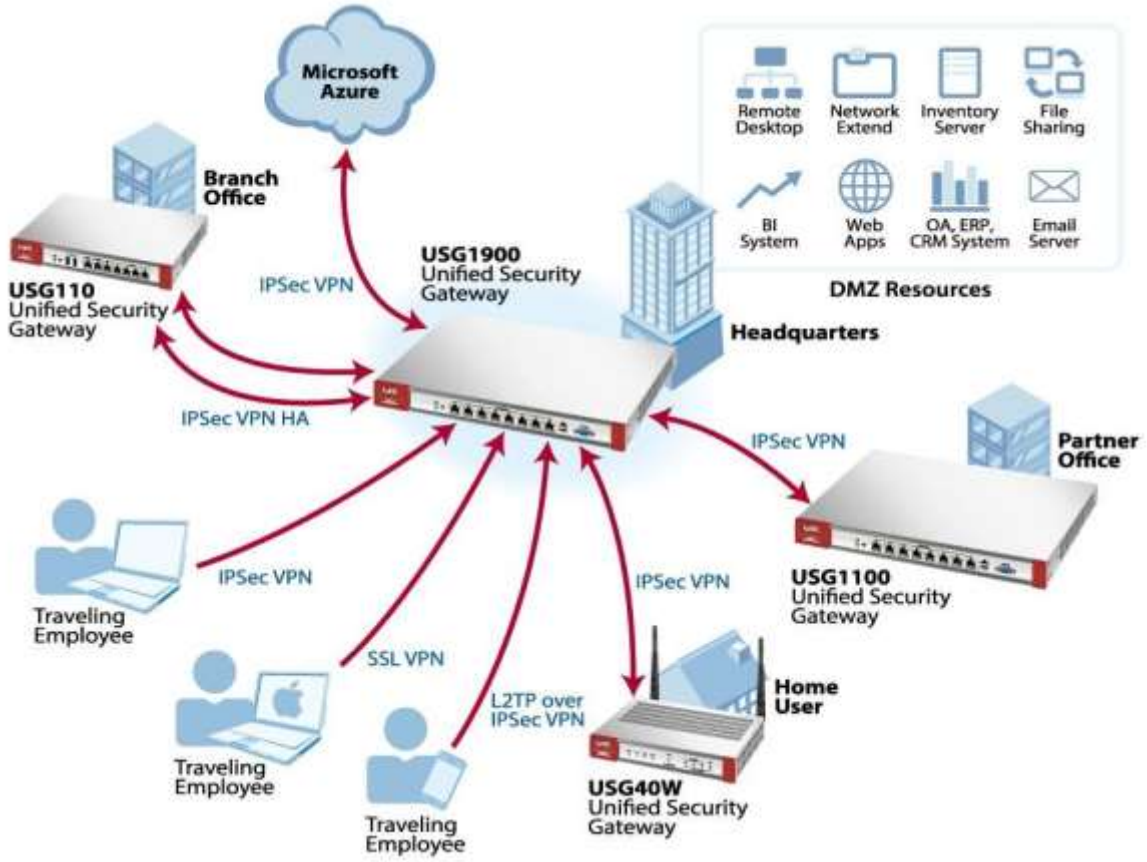
ТЕХНОЛОГИИ VPN

Антонов ДМ 2024

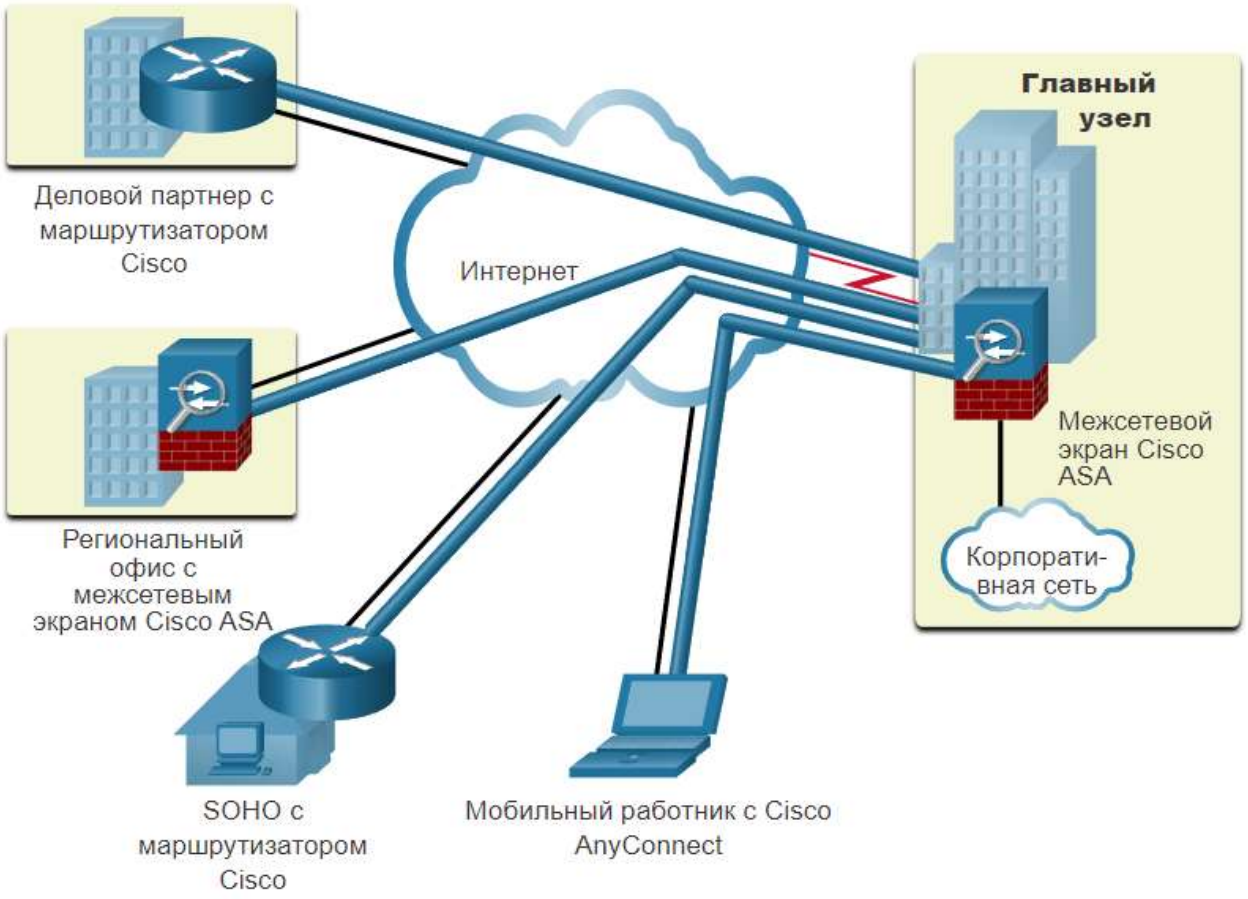
ТЕХНОЛОГИИ VPN



Чтобы защитить сетевой трафик между сайтами и пользователями, организации используют VPN для создания сквозных подключений к частной сети.

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.

ТЕХНОЛОГИИ VPN



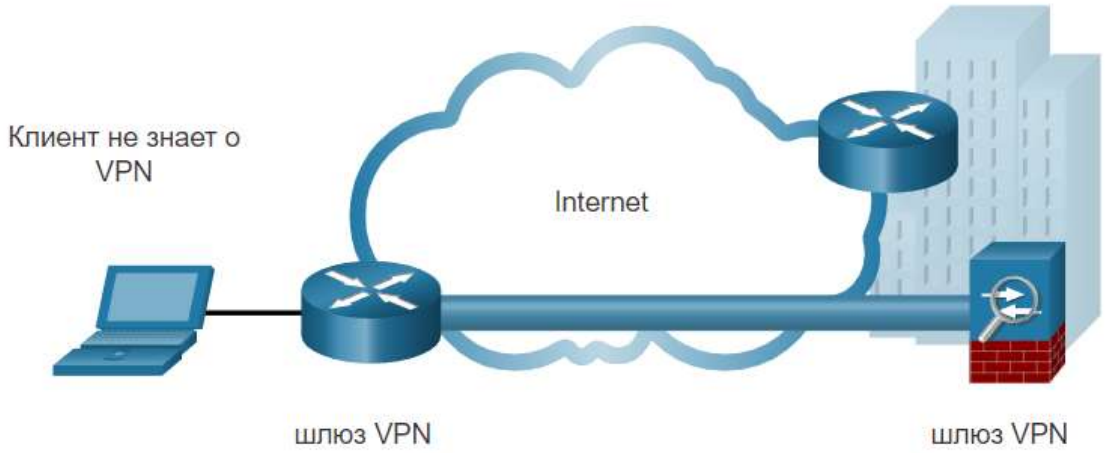
- Межсетевой экран Cisco Adaptive Security Appliance (ASA) помогает организациям предоставлять безопасные высокопроизводительные подключения, включая VPN и постоянный доступ для удаленных филиалов и мобильных пользователей.
- SOHO (small office/home office) - где VPN-маршрутизатор может обеспечить VPN подключения к корпоративному основному сайту.
- Решение Cisco AnyConnect - это программное обеспечение, которое удаленные работники могут использовать для установления клиентского VPN-соединения с основным сайтом.

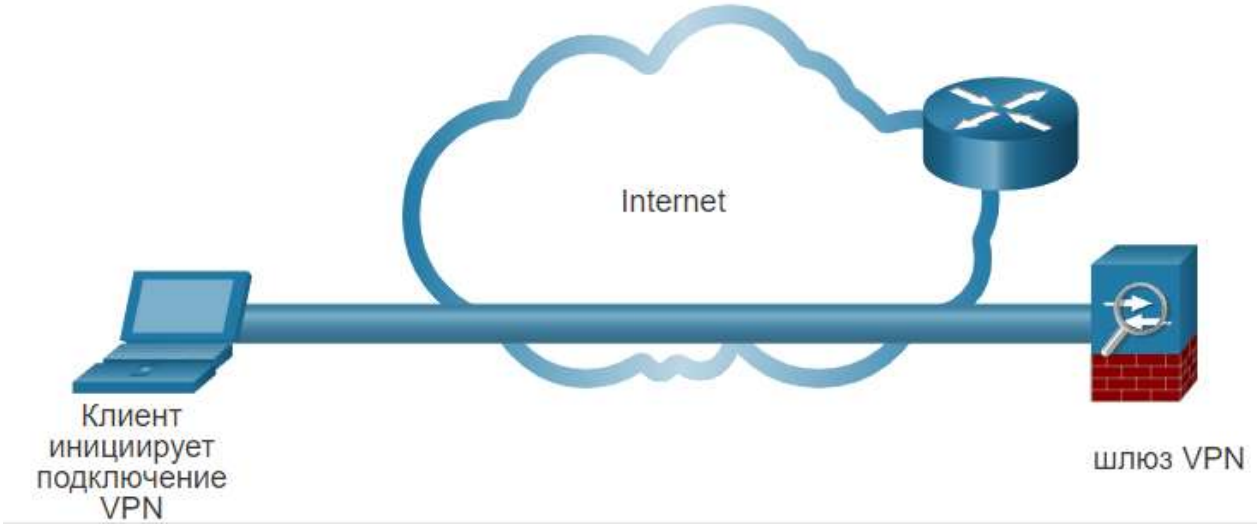
ТЕХНОЛОГИИ VPN

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.

ТЕХНОЛОГИИ VPN

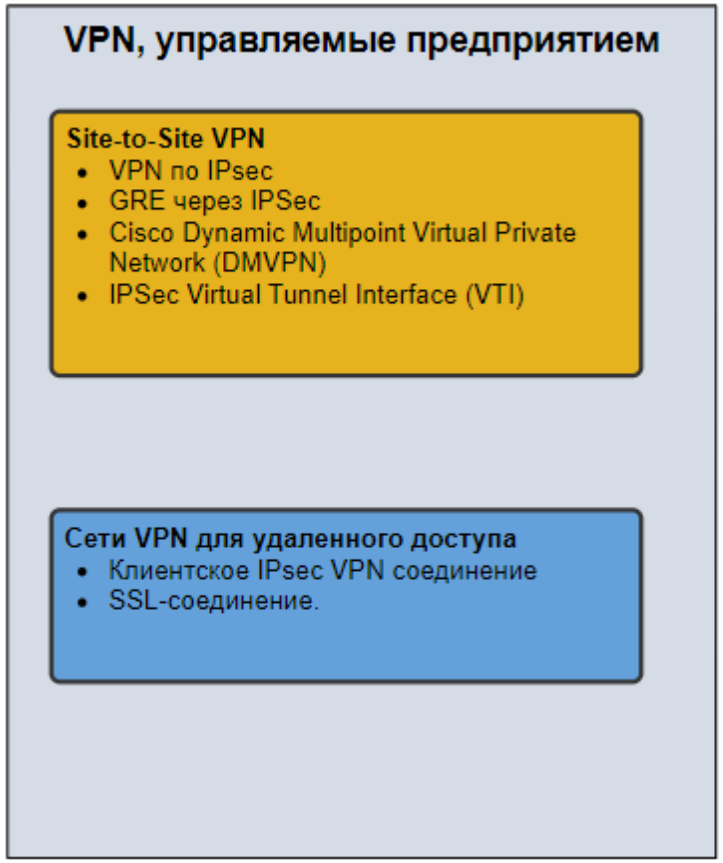
Site-to-Site VPN и VPN для удаленного доступа





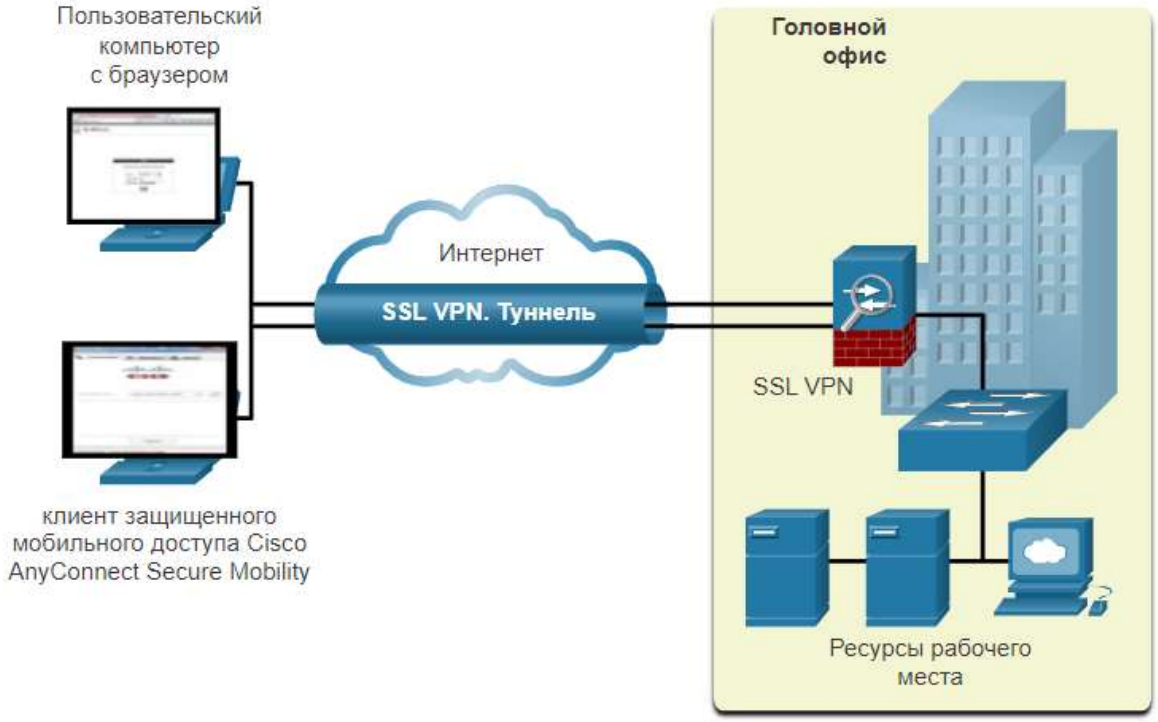
ТЕХНОЛОГИИ VPN

•**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.

