Тема 2.2. Обеспечение информационной безопасности на сетевом уровне

Лекция 3. Методы и средства обеспечения ИБ каналов

Дисциплина: Анализ информационных потребностей подразделений информационно-аналитического мониторинга

Доцент: Кирьянов Александр Владимирович
email:kiryanov_a@mirea.ru

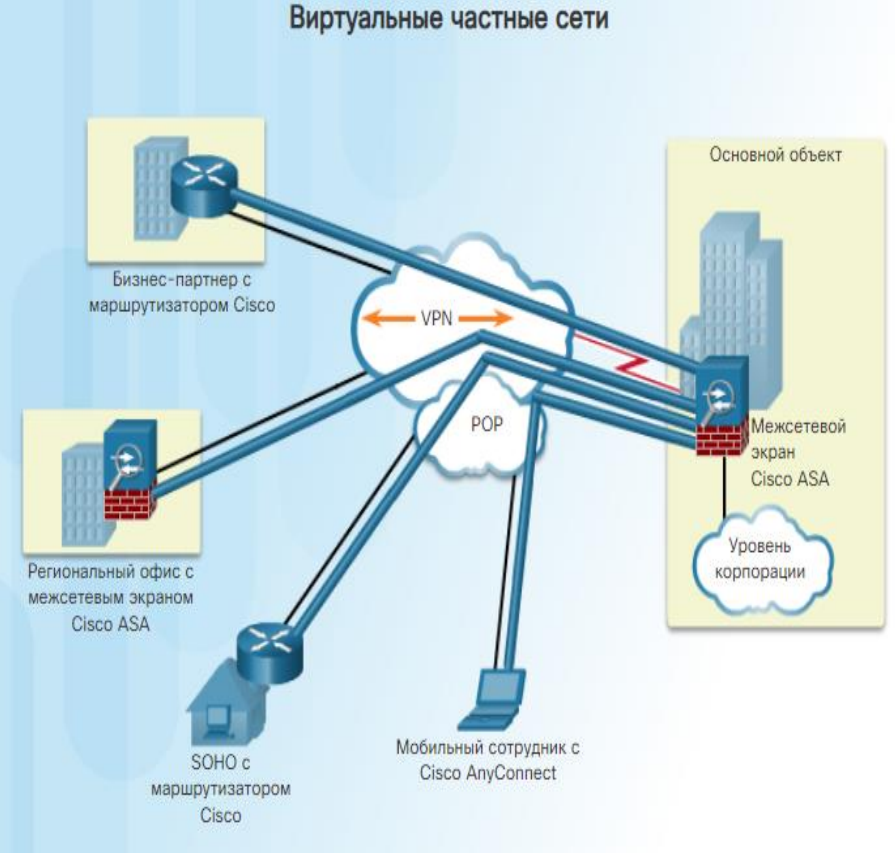
**Учебные вопросы:**

1. Сети VPN.
2. Протокол IPSec.
3. Протоколы GRE, PPTP, L2TP

Виртуальные частные сети (VPN - Virtual Private Networks) используются в организациях для создания сквозного частного сетевого подключения через сторонние сети, например через Интернет или экстранет. Сети VPN используют туннель, благодаря которому удаленные пользователи могут получать доступ к сетевым ресурсам центрального офиса. Однако сети VPN не могут гарантировать, что при передаче по туннелю информация останется конфиденциальной. Поэтому в сетях VPN применяются современные криптографические методы, позволяющие устанавливать защищенные, сквозные частные сетевые подключения.

# Первый учебный вопрос.
# Сети VPN.






VPN – это частная сеть, которая создана через сеть общего пользования, обычно через Интернет. Вместо применения выделенных физических подключений, в VPN используются виртуальные подключения, маршрутизируемые через Интернет из организации на удаленную площадку. Первыми сетями VPN фактически были обычные IP-туннели, в которых не выполнялись операции аутентификации или шифрования данных.

Например, универсальная инкапсуляция при маршрутизации (Generic Routing Encapsulation, GRE) — это протокол туннелирования, разработанный компанией Cisco, который позволяет инкапсулировать пакеты протоколов сетевого уровня различного типа внутри IP-туннелей. Благодаря этому создаётся виртуальный канал «точка-точка» до маршрутизаторов Cisco в удалённых точках поверх IP-сети.

В настоящее время под виртуальными частными сетями обычно понимают защищённую реализацию сети VPN с шифрованием (например IPsec VPN).

Для реализации сетей VPN требуется шлюз VPN. Шлюзом VPN может быть маршрутизатор, межсетевой экран или устройство адаптивной защиты. Обычно это автономный межсетевой экран, который объединяет в пределах одного образа программного обеспечения функции межсетевого экрана, концентратора VPN, а также системы предотвращения вторжений.

# Первый учебный вопрос.
# Сети VPN.

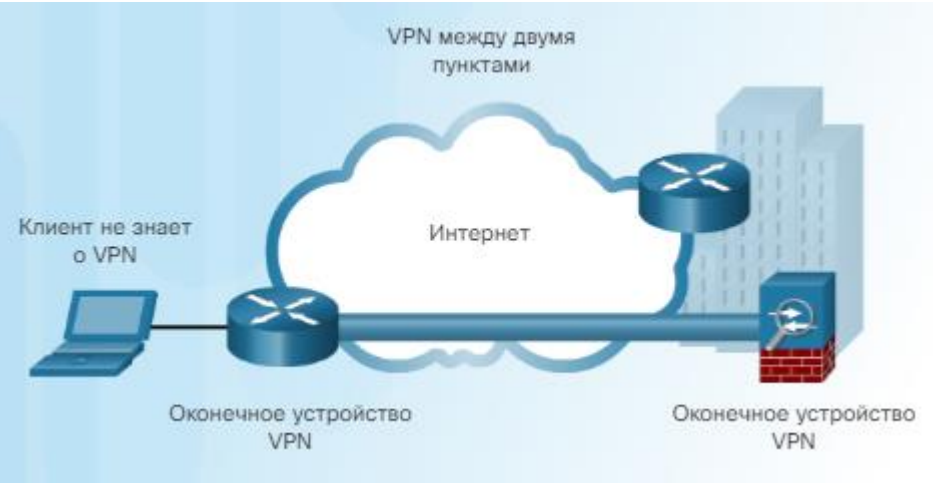


| Основные преимущества VPN | |
|---|---|
| **Преимущество** | Описание |
| **Сокращение затрат** | Благодаря появлению экономически эффективных, высокоскоростных технологий организации могут использовать сети VPN для сокращения своих затрат на подключение к сети при одновременном повышении пропускной способности удаленных подключений. |
| **Безопасность** | Сети VPN обеспечивают максимально возможный уровень безопасности благодаря применению сложных протоколов шифрования и аутентификации, защищающих данные от несанкционированного доступа. |
| **Масштабируемость** | Сети VPN позволяют организациям использовать Интернет, упрощая процесс добавления новых пользователей без существенного усложнения существующей инфраструктуры. |
| **Совместимость** | Сети VPN могут быть реализованы с использованием каналов WAN различного типа, включая все популярные широкополосные технологии. Удаленные сотрудники могут пользоваться возможностями таких высокоскоростных подключений для получения безопасного доступа к своим корпоративным сетям. |

**Типы сетей VPN:**

**Существуют сети VPN двух типов:**

- Site-to-site (межузловые или межфилиальные)
- Remote access (удалённого доступа)




**Site-to-site VPN**

Сеть site-to-site VPN создаётся, когда устройства на обеих сторонах подключения VPN заранее знают настройки сети VPN. Сеть VPN остается статической, и внутренние узлы не знают о существовании VPN. В межузловой сети VPN оконечные компьютеры отправляют и получают обычный трафик TCP/IP через шлюз VPN. Шлюз VPN отвечает за инкапсуляцию и шифрование исходящего трафика для всего трафика, поступающего с конкретного объекта. Затем шлюз VPN передаёт этот трафик через туннель VPN по Интернету в равноправный соседний шлюз VPN на стороне приема. При получении данных соседний шлюз VPN удаляет заголовки, расшифровывает содержимое и передаёт пакет в узел назначения по своей частной сети.

Межузловая сеть VPN представляет собой расширение классической сети WAN. Межузловые сети VPN позволяют подключать друг к другу целые сети, например сеть филиала с сетью главного офиса компании. Ранее для подключения площадок между собой требовалась выделенная линия или подключение Frame Relay. Но так как сегодня большинство корпораций имеют доступ к провайдеру, то вместо таких подключений можно использовать межузловые сети VPN.


**Сети VPN удалённого доступа**

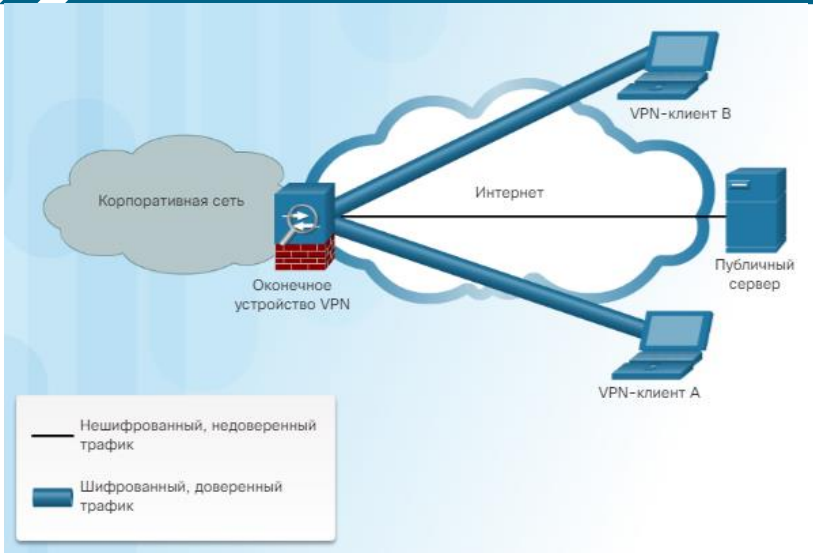
В то время как межфилиальная сеть VPN используется для подключения целых сетей, сеть VPN удалённого доступа (remote access) соответствует потребностям удалённых и мобильных сотрудников, а также позволяет передавать трафик от потребителей к компаниям через экстранет. VPN удалённого доступа создаётся в тех случаях, когда информация о VPN не является статической, и может изменяться динамически, а сам канал может включаться и отключаться. Сети VPN удалённого доступа поддерживают архитектуру «клиент-сервер», в рамках которой клиент VPN (удалённый компьютер) получает защищённый доступ к корпоративной сети через сервер VPN на границе сети.

Они используются для подключения отдельных компьютеров, которым требуется безопасный доступ к корпоративной сети через Интернет. На оконечных устройствах мобильных пользователей может требоваться установка клиентского ПО для VPN.

Когда узел пытается отправить любой трафик, клиентское ПО инкапсулирует и шифрует этот трафик. Затем зашифрованные данные отправляются через Интернет на шлюз VPN на границе сети назначения. При получении данных шлюз VPN работает точно так же, как для межузловых сетей VPN.

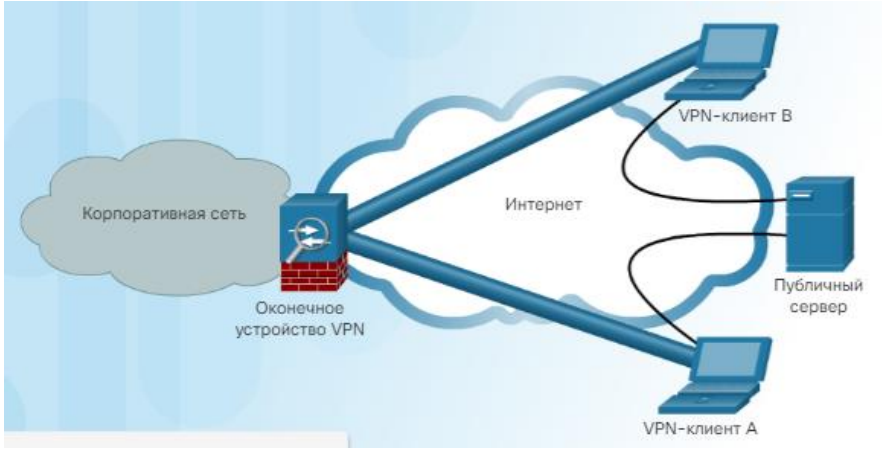
# Первый учебный вопрос.
# Сети VPN.





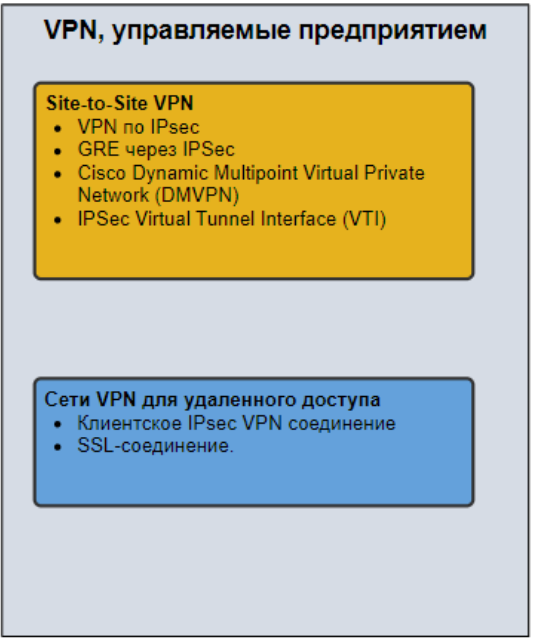

Разворот пакетов (Hairpinning) – термин, используемый для описания ситуации, при которой VPN-трафик, входящий в интерфейс, также может маршрутизироваться на выходе из того же интерфейса. Рассмотрим, например, топологию hub-and-spoke (звезда) на рисунке. Оконечное устройство VPN в корпоративной сети является «ступицей» (hub), а клиенты VPN для удаленного доступа – «спицами» (spoke). Чтобы обеспечить связь между двумя «спицами», трафик должен проходить через оконечное устройство VPN. Также можно использовать метод «разворота пакетов» (hairpinning), когда сети VPN для удаленного доступа необходимо подключать к оконечному устройству VPN в корпоративной штаб-квартире до того, как трафику будет разрешено проходить в Интернет.

