Защита информации

Павел Юдаев

МГТУ им. Баумана, Кафедра ИУ-9

Москва, 2014

Раздел 17 - Протокол IPsec

Сначала: вся сеть в одном здании. Ограничение доступа - физические замки.
Соединить два соседних здания - отдельный провод.
Соединить сети на разных концах континента - как?

История разработки IPsec:

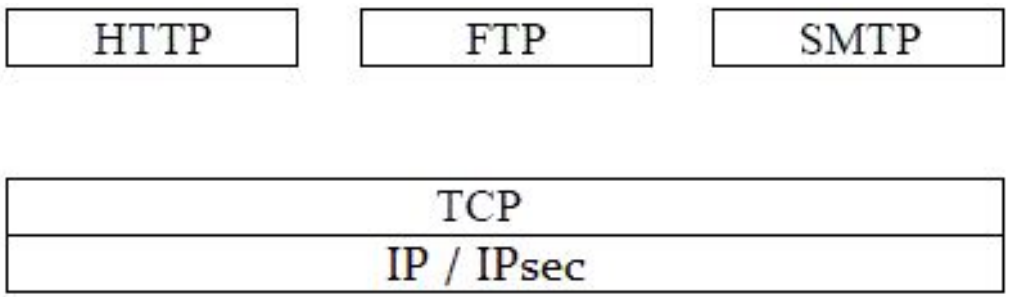
1993, Software IP Encryption protocol *swIPe* - Columbia University и AT&T Bell Labs
1994, Gauntlet firewall - первый реальный VPN между двумя подсетями в США.
1993, IP ESP - проект DARPA (параллельно с AT&T)
1995, начало разработки открытого стандарта в IETF
1998, RFC 2401 - первый стандарт IPsec.

Сейчас: около 30 документов IETF.

Цели IPsec:

- Конфиденциальность и/или целостность передачи информации между серверами
- Защита от вопроизведения
- Аутентификация источника данных
- Контроль доступа

Предоставить этот сервис для всех соединений поверх IP/IPsec.



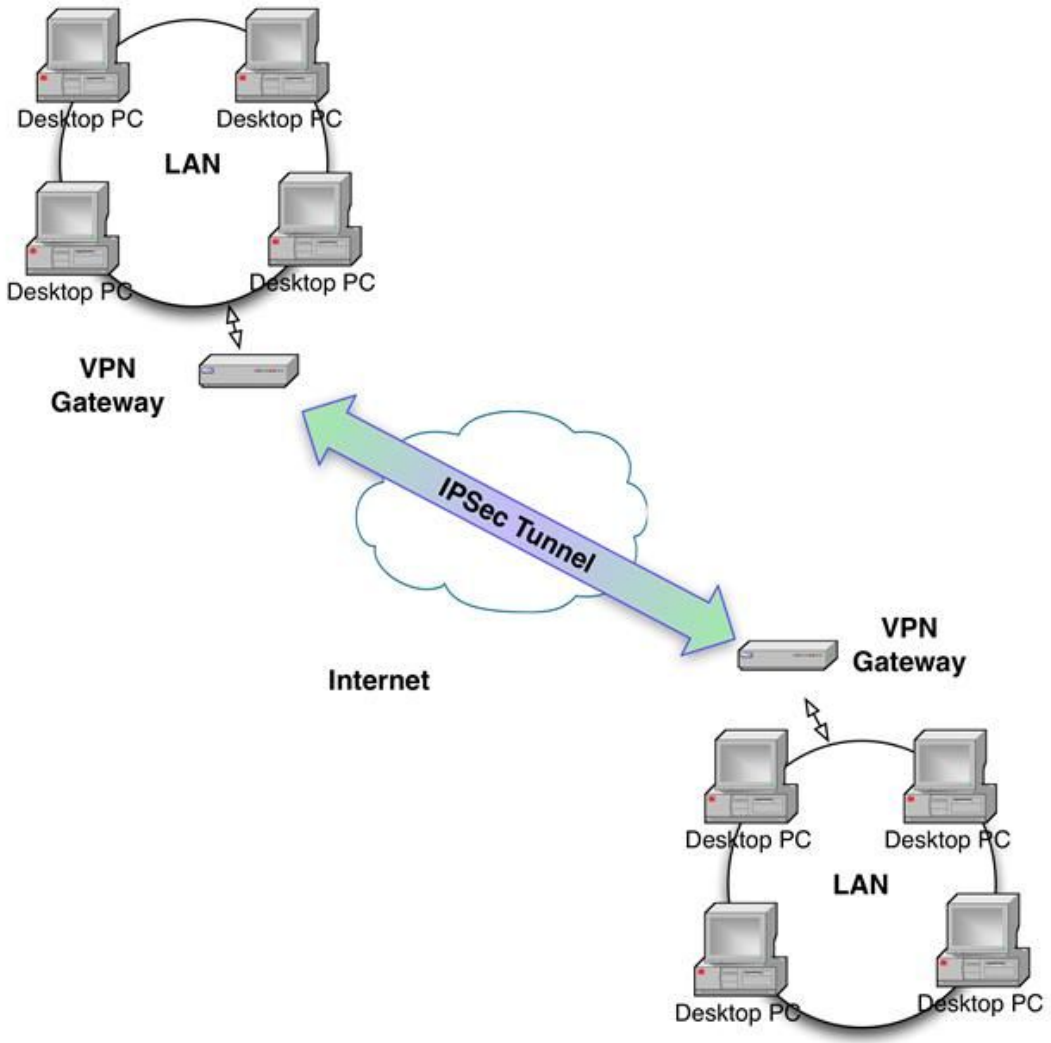
Протоколы:

