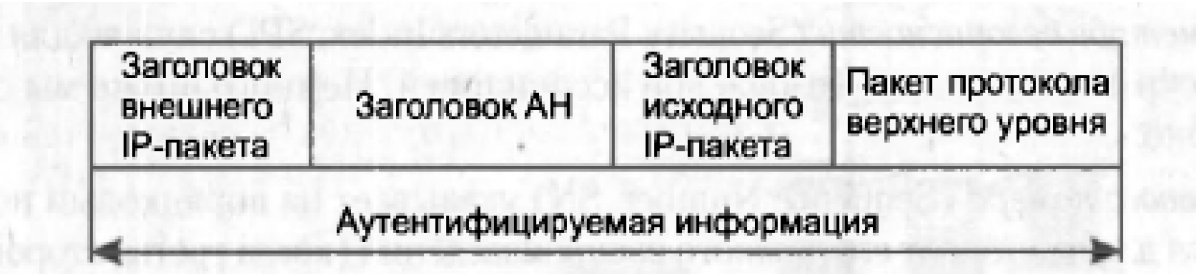


Рис. 10. Структура IP-пакета, обработанного протоколом AH в туннельном режиме

Протокол ESP

Протокол ESP решает две группы задач. К первой относятся задачи обеспечения аутентификации и целостности данных на основе дайджеста, аналогичные задачам протокола AH, ко второй — защита передаваемых данных путем их шифрования от несанкционированного просмотра.

Как видно на рис. 11, заголовок ESP делится на две части, разделяемые полем данных. Первая часть, называемая собственно заголовком ESP, образуется двумя полями (SPI и SN), назначение которых аналогично одноименным полям протокола AH, и размещается перед полем данных. Остальные служебные поля протокола ESP, называемые концевиком ESP, расположены в конце пакета.

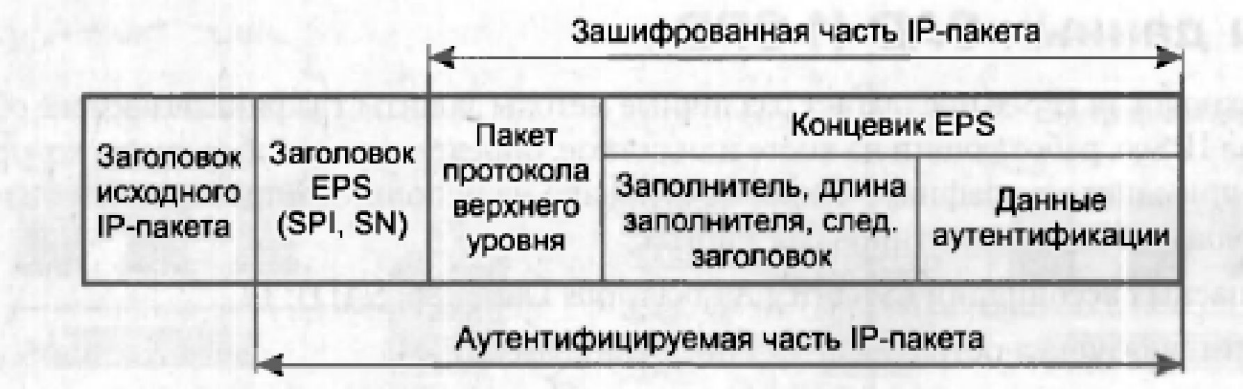


Рис. 11. Структура IP-пакета, обработанного протоколом ESP в транспортном режиме

Протокол ESP

Два поля концевика — *следующего заголовка и данных аутентификации* — также аналогичны полям заголовка AH. Поле данных аутентификации отсутствует, если при установлении безопасной ассоциации принято решение не использовать возможностей протокола ESP, касающихся обеспечения целостности. Помимо этих полей концевик содержит два дополнительных поля — *заполнителя и длины заполнителя*. 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, чтобы скрыть действительный размер пакета в целях обеспечения так называемой частичной конфиденциальности трафика. Правда, возможность маскировки ограничивается сравнительно небольшим объемом заполнителя — 255 байт, поскольку большой объем избыточных данных может снизить полезную пропускную способность канала связи.

Протокол ESP

На рис. 12 показано размещение полей заголовка ESP в транспортном режиме. 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 попадают также поля SPI и SN, которые должны передаваться в открытом виде для того, чтобы прибывший пакет можно было отнести к определенной ассоциации и предотвратить ложное воспроизведение пакета.

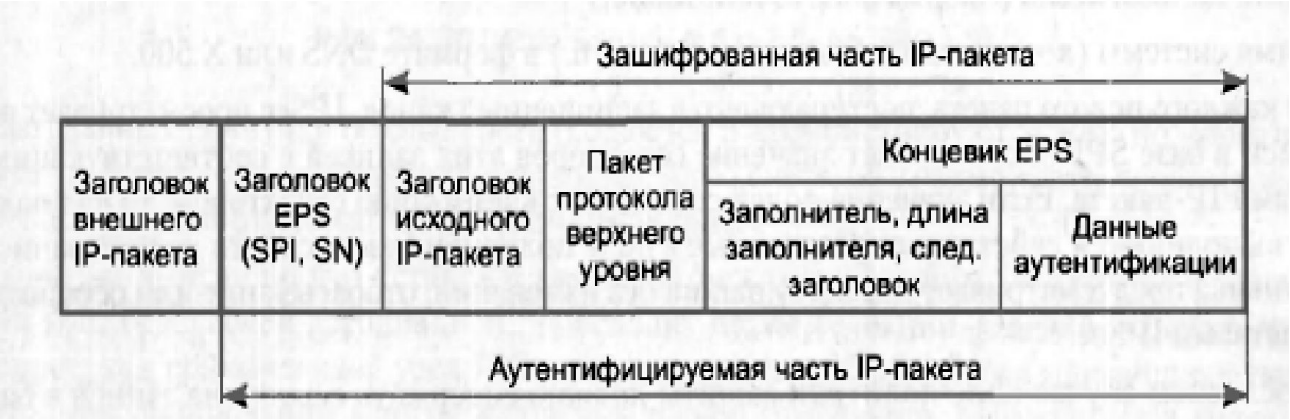


Рис. 12. Структура IP-пакета, обработанного протоколом ESP в туннельном режиме

В туннельном режиме заголовок исходного IP-пакета помещается после заголовка ESP и полностью попадает в число защищаемых полей, а заголовок внешнего IP-пакета протоколом ESP не защищается (рис. 12).

Базы данных SAD и SPD

Итак, технология IPSec предлагает различные методы защиты трафика. Каким же образом протокол IPSec, работающий на хосте или шлюзе, определяет способ защиты, который он должен применить к трафику. Решение основано на использовании в каждом узле, поддерживающем IPSec, двух типов баз данных:

- безопасных ассоциаций (Security Associations Database, SAD);
- политики безопасности (Security Policy Database, SPD).

При установлении безопасной ассоциации, как и при любом другом логическом соединении, две стороны принимают ряд соглашений, регламентирующих процесс передачи потока данных между ними. Соглашения фиксируются в виде набора параметров. Для безопасной ассоциации 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, другую для входящих.

Другой тип базы данных — база данных политики безопасности (SPD) — определяет соответствие между IP-пакетами и установленными для них правилами обработки. Записи SPD состоят из полей двух типов — *полей селектора пакета и полей политики защиты* для пакета с данным значением селектора (рис. 13).

