ИНФОРМАЦИОННЫЕ СЕТИ

ЛЕКЦИЯ 11.
ЗАЩИТА ДАННЫХ В ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМАХ

ЗАЩИТА СЕТЕВОГО ТРАФИКА

- Сервисы защиты сетевого трафика позволяют через публичную сеть, например Интернет, безопасно передавать информацию, обеспечивая ее аутентичность, целостность и конфиденциальность.
- Наиболее простым средством для предоставления такого сервиса является технология защищенного канала, которая обеспечивает защиту трафика между двумя пользователями публичной сети, то есть в соответствии с двухточечной топологией.
- Такая защита осуществляется за счет комплекса средств, опирающихся на различные методы аутентификации пользователей и шифрования их трафика.
- В IP-сетях широко применяются две технологии защищенного канала — SSL и IPSec.
  - Протокол SSL работает на уровне представления модели OSI, что делает его непрозрачным для приложений.
  - Протокол IPSec является более универсальным средством, так как относится к сетевому уровню и полностью прозрачен для приложений, которые в случае использования IPSec не требуют модификации.

СЕРВИС ЗАЩИЩЕННОГО КАНАЛА

- Основное назначение сервиса **IPSec** (Internet Protocol Security — защищенный протокол IP) состоит в обеспечении безопасной передачи данных по IP-сетям.
- Применение протокола IPSec гарантирует целостность, аутентичность и конфиденциальность данных.
- Базовой технологией обеспечивающей достижение этой цели является **шифрование**.
- Для протоколов такого назначения используется обобщенное название — **защищенный канал.**
- Термин «канал» подчеркивает тот факт, что защита данных обеспечивается на протяжении всего пути между двумя узлами сети (хостами или шлюзами)

ИЕРАРХИЯ СЕРВИСОВ ЗАЩИЩЕННОГО КАНАЛА

- IPSec — это одна из технология безопасной передачи данных по публичной сети.
- Защищенный канал может быть построен с помощью системных средств, реализованных на разных уровнях модели OSI

Уровни защищаемых протоколов	Протоколы защищенного канала	Свойства протоколов защищенного канала
Прикладной уровень	S/MIME	Непрозрачность для приложений, независимость от транспортной инфраструктуры
Уровень представления	SSL, TLS	
Сеансовый уровень		
Транспортный уровень		
Сетевой уровень	IPSec	Прозрачность для приложений, зависимость от транспортной инфраструктуры
Канальный уровень	PPTP	
Физический уровень		

ЗАЩИТА В СЕТЯХ НА ОСНОВЕ РАЗГРАНИЧЕНИЯ ТРАФИКА

- Защита данных достигается благодаря тому, что несанкционированный пользователь не может подключиться к постоянному виртуальному каналу, не изменив таблицы коммутации устройств поставщика услуг, а значит, ему не удастся провести атаку или прочитать данные.
- Свойство защищенности трафика является *естественным свойством* техники виртуальных каналов, поэтому сервисы ATM VPN и Frame Relay VPN являются на самом деле не чем иным, как обычными сервисами PVC сетей ATM или Frame Relay.
- Любой пользователь ATM или Frame Relay, использующий инфраструктуру PVC для связи своих локальных сетей, пользуется услугой VPN даже в том случае, когда он это явно не осознает.
- Это одно из преимуществ техники виртуальных каналов по сравнению с дейтаграммной техникой, так как при применении последней без дополнительных средств VPN пользователь оказывается не защищенным от атак любого другого пользователя сети.

РАСПРЕДЕЛЕНИЕ ФУНКЦИЙ МЕЖДУ ПРОТОКОЛАМИ IPSEC

- IPSec — это согласованный набор открытых стандартов, имеющий ядро, которое может быть достаточно просто дополнено новыми функциями и протоколами.
- Ядро IPSec составляют три протокола:
  - AH (Authentication Header — заголовок аутентификации) — гарантирует целостность и аутентичность данных;
  - ESP (Encapsulating Security Payload — инкапсуляция зашифрованных данных) — шифрует передаваемые данные, обеспечивая конфиденциальность, может также поддерживать аутентификацию и целостность данных;
  - IKE (Internet Key Exchange — обмен ключами Интернета) — решает вспомогательную задачу автоматического предоставления конечным точкам защищенного канала секретных ключей, необходимых для работы протоколов аутентификации и шифрования данных.

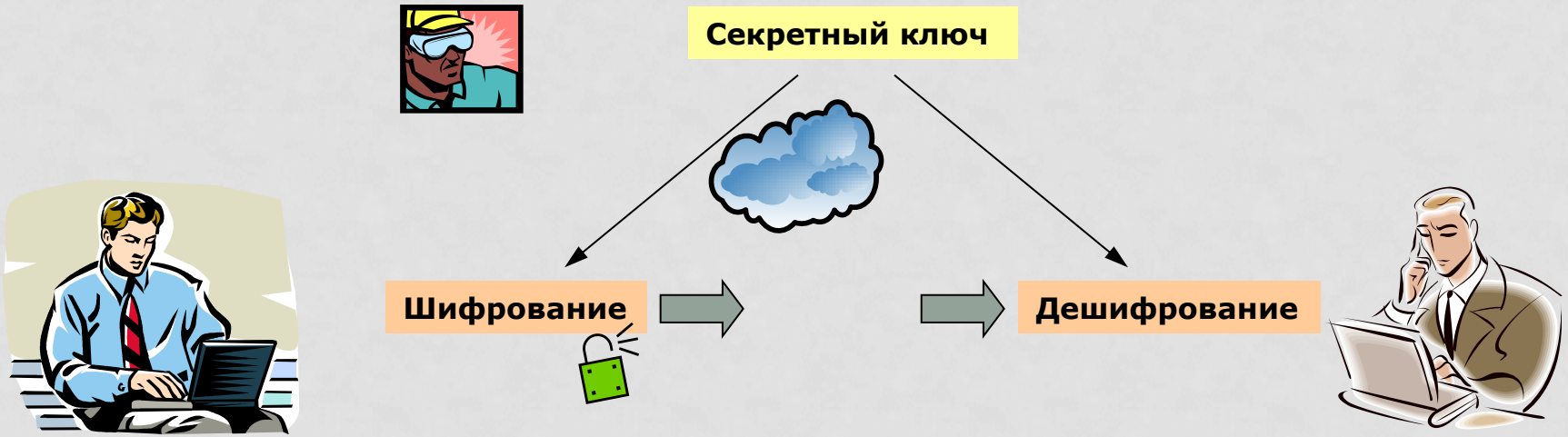
РАСПРЕДЕЛЕНИЕ ФУНКЦИЙ МЕЖДУ ПРОТОКОЛАМИ IPSEC

- Возможности протоколов AH и ESP частично перекрываются:
  - Протокол AH отвечает только за обеспечение целостности и аутентификации данных,
  - Протокол ESP может шифровать данные и, кроме того, выполнять функции протокола AH (в урезанном виде). ESP может поддерживать функции шифрования и аутентификации/целостности в любых комбинациях, то есть либо всю группу функций, либо только аутентификацию/целостность, либо только шифрование.

<table>
<tr><th>Выполняемые функции</th><th colspan="2">Протокол</th></tr>
<tr><td>Обеспечение целостности</td><td rowspan="2">AH</td><td rowspan="3">ESP</td></tr>
<tr><td>Обеспечение аутентичности</td></tr>
<tr><td>Обеспечение конфиденциальности (шифрование)</td><td></td></tr>
<tr><td>Распределение секретных ключей</td><td colspan="2">IKE</td></tr>
</table>

ШИФРОВАНИЕ В ПРОТОКОЛЕ IPSEC

- Для **шифрования** данных в протоколе IPSec может быть применен любой симметричный алгоритм шифрования.
- **В симметричных схемах шифрования** конфиденциальность основана на том, что отправитель и получатель обладают общим, известным только им, параметром функции шифрования.
- Этот параметр называется **секретным ключом.** Секретный ключ используется как для шифрования текста, так и для его дешифрирования.



ОБЕСПЕЧЕНИЕ ЦЕЛОСТНОСТИ ДАННЫХ

В основе обеспечения целостности и аутентификации данных также лежит один из приемов шифрования — шифрование с помощью **вычислительно необратимой функции** (One-Way Function, OWF), частными случаями которой являются **хэш-функция** и **дайджест-функция.**

Дайджест является своего рода контрольной суммой для исходного сообщения. Однако наличие контрольной суммы в передаваемом пакете не помешает злоумышленнику подменить исходное сообщение, добавив к нему новое значение контрольной суммы.

В отличие от контрольной суммы при вычислении дайджеста используется секретный ключ.

Если для получения дайджеста применялась необратимая функция с параметром (в качестве которого выступает секретный ключ), известным только отправителю и получателю, любая модификация исходного сообщения будет немедленно обнаружена.