ТЕХНОЛОГИИ VPN



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.

- **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.

ТЕХНОЛОГИИ VPN

SSL использует инфраструктуру открытых ключей и цифровые сертификаты для аутентификации партнеров. Технологии IPsec и SSL VPN делают возможным доступ практически к любому сетевому приложению или ресурсу. Однако, когда безопасность является проблемой, IPsec является лучшим выбором. Если первоочередными задачами являются поддержка и простота развёртывания, то следует иметь в виду протокол SSL.

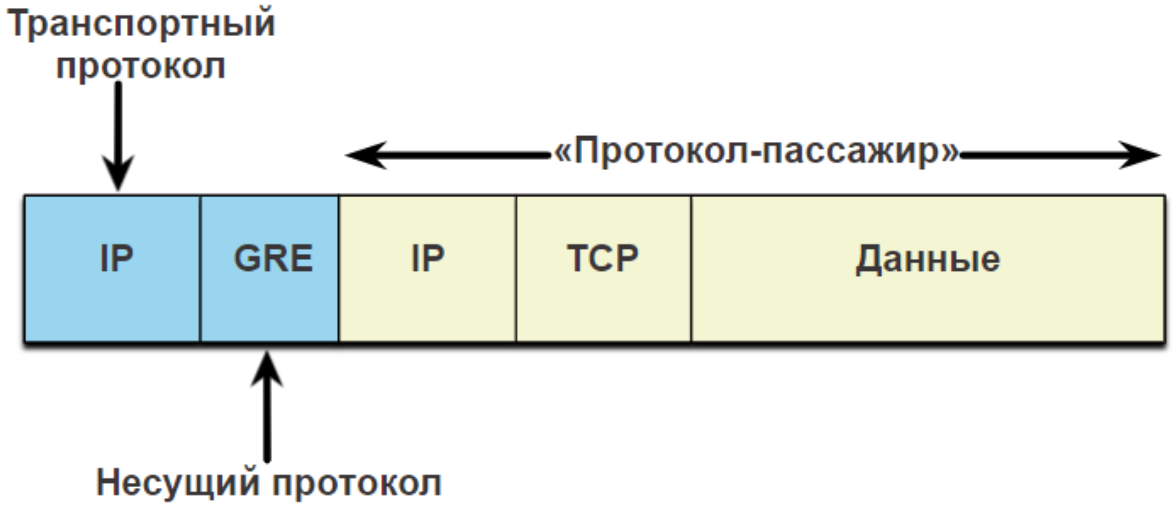
Функция	Протокол IPsec	SSL
Поддержка приложений	**Обширная** - все IP-приложения поддерживаются.	**Ограниченная** - поддерживаются только веб-приложения и обмен файлами.
Сила аутентификации	**Сильная** - использование двусторонней аутентификации с общими ключами или цифровыми сертификатами.	**Умеренная** - Использование односторонней или двусторонней аутентификации.
Сила шифрования	**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.

ТЕХНОЛОГИИ VPN

Site-to-site VPN используются для подключения сетей через другую недоверенную сеть, такую как Интернет. В site-to-site VPN конечные хосты отправляют и получают обычный незашифрованный трафик TCP/IP через оконечное устройство VPN. Оконечное устройство VPN обычно называется шлюзом VPN. Устройство шлюза VPN может быть маршрутизатором или межсетевым экраном

ТЕХНОЛОГИИ VPN

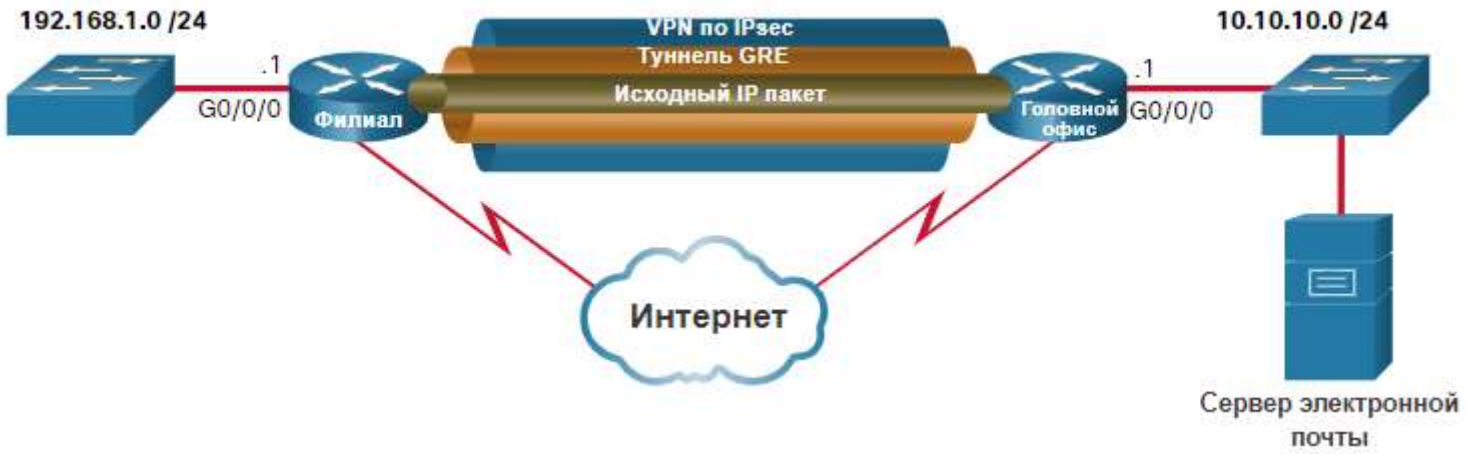
Универсальная инкапсуляция маршрутизации (Generic Routing Encapsulation, GRE) — это незащищенный протокол создания туннелей для сети VPN типа site-to-site. Он может инкапсулировать различные протоколы сетевого уровня. Он также поддерживает многоадресный и широковещательный трафик, который может быть необходим, если организации требуется протоколы маршрутизации для работы через VPN. Однако GRE по умолчанию не поддерживает шифрование; и, следовательно, он не обеспечивает безопасный VPN-туннель.



- **"Протокол-пассажир"** – Это оригинальный пакет, который должен быть инкапсулирован 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.

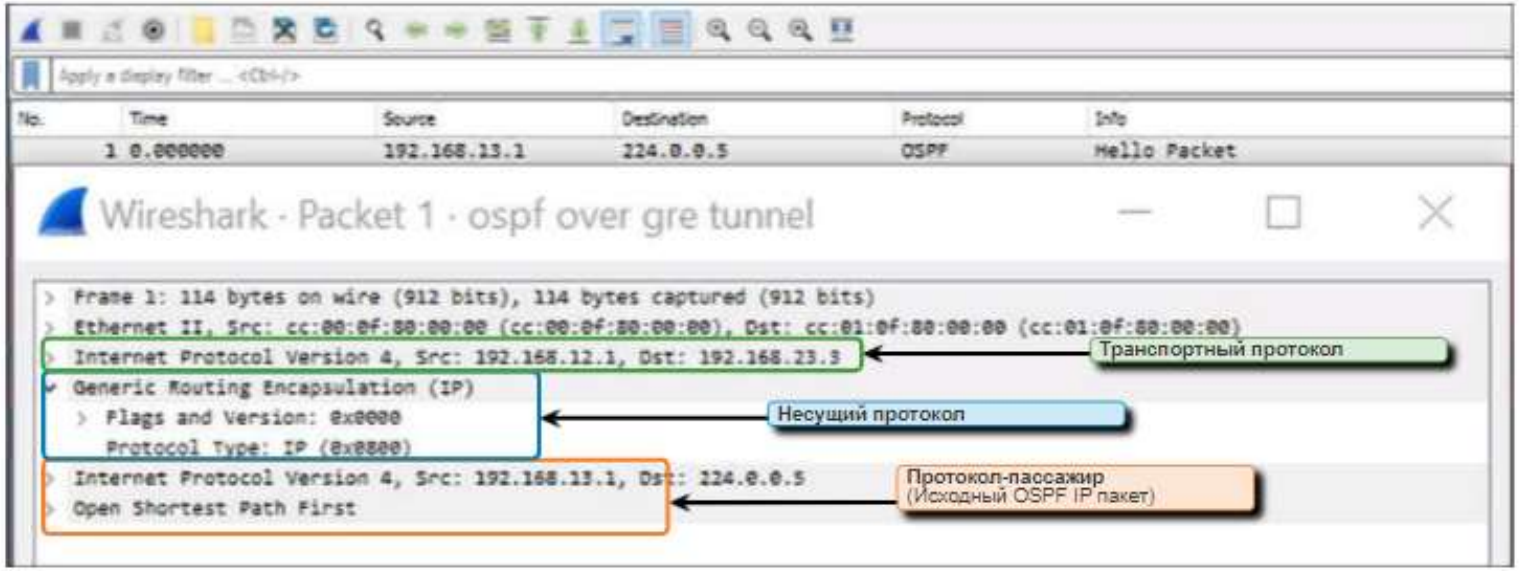
ТЕХНОЛОГИИ VPN

Branch и HQ хотели бы обмениваться информацией о маршрутизации OSPF через IPsec VPN. Однако IPsec не поддерживает многоадресный трафик. Поэтому 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.



ТЕХНОЛОГИИ VPN

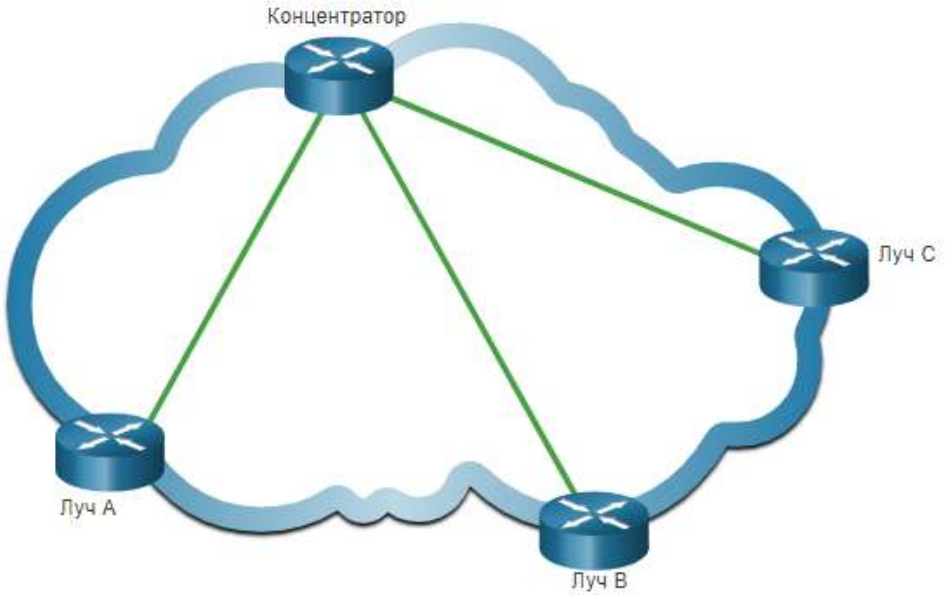
Пакет Hello OSPF, который был отправлен с использованием GRE через IPsec. В этом примере исходный многоадресный пакет Hello OSPF (то есть, пассажирский протокол) был инкапсулирован в заголовок GRE (то есть, в несущий протокол), который впоследствии инкапсулируется другим IP-заголовком (то есть транспортным протоколом). Тогда этот IP-заголовок будет пересылается через туннель IPsec.