Базы данных SAD и SPD

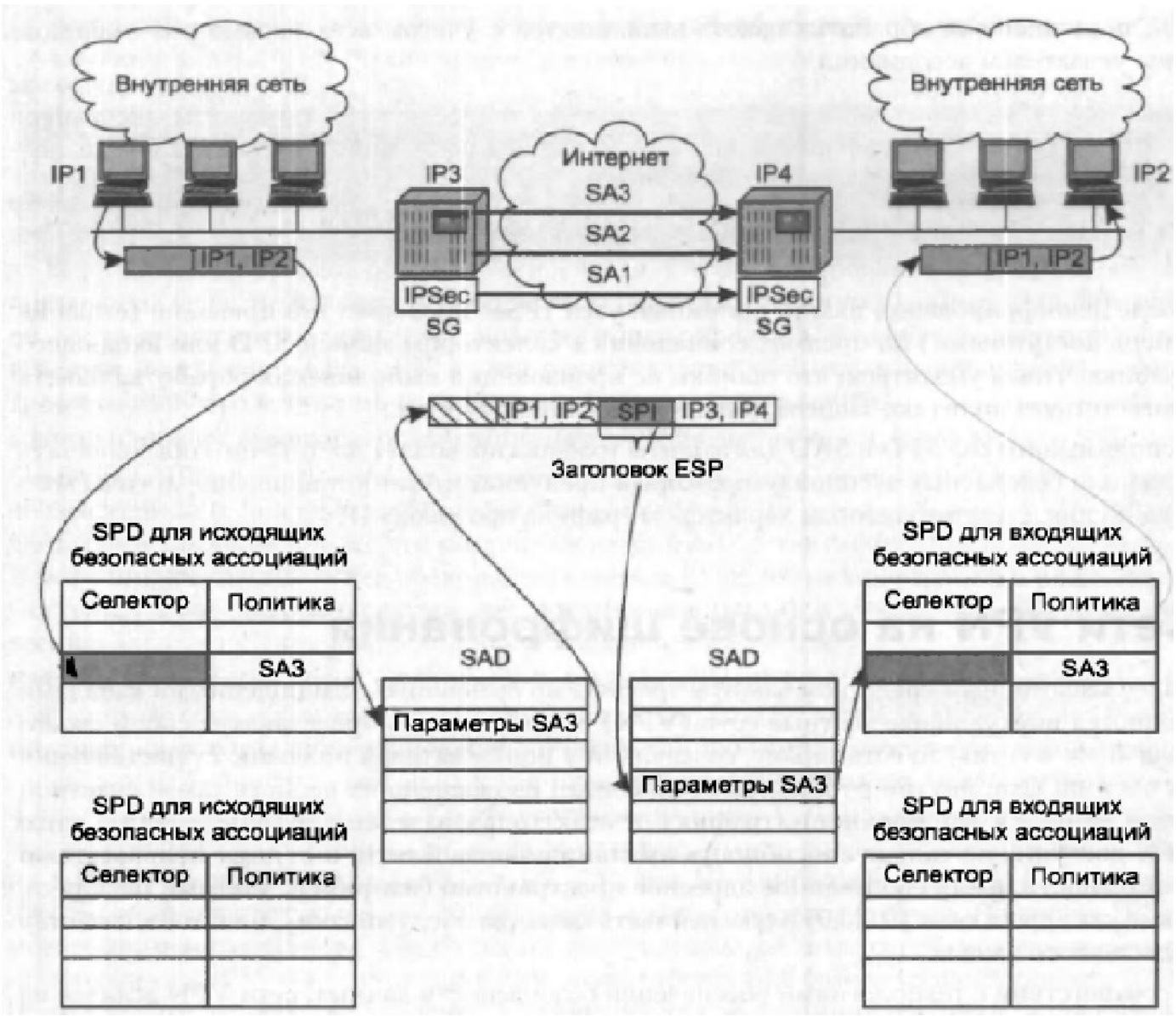


Рис. 13. Использование баз данных SPD и SAD

Базы данных SAD и SPD

Селектор в SPD включает следующий набор признаков, на основании которых можно с большой степенью детализации выделить защищаемый поток:

- IP-адреса источника и приемника могут быть представлены как в виде отдельных адресов (индивидуальных, групповых или широковещательных), так и диапазонами адресов, заданными с помощью верхней и нижней границ либо с помощью маски;
- порты источника и приемника (то есть TCP- или UDP-порты);
- тип протокола транспортного уровня (TCP, UDP);
- имя пользователя в формате DNS или X.500;
- имя системы (хоста, шлюза безопасности и т. п.) в формате DNS или X.500.

Для каждого нового пакета, поступающего в защищенный канал, IPSec просматривает все записи в базе SPD и сравнивает значение селекторов этих записей с соответствующими полями IP-пакета. Если значение полей совпадает с каким-либо селектором, то над пакетом выполняются действия, определенные в поле политики безопасности данной записи. Политика предусматривает передачу пакета без изменения, отбрасывание или обработку средствами IPSec.

В последнем случае поле политики защиты должно содержать ссылку на запись в базе данных SAD, в которую помещен набор параметров безопасной ассоциации для данного пакета (на рис. 13 для исходящего пакета определена ассоциация SA3). На основании заданных параметров безопасной ассоциации к пакету применяется соответствующие протокол (на рисунке — ESP), функции шифрования и секретные ключи.

Базы данных SAD и SPD

Если к исходящему пакету нужно применить некоторую политику защиты, но указатель записи SPD показывает, что в настоящее время нет активной безопасной ассоциации с требуемой политикой, то IPSec создает новую ассоциацию с помощью протокола IKE, помещая новые записи в базы данных SAD и SPD.

Базы данных политики безопасности создаются и администрируются либо пользователем (этот вариант больше подходит для хоста), либо системным администратором (вариант для шлюза), либо автоматически (приложением).

Ранее мы выяснили, что установление связи между исходящим IP-пакетом и заданной для него безопасной ассоциацией происходит путем селекции. Однако остается другой вопрос: как *принимающий узел* IPSec определяет способ обработки прибывшего пакета, ведь при шифровании многие ключевые параметры пакета, отраженные в селекторе, оказываются недоступными, а значит, невозможно определить соответствующую запись в базах данных SAD и SPJD и, следовательно, тип процедуры, которую надо применить к поступившему пакету? Именно для решения этой проблемы в заголовках AH и ESP предусмотрено поле SPI. В это поле помещается указатель на ту строку базы данных SAD, в которой записаны параметры соответствующей безопасной ассоциации. Поле SPI заполняется протоколом AH или ESP во время обработки пакета в отправной точке защищенного канала. Когда пакет приходит в конечный узел защищенного канала, из его внешнего заголовка ESP или AH (на рисунке — из заголовка ESP) извлекается значение SPI, и дальнейшая обработка пакета выполняется с учетом всех параметров заданной этим указателем ассоциации.

Базы данных SAD и SPD

Таким образом, для распознавания пакетов, относящихся к разным безопасным ассоциациям, используются:

- на узле-отправителе — селектор;
- на узле-получателе — индекс параметров безопасности (SPI).

После дешифрирования пакета приемный узел IPSec проверяет его признаки (ставшие теперь доступными) на предмет совпадения с селектором записи SPD для входящего трафика, чтобы убедиться, что ошибки не произошло и выполняемая обработка пакета соответствует политике защиты, заданной администратором.

Использование баз SPD и SAD для защиты трафика позволяет достаточно гибко сочетать механизм безопасных ассоциаций, который предусматривает установление логического соединения, с дейтаграммным характером трафика протокола IP.

Сети VPN на основе шифрования

Более масштабным средством защиты трафика по сравнению с защищенными каналами являются виртуальные частные сети (VPN). Подобная сеть представляет собой своего рода «сеть в сети», то есть сервис, создающий у пользователей иллюзию существования их частной сети внутри публичной сети. Одним из важнейших свойств такой «частной сети» является защищенность трафика от атак пользователей публичной сети. Сетям VPN доступна не только способность имитации частной сети; они дают пользователю возможность иметь собственное адресное пространство (например, частные IP-адреса, такие как адреса сети 10.0.0.0) и обеспечивать качество обслуживания, близкое к качеству выделенного канала.

В соответствии с технологиями обеспечения безопасности данных, сети VPN делятся на два класса:

- сети VPN на основе разграничения трафика изучаются в разделе «Виртуальные частные сети»;
- сети VPN на основе шифрования работают на основе рассмотренной ранее техники защищенных каналов.

Виртуальная частная сеть на основе шифрования *может быть определена как совокупность защищенных каналов, созданных предприятием в открытой публичной сети для объединения своих филиалов*.

То есть в VPN техника защищенных каналов применяется уже в других масштабах, связывая не двух пользователей, а произвольное количество клиентских сетей.

Сети VPN на основе шифрования

Технологии VPN на основе шифрования включают шифрование, аутентификацию и туннелирование.

- Шифрование гарантирует конфиденциальность корпоративных данных при передаче через открытую сеть.
- Аутентификация отвечает за то, чтобы взаимодействующие системы (пользователи) на обоих концах VPN были уверены в идентичности друг друга.
- Туннелирование предоставляет возможность передавать зашифрованные пакеты по открытой публичной сети.

Для повышения уровня защищенности виртуальных частных сетей технологии VPN на основе шифрования можно применять совместно с технологиями VPN на основе разграничения трафика. Технологии VPN на основе разделения трафика иногда критикуют за недостаточный уровень безопасности, считая, что без шифрования трафика персонал поставщика услуг может получить несанкционированный доступ к данным. Действительно, такая вероятность существует, поэтому клиент услуг VPN на основе разграничения трафика, например MPLS VPN, может самостоятельно повысить защищенность своего трафика, прибегнув, скажем, к шифрованию передаваемых данных.

Сейчас наиболее широко используются сети VPN на основе протоколов IPSec и SSL. Стандарты IPSec обеспечивают высокую степень гибкости, позволяя выбрать нужный режим защиты (с шифрованием или только с обеспечением аутентичности и целостности данных), а также использовать различные алгоритмы аутентификации и шифрования. Режим инкапсуляции IPSec позволяет изолировать адресные пространства получателя (клиента) и поставщика услуг за счет применения двух IP-адресов — внешнего и внутреннего.

Сети VPN на основе шифрования

Сети VPN на основе IPsec, как правило, строятся по типу CPVPN, то есть как виртуальные частные сети, в которых клиент самостоятельно создает туннели IPSec через IP-сеть поставщика услуг. Причем от последнего требуется только предоставление стандартного сервиса по объединению сетей, а значит, предприятию доступны как услуги сети поставщика, так и услуги Интернета. Конфигурирование сетей VPN на основе IPSec довольно трудоемко, поскольку туннели IPSec двухточечные, то есть при полносвязной топологии их количество пропорционально N x (M - 1), где N — число соединений. Необходимо учесть еще и непростую задачу поддержания инфраструктуры ключей. Протокол IPSec может применяться также для создания виртуальных частных сетей, поддерживаемых провайдером (PPVPN) — туннели в них также строятся на базе устройств клиента (CE-based), но эти устройства удаленно конфигурируются и администрируются поставщиком услуг.

Пропускная способность каналов и другие параметры QoS этой технологией не поддерживаются, но если оператор предоставляет определенные параметры QoS (например, за счет дифференцированного обслуживания), их можно использовать при создании туннеля IPSec.

Сети VPN на основе шифрования

В самое последнее время выросла популярность VPN на основе протокола SSL. Напомним, что этот протокол работает на уровне представления, непосредственно под уровнем приложений, так что приложения должны явным способом его вызывать, чтобы создать защищенный канал для своего трафика. Наиболее популярным приложением, использующим защищенные каналы SSL, является веб-браузер. В этом случае защищенные каналы SSL задействует протокол HTTP, и в этом режиме работы его часто называют протоколом HTTPS. Пользователи Интернета хорошо знают этот режим, так как браузер прибегает к нему во всех случаях, когда необходимо обеспечить конфиденциальность передаваемой информации: при покупках в интернет-магазинах, при интернет-банкинге и т. п. Служба VPN на основе SSL функционирует на основе веб-портала, развернутого в локальной сети организации. Пользователи такой защищенной службы VPN получают удаленный доступ к ресурсам этой локальной сети, обращаясь к веб-порталу посредством обычного браузера через порт 443 (TCP-порт протокола HTTPS). Отсутствие специального клиентского программного обеспечения, требующего настройки, является значительным преимуществом VPN на основе SSL.