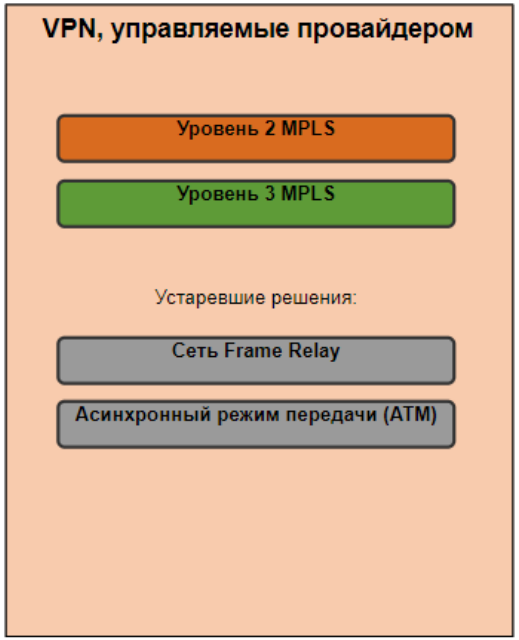
Если корпоративная политика обязывает, что VPN-трафик должен быть разделен на трафик, предназначенный для корпоративных (доверенных) подсетей, и трафик, предназначенный для (недоверенного) Интернета, можно использовать метод разделенного туннелирования (Split tunneling). В сценарии, показанном на рисунке, разделение трафика выполняется под управлением программного обеспечения VPN в клиенте удаленного доступа. Если трафик предназначен для корпоративной подсети, он отправляется через VPN-туннель. В противном случае он отправляется в виде нешифрованного (недоверенного) трафика в Интернет.



# Первый учебный вопрос.
# Сети VPN.






Существует много вариантов защиты корпоративного трафика. Эти решения различаются в зависимости от того, кто управляет VPN.

**VPN можно управлять и развертывать как:**

- **VPN для крупных компаний** - корпоративные VPN являются распространенным решением для защиты корпоративного трафика через Интернет. VPN типа site-to-site и удаленный доступ создаются и управляются предприятием с использованием IPsec и SSL VPN.
- **VPN операторов связи** - управляемые провайдером VPN-сервисы создаются и управляются через сеть провайдера. Провайдер использует многопротокольную коммутацию по меткам (MPLS) на уровне 2 или уровне 3 для создания безопасных каналов между сайтами предприятия. Multiprotocol Label Switching (MPLS) - это технология маршрутизации, которую провайдер использует для создания виртуальных путей между сайтами. Эта технология эффективно разделяет трафик от разных клиентов. Старые решения включают в себя Frame Relay и режим асинхронной передачи (ATM) VPN.

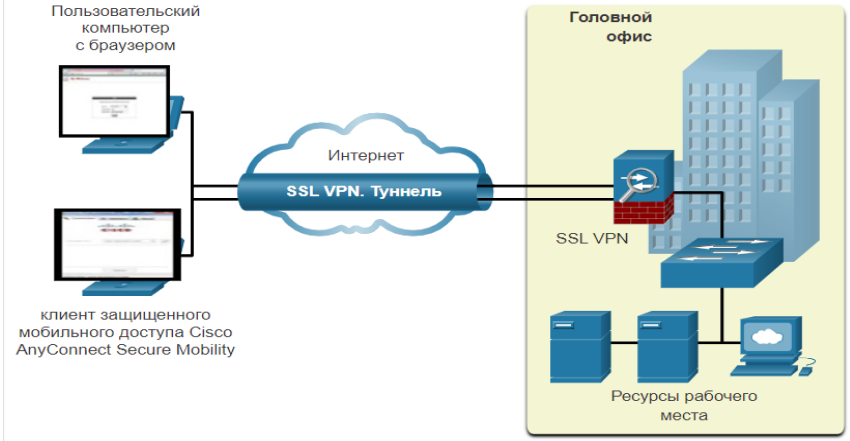
**Выводы по первому учебному вопросу.**

VPN стали логическим решением для подключения удаленного доступа по многим причинам.

VPN с удаленным доступом позволяют удаленным и мобильным пользователям безопасно подключаться к предприятию, создавая зашифрованный туннель. Удаленные пользователи могут безопасно копировать свой корпоративный доступ для обеспечения безопасности, включая электронную почту и сетевые приложения. VPN для удаленного доступа также позволяют подрядчикам и партнерам иметь ограниченный доступ к определенным серверам, веб-страницам или файлам по мере необходимости. Это означает, что эти пользователи могут способствовать повышению эффективности бизнеса без ущерба для безопасности сети.

# Второй учебный вопрос.
# Протокол IPSec.






Сети VPN для удаленного доступа обычно включаются пользователем динамически, когда это необходимо. VPN для удаленного доступа могут быть созданы с использованием IPsec или SSL. Как показано на рисунке, удаленный пользователь должен инициировать VPN-подключение удаленного доступа.

На рисунке изображены два способа, с помощью которых удаленный пользователь может инициировать VPN-подключение удаленного доступа: бесклиентное VPN и клиентское VPN.

На рисунке показаны два способа, с помощью которых удаленный пользователь может инициировать VPN-подключение удаленного доступа: бесклиентное VPN и клиентское VPN. Ноутбук одного пользователя подключен к Центральному офису через туннель SSL VPN через Интернет с помощью пользовательского веб-браузера. Второй ноутбук подключен к Центральному офису через Интернет с помощью Cisco AnyConnect Secure Mobility Client.

- **Бесклиентное VPN-соединение** -Соединение защищено с помощью SSL-соединения через веб-браузер. SSL в основном используется для защиты HTTP-трафика (HTTPS) и почтовых протоколов, таких как IMAP и POP3. Например, HTTPS на самом деле HTTP с использованием туннеля SSL. Сначала устанавливается SSL-соединение, а затем по нему происходит обмен данными HTTP.
- **Клиентское VPN-соединение** - Программное обеспечение VPN-клиента, такое как Cisco AnyConnect Secure Mobility Client, должно быть установлено на конечном устройстве удаленного пользователя. Пользователи должны инициировать VPN-соединение с помощью VPN-клиента, а затем пройти аутентификацию на целевом VPN-шлюзе. Когда удаленные пользователи аутентифицируются, они получают доступ к корпоративным файлам и приложениям. Программное обеспечение VPN-клиента шифрует трафик с использованием IPsec или SSL и передает его через Интернет на целевой VPN-шлюз.

# Второй учебный вопрос.
# Протокол IPSec.

## В таблице сравниваются протоколы IPsec и SSL

| Функция | Протокол IPsec | SSL |
|---|---|---|
| **Поддержка приложений** | Обширная - все IP-приложения поддерживаются. | Ограниченная - поддерживаются только веб-приложения и обмен файлами. |
| **Аутентификация** | Сильная - использование двусторонней аутентификации с общими ключами или цифровыми сертификатами. | Умеренная - Использование односторонней или двусторонней аутентификации. |
| **Шифрование** | Сильная - использует длину ключа от 56 до 256 бит. | От умеренного до сильного - С длиной ключа от 40 бит до 256 бит. |
| **Сложность подключения** | Средняя - для этого требуется предварительно установленный VPN-клиент на хосте. | Низкий - требуется только веб-браузер на хосте. |
| **Варианты подключения** | Ограниченный - только определенные устройства с определенными конфигурациями могут подключаться. | Обширный - любое устройство с веб-браузером может подключиться. |

# Второй учебный вопрос.
# Протокол IPSec.



**Технология IPsec**

IPsec – это стандарт IETF (RFC 2401-2412), который определяет способ защиты сетей VPN в IP-сетях. Протокол IPsec обеспечивает защиту и аутентификацию IP-пакетов между источником и местом назначения. IPsec может защищать практически весь трафик от уровня 4 до уровня 7.

**Благодаря структуре IPsec, данный протокол выполняет следующие основные функции обеспечения безопасности:**

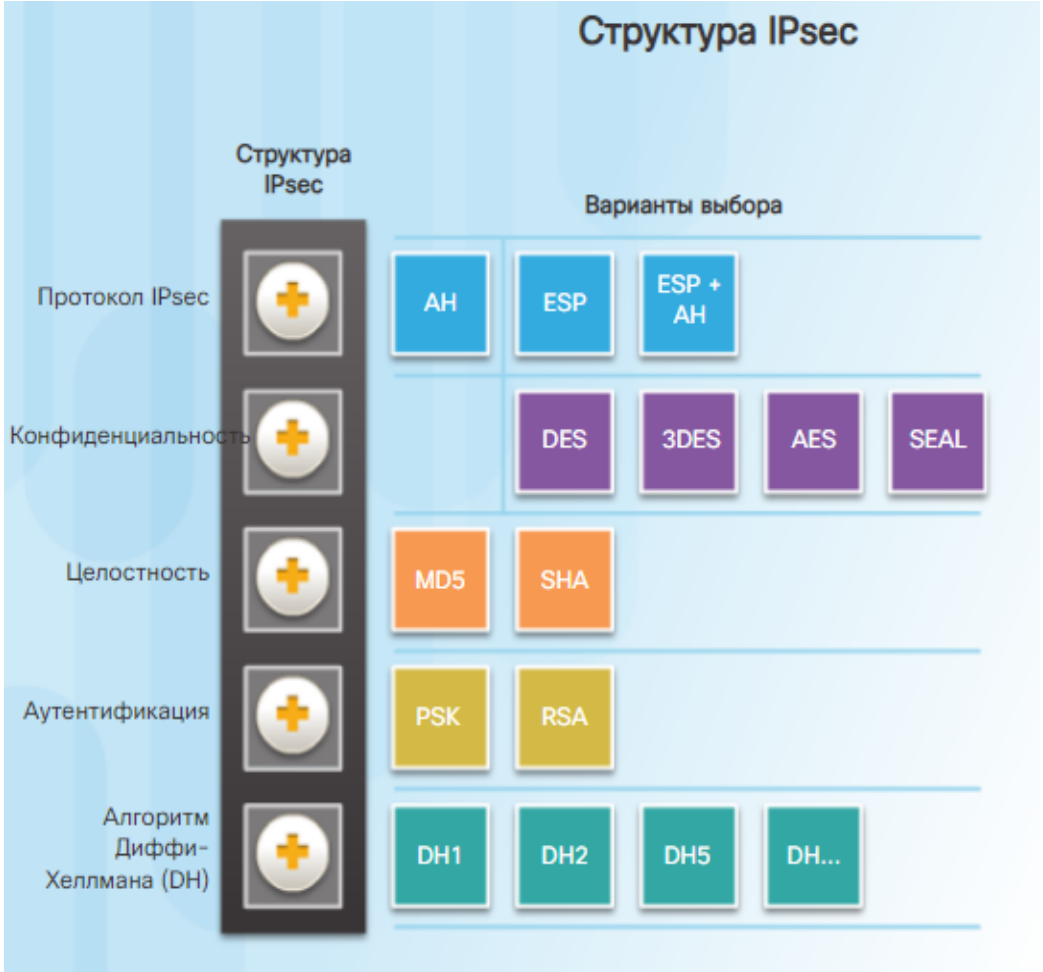
- конфиденциальность с помощью шифрования,
- целостность с помощью алгоритмов хеширования,
- аутентификация с помощью протокола Internet Key Exchange (IKE),
- безопасный обмен ключами с помощью алгоритма Диффи-Хеллмана (DH).

# Второй учебный вопрос.
# Протокол IPSec.



IPsec представляет собой структуру открытых стандартов, определяющую правила для организации защищённой связи.

Протокол IPsec не связан с конкретными методами шифрования и аутентификации, алгоритмами обеспечения безопасности или технологией обмена ключами.



# Второй учебный вопрос.
# Протокол IPSec.

Для обеспечения безопасной связи в протоколе IPsec используются существующие алгоритмы. IPsec позволяет создавать новые, более качественные алгоритмы, для разработки которых корректировать существующие стандарты IPsec не потребуется.

# Второй учебный вопрос.
# Протокол IPSec.

IPsec функционирует на сетевом уровне, обеспечивая защиту и аутентификацию пакетов IP между взаимодействующими устройствами IPsec, которые также называются узлами (peer). IPsec позволяет защитить путь между парой шлюзов, парой компьютеров или между шлюзом и компьютером. В результате IPsec может защищать практически любой трафик приложений, так как можно реализовать защиту на уровнях с 4-го по 7-й.

Во всех реализованных решениях протокола IPsec применяется незашифрованный заголовок 3-го уровня, поэтому никаких проблем с маршрутизацией не существует.

IPsec функционирует поверх любых протоколов 2-го уровня, таких как Ethernet, ATM и Frame Relay.

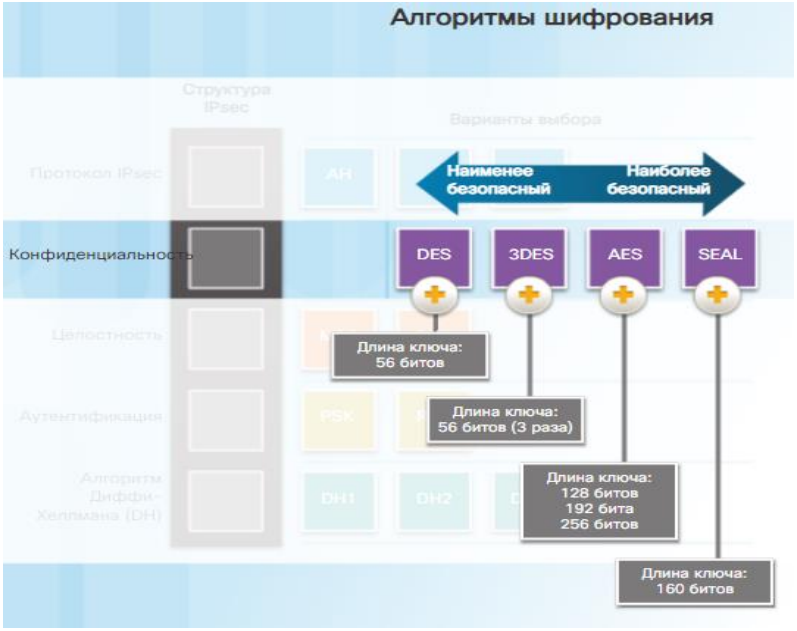
**Основные особенности протокола IPsec:**

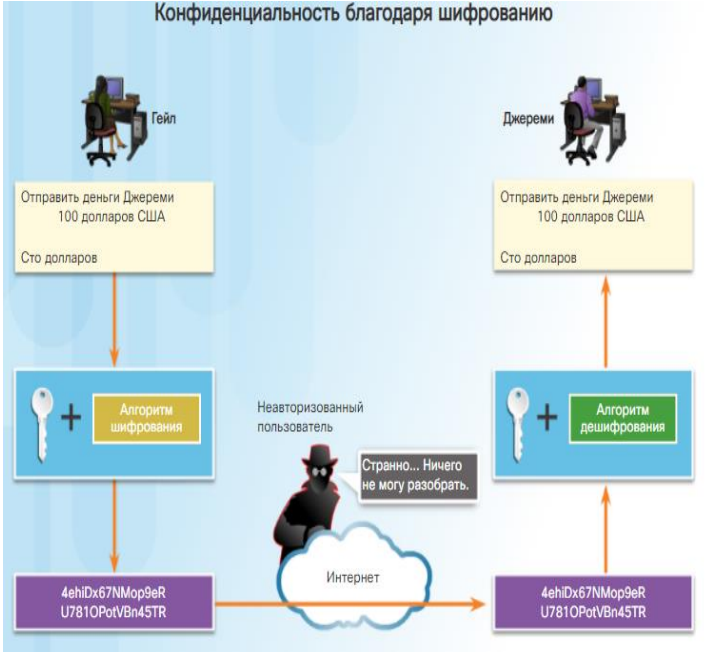
- IPsec — это структура открытых стандартов, независимая от алгоритмов.
- IPsec обеспечивает конфиденциальность и целостность данных, а также аутентификацию источника.
- IPsec действует как протокол сетевого уровня, защищая пакеты IP и проверяя их подлинность.

