ETU "LETI"
SAINT PETERSBURG ELECTROTECHNICAL UNIVERSITY

ОСНОВЫ ПОСТРОЕНИЯ ЗАЩИЩЕННЫХ КОМПЬЮТЕРНЫХ СЕТЕЙ

Виртуальные частные сети

Виртуальные частные сети

Защищенной виртуальной частной сетью– называется объединение локальных сетей и компьютеров, с территориально удаленными сетями через открытую внешнюю среду передачи данных, обеспечивающую безопасность информационного потока за счет использования механизмов туннелирования.

Преимущества:

•защита данных за счет использования механизмов шифрования

•анонимность в сети и обход ограничений при использовании стороннего IP-адреса и шифрования трафика

•доступ к удалённым ресурсам при организации соединение между этими устройствами в условиях публичной сети.

Ограничения:

•задержки сети чем удаленнее сервер, тем выше задержка передачи данных между клиентом и конечным ресурсом.

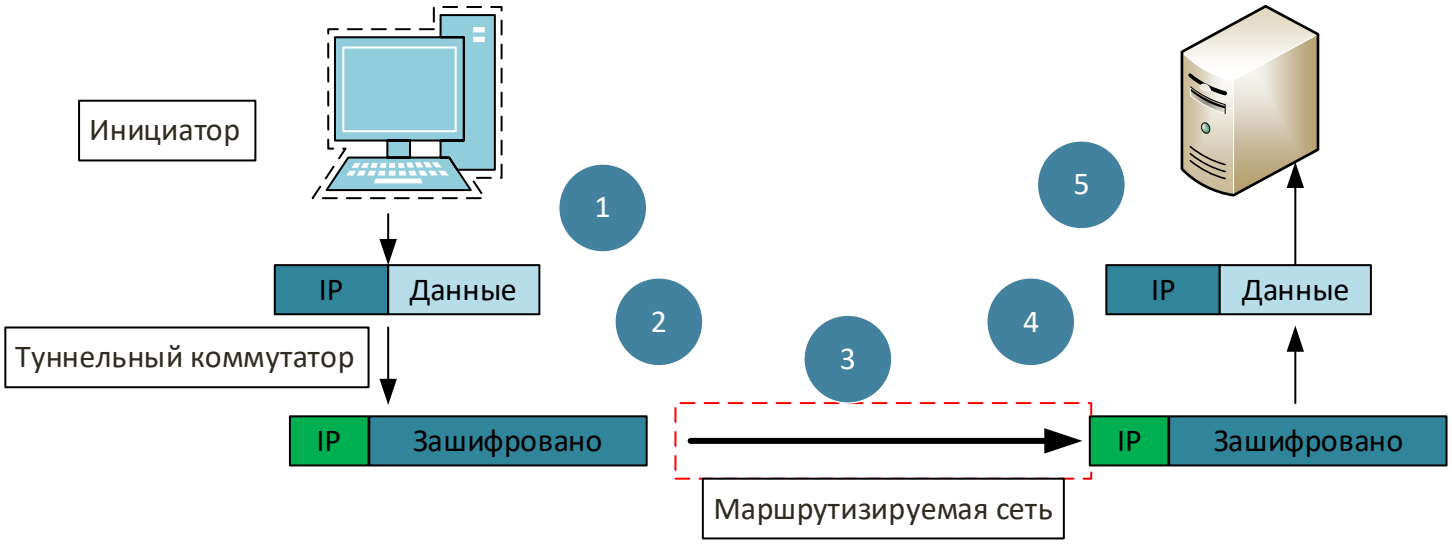
•снижение пропускной способности сети за счет криптографической обработки проходящих данных.

•релевантность запросов в поиске при неправильной идентификации пользователя.