Дополнительные материалы

Технология IPsec

IPsec представляет собой набор протоколов для обеспечения безопасности сетевого соединения. Протоколы IPsec разработаны IETF (Internet Engineering Task Force). Под безопасностью здесь подразумевается: контроль доступа, обеспечение сохранности данных, идентификация отправителя, защита от атак воспроизведения и секретность обмена. Первые документы, регламентирующие IPsec, были приняты в 1998-99 годах (RFC-2401-02, -2406, -2408 и -2709). Существуют версии IPsec для *IPv4* и *IPv6*. Важной особенностью этой технологии является то, что пользователь может даже не знать, что он пользуется IPsec и, как правило, нет необходимости адаптировать для работы с IPsec уже существующие приложения. И, тем не менее, дебаты и обсуждения области и способов применения этой технологии продолжаются. Связано это с тем, что если, например комбинация WEB-сервера/клиента поддерживает эту функцию, разработчик должен гарантировать, что данная услуга будет доступна на всех платформах, где данное приложение может работать.

В IPsec используются две базы данных: **SPD** (Security Policy Database, куда записываются правила обеспечения безопасности) и **SADB** (Security Association Database, где хранятся данные об активных ассоциациях безопасности).

Система IPsec предлагает многовариантный механизм реализации безопасности для обоих концов соединения. Эта техника пригодна для отдельного пользователя, особенно если он работает на выезде, и для виртуальных субсетей организаций, работающих с данными, которые требуют секретности.

При использовании совместно с Firewall IPsec предоставляет высокий уровень безопасности. При этом нужно иметь в виду, что для реализации IPsec оба партнера должны иметь оборудование и/или программы, которые поддерживают эти протоколы.

IPsec предусматривает процедуры аутентификации и шифрования. Формирование и удаления заголовка IPsec может осуществляться в машине клиента или в сетевом шлюзе (маршрутизаторе).

Протокол IPsec предоставляет три вида услуг: аутентификацию (**AH**), шифрование (**ESP**) и безопасную пересылку ключей. Обычно желательны обе первые услуги, так как неавторизованный клиент не сможет проникнуть в **VPN** (Virtual Private Network - виртуальная частная сеть), а шифрование не позволит злоумышленникам прочитать, исказить или подменить сообщения. По этой причине протокол ESP предпочтительнее, так как он позволяет совместить обе эти услуги. Схема транспортировки данных в рамках IPsec показана на рис. 14. Это типичный пример IPsec-туннеля.

Из рисунка видно, что IPsec-заголовки и шифрование данных присутствуют до тех пор, пока пакет транспортируется через среду, где не гарантирована безопасность.

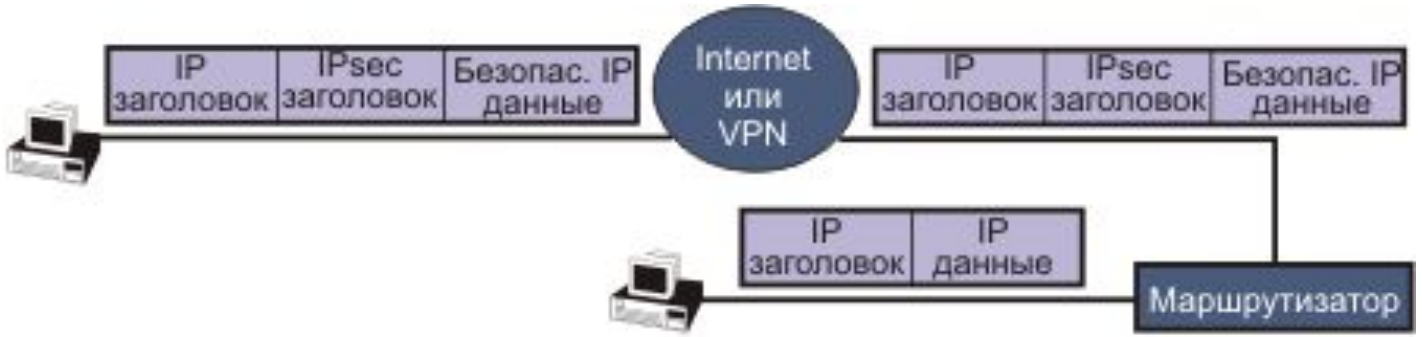


Рис. 14. Общая схема преобразования данных в IPsec

Дополнительные материалы
Режим туннеля и транспортный режим

Заголовок аутентификации (AH) и Encapsulating Security Payload (ESP) являются двумя протоколами нижнего уровня, используемыми IPsec, именно они осуществляют аутентификацию и шифрование+аутентификацию данных, передаваемых через соединение. Эти механизмы обычно используются независимо, хотя возможно (но не типично) их совместное применение.

Транспортный режим обеспечивает безопасное соединение двух терминалов путем инкапсуляции содержимого IP-данных, в то время как туннельный режим инкапсулирует весь IP-пакет на участке между шлюзами. Последний вариант используется для формирования традиционной VPN, где туннель создает безопасный путь через полный опасностей Интернет.

Установление IPsec-соединения подразумевает любые варианты крипто-алгоритмов, но ситуация существенно упрощается благодаря тому, что обычно допустимо использование двух, максимум трех вариантов.

На фазе аутентификации вычисляется контрольная сумма **ICV** (Integrity Check Value) пакета с привлечением алгоритмов MD5 или SHA-1. При этом предполагается, что оба партнера знают секретный ключ, который позволяет получателю вычислить ICV и сравнить с результатом, присланным отправителем. Если сравнение ICV прошло успешно, считается, что отправитель пакета аутентифицирован. Протокол AH всегда осуществляет аутентификацию, а ESP выполняет ее опционно.

Дополнительные материалы

Режим туннеля и транспортный режим

Шифрование использует секретный ключ для кодирования данных перед их транспортировкой, что исключает доступ к содержимому со стороны злоумышленников. В системе IPsec могут использоваться следующие алгоритмы: DES, 3DES, Blowfish, CAST, IDEA, RC5 и AES. Но, в принципе, разрешены и другие алгоритмы. Так как обе стороны диалога должны знать секретный ключ, используемый при хэшировании или шифровании, существует проблема транспортировки этих ключей. Возможен ввод ключей вручную, когда эти коды вводятся при конфигурации системы с помощью клавиатуры обоими партнерами. При этом предполагается, что доставка этих кодов осуществлена каким-то достаточно безопасным методом, алгоритм же **IKE** (Internet Key Exchange – обмен ключами по Интернет) является безопасным механизмом пересылки ключей в реальном масштабе времени, например, через Интернет.

Дополнительные материалы
Основной и агрессивный режимы

Эти режимы служат для управления балансом эффективности и безопасности при исходном обмене ключами IKE. "Основной режим" требует шести пакетов в обоих направлениях, но обеспечивает полную безопасность при установлении соединения IPsec. В агрессивном режиме используется вдвое меньше обменов, но безопасность в этом случае ниже, так как часть информации передается открытым текстом.

Пакеты IPsec транспортируются IP-дейтограммами. Заголовки IPsec (AH и ESP) размещаются сразу после IP-заголовка (описание формата IP-дейтограмм смотри в http://book.itep.ru/4/44/ip_441.htm). Тип вложенного пакета в IP идентифицируется содержимым поля протокол.

Некоторые коды поля протокол в IP-дейтограммах представлены в таблице ниже.

Код протокола	Назначение
6	Протокол TCP (Transmission Control Protocol)
17	Протокол UDP (User Datagram Protocol)
41	Протокол IPv6
50	IPsec: Протокол ESP (Инкапсулированное поле данных безопасности)
51	IPsec: Протокол AH (Заголовок аутентификации)

Эти коды поля протокол определены **IANA** (Internet Assigned Numbers Authority). Далее будут более подробно рассмотрены два последних протокола (AH и ESP).

Протокол АН

Протокол АН используется для аутентификации, но не для шифрования IP трафика, и служит для подтверждения того, что мы связаны именно с тем, с кем предполагаем, что полученные данные не искажены и не подменены при транспортировке.

Аутентификация выполняется путем вычисления зашифрованного аутентификационного хэш-кода сообщения. Хэширование охватывает практически все поля IP пакета (исключая только те, которые могут модифицироваться при транспортировке, например, TTL или контрольная сумма заголовка). Этот код записывается в АН заголовке и пересылается получателю. Формат АН заголовка представлен на рис. 15.