ЭЛЕКТРОННАЯ ЦИФРОВАЯ ПОДПИСЬ

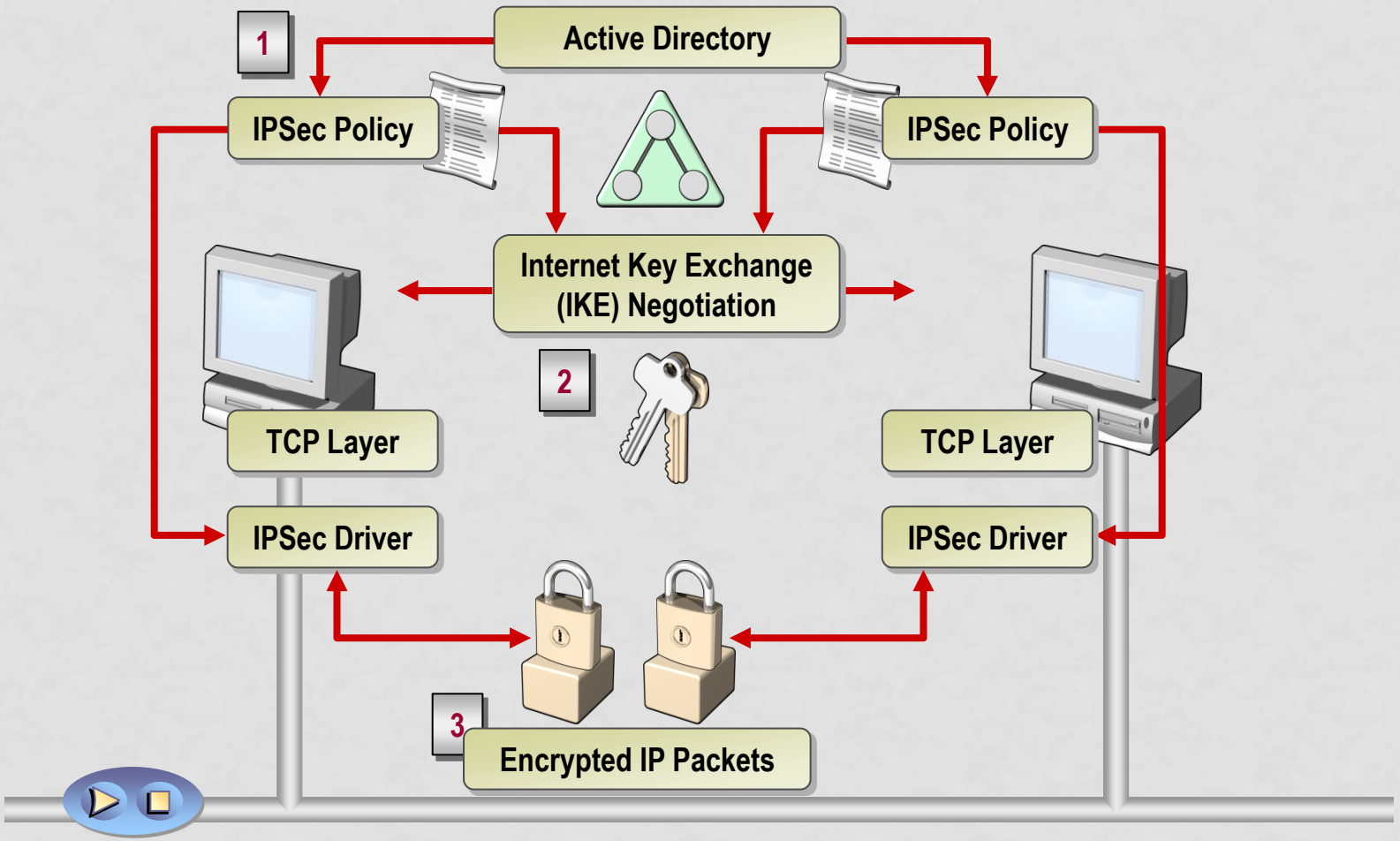
Вычислительно необратимая функция является средством решения сразу двух задач — контроля целостности и аутентичности данных.

Такую схему передачи данных наряду с другими методами, позволяющими устанавливать подлинность автора сообщения, согласно терминологии ISO называют **цифровой подписью.**

Наиболее часто для построения схемы цифровой подписи используется **асимметричный алгоритм шифрования.**

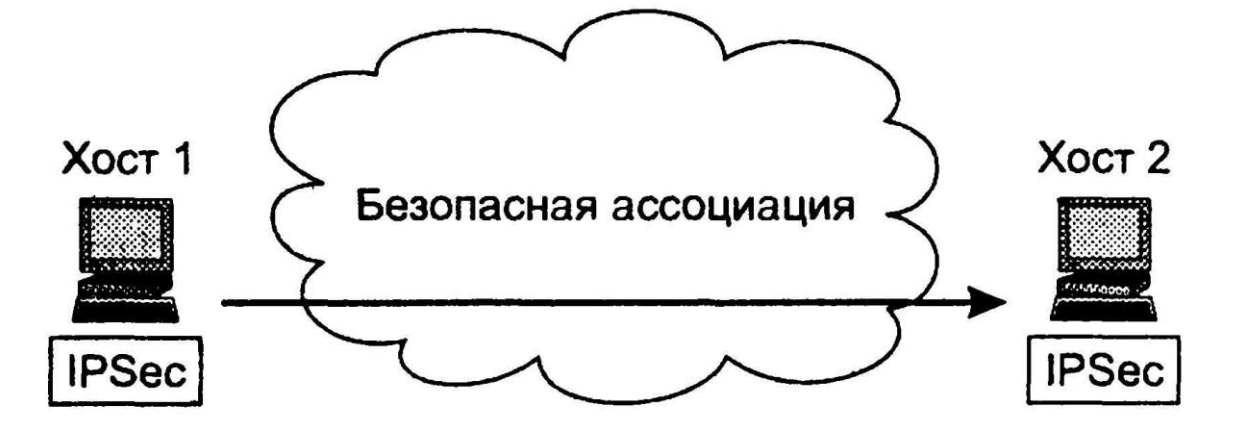
В основе этого алгоритма лежит концепция Диффи—Хеллмана (Diffie—Hellmann), заключающаяся в том, что каждый пользователь сети имеет свой секретный (закрытый) ключ, необходимый для формирования подписи в зашифрованном виде; все остальные пользователи используют для проверки подписи соответствующий этому секретному ключу открытый ключ.

ЗАЩИТА ТРАФИКА СРЕДСТВАМИ IPSEC



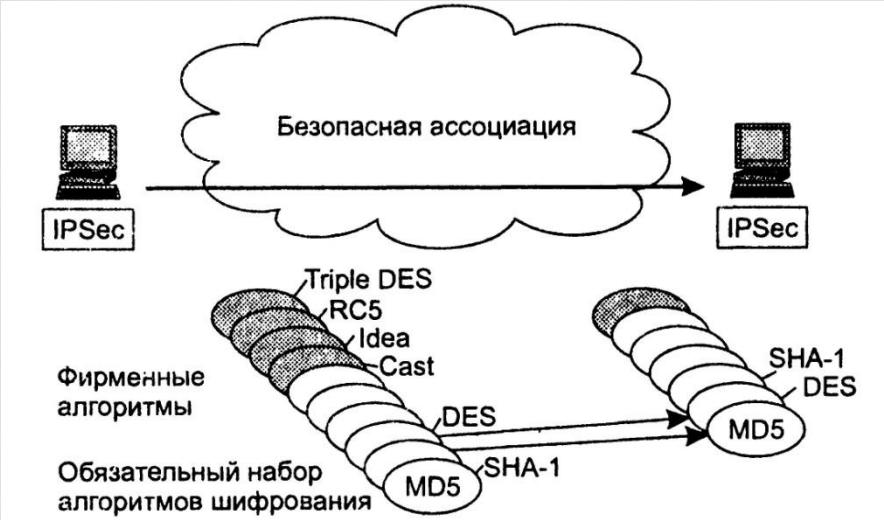
БЕЗОПАСНАЯ АССОЦИАЦИЯ

- Для того чтобы протоколы AH и ESP могли выполнять свою работу по защите передаваемых данных, протокол IKE устанавливает между двумя конечными точками логическое соединение, которое в стандартах IPSec носит название **безопасной ассоциации** (Security Association, SA).
- Стандарты IPSec позволяют конечным точкам защищенного канала использовать как одну ассоциацию SA для передачи трафика всех взаимодействующих через этот канал хостов, так и создавать для этой цели произвольное число ассоциаций SA, например, по одной на каждое соединение TCP.