# Второй учебный вопрос.
# Протокол IPSec.

**Рассмотрим сервисы безопасности IPsec:**

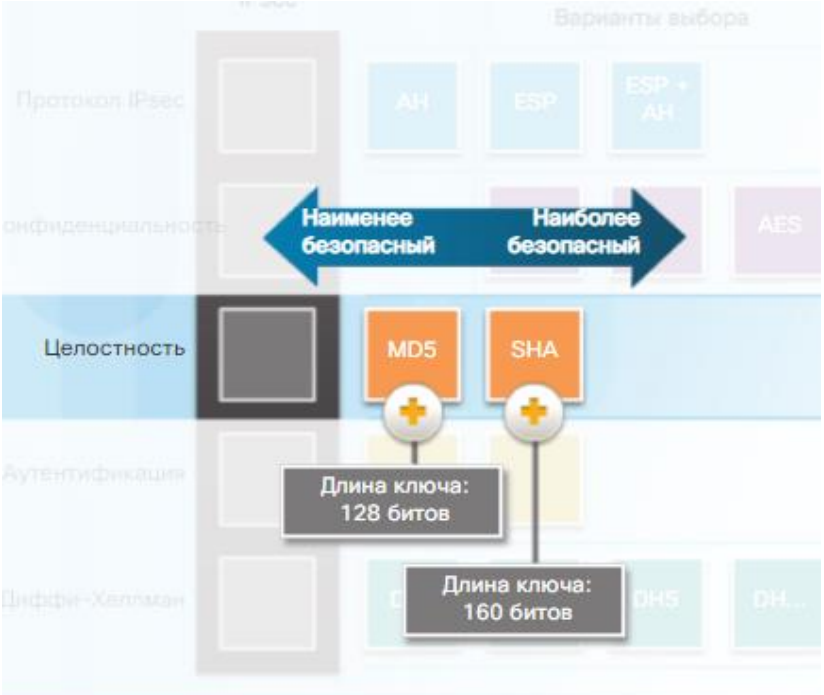
**1.Конфиденциальность (шифрование)** — в сети VPN частные данные передаются по публичной сети. Поэтому ключевой задачей является обеспечение конфиденциальности данных. Для этого перед передачей данных по сети выполняется шифрование данных.

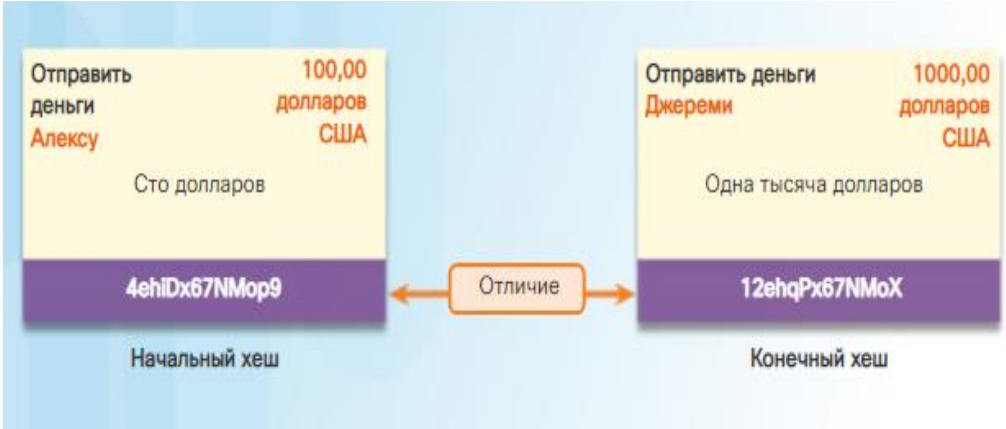



Шифрование — это процесс кодирования всех данных, отправляемых с одного компьютера на другой, в ту форму, которую может декодировать только принимающий компьютер. В случае перехвата сообщения злоумышленник (хакер) не сможет его прочесть. IPsec предоставляет расширенные функции безопасности (например, криптостойкие алгоритмы шифрования).

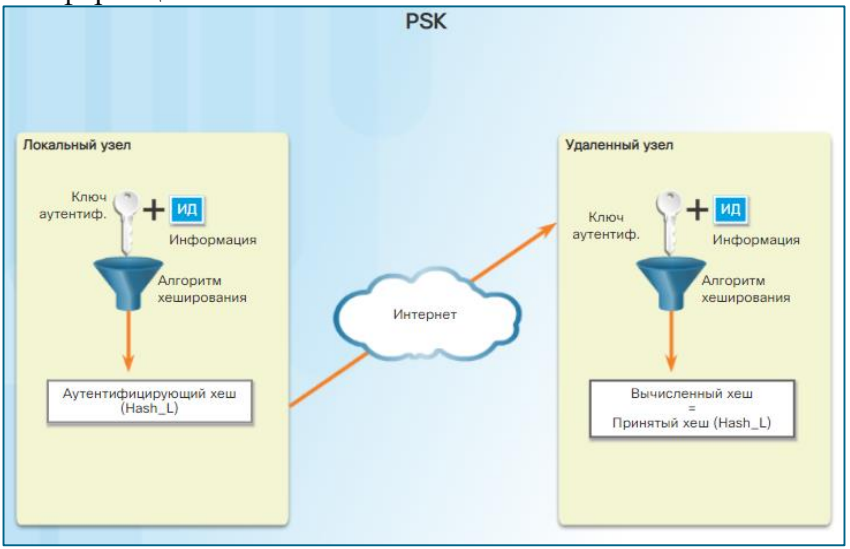
**2. Целостность данных** — Получатель может убедиться, что данные были нормально переданы через Интернет и никак не были изменены. Важно не только обеспечить шифрование данных в публичной сети, но и убедиться, что они не были изменены в пути.

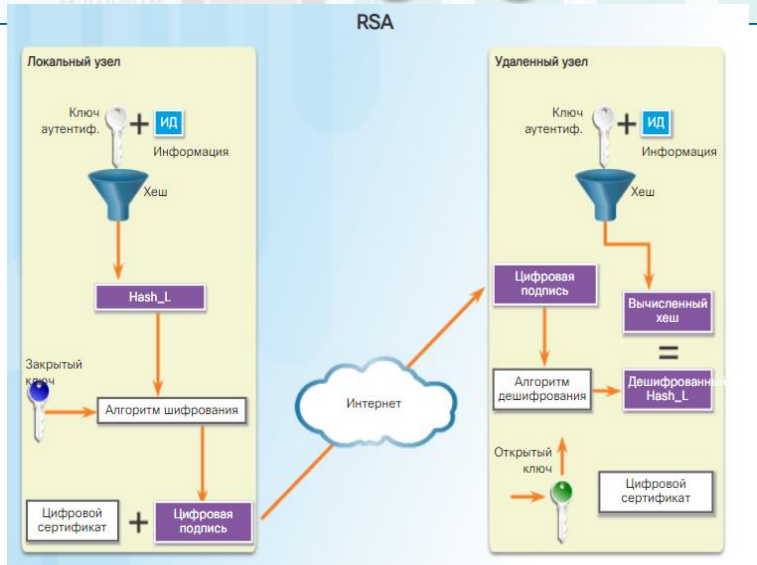



В IPsec предусмотрен механизм проверки отсутствия изменений в шифрованной части пакета, во всём заголовке или в теле данных пакета. IPsec гарантирует целостность данных с помощью контрольных сумм (применяется простая проверка с использованием избыточности). При обнаружении искажений пакет удаляется.

**3. Аутентификация** — позволяет проверить, кто был источником отправленных данных. Это необходимо для защиты от атак, использующих спуфинг (подмену отправителя). Аутентификация позволяет гарантировать установление подключения к нужному партнеру по связи. Получатель может проверять подлинность источника пакета, сертифицируя источник информации.


В IPsec используется технология обмена ключами по Интернету (Internet Key Exchange, IKE) для проверки подлинности пользователей и устройств, которые могут устанавливать связь независимо друг от друга. В IKE применяется аутентификация различного типа (в частности, используются имя пользователя и пароль, одноразовый пароль, биометрия, предварительно распространяемый общий ключ (Pre-Shared Key, PSK) и цифровые сертификаты).

**4. Безопасный обмен ключами** — В алгоритмах шифрования для выполнения операций шифрования и дешифрования требуется симметричный, общий секретный ключ. Как шифрующее и дешифрующее устройства получают общий секретный ключ? Самый простой метод обмена ключами состоит в том, чтобы использовать метод обмена открытыми ключами, например Диффи-Хеллмана (DH). Существуют методы обмена ключами DH разного типа, которые обозначаются как группы DH:


Группы DH 1, 2 и 5 поддерживают возведение в степень по простому модулю с размером ключа 768, 1024 и 1 536 битов соответственно. После 2012 г. эти группы использовать не рекомендуется.

Группы DH 14, 15 и 16 используют ключи большего размера, а именно 2048, 3072 и 4096 битов соответственно, и рекомендуются для использования до 2030 г.

Группы DH 19, 20, 21 и 24 с соответствующими размерами ключа 256, 384, 521 и 2048 битов поддерживают метод криптографии Elliptical Curve Cryptography (ECC), который уменьшает время, необходимое для генерирования ключей.

Группа DH 24 является предпочтительным методом шифрования следующего поколения.

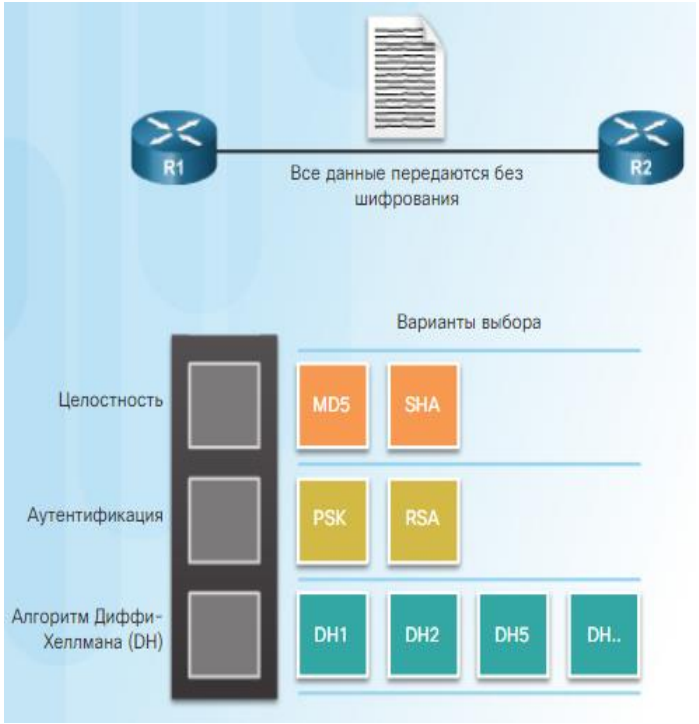
**Обзор протоколов Ipsec**

**Двумя основными протоколами IPsec являются Authentication Header (AH) и Encapsulation Security Protocol (ESP).**

Протокол IPsec представляет собой первый структурный блок в данной структуре. В зависимости от выбора AH или ESP, окажутся доступны другие структурные блоки.

**Аутентифицирующий заголовок (Authentication Header, AH)**

AH обеспечивает подлинность путем применения однонаправленной функции хеширования на основе ключа к пакету для создания хеша или дайджеста сообщения. Хеш объединяется с текстом и передается в открытом виде.
Получатель обнаруживает изменения в любой части пакета, которые происходят при передаче, путем выполнения той же однонаправленной функции хеширования в принятом пакете и сравнения результата со значением дайджеста сообщения, переданного отправителем. Подлинность обеспечивается благодаря тому, что однонаправленный хеш также использует общий секретный ключ между двумя системами.



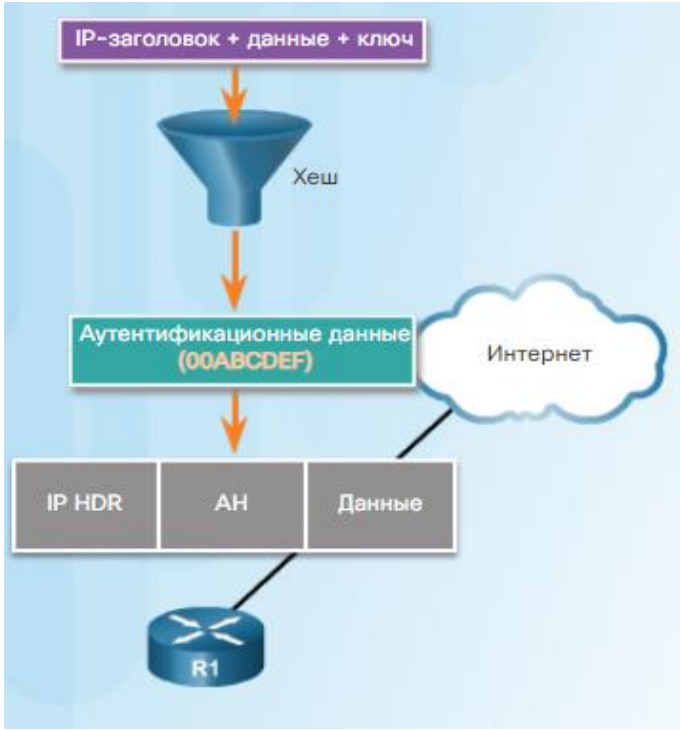
# Второй учебный вопрос.
# Протокол IPSec.



Функция AH применяется ко всему пакету, кроме любых полей IP-заголовка, которые, как правило, изменяются в ходе передачи. Поля, которые обычно изменяются во время передачи, называются мутабильными полями. Например, поле Time to Live (TTL) считается мутабильным, так как маршрутизаторы изменяют данное поле.