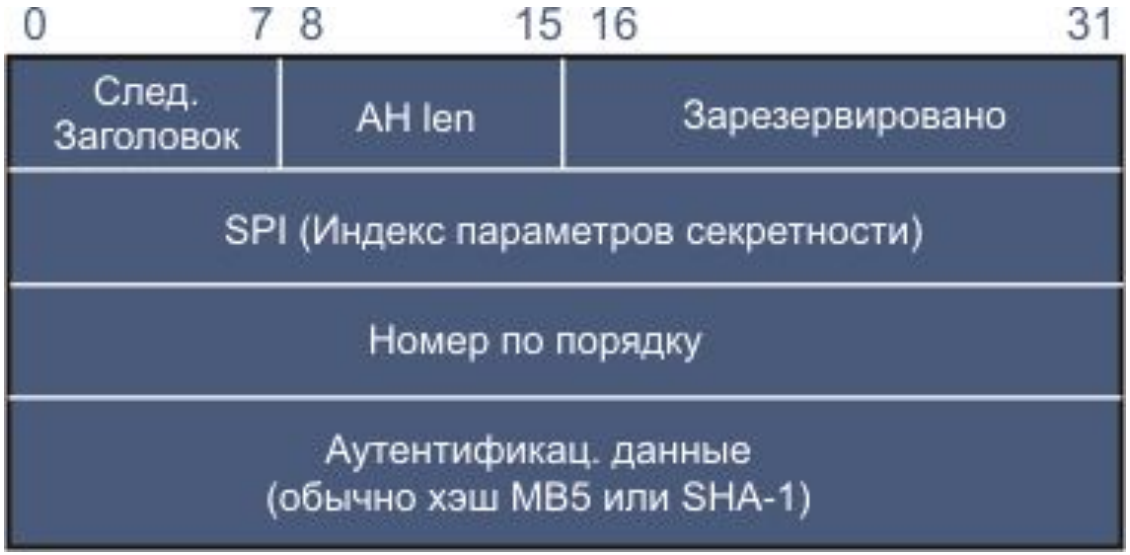


Рис. 15. Формат заголовка протокола АН

Этот АН заголовок содержит пять важных полей.

Дополнительные материалы
Протокол AH

1. ***Следующий заголовок***. Идентифицирует тип протокола, используемого для следующего поля данных. Фактически это тип пакета, инкапсулированного в AH.
2. ***AH len***. Определяет длину заголовка пакета, измеренную в 32-битовых словах, за вычетом двух слов (это диктуется RFC 1883 для IPv6).
3. ***Зарезервировано***. Поле зарезервировано и должно содержать нули.
4. ***Индекс параметров безопасности (SPI)***. 32-битовый идентификатор, который помогает получателю выбрать, к какому из входных обменов относится этот пакет. Каждый обмен, защищенный AH, использует хэш-алгоритм (MD5, SHA-1 и т.д..), какие-то секретные и возможно некоторые иные данные. SPI может рассматриваться как индекс таблицы наборов таких параметров, чтобы облегчить выбор нужного набора.
5. ***Номер по порядку***. Монотонно увеличивающийся идентификатор, который позволяет установить соответствие между посланным пакетом и откликом подтверждения его получения. Этот код включается в аутентификационные данные - позволяет детектировать любые модификации и атаки воспроизведения.
6. ***Аутентификационные данные***. Это контрольная сумма **ICV** (Integrity Check Value), вычисленная для всего пакета, включая большинство полей заголовка (см. рис. 16). Получатель повторно вычисляет тот же хэш. Если значения кодов не совпадут, пакет был поврежден в пути или не соответствует секретному ключу. Такие пакеты отбрасываются. ICV часто называется также **MAC** (Message Authentication Code). Для вычисления MAC используются следующие поля:

- Поля IP-заголовка, которые не меняются при транспортировке.
- Заголовок AH, кроме поля данных *аутентификации.*
- Поле данных протокола ВУ, которые остаются неизменными при транспортировке.

Дополнительные материалы
Транспортный режим

Транспортный режим используется для защиты виртуальных соединений точка-точка. Эта защита осуществляется с использованием аутентификации, шифрования или обоих методов.

При транспортном режиме AH IP-пакет модифицируется лишь слегка путем включения AH заголовка между IP заголовком и полем данных (TCP, UDP и т.д.) и перестановки кодов протокола.

Перестановка кодов протокола необходима для восстановления исходного вида IP пакетов конечным получателем: после выполнения проверки получателем корректности IPsec заголовка, этот заголовок удаляется, а в поле код протокола IP заносится прежнее значение (TCP, UDP и т.д.).

Когда к адресату приходит пакет, успешно прошедший процедуру аутентификации, заголовок AH удаляется, а содержимое поля протокол (=AH) в IP заголовке заменяется запомненным значением поля следующий заголовок. Таким образом, восстанавливается первоначальный вид IP дейтограммы, и пакет может быть передан ожидающему процессу.

Дополнительные материалы
Транспортный режим

На рис. 16 показано преобразование форматов заголовков в транспортном режиме IPsec. Слева на рисунке размешен формат исходной дейтограммы с инкапсулированным TCP-сегментом. Закрашенные области защищены аутентификационными данными AH. Поля TOS, TTL, флаги, указатель (фрагмента) и контрольная сумма заголовка не защищаются, так как их содержимое может изменяться в процессе транспортировки, а промежуточные узлы не владеют необходимыми ключами для дешифрования и повторного шифрования. Поля, не охватываемые защитой хэша, перед вычислением ICV заполняются нулями.

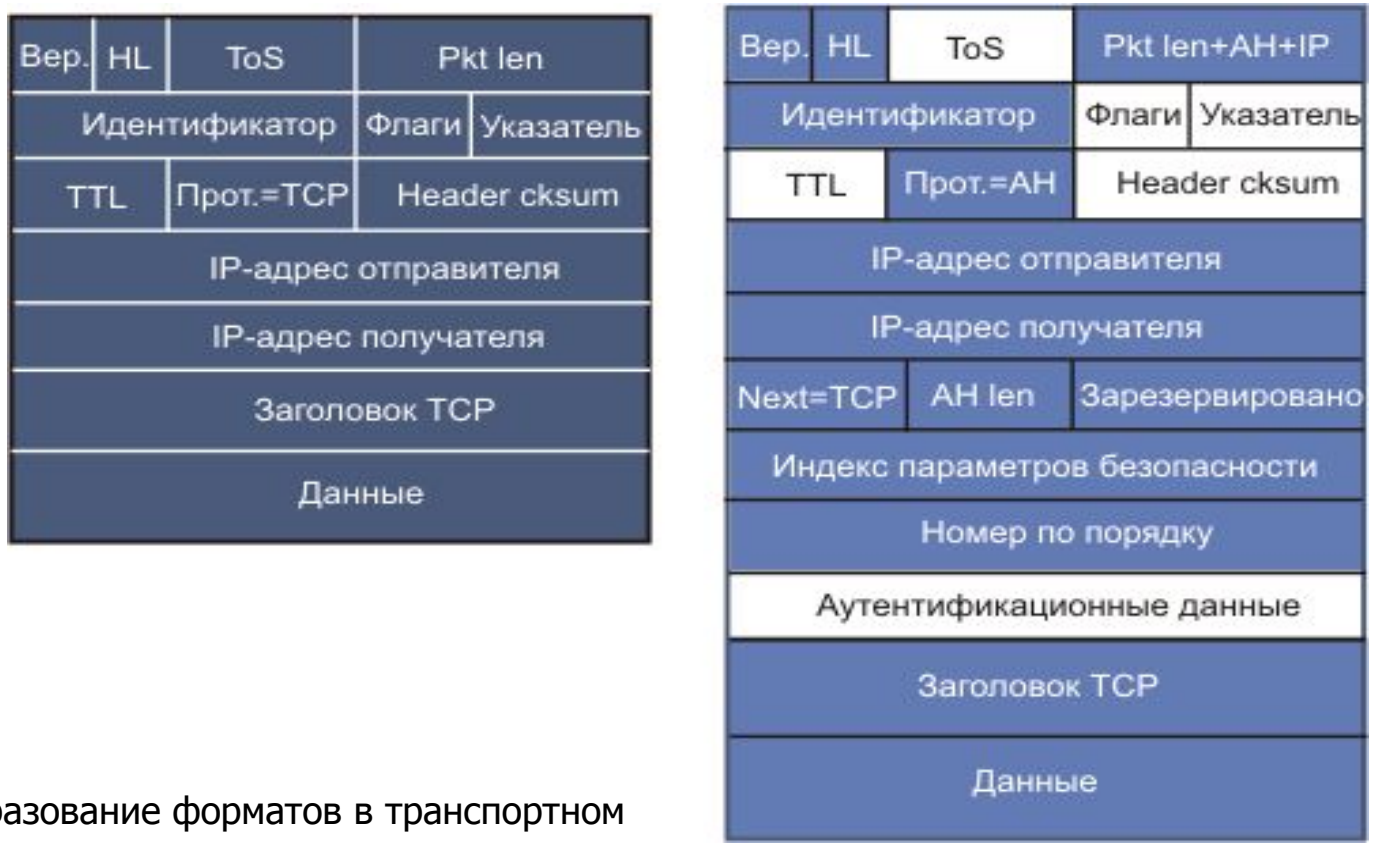


Рис. 16. Преобразование форматов в транспортном режиме AH IPsec

Дополнительные материалы
Туннельный режим

Режим туннеля реализует функциональность VPN, где IP пакет целиком инкапсулируются в другой пакет и в таком виде доставляются адресату.

Также как и в транспортном режиме, пакет защищается контрольной суммой ICV, чтобы аутентифицировать отправителя и предотвратить модификацию пакета при транспортировке. Но в отличие от транспортного режима, здесь инкапсулируется весь IP пакет, а это позволяет адресам отправителя и получателя отличаться от адресов, содержащихся в пакете, что позволяет формировать туннель.

На рис. 17 показано преобразование форматов заголовков в туннельном режиме IPsec. Слева на рисунке размешен формат исходной дейтограммы с инкапсулированным TCP-сегментом. Закрашенные области защищены аутентификационными данными AH.

