52. Системы безопасности. Обеспечение безопасности при передачи данных по открытым каналам связи. Безопасность на канальном и сетевом уровне и на уровне приложений. (VLAN, VPN, IPSec, SSL). Раскрыть принципы функционирования.

Протокол SSL

Один из подходов к решению проблемы безопасности в Интернете был предложен компанией Netscape Communications. Ею был разработан протокол SSL (Secure Sockets Layer) защищенного обмена информацией между клиентом и сервером. SSL требует применения надежного транспортного протокола (например, TCP).

Протокол SSL предназначен для решения традиционных задач обеспечения защиты информационного взаимодействия, которые в среде клиент/сервер интерпретируются следующим образом:

- пользователь, подключаясь к серверу, должен быть уверен, что он обменивается информацией не с подставным сервером, а именно с тем, который ему нужен (в противном случае это может привести к курьезным, если не к печальным, последствиям). Во многих приложениях необходимо также, чтобы и сервер мог надежно идентифицировать клиента, не ограничиваясь защитой паролем;
- после установления соединения между сервером и клиентом весь информационный поток между ними должен быть защищен от несанкционированного доступа;
- при обмене информацией стороны должны быть уверены в отсутствии случайных или умышленных искажений при ее передаче.

Протокол SSL позволяет серверу и клиенту перед началом информационного взаимодействия аутентифицировать друг друга, согласовать алгоритм шифрования и сформировать общие криптографические ключи. С этой целью протокол использует двухключевые криптосистемы, в частности RSA.

Конфиденциальность информации, передаваемой по установленному защищенному соединению, обеспечивается путем шифрования потока данных на сформированном общем ключе с использованием симметричных криптографических алгоритмов (например, RC4_128, RC4_40, RC2_128, RC2_40, DES40 и др.), а контроль целостности передаваемых блоков данных - за счет использования так называемых кодов аутентификации сообщений (Message Autentification Code, MAC), вычисляемых с помощью хеш-функций (в частности, MD5).
Протокол SSL включает в себя два этапа взаимодействия сторон защищаемого соединения:

- установление SSL-сессии;
- защита потока данных.

На этапе установления SSL-сессии осуществляется аутентификация сервера и (опционально) клиента, стороны договариваются об используемых криптографических алгоритмах и формируют общий "секрет", на основе которого создаются общие сеансовые ключи для последующей защиты соединения. Этот этап называют также процедурой "рукопожатия".

На втором этапе (защита потока данных) информационные сообщения прикладного уровня нарезаются на блоки, для каждого блока вычисляется код аутентификации сообщений, затем данные шифруются и отправляются приемной стороне. Приемная сторона производит обратные действия: дешифрование, проверку кода аутентификации сообщения, сборку сообщений, передачу на прикладной уровень.

Преимуществом SSL является то, что он независим от прикладного протокола. Протоколы приложения, такие как HTTP, FTP, TELNET и т.д. могут работать поверх протокола SSL совершенно прозрачно. Протокол SSL может согласовывать алгоритм шифрования и ключ сессии, а также аутентифицировать сервер до того как приложение примет или передаст первый байт данных. Все протокольные прикладные данные передаются зашифрованными с гарантией конфиденциальности.
Протокол SSL предоставляет "безопасный канал", который имеет три основные свойства:

- канал является частным *шифрование используется для всех сообщений после простого диалога, который служит для определения секретного ключа+
- канал аутентифицирован *серверная сторона диалога всегда аутентифицируется, в то время как клиентская аутентифицируется опционно+
- канал надежен *транспортировка сообщений включает в себя проверку целостности (с привлечением MAC)+.

Архитектура IPSec

IP Security - это комплект протоколов, касающихся вопросов шифрования, аутентификации и обеспечения защиты при транспортировке IP-пакетов; в его состав сейчас входят почти 20 предложений по стандартам и 18 RFC. Спецификация IP Security (известная сегодня как IPsec) разрабатывается Рабочей группой IP Security Protocol IETF. Первоначально IPsec включал в себя 3 алгоритмо-независимые базовые спецификации, опубликованные в качестве RFC-документов "Архитектура безопасности IP", "Аутентифицирующий заголовок (AH)", "Инкапсуляция зашифрованных данных (ESP)" (RFC1825, 1826 и 1827). Необходимо заметить, что в ноябре 1998 года Рабочая группа
IP Security Protocol предложила новые версии этих спецификаций, имеющие в настоящее время статус предварительных стандартов, это RFC2401 - RFC2412. Отметим, что RFC1825-27 на протяжении уже нескольких лет считаются устаревшими и реально не используются. Кроме этого, существуют несколько алгоритмо-зависимых спецификаций, использующих протоколы MD5, SHA,

DES.