СОГЛАСОВАНИЕ ПАРАМЕТРОВ В ПРОТОКОЛЕ ESP

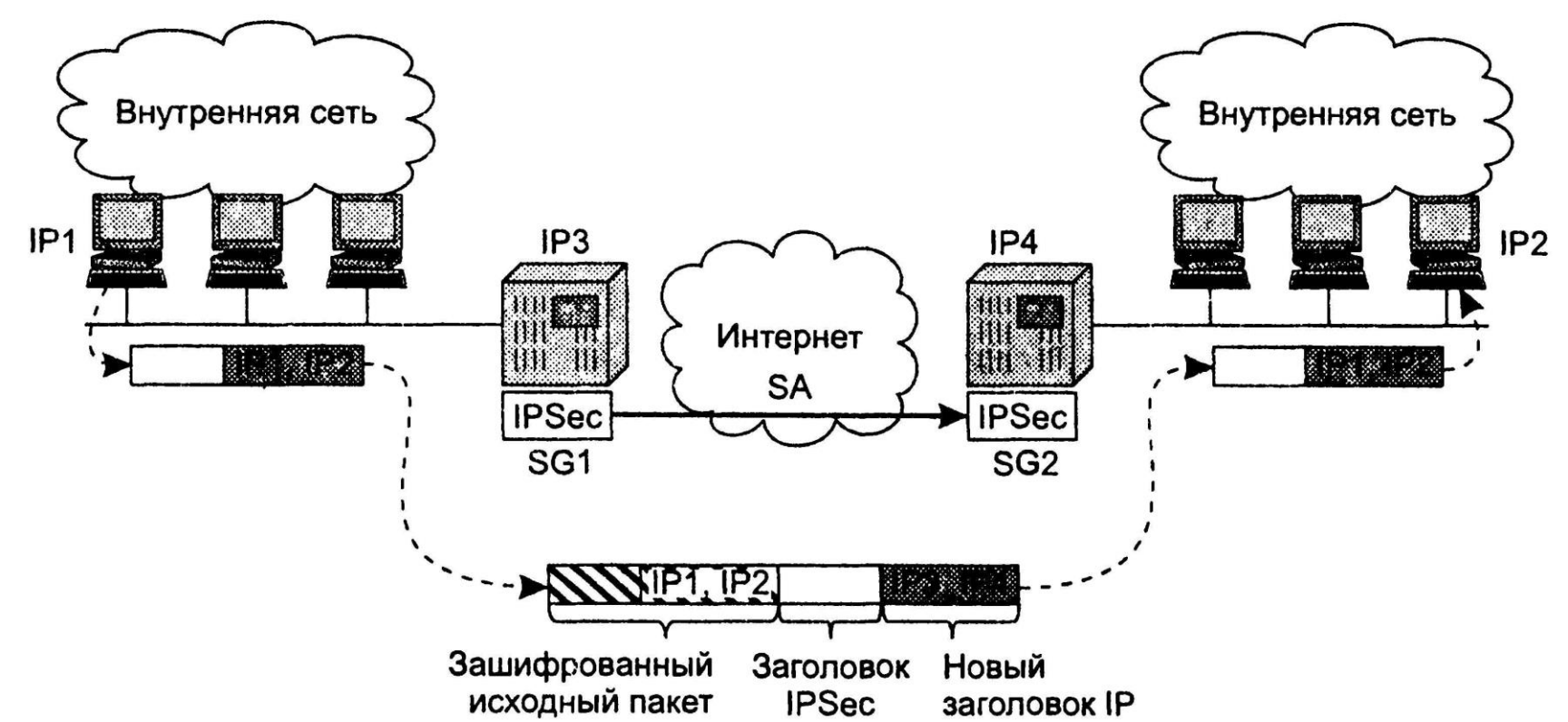
- Протокол IPSec допускает как автоматическое, так и ручное установление безопасной ассоциации.
  - При ручном способе администратор конфигурирует конечные узлы так, чтобы они поддерживали согласованные параметры ассоциации, включая и секретные ключи.
  - При автоматической процедуре установления SA протоколы IKE. работающие по разные стороны канала, выбирают параметры в ходе переговорного процесса.



ТРАНСПОРТНЫЙ И ТУННЕЛЬНЫЙ РЕЖИМЫ

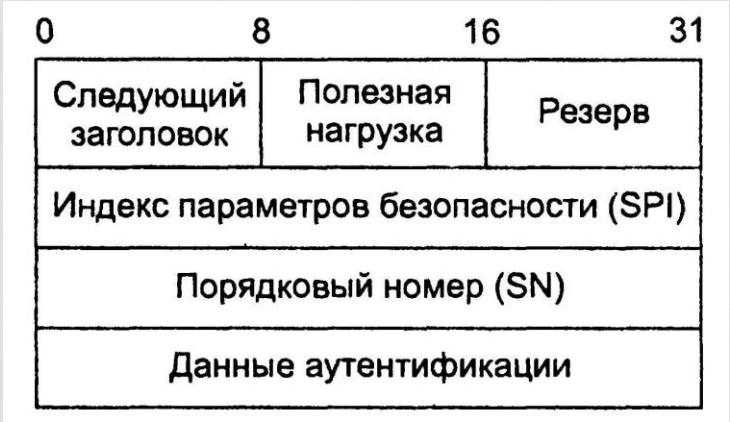
- Протоколы AH и ESP могут защищать данные в двух режимах:
  - **в транспортном** – передача ведется с оригинальными ip-заголовками;
  - **в туннельном** – исходный пакет помещается в новый ip-пакет и передача ведется с новыми заголовками.
- Применение того или иного режима зависит от требований, предъявляемых к защите данных, а также от роли, которую играет в сети узел, завершающий защищенный канал.
- Так, узел может быть хостом (конечным узлом) или шлюзом (промежуточным узлом). Соответственно, имеются три схемы применения протокола IPSec:
  - хост—хост;
  - шлюз—шлюз;
  - хост—шлюз.

РАБОТА ЗАЩИЩЕННОГО КАНАЛА ПО СХЕМЕ ШЛЮЗ – ШЛЮЗ В ТУННЕЛЬНОМ РЕЖИМЕ



ПРОТОКОЛ AH

- Основное назначение протокола AH – он позволяет приемной стороне убедиться, что:
  - пакет был отправлен стороной, с которой установлена безопасная ассоциация;
  - содержимое пакета не было искажено в процессе его передачи по сети;
  - пакет не является дубликатом уже полученного пакета.
- Две первые функции обязательны для протокола AH, а последняя выбирается при установлении ассоциации по желанию. Для выполнения этих функций протокол AH использует специальный заголовок.



СТРУКТУРА ЗАГОЛОВКА ПРОТОКОЛА AH

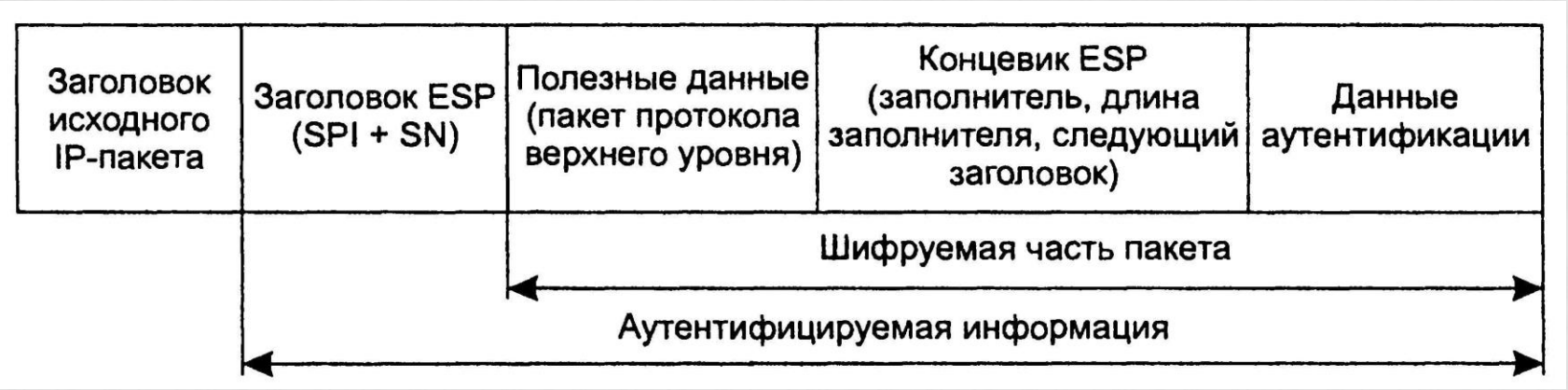
- В поле *следующего заголовка* (next header) указывается код протокола более высокого уровня, то есть протокола, сообщение которого размещено в поле данных IP-пакета.
- В поле *длины полезной нагрузки* (payload length) содержится длина заголовка AH.
- *Индекс параметров безопасности* (Security Parameters Index, SPI) используется для связи пакета с предусмотренной для него безопасной ассоциацией.
- Поле *порядкового номера* (Sequence Number, SN) указывает на порядковый номер пакета и применяется для защиты от его ложного воспроизведения (когда третья сторона пытается повторно использовать перехваченные защищенные пакеты, отправленные реально аутентифицированным отправителем).
- Поле *данных аутентификации* (authentication data), которое содержит так называемое **значение проверки целостности** (Integrity Check Value, ICV), используется для аутентификации и проверки целостности пакета. Это значение, называемое также дайджестом, вычисляется с помощью одной из двух обязательно поддерживаемых протоколом AH вычислительно необратимых функций MD5 или SHA-1, но может использоваться и любая другая функция.

