Протокол IPSec

IPsec

Набор протоколов для обеспечения защиты данных, передаваемых по межсетевому протоколу IP

Позволяет осуществлять подтверждение подлинности и/или шифрование IP-пакетов.

IPsec

- Протокол Kerberos применяется для аутентификации участников соединения.
- Но и после этапа аутентификации данные, передаваемые по сети, следует защищать.
- Стандартные протоколы стека TCP/IP, такие, как IP, TCP, UDP, не обладают встроенными средствами защиты.

IPsec

- В 1994 году Совет по архитектуре Интернета (Internet Architecture Board, IAB), издал RFC 1636 «*Report of IAB Workshop on Security in the Internet Architecture» («Отчет семинара IAB по безопасности в* архитектуре Интернета»).
- Инициированная этим сообщением работа привела к появлению протокола *IPsec (IP Security), описанного в* нескольких стандартах RFC (в частности, в RFC 2401-2412).

IPsec

- Новая технология безопасности является необходимой частью протокола IPv6, а также может применяется и в сетях IPv4.
- Протокол IPsec действует на сетевом уровне модели OSI и может применяться независимо от протоколов верхнего уровня, т. е. прикладной протокол может использовать IPsec, считая, что работает с обычным протоколом IP.
- При этом данные протоколов верхних уровней упаковываются в пакеты IPsec, которые, в свою очередь, помещаются в пакеты протокола IP.

Функции протокола IPsec

Протокол IPsec обеспечивает наличие следующих функций:

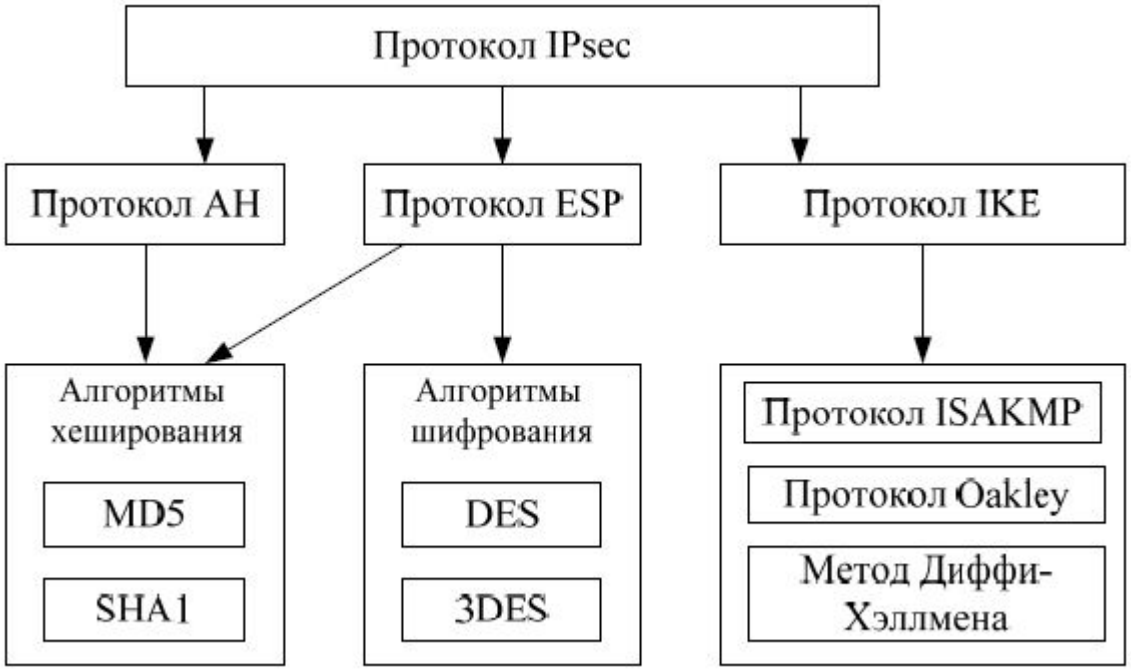
- Аутентификация – приемник пакетов в состоянии проверить подлинность их источника;
- Целостность – осуществляется контроль того, что данные дойдут до получателя в неизменном виде;
- Конфиденциальность – шифрование данных обеспечивает их недоступность для несанкционированного просмотра;
- Распределение секретных ключей – для правильной работы протокола IPsec необходимо автоматически обеспечивать источник и приемник пакетов секретными ключами для шифрования и расшифрования данных.