ТЕХНОЛОГИИ VPN

Динамическая многоточечная VPN-сеть (DMVPN)

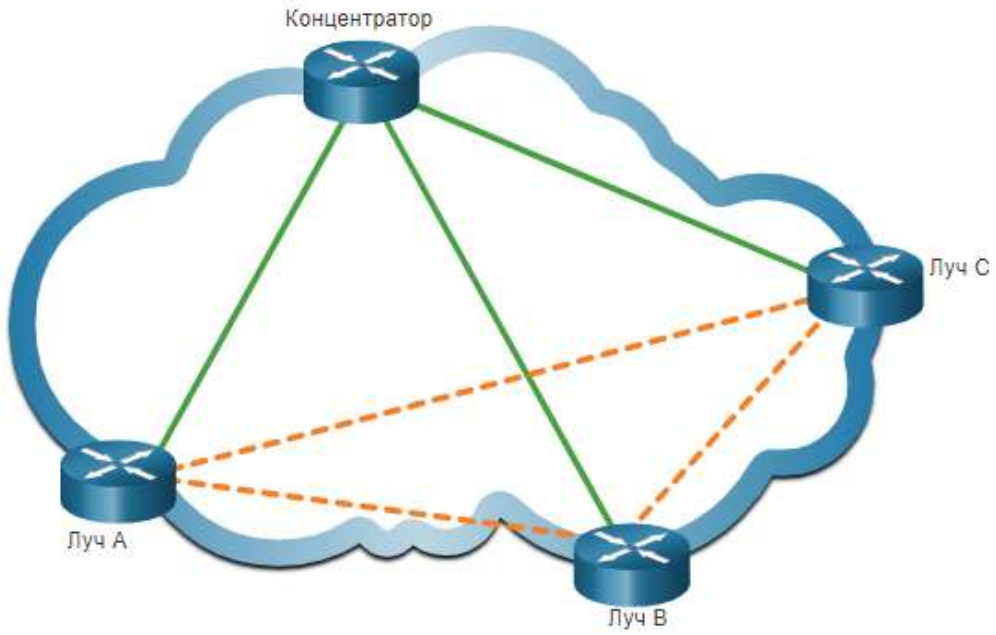
Site-to-site IPSec VPN и GRE через IPSec подходят для использования, когда для безопасного соединения существует всего несколько сайтов. Однако их недостаточно, когда предприятие добавляет больше сайтов. Это связано с тем, что для каждого сайта требуются статические конфигурации всех других сайтов или центрального сайта.



Динамическая многоточечная VPN-сеть (DMVPN) — это программное решение Cisco, обеспечивающее удобство, оперативность и масштабируемость при создании большого количества VPN. Как и другие типы VPN, DMVPN использует протокол IPsec для обеспечения безопасной передачи через общедоступные сети, такие как Интернет.

ТЕХНОЛОГИИ VPN

Туннели DMVPN типа «звезда» и «луч-луч»

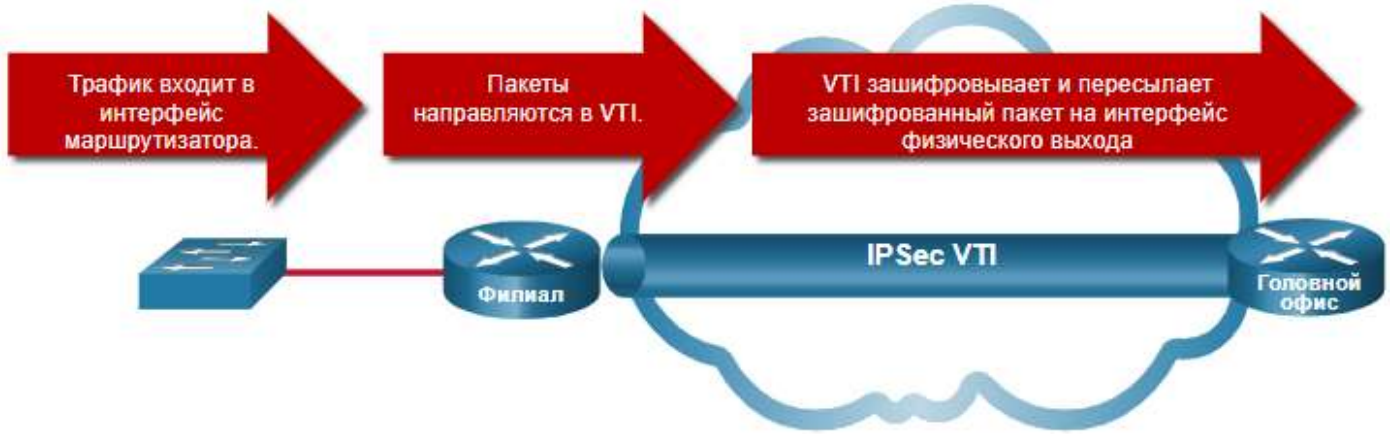


Каждый сайт конфигурируется с использованием технологии Multipoint Generic Routing Encapsulation (mGRE). Туннельный интерфейс mGRE позволяет одному GRE интерфейсу поддерживать несколько динамических IPsec туннелей. Следовательно, когда нужно установить новое безопасное соединение с центральным маршрутизатором, будет использоваться та же конфигурация для создания туннеля.

ТЕХНОЛОГИИ VPN

Интерфейс виртуальных туннелей IPsec

Как и DMVPN, интерфейс виртуального туннеля IPsec (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.

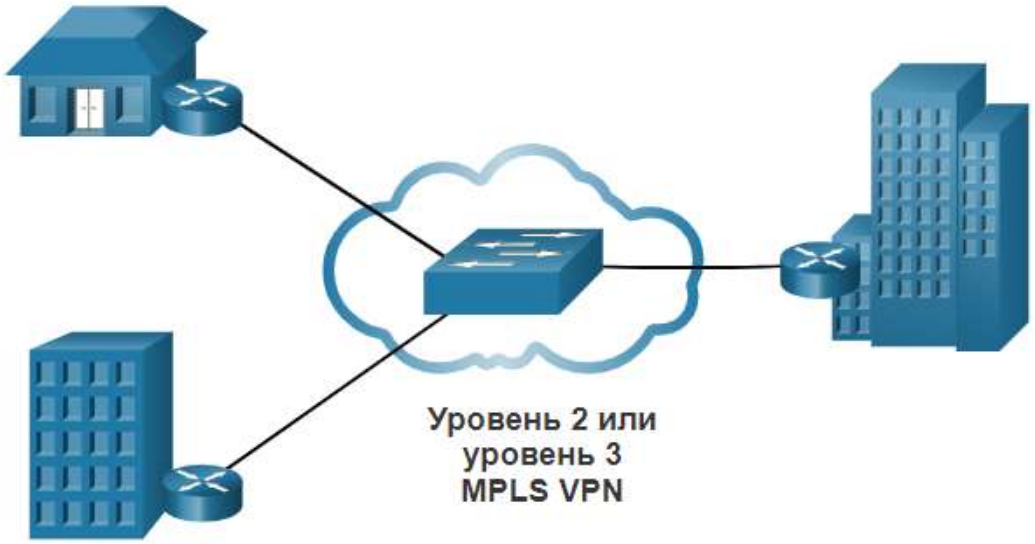


IPsec VTI способен отправлять и получать как одноадресный, так и многоадресный зашифрованный трафик. Поэтому протоколы маршрутизации поддерживаются автоматически без необходимости настройки туннелей GRE.

ТЕХНОЛОГИИ VPN

MPLS VPN уровня провайдера

Традиционные решения WAN для провайдеров изначально были безопасными в своей конструкции. Сегодня провайдеры используют MPLS в своей сети ядра. Трафик передается через магистраль MPLS с использованием меток, которые ранее были распределены между основными маршрутизаторами. Как и в случае устаревших WAN-соединений, трафик защищен, потому что клиенты поставщика услуг не могут видеть трафик друг друга.



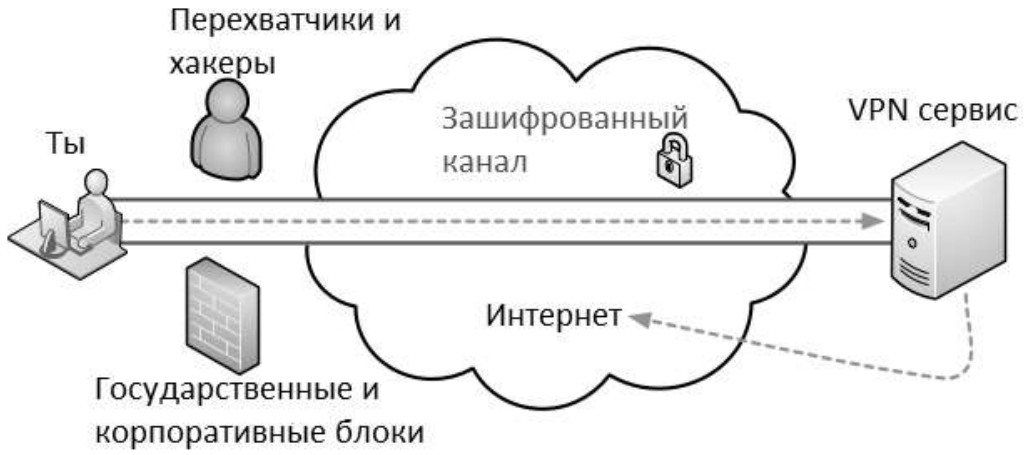
- **Уровень 3 MPLS VPN** - Провайдер участвует в маршрутизации клиентов, устанавливая пиринг между маршрутизаторами клиента и маршрутизаторами провайдера.
- **Уровень 2 MPLS VPN** - Провайдер не участвует в маршрутизации клиента. Вместо этого провайдер разворачивает службу виртуальной частной локальной сети (VPLS) для эмуляции сегмента локальной сети Ethernet с множественным доступом по сети MPLS.

ТЕХНОЛОГИИ VPN

Преимущество того или иного протокола VPN зависит от ряда факторов и условий использования:

Устройства — разные устройства поддерживают разные протоколы.

Сеть — если определенные сервисы не доступны в вашей локации, некоторые протоколы могут не подойти. Например, есть VPN Providers, которые работают в Китае, тогда как большинство существующих провайдеров заблокированы.



Производительность — некоторые протоколы обладают бОльшей производительностью, особенно на мобильных устройствах. Другие — более удобны для использования в больших сетях.

Модель угроз — некоторые протоколы менее безопасны, чем другие, поэтому и злоумышленники могут воздействовать на них по-разному.