- обеспечение только целостности - Authenticated Header (AH), RFC 2402
- шифрование и контроль целостности - Encapsulation Security Payload (ESP), RFC 2406

Режимы:

- транспортный (точка-точка, защита содержимого IP датаграммы)
- туннельный (gateway-gateway, защита всей IP датаграммы)

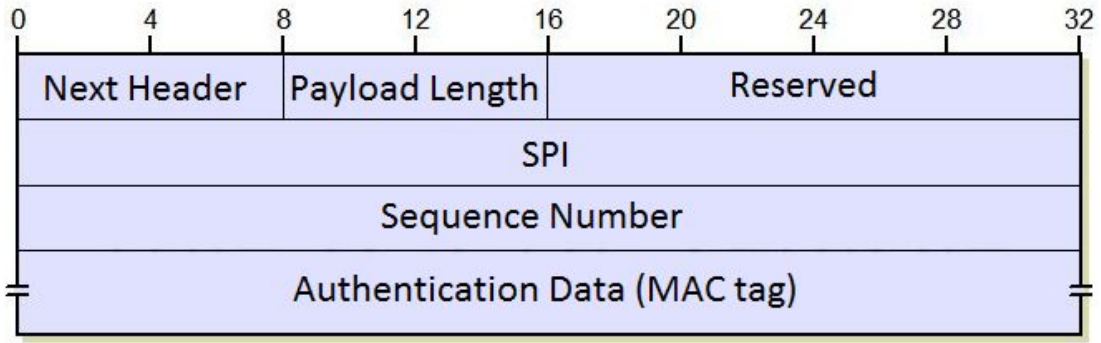
IPsec VPN



(Источник: [1])