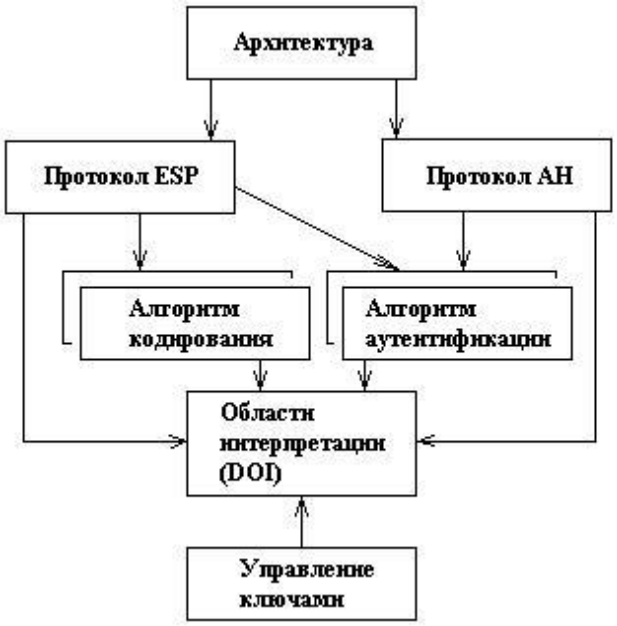

Рис. 1 – Архитектура IPSec.

Рабочая группа IP Security Protocol разрабатывает также и протоколы управления ключевой информацией. В задачу этой группы входит разработка Internet Key Management Protocol (IKMP), протокола управления ключами прикладного уровня, не зависящего от используемых протоколов обеспечения безопасности. В настоящее время рассматриваются концепции управления ключами с использованием спецификации Internet Security Association and Key Management Protocol (ISAKMP) и протокола Oakley Key Determination Protocol. Спецификация ISAKMP описывает механизмы согласования атрибутов используемых протоколов, в то время как протокол Oakley позволяет устанавливать сессионные ключи на компьютеры сети Интернет. Ранее рассматривались также возможности использования механизмов управления ключами протокола SKIP, однако сейчас такие возможности реально практически нигде не используются. Создаваемые стандарты управления ключевой информацией, возможно, будут поддерживать Центры распределения ключей, аналогичные используемым в системе Kerberos. Протоколами ключевого управления для IPSec на основе Kerberos сейчас занимается относительно новая рабочая группа KINK (Kerberized Internet Negotiation of Keys).

Гарантии целостности и конфиденциальности данных в спецификации IPsec обеспечиваются за счет использования механизмов аутентификации и шифрования соответственно. Последние, в свою очередь, основаны на предварительном согласовании сторонами информационного обмена т.н. "контекста безопасности" – применяемых криптографических алгоритмов, алгоритмов управления ключевой информацией и их параметров. Спецификация IPsec предусматривает возможность поддержки сторонами информационного обмена различных протоколов и параметров аутентификации и шифрования пакетов данных, а также различных схем распределения ключей. При этом результатом согласования контекста безопасности является установление индекса параметров безопасности (SPI), представляющего собой указатель на определенный элемент внутренней структуры стороны информационного обмена, описывающей возможные наборы параметров безопасности.

По сути, IPSec, который станет составной частью IPv6, работает на третьем уровне, т. е. на сетевом уровне. В результате передаваемые IP-пакеты будут защищены прозрачным для сетевых приложений и инфраструктуры образом. В отличие от SSL (Secure Socket Layer), который работает на четвертом (т. е. транспортном) уровне и теснее связан с более высокими уровнями модели OSI, IPSec призван обеспечить низкоуровневую защиту.

Уровни TCP/IP	Уровни ISO/OSI
4. Прикладных программ	7. Прикладных программ 6. Представление данных
3. Транспортный	5. Сеансовый 4. Транспортный
2. Межсетевой	3. Сетевой
1. Доступа к сети	2. Канальный 1. Физический

Рис. 2 – Модель OSI/ISO.

