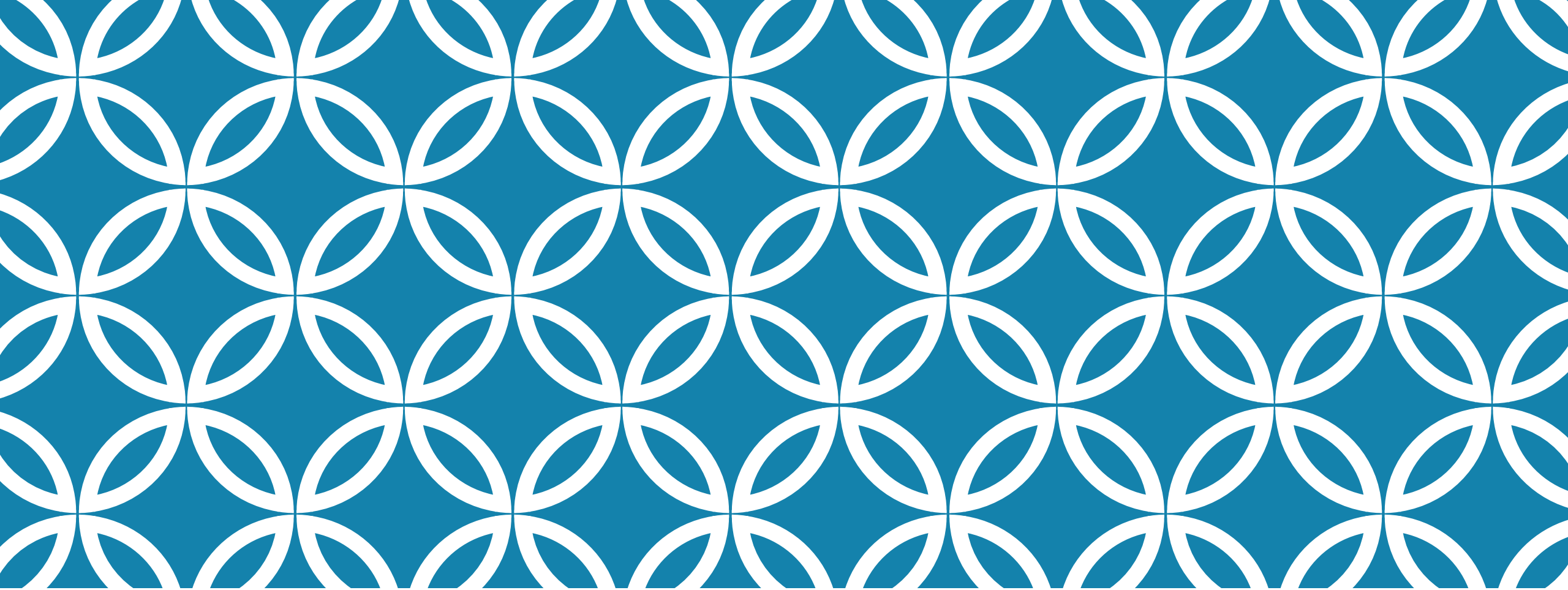


МОДУЛЬ 8. ПРИНЦИПЫ РАБОТЫ VPN И IPSEC

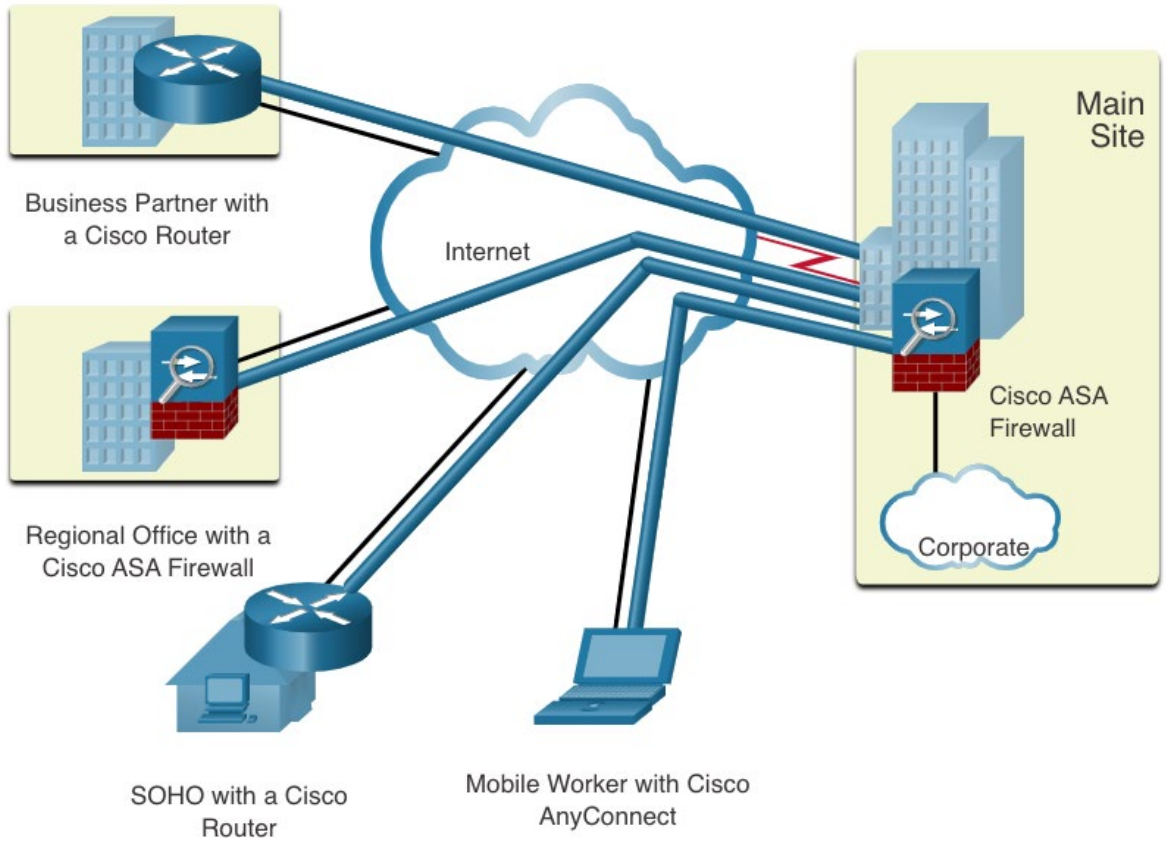
КАФЕДРА ТЕЛЕКОММУНИКАЦИЙ

8.1 ТЕХНОЛОГИЯ VPN
8.1.1 ВИРТУАЛЬНАЯ ЧАСТНАЯ СЕТЬ

Виртуальная частная сеть (VPN) предназначена для создания подключений «site-to-site» и удаленного доступа.

Сеть VPN является виртуальной в том смысле, что информация в ней находится в пределах частной сети, но фактически эта информация передается по общедоступной сети.

Сеть VPN является частной в том смысле, что трафик в ней шифруется для сохранения конфиденциальности данных при их передаче через общедоступную сеть.