ПРОТОКОЛ ESP

- Протокол ESP решает две группы задач.
  - к первой относятся задачи, аналогичные задачам протокола AH, — это обеспечение аутентификации и целостности данных на основе дайджеста,
  - ко второй — защита передаваемых данных путем их шифрования от несанкционированного просмотра.
- Заголовок делится на две части, разделяемые полем данных.
  - Первая часть, называемая собственно **заголовком ESP**, образуется двумя полями (SPI и SN), назначение которых аналогично одноименным полям протокола AH, и размещается перед полем данных.
  - Остальные служебные поля протокола ESP, называемые концевиком ESP, расположены в конце пакета.
- Два поля концевика — *следующего заголовка* и *данных аутентификации* — аналогичны полям заголовка AH. Поле данных аутентификации отсутствует, если при установлении безопасной ассоциации принято решение не использовать возможностей протокола ESP по обеспечению целостности. Помимо этих полей концевик содержит два дополнительных поля — *заполнителя* и *длины заполнителя*.

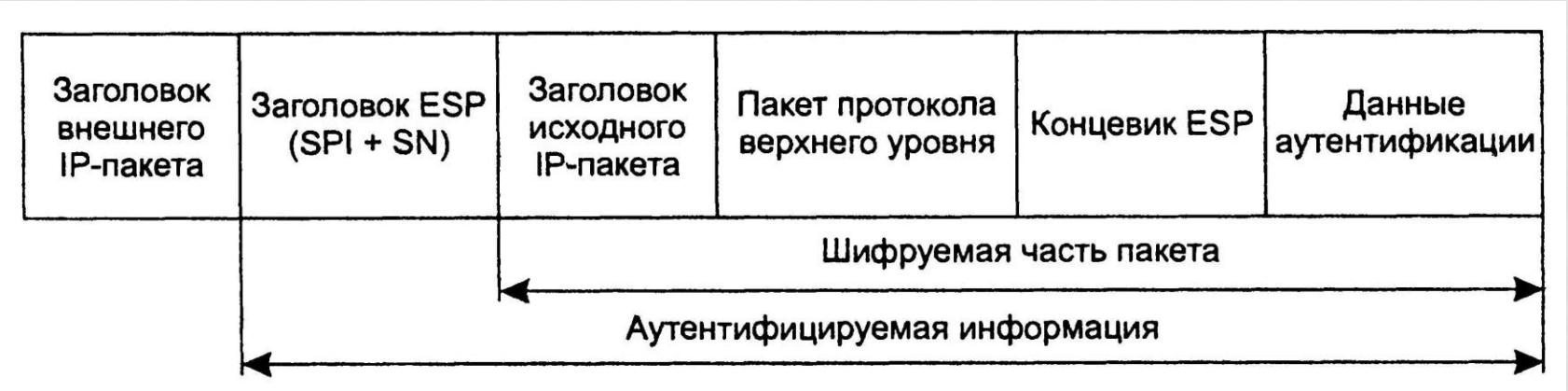
СТРУКТУРА IP-ПАКЕТА, ОБРАБОТАННОГО ПРОТОКОЛОМ ESP В ТРАНСПОРТНОМ РЕЖИМЕ

- В этом режиме ESP не шифрует заголовок IP-пакета, иначе маршрутизатор не сможет прочитать поля заголовка и корректно осуществить продвижение пакета между сетями.
- В число шифруемых полей не попадают также поля SPI и SN, которые должны передаваться в открытом виде для того, чтобы прибывший пакет можно было отнести к определенной ассоциации и защититься от ложного воспроизведения пакета.



СТРУКТУРА IP-ПАКЕТА, ОБРАБОТАННОГО ПРОТОКОЛОМ ESP В ТУННЕЛЬНОМ РЕЖИМЕ

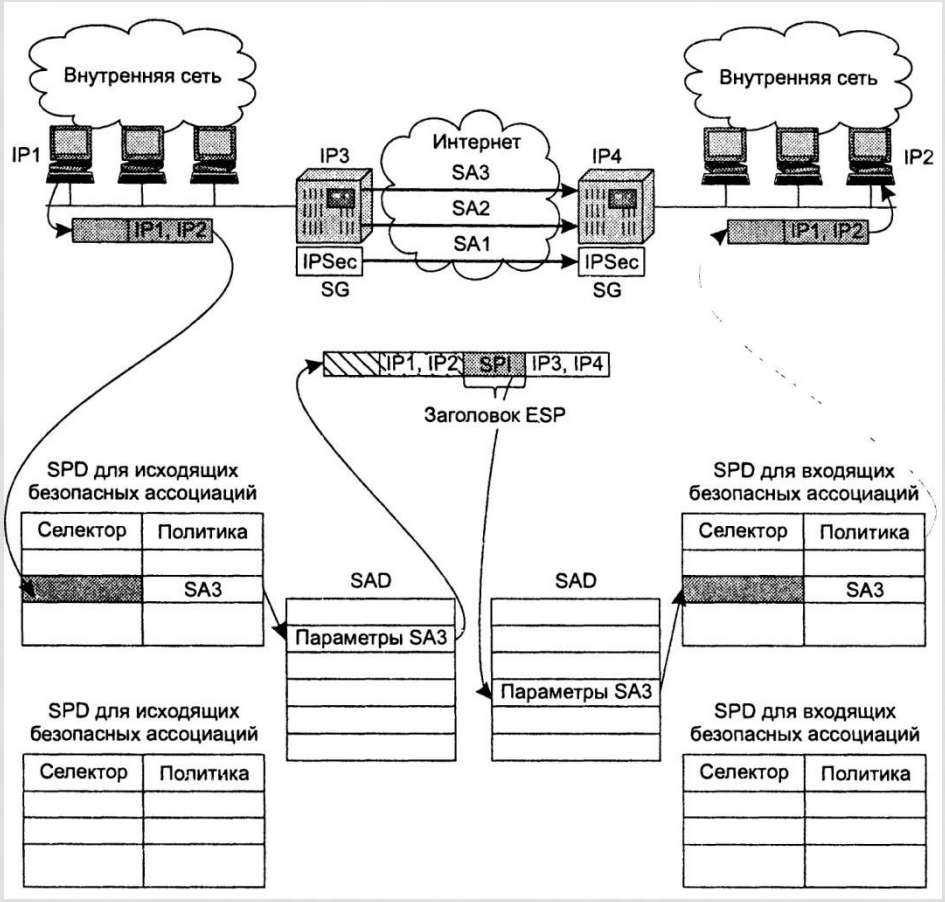
- В туннельном режиме заголовок исходного IP-пакета помещается после заголовка ESP и полностью попадает в число защищаемых полей, а заголовок внешнего IP-пакета протоколом ESP не защищается.



БАЗЫ ДАННЫХ SAD И SPD

- Протокол IPSec, работающий на хосте или шлюзе, определяет способ защиты, который он должен применить к трафику на основании использования в каждом узле, поддерживающем IPSec, двух типов баз данных:
  - **безопасных ассоциаций** (Security Associations Database, SAD);
  - **политики безопасности** (Security Policy Database, SPD).
- Наборы текущих параметров, определяющих все активные ассоциации, хранятся на обоих оконечных узлах защищенного канала в виде баз данных безопасных ассоциаций (SAD). Каждый узел IPSec поддерживает две базы SAD — одну для исходящих ассоциаций, другую для входящих.
- Другой тип базы данных — база данных политики безопасности (SPD) — определяет соответствие между IP-пакетами и установленными для них правилами обработки.

ИСПОЛЬЗОВАНИЕ БАЗ ДАННЫХ SPD И SAD



СТРУКТУРА БД SPD

- Записи SPD состоят из нолей двух типов — полей селектора пакета и полей политики защиты для пакета с данным значением селектора.
- Селектор в SPD включает следующий набор признаков, на основании которых можно с большой степенью детализации выделить защищаемый поток:
  - IP-адреса источника и приемника могут быть представлены как в виде отдельных адресов (индивидуальных, групповых или широковещательных), так и диапазонами адресов, заданными с помощью верхней и нижней границ либо с помощью маски;
  - порты источника и приемника (то есть TCP- или UDP-портов);
  - тип протокола транспортного уровня (TCP, UDP);
  - имя пользователя в формате DNS или X.500;
  - имя системы (хоста, шлюза безопасности и т. п.) в формате DNS или X.500.