Процесс AH выполняется в следующем порядке:

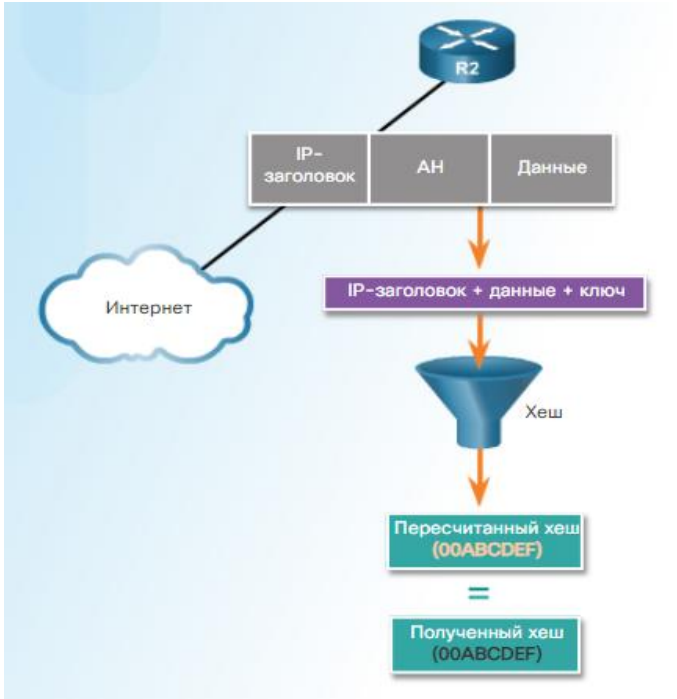
1. IP-заголовок и полезная нагрузка хешируются с помощью общего секретного ключа.
2. Хеш формирует новый заголовок AH, который вставляется в исходный пакет.



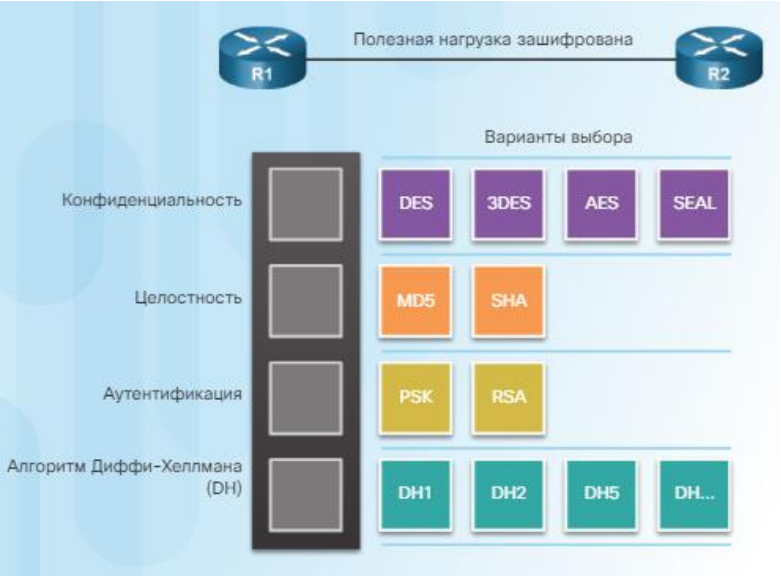
3. Новый пакет передается на маршрутизатор другого узла IPsec.
4. Другой маршрутизатор хеширует IP-заголовок и полезную нагрузку, используя общий секретный ключ, извлекает переданный хеш из заголовка AH и сравнивает два хеша.

Хеши должны полностью совпасть друг с другом. Если в переданном пакете один бит изменяется, то результат хеша в пакете будет изменен и заголовки AH не будут совпадать.

AH поддерживает алгоритмы MD5 и SHA. Процесс AH может не работать, если в среде используется NAT.



# Второй учебный вопрос.
# Протокол IPSec.




Как показано на рисунке, ESP обеспечивает конфиденциальность путем шифрования полезной нагрузки. Данная функция поддерживает различные алгоритмы симметричного шифрования. Если в качестве протокола IPsec выбран ESP, также необходимо выбрать алгоритм шифрования. По умолчанию для IPsec используется 56-битовый алгоритм DES. В продуктах Cisco для более стойкого шифрования также могут применяться алгоритмы 3DES, AES и SEAL.

ESP также может обеспечивать целостность и аутентификацию. Сперва шифруется полезная нагрузка. Затем шифрованная полезная нагрузка обрабатывается с помощью алгоритма хеширования, например MD5 или SHA. Хеш обеспечивает аутентификацию и целостность данных для полезной нагрузки.

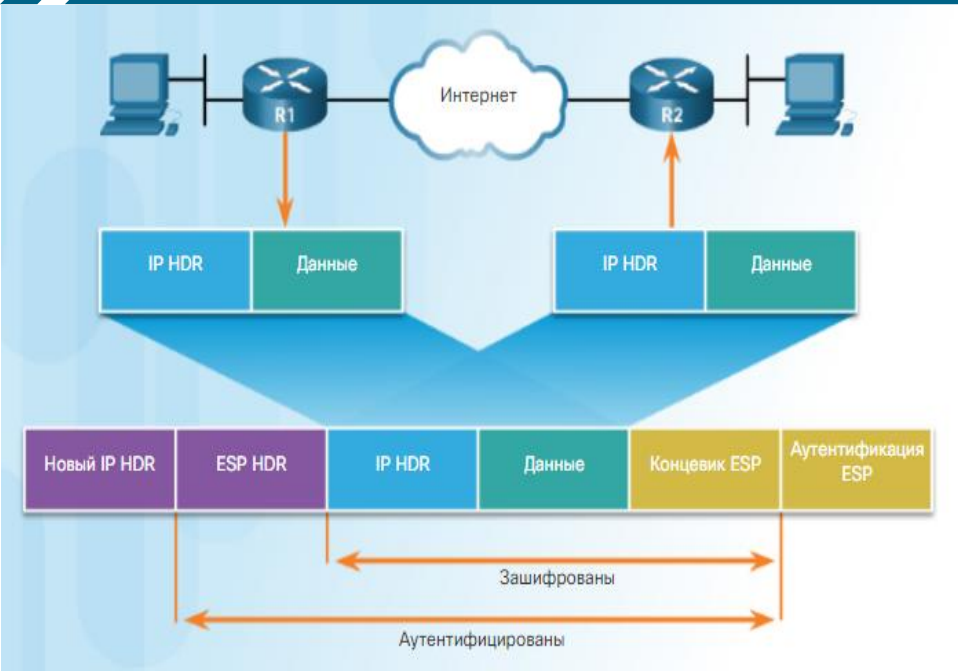
Кроме того, ESP также может принудительно применять защиту от повтора. Функция защиты от повтора позволяет убедиться, что каждый пакет является уникальным и не дублирован. Благодаря этой функции хакер не сможет перехватить пакеты и вставить измененные пакеты в поток данных. Защита от повтора работает путем отслеживания порядковых номеров пакетов и использования скользящего окна в месте назначения.

После установления соединения между источником и местом назначения их счетчики сбрасываются в нуль. При каждой отправке пакета источник добавляет в него порядковый номер. Место назначения использует скользящее окно, чтобы определить ожидаемые порядковые номера. Место назначения проверяет, что порядковый номер пакета не дублирован и принят в правильном порядке.

Например, если скользящее окно в месте назначения установлено на единицу, то место назначения ожидает получить пакет с порядковым номером 1. После приема этого пакета скользящее окно перемещается к двойке. В случае обнаружения повторного пакета, например если место назначения принимает второй пакет с порядковым номером 1, генерируется сообщение об ошибке, повторный пакет отбрасывается и событие регистрируется в журнале.

Обычно функция защиты от повтора используется в ESP, но также поддерживается в AH.

# Второй учебный вопрос.
# Протокол IPSec.




**ESP выполняет шифрование и аутентификацию**

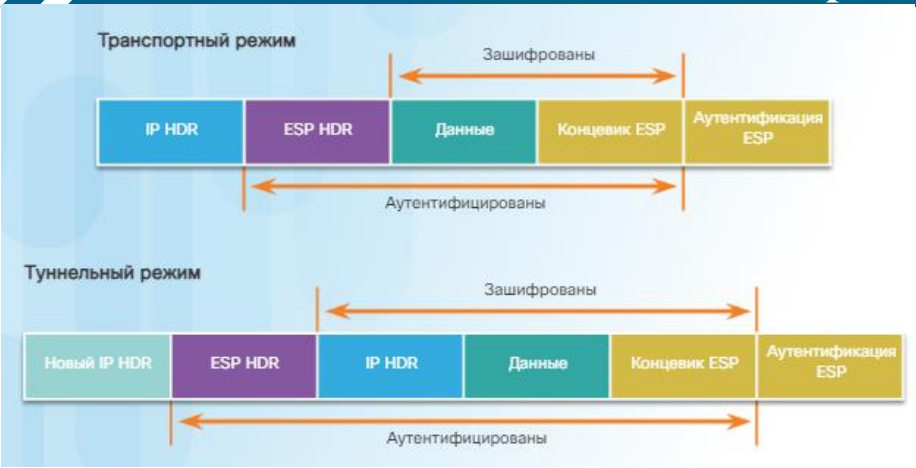
ESP позволяет защищать исходные данные, так как полностью шифруются исходная IP-датаграмма и концевик ESP. Как показано на рисунке, в случае аутентификации ESP шифрованные IP-датаграмма и концевик и заголовок ESP применяются в процессе хеширования. Затем новый IP-заголовок добавляется к аутентифицированной полезной нагрузке. Для маршрутизации пакета через Интернет используется новый IP-адрес.

Если выбраны как аутентификация, так и шифрование, сначала выполняется шифрование. Одна из причин такого порядка обработки состоит в том, что это упрощает процесс быстрого обнаружения и отклонения повторных или поддельных пакетов устройством приема. До дешифрования пакета получатель может аутентифицировать входящие пакеты. Это позволяет быстро обнаружить проблемы и потенциально уменьшить степень воздействия DoS-атак. Следует напомнить, что ESP обеспечивает конфиденциальность благодаря шифрованию и целостность с помощью аутентификации.

Говоря о протоколе IPsec, мы пока имели в виду IPv4. Однако изначально IPsec был задуман с целью обеспечения защиты для IPv6-пакетов. Следовательно, с точки зрения стандартов, варианты реализации протокола IPsec для IPv4 и IPv6 очень похожи друг на друга. В случае IPv4 AH и ESP являются заголовками IP-протокола. В IPv6 используются заголовки расширений со значением следующего заголовка 50 для ESP и 51 для AH.

# Второй учебный вопрос.
# Протокол IPSec.







Как показано на рисунке, ESP и AH могут применяться к IP-пакетам в двух разных режимах: транспортном и туннельном.

**Транспортный режим**

В транспортном режиме безопасность обеспечивается только для транспортного уровня модели OSI и более высоких уровней. Транспортный режим защищает полезную нагрузку пакета, но оставляет исходный IP-адрес в открытом виде. Для маршрутизации пакета через Интернет используется исходный IP-адрес. Между хостами используется транспортный режим ESP.

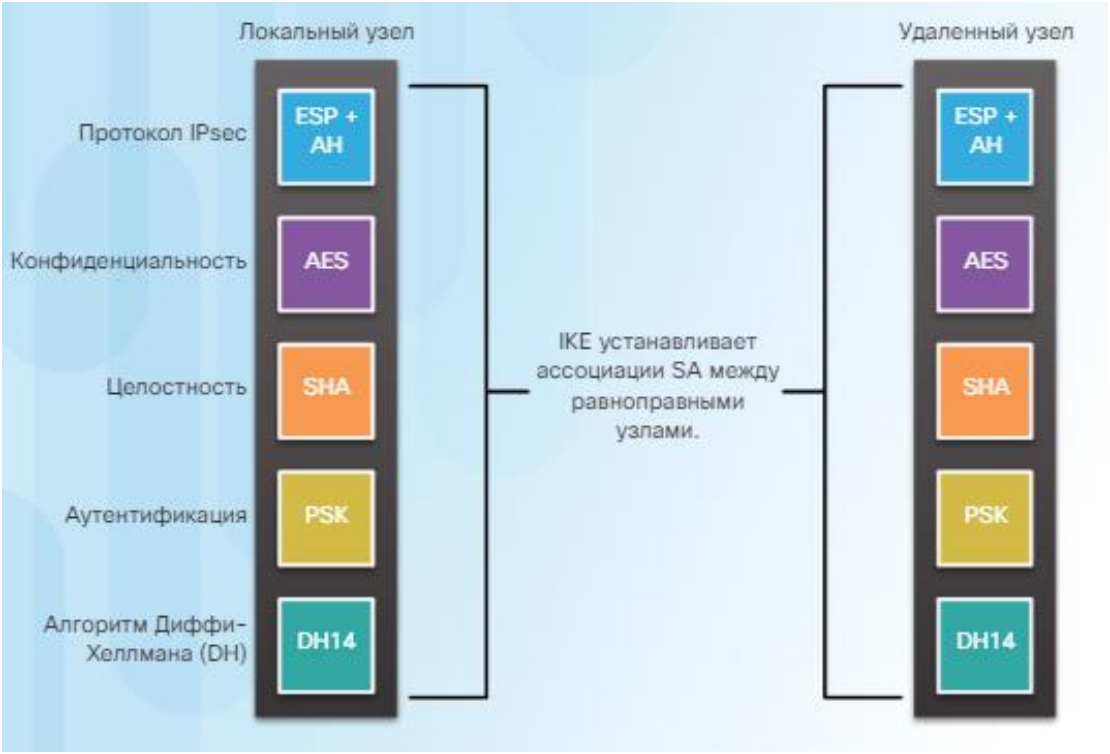
**Туннельный режим**

Туннельный режим обеспечивает безопасность для всего исходного IP-пакета. Исходный IP-пакет шифруется, а затем инкапсулируется в другом IP-пакете. Такой метод называется шифрованием IP-в-IP. Для маршрутизации пакета через Интернет используется IP-адрес во внешнем IP-пакете.

Как показано на рисунке, транспортный режим AH обеспечивает аутентификацию и целостность для всего пакета. Он не шифрует данные, но защищен от изменения. Туннельный режим AH инкапсулирует IP-пакет с AH и новым IP-заголовком и подписывает весь пакет для целостности и аутентификации.