Технология туннелирования

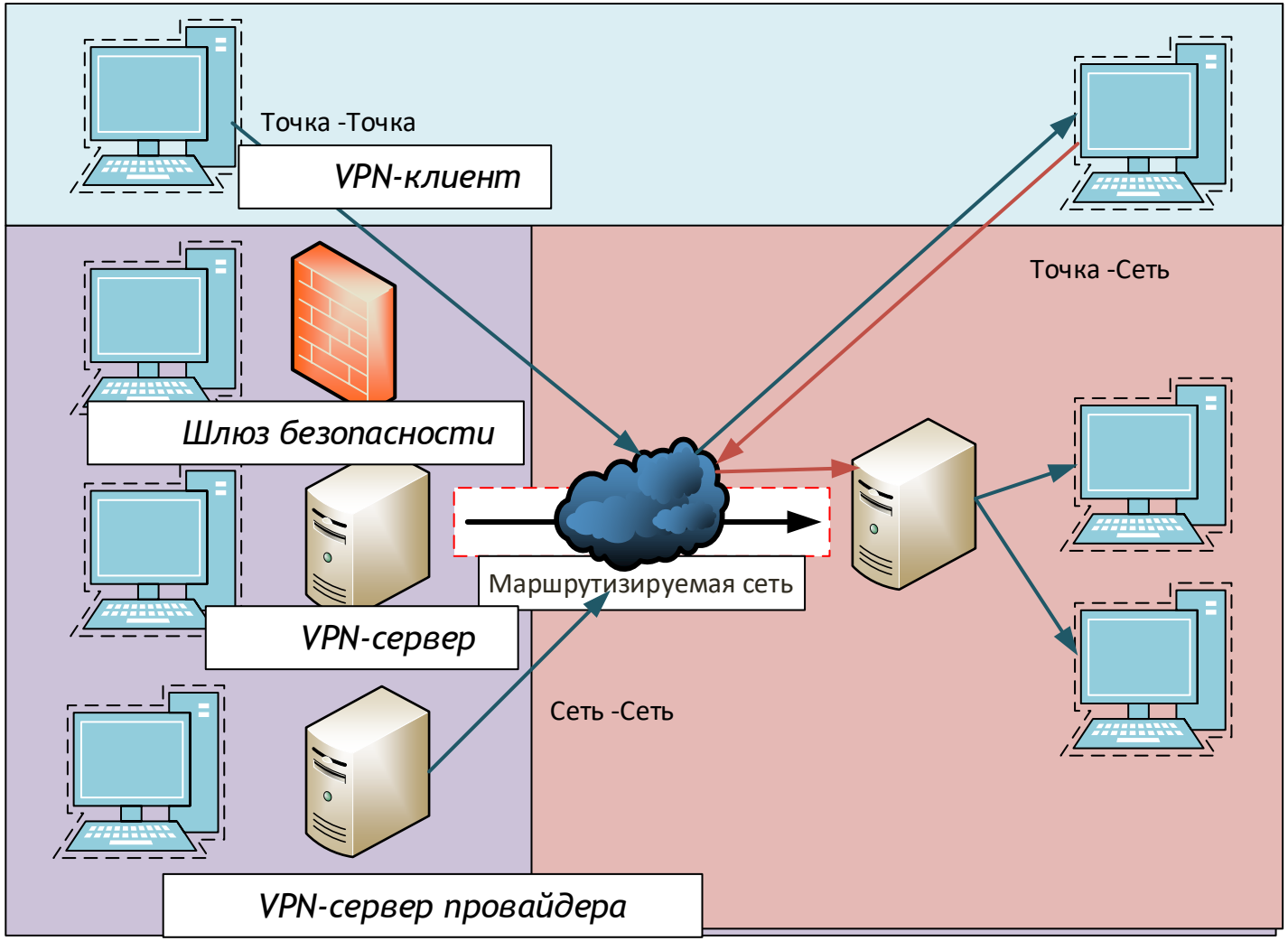
Туннель VPN туннель представляет собой логическое соединение, позволяющее инкапсулировать данные одного протокола в пакеты другого.

1. Инициатором осуществляется формирование сообщение подлежащее защите.
2. Полученное сообщение более низкого уровня шифруется вместе с заголовком и помещается в поле данных пакета протокола более высокого или такого же уровня и передается по сети (сокрытие информации и IP-адреса).
3. Осуществляется передача по сети
4. При получении пакета из него извлекается и расшифровывается внутренний исходный пакет.
5. Происходит передача информации по внутренней сети.



Виртуальные частные сети

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



Классификация виртуальных частных сетей

Протоколы

•PPTP поддерживается всеми системами, имеет максимальную производительность, но имеет слабую защиту.

• L2TP поддерживается всеми распространёнными операционными системами, осуществляется двойное инкапсулирование данных.

• OpenVPN - один из самых популярных протоколов, шифрование которого реализуется за счёт использования библиотеки OpenSSL.

•SSTP -надежный протокол, сравнимый по уровню безопасности с OpenVPN. Отсуствует поддержка на Android или IOS.

•IKEv2 производителен и работает быстрее OpenVPN. Поддерживается на большинстве операционных систем. Кроме того, подключение к серверу автоматически восстанавливается в случае обрыва сети, возможно использование на мобильных системах.

Канальный уровень

На канальном уровне могут использоваться протоколы туннелирования данных L2TP и PPTP.

Свойства протокола PPTP

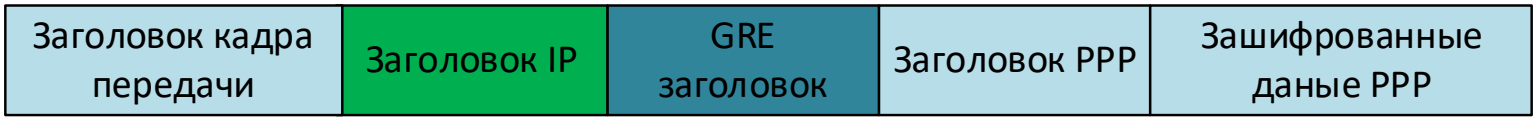
- Позволяет инкапсулировать пакеты PPP в пакеты протокола IP и передавать их по сетям IP, прост в настройке, прозрачен для пользователя.

- Использует TCP-соединение для обслуживания туннеля.
- Для шифрования трафика используется MPPE (Microsoft Point-to-Point Encryption).
- Для аутентификация клиентов могут использоваться различные механизмы PAP MSCHAPv2 и EAP-TLS.
- Клиент PPTP встроен почти во все операционные системы.