8.1 ТЕХНОЛОГИЯ VPN
8.1.2 ПРЕИМУЩЕСТВА VPN

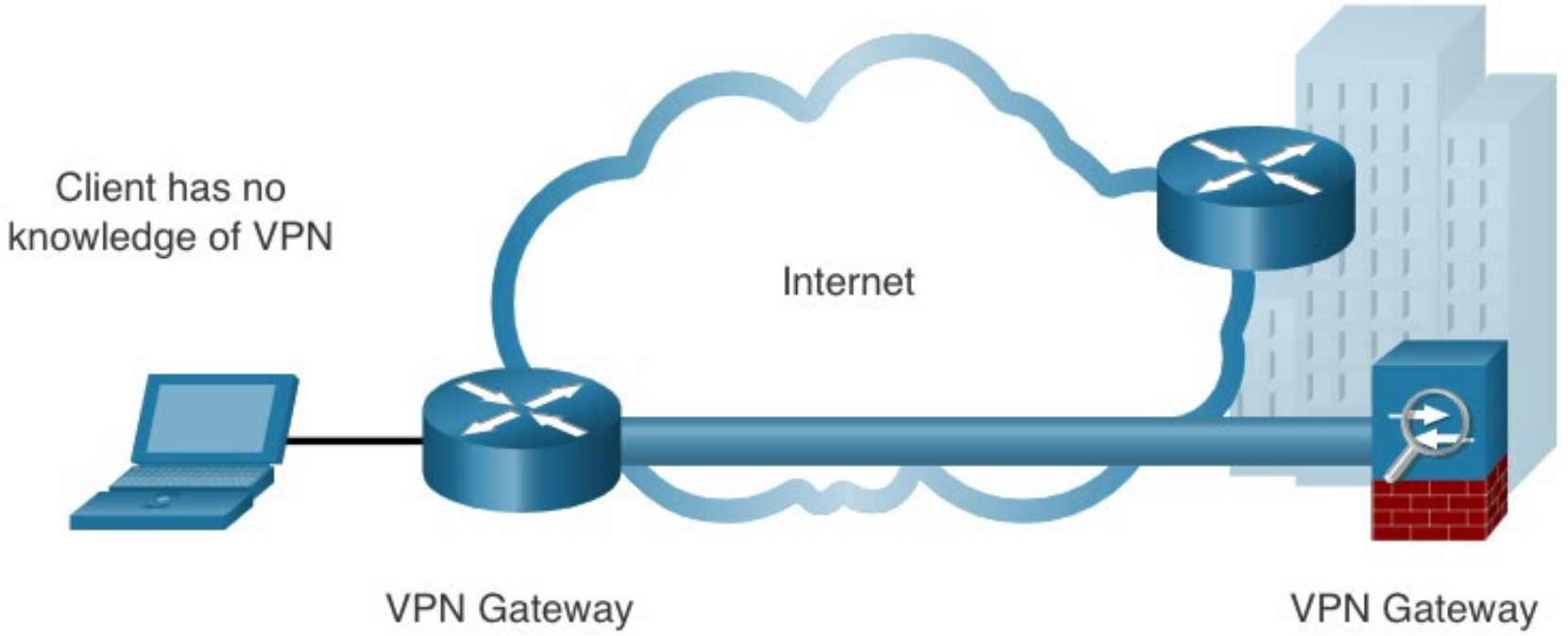
Современные VPN теперь поддерживают функции шифрования, такие как Internet Protocol Security (IPsec) и Secure Sockets Layer (SSL), для защиты сетевого трафика между сайтами.

Основные преимущества VPN показаны в таблице:

Преимущество	Описание
Сокращение затрат	Организации могут использовать сети VPN для сокращения своих затрат на организацию связи при одновременном повышении уровня пропускной способности удаленных подключений.
Безопасность	Протоколы шифрования и аутентификации защищают данные от несанкционированного доступа.
Масштабируемость	VPN позволяет организациям использовать Интернет, чтобы легко добавлять новых пользователей.
Совместимость	VPN могут быть реализованы в широком диапазоне вариантов каналов WAN, включая широкополосные технологии. Удаленные работники могут использовать эти высокоскоростные соединения для получения безопасного доступа к корпоративным сетям.

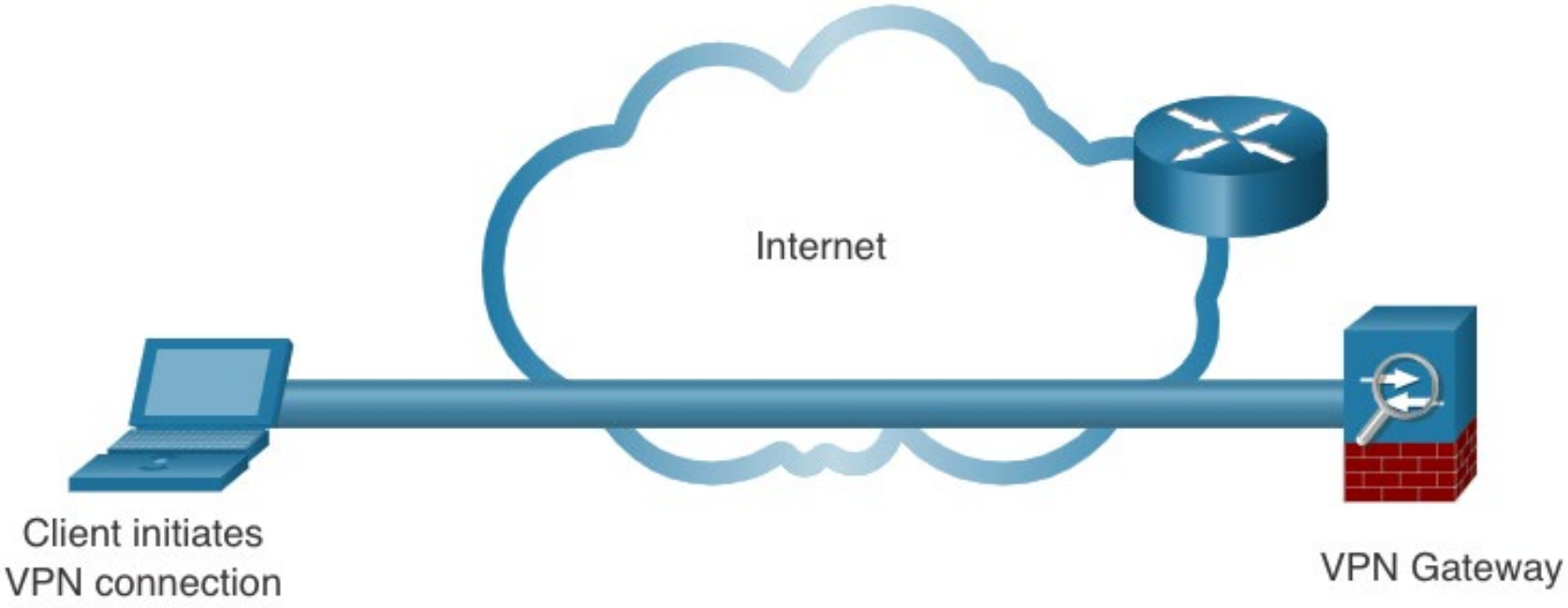
8.1 ТЕХНОЛОГИЯ VPN
8.1.3 VPN SITE-TO-SITE И УДАЛЕННЫЙ ДОСТУП

VPN типа site-to-site определяется шлюзами VPN. VPN трафик шифруется только между шлюзами. Внутренние узлы не знают о существовании VPN.