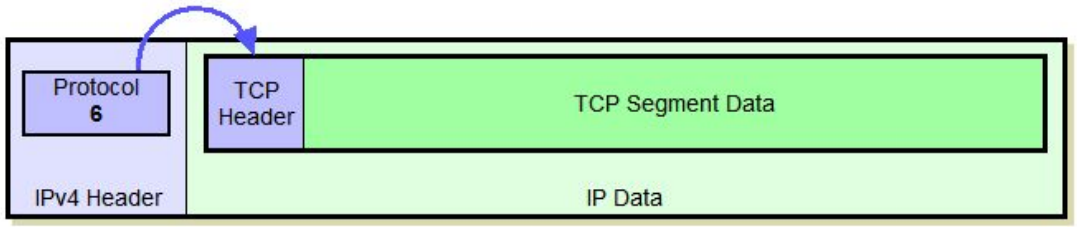
Протокол Authenticated Header

Authenticated Header

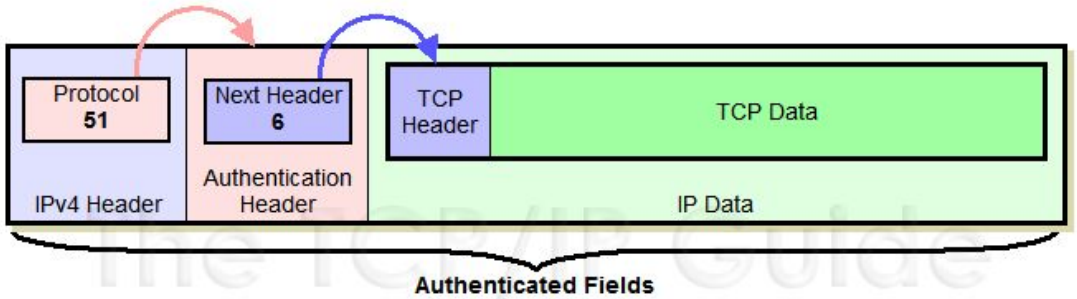


- Next Header - номер протокола следующего заголовка.
- Payload Length - длина этого заголовка AH минус 2.
- Resered - не используется, 0
- SPI - security parameter index, уникальный индекс SA (позже).
- Seq No - счетчик сообщений, отправленных с этой SA.
- Authentication Data - MAC тэг от всех неизменных частей IP заголовка, AH заголовка, и данных.

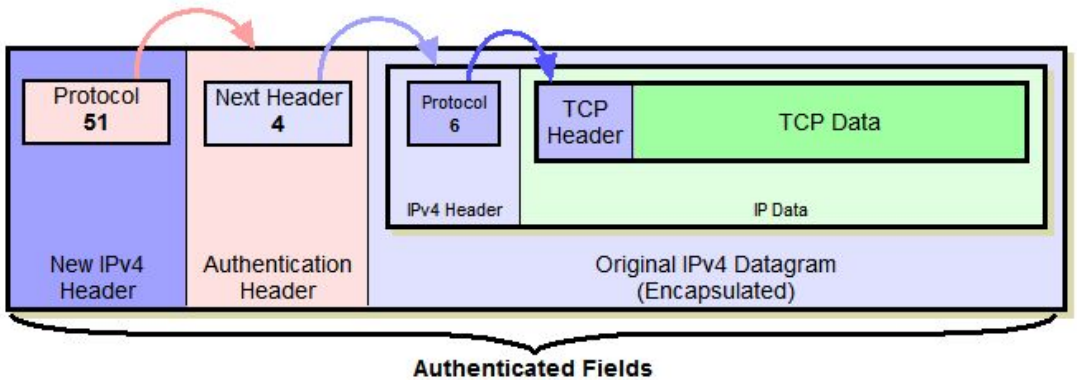
Создание AH в туннельном и транспортном режимах.



Original IPv4 Datagram Format



IPv4 AH Datagram Format - IPSec Transport Mode



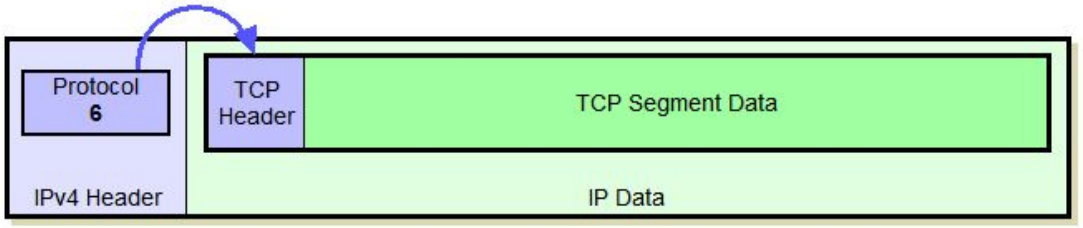
IPv4 AH Datagram Format - IPSec Tunnel Mode

