Протокол IPSec

Главная задача протокола IPSec это реализация безопасности передачи информации по сетям IP. IPSec гарантирует:

* целостность — при передачи данные не будут искажены, дублированы и потеряны
* конфиденциальность — предотвращает от несанкционированного просмотра
* аутентичность отправителя

Доступность — протокол не реализует, это входит в задачу протоколов транспортного уровня TCP. Реализуемая защиты на сетевом уровне делает такую защиту невидимой для приложений. Протокол работает на основе криптографических технологий:

* обмен ключами с помощью алгоритма Диффи-Хеллмана
* криптография открытых ключей для подлинности двух сторон, чтобы избежать атак типа «человек по середине»
* [блочное](http://infoprotect.net/note/Blochnoe_shifrovanie) шифрование
* алгоритмы аутентификации на основе хеширования

Протокол IPSec имеет следующие компоненты:

* Компоненты ESP и АН, работают с заголовками и взаимодействуют с базами данных SAD и SPD для обозначения политики безопасности для данного пакета
* Компонент обмена ключевых данных IKE
* SPD — база данных политик безопасности
* SAD — хранит список безопасных ассоциаций SA для исходящей и входящей информации

Ядро протокола IPSec составляет 3 протокола: AH (протокол аутентифицирующего заголовка), ESP (протокол инкапсулирующей защиты) и IKE (протокол согласования параметров управления ключами и виртуального канала). Архитектура стека протоколов IPSec показана на рис.7.

[](http://infoprotect.net/wp-content/uploads/2015/11/arhitektura-steka-protokolov-IPSec.jpg)

Рисунок — 7, архитектура стека протоколов IPSec

Протокол АН ответственен только за реализацию аутентификации и целостности информации, в то время как протокол ESP и реализует функции АН и алгоритмы шифрования. Протоколы **IKE, AH и ESP** работают следующим образом.

С помощью протокола IKE создается логическое соединение между 2 точками, которое имеет название **безопасная ассоциация** SA. При реализации такого алгоритма, происходит аутентификация конечных точек линии, и выбираются параметры защиты информации. В рамках созданной безопасной ассоциации SA стартует протокол AH или ESP, которые реализуют нужную защиту и передачу данных.

Нижнй уровень архитектуры основан на домене интерпретации DOI. Протоколы AH и ESP основаны на модульной структуре, разрешая выбор пользователю относительно используемых алгоритмов шифрования и аутентификации. Именно DOI согласует все моменты, и адаптирует IPSec под выбор пользователя.

Формат заголовка пакета AH и ESP показаны на рис.8. Протокол АН защищает весь IP-пакет, кроме полей в Ip-заголовке и поля TTL и типа службы, которые могут модифицироваться при передаче в сети.

[](http://infoprotect.net/wp-content/uploads/2015/11/Format-zagolovkov-AH-i-ESP.jpg)Рисунок — 8, формат заголовков AH и ESP

Протокол АН может работать в 2 режимах: транспортном и туннельном. Местоположение заголовка АН зависит от того, какой режим был задействован. В **транспортном режиме** заголовок исходного IP-пакета становится внешним заголовком, затем уже заголовок АН. В таком режиме IP-адрес адресата/адресанта читабелен третьим лицам. **В туннельном режиме** в качестве заголовка внешнего IP-пакета создается новый заголовок. Это видно на рис.9. Также на рис.10 можно увидеть 2 режима работы протокола ESP. Более подробно об этих протоколах реализации протокола IPSec можно прочитать, к примеру в работе Шаньгина В.Ф. — «Защита информации в компьютерных системах и сетях».

[](http://infoprotect.net/wp-content/uploads/2015/11/rezhimy-primeneniya-zagolovka-AN.jpg)Рисунок — 9, режимы применения заголовка АН

[](http://infoprotect.net/wp-content/uploads/2015/11/rezhimy-primeneniya-ESP.jpg)Рисунок — 10, режимы применения ESP

IPSec разрешает защитить сеть от множества сетевых атак, откидывая чужие пакеты до того, как они дойдут к уровню IP на узле. На узел могут войти те пакеты, которые приходят от аутентифицированных пользователей.

Протоколы SSL и TLS

Сразу нужно отметить, что это один и тот же протокол. Сначала был SSL, но его однажды взломали. Его доработали и выпустили TLS. Конфиденциальность реализуется шифрованием данных с реализацией симметричных сессионных ключей. Сессионные ключи также шифруются, только на основе открытых ключей взятых из сертификатов абонентов. Протокол SSL предполагает следующие шали при установки соединения:

* аутентификация сторон
* согласование криптоалгоритмов для реализации
* создание общего секретного мастер-ключа
* генерация сеансовых ключей на основе мастер-ключа

Процесс аутентификации клиента сервером с помощью протокола SSL виден на рис.11.

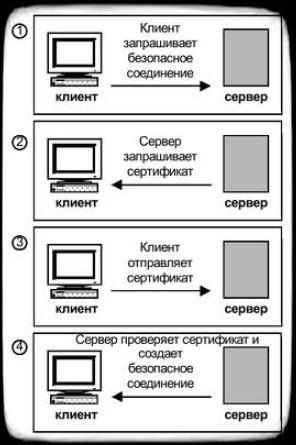
[](http://infoprotect.net/wp-content/uploads/2015/11/Protsess-autentifikatsii-klienta-serverom-s-pomoshhyu-protokola-SSL.jpg)

Рисунок — 11

К недостаткам TLS и SSL относят то, что они работают только с одним протоколом сетевого уровня — IP.

Протокол SSL обеспечивает решение двух задач — шифрование передаваемой информации и передача информации именно туда, куда требуется (аутентификация). Основное назначение протокола — предоставление надежного способа обмена данными между приложениями. Реализация SSL выполнена в виде многослойной среды, которая используется для безопасной передачи информации посредством незащищенных каналов связи.

Многослойная структура представлена слоем протокола подтверждения подключения и слоем протокола записи. Первым слоем выступает транспортный протокол, например, TCP — вместе с SSL Record Protocol данные слои образуют ядро SSL, которое впоследствии участвует в формировании сложных инфраструктур.

Среди основных особенностей протокола SSL следует отметить программно-платформенную независимость. В настоящее время протокол SSL не обеспечивает должную защиту — на смену ему пришел протокол TLS.

В протоколе TLS используются следующие алгоритмы:

* RC4, Triple DES, SEED, IDEA и др. для симметричного шифрования.
* RSA, DSA, Diffie-Hellman и ECDSA для проверки подлинности ключей.
* MD5, SHA и SHA-256/384 для хэш-функций.

Приложения осуществляют обмен записями, которые хранят в себе данные. Записи могут быть сжаты, дополнены, зашифрованы или же идентифицированы. При этом в каждой записи указываются данные о длине пакета и используемой версии TLS.

В общем случае применение криптографии в протоколах SSL/TLS значительно снижает производительность приложений, зато обеспечивает надежную защиту передачи данных. Протоколы не требуют практически никаких настроек с клиентской стороны, считаются самыми распространенными протоколами защиты в сети интернет.