8.1 ТЕХНОЛОГИЯ VPN
8.1.3 VPN SITE-TO-SITE И VPN УДАЛЕННОГО ДОСТУПА

VPN с удаленным доступом динамически создается для установления безопасного соединения между клиентом и оконечным устройством VPN.

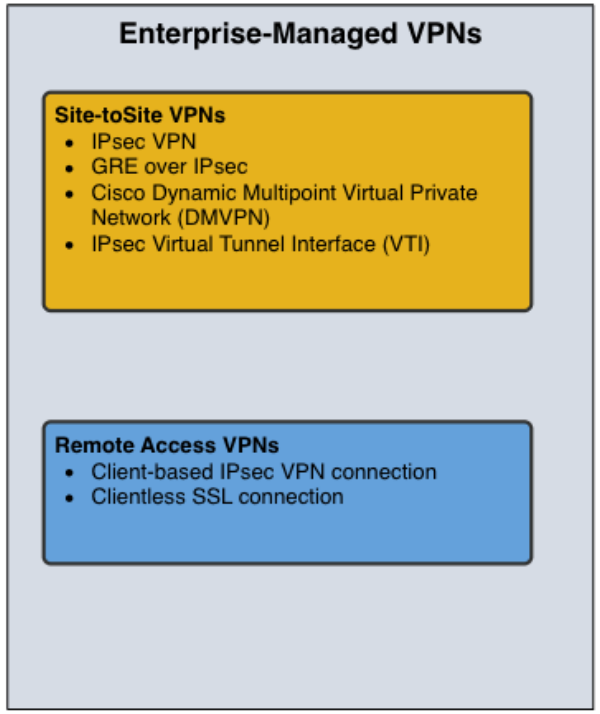


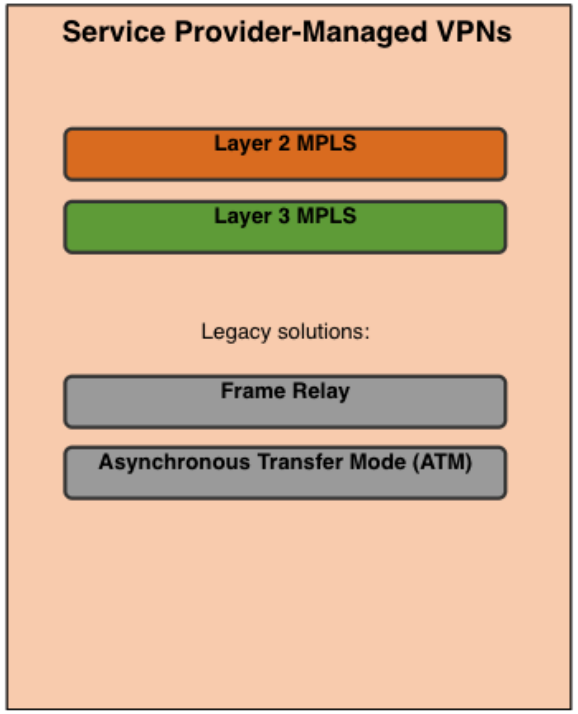
8.1 ТЕХНОЛОГИЯ VPN
8.1.4 VPN ДЛЯ КРУПНЫХ КОМПАНИЙ И ОПЕРАТОРОВ СВЯЗИ

VPN можно управлять и развертывать как:

VPN для крупных компаний - распространенное решение 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 - 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, эффективно отделяя трафик от трафика других клиентов.





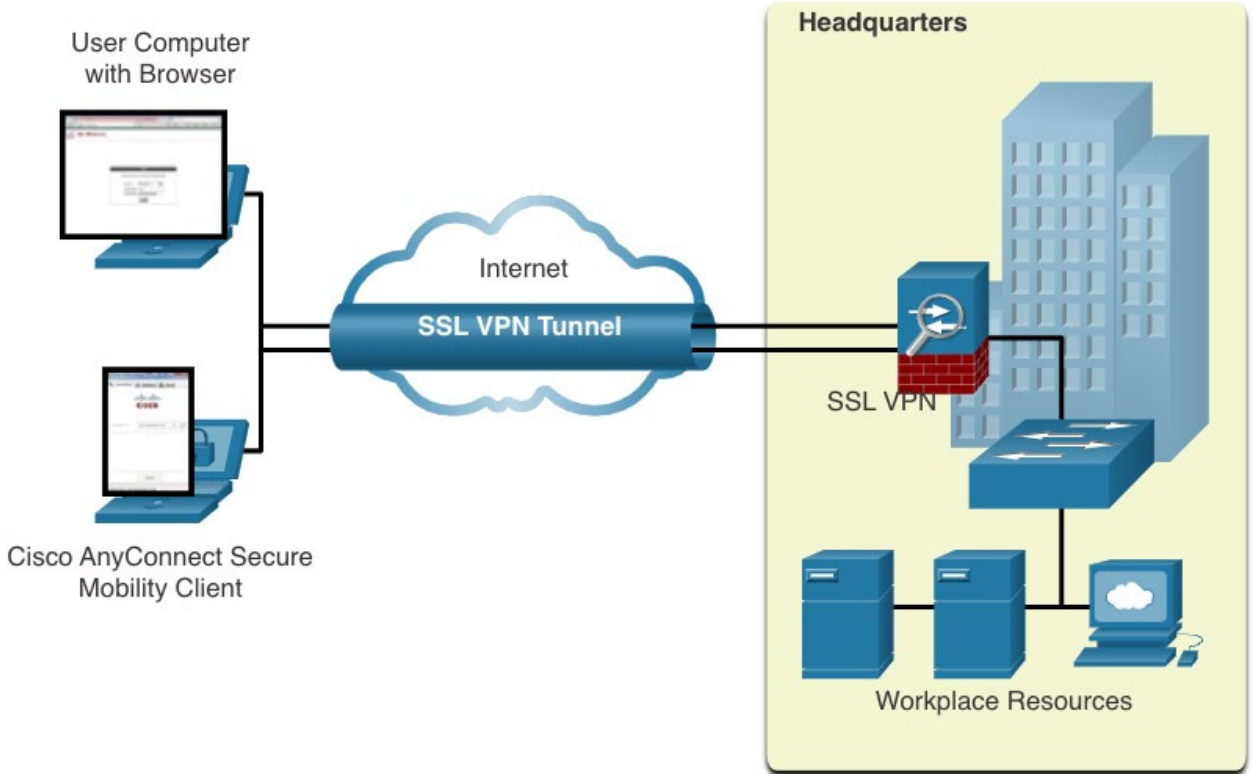
8.2 ТИПЫ СЕТЕЙ VPN
8.2.1 СЕТИ VPN УДАЛЕННОГО ДОСТУПА

VPN с удаленным доступом позволяют удаленным и мобильным пользователям безопасно подключаться к предприятию.

Сети VPN для удаленного доступа обычно включаются пользователем динамически, когда это необходимо, они могут создаваться с использованием IPsec или SSL.

Бесклиентное VPN-соединение - соединение защищено с помощью SSL-соединения через веб-браузер.

Клиентское VPN-соединение - программное обеспечение VPN-клиента, такое как Cisco AnyConnect Secure Mobility Client, должно быть установлено на конечном устройстве удаленного пользователя.