ТЕХНОЛОГИИ VPN

Типы VPN соединений

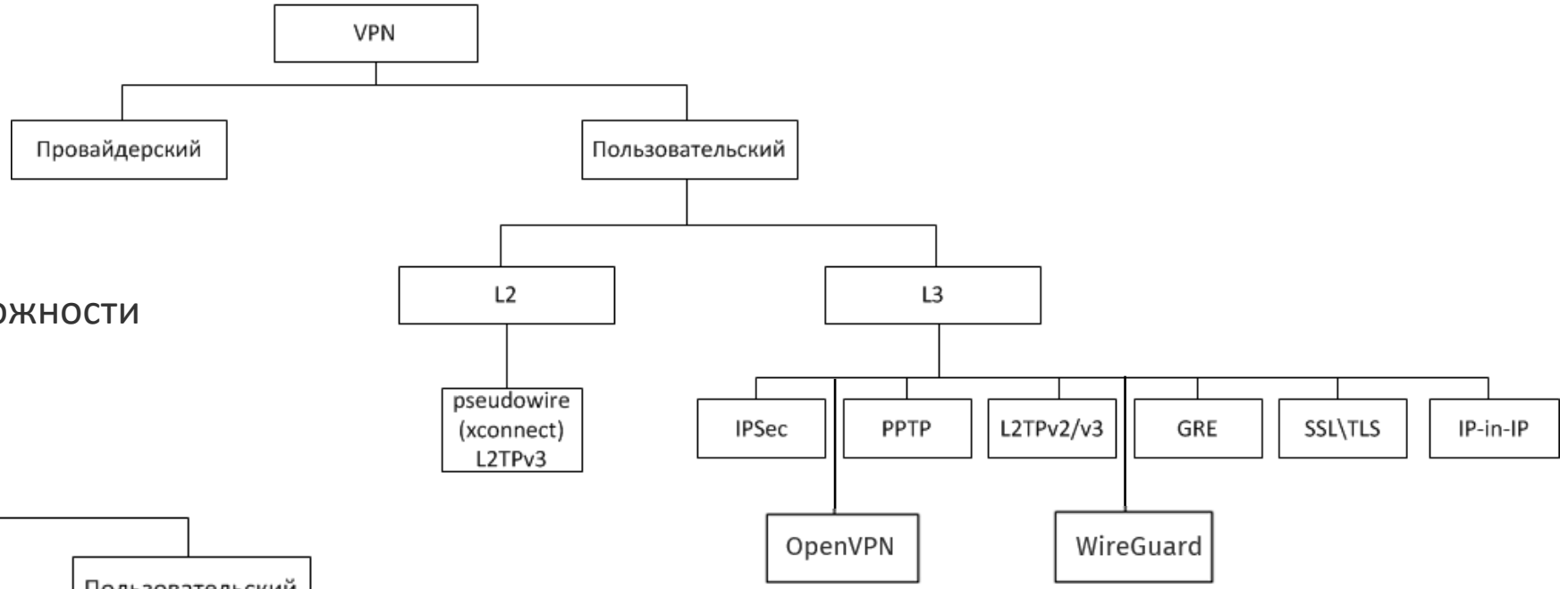
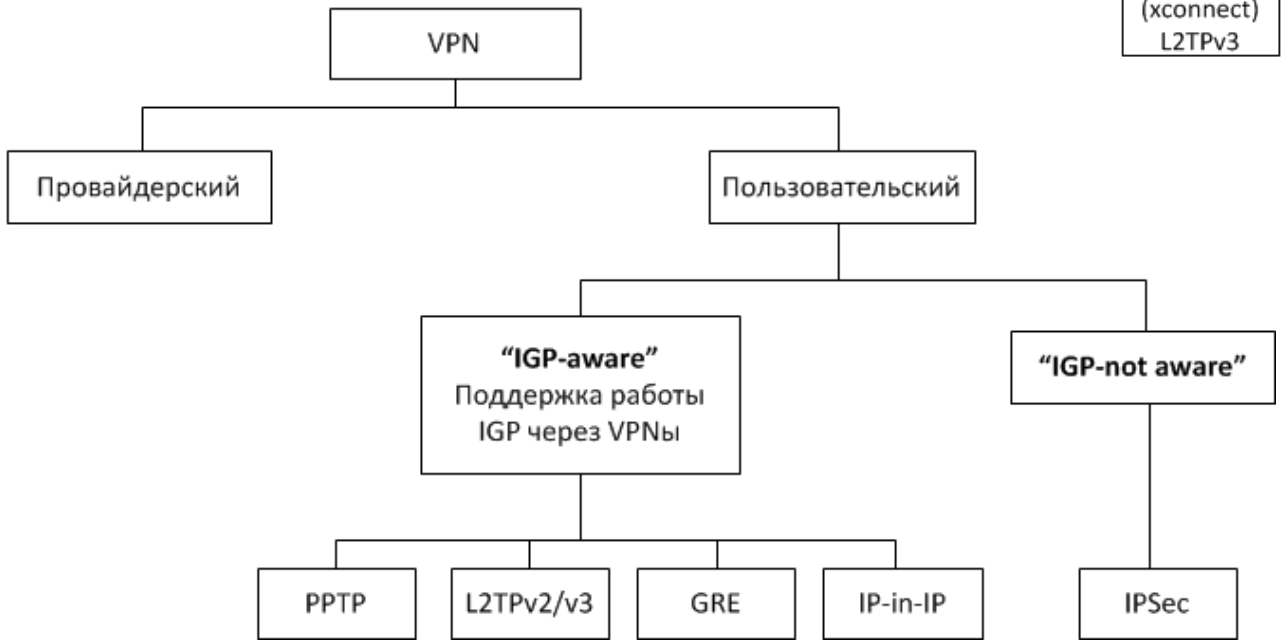
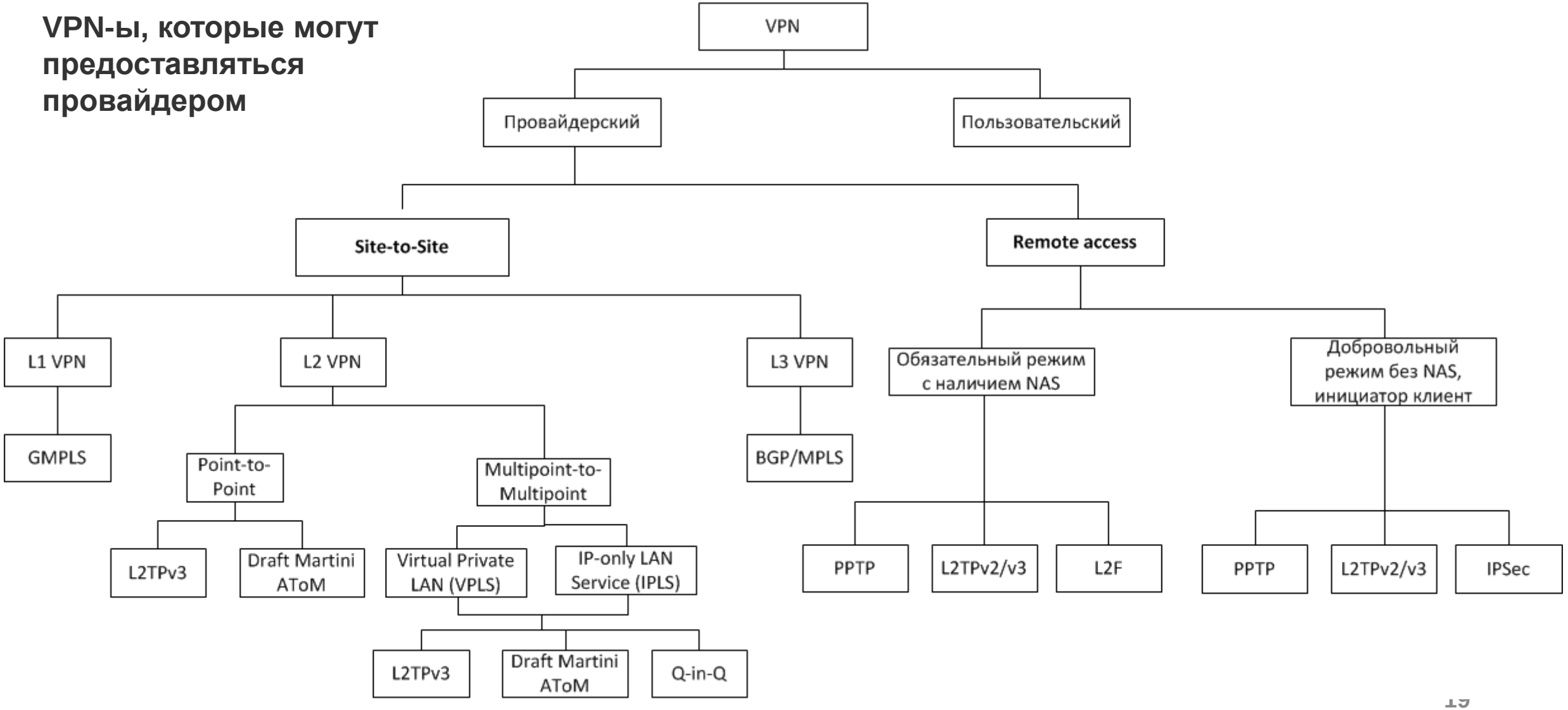


Схема VPN-ов относительно возможности пропуска мультикаста



ТЕХНОЛОГИИ VPN

VPN-ы, которые могут предоставляться провайдером

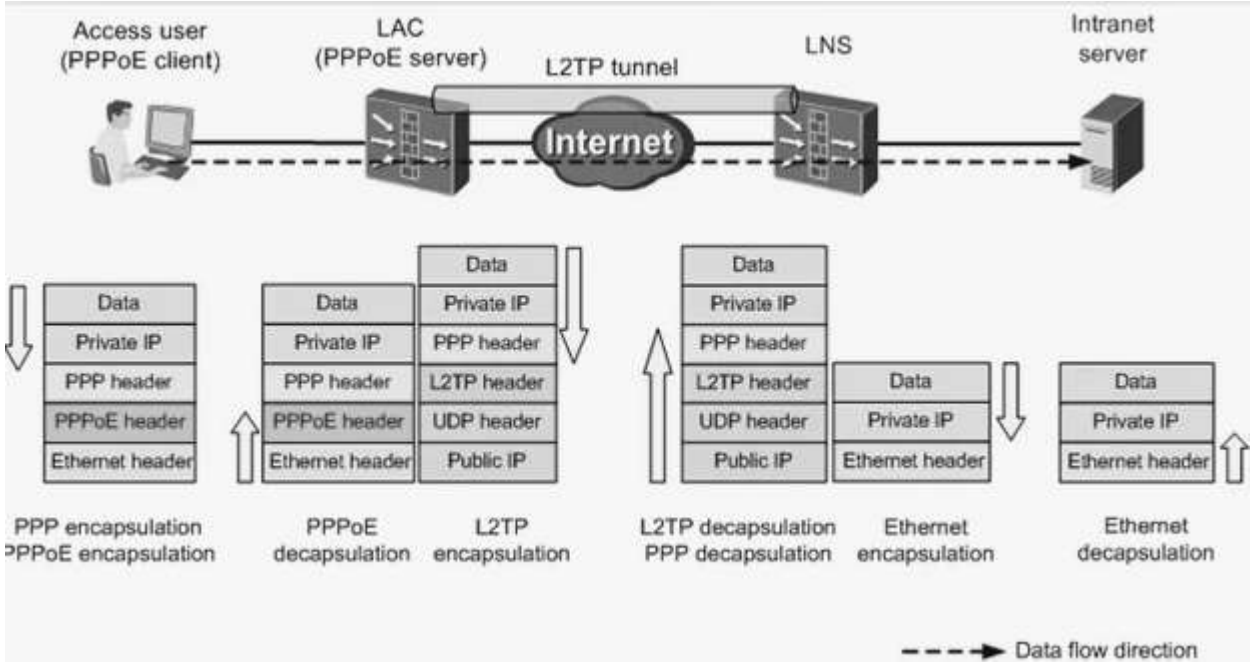


ТЕХНОЛОГИИ VPN

L2TP

L2TP — это протокол туннелирования уровня 2, который инкапсулирует пакеты данных между двумя точками сети. Он часто используется в сочетании с другим протоколом, например IPsec, для обеспечения шифрования и аутентификации. L2TP обычно используется в VPN для создания безопасного соединения между клиентом и VPN-сервером.

L2TP сам по себе не обеспечивает никакого шифрования или аутентификации. Для обеспечения безопасности и конфиденциальности L2TP должен полагаться на протокол шифрования для прохождения внутри туннеля. Обычно это делается с помощью IPsec, который обеспечивает шифрование и аутентификацию для туннеля L2TP.



ТЕХНОЛОГИИ VPN

OpenVPN

OpenVPN — это универсальный протокол VPN с открытым исходным кодом, разработанный компанией OpenVPN Technologies. На сегодняшний день это, пожалуй, самый популярный протокол VPN. Будучи открытым стандартом, он прошел не одну независимую экспертизу безопасности.

В большинстве ситуаций, когда нужно подключение через VPN, скорее всего подойдет OpenVPN. Он стабилен и предлагает хорошую скорость передачи данных. OpenVPN использует стандартные протоколы TCP и UDP и это позволяет ему стать альтернативой IPsec тогда, когда провайдер блокирует некоторые протоколы VPN.

Для работы OpenVPN нужно специальное клиентское программное обеспечение, а не то, которое работает из коробки. Большинство VPN-сервисов создают свои приложения для работы с OpenVPN, которые можно использовать в разных операционных системах и устройствах. Протокол может работать на любом из портов TCP и UPD и может использоваться на всех основных платформах через сторонние клиенты: Windows, Mac OS, Linux, Apple iOS, Android.

Недостатками OpenVPN являются отсутствие масштабируемости и зависимость от установки клиентского программного обеспечения. Еще одним недостатком является отсутствие графического интерфейса для настройки и управления. В частности, драйвер интерфейса tap для Microsoft Windows часто вызывал проблемы развертывания при выпуске новой версии Windows.

ТЕХНОЛОГИИ VPN

WireGuard

Самый новый протокол VPN — WireGuard. Позиционируется разработчиками как замена IPsec и OpenVPN для большинства случаев их использования, будучи при этом более безопасным, более производительным и простым в использовании.

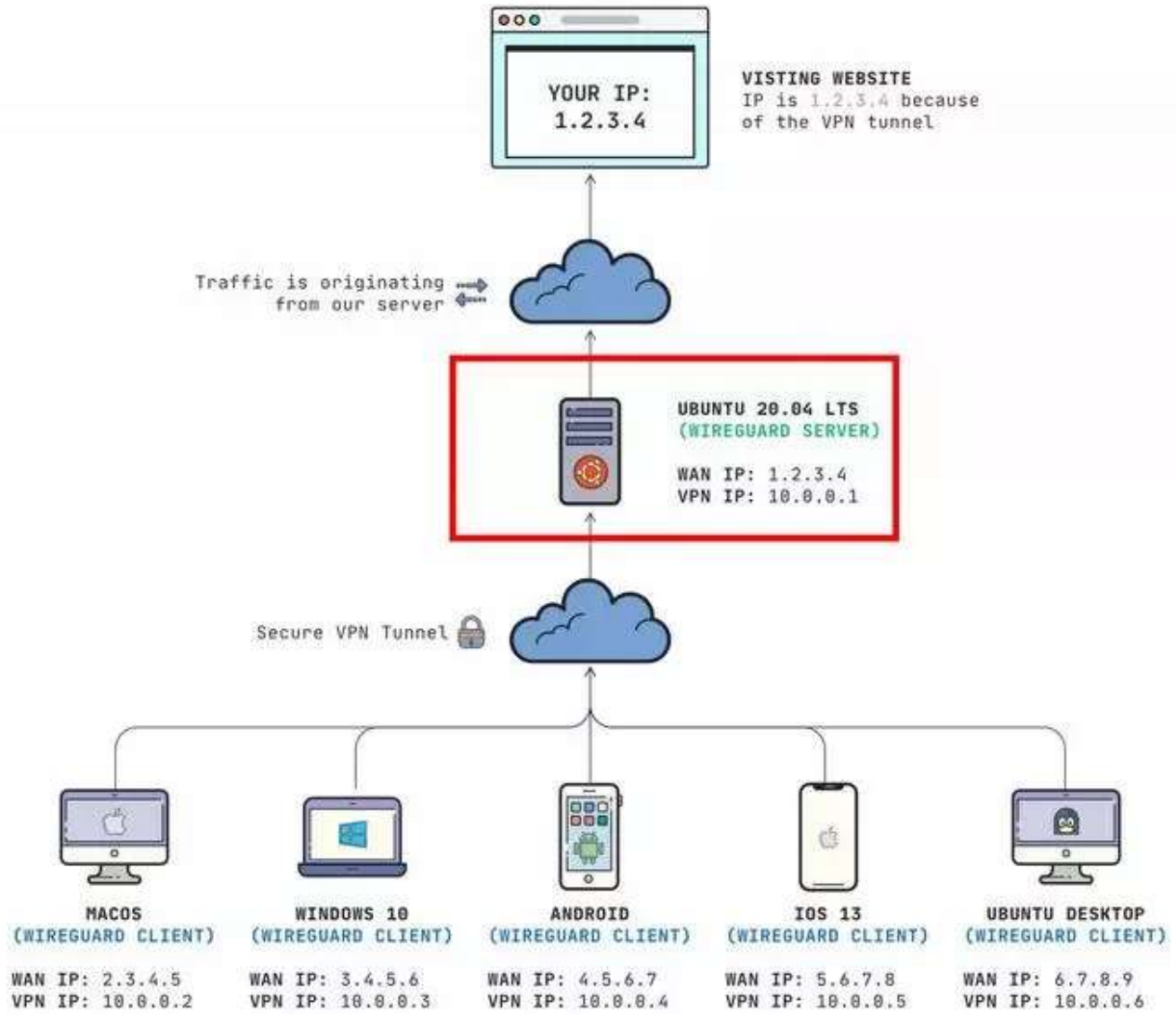
Все IP-пакеты, приходящие на WireGuard интерфейс, инкапсулируются в UDP и безопасно доставляются другим пирам. WireGuard использует современную криптографию:

- Curve25519 для обмена ключами,
- ChaCha20 для шифрования,
- Poly1305 для аутентификации данных,
- SipHash для ключей хеш-таблицы,
- BLAKE2 для хеширования.