Функции протокола IPsec

Для реализации представленных функций используются три основных протокола:

- AH (Authentication Header – заголовок аутентификации) обеспечивает целостность и аутентичность;
- ESP (Encapsulating Security Payload – инкапсуляци зашифрованных данных) предоставляет функции целостности, аутентичности и конфиденциальности (шифрование);
- IKE (Internet Key Exchange – обмен ключами Интернета) генерирует и распределяет секретные ключи.

Структура протокола IPsec



Протокол AH

Протокол AH (описан в RFC 2402) снабжает пакет IPsec своим незашифрованным заголовком, который обеспечивает:

- Аутентификацию исходных данных;
- Целостность данных;
- Защиту от дублирования уже полученных данных.

Протокол AH

Первые две функции протокола AH реализуются путем применения алгоритмов хеширования (MD51 или SHA12) к исходным данным.

- Процедура хеширования осуществляется источником с помощью секретного ключа, который был выдан источнику и приемнику пакета с использованием протокола IKE.
- Полученное значение хеша помещается в специальное поле заголовка AH. Приемник также осуществляет процедуру хеширования, применяя тот же секретный ключ.
- В том случае, если вычисленный хеш совпадает с хешем, извлеченным из пакета, данные считаются аутентифицированными и целостными. Иначе пакет в процессе передачи подвергся каким-либо изменениям и не является правильным.

Протокол AH

- Функция защиты от дублирования уже полученных пакетов осуществляется с помощью поля номера пакета в заголовке AH.
- В это поле источник заносит значение счетчика, увеличивающееся при отправке каждого пакета на единицу.
- Приемник отслеживает номера получаемых пакетов, и, если такой номер совпадает с недавно полученным, пакет отбрасывается.

Протокол ESP

- Протокол ESP решает задачи, подобные протоколу AH, – обеспечение аутентификации и целостности исходных данных, а также защиту от дублирования пакетов.
- Кроме того, протокол ESP предоставляет средства обеспечения конфиденциальности данных при помощи алгоритмов шифрования.
- Задачи аутентификации, целостности и защиты от дублирования решаются теми же методами, что и в протоколе AH.
- Передаваемый пакет, за исключением нескольких служебных полей, шифруется с применением алгоритмов шифрования DES и 3DES (DES с тремя ключами).

Протокол IKE

- Управление секретными ключами в протоколе IPsec осуществляется при помощи протокола IKE (описан в RFC 2409).
- Данный протокол основан на двух протоколах: 1. ISAKMP (Internet Security Association and Key Management Protocol – протокол межсетевой ассоциации защиты и управления ключами)

  2. Протокол определения ключей Оакли (Oakley Key Determination Protocol).

Протокол IKE

- Протокол IKE устанавливает соединение между двумя узлами сети, называемое *безопасной ассоциацией (Security Association, SA).*
- *Безопасная* ассоциация обеспечивает передачу защищенных данных только в одну сторону, поэтому для установки двустороннего соединения требуется определить две безопасные ассоциации.
- Для аутентификации узлов безопасной ассоциации, согласования между ними методов хеширования и шифрования IKE использует протокол ISAKMP (описан в RFC 2408).

Протокол IKE

- Для генерации и обмена секретными ключами IKE использует протокол определения ключей Оакли (описан в RFC 2412), разработанный на основе метода обмена ключами Диффи-Хэллмена (Diffie-Hellman).
- В этом методе секретный ключ генерируется на двух узлах путем обмена двумя числами через открытую сеть. При этом перехват чисел не даст информации о ключах.