# Второй учебный вопрос.
# Протокол IPSec.





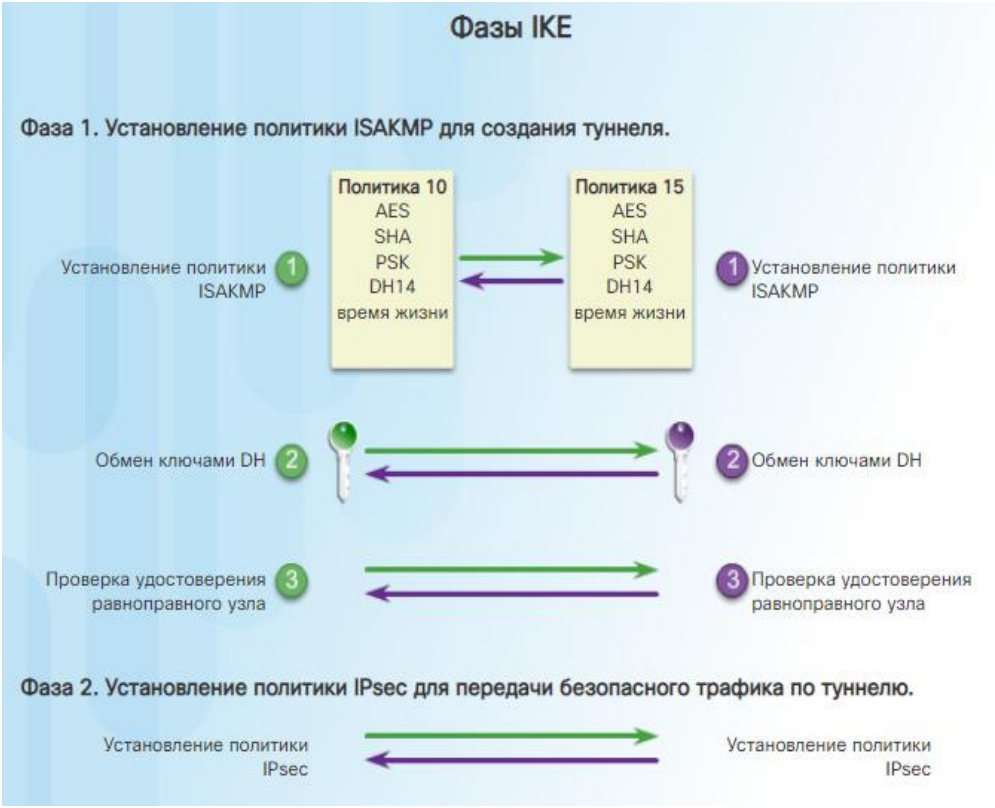

**Протокол Internet Key Exchange (IKE)** представляет собой стандарт протокола управления ключами. IKE используется вместе со стандартом IPsec. Как показано на рисунке, IKE автоматически устанавливает ассоциации безопасности IPsec и обеспечивает безопасную связь по IPsec. IKE расширяет возможности IPsec путем добавления функций и упрощает настройку для стандарта IPsec. Если бы IKE не было, настройка IPsec была бы сложным процессом, выполняемым вручную, и с ограниченными возможностями по масштабированию.

IKE – это гибридный протокол, реализующий протоколы обмена ключами на базе платформы Internet Security Association Key Management Protocol (ISAKMP). ISAKMP (произносится как «айс-э-кэмп») определяет формат сообщений, механизм протокола обмена ключами и процесс согласования с целью создания SA для IPsec.

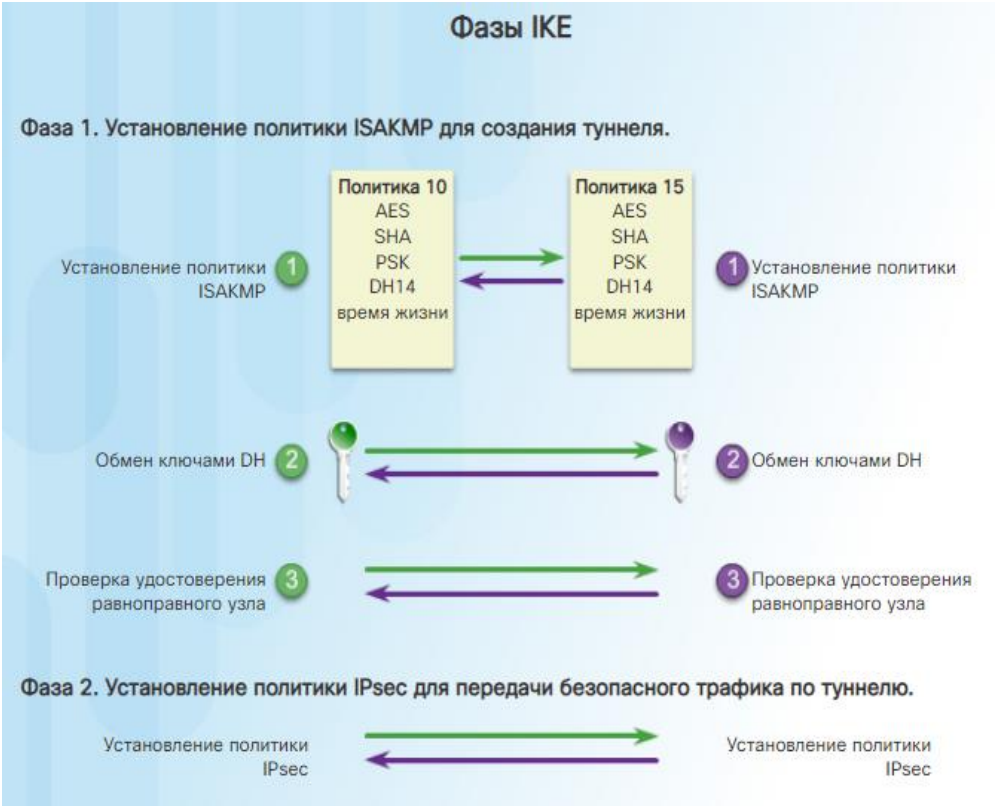
Вместо передачи ключей непосредственно через сеть, IKE вычисляет общие ключи путем обмена серией пакетов данных. Благодаря этому третье лицо не может дешифровать ключи даже в том случае, если собрало все переданные данные, которые использовались для вычисления ключей. Для обмена информацией IKE между шлюзами безопасности протокол IKE использует UDP-порт 500. Пакеты, поступающие из UDP-порта 500, должны быть разрешены на любом IP-интерфейсе, который подключается к другому шлюзу безопасности.

**Согласование ключей на фазе 1 и 2**

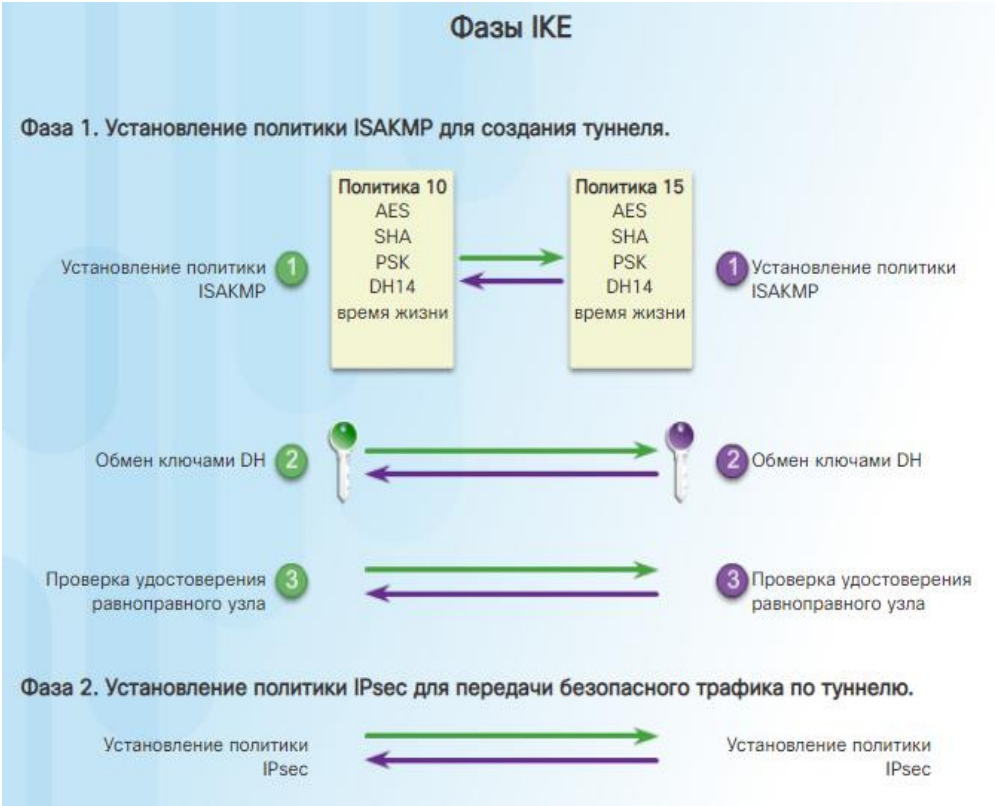
Для согласования ключей на фазах 1 и 2 протокол IKE использует ISAKMP. Фаза 1 обеспечивает установление ассоциации безопасности (ключа) между двумя равноправными узлами IKE. Ключ, установленный на фазе 1, позволяет равноправным узлам IKE взаимодействовать в защищенном режиме на фазе 2. В ходе согласования на фазе 2 протокол IKE устанавливает ключи (ассоциации безопасности) для других приложений, например для IPsec.



На фазе 1 два равноправных узла IPsec выполняют начальное согласование ассоциаций SA. Фаза 1 в первую очередь служит для согласования политики ISAKMP, аутентификации равноправных узлов и установления безопасного туннеля между равноправными узлами. Затем этот туннель будет использоваться на фазе 2 для согласования политики IPsec.



Фаза 1 может быть реализована в основном или агрессивном режимах. Если применяется основной режим, то идентификаторы двух равноправных узлов IKE являются скрытыми. В агрессивном режиме согласование ключей между равноправными узлами выполняется быстрее, чем в основном режиме. Однако так как хеш аутентификации отправляется в нешифрованном виде до установления туннеля, то агрессивный режим оказывается уязвим к атакам с подбором пароля.




Фаза 2 предназначена для согласования параметров безопасности IPsec, которые будут использоваться для защиты туннеля IPsec. Фаза IKE 2 называется «быстрым режимом» и может произойти только после того, как протокол IKE установит безопасный туннель на фазе 1.

Ассоциации SA согласовываются процессом IKE (ISAKMP) от имени IPsec, которому для работы требуются ключи шифрования. Быстрый режим обеспечивает согласование ассоциаций SA на фазе IKE 2. На этой фазе ассоциации SA, применяемые протоколом IPsec, являются однонаправленными. Следовательно, для каждого потока данных требуется отдельная операция по обмену ключами.

Быстрый режим также повторно согласовывает новую ассоциацию IPsec SA, когда истекает время жизни IPsec SA.

В основном быстрый режим обновляет ключевой материал, который создает общий секретный ключ. Это основано на ключевом материале, который получен в ходе обмена DH на фазе 1.

# Второй учебный вопрос.
# Протокол IPSec.


Все сети VPN XYZCORP должны реализовывать следующую политику:

- Шифрование трафика с помощью AES 256 и SHA
- Аутентификация с помощью PSK
- Обмен ключами с помощью группы 24
- Время жизни туннеля ISAKMP – 1 час
- Туннель IPsec использует ESP со временем жизни 15 минут

Задача 1. Настройка политики ISAKMP для фазы 1 IKE
Задача 2. Настройка политики IPsec для фазы 2 IKE
Задача 3. Настройка криптокарты для политики IPsec
Задача 4. Применение политики IPsec
Задача 5. Проверка работы туннеля IPsec


```
R1(config)# ip access-list extended INBOUND
R1(config-ext-nacl)# permit ip 192.168.1.0 0.0.0.255 10.0.1.0 0.0.0.255
R1(config-ext-nacl)# permit icmp host 172.30.2.2 host 172.30.2.1
R1(config-ext-nacl)# permit udp host 172.30.2.2 host 172.30.2.1 eq isakmp
R1(config-ext-nacl)# permit esp host 172.30.2.2 host 172.30.2.1
R1(config-ext-nacl)# permit ahp host 172.30.2.2 host 172.30.2.1
R1(config-ext-nacl)# deny ip any any
R1(config-ext-nacl)# exit
R1(config)# interface serial0/0/0
R1(config-if)# ip access-group INBOUND in
```

Маршрутизаторы периметра обычно реализуют ограничительную политику безопасности, блокируя весь трафик, кроме специально разрешенного трафика. До реализации сети IPsec VPN между двумя пунктами убедитесь, что существующие списки ACL не блокируют трафик, необходимый для установления IPsec-соединения. На рисунке показан синтаксис команд в ACL для разрешения трафика ISAKMP, ESP и AH.

```
R1(config)# crypto isakmp policy ?
  <1-10000>  Priority of protection suite

R1(config)# crypto isakmp policy 1
R1(config-isakmp)# ?
ISAKMP commands:
  authentication  Set authentication method for protection suite
  default         Set a command to its defaults
  encryption      Set encryption algorithm for protection suite
  exit            Exit from ISAKMP protection suite configuration mode
  group           Set the Diffie-Hellman group
  hash            Set hash algorithm for protection suite
  lifetime        Set lifetime for ISAKMP security association
  no              Negate a command or set its defaults
```

Для настройки новой политики ISAKMP используйте команду **crypto isakmp policy** , как показано на рисунке. Единственным аргументом для команды является задание приоритета для политики (от 1 до 10000). Равноправные узлы будут пытаться выполнять согласование с помощью политики с наименьшим номером (наивысшим приоритетом). Для равноправных узлов не требуется совпадение номеров приоритета.