(Источник: [2])

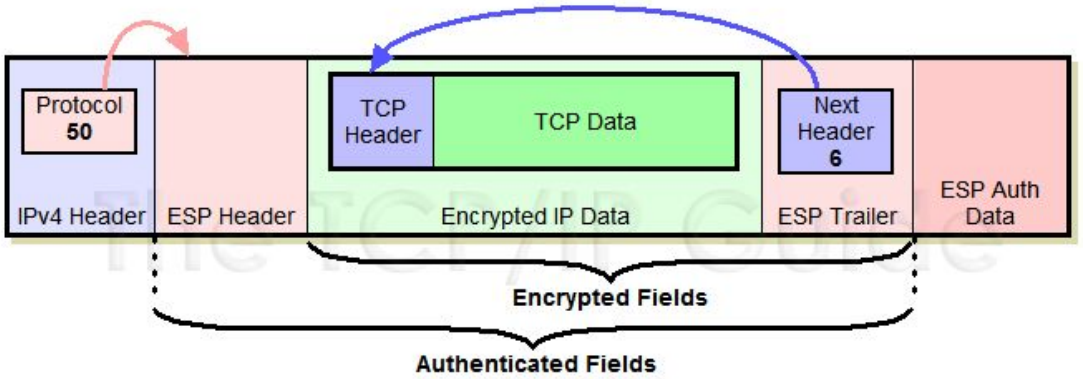
Протокол Encapsulation Security Payload

ESP Envelope включает в себя

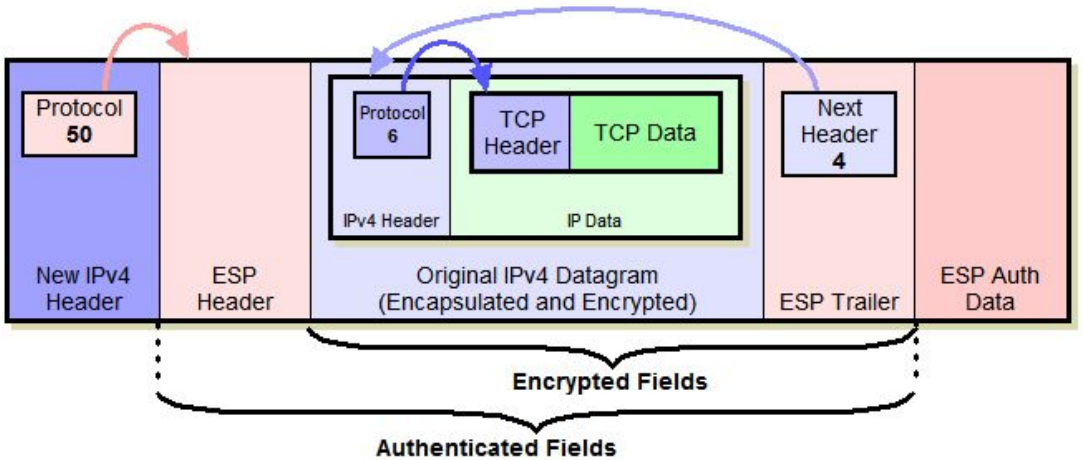
1. ESP Header:
   - SPI - уникальный индекс SA (позже).
   - Seq No - счетчик сообщений, отправленных с этой SA.
2. Payload - данные.
3. ESP Trailer:
   - Padding - для шифра, 0..255 байт.
   - Pad Length - число байт в Padding.
   - Next Header - номер протокола заголовка в Payload.
4. ESP Authentication Data - MAC тэг по всему ESP Envelope.