Канальный уровень

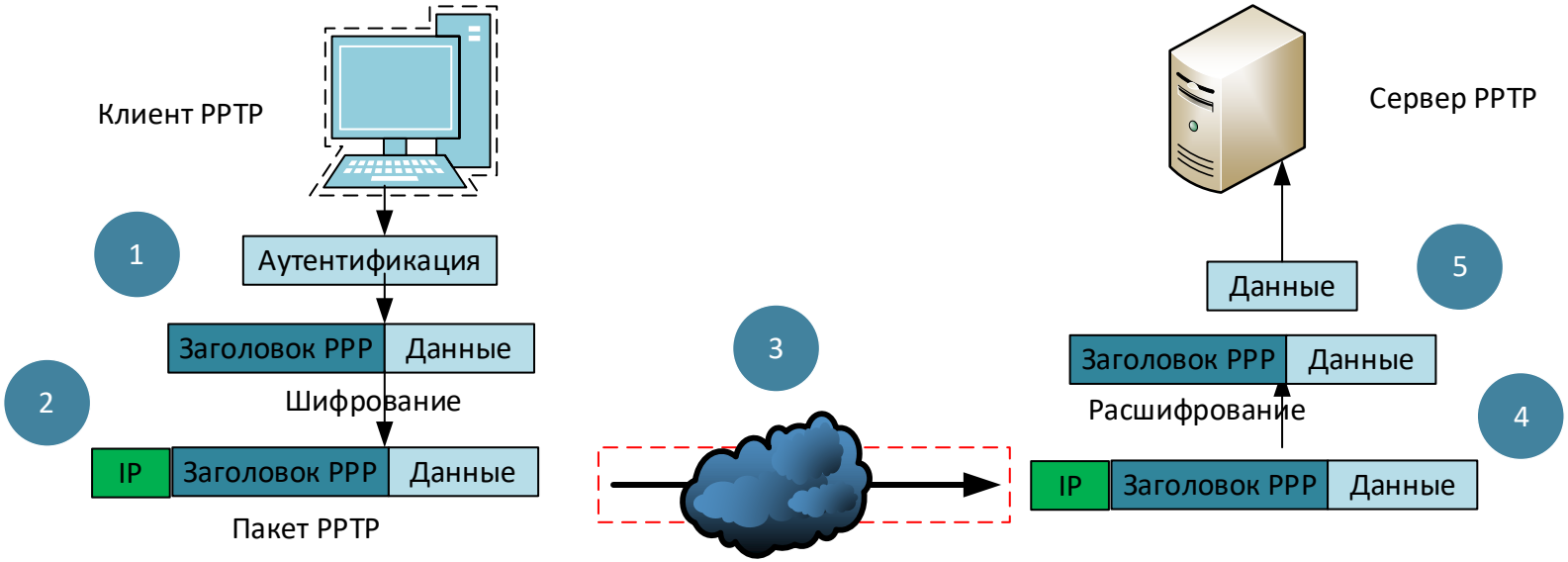
Пакеты, передаваемые в рамках сессии PPTP, имеют следующую структуру

- заголовок канального уровня, используемый внутри Интернета, например, заголовок кадра Ethernet;
- заголовок IP, содержащий адреса отправителя и получателя пакета;
- заголовок общего метода инкапсуляции для маршрутизации GRE (Generic Routing Encapsulation);
- исходный пакет PPP, включающий пакет IP, IPX или NetBEUI.



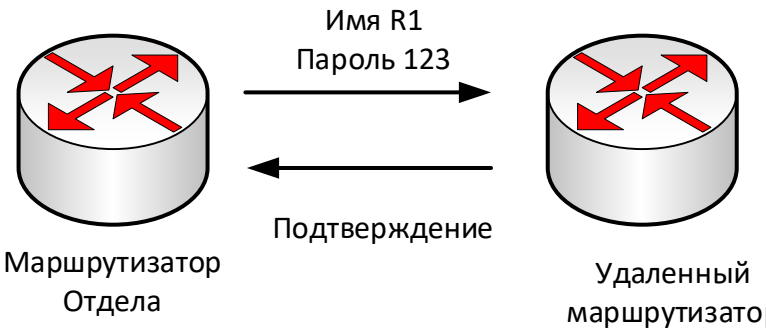
Канальный уровень

1. Клиентом PPTP осуществляется установление канала для управления передачи по туннелю. Затем происходить формирование сообщение PPP, подлежащее защите, при необходимости формируется пакет с данными и заголовком GRE.
2. Полученное сообщение канального уровня шифруется вместе с заголовком и помещается в поле данных IP пакета.
3. Сообщение передается по сети.
4. При получении пакета из него извлекается и расшифровывается внутренний исходный пакет.
5. Происходит передача информации PPTP серверу.

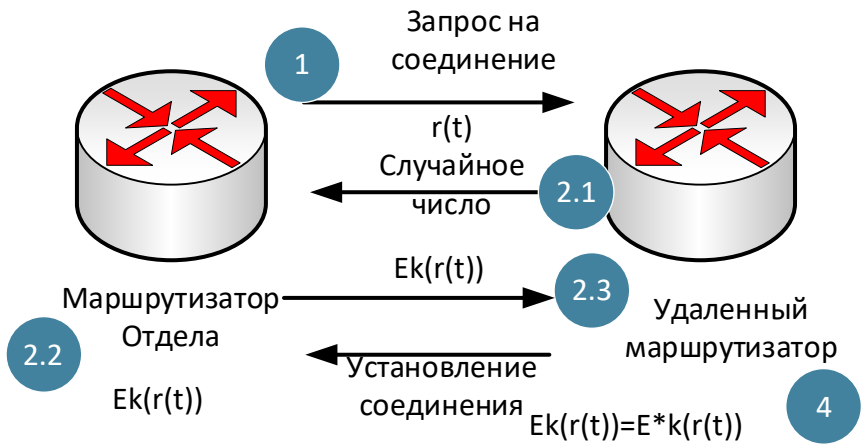


Аутентификация в протоколе PPTP

PAP



CHAP



Протокол L2TP

L2TP (Layer 2 Tunneling Protocol) - протокол туннелирования канального уровня. Объединяет протокол L2F (Layer 2 Forwarding), разработанный компанией Cisco, и протокол PPTP корпорации Microsoft.