РАБОТА ПОЛИТИКИ БЕЗОПАСНОСТИ

- Для каждого нового пакета, поступающего в защищенный канал, IPSec просматривает все записи в базе SPD и сравнивает значение селекторов этих записей с соответствующими полями IP-пакета.
- Если значение полей совпадает с каким-либо селектором, то над пакетом выполняются действия, определенные в поле политики безопасности данной записи.
- Политика предусматривает одну из следующих возможностей:
  - передача пакета без изменения,
  - отбрасывание,
  - обработка средствами IPSec.
- В последнем случае поле политики защиты должно содержать ссылку на запись в базе данных SAD, в которую помещен набор параметров безопасной ассоциации для данного пакета.
- На основании заданных параметров безопасной ассоциации к пакету применяется соответствующий протокол шифрования и секретные ключи.

СОЗДАНИЕ ПОЛИТИКИ ЗАЩИТЫ

Если к исходящему пакету нужно применить некоторую политику защиты, но указатель записи SPD показывает, что в настоящее время нет активной безопасной ассоциации с требуемой политикой, то IPSec создает новую ассоциацию с помощью протокола IKE, помещая новые записи в базы данных SAD и SPD.

Базы данных политики безопасности создаются и администрируются либо пользователем (этот вариант больше подходит для хоста), либо системным администратором (вариант для шлюза), либо автоматически (приложением).

ОБРАБОТКА ПАКЕТОВ IPSEC

- Однако остается другой вопрос: как *принимающий* узел IPSec определяет способ обработки прибывшего пакета?
- При шифровании многие ключевые параметры пакета, отраженные в селекторе, оказываются недоступными – следовательно невозможно определить соответствующую запись в базах данных SAD и SPD и, следовательно, тип процедуры, которую надо применить к поступившему пакету.
- Для решения этой проблемы в заголовках AH и ESP используется **поле SPI**.
- В это поле помещается указатель на строку базы данных SAD, в которой записаны параметры соответствующей безопасной ассоциации.
- Поле SPI заполняется протоколом AH или ESP во время обработки пакета в отправной точке защищенного канала.
- Когда пакет приходит в конечный узел защищенного канала, из его внешнего заголовка ESP или AH извлекается значение SPI, и дальнейшая обработка пакета выполняется с учетом всех параметров заданной этим указателем ассоциации.

СЕРВИС ВИРТУАЛЬНЫХ ЧАСТНЫХ СЕТЕЙ

Виртуальная частная сеть (Virtual Private Network, VPN) — это логическая сеть, которая проходит через публичную сеть и определенным образом воспроизводящая свойства *реальной частной сети*.

Сеть является *частной* в случае, если предприятие единолично владеет и управляет всей сетевой инфраструктурой — кабелями, кроссовым оборудованием, каналообразующей аппаратурой, коммутаторами, маршрутизаторами и другим коммуникационным оборудованием.

Основное отличие частной сети от публичной – свойство *изолированности*.

ИЗОЛИРОВАННОСТЬ ЧАСТНОЙ СЕТИ

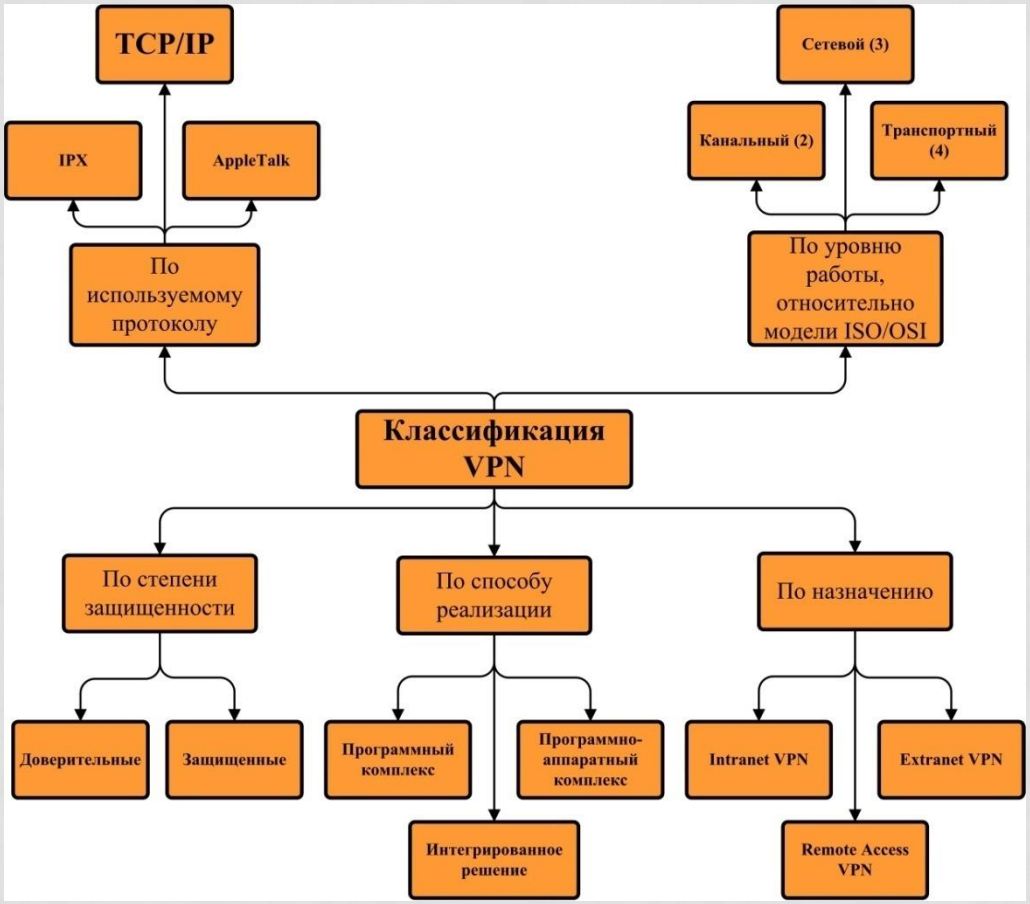
Основные признаки изолированности

- *Независимый выбор сетевых технологий.* Выбор ограничивается только возможностями производителей оборудования.
- *Независимая система адресации.* В частных сетях нет ограничений на выбор адресов — они могут быть любыми.
- *Предсказуемая производительность.* Собственные линии связи гарантируют заранее известную пропускную способность между узлами предприятия (для глобальных соединений) или коммуникационными устройствами (для локальных соединений).
- *Максимально возможная безопасность.* Отсутствие связей с внешним миром ограждает сеть от атак извне и существенно снижает вероятность «прослушивания» трафика по пути следования.

ВИРТУАЛЬНЫЕ ЧАСТНЫЕ СЕТИ

- Более масштабным средством защиты трафика являются виртуальные частные сети (VPN).
- Сеть VPN представляет собой своего рода «сеть в сети» - сервисом, создающим у пользователей иллюзию существования их частной сети внутри публичной сети.
- Важнейшим свойством частной сети является защищенность трафика от атак пользователей публичной сети.
- Сетям VPN доступна не только возможность имитации частной сети:
  - возможность задействовать собственное адресное пространство (например, частные IP-адреса, такие как адреса сети 10.0.0.0);
  - обеспечивать качество обслуживания, близкое к качеству выделенного канала.

КЛАССИФИКАЦИЯ VPN



КЛАССИФИКАЦИЯ VPN

- В зависимости от того, кто реализует сети VPN, они подразделяются на два вида:
  - **Поддерживаемая клиентом виртуальная частная сеть** (Customer Provided VPN, CPVPN) отражает тот факт, что все тяготы поддержки сети VPN ложатся на плечи потребителя. Поставщик предоставляет только «простые» традиционные услуги общедоступной сети по объединению узлов клиента, а специалисты предприятия самостоятельно конфигурируют средства VPN и управляют ими.
  - В случае **поддерживаемой поставщиком виртуальной частной сети** (Provider Provisioned VPN, PPVPN) поставщик услуг на основе собственной сети воспроизводит частную сеть для каждого своего клиента, изолируя и защищая ее от остальных.
- Существует еще и другая классификация — в зависимости от места расположения устройств, выполняющих функции VPN.
- Виртуальная частная сеть может строиться:
  - **на базе оборудования, установленного на территории потребителя** (Customer Premises Equipment based VPN, CPE-based VPN, или Customer Edge based VPN, CE-based VPN);
  - **на базе собственной инфраструктуры поставщика** (Network-based VPN или Provider Edge based VPN, PE-based VPN).

СЕТИ VPN НА ОСНОВЕ РАЗГРАНИЧЕНИЯ ТРАФИКА

- В технологиях разграничения трафика используется техника **постоянных виртуальных каналов**, обеспечивающая надежную защиту трафика каждого клиента от преднамеренного или непреднамеренного доступа к нему других клиентов публичной сети.
- К этому типу технологий относятся:
  - ATM VPN;
  - Frame Relay VPN;
  - MPLS VPN.
- Двухточечные виртуальные каналы этих технологий имитируют сервис выделенных каналов, проходя от пограничного устройства (Client Edge, CE) одного сайта клиента через поставщика к CE другого сайта клиента.