Original IPv4 Datagram Format



IPv4 ESP Datagram Format - IPSec Transport Mode



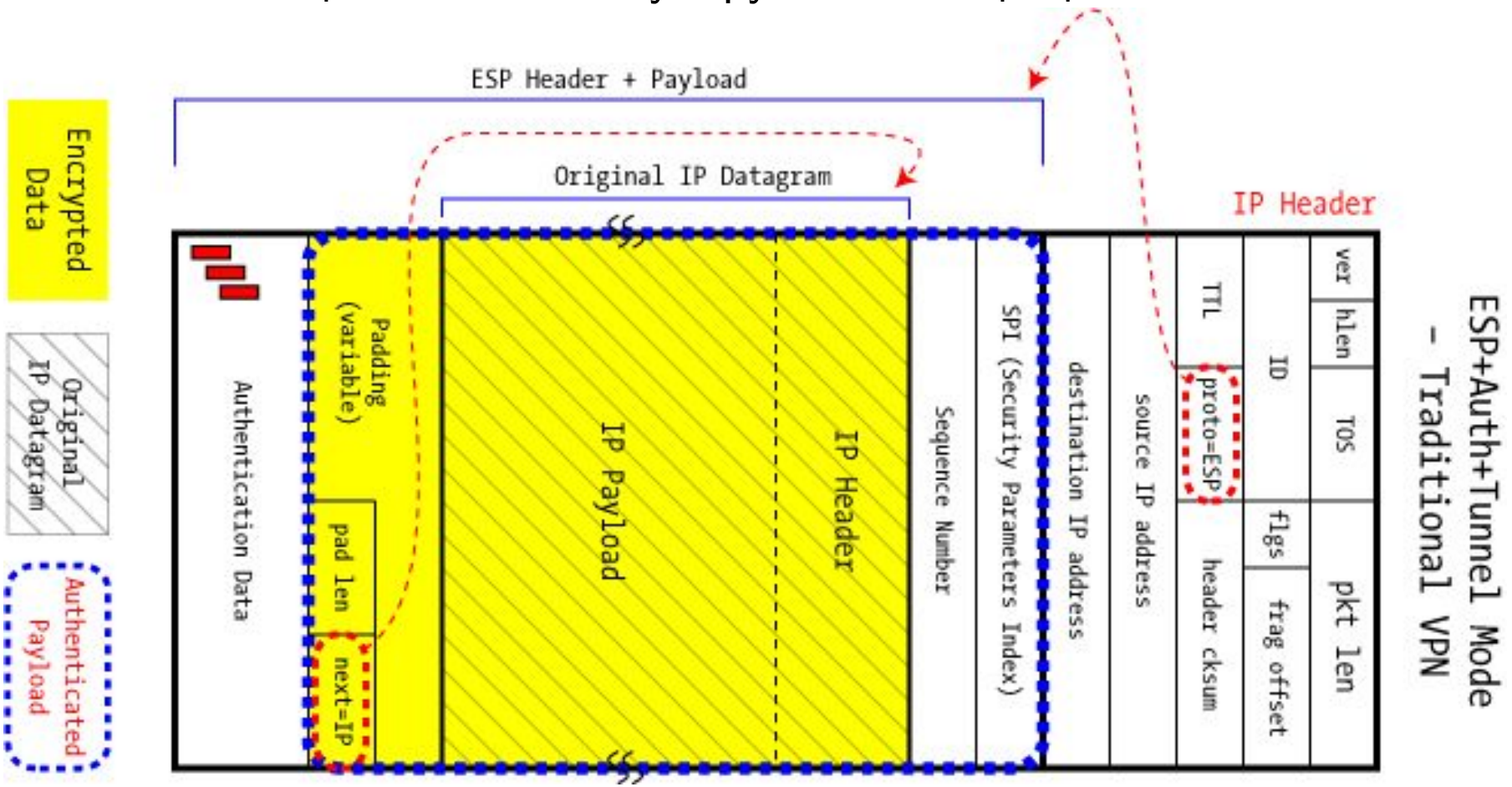
IPv4 ESP Datagram Format - IPSec Tunnel Mode

ESP: настройки определяют, какое использовать шифрование (или без него) и MAC (или без него). EtM режим.