Достоинства:

- гибкость аутентификации и автоизации с отсутствием привязки к конкретным протоколам подтверждения подлинности;
- прозрачность;
- адрес сервера удаленного доступа назначается не сервером провайдера, а сервером локальной сети;
- аудит, регистрация событий по доступу к серверу локальной сети не только сервером удаленного доступа этой сети, но и сервером провайдера.

Протокол L2TP

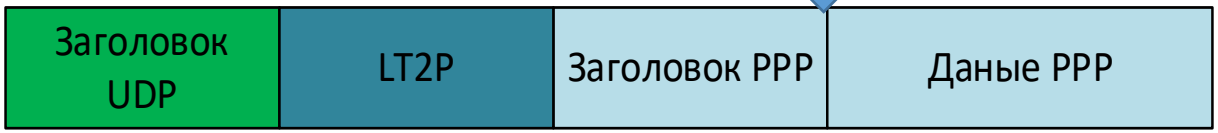
Протокол использует 2 канала для организации защищённого соединения

Исходный инкапсулируемый протокол (по которому функционирует ЛВС)

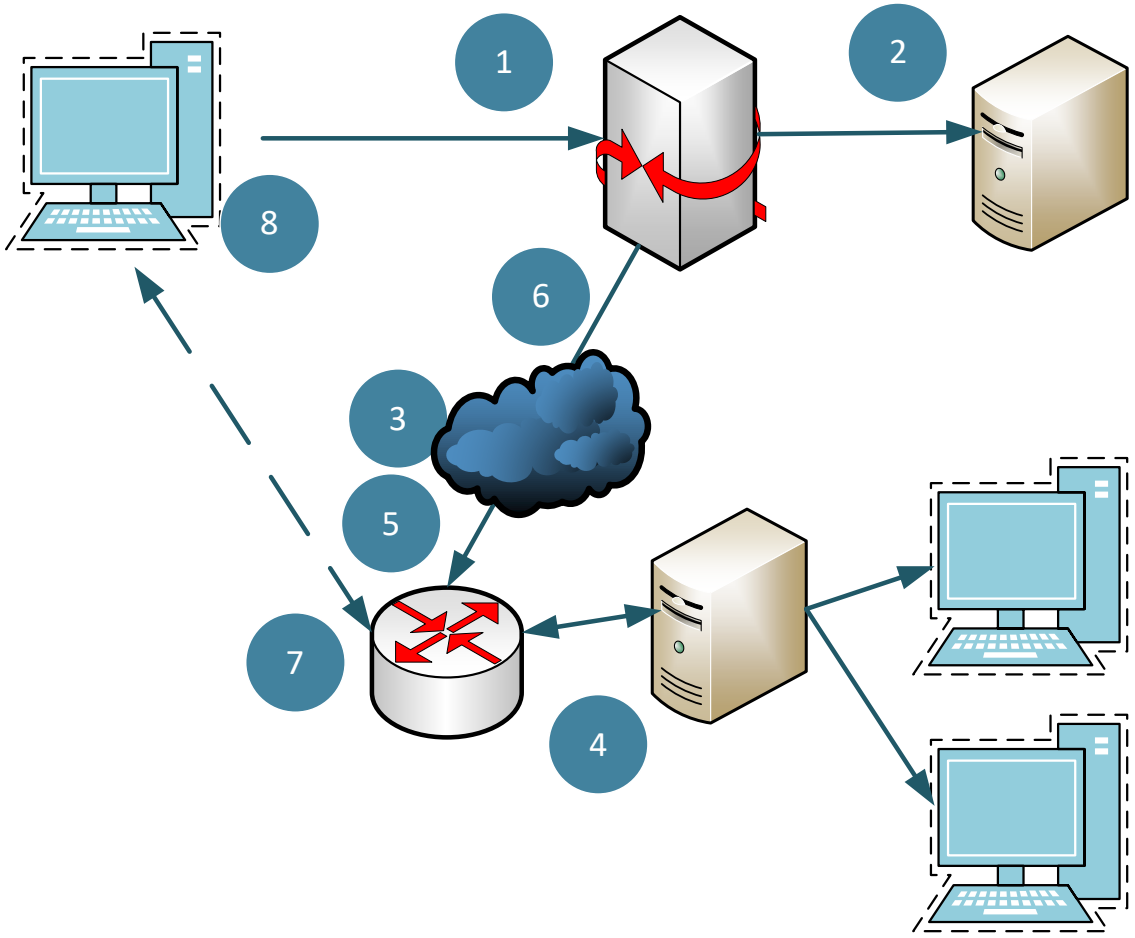
протокол-пассажир, в который инкапсулируется исходный протокол (PPP)

Инкапсулирующий протокол – это управляющий протокол, который используется для создания, поддержания и разрыва туннеля (L2F);

Протокол провайдера, который используется для переноса инкапсулируемых протоколов (исходного протокола и протокола-пассажира)



Протокол L2TP



Протокол IPSec

IPsec (IP Security) — набор протоколов для обеспечения защиты данных, передаваемых по межсетевому протоколу IP.