В режиме настройки политики ISAKMP можно настроить ассоциации SA для туннеля для фазы 1 IKE. Используйте мнемонику HAGLE , чтобы запомнить следующие пять ассоциаций SA, которые необходимо настроить:

Hash (хеш)
Authentication (аутентификация)
Group (группа)
Lifetime (Время существования)
Encryption (шифрование)

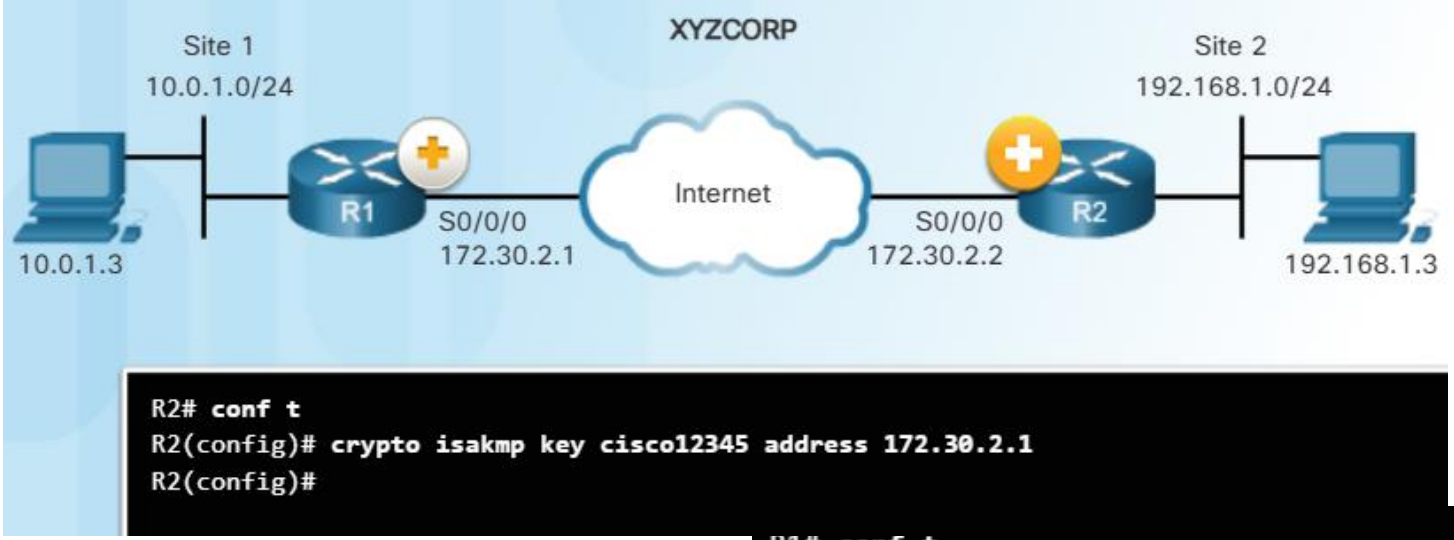
```
R1(config)# crypto isakmp policy 1
R1(config-isakmp)# hash sha
R1(config-isakmp)# authentication pre-share
R1(config-isakmp)# group 24
R1(config-isakmp)# lifetime 3600
R1(config-isakmp)# encryption aes 256
R1(config-isakmp)# end
R1# show crypto isakmp policy

Global IKE policy
Protection suite of priority 1
        encryption algorithm:    AES - Advanced Encryption Standard (256 bit keys).
        hash algorithm:          Secure Hash Standard
        authentication method:   Pre-Shared Key
        Diffie-Hellman group:    #24 (2048 bit, 256 bit subgroup)
        lifetime:                3600 seconds, no volume limit
R1#
```

Чтобы соответствовать требованиям политики безопасности для XYZCORP, настройте политику ISAKMP со следующими ассоциациями SA:

Хеш – SHA
Аутентификация – общий ключ
Группа – 24
Время жизни – 3600 секунд
Шифрование – AES

Используйте команду **show crypto isakmp policy** для проверки конфигурации.




```
R2# conf t
R2(config)# crypto isakmp key cisco12345 address 172.30.2.1
R2(config)#
```

```
R1# conf t
R1(config)# crypto isakmp key cisco12345 address 172.30.2.2
R1(config)#
```

Политика безопасности XYZCORP требует использовать общий ключ для аутентификации между равноправными узлами. Синтаксис команды показан на рисунке. Администратор может указать либо имя узла, либо IP-адрес для другого узла. XYZCORP использует фразу-пароль **cisco12345** и IP-адрес другого узла.

Хотя политика ISAKMP для туннеля для фазы 1 IKE настроена, сам туннель пока еще не существует. Это можно проверить с помощью команды **show crypto isakmp sa** . «Интересный» трафик должен быть обнаружен до согласования фазы 1 IKE. Для сети VPN между двумя пунктами XYXCORP «интересный» трафик представляет собой любой трафик между сетями LAN на площадках 1 и 2.

Чтобы определить «интересный» трафик, настройте каждый маршрутизатор со списком ACL на разрешение трафика из локальной LAN в удаленную LAN. Список ACL будет использоваться в конфигурации криптокарты для указания трафика, который будет инициировать начало фазы 1 IKE.

```
R2# conf t
R2(config)# access-list 102 permit ip 192.168.1.0 0.0.0.255 10.0.1.0 0.0.0.255
R2(config)#
```

```
R1(config)# crypto ipsec transform-set R1-R2 ?
  ah-md5-hmac      AH-HMAC-MD5 transform
  ah-sha-hmac      AH-HMAC-SHA transform
  ah-sha256-hmac   AH-HMAC-SHA256 transform
  ah-sha384-hmac   AH-HMAC-SHA384 transform
  ah-sha512-hmac   AH-HMAC-SHA512 transform
  comp-lzs         IP Compression using the LZS compression algorithm
  esp-3des         ESP transform using 3DES(EDE) cipher (168 bits)
  esp-aes          ESP transform using AES cipher
  esp-des          ESP transform using DES cipher (56 bits)
  esp-gcm          ESP transform using GCM cipher
  esp-gmac         ESP transform using GMAC cipher
  esp-md5-hmac     ESP transform using HMAC-MD5 auth
  esp-null         ESP transform w/o cipher
  esp-seal         ESP transform using SEAL cipher (160 bits)
  esp-sha-hmac     ESP transform using HMAC-SHA auth
  esp-sha256-hmac  ESP transform using HMAC-SHA256 auth
  esp-sha384-hmac  ESP transform using HMAC-SHA384 auth
```

Теперь нам нужно настроить набор алгоритмов шифрования и хеширования, которые будут использоваться для преобразования данных, отправляемых через туннель IPsec. Это называется набором преобразований. В ходе согласований на фазе 2 IKE равноправные узлы договариваются о наборе преобразований IPsec, который будет использоваться для защиты «интересного» трафика.

Настройте набор преобразований с помощью команды **crypto ipsec transform-set**. Сначала укажите имя для набора преобразований (R1-R2 в данном примере). Затем можно настроить алгоритм шифрования и хеширования в любом порядке.

# Второй учебный вопрос.
# Протокол IPSec.

```
R1(config)# crypto ipsec transform-set R1-R2 ?
  ah-md5-hmac       AH-HMAC-MD5 transform
  ah-sha-hmac       AH-HMAC-SHA transform
  ah-sha256-hmac    AH-HMAC-SHA256 transform
  ah-sha384-hmac    AH-HMAC-SHA384 transform
  ah-sha512-hmac    AH-HMAC-SHA512 transform
  comp-lzs          IP Compression using the LZS compression algorithm
  esp-3des          ESP transform using 3DES(EDE) cipher (168 bits)
  esp-aes           ESP transform using AES cipher
  esp-des           ESP transform using DES cipher (56 bits)
  esp-gcm           ESP transform using GCM cipher
  esp-gmac          ESP transform using GMAC cipher
  esp-md5-hmac      ESP transform using HMAC-MD5 auth
  esp-null          ESP transform w/o cipher
  esp-seal          ESP transform using SEAL cipher (160 bits)
  esp-sha-hmac      ESP transform using HMAC-SHA auth
  esp-sha256-hmac   ESP transform using HMAC-SHA256 auth
  esp-sha384-hmac   ESP transform using HMAC-SHA384 auth
```

```
R2(config)# crypto ipsec transform-set R1-R2 esp-aes esp-sha-hmac
```

Теперь нам нужно настроить набор алгоритмов шифрования и хеширования, которые будут использоваться для преобразования данных, отправляемых через туннель IPsec. Это называется набором преобразований. В ходе согласований на фазе 2 IKE равноправные узлы договариваются о наборе преобразований IPsec, который будет использоваться для защиты «интересного» трафика.

Настройте набор преобразований с помощью команды **crypto ipsec transform-set**. Сначала укажите имя для набора преобразований (R1-R2 в данном примере). Затем можно настроить алгоритм шифрования и хеширования в любом порядке.

```
R1(config)# crypto map R1-R2_MAP 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
and a valid access list have been configured.
R1(config-crypto-map)# ?
Crypto Map configuration commands:
  default         Set a command to its defaults
  description     Description of the crypto map statement policy
  dialer          Dialer related commands
  exit            Exit from crypto map configuration mode
  match           Match values.
  no              Negate a command or set its defaults
  qos             Quality of Service related commands
  reverse-route   Reverse Route Injection.
  set             Set values for encryption/decryption
```

Теперь, когда «интересный» трафик определен и набор преобразований IPsec настроен, можно привязать эти конфигурации к остальной части политики IPsec в криптокарте. На рисунке показан синтаксис для запуска заданной криптокарты. При настройке нескольких записей (значений) криптокарты большое значение имеет порядковый номер. Для XYZCORP будет требоваться только одна запись криптокарты при сопоставлении трафика и учете остающихся ассоциаций SA. Доступные конфигурации для записи криптокарты, когда вы находитесь в режиме настройки криптокарты. Имя карты – **R1-R2_MAP**, а порядковый номер – **10**.

```
R1(config)# crypto map R1-R2_MAP 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
and a valid access list have been configured.
R1(config-crypto-map)# match address 101
R1(config-crypto-map)# set transform-set R1-R2
R1(config-crypto-map)# set peer 172.30.2.2
R1(config-crypto-map)# set pfs group24
R1(config-crypto-map)# set security-association lifetime seconds 900
R1(config-crypto-map)# exit
R1(config)#
```

Для завершения процесса настройки с учетом требований политики безопасности IPsec для XYZCORP выполните следующее:

**Шаг 1.** Привяжите список ACL и набор преобразований к карте.

**Шаг 2.** Укажите IP-адрес другого узла.

**Шаг 3.** Настройте группу DH.

**Шаг 4.** Настройте время жизни туннеля IPsec.

Конфигурация криптокарты для R1.

С помощью команды **show crypto map** проверьте конфигурацию криптокарты. Должны иметься все требуемые ассоциации SA. Обратите внимание, что в настоящее время никакие интерфейсы не используют криптокарту.

```
R1(config)# interface serial0/0/0
R1(config-if)# crypto map R1-R2_MAP
R1(config-if)#
*Mar 19 19:36:36.273: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
R1(config-if)# end
R1# show crypto map
          Interfaces using crypto map NiStTeSt1:

Crypto Map IPv4 "R1-R2_MAP" 10 ipsec-isakmp
          Peer = 172.30.2.2
          Extended IP access list 101
              access-list 101 permit ip 10.0.1.0 0.0.0.255 192.168.1.0 0.0.0.255
          Security association lifetime: 4608000 kilobytes/900 seconds
          Responder-Only (Y/N): N
          PFS (Y/N): Y
          DH group:  group24
          Mixed-mode : Disabled
          Transform sets={
                    R1-R2:  { esp-aes esp-sha-hmac  } ,
          }
          Interfaces using crypto map R1-R2_MAP:
                    Serial0/0/0
```

Для применения криптокарты войдите в режим интерфейсной настройки для исходящего интерфейса и настройте команду **crypto map** *map-name* .

Обратите внимание, что в результате команды **show crypto map** теперь отображается, что последовательный интерфейс 0/0/0 использует криптокарту. Маршрутизатор R2 настраивается с помощью этой же команды на своем последовательном интерфейсе 0/0/0.

```
R1# show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id status
172.30.2.2      172.30.2.1      QM_IDLE           1005 ACTIVE

IPv6 Crypto ISAKMP SA

R1#
```

```
R1# show crypto ipsec sa

interface: Serial0/0/0
    Crypto map tag: R1-R2_MAP, local addr 172.30.2.1

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (10.0.1.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
   current_peer 172.30.2.2 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 4, #pkts encrypt: 4, #pkts digest: 4
    #pkts decaps: 4, #pkts decrypt: 4, #pkts verify: 4
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
```

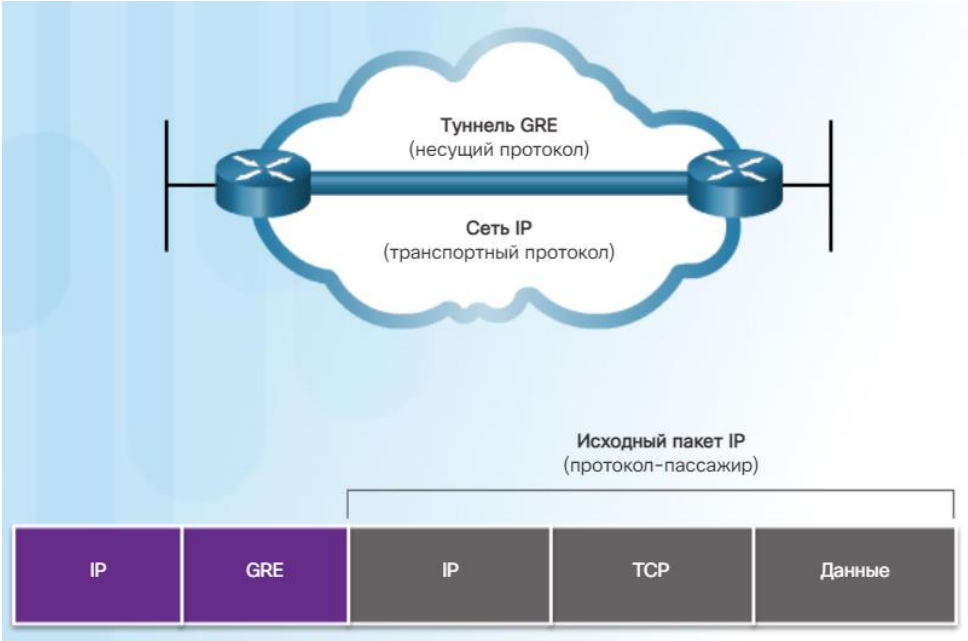
Отправка «интересного» трафика не означает фактически, что туннели установлены. Маршрутизаторы R1 и R2 будут маршрутизировать трафик между этими локальными сетями даже в том случае, если конфигурации политик ISAKMP и IPsec неправильные. Убедитесь, что туннели установлены, с помощью команд **show crypto isakmp sa** и **show crypto ipsec sa** .

**Выводу по второму учебному вопросу.**

IPsec основана на применении существующих алгоритмов, обеспечивающих шифрование, аутентификацию и обмен ключами. IPsec может инкапсулировать пакет с помощью протокола Authentication Header (AH) или более защищенного варианта – протокола Encapsulation Security Protocol (ESP).

Для установления процесса обмена ключами в IPsec применяется протокол IKE. Для создания сети VPN между двумя пунктами необходимо выполнить следующие задачи:

Настроить политику ISAKMP для фазы 1 IKE.
Настроить политику IPsec для фазы 2 IKE.
Настроить криптокарту для политики IPsec.
Применить политику IPsec.
Проверить работу туннеля IPsec.




**Протокол GRE**

Универсальная инкапсуляция при маршрутизации (Generic Routing Encapsulation, GRE) — один из примеров базового, незащищенного протокола создания туннелей для site-to-site VPN. GRE — это протокол туннелирования, разработанный компанией Cisco, позволяющий инкапсулировать пакеты протоколов различного типа внутри IP-туннелей. Благодаря этому создается виртуальный канал «точка-точка» до маршрутизаторов в удаленных точках поверх IP-сети.

GRE предназначен для управления процессом передачи многопротокольного и группового IP-трафика между двумя и более площадками, между которыми связь может обеспечиваться только по IP. Он может инкапсулировать пакеты протоколов различного типа в IP-туннеле.