К IP-данным, готовым к передаче по виртуальной частной сети, IPSec добавляет заголовок для идентификации защищенных пакетов. Перед передачей по Internet эти пакеты инкапсулируются в другие IP-пакеты. IPSec поддерживает несколько типов шифрования, в том числе Data Encryption Standard (DES) и Message Digest 5 (MD5).

Чтобы установить защищенное соединение, оба участника сеанса должны иметь возможность быстро согласовать параметры защиты, такие как алгоритмы аутентификации и ключи. IPSec поддерживает два типа схем управления ключами, с помощью которых участники могут согласовать параметры сеанса. Эта двойная поддержка в свое время вызвала определенные трения в IETF Working Group.

С текущей версией IP, IPv4, могут быть использованы или Internet Secure Association Key Management Protocol (ISAKMP), или Simple Key Management for Internet Protocol. С новой версией IP, IPv6, придется использовать ISAKMP, известный сейчас как IKE, хотя не исключается возможность использования SKIP. Однако, следует иметь в виду, что SKIP уже давно не рассматривается как кандидат управления ключами, и был исключён из списка возможных кандидатов ещё в 1997 г.

Заголовок AH

Аутентифицирующий заголовок (AH) является обычным опциональным заголовком и, как правило, располагается между основным заголовком пакета IP и полем данных. Наличие AH никак не влияет на процесс передачи информации транспортного и более высокого уровней. Основным и единственным назначением AH является обеспечение защиты от атак, связанных с несанкционированным изменением содержимого пакета, и в том числе от подмены исходного адреса сетевого уровня. Протоколы более высокого уровня должны быть модифицированы в целях осуществления проверки аутентичности полученных данных.

Формат AH достаточно прост и состоит из 96-битового заголовка и данных переменной длины, состоящих из 32-битовых слов. Названия полей достаточно ясно отражают их содержимое: Next Header указывает на следующий заголовок, Payload Len представляет длину пакета, SPI является указателем на контекст безопасности и Sequence Number Field содержит последовательный номер пакета.

Следующий заголовок	Длина нагрузки	Зарезервировано
Индекс параметров безопасности		
Поле последовательного номера		
Данные аутентификации (переменной длины)		

Рис. 3 – Формат заголовка AH.

Последовательный номер пакета был введен в AH в 1997 году в ходе процесса пересмотра спецификации IPsec. Значение этого поля формируется отправителем и служит для защиты от атак, связанных с повторным использованием данных процесса аутентификации. Поскольку сеть Интернет не гарантирует порядок доставки пакетов, получатель должен хранить информацию о максимальном последовательном номере пакета, прошедшего успешную аутентификацию, и о получении некоторого числа пакетов, содержащих предыдущие последовательные номера (обычно это число равно 64).

В отличие от алгоритмов вычисления контрольной суммы, применяемых в протоколах передачи информации по коммутируемым линиям связи или по каналам локальных сетей и ориентированных на исправление случайных ошибок среды передачи, механизмы обеспечения целостности данных в открытых телекоммуникационных сетях должны иметь средства защиты от внесения целенаправленных изменений. Одним из таких механизмов является специальное применение алгоритма MD5: в процессе формирования AH последовательно вычисляется хэш-функция от объединения самого пакета и некоторого предварительно согласованного ключа, а затем от

объединения полученного результата и преобразованного ключа. Данный механизм применяется по умолчанию в целях обеспечения всех реализаций IPv6, по крайней мере, одним общим алгоритмом, не подверженным экспортным ограничениям.

Заголовок ESP

В случае использования инкапсуляции зашифрованных данных заголовок ESP является последним в ряду опциональных заголовков, "видимых" в пакете. Поскольку основной целью ESP является обеспечение конфиденциальности данных, разные виды информации могут требовать применения существенно различных алгоритмов шифрования. Следовательно, формат ESP может претерпевать значительные изменения в зависимости от используемых криптографических алгоритмов. Тем не менее, можно выделить следующие обязательные поля: SPI, указывающее на контекст безопасности и Sequence Number Field, содержащее последовательный номер пакета. Поле "ESP Authentication Data" (контрольная сумма), не является обязательным в заголовке ESP. Получатель пакета ESP расшифровывает ESP заголовок и использует параметры и данные применяемого алгоритма шифрования для декодирования информации транспортного уровня.