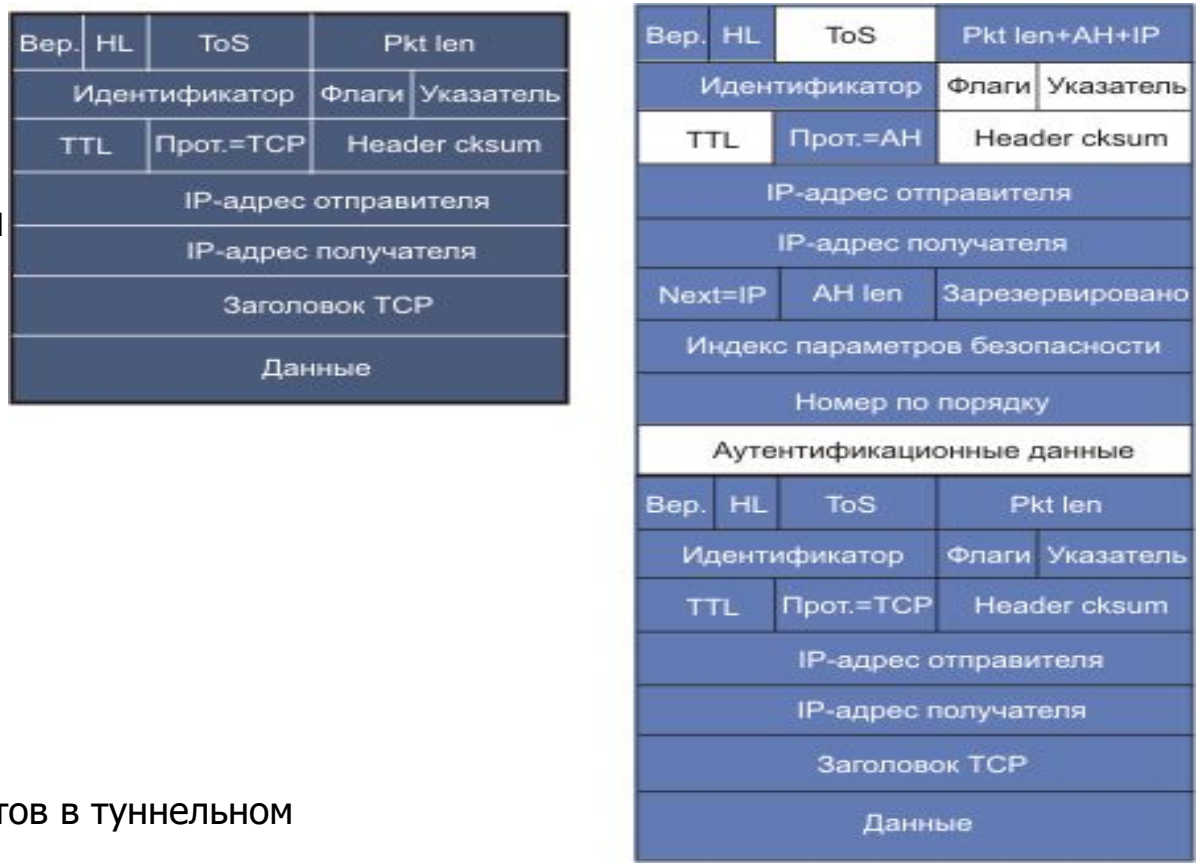


Рис. 17. Преобразование форматов в туннельном режиме AH IPsec

Дополнительные материалы
Туннельный режим

Когда пакет туннельного режима приходит адресату, он проходит ту же аутентификационную проверку, что и пакет AH-типа, после чего удаляются заголовки IP и AH и восстанавливается первоначальный формат пакета.

Большинство реализаций рассматривает оконечную точку туннеля в качестве сетевого интерфейса.

Реконструированный пакет может быть доставлен локальной машине или маршрутизован куда-либо еще (согласно IP-адресу места назначения в инкапсулированном пакете). Дальнейшая его транспортировка уже не обеспечивается средствами безопасности IPsec.

В то время как транспортный режим используется исключительно для обеспечения безопасной связи между двумя компьютерами, туннельный режим обычно применяется между шлюзами (маршрутизаторами, сетевыми экранами, или отдельными VPN устройствами) для построения **VPN** (Virtual Private Network).

Следует заметить, что в пакете IPsec нет специального поля "режим": которое бы позволяло разделить транспортный режим от туннельного, эту функцию выполняет поле *следующий заголовок* пакета AH.

Когда поле следующий заголовок соответствует *IP*, это означает, что пакет инкапсулирует всю IP-дейтограмму (туннельный режим), включая независимые адреса отправителя и получателя, которые позволяют реализовать маршрутизацию после туннеля.

Туннельный режим

Любое другое значение поля (TCP, UDP, ICMP и т.д.) означает транспортный режим (безопасная транспортировка по схеме точка-точка).

IP дейтограмма верхнего уровня имеет ту же структуру вне зависимости от режима, и промежуточные маршрутизаторы обрабатывают трафик, не анализируя внутреннее содержание IPsec/AH.

Заметим, что ЭВМ, в отличие от сетевого шлюза, должна поддерживать как транспортный, так и туннельный режим, но при формировании соединения машина-машина формирование туннеля представляется избыточным.

Кроме того, для сетевого шлюза (маршрутизатора, сетевого экрана и т.д.) необходимо поддерживать туннельный режим, в то же время поддержка транспортного режима представляется полезной лишь для случая, когда шлюз сам является конечным адресатом (например, в случае реализации процедур удаленного управления сетью).

AH содержит **ICV** (Integrity Check Value) в аутентификационной части заголовка, и эта контрольная сумма формируется обычно (но не всегда) с помощью стандартного криптографического хэш алгоритма, например, MD5 или SHA-1.

Здесь используется не традиционная контрольная сумма, которая не может предотвратить намеренное искажение содержимого, а алгоритм **HMAC** (Hashed Message Authentication Code), который при вычислении ICV применяет секретный ключ. Несмотря на то, что хакер может заново вычислить хэш, без секретного ключа он не сможет корректно сформировать ICV. Алгоритм HMAC описан в документе RFC 2104.

Заметим, что IPsec/AH не определяет, какой должна быть аутентификационная функция, вместо этого предоставляются рамки, в которых можно реализовать любую функцию, согласованную отправителем и получателем. Можно использовать для аутентификации цифровую подпись или криптографическую функцию, если оба участника их поддерживают.

Дополнительные материалы
AH и NAT

Именно потому, что AH обеспечивает хорошую защиту содержимого пакета, так как этот протокол покрывает все, что только нужно защитить, эта защита приводит к несовместимости с NAT (Network Address Translation).

Протокол NAT используется для установления соответствия между частными IP-адресами (например, 19.125.1.X) и легальными IP. При этом IP заголовок модифицируется устройством NAT путем замены IP-адресов отправителя и получателя.

Когда изменяются IP-адреса, нужно заново вычислить контрольную сумму заголовка. Это нужно сделать в любом случае. Так как устройство NAT обычно размещается в одном шаге между отправителем и получателем это требует, кроме того декрементации значения TTL (Time To Live).

Так как поля TTL и контрольная сумма заголовка всегда модифицируются на пролете, AH знает, что эти поля следует исключить из зоны защиты, но это не касается IP адресов. Адреса включены в область вычисления ICV, и любая модификация вызовет сбой при проверке ICV получателем. Так как вычисление ICV требует знания секретного ключа, который неизвестен промежуточным узлам, маршрутизатор NAT не сможет заново вычислить ICV.

Аналогичная проблема возникает при использовании протокола **PAT** (Port Address Translation), который устанавливает соответствие нескольких частных IP адресов одному внешнему IP. В этом случае изменяются не только IP-адреса. Но и коды портов в UDP и TCP пакетах (а иногда и в поле данных). Это требует много большей адаптивности со стороны устройства NAT, и более серьезных модификаций всей IP дейтограммы.

По этой причине, протокол AH в туннельном или транспортном режиме полностью несовместим с NAT.

Заметим, что эта трудность не относится к ESP, так как аутентификация и шифрование в этом варианте не охватывает IP заголовок, модифицируемый NAT. Несмотря на это, NAT создает определенные проблемы и для ESP.

Протокол NAT транслирует IP адреса “на пролете” — но он должен отслеживать то, с каким соединением происходит работа, чтобы корректно связывать отклики с источником пакетов. При использовании TCP или UDP, это обычно делается с привлечением номеров порта, но IPsec не оставляет такой возможности.

На первый взгляд можно предположить, что для решения проблемы можно использовать идентификатор SPI, но так как SPI отличаются для разных направлений обмена, для устройства NAT нет способа связать возвращаемый пакет с конкретным соединением.

Дополнительные материалы
ESP (Encapsulating Security Payload – поле данных безопасной инкапсуляции)

На рис. 18 показан формат заголовка пакета ESP. Первое поле заголовка имеет длину 32 бита и содержит значение индекса параметров безопасности (SPI), которое определяет конкретный набор таких параметров, используемый для данного пакета. За ним следует 32-битовое поле номера по порядку.

Рис. 18. Формат ESP-пакета без аутентификации

Далее размещается поле зашифрованных данных, для выравнивания его длины (+ 2 октета *Pad len* и *Next hdr*) до кратного размеру блока шифрования может использоваться поле заполнитель, которое, как и поле данных, может иметь переменную длину. После поля *заполнителя* размещается хвостовик, содержащий два однооктетных поля: длины заполнителя (*Pad len*) и кода следующего заголовка (*Next hdr*). Поле *Next hdr* характеризует тип поля данных, расположенного выше на рисунке. Протокол ESP требует, чтобы поля *Pad len* и *Next hdr* были выровнены по правому полю 32-битового слова. Для решения этой задачи также может использоваться поле заполнитель.

Дополнительные материалы
ESP (Encapsulating Security Payload – поле данных безопасной инкапсуляции)

Добавление шифрования делает ESP несколько более сложным, из-за того, что служебные поля ESP окружают поле данных, а не предшествует ему, как это сделано в протоколе AH: ESP включает в себя поля заголовка и хвостовика. Этот протокол предоставляет также туннельный и транспортный режимы обмена.

Документы RFC IPsec не регламентируют конкретный алгоритм шифрования, но допускают использование DES, triple-DES, AES и Blowfish для шифрования поля данных. Алгоритм, используемый для конкретного соединения, специфицируется *ассоциацией безопасности* SA (рассмотренной ниже), SA включает в себя не только алгоритм, но и используемый ключ.