Позволяет обеспечить:

- аутентификацию отправителя, с использованием протоколов аутентификации IKE, основанного на алгоритме Диффи-Хелмана
- конфиденциальность передаваемого трафика, за счет использования механизмов шифрования DES, 3DES
- целостность данных с применением AH и HMAC
- защиту от воспроизведения путем использования протокола AH

Ядро IPSec

- AH (Authentication Header) гарантирует целостность и аутентичность данных за счет использования механизмов аутентификации.
- ESP (Encapsulating Security Payload) обеспечивает инкапсуляцию зашифрованных данных, обеспечивая конфиденциальность позволяет поддерживать аутентификацию и целостность данных.
- IKE (Internet Key Exchange) осуществляет обмен ключами и предоставляет конечным точкам защищенного канала секретные ключи, необходимые для работы протоколов аутентификации и шифрования данных.

Ядро IPSec

- Существует несколько способов реализации IPSec:
- -интеграция IPSec в конкретную реализацию IP (с изменением исходного кода IP на хосте, или шлюзе безопасности);
- -bump-in-the-stack (BITS) реализация (между обычным IP и локальными сетевыми драйверами без доступа к исходному коду стека IP, удобен для встраивания в существующие системы, и реализации на хостах);
- -использование внешнего криптопроцессора.

Протокол IPSec. Протокол AH

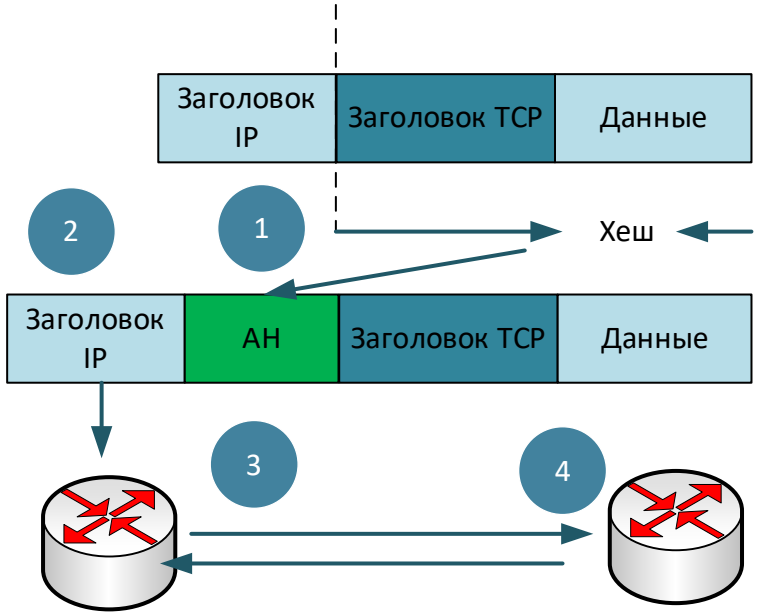
Протокол AH обеспечивает аутентификацию и целостность данных для пакетов IP, передаваемых между двумя системами.

1. Осуществляется хэш преобразование IP-заголовка и поля данных исходного пакета.

2. Полученный хэш-код используется при построении нового заголовка AH, который подсоединяется к исходному пакету между заголовком и блоком данных.

3. Осуществляется передача пакета получателю.

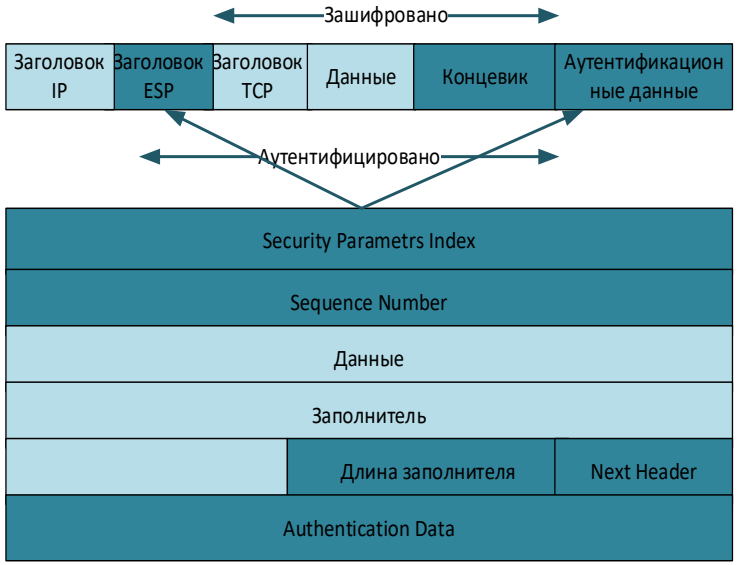
4. Получатель проверяет значение хэша. При этом изменяемые поля (TTL) изменяются промежуточными сетевыми устройствами и не защищаются протоколом AH). Защита от воспроизведения пакетов, осуществляется путем присвоения порядкового номера пакета.