Код WireGuard - 4 тысячи строк
код OpenVPN нескольких сотен тысяч.

https://www.wireguard.com/

ТЕХНОЛОГИИ VPN



ТЕХНОЛОГИИ VPN

	Компания-разработчик	Лицензия	Развертывание	Шифрование	Порты	Недостатки безопасности
PPTP	Microsoft	Proprietary	Windows, macOS, iOS, некоторое время GNU/Linux. Работает “из коробки”, не требуя установки дополнительного ПО	Использует Microsoft Point-to-Point Encryption (MPPE), который реализует RSA RC4 с максимум 128-битными сеансовыми ключами	TCP-порт 1723	Обладает серьезными уязвимостями. MSCHAP-v2 уязвим для атаки по словарю, а алгоритм RC4 подвергается атаке Bit-flipping
SSTP	Microsoft	Proprietary	Windows. Работает “из коробки”, не требуя установки дополнительного ПО	SSL (шифруются все части, кроме TCP- и SSL-заголовков)	TCP-порт 443	Серьезных недостатков безопасности не было выявлено
L2TP/IPsec	L2TP — совместная разработка Cisco и Microsoft, IPsec — The Internet Engineering Task Force	Proprietary	Windows,Mac OS X, Linux, iOS, Android. Многие ОС (включая Windows 2000/XP +, Mac OS 10.3+) имеют встроенную поддержку, нет необходимости ставить дополнительное ПО	3DES или AES	UDP-порт 500 для первонач. обмена ключами и UDP-порт 1701 для начальной конфигурации L2TP, UDP-порт 5500 для обхода NAT	3DES уязвим для Meet-in-the-middle и Sweet32, но AES не имеет известных уязвимостей. Однако есть мнение, что стандарт IPsec скомпрометирован АНБ США

ТЕХНОЛОГИИ VPN

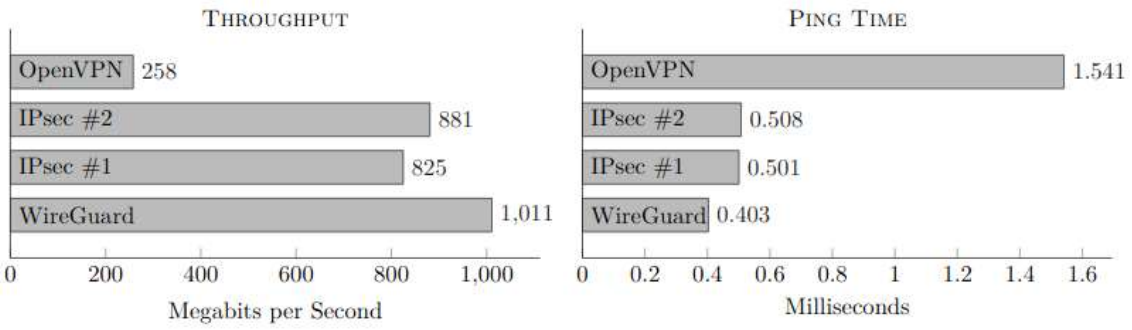
	Компания-разработчик	Лицензия	Развертывание	Шифрование	Порты	Недостатки безопасности
IKEv2/IPsec	IKEv2 — совместная разработка Cisco и Microsoft, IPsec — The Internet Engineering Task Force	Proprietary, но существуют реализации протокола с открытым исходным кодом	Windows 7+, macOS 10.11+ и большинство мобильных ОС имеют встроенную поддержку	Реализует большое количество криптографических алгоритмов, включая AES, Blowfish, Camellia	UDP-порт 500 для первоначального обмена ключами, а UDP-порт 4500 — для обхода NAT	Не удалось найти информации об имеющихся недостатках безопасности, кроме инцидента с утечкой докладов АНБ касательно IPsec
OpenVPN	OpenVPN Technologies	GNU GPL	Windows, Mac OS, GNU/Linux, Apple iOS, Android и маршрутизаторы. Необходима установка специализированного ПО, поддерживающего работу с данным протоколом	Использует библиотеку OpenSSL (реализует большинство популярных криптографических стандартов)	Любой UDP- или TCP-порт	Серьезных недостатков безопасности не было выявлено
WireGuard	Jason A. Donenfeld	GNU GPL	Windows, Mac OS, GNU/Linux, Apple iOS, Android. Установить сам WireGuard, а затем настроить по руководству	Обмен ключами по 1-RTT, Curve25519 для ECDH, RFC7539 для ChaCha20 и Poly1305 для аутентификационного шифрования, и BLAKE2s для хеширования	Любой UDP-порт	Серьезных недостатков безопасности не было выявлено

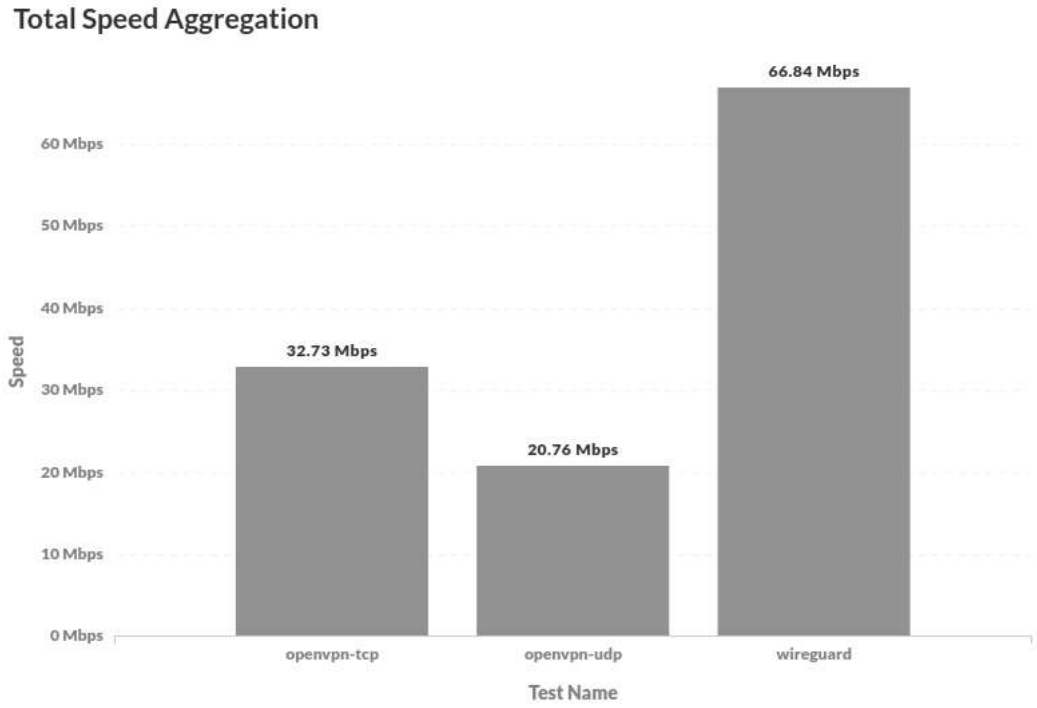
ТЕХНОЛОГИИ VPN

Сравнение производительности

Тесты на пропускную способность и время отклика ping.
Wireguard значительно превзошел OpenVPN, а заодно и две вариации IPSec-а. Во время теста на пропускную способность с использованием OpenVPN и IPSec утилизация CPU **достигала 100%**. В то же время использование Wireguard так сильно не загружало центральный процессор, давая тем самым возможность полностью утилизировать ресурсы сетевой карты Gigabit Ethernet.

Protocol	Configuration
WireGuard	256-bit ChaCha20, 128-bit Poly1305
IPsec #1	256-bit ChaCha20, 128-bit Poly1305
IPsec #2	256-bit AES, 128-bit GCM
OpenVPN	256-bit AES, HMAC-SHA2-256, UDP mode





https://blog.entrostat.com/openvpn-vs-wireguard-network-performance-tests/

ТЕХНОЛОГИИ VPN

Какой же VPN выбрать?
Есть огромное количество пользовательских сценариев использования VPN, и вряд ли одна и та же рекомендация будет хороша для всех. Соответственно, для разных сценариев можно выделить две группы с наиболее подходящим решением для VPN.

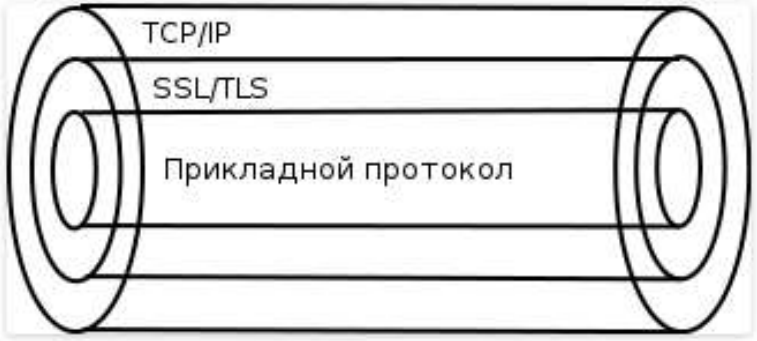
Wireguard
Если вы обычный пользователь;

- VPN вам нужен для обхода всяких нелепых ограничений РКН;
- скорость для вас имеет значение, например для файлообмена, или работы вашего приложения;

- OpenVPN
  Бизнес пользователи средней и крупной компании использующие VPN для удаленного доступа к внутренней сети;
- бизнес пользователи, предоставляющие удаленный доступ по VPN к ИТ ресурсам, содержащим конфиденциальные данные, или коммерческую тайну;
- все, кому нужно надежное и проверенное временем решение для VPN;

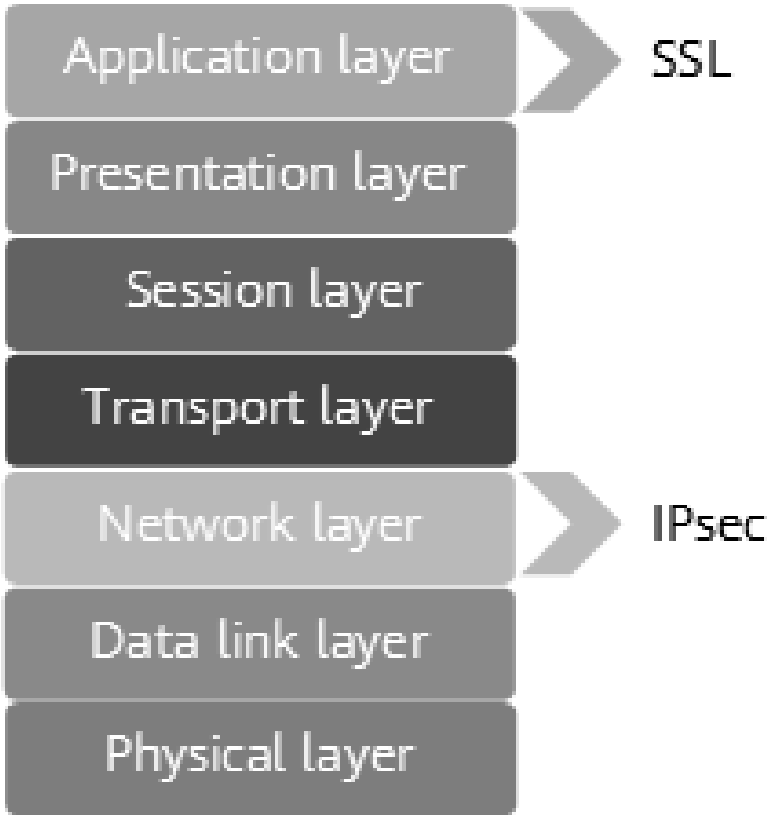
ТЕХНОЛОГИЯ SSL

SSL (*Secure Sockets Layer* — уровень защищённых сокетов) — криптографический протокол, который подразумевает безопасную связь. Он использует **а**симметричную криптографию для аутентификации ключей обмена, симметричное шифрование для сохранения конфиденциальности, коды аутентификации сообщений для целостности сообщений.



Прикладной протокол «заворачивается» в TLS/SSL, а тот в свою очередь в TCP/IP. Данные по прикладному протоколу передаются по TCP/IP, но они зашифрованы. И расшифровать передаваемые данные может только та машина, которая установила соединения. Для всех остальных, кто получит передаваемые пакеты, эта информация будет бессмысленной, если они не смогут ее расшифровать.

ТЕХНОЛОГИИ SSL

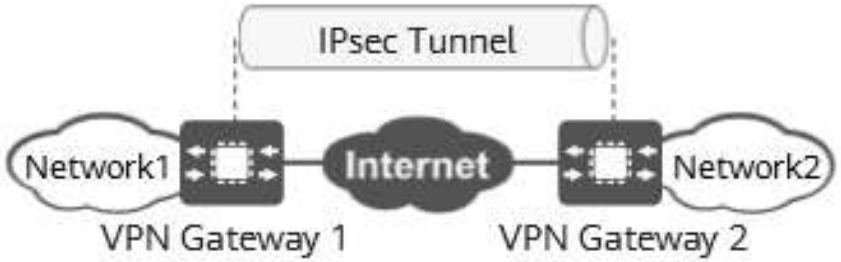


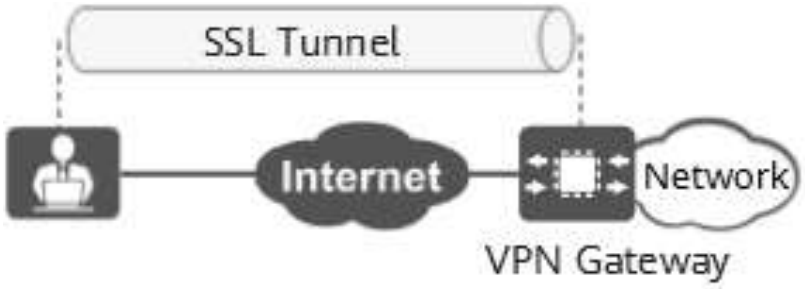
Рабочие уровни эталонной модели OSIOSI определяет семиуровневую структуру сетевого взаимодействия: физический уровень, уровень канала передачи данных, сетевой уровень, транспортный уровень, сеансовый уровень, уровень представления и уровень приложений. IPsec работает на сетевом уровне и напрямую работает через Интернет-протокол (IP). SSL , работающий на уровне приложений, представляет собой протокол прикладного уровня, который шифрует HTTP-трафик вместо IP-пакетов.