8.2 ТИПЫ СЕТЕЙ VPN
8.2.2 SSL VPN

SSL использует инфраструктуру открытых ключей и цифровые сертификаты для аутентификации партнеров. Используемый метод создания сети VPN основан на требованиях к доступу пользователей, а также процедурах ИТ в организации. В таблице сравниваются развертывания удаленного доступа IPsec и SSL.

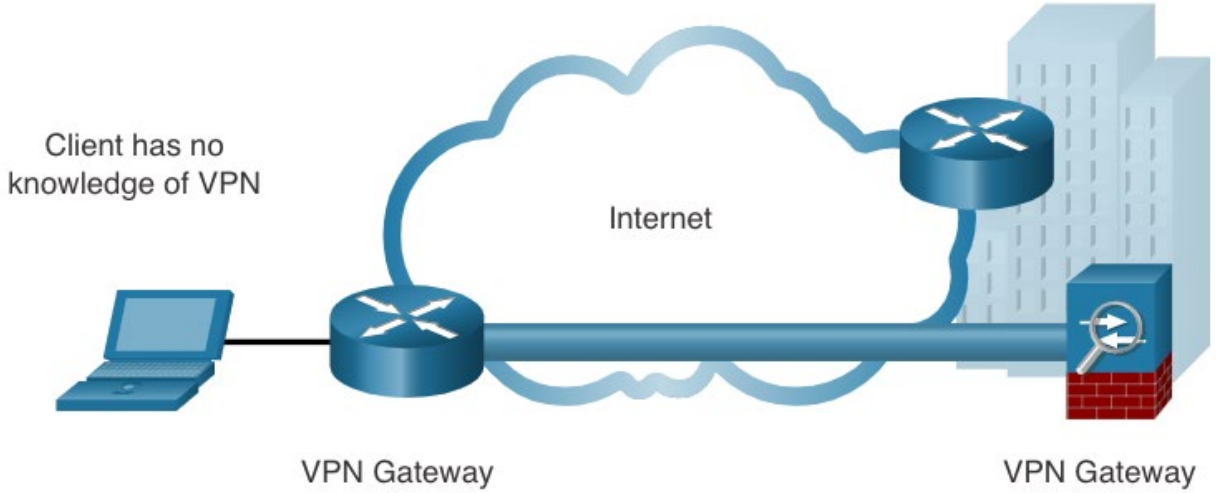
Функция	Протокол IPsec	SSL
Поддержка приложений	**Обширная** – поддерживаются все IP-приложения	**Ограниченная** – поддерживаются только веб-приложения
Сила аутентификации	**Сильная** – Использует двустороннюю аутентификацию с общими ключами или цифровыми сертификатами	**Умеренная** – Использует одностороннюю или двустороннюю аутентификацию
Сила шифрования	**Сильная** – Длина ключа 56 – 256 бит	**От умеренного до сильного** - Длина ключа 40 – 256 бит
Сложность подключения	**Средняя** – Требуется VPN-клиент, установленный на хосте	**Низкая** – Требуется только веб-браузер на хосте
Варианты подключения	**Ограниченный** – только определенные устройства с определенными устройствами	**Обширный** – любое устройство с веб-браузером может подключиться

8.2 ТИПЫ СЕТЕЙ VPN
8.2.3 SITE-TO-SITE IPSEC VPN

Site-to-site VPN используются для подключения сетей через другую ненадежную сеть, такую как Интернет.

Оконечные компьютеры отправляют и получают обычный трафик TCP/IP через шлюз VPN.

Шлюз VPN инкапсулирует и шифрует исходящий трафик с сайта и отправляет трафик через VPN-туннель на шлюз VPN на целевом сайте. Получающий данные шлюз VPN удаляет заголовки, расшифровывает содержимое и передает пакет в узел назначения по своей частной сети.



8.2 ТИПЫ СЕТЕЙ VPN
8.2.4 GRE ЧЕРЕЗ IPSEC

Универсальная инкапсуляция маршрутизации (Generic Routing Encapsulation, GRE) — это незащищенный протокол создания туннелей для сети VPN типа site-to-site.

Туннель GRE может инкапсулировать различные протоколы сетевого уровня, а также многоадресный и широковещательный трафик.

GRE по умолчанию не поддерживает шифрование и, следовательно, он не обеспечивает безопасный VPN-туннель.

Пакет GRE может быть инкапсулирован в пакет IPsec для безопасной пересылки на целевой VPN-шлюз.

Стандартный IPsec VPN (не GRE) может создавать безопасные туннели только для одноадресного трафика.

Инкапсуляция GRE в IPsec позволяет защищать обновления протокола многоадресной маршрутизации через VPN.

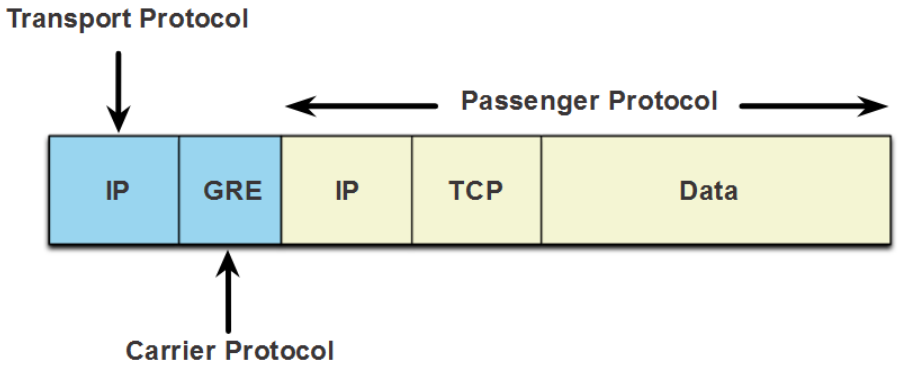
8.2 ТИПЫ СЕТЕЙ VPN
8.2.4 GRE ЧЕРЕЗ IPSEC

Термины, используемые для описания инкапсуляции GRE через туннель IPsec, представляют собой "протокол-пассажир", несущий протокол и транспортный протокол.

"Протокол-пассажир" – это оригинальный пакет, который должен быть инкапсулирован в GRE. Это может быть пакет IPv4 или IPv6, обновление маршрутизации и многое другое.