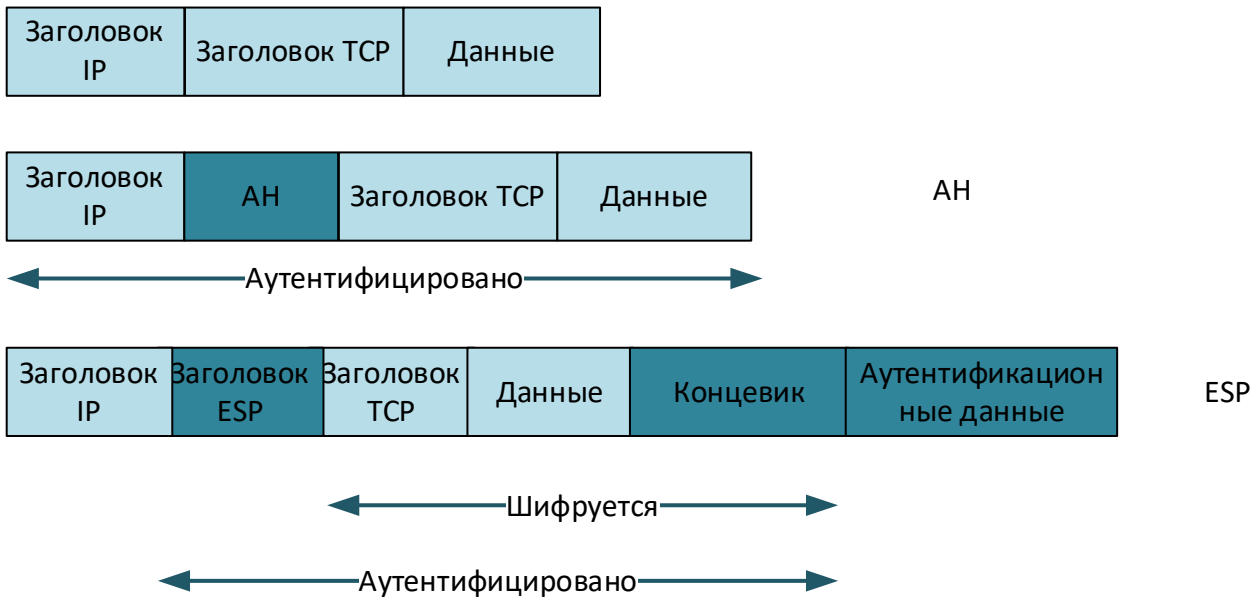
Протокол IPSec. Протокол ESP

Для обеспечения шифрования необходимо:

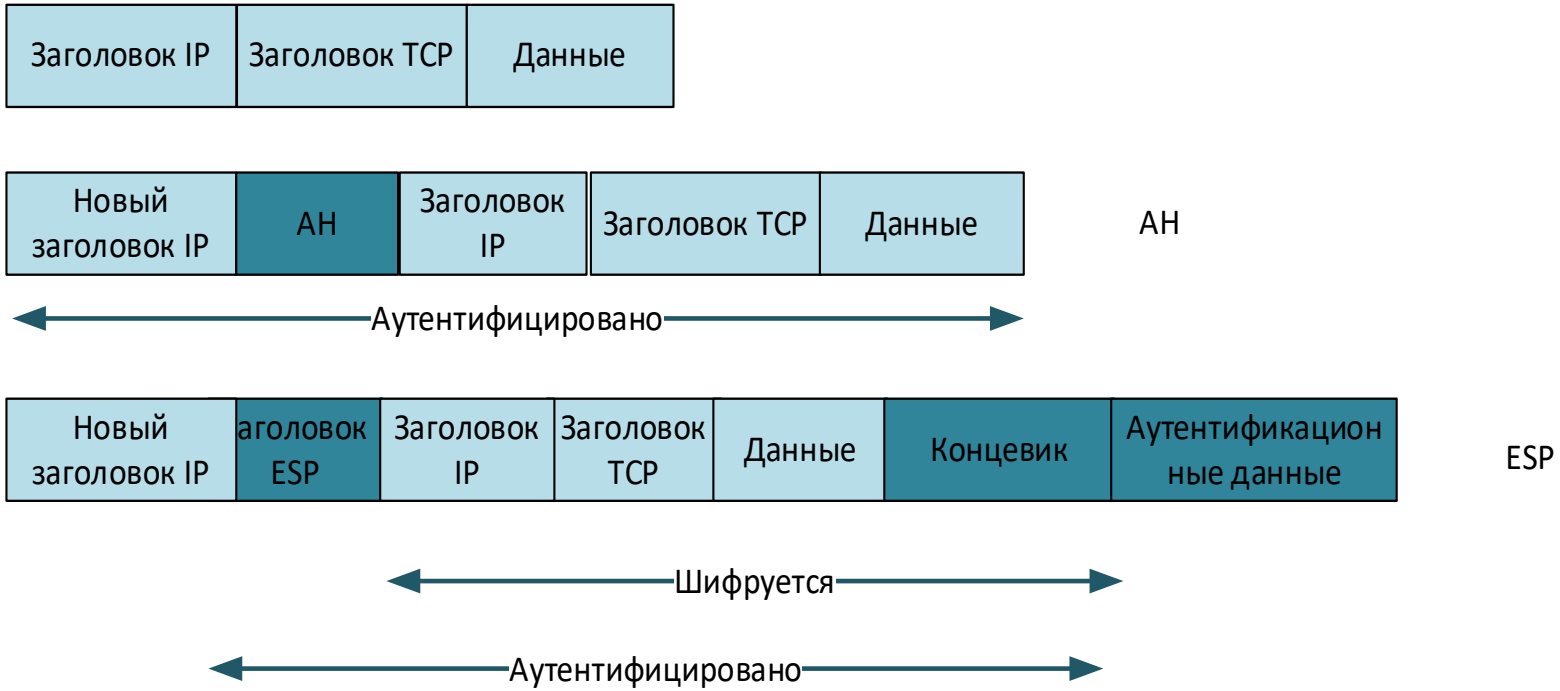
1. Скопировать содержимое пакета (заголовок TCP, данные и контрольную суммы) в буфер обмена.
2. Остаток дополнить байтами, с тем чтобы номер был прижат к границе 32-битного слова, а размер буфера удовлетворял требованиям алгоритма шифрования;
3. Осуществить криптографическое преобразование содержимого буфера;
4. Дополнить сообщение полями «индекс параметров безопасности (SPI)» и «порядковый номер» с соответствующими значениями;
5. Полученное на ш 5 сообщение аутентифицировать и поместить в поле «Аутентификационные данные»;
6. В полученное сообщение поместить заголовки старого пакета (IP) и конечное содержимое буфера.