В отличие от протокола AH, который вводит небольшой заголовок перед полем данных, ESP “окружает” защищаемое поле данных. Поля индекс *параметров безопасности* (Security Parameters Index) и номер по порядку служат для тех же целей, что и в случае AH, но в ESP имеются также поля *заполнителя, следующего заголовка*, и опционно *аутентификационных данных* в конце, в хвостовике ESP (см. рис. 19).

Возможно использование ESP без какого-либо шифрования (чтобы применить NULL алгоритм). Этот режим не обеспечивает конфиденциальности, и его имеет смысл использовать в сочетании с аутентификацией ESP. Неэффективно использовать ESP без шифрования или аутентификации (если только это не делается для тестирования протокола).

ESP (Encapsulating Security Payload – поле данных безопасной инкапсуляции)

Заполнение делается для того, чтобы сделать возможным применение блочных алгоритмов шифрования, длина поля заполнителя определяется значением поля ***pad len***. Поле ***next hdr*** определяет тип протокола поля данные (IP, TCP, UDP и т.д.). Следует иметь в виду, что поле данные размещено до этого указателя (см. рис. 19).

Помимо шифрования, ESP может опционно предоставлять возможность аутентификации, с привлечение алгоритма HMAC. В отличие от AH, однако, эта аутентификация производится только для ESP заголовка и зашифрованного поля данных. При этом не перекрывается весь IP пакет. Это не существенно ослабляет безопасность аутентификации, но дает некоторые важные преимущества.

Когда посторонний рассматривает IP пакет, содержащий данные ESP, принципиально невозможно определить IP адреса отправителя и получателя. Атакер конечно узнает, что это ESP данные (это видно из заголовка пакета), но тип поля данных и сами данные зашифрованы.

Глядя на сам пакет, невозможно даже определить, присутствуют или нет аутентификационные данные (это можно сделать лишь, используя индекс параметров безопасности).

Дополнительные материалы
ESP в транспортном режиме

Как и в случае AH, транспортный режим предполагает инкапсуляцию поля данных дейтограмм, и протокол ориентирован на обмен машина-машина. Исходный IP заголовок оставлен на месте (за исключением замененного поля протокол), и это означает, что адреса отправителя и получателя также остаются неизмененными.

Структура данных в пакете для протокола ESP в транспортном режиме показана на рис. 19. Жирным контуром выделены аутентификацируемые данные, а закрашенная область отмечает шифруемую часть данных. Поле *Next* внизу рисунка характеризует тип протокола поля данных, закрашенного на рисунке (в приведенном примере это TCP).

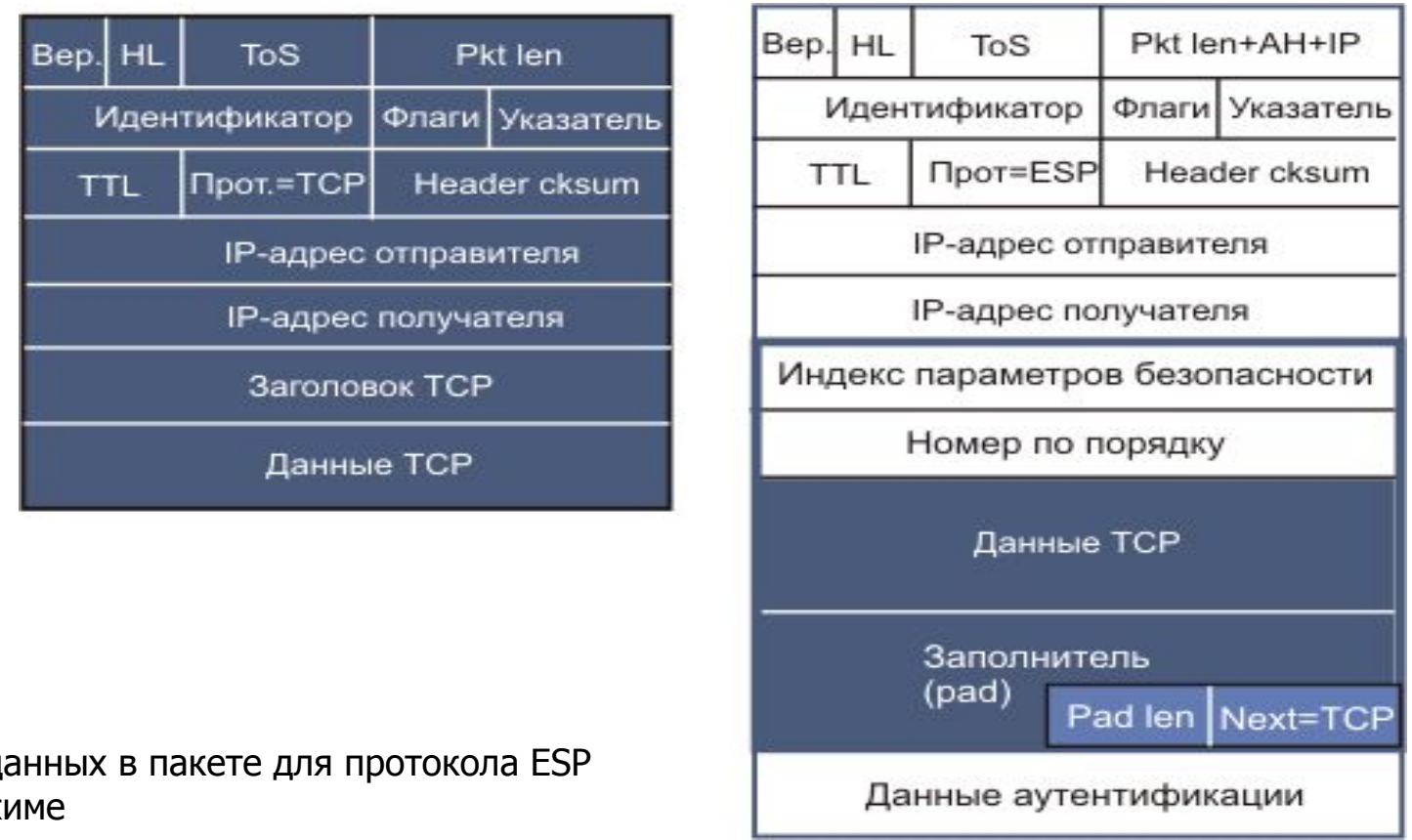


Рис. 19. Структура данных в пакете для протокола ESP в транспортном режиме

Дополнительные материалы
ESP в туннельном режиме

Посмотрим еще раз на ESP в туннельном режиме, когда инкапсулируется вся IP-дейтограмма внутрь зашифрованной оболочки.

Структура данных в пакете для протокола ESP в туннельном режиме показана на рис. 20. Слева на рисунке размешен формат исходной дейтограммы с инкапсулированным TCP-сегментом. Жирным контуром выделены аутентифицированные данные, а закрашенная область отмечает шифруемую часть данных. Поле *Next* внизу рисунка характеризует тип протокола данных (на рисунке закрашено, в приведенном примере это IP).

Реализация шифрованного соединения в туннельном режиме очень близка к традиционным VPN.

В отличие от AH, где наблюдатель может легко сказать, происходил обмен в туннельном или транспортном режиме, здесь эта информация недоступна. Это происходит из-за того, что указание на то, что следующий заголовок является IP, находится в зашифрованном поле данных и, поэтому не виден для участника, неспособного дешифровать пакет.

Рис. 20. Структура данных в пакете для протокола ESP в туннельном режиме

Построение VPN

При полном перекрытии аутентификационного заголовка и инкапсулированного поля данных можно построить настоящую VPN (Virtual Private Network). Конечной целью VPN является объединение двух безопасных сетей через небезопасные каналы (например, сети двух отделений компании через Internet). Схема построения VPN показана на рис. 21. Предполагается, что обработка пакетов VPN на входе/выходе локальных сетей осуществляется в сетевых шлюзах (GW). Функции GW могут выполнять и сетевые экраны (Firewall).

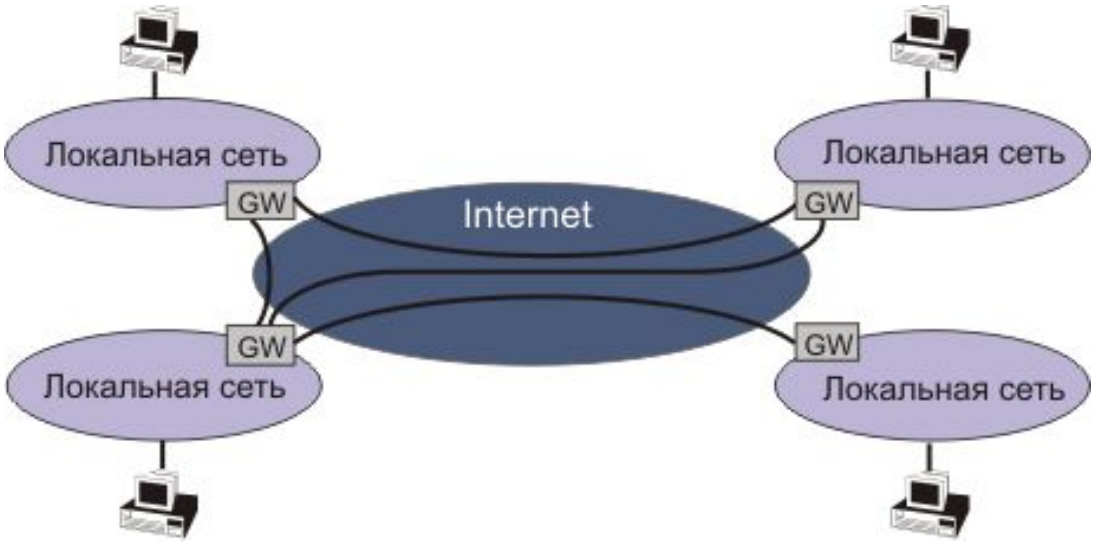


Рис. 21. Схема построения VPN

Понятно, что безопасные VPN требуют применения, как аутентификации, так и шифрования. Известно, что ESP является лишь средством обеспечения шифрования, но ESP и AH могут осуществлять аутентификацию.