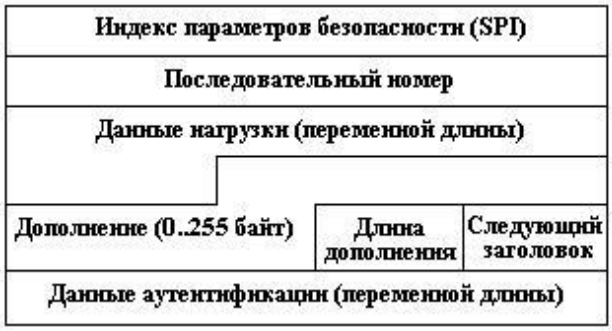

Рис. 4 – Формат заголовка ESP.

Различают два режима применения ESP и AH (а также их комбинации) - *транспортный* и *туннельный*.

Транспортный режим

Транспортный режим используется для шифрования поля данных IP пакета, содержащего протоколы транспортного уровня (TCP, UDP, ICMP), которое, в свою очередь, содержит информацию прикладных служб. Примером применения транспортного режима является передача электронной почты. Все промежуточные узлы на маршруте пакета от отправителя к получателю используют только открытую информацию сетевого уровня и, возможно, некоторые опциональные заголовки пакета (в IPv6). Недостатком транспортного режима является отсутствие механизмов скрытия конкретных отправителя и получателя пакета, а также возможность проведения анализа трафика. Результатом такого анализа может стать информация об объемах и направлениях передачи информации, области интересов абонентов, расположение руководителей.

Туннельный режим

Туннельный режим предполагает шифрование всего пакета, включая заголовок сетевого уровня. Туннельный режим применяется в случае необходимости скрытия информационного обмена организации с внешним миром. При этом, адресные поля заголовка сетевого уровня пакета, использующего туннельный режим, заполняются межсетевым экраном организации и не содержат информации о конкретном отправителе пакета. При передаче информации из внешнего мира в локальную сеть организации в качестве адреса назначения используется сетевой адрес межсетевого экрана. После расшифровки межсетевым экраном начального заголовка сетевого уровня пакет направляется получателю.

Security Associations

Security Association (SA) – это соединение, которое предоставляет службы обеспечения безопасности трафика, который передаётся через него. Два компьютера на каждой стороне SA хранят режим, протокол, алгоритмы и ключи, используемые в SA. Каждый SA используется только в одном направлении. Для двунаправленной связи требуется два SA. Каждый SA реализует один режим и протокол; таким образом, если для одного пакета необходимо использовать два протокола (как например AH и ESP), то требуется два SA.

Политика безопасности хранится в SPD (База данных политики безопасности). SPD может указать для пакета данных одно из трёх действий: отбросить пакет, не обрабатывать пакет с помощью IPSec, обработать пакет с помощью

IPSec. В последнем случае SPD также указывает, какой SA необходимо использовать (если, конечно, подходящий SA уже был создан) или указывает, с какими параметрами должен быть создан новый SA.

SPD является очень гибким механизмом управления, который допускает очень хорошее управление обработкой каждого пакета. Пакеты классифицируются по большому числу полей, и SPD может проверять некоторые или все поля для того, чтобы определить соответствующее действие. Это может привести к тому, что весь трафик между двумя машинами будет передаваться при помощи одного SA, либо отдельные SA будут использоваться для каждого приложения, или даже для каждого TCP соединения.

ISAKMP/Oakley

Протокол ISAKMP определяет общую структуру протоколов, которые используются для установления SA и для выполнения других функций управления ключами. ISAKMP поддерживает несколько Областей Интерпретации (DOI), одной из которых является IPSec-DOI. ISAKMP не определяет законченный протокол, а предоставляет "строительные блоки" для различных DOI и протоколов обмена ключами.

Протокол Oakley – это протокол определения ключа, использующий алгоритм замены ключа Диффи-Хеллмана. Протокол Oakley поддерживает идеальную прямую безопасность (Perfect Forward Secrecy – PFS). Наличие PFS означает невозможность расшифровки всего траффика при компрометации любого ключа в системе.

IKE – протокол обмена ключами по умолчанию для ISAKMP, на данный момент являющийся единственным. IKE находится на вершине ISAKMP и выполняет, собственно, установление как ISAKMP SA, так и IPSec SA. IKE поддерживает набор различных примитивных функций для использования в протоколах. Среди них можно выделить хэш-функцию и псевдослучайную функцию (PRF).