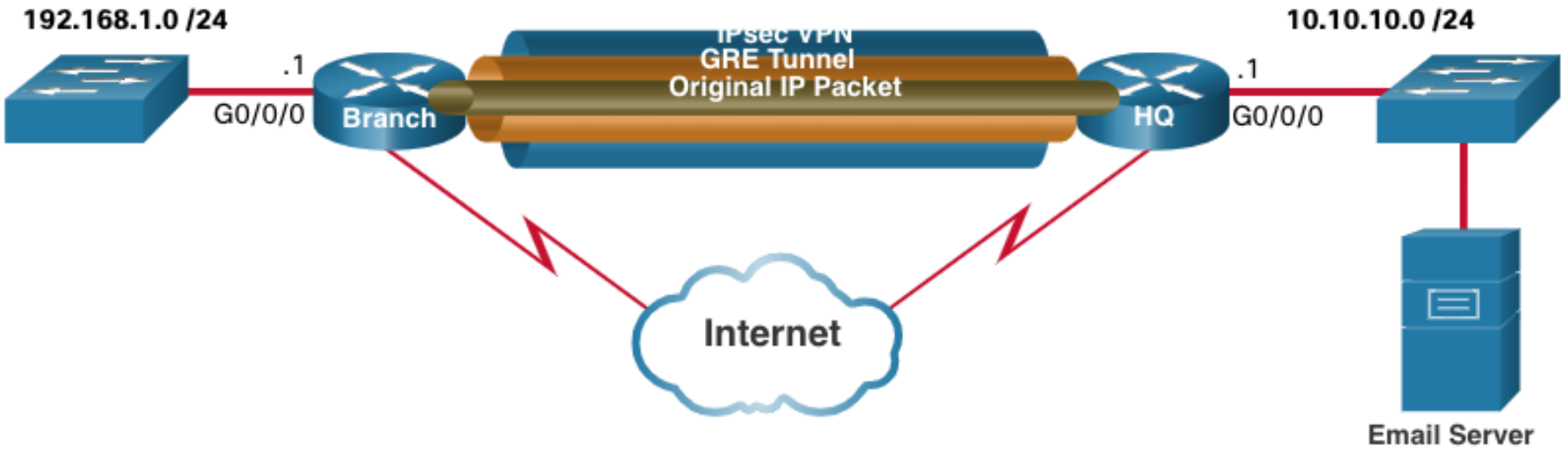
Несущий протокол – GRE является несущим протоколом, который инкапсулирует исходный пассажирский пакет.

Транспортный протокол – это протокол, который фактически будет использоваться для пересылки пакета. Это может быть IPv4 или IPv6.



8.2 ТИПЫ СЕТЕЙ VPN
8.2.4 GRE ЧЕРЕЗ IPSEC

Например, Branch и HQ хотели бы обмениваться информацией о маршрутизации OSPF через IPsec VPN. GRE через IPsec используется для поддержки трафика протокола маршрутизации через IPsec VPN. В частности, пакеты OSPF (то есть протокол-пассажир) будут инкапсулированы GRE (то есть несущим протоколом) и впоследствии инкапсулированы в VPN-туннель IPsec.



8.2 ТИПЫ СЕТЕЙ VPN

8.2.5 ДИНАМИЧЕСКАЯ МНОГОТОЧЕЧНАЯ VPN-СЕТЬ (DMVPN)

Site-to-site IPSec VPN и GRE через IPSec недостаточно, когда предприятие добавляет еще много сайтов. Динамическая многоточечная VPN-сеть (DMVPN) — это программное решение Cisco, обеспечивающее удобство, оперативность и масштабируемость при создании большого количества VPN.

DMVPN упрощает настройку VPN-туннеля и предоставляет гибкую возможность подключения центрального сайта к сайтам филиалов.

Он использует конфигурацию звезда для установления полносвязанной топологии.

Филиалы устанавливают безопасные VPN туннели до центра топологии.

Каждый сайт конфигурируется с использованием технологии Multipoint Generic Routing Encapsulation (mGRE). Туннельный интерфейс mGRE позволяет одному GRE интерфейсу поддерживать несколько динамических IPsec туннелей.

Сайты-получатели могут также получать информацию друг о друге и альтернативно строить прямые туннели между собой (spoke-to-spoke туннели).

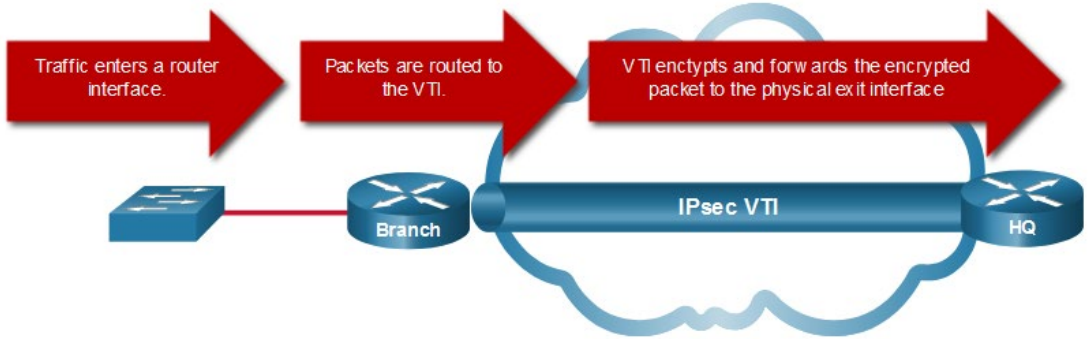
8.2 ТИПЫ СЕТЕЙ VPN
8.2.6 ИНТЕРФЕЙС ВИРТУАЛЬНОГО ТУННЕЛЯ IPSEC (VTI)

Интерфейс виртуального туннеля IPSec (Virtual Tunnel Interface - VTI) упрощает процесс настройки, необходимый для поддержки нескольких сайтов и удаленного доступа.

Конфигурации IPsec VTI применяются к виртуальному интерфейсу вместо статического сопоставления сеансов IPsec с физическим интерфейсом.

IPsec VTI способен отправлять и получать как одноадресный, так и многоадресный зашифрованный трафик. Поэтому протоколы маршрутизации поддерживаются автоматически без необходимости настройки туннелей GRE.

IPsec VTI может быть настроен между сайтами или в топологии hub-and-spoke.



8.2 ТИПЫ СЕТЕЙ VPN
8.2.7 MPLS VPN УРОВНЯ ПРОВАЙДЕРА

Сегодня провайдеры используют MPLS в своей сети ядра. Трафик передается через магистраль MPLS с использованием меток. Трафик защищен, потому что клиенты поставщика услуг не могут видеть трафик друг друга.

MPLS может предоставлять клиентам управляемые решения VPN, следовательно, защита трафика между клиентскими сайтами является обязанностью поставщика услуг.

Провайдеры поддерживают два типа решений MPLS VPN:

Layer 3 MPLS VPN - Провайдер участвует в маршрутизации клиентов, устанавливая пиринг между маршрутизаторами клиента и маршрутизаторами провайдера.

Layer 2 MPLS VPN - Провайдер не участвует в маршрутизации клиента. Вместо этого провайдер разворачивает службу виртуальной частной локальной сети (VPLS) для эмуляции сегмента локальной сети Ethernet с множественным доступом по сети MPLS без участия в маршрутизации. Маршрутизаторы клиента фактически принадлежат к одной и той же сети.

8.3 IPSec
8.3.1 IPSec ТЕХНОЛОГИИ

IPsec - это стандарт IETF, который определяет, как можно защитить VPN в IP-сетях. IPsec защищает и аутентифицирует IP-пакеты между источником и местом назначения и обеспечивает следующие важные функции безопасности:

Конфиденциальность - IPsec использует алгоритмы шифрования для предотвращения чтения содержимого пакета злоумышленниками.

Целостность - IPsec использует алгоритмы хеширования, чтобы гарантировать, что пакеты не были изменены между источником и назначением.

Аутентификация источника - IPsec использует протокол Internet Key Exchange (IKE) источника и получателя.