ВИРТУАЛЬНЫЕ СЕТИ КАНАЛЬНОГО УРОВНЯ

- В технологиях ATM и Frame Relay при передаче данных используется только два уровня стека протоколов, варианты VPN, построенные на их основе, называют также **сетями VPN уровня 2** (Layer 2 VPN, L2VPN).
- Наличие в технологиях ATM и Frame Relay механизмов поддержки параметров QoS позволяет ATM VPN и Frame Relay VPN достаточно хорошо приближаться к частным сетям на выделенных каналах.
- Информация третьего уровня не анализируется и не меняется в этих сетях — это одновременно и достоинство, и недостаток.
  - Преимущество в том, что клиент может передавать по такому виртуальному каналу трафик любых протоколов, а не только IP. IP-адреса клиентов и поставщика услуг изолированы и независимы друг от друга.
  - Недостаток этого подхода состоит в том, что поставщик не оперирует IP-трафиком клиента и, следовательно, не может оказывать дополнительные услуги, связанные с сервисами IP.

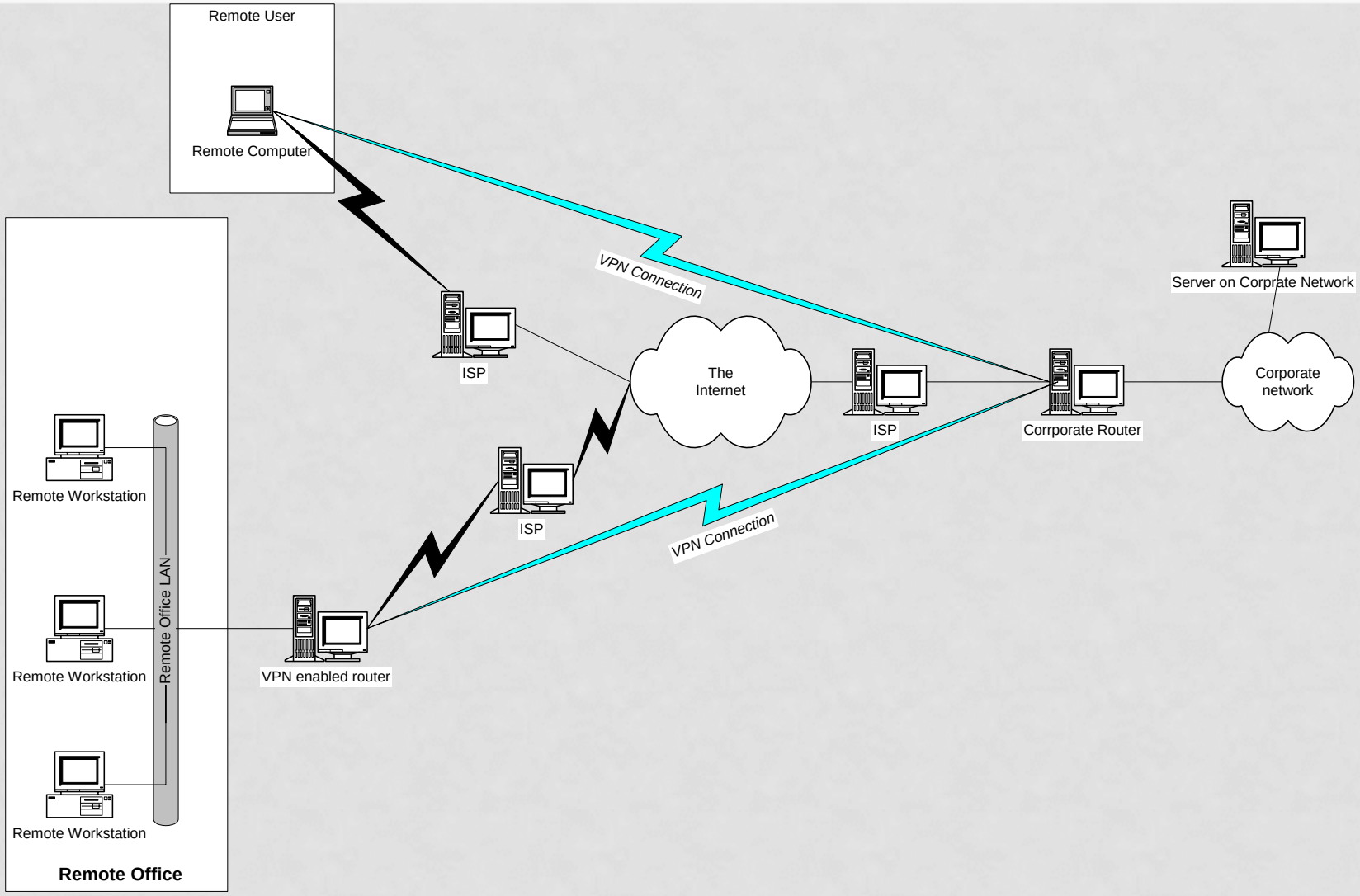
ВИРТУАЛЬНЫЕ ЧАСТНЫЕ СЕТИ (VPN) В WINDOWS

- Поддержка VPN в Windows
- PPTP
- L2TP/IPSec
- SSTP

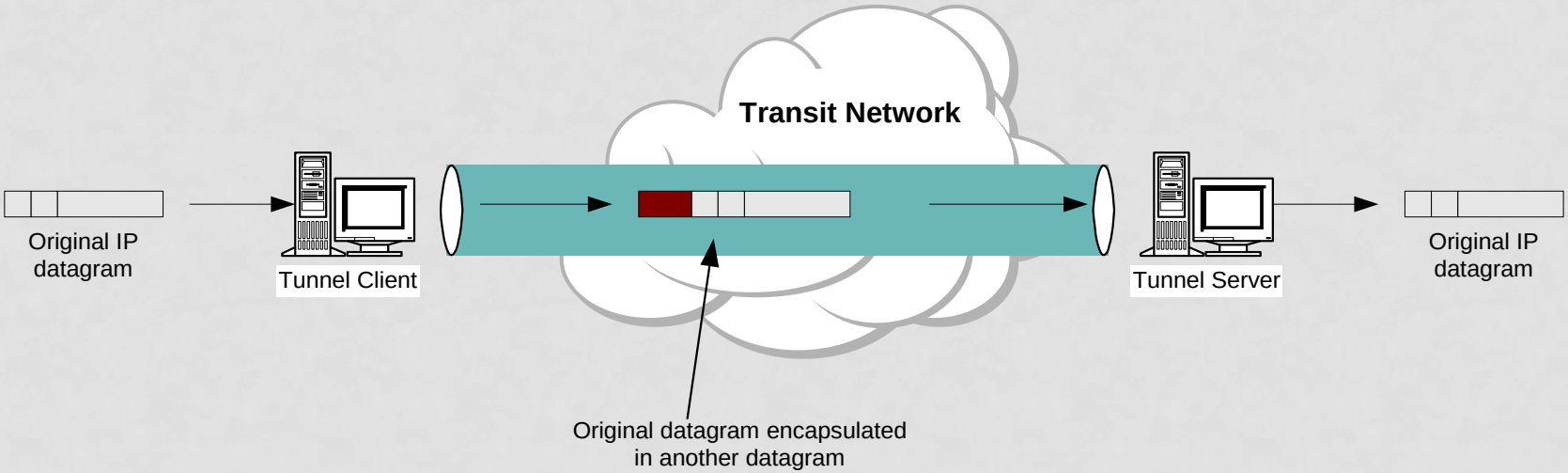
ОБЗОР VPN

- Клиенты и серверы VPN
- Типы VPN соединений
  - Удаленный доступ
  - Соединение шлюз-шлюз
- Протоколы VPN
  - Point-to-Point Tunneling Protocol (PPTP)
  - Layer Two Tunneling Protocol with Internet Protocol Security (L2TP/IPSec)
  - Secure Socket Tunneling Protocol (SSTP)