Хэш-функция – это функция, устойчивая к коллизиям. Под устойчивостью к коллизиям понимается тот факт, что невозможно найти два разных сообщения m_1 и m_2, таких, что $H(m_1)=H(m_2)$, где H – хэш функция.

Что касается псеводслучайных функций, то в настоящее время вместо специальных PRF используется хэш функция в конструкции HMAC (HMAC - механизм аутентификации сообщений с использованием хэш функций). Для определения HMAC нам понадобится криптографическая хэш функция (обозначим её как H) и секретный ключ K. Мы предполагаем, что H является хэш функцией, где данные хэшируются с помощью процедуры сжатия, последовательно применяемой к последовательности блоков данных. Мы обозначим за B длину таких блоков в байтах, а длину блоков, полученных в результате хэширования - как L (L<B). Ключ K может иметь длину, меньшую или равную B. Если приложение использует ключи большей длины, сначала мы должны хэшировать сам ключ с использованием H, и только после этого использовать полученную строку длиной L байт, как ключ в HMAC. В обоих случаях рекомендуемая минимальная длина для K составляет L байт. Определим две следующие различные строки фиксированной длины:

ipad = байт 0x36, повторённый B раз;
opad = байт 0x5C, повторённый B раз.

Для вычисления HMAC от данных 'text' необходимо выполнить следующую операцию:

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

Из описания следует, что IKE использует для аутентификации сторон HASH величины. Отметим, что под HASH в данном случае подразумевается исключительно название Payload в ISAKMP, и это название не имеет ничего общего со своим содержимым.

Атаки на AH, ESP и IKE.

Все виды атак на компоненты IPSec можно разделить на следующие группы: атаки, эксплуатирующие конечность ресурсов системы (типичный пример - атака "Отказ в обслуживании", Denial-of-service или DOS-атака), атаки, использующие особенности и ошибки конкретной реализации IPSec и, наконец, атаки, основанные на слабостях самих протоколов. AH и ESP. Чисто криптографические атаки можно не рассматривать - оба протокола определяют понятие "трансформ", куда скрывают всю криптографию. Если используемый криптоалгоритм стоек, а определенный с ним трансформ не вносит дополнительных слабостей (это не всегда так, поэтому правильнее рассматривать стойкость всей системы - Протокол-Трансформ-Алгоритм), то с этой стороны все нормально. Что остается? Replay Attack - нивелируется за счет использования Sequence Number (в одном единственном случае это не работает - при использовании ESP без аутентификации и без AH). Далее, порядок выполнения действий (сначала шифрация, потом аутентификация) гарантирует быструю отбраковку "плохих" пакетов (более того, согласно последним исследованиям в мире криптографии, именно такой порядок действий наиболее безопасен, обратный порядок в некоторых, правда очень частных случаях, может привести к потенциальным дырам в безопасности; к счастью, ни SSL, ни IKE, ни другие распространенные протоколы с порядком действий "сначала аутентифицировать, потом зашифровать", к этим частным случаям не относятся, и, стало быть, этих дыр не имеют). Остается Denial-Of-
Service атака. Как известно, это атака, от которой не существует полной защиты. Тем не менее быстрая отбраковка

плохих пакетов и отсутствие какой-либо внешней реакции на них (согласно RFC) позволяют более-менее хорошо справляться с этой атакой. В принципе, большинству (если не всем) известным сетевым атакам (sniffing, spoofing, hijacking и т.п.) AH и ESP при правильном их применении успешно противостоят. С IKE несколько сложнее. Протокол очень сложный, тяжел для анализа. Кроме того, в силу опечаток (в формуле вычисления HASH_R) при его написании и не совсем удачных решений (тот же HASH_R и HASH_I) он содержит несколько потенциальных "дыр" (в частности, в первой фазе не все Payload в сообщении аутентифицируются), впрочем, они не очень серьезные и ведут, максимум, к отказу в установлении соединения.От атак типа replay, spoofing, sniffing, hijacking IKE более-менее успешно защищается. С криптографией несколько сложнее, - она не вынесена, как в AH и ESP, отдельно, а реализована в самом протоколе. Тем не менее, при использовании стойких алгоритмов и примитивов (PRF), проблем быть не должно. В какой-то степени можно рассматривать как слабость IPsec то, что в качестве единственного обязательного к реализации криптоалгоритма в нынешних спецификациях указывается DES (это справедливо и для ESP, и для IKE), 56 бит ключа которого уже не считаются достаточными. Тем не менее, это чисто формальная слабость - сами спецификации являются алгоритмо-независимыми, и практически все известные вендоры давно реализовали 3DES (а некоторые уже и AES).Таким образом, при правильной реализации, наиболее "опасной" атакой остается Denial-Of-Service.