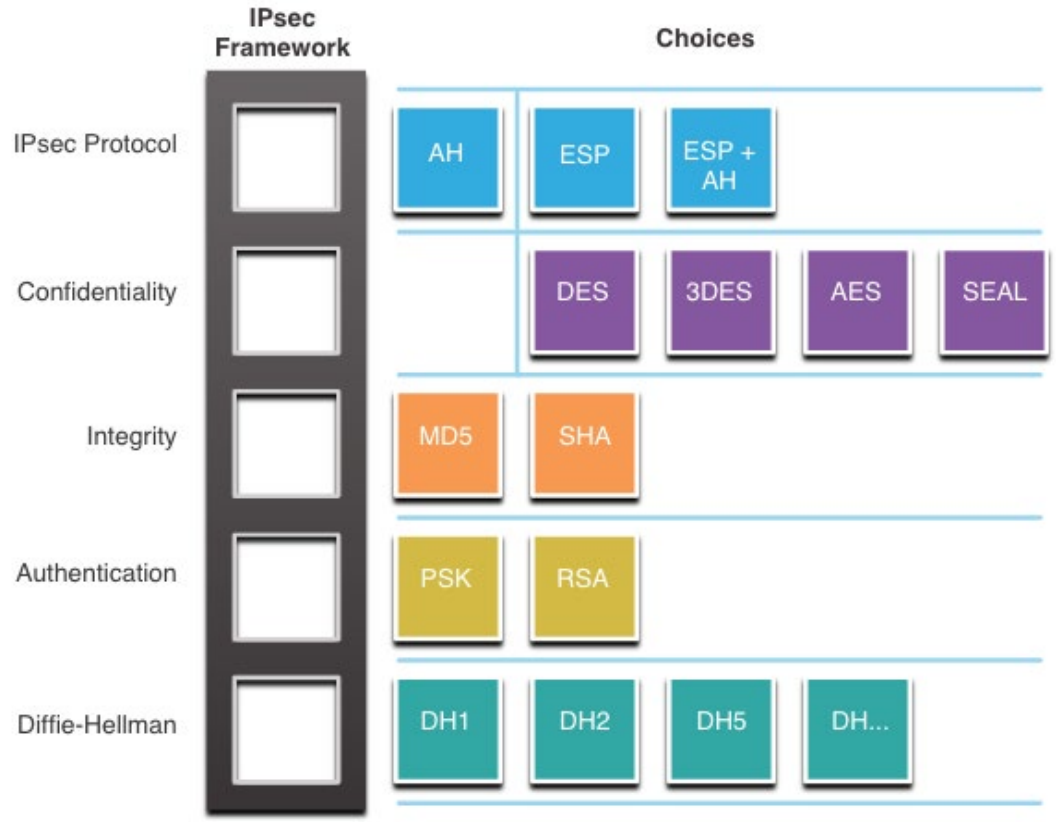
Диффи-Хеллман – используется для безопасного обмена ключами.

8.3 IPSec
8.3.1 IPSec ТЕХНОЛОГИИ

Для обеспечения безопасной связи протокол IPsec не привязан ни к каким специальным правилам.

IPsec может легко интегрировать новые технологии обеспечения безопасности без обновления существующих стандартов IPsec.

Открытые слоты, показанные в структуре IPsec на рисунке, могут быть заполнены любым из вариантов, доступных для этой функции IPsec, для создания уникальной ассоциации безопасности (SA).



8.3 IPSec
8.3.2 ИНКАПСУЛЯЦИЯ ПРОТОКОЛА IPSec

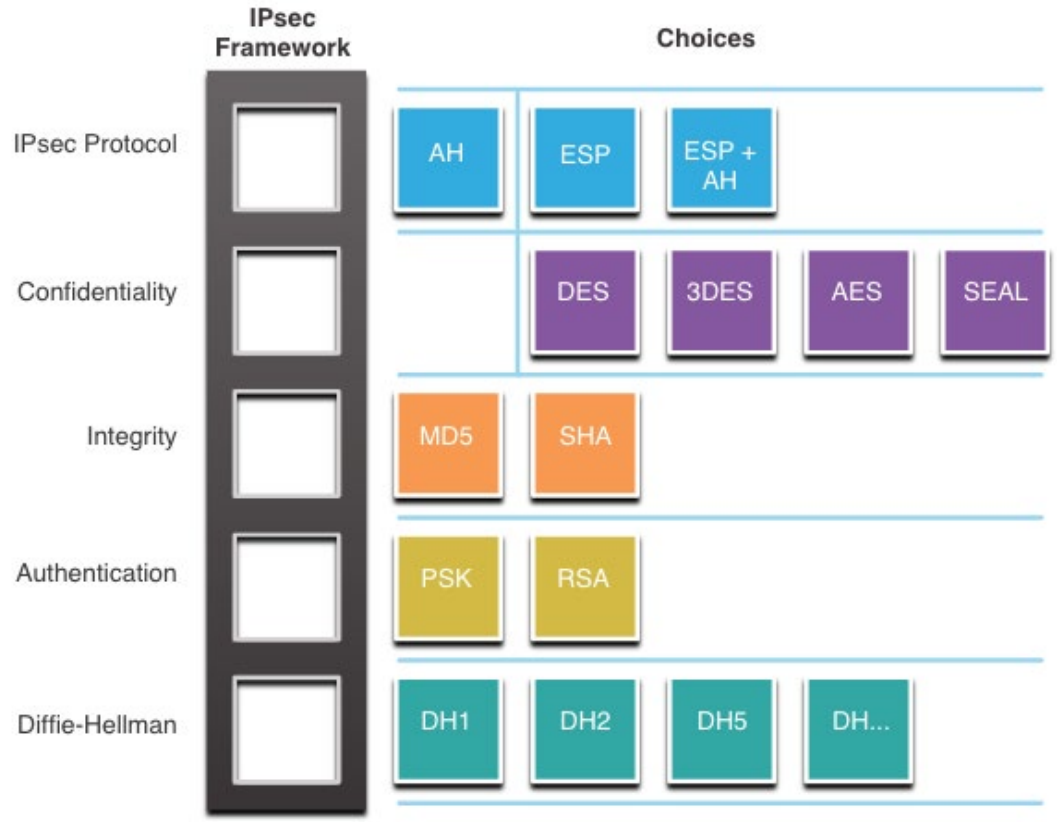
Выбор инкапсуляции протокола IPsec является основой фреймворка.

IPsec инкапсулирует пакеты с использованием Authentication Header (AH) или Encapsulation Security Protocol (ESP).

Выбор AH или ESP определяет, какие другие блоки будут доступны.

AH уместен только тогда, когда конфиденциальность не требуется или не разрешается.