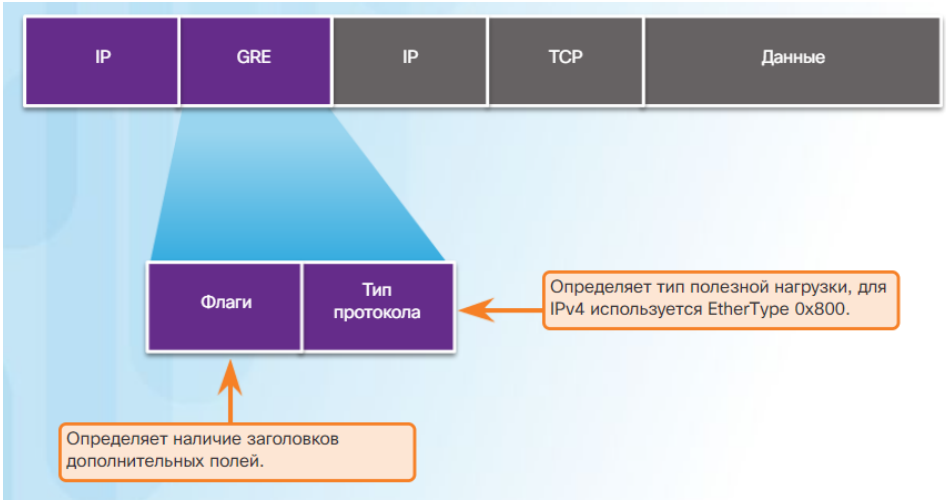
Как показано на рисунке, интерфейс туннеля поддерживает заголовки для всех указанных ниже протоколов:

Инкапсулированный протокол (или «протокол-пассажир»), например IPv4, IPv6, AppleTalk, DECnet или IPX

Протокол инкапсуляции (или несущий протокол), в данном случае GRE

Протокол доставки («протокол-транспорт»), например IP, который передает данные протокола инкапсуляции.

# Третий учебный вопрос. Протоколы GRE, PPTP, L2TP




**Характеристики протокола GRE**

GRE — это протокол туннелирования, разработанный компанией Cisco, который позволяет инкапсулировать пакеты протоколов различного типа внутри IP-туннелей и создавать виртуальный канал «точка-точка» до маршрутизаторов Cisco в удаленных точках поверх IP-сети. Туннелирование IP с помощью GRE позволять расширять сеть через однопротокольную магистральную среду. Это обеспечивается путем соединения между собой различных многопротокольных подсетей в однопротокольной магистральной среде.

**Протокол GRE обладает следующими характеристиками:**

- Спецификации GRE определены в стандарте IETF (RFC 2784).
- Во внешнем заголовке IP в поле протокола используется значение 47, указывающее на то, что за ним будет следовать заголовок GRE.
- При инкапсуляции GRE для поддержки инкапсуляции любого протокола 3 уровня модели OSI в заголовке GRE используется поле «типа протокола» (protocol type). Типы протоколов определены в стандарте RFC 1700 как EtherTypes.
- Сам по себе протокол GRE не предусматривает сохранения информации о состоянии. По умолчанию механизмы управления потоком отсутствуют.
- Для защиты полезной нагрузки в протоколе GRE отсутствуют какие-либо стойкие механизмы безопасности.
- Заголовок GRE вместе с заголовком IP туннелирования, указанным на рисунке, создает, по крайней мере, 24 байта дополнительной служебной информации для туннелированных пакетов.

# Формат заголовка GRE

| бит | значение | Описание |
|---|---|---|
| 0 | Checksum Present | Если бит Checksum Present имеет значение 1, поле Checksum должно присутствовать в заголовке и содержать корректную информацию.<br>Если установлен любой из битов Checksum Present или Routing Present, оба поля Checksum и Offset присутствуют в заголовке пакета GRE. |
| 1 | Routing Present | Если бит Routing Present имеет значение 1, это говорит о том, что поля Offset и Routing присутствуют в заголовке и содержат корректную информацию.<br>Если установлен любой из битов Checksum Present или Routing Present, оба поля Checksum и Offset присутствуют в заголовке пакета GRE. |
| 2 | Key Present | Если бит Key Present имеет значение 1, это говорит о присутствии поля Key в заголовке GRE. В противном случае поле Key в заголовок GRE не включается. |
| 3 | Sequence Number Present | Если бит Sequence Number Present имеет значение 1, это говорит о присутствии поля Sequence Number. В противном случае поле Sequence Number в заголовок GRE не включается. |

# Формат заголовка GRE продолжение

| | | |
|---|---|---|
| **4** | **Strict Source Route** | **Значение бита Strict Source Route определено в других документах. Рекомендуется устанавливать для этого бита значение 1 только в тех случаях, когда вся маршрутная информация (Routing Information) состоит из маршрутов Strict Source Route** |
| **5-7** | Recursion Control | Поле Recursion Control содержит трехбитовое целое число без знака, указывающее допустимое количество дополнительных инкапсуляций. По умолчанию для этого поля следует устанавливать значение 0. |
| **8-12** | 00000 | зарезервированы |
| **13-15** | Version Number | Поле Version Number должно содержать значение 0. Другие значения этого поля выходят за пределы рассмотрения данного документа. |
| **2 байта** | Protocol Type | Поле Protocol Type указывает тип протокола во вложенном пакете. В общем случае это поле будет содержать значение поля типа протокола Ethernet для пакета. Определенные в настоящее время значения типов перечислены ниже. Дополнительные значения поля типа могут быть определены в других документах. |

# Формат заголовка GRE

| | | |
|---|---|---|
| **2 байта** | **Offset** | **Поле Offset показывает смещение в октетах от начала поля Routing до первого октета активной записи Source Route Entry, которая будет проверяться. Это поле присутствует в заголовке, если хотя бы один из битов Routing Present и Checksum Present имеет значение 1; поле содержит корректную информацию лишь при условии Routing Present = 1.** |
| **2 байта** | Checksum | Поле Checksum содержит контрольную сумму IP (дополнение до единицы) заголовка GRE и вложенного пакета. Это поле присутствует лишь в тех случаях, когда хотя бы один из битов Routing Present и Checksum Present имеет значение 1; поле содержит корректную информацию лишь при условии Checksum Present = 1. |
| **4 байта** | Key | Поле Key содержит 4-октетное число, которое включается при инкапсуляции. Это поле может использоваться получателем для аутентификации источника пакета. Методы такой аутентификации выходят за пределы настоящего документа. Поле Key присутствует в заголовке лишь при условии Key Present = 1. |
| **4 байта** | Sequence Number | Поле Sequence Number содержит 32-битовое целое число без знака, добавляемое при инкапсуляции. Это значение может использоваться получателем для отслеживания порядка передачи пакетов со стороны инкапсулятора. Точный алгоритм генерации значений поля Sequence Number и семантика порядковых номеров для получателя выходят за пределы настоящего документа. |
| **--** | Routing | Поле Routing является необязательным и присутствует лишь при условии Routing Present = 1.<br>Поле Routing представляет собой список записей SRE (Source Route Entries) |

Настройка туннелей GRE

Для реализации туннеля GRE сетевой администратор должен сначала узнать IP-адреса конечных точек туннеля. После этого для настройки туннеля GRE следует выполнить следующую процедуру:

Шаг 1. Создайте интерфейс туннеля с помощью команды interface tunnel number.

Шаг 2. Укажите IP-адрес источника туннеля.

Шаг 3. Укажите IP-адрес назначения туннеля.

Шаг 4. Укажите IP-адрес для интерфейса туннеля.

Шаг 5. (Дополнительно) Укажите на интерфейсе туннеля в качестве используемого режима режим GRE. Режим GRE является режимом по умолчанию для интерфейса туннеля в программном обеспечении Cisco IOS.

На рисунке приведен пример базовой настройки туннеля GRE для маршрутизатора R1.


**Настройка R1:**

```
R1(config)# interface Tunnel0
R1(config-if)# tunnel mode gre ip
R1(config-if)# ip address 192.168.2.1 255.255.255.0
R1(config-if)# tunnel source 209.165.201.1
R1(config-if)# tunnel destination 198.133.219.87
R1(config-if)# router ospf 1
R1(config-router)# network 192.168.2.0 0.0.0.255 area 0
```

```
R2(config)# interface Tunnel0
R2(config-if)# tunnel mode gre ip
R2(config-if)# ip address 192.168.2.2 255.255.255.0
R2(config-if)# tunnel source 198.133.219.87
R2(config-if)# tunnel destination 209.165.201.1
R2(config-if)# router ospf 1
R2(config-router)# network 192.168.2.0 0.0.0.255 area 0
```

| Команда | Описание |
|---|---|
| **tunnel mode gre ip** | Указывает, что режимом работы интерфейса туннеля является GRE по IP. |
| **tunnel source** *ip_address* | Указывает адрес источника туннеля. |
| **tunnel destination** *ip_address* | Указывает адрес назначения туннеля. |
| **ip address** *ip_address mask* | Указывает IP-адрес интерфейса туннеля. |

Для наблюдения и устранения неполадок в туннелях GRE можно использовать несколько команд. Для определения работоспособности интерфейса туннеля используйте команду **show ip interface brief**, как показано на рисунке

```
R1# show ip interface brief | include Tunnel
Tunnel0                192.168.2.1     YES manual up        up
```

```
R1# show interface Tunnel 0
Tunnel0 is up, line protocol is up
  Hardware is Tunnel
  Internet address is 192.168.2.1/24
  MTU 17916 bytes, BW 100 Kbit/sec, DLY 50000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation TUNNEL, loopback not set
  Keepalive not set
  Tunnel source 209.165.201.1, destination 209.165.201.2
  Tunnel protocol/transport GRE/IP
<выходные данные опущены>
```

Для проверки состояния туннеля GRE используйте команду show interface tunnel. Протокол канального уровня в интерфейсе туннеля GRE активен до тех пор, пока существует маршрут до адреса назначения туннеля. Перед реализацией туннеля GRE между IP-адресами физических интерфейсов на противоположных сторонах потенциального туннеля GRE должна уже существовать связь по IP. Транспортный протокол туннелирования отображается в выходных данных, также показанных на рисунке 9.
Если OSPF также настроен на обмен маршрутами по туннелю GRE, то с помощью команды show ip ospf neighbor убедитесь, что через интерфейс туннеля установлены отношения смежности OSPF. На рисунке 10 видно, что адрес соседнего устройства OSPF находится в сети IP, созданной для туннеля GRE.

```
R1# show ip ospf neighbor

Neighbor ID     Pri State           Dead Time   Address         Interface
209.165.201.2   0   FULL/  -        00:00:37    192.168.2.2     Tunnel0
```

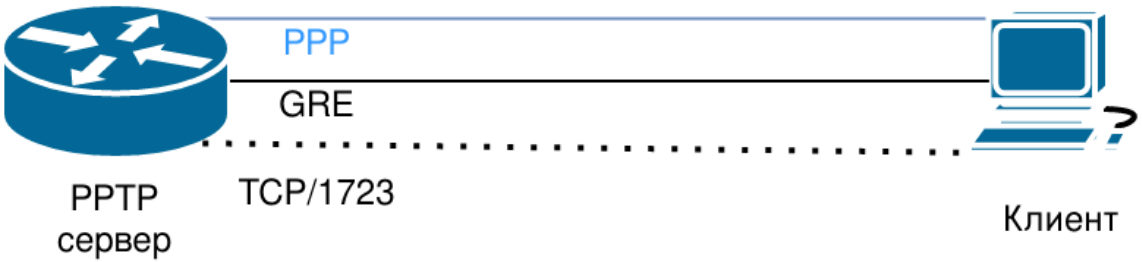
Однако GRE не обеспечивает шифрования и никаких других механизмов безопасности. Поэтому данные, отправляемые по туннелю GRE, не защищены. Если требуется безопасная передача данных, то необходимо настроить сети VPN с IPsec или с SSL.

**PPTP (Point-to-Point Tunneling Protocol)** — туннельный протокол типа «точка-точка», позволяющий компьютеру устанавливать защищённое соединение с сервером за счёт создания специального туннеля в стандартной незащищённой сети.

Спецификация протокола PPTP приведена в RFC 2637. Протокол считается менее безопасным, чем другие протоколы, используемые для построения VPN, например, IPSec. Безопасность решения PPTP напрямую зависит от сложности паролей, которые используются пользователями. По этой причине при использовании в практических условиях следует внимательно следить за стойкостью используемых паролей. Как следствие этого, решения на базе PPTP слабее по сравнению с другими решениями.

К преимуществам данной технологии построения VPN можно отнести простоту настройки, а также тот факт, что все версии ОС Microsoft Windows, начиная с Windows 95 OSR2, включают в свой состав встроенный клиент PPTP.

На рисунке ниже приведена схема использования режима удаленного доступа VPN с использованием PPTP.



## VPN удаленного доступа на основе протокола PPTP

**При использовании такого решения:**

- Клиент PPTP устанавливает соединение TCP с сервером (порт 1723).
- Через установленное соединение клиент PPTP и сервер устанавливают туннель GRE (Generic Routing Encapsulation).
- Затем поверх туннеля GRE устанавливается сеанс протокола PPP (Point-to-Point Protocol): пакеты PPP инкапсулируются и принимаются/отправляются через туннель GRE.

Аутентификация пользователей и шифрование данных осуществляется на уровне PPP при помощи комбинации имени и пароля с использованием протокола MS CHAP или MS CHAP v2 для аутентификации и протокола MPPE для шифрования.

Структура кадров PPTP

– заголовок канального уровня, используемый внутри Internet, например заголовок кадра Ethernet;

– заголовок IP, содержащий адреса отправителя и получателя пакета;

– заголовок общего метода инкапсуляции для маршрутизации GRE (Generic Routing Encapsulation);

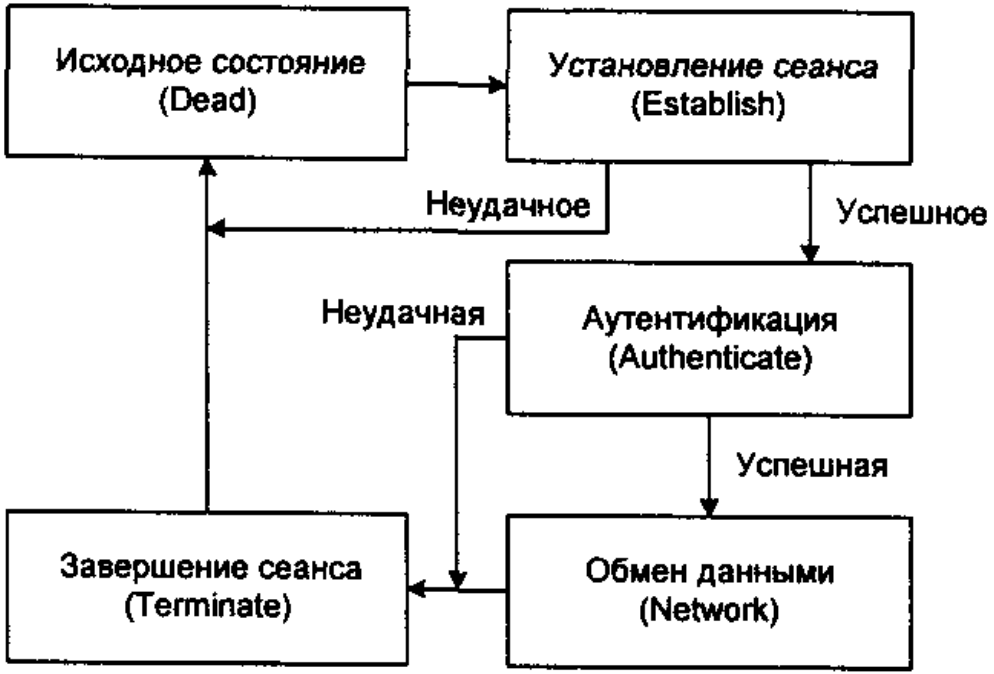
– исходный пакет PPP, включающий пакет IP, IPX или NetBEUI.