ТЕХНОЛОГИИ SSL

Конфигурация и развертывание

IPsec VPN применим к сетям типа «сеть-сеть». В этой сети VPN- шлюзы должны быть развернуты на каждом сайте, или удаленным пользователям необходимо установить выделенные VPN-клиенты. Поэтому настройка и развертывание сложны, а стоимость обслуживания высока. SSL VPN применим к сети клиент-сайт. В этой сети удаленным пользователям достаточно установить указанный плагин в стандартный браузер, поддерживающий SSL. VPN-шлюз развертывается в центре обработки данных для централизованного управления и обслуживания. Таким образом, конфигурация и развертывание просты, а стоимость обслуживания невелика.





ТЕХНОЛОГИИ SSL

Контроль доступа

IPsec работает на сетевом уровне и не может реализовать детальный контроль доступа на основе приложений. SSL VPN более гибок в детальном контроле доступа. Сетевые администраторы могут классифицировать сетевые ресурсы по различным типам в зависимости от типов приложений. Каждый тип ресурсов имеет разные права доступа.

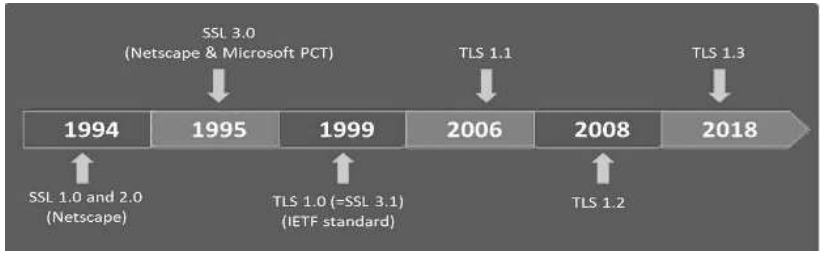
Ключевые отличия SSL и TLS

- *Аутентификация сообщений*: в TLS используется HMAC, работающий с любой хэш-функцией (а не только с MD5 или SHA, как в SSL).
- *Генерация ключа*: в TLS при создании ключа используется псевдослучайная функция стандарта HMAC; в SSL — RSA, Diffie-Hellman или Fortezza/DMS.
- *Проверка сертификата*: в SSL проверка требует передачи сложной последовательности сообщений; в TLS информация о проверке полностью передается в сообщениях во время handshake.
- *Методы шифрования*: SSL поддерживает только алгоритмы RSA, Diffie-Hellman и Fortezza/DMS. В TLS отказались от поддержки Fortezza/DMS, но возможно добавление новых методов шифрования в последующих версиях.

ТЕХНОЛОГИИ SSL

Особенности	IPSec	SSL
Аппаратная независимость	Да	Да
Код	Не требуется изменений для приложений. Может потребовать доступ к исходному коду стека TCP/IP.	Требуются изменения в приложениях. Могут потребоваться новые DLL или доступ к исходному коду приложений.
Защита	IP пакет целиком. Включает защиту для протоколов высших уровней.	Только уровень приложений.
Фильтрация пакетов	Основана на аутентифицированных заголовках, адресах отправителя и получателя, и т.п. Простая и дешёвая. Подходит для роутеров.	Основана на содержимом и семантике высокого уровня. Более интеллектуальная и более сложная.
Производительность	Меньшее число переключений контекста и перемещения данных.	Большее число переключений контекста и перемещения данных. Большие блоки данных могут ускорить криптографические операции и обеспечить лучшее сжатие.
Платформы	Любые системы, включая роутеры	В основном, конечные системы (клиенты/серверы), также firewalls.
Firewall/VPN	Весь трафик защищён.	Защищён только трафик уровня приложений. ICMP, RSVP, QoS и т.п. могут быть незащищены.
Прозрачность	Для пользователей и приложений.	Только для пользователей.
Текущий статус	Появляющийся стандарт.	Широко используется WWW браузерами, также используется некоторыми другими продуктами.

IETF официально прекратил поддержку протоколов TLS 1.0, 1.1, 1.2.

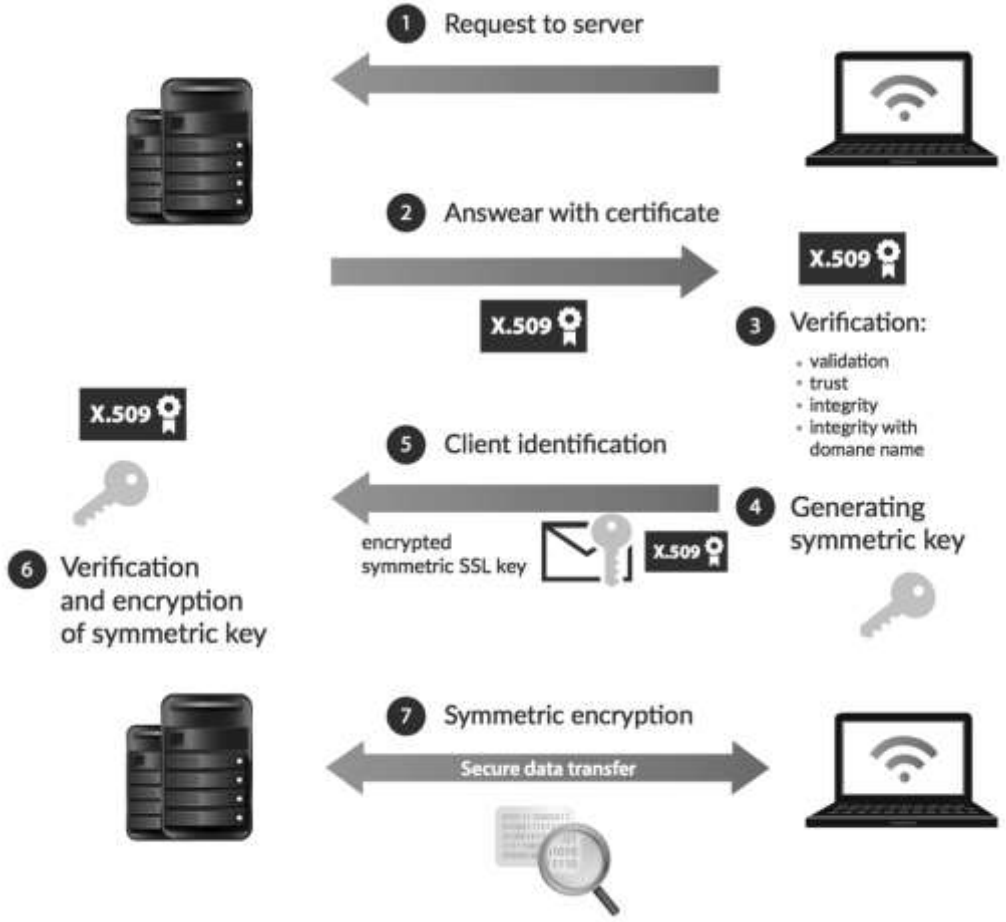


ТЕХНОЛОГИИ SSL

Сертификаты TLS стали результатом итераций сертификатов SSL и со временем их усовершенствовали. Конечная функция сертификатов SSL и TLS не изменилась.

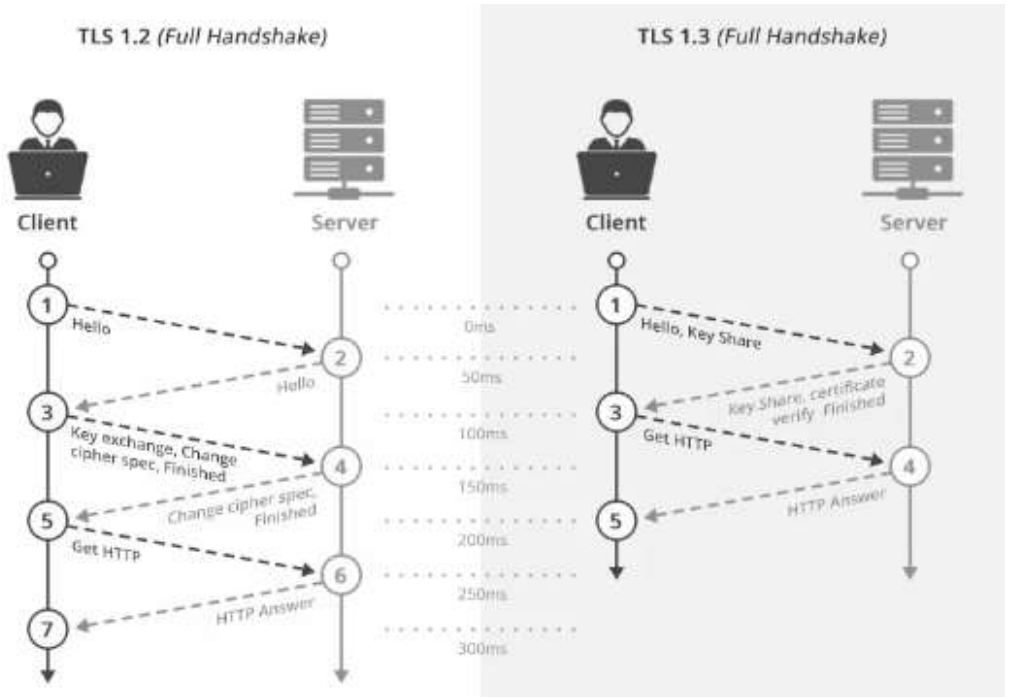
	SSL	TLS
Означает	SSL означает уровень защищенных сокетов.	TLS означает протокол безопасности транспортного уровня.
История версий	SSL теперь заменяется на TLS. SSL развивался до версий 1.0, 2.0 и 3.0.	TLS – это обновленная версия SSL. TLS развивался до версий 1.0, 1.1, 1.2 и 1.3.
Активность	Все версии SSL устарели.	Активно используются версии TLS 1.2 и 1.3.
Оповещения	В SSL есть только два типа оповещений. Оповещения не шифруются.	Оповещения TLS зашифрованы и более разнообразны.
Аутентификация сообщений	SSL использует MAC.	TLS использует HMAC.
Наборы шифров	SSL поддерживает старые алгоритмы с известными уязвимостями безопасности.	TLS использует современные алгоритмы шифрования.
Рукопожатие	Рукопожатие по протоколу SSL сложное и медленное.	Рукопожатие по протоколу TLS состоит из меньшего количества шагов и обеспечивает более быстрое соединение.

ТЕХНОЛОГИИ SSL



1. Браузер или сервер пытается подключиться к веб-сайту (веб-серверу), защищенному с помощью SSL.
2. Браузер или сервер запрашивает идентификацию у веб-сервера.
3. В ответ веб-сервер отправляет браузеру или серверу копию своего SSL-сертификата.
4. Браузер или сервер проверяет, является ли этот SSL-сертификат доверенным. Если это так, он сообщает об этом веб-серверу.
5. Затем веб-сервер возвращает подтверждение с цифровой подписью и начинает сеанс, зашифрованный с использованием SSL.
6. Зашифрованные данные используются совместно браузером или сервером и веб-сервером.

ТЕХНОЛОГИИ SSL



№	TLS 1.2	TLS 1.3
1.	В TLS версии 1.2 многие сообщения перемещаются туда-сюда между клиентом и сервером.	В то время как TLS версии 1.3 направлен на сокращение времени, затрачиваемого на процесс рукопожатия, за счет сокращения количества сообщений между клиентом и сервером.
2.	TLS версии 1.2 имеет более медленное рукопожатие TLS	While; TLS версии 1.3 имеет более быстрое рукопожатие TLS
3.	У него более сложное рукопожатие.	While; у него более простое рукопожатие.
4.	Версия TLS 1.2 имеет менее безопасные наборы шифров.	While; TLS версии 1.3 имеет более безопасные наборы шифров.
5.	Его время прохождения туда-обратно не равно нулю.	While; его время прохождения туда и обратно равно нулю.
6.	Типичное рукопожатие в TLS версии 1.2 включает обмен от 5 до 7 пакетов.	While; в TLS версии 1.3 типичное рукопожатие включает обмен от 0 до 3 пакетов.
7.	У него более медленное и менее отзывчивое соединение.	While; у него более быстрое и отзывчивое соединение.
8.	TLS версии 1.2 не уменьшает размер наборов шифров.	В то время как TLS версии 1.3 уменьшает размер наборов шифров.
9.	Сравнительно низкая производительность сайта и пользовательский опыт.	While; он предлагает лучшую производительность веб-сайта и пользовательский опыт.

ТЕХНОЛОГИИ SSL

Когда клиент обращается к сайту, то запрашивает его сертификат и проверяет следующие данные:

•Кем был выдан сертификат.