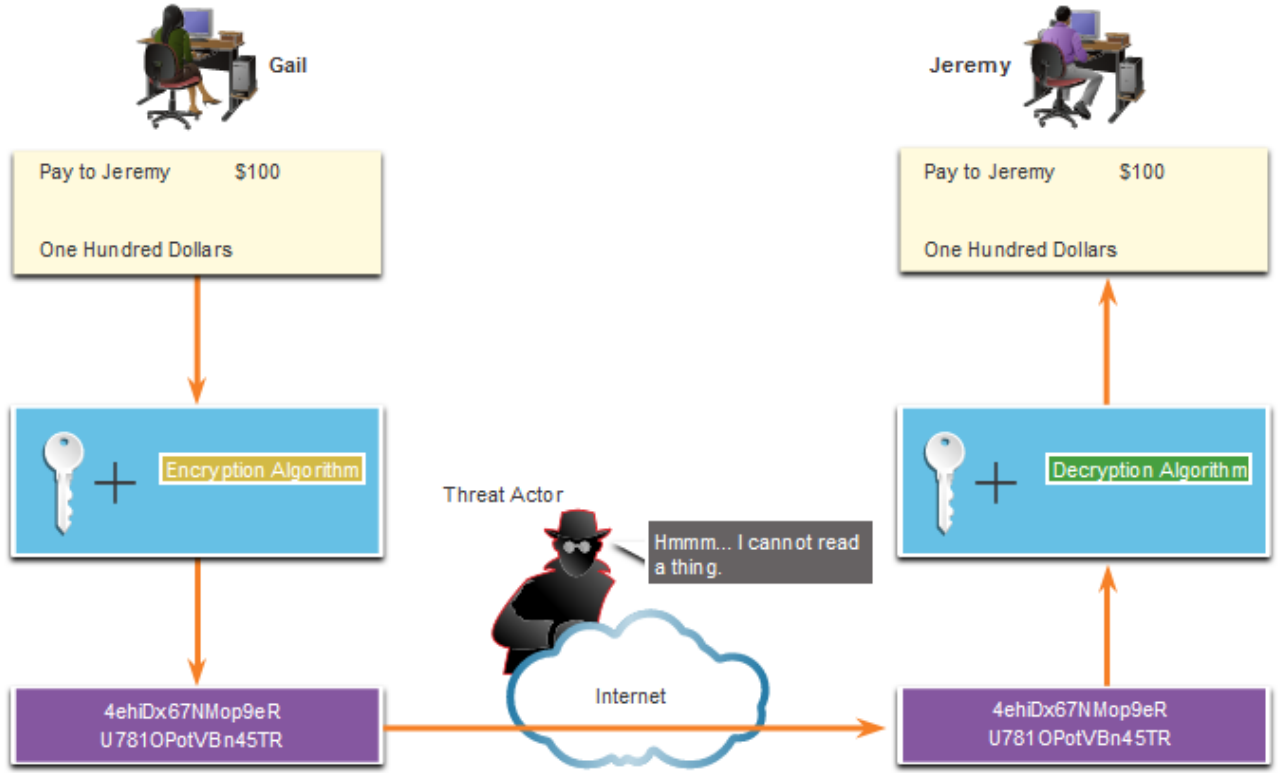
ESP обеспечивает конфиденциальность и аутентификацию.



8.3 IPSec
8.3.3 КОНФИДЕНЦИАЛЬНОСТЬ

Степень конфиденциальности зависит от алгоритма шифрования и длины ключа, используемого в алгоритме шифрования.

Количество попыток взлома ключа зависит от длины ключа: чем короче ключ, тем легче его взломать.



8.3 IPSec
8.3.3 КОНФИДЕНЦИАЛЬНОСТЬ

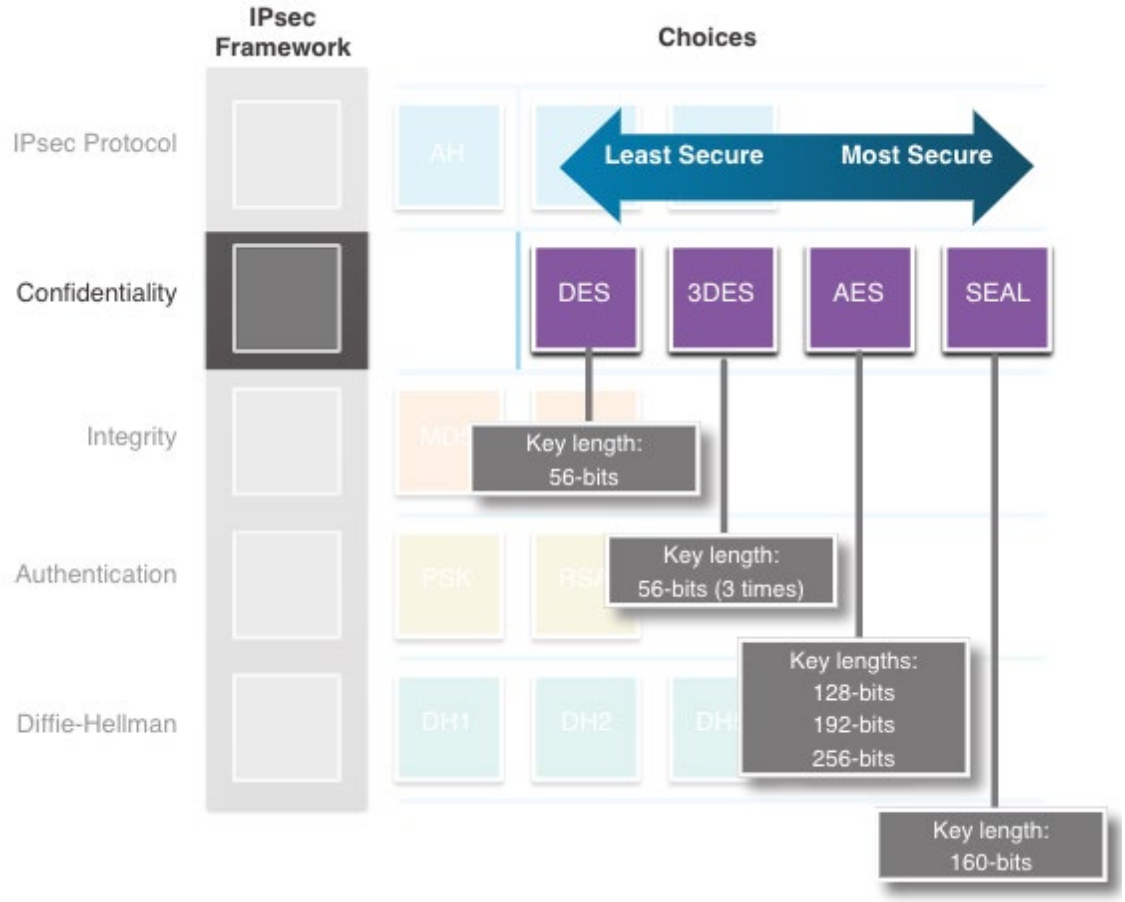
Все алгоритмы шифрования, выделенные на рисунке, представляют собой криптосистемы с симметричным ключом:

- DES использует 56-битный ключ.

- 3DES использует три независимых 56-битных ключа шифрования на 64-битный блок.

- AES предлагает три разных длины ключа: 128 бит, 192 бит и 256 бит.

- SEAL - это потоковый шифр, который означает, что он непрерывно шифрует данные, а не шифрует блоки данных. SEAL использует 160-битный ключ.