**PPTP работает, устанавливая обычную PPP сессию с противоположной стороной с помощью протокола GRE. Второе соединение на TCP-порту 1723 используется для инициации и управления GRE-соединением.**

| Заголовок кадра передачи | IP-заголовок | GRE-заголовок | PPP-заголовок | Зашифрованные данные PPP | Окончание кадра передачи |
|---|---|---|---|---|---|

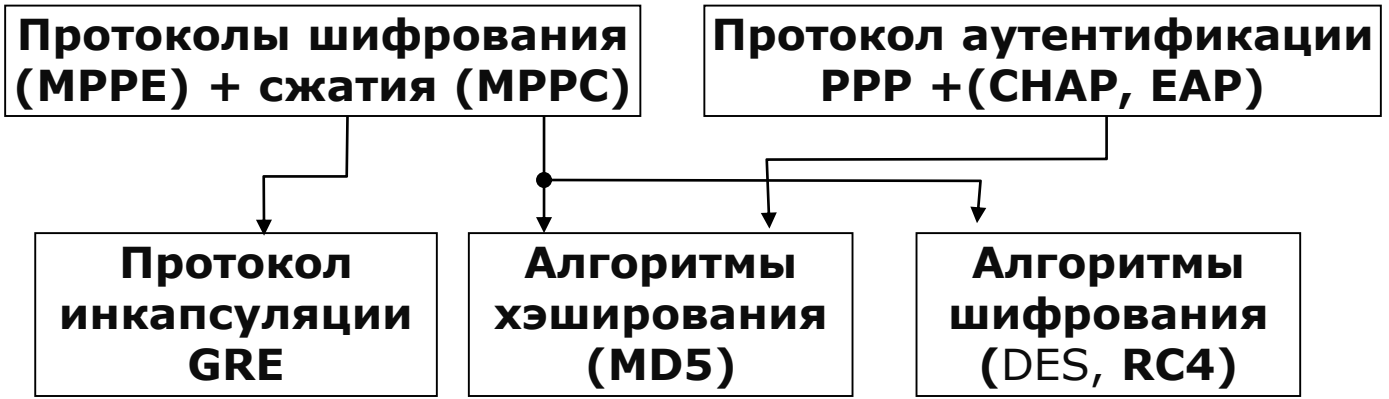
В основе обмена данными по протоколу PPTP лежит управляющее соединение PPTP - последовательность управляющих сообщений, которые устанавливают и обслуживают туннель.

| Управляющее сообщение | Функция |
|---|---|
| Start-Control-Connection-Request | Запрос на установление управляющего соединения |
| Start-Control-Connection-Replay | Ответ на сообщение Start-Control-Connection-Request |
| Echo-Request | Сообщение "Keep-alive" ("все живы") для управляющего соединения |
| Echo-Replay | Ответ на сообщение Echo-Request |
| Set-Link-Info | Посылается сервером сети для задания PPP-параметров переговоров |
| Stop-Control-Connection-Request | Команда завершить управляющее соединение |
| Stop-Control-Connection-Replay | Ответ на сообщение Stop-Control-Connection-Request |



Для шифрования данных при организации туннеля по протоколу PPTP применяется протокол MPPE – Microsoft Point-to-Point Encryption с длиной ключа 40, 56 или 128 бит

Протокол GRE (Generic Routing Encapsulation) используется для управления данными, передаваемыми в инкапсулированных дейтаграммах, и контроля плотности потока.



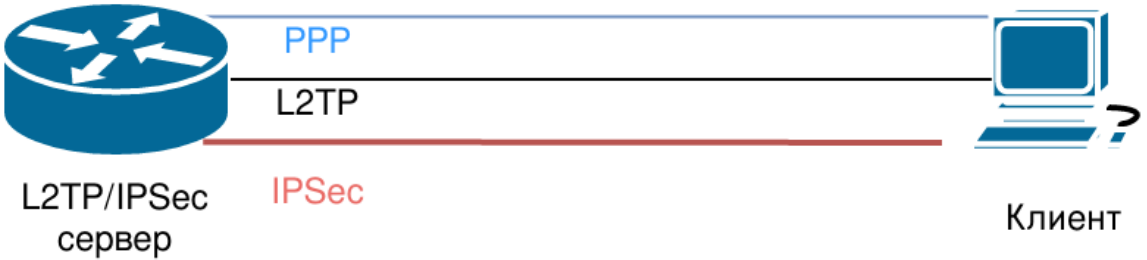
**L2TP (Layer 2 Tunneling Protocol)** — туннельный протокол, использующийся для поддержки виртуальных частных сетей.

Для обеспечения безопасности пакетов L2TP используется набор протоколов IPSec, который обеспечивает конфиденциальность, аутентификацию и целостность передаваемых данных.

После запуска сервера L2TP начинается прослушивание порта UDP/1701 на предмет входящих соединений L2TP на внешнем интерфейсе сервера VPN. В штатном режиме работы клиент VPN первым устанавливает сеанс IPSec с сервером VPN, после чего через туннель IPSec устанавливается соединение L2TP.

При прослушивании порта UDP/1701 L2TP сервер также принимает входящие подключения L2TP, которые не туннелируются при помощи IPSec. Это может быть использовано, например, в том случае, если пользователь устанавливает соединение L2TP VPN без туннеля IPSec (следует отметить, что клиенты VPN под управлением ОС Windows не имеют такой возможности), при этом весь трафик пользователя будет «открытым», то есть не будет шифроваться.

На рисунке ниже приведен режим VPN удаленного доступа с использованием протокола L2TP (Layer 2 Tunneling Protocol) и IPSec.



## VPN удаленного доступа на основе протокола L2TP/IPSec

При использовании такого решения:

- Удаленный компьютер сначала устанавливает туннель IPSec к серверу VPN.
- Затем клиент и сервер L2TP устанавливают туннель L2TP поверх туннеля IPSec.
- Далее сеанс PPP устанавливается поверх туннеля L2TP: пакеты PPP инкапсулируются и принимаются/отправляются через туннель L2TP.

В практических условиях рекомендуется ограничивать использование L2TP соединений без использования IPSec. В зависимости от ситуации этого можно добиться следующими способами:

- В том случае если сервер VPN размещается в демилитаризованной зоне (DMZ) и перед ним установлен межсетевой экран, то межсетевой экран может быть настроен на прохождение к серверу VPN только трафика IPSec (то есть прохождение пакетов на UDP порт 1701 запрещено). Таким образом, соединения L2TP/IPSec смогут быть установлены, а соединения L2TP будут заблокированы.
- В том случае если сервер VPN напрямую подключен ко внешней сети, межсетевой экран на сервере VPN должен быть настроен таким образом, чтобы запрещать отдельные соединения L2TP. Например, для того чтобы разрешить подключения L2TP/IPSec, можно определить в системе следующее правило и применить его к внешнему интерфейсу с использованием ключевого слова **local** (правило в этом случае будет применяться к пакетам, предназначенным для системы Numa Edge). Соединения L2TP без использования IPSec могут быть заблокированы правилом **default-drop**.

## L2TP/IPSec с использованием предварительных ключей

Настройка режима с использованием предварительных ключей проще, чем настройка режима с использованием сертификатов стандарта X.509.

Следует учесть, что всеми удаленными пользователями VPN в части IPSec их подключений должны быть использованы одинаковые предварительные ключи, что может создавать определенные трудности — например, когда доступ VPN необходимо отозвать у одного из пользователей. Несмотря на то, что доступ можно ограничить на основе более высокоуровневой аутентификации, пользователь все же будет обладать ключом IPSec и сможет устанавливать сеансы IPSec, что нежелательно. Для того чтобы предотвратить такую ситуацию, необходимо будет настроить новый ключ на сервере VPN и всех клиентах VPN.

В этом случае на уровне PPP (с использованием имени и пароля) осуществляется только аутентификация пользователей. Шифрование данных обеспечивается средствами IPSec. Более того, чтобы осуществить шифрование, IPSec также требует аутентификации (использование IPSec в режиме, при котором осуществляется только шифрование, считается менее безопасным).

При использовании L2TP/IPSec с аутентификацией на основе предварительных ключей на всех удаленных клиентах должны быть настроены одинаковые ключи. Следовательно, при смене ключа необходимо будет настраивать заново все удаленные клиенты. Использование аутентификации на основе сертификатов стандарта X.509 позволяет избежать указанной ситуации.

**L2TP/IPSec с использованием сертификатов стандарта X.509**

Использование сертификатов X.509 совместно с L2TP/IPSec позволит предотвратить вышеупомянутую ситуацию, однако применение сертификатов имеет свои сложности:

- Сертификаты стандарта X.509 необходимо создавать с использованием инфраструктуры открытых ключей (PKI) при помощи удостоверяющего центра (CA). Для этого могут использоваться PKI, созданные при помощи коммерческих или свободно распространяемых продуктов (например, OpenSSL), а также модуля PKI системы Numa Edge. Установка PKI требует комплексного подхода к вопросам безопасности.
- После получения сертификатов необходимо решить вопрос безопасной доставки сертификатов удаленным пользователям. Для этого, например, можно записать сертификаты на USB-флеш-накопитель и перенести их на каждое из клиентских устройств. Также сертификаты можно передать по протоколу SCP.
- При использовании сертификатов X.509 с L2TP/IPSec, настройка клиентов VPN в ОС Windows сложнее, чем при использовании предварительных ключей. По этой причине, а также из-за проблемы распределения сертификатов, может возникнуть необходимость предварительной настройки компьютеров клиентов для организации удаленного доступа.

Общая схема работы L2TP/IPSec VPN с использованием сертификатов X.509 функционирует следующим образом:

- Сетевой администратор получает сертификат, подписанный удостоверяющим центром для каждого удаленного пользователя, и распространяет их пользователям через безопасные каналы совместно с пользовательскими открытыми/секретными ключами.
- Сетевой администратор настраивает сервер VPN с открытым ключом удостоверяющего центра.
- Когда удаленный клиент подключается к серверу VPN, он предоставляет свой сертификат.
- Сервер VPN подтверждает подлинность сертификата при помощи открытого ключа удостоверяющего центра. В результате успешной проверки подлинности сервер получает открытый ключ клиента. Впоследствии сервер может использовать данный открытый ключ для аутентификации.
- В результате успешной аутентификации устанавливается туннель IPSec между клиентом и сервером, после чего этапы использования L2TP и PPP аналогичны тем, которые применяются при аутентификации с помощью предварительных ключей.

**Сравнительный анализ протоколов L2TP и PPTP:**

- PPTP требует, чтобы другая сеть была сетью, основанной на использовании протокола IP. L2TP может, применяя UDP в качестве транспортного протокола, передавать данные по сетям IP, Frame Relay, X.25 и ATM.
- L2TP может использовать несколько туннелей между одной и той же парой оконечных узлов, тогда как PPTP позволяет создать только один туннель.
- L2TP может использовать сжатие заголовков, а PPTP — нет.
- L2TP может обеспечивать аутентификацию туннеля, а PPTP— нет.
- В отличие от туннеля PPTP, туннель L2TP имеет собственный управляющий канал.

**Недостатки протокола L2TP :**

- для реализации протокола L2TP необходима поддержка провайдеров ISP;
- протокол L2TP ограничивает трафик рамками выбранного туннеля и лишает пользователей доступа к другим сегментам сети Internet;
- предложенная спецификация L2TP обеспечивает стандартное шифрование только в IP-сетях с помощью протокола IPSec.

**L2VPN (Layer 2 Virtual Private Network)** — это технология, позволяющая создать виртуальные частные сети на канальном уровне, обеспечивая прозрачность передачи данных между локальными сетями через общую инфраструктуру. L2VPN используется для соединения удаленных сетей, что позволяет им взаимодействовать так, как будто они находятся в одной локальной сети.

**Как работает L2VPN?**

L2VPN инкапсулирует канальные кадры в IP-пакеты для передачи через общие сети.

**Основные этапы работы L2VPN:**

**Инкапсуляция**. Канальные кадры помещаются в заголовок L2VPN;
**Передача**. Инкапсулированные кадры передаются через сеть провайдера;
**Декапсуляция**. На конечном узле кадры распаковываются и передаются получателю.

**Пример**: Ethernet-кадры могут быть инкапсулированы и переданы через L2VPN, обеспечивая возможность взаимодействия различных локальных сетей через общую сеть.

**Преимущества L2VPN:**

- Простота использования и развертывания;
- Возможность объединения сетей различных типов на канальном уровне.

**Недостатки L2VPN:**

- Необходимость в управлении на уровне канала;
- Зависимость от качества и надежности провайдерских сетей.

**L3VPN (Layer 3 Virtual Private Network)** представляет собой решение для создания виртуальных частных сетей на уровне сетевого протокола. Он используется для соединения различных сетей через общую инфраструктуру, обеспечивая защиту и изоляцию трафика между ними.

**Как работает L3VPN?**

L3VPN использует инкапсуляцию IP-пакетов для передачи данных через общие сети.

**Основные этапы работы L3VPN:**

- **Инкапсуляция**. IP-пакеты инкапсулируются в заголовок L3VPN;
- **Передача**. Инкапсулированные пакеты передаются через сеть провайдера;
- **Декапсуляция**. На конечном узле пакеты распаковываются и передаются получателю.

**Пример**: две удаленные офисные сети могут быть связаны через L3VPN, обеспечивая защищенный доступ к ресурсам друг друга через публичную сеть.

**Преимущества L3VPN:**

- Высокий уровень безопасности и изоляции трафика;
- Поддержка маршрутизации, что позволяет использовать различные протоколы на уровне 3.

**Недостатки L3VPN:**

- Необходимость в поддержке со стороны провайдеров;
- Сложности в настройке и управлении.

# Заключительная часть.

Сети VPN используются для создания защищённого сквозного соединения по частной сети через стороннюю сеть, например Интернет. В межфилиальной сети VPN на границе обоих узлов используются шлюзовые устройства VPN. Оконечные компьютеры не знают о сети VPN и не имеют дополнительного поддерживающего программного обеспечения.

Использование специализированных протоколов позволяет решить проблемы обеспечения информационной безопасности при подключении удаленных пользователей в сеть организации, а также объединить удаленные площадки организации в единую защищенную сеть.