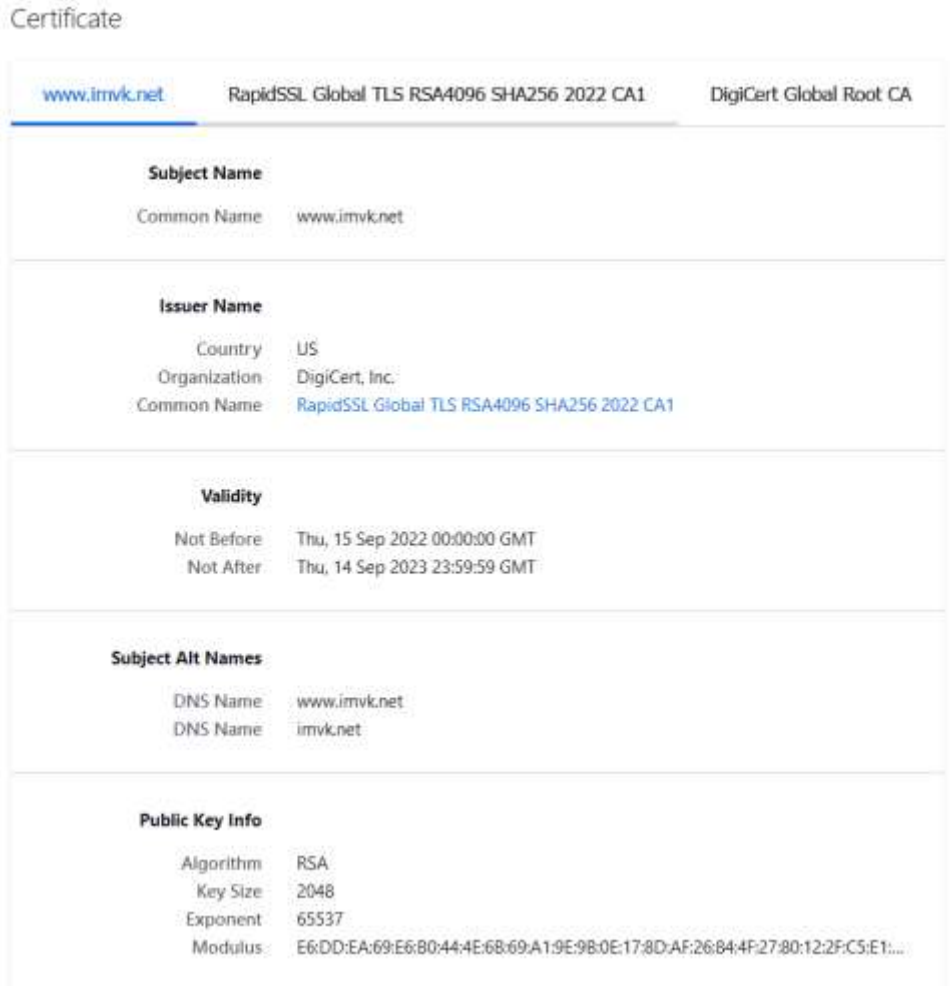
Современные браузеры поставляются с некоторыми предустановленными сертификатами и содержат список доверенных организаций и центров сертификации.

•Срок действия сертификата.

•Доменное имя сайта.

•Цифровая подпись.

•Был ли отозван сертификат. Иногда по тем или иным причинам центр сертификации может отозвать сертификат и сделать его недействительным.



ТЕХНОЛОГИИ SSL

SSL сертификаты

Цифровые сертификаты (стандарт X.509)

- Удобный способ показать, что кто-то владеет публичным ключом.
- Выпускаются центрами сертификации (**Certificate Authority, CA**): GlobalSign, Comodo и др.
- PKI (public key infrastructure) — механизм, регулирующий распространение и использование сертификатов (включая создание, отзыв и проверку подлинности).
- Список доверенных CA поддерживается приложением (у браузеров свои списки).
- Сертификаты подписываются другими сертификатами, что повышает надежность.
- Сертификат может быть отозван. Система поддерживает список таких сертификатов (**Certificate Revocation List, CRL**). На стороне CA список обновляется каждые несколько часов.

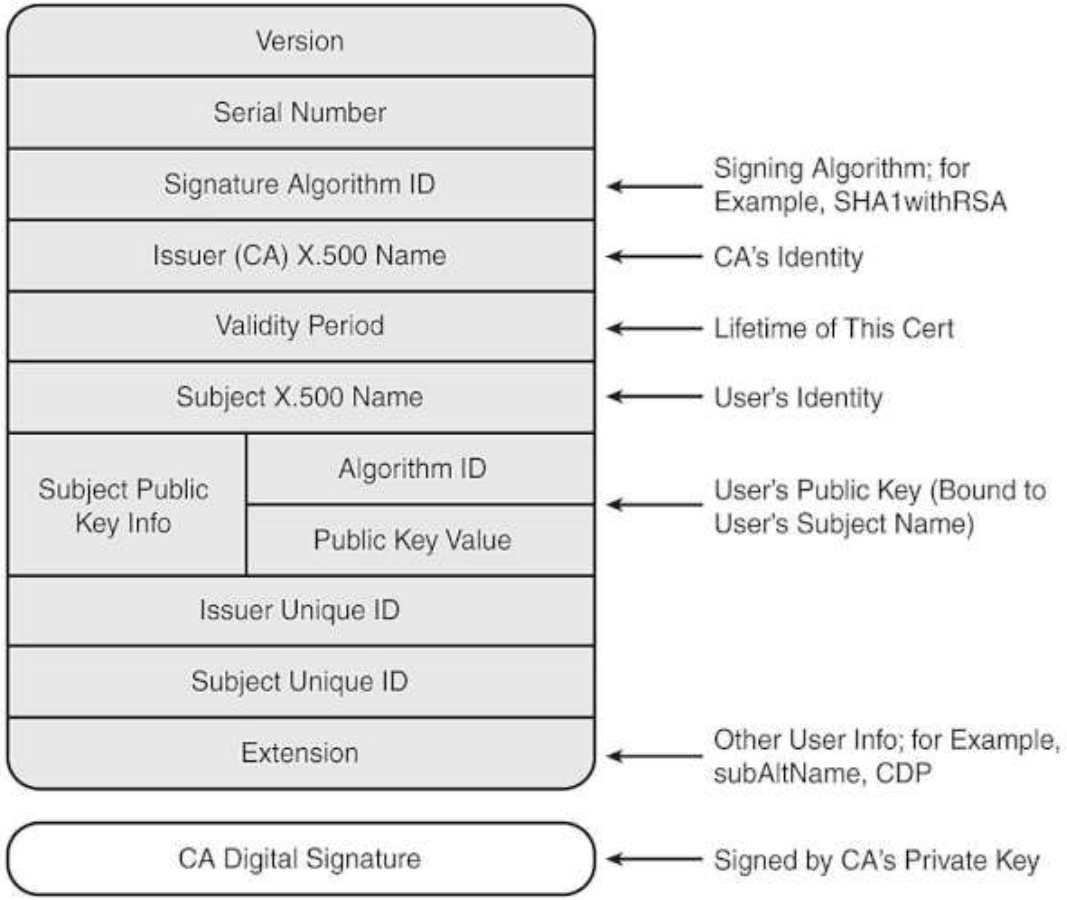
Получение сертификата

1. Пользователь генерирует ключ и посылает запрос серверу CA.
2. CA отвечает сообщением со своим сертификатом.
3. Пользователь собирает данные, необходимые для выдачи сертификата (email, отпечаток ключа и т.д.).
4. Пользователь отправляет данные в CA, зашифровав их публичным ключом CA.
5. CA проверяет полученные данные и отправляет сертификат пользователю.

ТЕХНОЛОГИИ SSL

Структура сертификата

- Собственно сертификат
  - Версия
  - Серийный номер
  - Эмитент (тот, кто выпустил сертификат)
  - Субъект
  - Публичный ключ субъекта
  - Период действия
  - Дополнительные поля
- Алгоритм подписи сертификата
- Значение подписи сертификата



ТЕХНОЛОГИИ SSL

Виды возможных атак

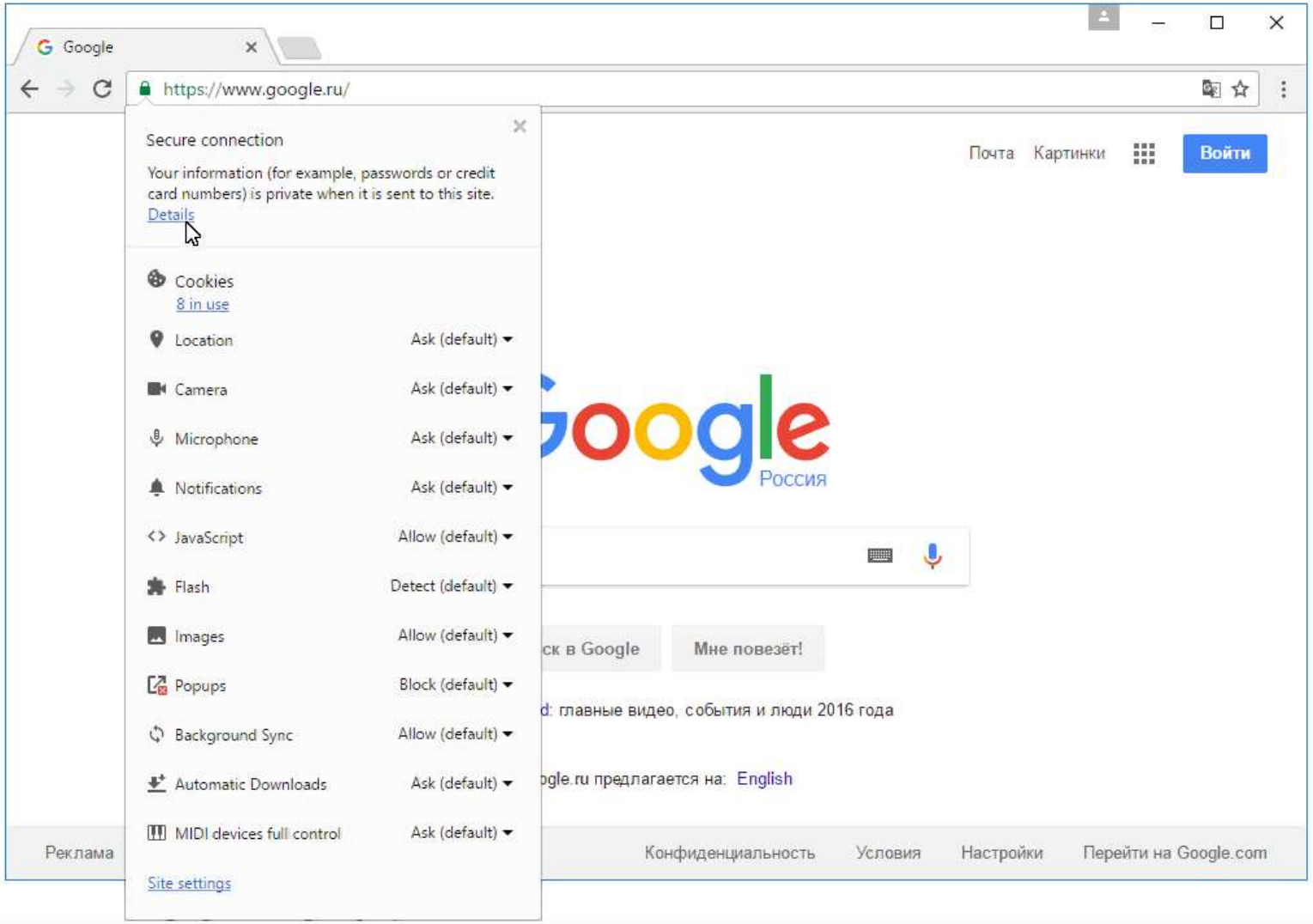
- Атака по словарю
- Атака отражением
- Атака протокола рукопожатия
- Взлом SSL-соединений внутри ЦОД
- BEAST атака
- Раскрытие шифров
- Атака «злоумышленник посередине»
- THC-SSL-DOS
- SSLstrip

Меры безопасности в TLS

- Защита от downgrade-атаки — понижения версии протокола к предыдущей (менее защищённой) версии или менее надёжному алгоритму шифрования;
- Нумерация последовательных записей приложения и использование порядкового номера в коде аутентификации сообщения (MAC);
- Использование ключа в идентификаторе сообщения (только владелец ключа может сгенерировать код аутентификации сообщения).
- Сообщение, которым заканчивается подтверждение связи («Finished»), содержит хэш всех handshake-сообщений, отправленных обеими сторонами, что позволяет проверить подлинность выбранных параметров TLS-соединения.
- Псевдослучайная функция делит подаваемые ей на вход данные пополам, применяет к половинкам разные хэш-алгоритмы (MD5 и SHA-1), а затем XOR'ит результаты для получения MAC. Это повышает безопасность в случае, если в одном из алгоритмов обнаружится уязвимость.

ТЕХНОЛОГИИ SSL

Как посмотреть характеристики сертификата



ТЕХНОЛОГИИ SSL

Номенклатура сертификатов

Какие сертификаты X.509 встречаются, если рассматривать их по расположению в цепочке доверия.

- **Корневые сертификаты** — изготовлены в корневом УЦ (удостоверяющий центр) и имеют следующие признаки: атрибуты issue и subject идентичны, а в расширении basicConstraints атрибут CA принимает значение TRUE.
- **Промежуточные сертификаты** — расплывчатый термин, обозначающий сертификаты не подписанные корневым УЦ, которые могут формировать цепочку произвольной длины, начиная от *корневого сертификата* и заканчивая *сертификатом конечного субъекта*.
- **Сертификаты конечного субъекта** — конечные сертификаты в цепочке, которые не могут подписывать другие *промежуточные сертификаты* своим закрытым ключом.

По степени дороговизны и надежности сертификаты делятся на 3 вида: **DV**, **OV** и **EV**.

ТЕХНОЛОГИИ SSL

Откуда берутся сертификаты?