Можно комбинировать AH и ESP.

VPN: IPsec, туннельный режим, ESP с шифрованием и MAC.

T.e. IP пакет целиком инкапсулируется и защищается.



(Источник: [4])

Security Association - набор параметров IPsec.

SA - односторонняя. Две для соединения.
Можно настроить вручную или автоматически (Internet Key Exchange protocol)

Некоторые параметры SA:

- IP адрес отправителя
- IP адрес получателя
- режим (туннельный, транспортный)
- шифр, ключ шифра
- MAC, ключ MAC

  ...

Некоторые параметры SA: (*)

- IP адрес отправителя
- IP адрес получателя
- режим (туннельный, транспортный)
- шифр, ключ шифра
- MAC, ключ MAC
- флаг защиты от воспроизведения
- счетчик сообщений
- время жизни SA в секундах
- время жизни SA в байтах
- **SPI** - индекс локальной базы данных

Шифр, MAC, защита от воспроизведения могут не использоваться (null).

Раздел 17 - Протокол IPsec

IKE - internet key exchange

Методы авторизации сторон:

1. Pre-shared key. Симметричный секретный ключ может быть задан вручную при настройке соединения.

2. Сертификат (ЭЦП).

3. Асимметричное шифрование.

Обозначения:

I - инициатор
R - отвечает на запрос

HDR - заголовок: тип режима (основной, агрессивный) и т.д.
EHAO - предложение SA (encryption, hash, authentication offer)
EHAS - выбор SA
GRP - описание группы G для протокола Диффи-Хеллмана
g - генератор (под)группы G
x, y - секретные значения в протоколе Диффи-Хеллмана
Nz - nonce стороны z
ID(Z) - IP адрес Z и другие данные.
AUTH - HMAC(pre-shared key || Ni || Nr, $\cdot$) или ЭЦП, в зависимости от настроек протокола.

Фаза 1. Цель - взаимная авторизация и создание первичного ключа для SA фазы 2.

(*) Основной режим. ID сторон не разглашаются.

1. I→R: HDR, EHAO, GRP.
2. R→I: HDR, EHAS, GRP.

Каждая сторона сохраняет по две SA и SPI.

3. I→R: HDR, g^x, Ni
4. R→I: HDR, g^y, Nr.

I, R: вычислить k := HMAC(Ni || Nr, g^{xy}).

5. I→R: HDR, E_k(ID(I) || [CERT(I)],
AUTH(ID(R) || ID(I) || Nr || Ni || GRP || g^y || g^x || EHAS)).
6. R→I: HDR, E_k(ID(R) || [CERT(R)],
AUTH(ID(I) || ID(R) || Nr || Ni || GRP || g^y || g^x || EHAS)).

[XX] - опциональные данные.

100 мс (pre-shared key, 2005 год); 170 мс (RSA, 2005 год)

(*) DoS (clogging) attack:
Запросы с подмененным IP, равным IP I
=> сервер R вычисляет ключи DH, загружает ЦП.

Решение: протокол OAKLEY, RFC 2412.

CKY(I) - cookie I, псевдослучайное число. Не меняется в одном соединении. Также CKY(R).

Изменение: HDR = CKY(I) || CKY(R) || тип режима
и k := HMAC(Ni || Nr, g^{xy} || CKY(I) || CKY(R)).

Cookies предотвращают DoS атаки без MitM: теперь в третьем сообщении должно быть то же самое CKY(R).

Агрессивный режим: (это мы рассм.)

1. I→R: HDR, EHAO, GRP, g^x, Ni, ID(I), [CERT(I)]
2. R→I: HDR, EHAS, GRP, g^y, Nr, ID(R), [CERT(R)], AUTH(ID(R) || ID(I) || Nr || Ni || GRP || g^y || g^x || EHAS || [CERT(R)])
3. I→R: HDR, AUTH(ID(I) || ID(R) || Nr || Ni || GRP || g^y || g^x || EHAS || [CERT(I)])
4. I, R: вычислить k := HMAC(Ni || Nr, g^{xy}). Это master secret (первичный ключ).