На рис. 22 показана структура VPN-пакета при использовании протокола ESP и аутентификации.

Поле Next в данном случае характеризует тип протокольного пакета, размещенного выше на рисунке (тип=IP, закрашенная область).

Очевидным решением является встраивание ESP в AH, что технически возможно, но на практике не используется, из-за ограничений AH в отношении протокола NAT. Применение комбинации AH и ESP не позволит использовать технику NAT.

Вместо этого, комбинация ESP и Auth используется в туннельном режиме при полной инкапсуляции трафика в процессе транспортировки через области сети, где нет гарантии безопасности.

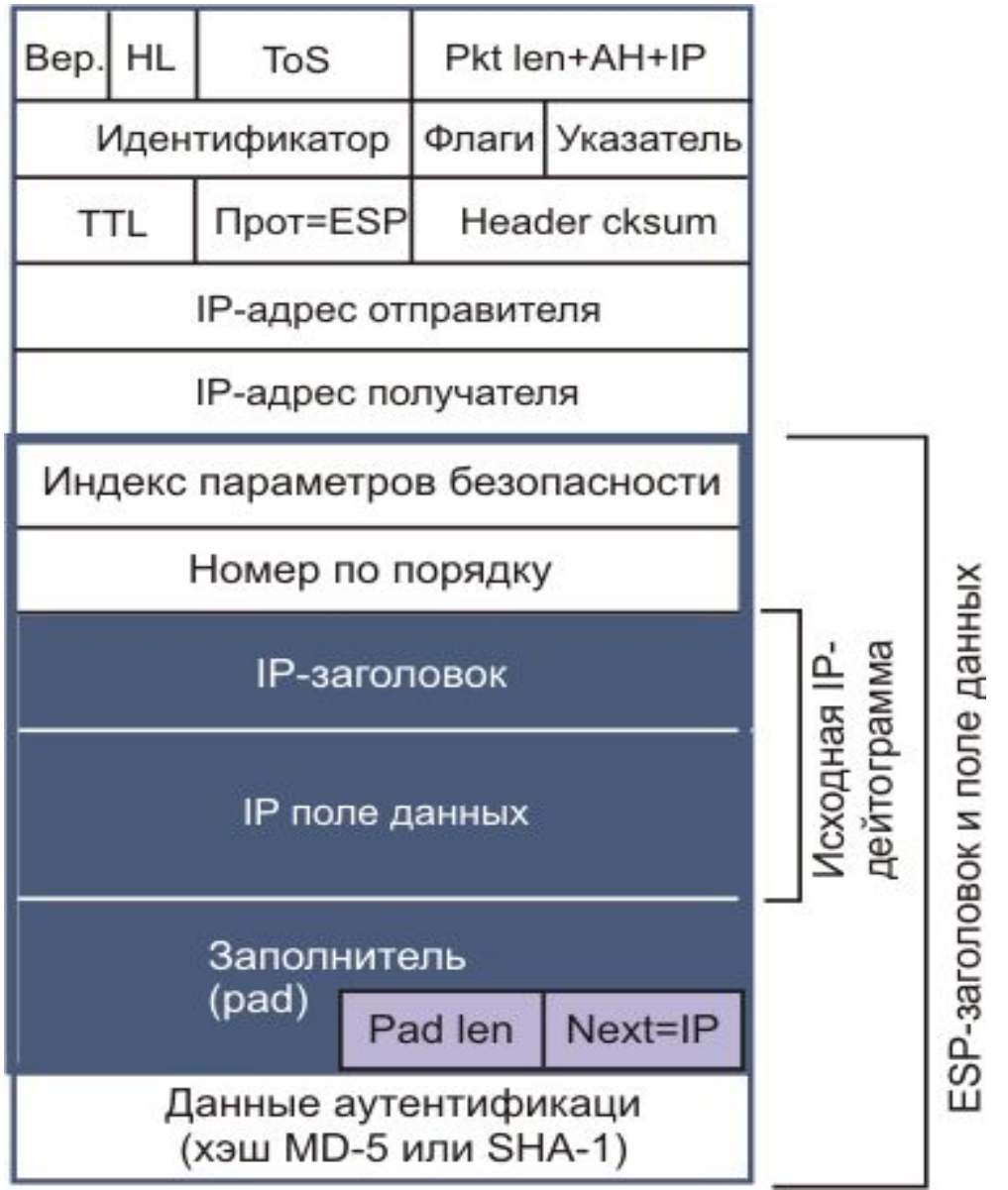


Рис. 22. Структура VPN-пакета при использовании протокола ESP и аутентификации

Трафик, защищенный так, не предоставляет перехватчику информации о том, что два сетевых объекта соединены VPN. Эта информация может оказаться атакеру полезной для понимания структуры отношений партнеров. В протоколе ESP даже тип транспортного протокола (TCP, UDP или ICMP) оказывается скрыт от постороннего.

Достаточно важно то, что даже конечный пользователь не знает ничего о VPN или других используемых мерах безопасности. VPN реализуется сетевым шлюзом, который выглядит как один из интерфейсов, маршрутизация же осуществляется обычным образом.

Вложение пакет-в-пакет может быть многослойным. ЭВМ **A** и ЭВМ **B** могут установить свое аутентифицированное соединение (с помощью протокола AH), и осуществлять маршрутизацию через VPN. Это приведет к тому, что внутренний пакет AH будет помещен внутрь пакета ESP+Auth.

Важно использовать аутентификацию даже в случае применения шифрования, так как такое соединение может стать объектом атаки, описанной в http://eprint.iacr.org/2005/416 (Paterson & Yau).

Дополнительные материалы
Ассоциации безопасности и SPI

Кажется самоочевидным, что если два партнера или шлюза намереваются установить безопасное соединение, необходим некоторый объем общих секретных данных для реализации аутентификации и/или алгоритмов шифрования. Существует, конечно, проблема безопасной транспортировки этих секретных данных.

Когда IPsec-дейтограмма, AH или ESP попадает в интерфейс, как интерфейс узнает, какой набор параметров (ключ, алгоритм и политика) использовать? Любая машина может вести много диалогов, каждый со своим набором параметров безопасности и нужен механизм управления этим процессом.

Параметры безопасности задаются ***SA*** (*Security Association*), которая определяет параметры и процедуры, специфические для конкретного соединения. Каждый партнер может иметь один или более SA. Когда дейтограмма приходит, для нахождения правильного SA в базе данных **SADB** (Security Associations Database – база данных ассоциаций безопасности) используются три значения:

- IP адрес места назначения.
- IPsec протокол (ESP или AH, содержится в заголовке).
- Индекс параметров безопасности (SPI).

Во многих отношениях эта тройка может быть уподоблена IP сокету, который однозначно определяется IP адресом удаленного партнера (IPv4 или IPv6), протоколом и номером порта.

Дополнительные материалы
Ассоциации безопасности и SPI

В перечень компонентов SA входят:

- *Номер по порядку*. 32-битовый код, используемый для формирования поля порядковый номер в заголовках AH и ESP.
- *Переполнение счетчика порядкового номера*. Флаг, индицирующий переполнение счетчика порядкового номера. При его установке дальнейшая посылка пакетов для заданной SA должна быть прекращена.
- *Окно для подавления попыток атак воспроизведения*. Используется для определения того, является ли входящий AH- или ESP-пакет воспроизведением. Задача решается путем контроля того, попадает ли номер пакета в скользящее окно номеров.
- *Информация AH*. Алгоритм аутентификации, ключи, время жизни ключей и др.
- *Информация ESP*: алгоритмы шифрования и аутентификации, ключи, параметры инициализации (IV), времена жизни ключей и другие параметры.
- *Окно для подавления попыток атак воспроизведения*. Используется для определения того, является ли входящий AH- или ESP-пакет воспроизведением. Задача решается путем контроля того, попадает ли номер пакета в скользящее окно номеров.
- *Информация AH*. алгоритм аутентификации, ключи, время жизни ключей и другие параметры.
- *Информация ESP*: алгоритмы шифрования и аутентификации, ключи, параметры инициализации (**IV**), времена жизни ключей и другие параметры.
- *Режим работы IPsec*. Туннельный, транспортный или любой.
- *MTU пути*. Максимальный размер пакета, который может быть передан через виртуальный канал без фрагментации.

Дополнительные материалы
Ассоциации безопасности и SPI

При создании новой SA в счетчик номера по порядку заносится нуль, далее он инкрементируется при посылке каждого пакета. Когда содержимое счетчика достигает значения 232-1, текущая SA аннулируется и должна быть согласована новая ассоциация безопасности и новый ключ.

Так как IP работает без установления соединения и доставка пакетов по порядку не гарантируется, протокол требует, чтобы получатель сформировал скользящее окно с шириной W, например, W=64 пакета. Правый край окна соответствует наибольшему номеру по порядку N для благополучно принятых пакетов. Любой пакет с номером в диапазоне от N-W+1 до N считается принятым корректно. Если полученный пакет оказался по левую границу окна, или его аутентификация потерпела неудачу, то такой пакет отбрасывается. Ниже приведен пример из [1], где длина W=7 (реально это число может достигать 232). Первые две строки показывают состояние окна с началом в позиции 1 и концом в позиции 7, пакет с номером 9 получен, но его подлинность не подтверждена. Буквами П обозначены полученные пакеты с подтвержденной подлинностью, буквами Н – неполученные пакеты; а буквой О, полученный пакет, подлинность которого не подтверждена. Красным цветом отмечено окно W.