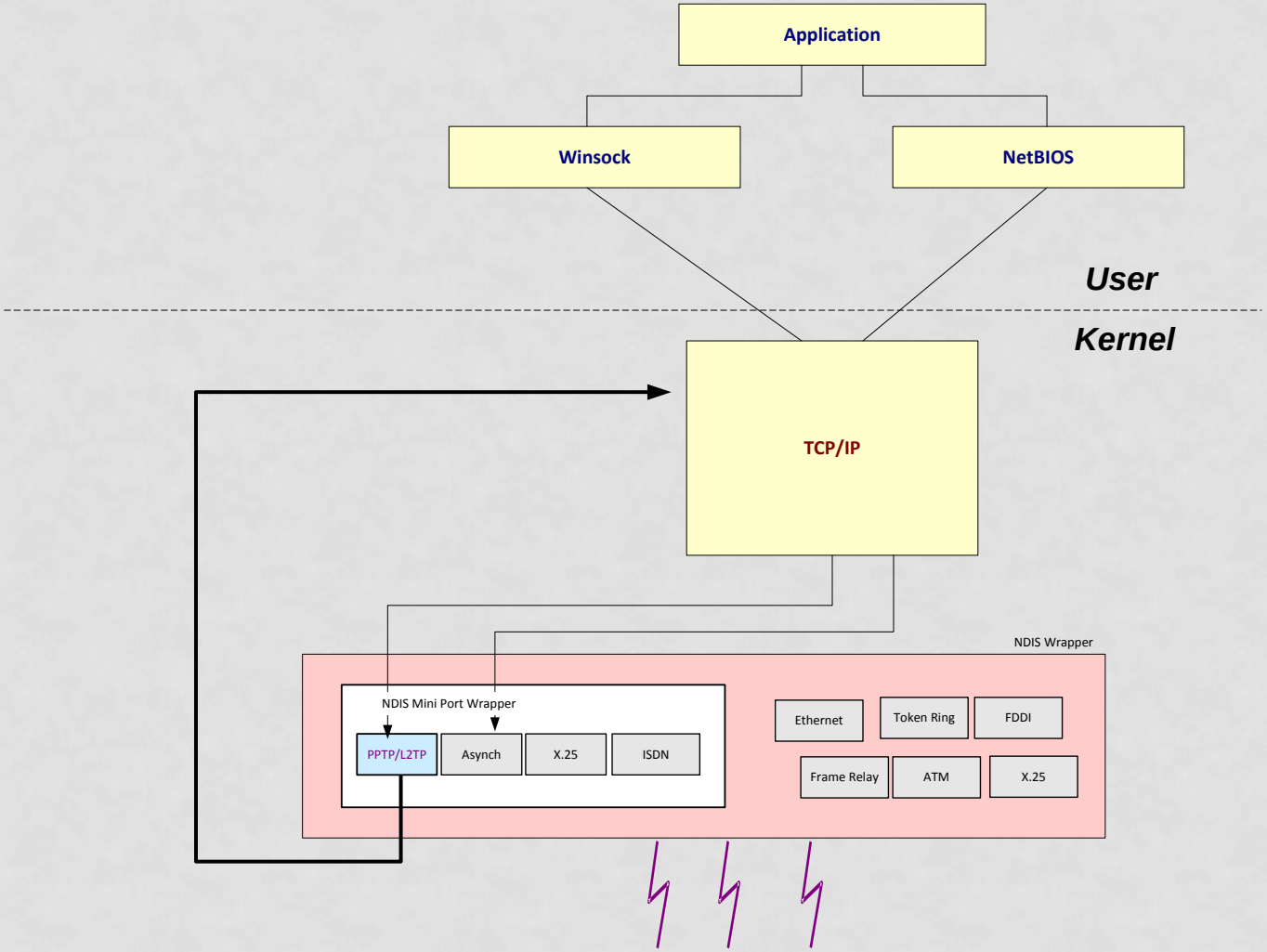
ВИРТУАЛЬНАЯ ЧАСТНАЯ СЕТЬ



ТУННЕЛИРОВАНИЕ В VPN



АРХИТЕКТУРА ТУННЕЛИРОВАНИЯ В WINDOWS



ОБЗОР VPN (ПРОДОЛЖЕНИЕ)

- VPN и PPP
  - Аутентификация пользователя
  - Сжатие данных
  - Шифрование данных (для PPTP)
- Выделение VPN адресов
- Сжатие VPN данных
- Шифрование данных в VPN

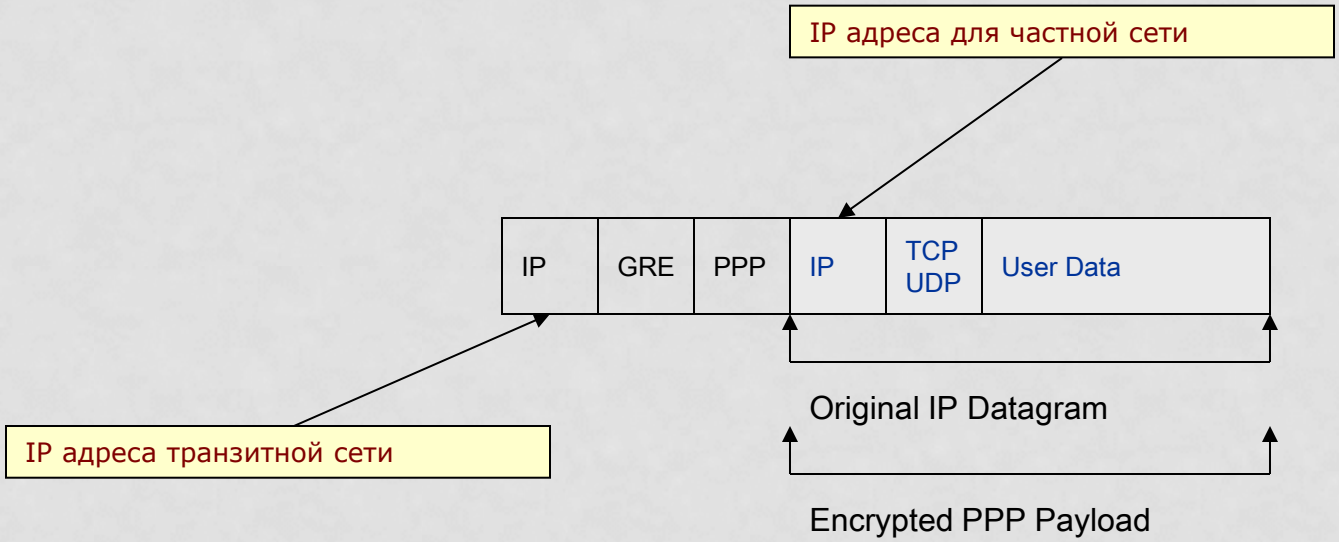
ПРОТОКОЛ PPTP

- Средства защищенного канала становятся прозрачными для приложений в тех случаях, когда они защищают кадры протоколов сетевого и канального уровней.
- Например, протокол PPTP (сам не являясь протоколом канального уровня) защищает кадры протокола PPP канального уровня, упаковывая их в IP-пакеты.
- В этом случае не имеет никакого значения, пакет какого протокола в свою очередь упакован в данном PPP-кадре: IP, IPX, SNA или NetBIOS.
  - С одной стороны, это делает сервис PPTP достаточно универсальным, так как клиент сервиса защищенного канала может использовать любые протоколы в своей сети.
  - С другой стороны, такая схема предъявляет жесткие требования к типу протокола канального уровня, используемому на участке доступа клиента к защищенному каналу — для протокола PPTP таким протоколом может быть *только PPP*.
- Протокол PPP очень распространен в линиях доступа, однако сегодня конкуренцию ему составляют протоколы Gigabit/Fast Ethernet, которые все чаще работают не только в локальных, но и глобальных сетях.

СПЕЦИФИКАЦИЯ PPTP

- Спецификация протокола была опубликована как «информационный» RFC 2637 в 1999 году. Она не была ратифицирована IETF.
- Протокол считается менее безопасным, чем другие VPN-протоколы, например, IPSec. PPTP работает, устанавливая обычную PPP сессию с противоположной стороной с помощью протокола GRE (Generic Routing Encapsulation). Второе соединение на TCP-порту 1723 используется для инициации и управления GRE-соединением.
- PPTP сложно перенаправлять за сетевой экран, так как он требует одновременного установления двух сетевых сессий.
- PPTP-трафик может быть зашифрован с помощью MPPE. Для аутентификации клиентов могут использоваться различные механизмы, наиболее безопасные из них — MSCHAP-v2 и EAP-TLS.

ИНКАПСУЛЯЦИЯ ДАННЫХ PPTP



УПРАВЛЕНИЕ СОЕДИНЕНИЯМИ В PPTP

- Управление созданием PPTP соединения
- Управление поддержкой PPTP соединения
- Управление завершением PPTP соединения

ПРОТОКОЛ GRE

- **GRE** (*Generic Routing Encapsulation* — общая инкапсуляция маршрутов) — протокол туннелирования сетевых пакетов, разработанный фирмой Cisco.
- Его основное назначение — инкапсуляция пакетов сетевого уровня сетевой модели OSI в IP пакеты. Номер протокола в IP — 47.