ID сторон разглашаются, но это не очень важно.

Фаза 2. Цель - создание сессионных ключей.

Perfect Forward Secrecy

Временный ключ - ключ для одной SA. Они выводятся из первичного ключа, который создан на фазе 1.

Совершенная прямая секрестность:
1) если один временный ключ скомпрометирован, ни постоянный ключ, ни другие временные ключи не могут быть найдены.
2) если постоянный ключ скомпрометирован, временные ключи не могут быть найдены.

Это одна из опций IPsec, TLS 1.2, SSH v2.

Для PFS создаем новый секрет DH на фазе 2. Когда SA фазы 2 устаревает, повторяется только фаза 2, не фаза 1.

SA для этой фазы установлена в результате фазы 1, защищает обмен данными.

1. I→R: HDR, E_k([ID(I)], [ID(R)], SPI для исходящей SA, EHAO, Ni, [g^x])

2. R→I: HDR, E_k([ID(I)], [ID(R)], SPI для исходящей SA, EHAS, Nr, [g^y])

3. I→R: HDR, E_k(MAC_k([ID(I)], [ID(R)], SPI(I), SPI(R), EHAO, EHAS, Ni, Nr, [g^x], [g^y])

4. I,R: k := HMAC(Ni || Nr, g^{xy}) - сессионный ключ.
Источник: [5, 6].

Раздел 17 - Протокол IPsec

Достоинства IPsec

- Конфиденциальность данных, защита от изменений и воспроизведения.
- L3 OSI. Предоставляет защищенный сетевой уровень для любого транспорта или приложения. Они могут и не знать об этом.
- Транспортный режим (точка - точка), туннельный режим (gateway - gateway)
- Поддерживает много протоколов управления ключами
- Большинство VPN используют IPsec
- Может использоваться в Kerberos

Недостатки IPsec

- Специальный режим для NAT. (Усложнение.)
- L3, поэтому изменения в протоколе - изменения в ядре.
- Аутентификация устройства (хоста или gateway), а не пользователя.
- Неявное начало, ведение и завершение сессии. Приложения не знают, предоставляется ли этот сервис.
- Нет контроля потери связи. (Отдан протоколам выше в стеке OSI.)
- Нет функции контроля доступа для приложений. Вся машина - часть сети VPN.
- Запутанная конфигурация IPsec и IKE. (Специалисты по Cisco?)

Литература к лекции

1. Tom Olzak, *Enterprise Security. Chapter 9: Securing remote access* http://resources.infosecinstitute.com/securing-remote-access/. Также использованы изображения для IPsec.

2. *IP Security (IPSec) Protocols* http://www.tcpipguide.com/free/t_IPSecurityIPSecProtocols.htm Также использованы изображения для IPsec.

3. Avi Kak, *PGP, IPSec, SSL/TLS, and Tor Protocols* https://engineering.purdue.edu/kak/compsec/NewLectures/Lecture20.pdf

4. http://www.unixwiz.net/techtips/iguide-ipsec.html

5. Jie Qian, Ben Smeets, *IPSec and OpenVPN worked-out examples* - Анализ пакетов IPsec в программе Wireshark: http://ipseclab.eit.lth.se/tiki-index.php?page=5.+IPSec

6. Alshamsi, Saito, *A Technical Comparison of IPSec and SSL* http://eprint.iacr.org/2004/314.pdf

7. Eric Rescorla, *SSH, SSL, and IPsec: wtf?* http://cseweb.ucsd.edu/classes/fa08/cse127/rescorla-comsec.pdf

тж. http://www.webeks.net/information-systems/oakley-key-exchange-protocol.html

см. тж. картинки в https://www-rnks.informatik.tu-cottbus.de/content/unrestricted/materials/ws2002seRecent/neumann.pdf