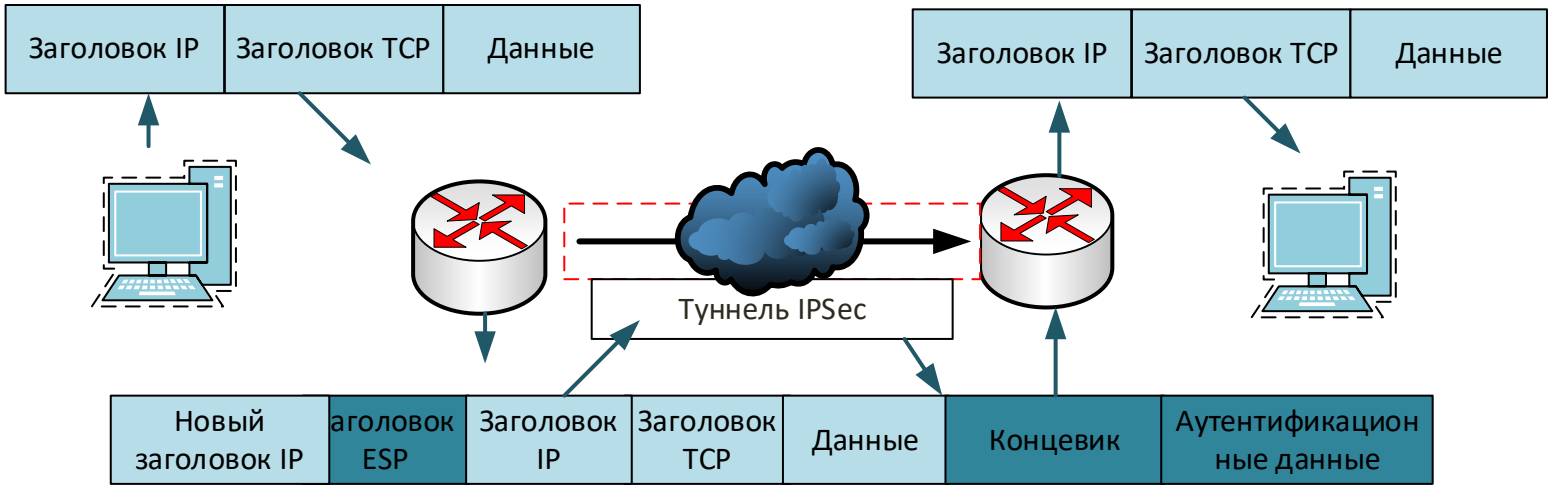
Транспортный режим IPSec



Туннельный режим IPSec



Туннельный режим IPSec



Сервисы безопасности IPsec

Протоколы IKE решают задачи:

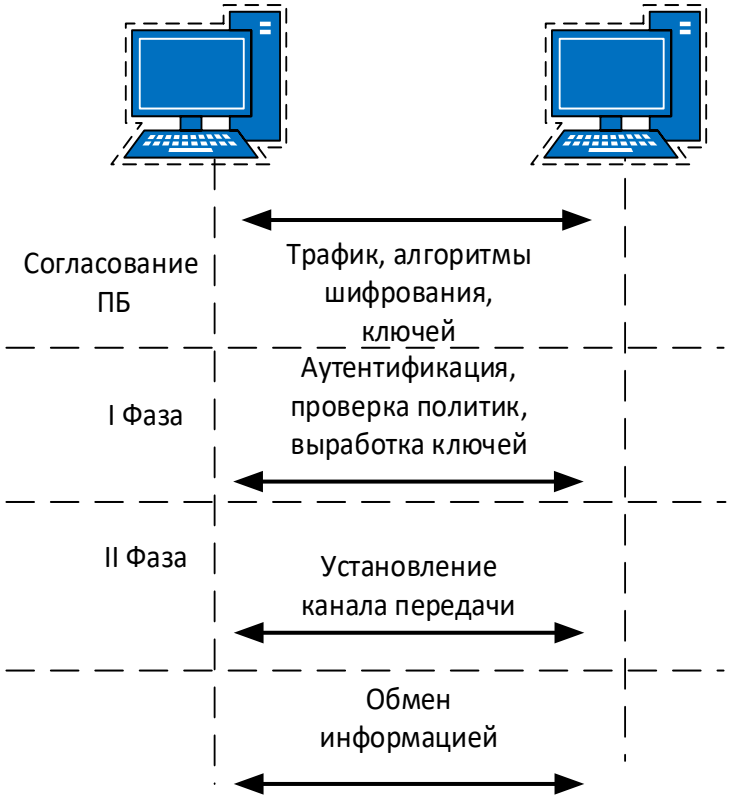
- аутентификации сторон, согласования алгоритмов шифрования и характеристик ключей
- создание, обмен и управление ключевой информации соединения (в том числе возможность их частой смены)
- управление параметрами соединения и защитой от некоторых типов атак