Оценка протокола

Протокол IPSec получил неоднозначную оценку со стороны специалистов. С одной стороны, отмечается, что протокол IPSec является лучшим среди всех других протоколов защиты передаваемых по сети данных, разработанных ранее (включая разработанный Microsoft PPTP). По мнению другой стороны, присутствует чрезмерная сложность и избыточность протокола. Так, Niels Ferguson и Bruce Schneier в своей работе "A Cryptographic Evaluation of IPsec" отмечают, что они обнаружили серьёзные проблемы безопасности практически во всех главных компонентах IPsec. Эти авторы также отмечают, что набор протоколов требует серьёзной доработки для того, чтобы он обеспечивал хороший уровень безопасности. В работе приведено описание ряда атак, использующих как слабости общей схемы обработки данных, так и слабости криптографических алгоритмов.

Таблица – Сравнение IPSec и SSL

Особенности	**IPSec**	**SSL**
Аппаратная независимость	Да	Да
Код	Не требуется изменений для приложений. Может потребовать доступ к исходному коду стека TCP/IP.	Требуются изменения в приложениях. Могут потребоваться новые DLL или доступ к исходному коду приложений.
Защита	IP пакет целиком. Включает защиту для протоколов высших уровней.	Только уровень приложений.
Фильтрация пакетов	Основана на аутентифицированных заголовках, адресах отправителя и получателя, и т.п. Простая и дешёвая. Подходит для роутеров.	Основана на содержимом и семантике высокого уровня. Более интеллектуальная и более сложная.
Производительность	Меньшее число переключений контекста и перемещения данных.	Большее число переключений контекста и перемещения данных. Большие блоки данных могут ускорить криптографические операции и обеспечить лучшее сжатие.
Платформы	Любые системы, включая роутеры	В основном, конечные системы (клиенты/серверы), также firewalls.
Firewall/VPN	Весь трафик защищён.	Защищён только трафик уровня приложений. ICMP, RSVP, QoS и т.п. могут быть незащищены.
Прозрачность	Для пользователей и приложений.	Только для пользователей.
Текущий статус	Появляющийся стандарт.	Широко используется WWW браузерами, также используется некоторыми другими продуктами.

УРОВНИ В СТЕКЕ IP

В обоих случаях — как IPSec, так и SSL — речь идет о сетевых протоколах, находящихся, однако, на разных уровнях сетевого стека. IPSec работает на уровне IP и является самостоятельным типом IP, наподобие TCP или UDP (см. рисунок ниже). Если после успешной аутентификации строится зашифрованное соединение, то все типы протоколов над уровнем IP могут запаковываться в пакеты IPSec. На практике чаще всего ими становятся уже упомянутые протоколы TCP и UDP. Поскольку почти все приложения базируются на одном из них, виртуальная частная сеть с IPSec может быть универсальным образом сконфигурирована для любых вариантов.