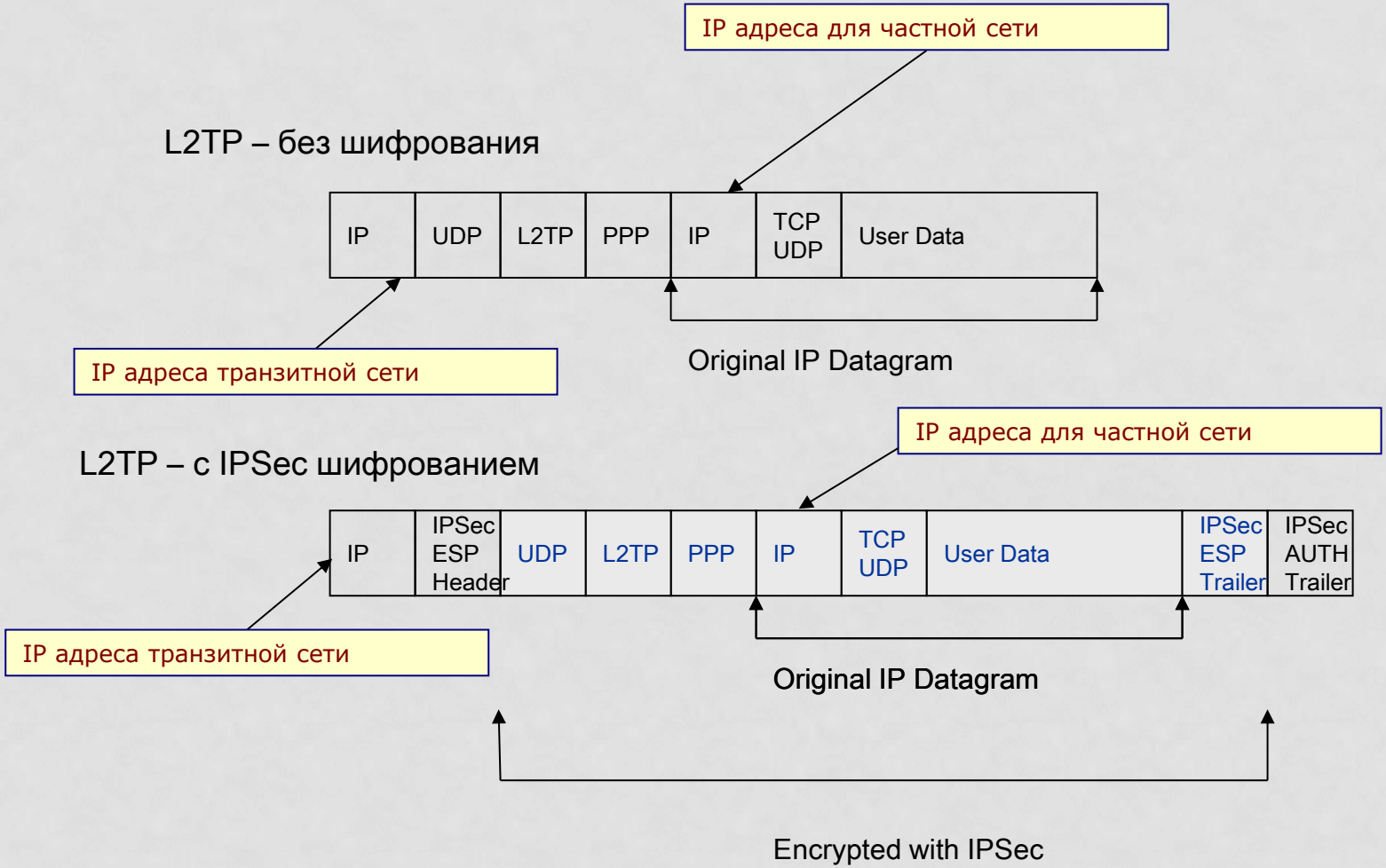
СЕТИ VPN НА ОСНОВЕ ШИФРОВАНИЯ

- Сети на основе шифрования применяются в тех случаях, когда VPN строится в дейтаграммной сети, которая не может обеспечить разграничения трафика. Такой сетью является классическая IP-сеть.
- Сегодня базовой технологией VPN на основе шифрования является технология IPSec, с помощью которой создается инфраструктура защищенных каналов.
- Стандарты IPSec обеспечивают высокую степень гибкости, позволяя выбирать нужный режим защиты (с шифрованием или только с обеспечением аутентичности и целостности данных), а также использовать различные алгоритмы аутентификации и шифрования.
- **Режим инкапсуляции IPSec** позволяет изолировать адресные пространства получателя (клиента) и поставщика услуг за счет применения двух IP-адресов — внешнего и внутреннего.

СОЗДАНИЕ ЗАЩИЩЕННЫХ КАНАЛОВ

- Защищенные каналы нужны для сетей CPVPN, в которых клиент самостоятельно создает туннели IPSec через IP-сеть поставщика услуг.
- От поставщика требуется только предоставление стандартного сервиса по объединению сетей, а значит, доступны как услуги сети поставщика, так и услуги Интернета.
- Сложность конфигурирования сетей IPSec VPN высокая, поскольку туннели IPSec двухточечные, то есть при полносвязной топологии их количество пропорционально N x (N - 1).
- Необходимо учесть задачу поддержания инфраструктуры открытых ключей (PKI).
- Пропускная способность каналов и другие параметры QoS этой технологией не поддерживаются, но если оператор предоставляет определенные параметры QoS (например, за счет дифференцированного обслуживания), это можно использовать при создании туннеля IPSec.

ИНКАПСУЛЯЦИЯ ДАННЫХ В L2TP/IPSEC



L2TP СОЕДИНЕНИЯ

- Создание L2TP соединения
- Поддержка L2TP соединения
- Завершение L2TP соединения

СОВМЕСТНОЕ ИСПОЛЬЗОВАНИЕ ТЕХНОЛОГИЙ

Технологии VPN на основе шифрования можно применять *совместно* с технологиями VPN на основе разделения трафика для повышения уровня защищенности виртуальных частных сетей.

Технологии VPN на основе разделения трафика иногда критикуют за недостаточный уровень безопасности, считая, что отсутствие шифрования трафика позволяет персоналу поставщика услуг получить несанкционированный доступ к данным.

Такая вероятность существует, поэтому клиент услуг VPN на основе разделения трафика, например MPLS VPN, может самостоятельно повысить защищенность своего трафика, применив технику IPSec.

КРИТЕРИИ ОЦЕНКИ И СРАВНЕНИЯ VPN

Практически все сети VPN имитируют *собственные каналы* в сетевой инфраструктуре поставщика, предназначенной для обслуживания множества клиентов.

Когда имитируется инфраструктура каналов одного предприятия, услуги VPN называют также услугами **intranet** *(интранет, или внутренней сети)*

Когда к таким каналам добавляются также каналы, соединяющие предприятие с его предприятиями-партнерами, с которыми также необходимо обмениваться информацией в защищенном режиме, — услугами **extranet** *(экстранет, или внешней сети)*.

КРИТЕРИИ ОЦЕНКИ И СРАВНЕНИЯ VPN

- Другим критерием, используемым при сравнении VPN, является *степень приближенности сервисов, предлагаемых VPN, к свойствам сервисов частной сети*.
- Во-первых, важнейшим свойством сервисов частной сети является *безопасность*.
  - Безопасность VPN подразумевает весь набор атрибутов защищенной сети — конфиденциальность, целостность и доступность информации при передаче через общедоступную сеть, а также защищенность внутренних ресурсов сетей потребителя и поставщика от внешних атак.
  - Степень безопасности VPN варьируется в широких пределах, в зависимости от применяемых средств защиты — шифрования трафика, аутентификации пользователей и устройств, изоляции адресных пространств (например, на основе техники NAT), использования виртуальных каналов и двухточечных туннелей, затрудняющих подключение к ним несанкционированных пользователей.

КРИТЕРИИ ОЦЕНКИ И СРАВНЕНИЯ VPN

- Во-вторых, желательно, чтобы сервисы VPN приближались к сервисам частной сети *по качеству обслуживания*.
  - Качество транспортного обслуживания подразумевает, в первую очередь, гарантии пропускной способности для трафика клиента, к которым могут добавляться и другие параметры QoS — максимальные задержки и процент потерянных данных.
  - В пакетных сетях пульсации трафика, переменные задержки и потери пакетов — неизбежное зло, поэтому степень приближения виртуальных каналов к каналам TDM всегда неполная и вероятностная (в среднем, но никаких гарантий для отдельно взятого пакета).
  - Разные пакетные технологии отличаются различным уровнем поддержки параметров QoS.
  - В ATM, например, механизмы качества обслуживания наиболее совершенны и отработаны, а в IP-сетях они только начинают внедряться.
  - Считается, что безопасность — обязательное свойство VPN, а качество транспортного обслуживания — только желательное.

КРИТЕРИИ ОЦЕНКИ И СРАВНЕНИЯ VPN

- В-третьих, сеть VPN приближается к реальной частной сети, если она обеспечивает для клиента *независимость адресного пространства.*
  - Независимость адресного пространства дает клиенту одновременно и удобство конфигурирования, и способ поддержания безопасности.
  - Желательно, чтобы не только клиенты ничего не знали об адресных пространствах друг друга, но и магистраль поставщика имела собственное адресное пространство, неизвестное пользователям.
  - В этом случае сеть поставщика услуг будет надежнее защищена от умышленных атак или неумышленных действий своих клиентов.