IKE совмещает в себе три основных направления (отдельных протокола):

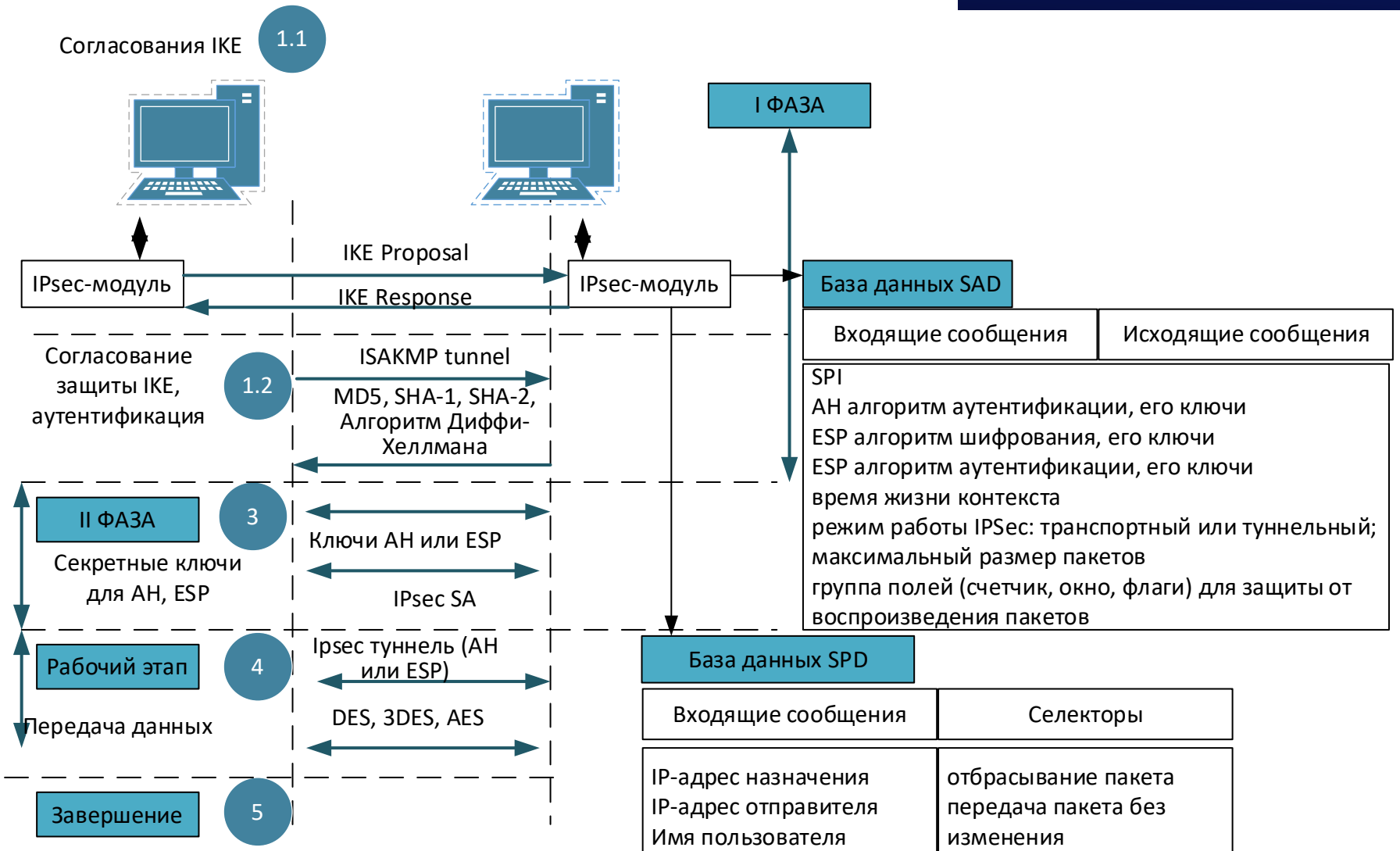
- ISAKMP (Internet Security Association and Key Management Protocol) - протокол ассоциаций безопасности и управления ключами в интернете, ; отвечает за обеспечение аутентификации и обмена ключей без указания конкретных прикладных алгоритмов
- Oakley (Oakley key determination protocol) - протокол определения ключей описывает последовательности обмена ключами
- SKEMI (Secure Key Exchange Mechanism for Internet) - механизм безопасного обмена ключами в Интернете.

Этапы функционирования IPsec

1. Создание на хосте политики безопасности.
2. Первая фаза IKE (аутентификация и защита идентификационной информации хостов; проверка соответствий политик безопасности хостов; получение ключевой последовательности по алгоритму Диффи-Хеллмана)
3. Вторая фаза IKE (Согласование параметров передачи данных; установление канала передачи данных)
4. Обмен информацией между узлами через IPsec-туннель.
5. Прекращение действия текущих IPsec SA. (при удалении или истечении времени жизни.



Этапы функционирования IPsec



Литература

1. Методическое пособие по IPSec. Электронный ресурс http://dfe.petrsu.ru/koi/posob/security/
2. Лекция №20. Защита на сетевом уровне. Электронный ресурс https://yztm.ru/lekc2/l20/
3. Национальная библиотека им. Н. Э. Баумана. IPSec. Электронный ресурс. https://ru.bmstu.wiki/IPsec_(IP_Security)
4. Википедия. IPSec. Электронный ресурс https://ru.wikipedia.org/wiki/IPsec