8.3 IPSec
8.3.4 ЦЕЛОСТНОСТЬ

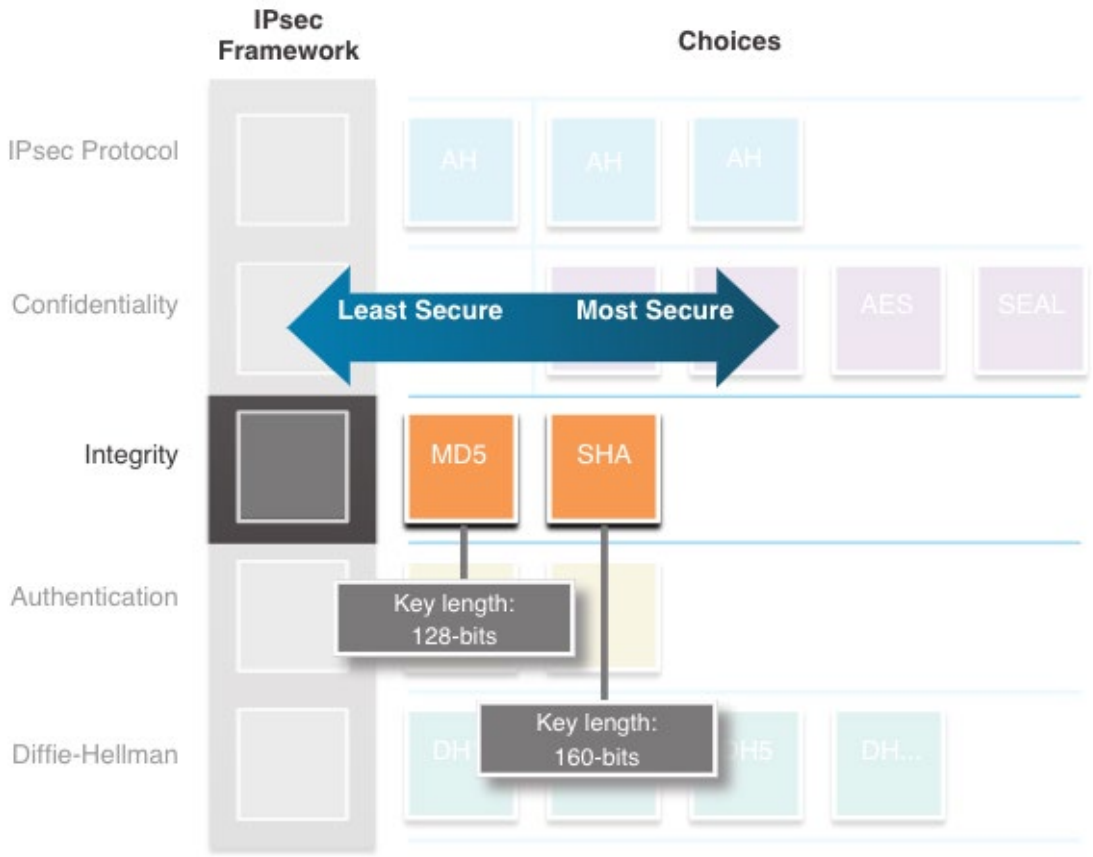
Целостность данных означает, что данные не изменились при передаче.

Существует потребность в методе доказательства целостности данных.

Hashed Message Authentication Code (HMAC) – это алгоритм обеспечения целостности данных, который гарантирует целостность сообщения с помощью хеш-значения.

Message-Digest 5 (MD5) использует 128-битный общий секретный ключ.

Secure Hash Algorithm (SHA) использует 160-битный секретный ключ.



8.3 IPSec
8.3.5 АУТЕНТИФИКАЦИЯ

Существует два метода аутентификации IPsec:

1. Предварительный общий ключ (Pre-shared key, PSK) - вводится в каждый узел вручную.

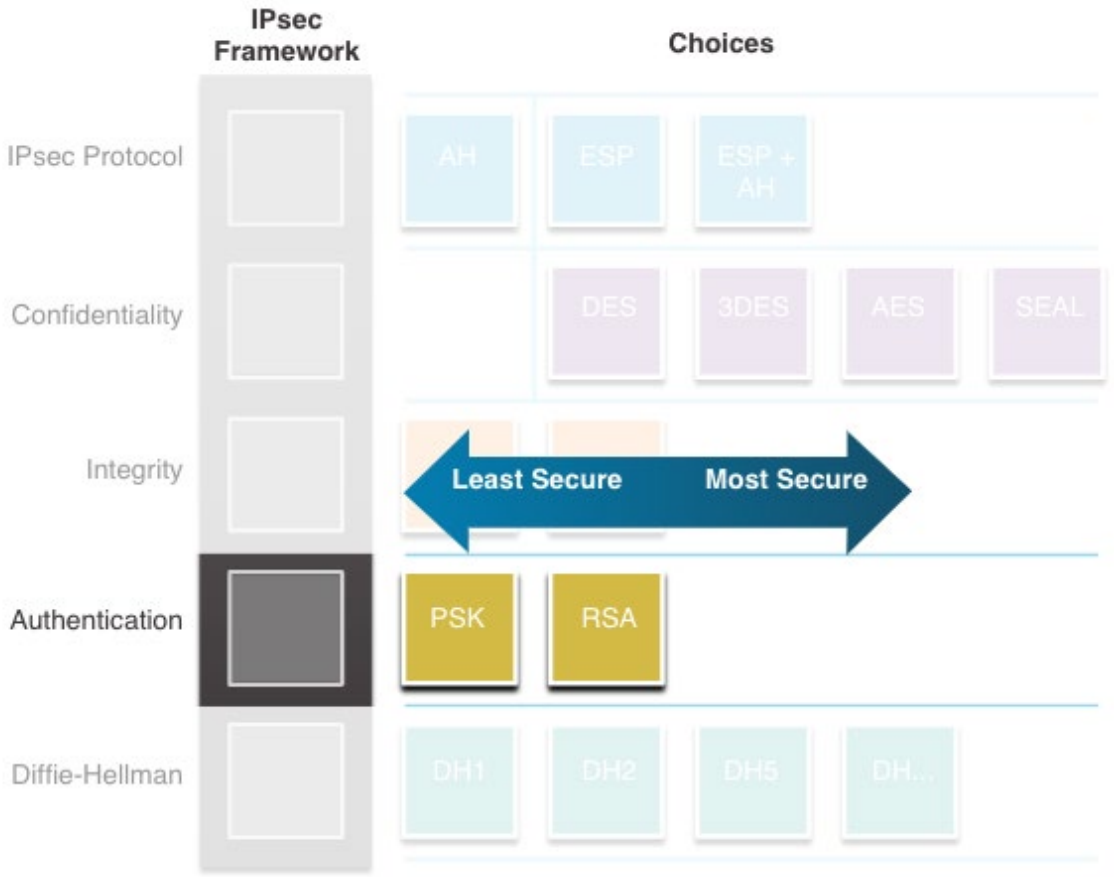
Простота настройки

Плохо масштабируется

Должен быть настроен на каждого участника.

2. Аутентификация Rivest, Shamir и Adleman (RSA) - использует цифровые сертификаты для аутентификации партнеров.

Каждый узел должен подтвердить подлинность своего противоположного узла, прежде чем туннель будет считаться безопасным.



8.3 IPSec
8.3.6 Безопасный обмен ключами с помощью алгоритма Диффи-Хеллмана

DH предоставляет двум участникам возможность установить общий секретный ключ по небезопасному каналу.

Варианты обмена ключами DH указаны как группы DH:

Группы DH 1, 2 и 5 больше не должны использоваться.

Группы DH 14, 15 и 16 используют ключи больших размеров с 2048 битами, 3072 битами и 4096 битами соответственно.

Группы DH 19, 20, 21 и 24 с соответствующими размерами ключей 256 бит, 384 бит, 521 бит и 2048 бит поддерживают криптографию с эллиптической кривой (ECC), которая сокращает время, необходимое для генерации ключей.