П	Н	П	П	П	Н	П	П	Н	О	Н	Н	Н
0	1	2	3	4	5	6	7	8	9	10	11	….
П	Н	П	П	П	Н	П	П	Н	П	Н	Н	Н
0	1	2	3	4	5	6	7	8	9	10	11	….

Когда подлинность полученного пакета с номером 9 оказалась подтвержденной, правая граница окна смещается на эту позицию и занимает положение, показанное на вторых строках данного примера. В этом состоянии, если придет пакет с номером 1 или 2, они будут отвергнуты. Если же придут пакеты с номерами 5 или 8 они будут подвергнуты обработке, так как находятся в пределах окна W.

Ассоциации безопасности сопрягаются с однонаправленными соединениями, так что для двунаправленной связи требуется как минимум две такие ассоциации. Кроме того, каждый протокол (ESP/AH) имеет свою собственную SA, для каждого из направлений обмена, таким образом, полномасштабная VPN AH+ESP требует наличия четырех ассоциаций безопасности. Все эти данные хранятся в базе данных SADB.

В базе данных SADB содержится:

- AH: алгоритм аутентификации.
- AH: аутентификационный секретный ключ (authentication secret).
- ESP: алгоритм шифрования.
- ESP: секретный ключ шифрования.
- ESP: разрешение аутентификации (yes/no).
- *Параметры обмена ключами*.
- Ограничения маршрутизации.
- IP политика фильтрации.

Некоторые реализации поддерживают **SPD** (Security Policy Database) со средствами работы из командной строки, другие с GUI, в то время как прочие предоставляют WEB-интерфейс для работы через сеть.

Дополнительные материалы
Ассоциации безопасности и SPI

Каждая запись в SPD определяется набором значений полей IP и протокола верхнего уровня, называемых селекторами. Эти селекторы используются для фильтрации исходящего трафика, для того чтобы поставить его в соответствие с определенной SA.

Обработка исходящих IP-пакетов производится в следующей последовательности:

- сравниваются значения соответствующих полей в пакете (селекторные поля) с SPD и находится нуль или более SA.
- Определяется SA (если таковая имеется) для пакета и сопряженный с ней SPI.
- Выполняются необходимые операции IPsec (AH или ESP).

SPD запись определяется следующими селекторами:

- *IP-адрес места назначения*. Это может быть один IP-адрес (обязательно уникастный!), нумерованный список адресов или адресная маска (префикс). Последние два варианта нужны для работы группами адресов, имеющими идентичную SA (например, за firewall).
- *IP-адрес отправителя*. Это может быть один IP-адрес, нумерованный список адресов или адресная маска (префикс). Последние два варианта нужны для поддержки нескольких отправителей, имеющих идентичную SA, (например, за firewall).
- *UserID*. Идентификатор пользователя служит для идентификации политики, соответствующей имени пользователя или системы.
- *Уровень чувствительности данных*. Уровень чувствительности данных используется для определения характера данных (например, “Секретно” или “Unclassified”).

Дополнительные материалы
Ассоциации безопасности и SPI

- *Протокол транспортного уровня*. Это значение извлекается из поля следующий заголовок пакета IPv4 или IPv6. Это может быть индивидуальный код протокола, список кодов протокола или диапазон таких кодов.
- *Протокол IPsec* (AH, ESP или AH/ESP). Извлекается (если присутствует) из поля следующий заголовок пакета IPv4 или IPv6.
- *Порты отправителя и получателя*. Это могут быть индивидуальные номера портов TCP или UDP, список портов или произвольный порт.
- *Класс IPv6*. Значение класса получается из заголовка IPv6. Это может быть специфическое значение и код произвольного класса.
- *Метка потока IPv6*. Значение метки потока получается из заголовка IPv6. Это может быть специфическое значение метки потока или код произвольной метки.
- *Тип сервиса IPv4*. Значение ToS получается из заголовка IPv4. Это может быть специфическое значение ToS или указатель произвольного значения.

Дополнительные материалы
Управление ключами

Для управления ключами используется несколько протоколов. IPsec был бы бесполезным без шифрования и аутентификации, которые в свою очередь невозможны без секретных ключей, известных партнерам обмена и неизвестных больше никому.

Наиболее простым способом задания этих секретных ключей является ручная конфигурация: один партер генерирует набор ключей и передает ключи другим партерам.

Но такая схема плохо масштабируется, кроме того, кто-то из партнеров может пренебречь мерами безопасности и в результате вся сеть будет скомпрометирована. В больших системах с большим числом узлов такая схема обычно не приемлема.

Система **IKE** (Internet Key Exchange) позволяет двум партнерам динамически аутентифицировать друг друга, согласовать использование ассоциации безопасности (Security Association), включая секретные ключи, и генерировать сами ключи. Система IKE использует **ISAKMP** (Internet Security Association Key Management Protocol – протокол управления ключами ассоциации безопасности Интернет, разработан Национальным агентством безопасности США - NSA). Протокол ISAKMP сам по себе не регламентирует какой-либо конкретный алгоритм обмена ключами, он содержит в себе описание ряда сообщений, которые позволяют согласовать использование алгоритмов обмена ключами.

Управление ключами

Согласование осуществляется в два этапа:

- Узлы ISAKMP согласуют механизмы защиты дальнейшего обмена данными, путем установления SA. Эта ассоциация служит для защиты последующих операций и отличается от прочих SA.
- Протокол ISAKMP устанавливает SA для других протоколов, например, из семейства IPsec.

Механизм обмена ключами в IKE берется из протокола Oakley (RFC-2412). Основой протокола обмен ключами Oakley является алгоритм Диффи-Хелмана (см. http://book.itep.ru/6/difi_646.htm), дополненный некоторыми усовершенствованиями. В частности в каноническом алгоритме Диффи-Хелмана отсутствует аутентификация партнеров, что допускает возможность атаки с подменом ключей. В IPsec версии алгоритма, аутентификация партнеров является обязательной процедурой.

Заметим, что IPsec осуществляет пересылку ключей через порт 500/udp. В IPsec при обмене ключами предусмотрено использование сертификатов. Для получения сертификата посылается запрос в сертификационный центр CA (Certificate Authority).

Дополнительные материалы
Управление ключами

Сертификация включает в себя следующие операции:

- Клиент генерирует пару ключей (общедоступный и секретный). Далее он готовит неподписанный сертификат, который содержит идентификатор клиента и его общедоступный ключ. После этого клиент посылает этот сертификат в CA, шифруя его открытым ключом CA.
- CA формирует хэш для присланного неподписанного сертификата и шифрует его своим секретным ключом. CA добавляет сформированную так электронную подпись к неподписанному сертификату и посылает уже подписанный сертификат клиенту.
- Клиент теперь может послать свой подписанный сертификат любому другому пользователю. Получатель сертификата может легко его проверить, если располагает общедоступным ключом CA.

Клиенты могут пользоваться одним и тем же CA или быть клиентами разных CA. На практике обычно реализуется иерархическая структура CA.

В Интернет имеется огромное количество материалов по проблематике IPsec, но начинать всегда лучше с документов RFC (Requests for Comment), которые со временем обретают статус стандартов.

В декабре 2005, весь набор документов RFC по IPsec был обновлен IETF, а серия RFC 43xx по большей части заменила серию RFC 24xx.

Дополнительные материалы

Ссылки

RFC 4301	Security Architecture for the Internet Protocol, S. Kent, K. Seo, December 2005. (обзор протокола IPsec в целом).
RFC 4302	IP Authentication Header, S. Kent. December 2005
RFC 4303	IP Encapsulating Security Payload (ESP). S. Kent. December 2005
RFC 4304	Extended Sequence Number (ESN) Addendum to IPsec Domain of Interpretation (DOI) for Internet Security Association and Key Management Protocol (ISAKMP). S. Kent. December 2005
RFC 2104	HMAC: Keyed-Hashing for Message Authentication. H. Krawczyk, M. Bellare, R. Canetti. February 1997
RFC 2405	The Use of HMAC-SHA-1-96 within ESP and AH. C. Madson, R. Glenn. November 1998
RFC 2407	The Internet IP Security Domain of Interpretation for ISAKMP. D. Piper. November 1998
RFC 2408	Internet Security Association and Key Management Protocol (ISAKMP). D. Maughan, M. Schertler, M. Schneider, J. Turner. November 1998
RFC 4306	Internet Key Exchange (IKEv2) Protocol. C. Kaufman, Ed.. December 2005
RFC 2410	The NULL Encryption Algorithm and Its Use With IPsec. R. Glenn, S. Kent. November 1998
RFC 2411	IP Security Document Roadmap. R. Thayer, N. Doraswamy, R. Glenn. November 1998
RFC 2412	The OAKLEY Key Determination Protocol. H. Orman. November 1998
RFC 3884	Use of IPsec Transport Mode for Dynamic Routing. J. Touch, L. Eggert, Y. Wang. September 2004
1	У.Блэк, Интернет. Протоколы безопасности, “Питер”, Санкт-Петербург, 2001
2	Терри Оглтри, Firewalls. Практическое применение межсетевых экранов, Москва, ДМК, 2001
3	http://www.yars.free.net/CiscoCD/cc/td/doc/product/ software/ios113ed/113t/ 113t_3/ipsec.htm#xtocid25940
4	http://www.schneier.com/paper-ipsec.pdf, by Bruce Schneier and Niels Ferguson
5	С.Г.Баричев, В.В.Гончаров, Р.Е.Серов, Основы современной криптографии, Горячая линия-Телеком, 2002