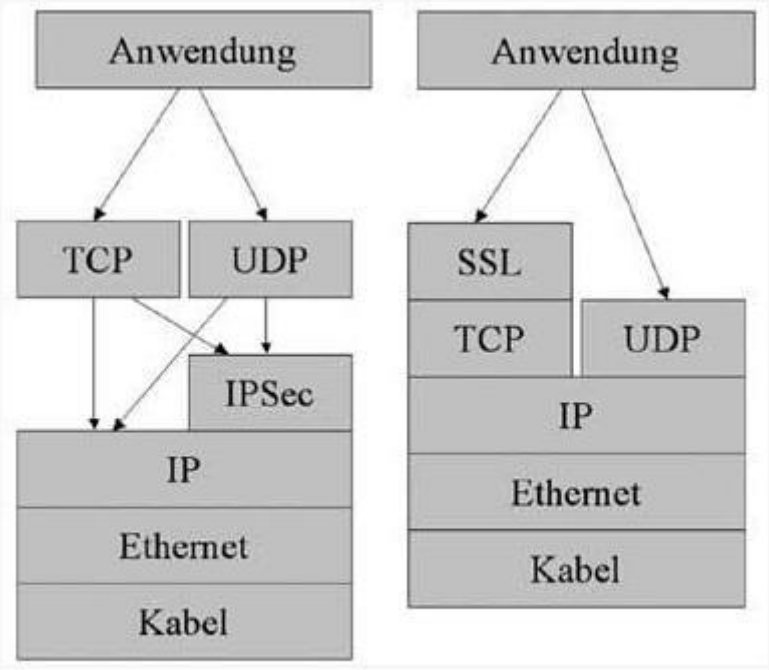

Рисунок - Сетевой стек IPSec (слева), сетевой стек SSL (справа). На примере Ethernet.

Несколько иначе выглядит ситуация с SSL. Хотя SSL в сетевом стеке и расположен над уровнем TCP, он все еще находится на транспортном уровне. Поэтому после построения аутентифицированного и зашифрованного соединения все базирующиеся на TCP приложения могут работать по каналу SSL. Коммуникацию по UDP, к примеру, при разрешении имени DNS, возможно выполнить с привлечением SSL лишь нетривиальным образом.

VPN (англ. Virtual Private Network — виртуальная частная сеть) — обобщённое название технологий, позволяющих обеспечить одно или несколько сетевых соединений (логическую сеть) поверх другой сети (например, Интернет). Несмотря на то, что коммуникации осуществляются по сетям с меньшим неизвестным уровнем доверия (например, по публичным сетям), уровень доверия к построенной логической сети не зависит от уровня доверия к базовым сетям благодаря использованию средств криптографии (шифрования, аутентификации, инфраструктуры открытых ключей, средств для защиты от повторов и изменений передаваемых по логической сети сообщений).

В зависимости от применяемых протоколов и назначения, VPN может обеспечивать соединения трёх видов: узел-узел, узел-сеть и сеть-сеть.

Сеть VPN состоит из четырех ключевых компонентов:

- Сервер VPN.
- Алгоритмы шифрования.
- Система аутентификации.
- Протокол VPN.

Эти компоненты реализуют соответствие требованиям по безопасности, производительности и способности к взаимодействию. То, насколько правильно реализована архитектура VPN, зависит от правильности определения требований. Определение требований должно включать в себя следующие аспекты.

- Количество времени, в течение которого необходимо обеспечивать защиту информации.
- Число одновременных соединений пользователей.
- Ожидаемые типы соединений пользователей (сотрудники, работающие из дома или находящиеся в поездке).
- Число соединений с удаленным сервером.
- Типы сетей VPN, которым понадобится соединение.

- Ожидаемый объем входящего и исходящего трафика на удаленных узлах.
- Политика безопасности, определяющая настройки безопасности.

VPN-сервер должен быть расположен в сети. Сервер может быть межсетевым экраном или пограничным маршрутизатором, что упрощает размещение VPN-сервера. В качестве альтернативы сервер может являться и отдельной системой. В этом случае сервер должен быть расположен в выделенной демилитаризованной зоне (DMZ). В идеальном случае демилитаризованная зона VPN должна содержать только VPN-сервер и быть отдельной от DMZ интернета, содержащей веб-серверы и почтовые серверы организации. Причиной является то, что VPN-сервер разрешает доступ ко внутренним системам авторизованным пользователям и, следовательно, должен рассматриваться как объект с большей степенью доверия, нежели почтовые и веб-серверы, доступ к которым может быть осуществлен лицами, не пользующимися доверием. Демилитаризованная зона VPN защищается набором правил межсетевого экрана и разрешает передачу только того трафика, который требует VPN.

Протокол VPN определяет, каким образом система VPN взаимодействует с другими системами в интернете, а также уровень защищенности трафика. При соединении рекомендуется использовать стандартные протоколы. В настоящее время стандартным протоколом для VPN является IPSec. Этот протокол представляет собой дополнение к IP, осуществляющее инкапсуляцию и шифрование заголовка TCP и полезной информации, содержащейся в пакете. IPSec также поддерживает обмен ключами, удаленную аутентификацию сайтов и согласование алгоритмов (как алгоритма шифрования, так и хэш-функции). IPSec использует UDP-порт 500 для начального согласования, после чего используется IP-протокол 50 для всего трафика. Для правильного функционирования VPN эти протоколы должны быть разрешены. С работой IPSec через межсетевые экраны связаны некоторые особенности. Во-первых, на межсетевом экране должен быть разрешен трафик UDP через порт 500 и последующий IP-трафик с протоколом 50. Возможность установки этих разрешений зависит от межсетевого экрана. Во-вторых, возникает вопрос, связанный с использованием трансляции межсетевых адресов (NAT). Если межсетевой экран осуществляет трансляцию адресов для пакетов при их поступлении из интернета во внутреннюю сеть, то ему нужно соответствующим образом транслировать конечный адрес, чтобы трафик достиг внутреннего клиента. Немногие межсетевые экраны способны выполнять эту функцию при работе с трафиком, не использующим порты UDP или TCP.

IPSec - это набор протоколов, с помощью которого поддерживается безопасный обмен информационными пакетами на IP-уровне. Так как IPSec работает на сетевом уровне, то он предоставляет безопасное средство передачи данных, способное поддерживать любое приложение, использующее IP.
IPSec предоставляет три способа обеспечения безопасности при передаче информации в сети:

- Аутентификация пакетов между отправляющим и принимающим устройствами.
- Сохранение целостности данных при транспортировке.
- Сохранение секретности данных при транспортировке.

IPSec работает в двух режимах: *транспортировочном* и в режиме *туннелирования*.

В **транспортировочном** режиме ESP (Encapsulation Security Protocol) и AHs (Authentication Headers) находятся в исходном IP-пакете между IP заголовком и расширенной информацией заголовка верхнего уровня.

В режиме **туннелирования** IPSec помещает исходный IP-пакет в новый IP-пакет и вставляет AH и ESP между IP-заголовком нового пакета и исходным IP-пакетом. Новый IP-пакет указывает направление к конечной точке туннеля, а исходный IP-пакет указывает пункт назначения пакета. Вы можете использовать режим туннелирования между двумя безопасными шлюзами, такими как серверы туннелирования, маршрутизаторы или межсетевые экраны.

IPSec-туннелирование является распространенным режимом. Оно работает следующим образом.

1. Стандартный IP-пакет посылается на IPSec-устройство, где он должен быть зашифрован и направлен в конечную систему по локальной сети.
2. Первое IPSec-устройство, которым в данном случае оказывается межсетевой экран или маршрутизатор, проводит аутентификацию принимающего устройства.
3. Два IPSec-устройства договариваются о шифре и алгоритме аутентификации, которыми будут пользоваться.
4. Отправляющее IPSec-устройство шифрует IP-пакет с информацией и помещает его в другой пакет с AH.
5. Пакет пересылается по TCP/IP-сети.
6. Принимающее IPSec-устройство читает IP-пакет, проверяет его подлинность и извлекает зашифрованное вложение для расшифровки.
7. Принимающее устройство отправляет исходный пакет в пункт его назначения.

Протокол PPTP

Протокол туннелирования от точки к точке (Point-to-Point Tunneling Protocol, PPTP) осуществляет безопасную пересылку данных от удаленного клиента на сервер организации. PPTP поддерживает многочисленные сетевые протоколы, включая IP, IPX и NetBEUI. Вы можете использовать протокол PPTP для создания безопасной виртуальной сети, в которой применяются dial-up-соединения, в рамках локальной сети LAN, WAN или в интернете и других сетях, в основе которых лежит протокол TCP/IP. Для создания PPTP-VPN необходим PPTP-сервер и PPTP-клиент.

Протокол L2TP (Layer Two Tunneling Protocol)

PPTP является технологией компании Microsoft для создания виртуальных каналов связи внутри коллективной сети. PPTP вместе с системами шифрования и аутентификации создает частную безопасную сеть. Компания Cisco Systems разработала протокол, аналогичный PPTP, под названием Layer Two Forwarding (L2F), но для его поддержки требуется оборудование Cisco на обоих концах соединения. Тогда Microsoft и Cisco объединили лучшие качества протоколов PPTP и L2F и разработали протокол L2TP. Как и PPTP, L2TP позволяет пользователям создать в интернете PPP-линию связи, соединяющую ISP и корпоративный сайт.