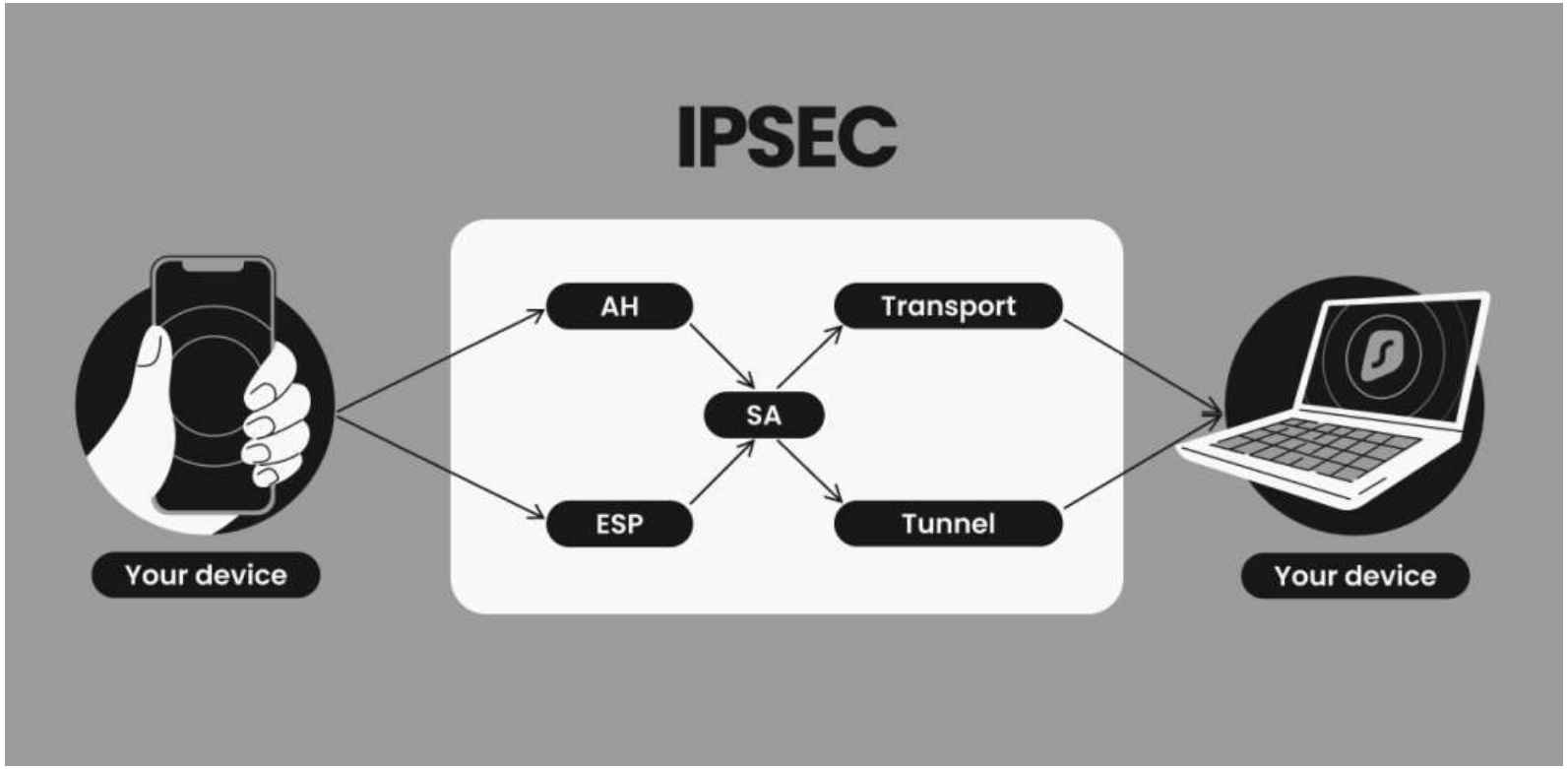
2 основных способа заполучить X.509 сертификат + третий путь.

1. Создать свой собственный сертификат и самому же его подписать. Плюсы — это бесплатно, минусы — сертификат будет принят лишь вами и, в лучшем случае, вашей организацией.
2. Приобрести сертификат в УЦ. Это будет стоить денег в зависимости от различных его характеристик и возможностей, указанных выше.
3. Получить бесплатный сертификат LetsEncrypt, доступны только самые простые **DV** сертификаты.

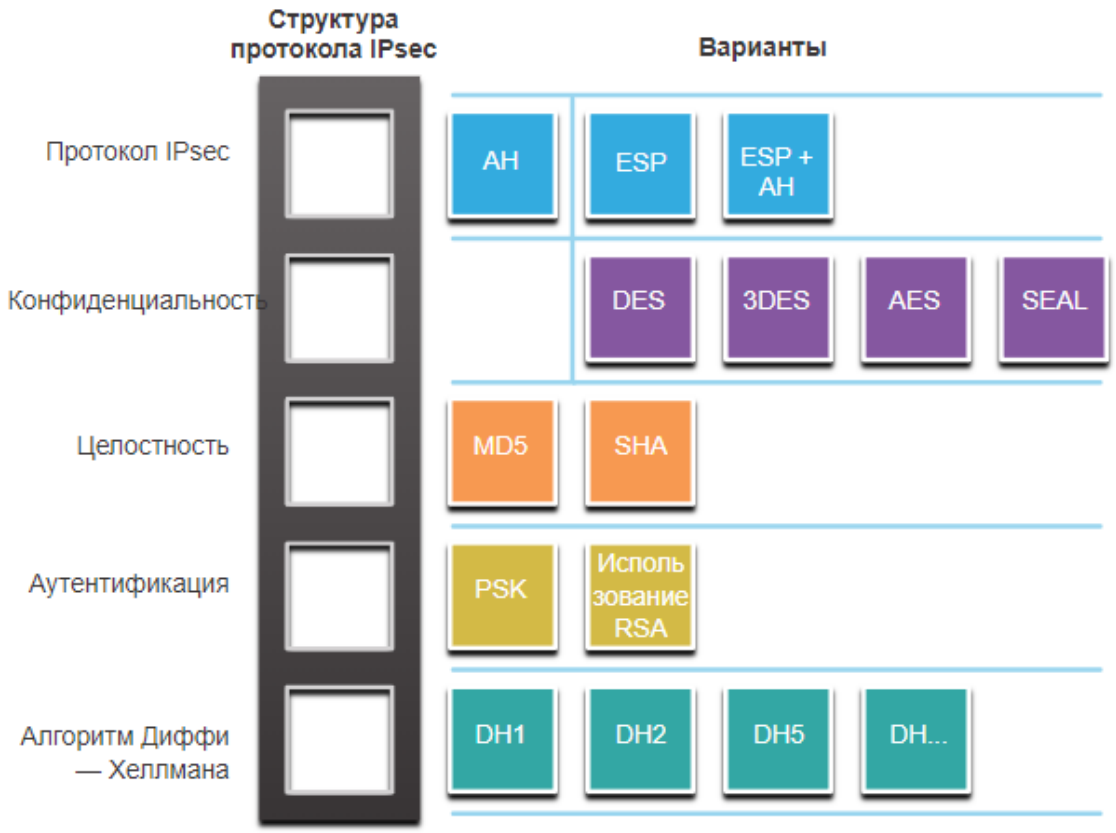
Let’s Encrypt — центр сертификации, предоставляющий бесплатные криптографические сертификаты X.509 для шифрования передаваемых через интернет данных HTTPS и других протоколов, используемых серверами в Интернете. Процесс выдачи сертификатов полностью автоматизирован

ТЕХНОЛОГИИ IPSEC

IPsec - это стандарт IETF (RFC 2401-2412), который определяет, как можно защитить VPN в IP-сетях. IPsec защищает и аутентифицирует IP-пакеты между источником и местом назначения. IPsec может защитить трафик от уровня 4 до уровня 7.



ТЕХНОЛОГИИ IPSEC



Благодаря структуре IPsec данный протокол выполняет следующие основные функции обеспечения 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. Методы аутентификации включают использование общих ключей (паролей), цифровых сертификатов или сертификатов RSA.
- **Диффи-Хеллман** - безопасный обмен ключами обычно различных групп алгоритма DH.

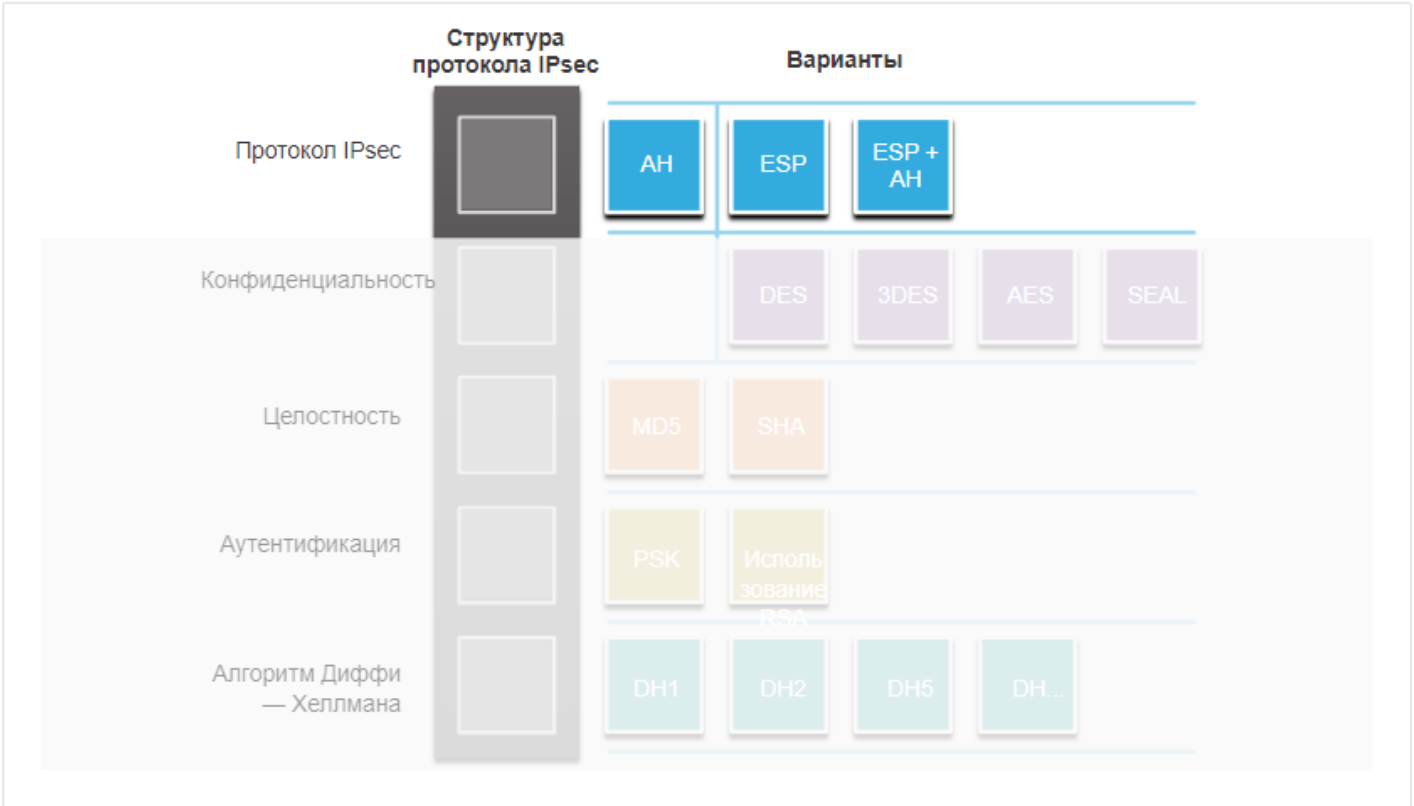
IKE — Самый центровой протокол в IPsec Framework это IKE (Internet Key Exchange). Остальные протоколы работают под его управлением;

ТЕХНОЛОГИИ IPSEC

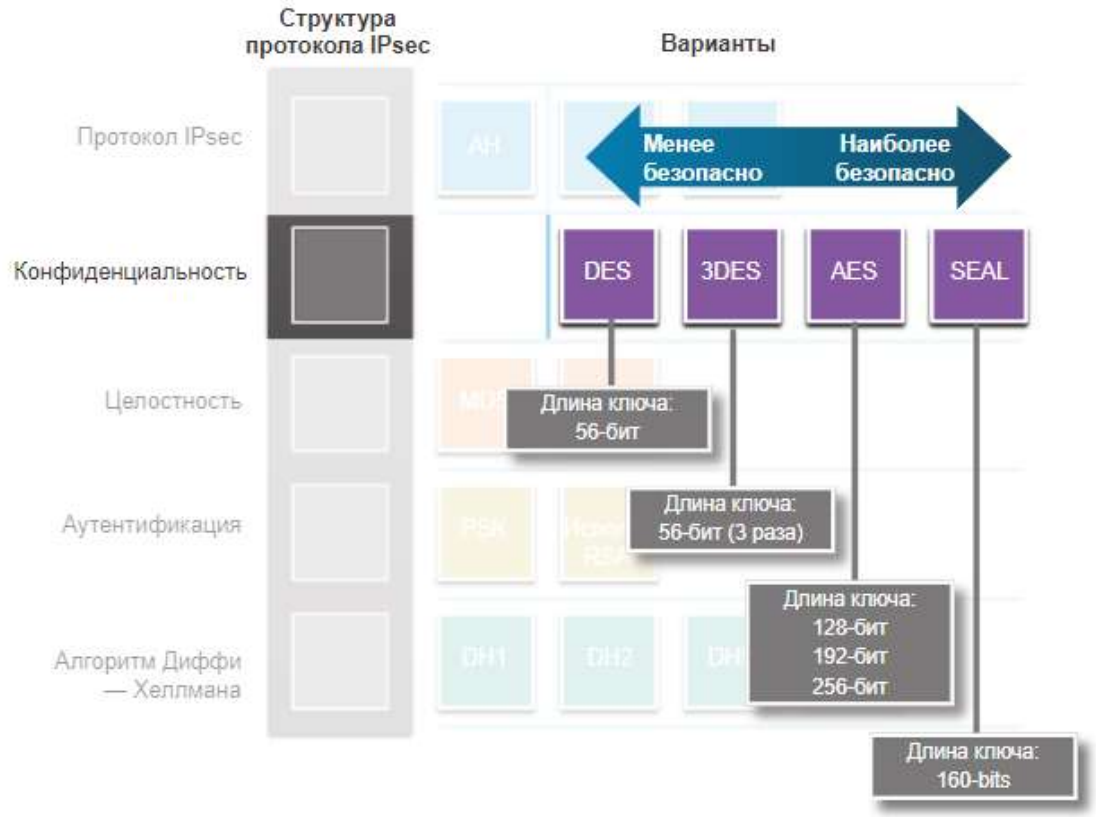
Функция IPSec	Описание
Протокол IPsec	Выбор протокола IPsec включает в себя Authentication Header (AH) или Encapsulation Security Protocol (ESP). AH аутентифицирует пакеты уровня 3 уровня. ESP шифрует пакет уровня 3. Примечание: ESP+AH редко используется, так как эта комбинация не будет успешно проходить через устройство NAT.
Конфиденциальность	Шифрование обеспечивает конфиденциальность пакета уровня 3. Варианты включают в себя Data Encryption Standard (DES), Triple DES (3DES), Advanced Encryption Standard (AES), или Software-Optimized Encryption Algorithm SEAL Доступна опция без шифрования.
Целостность	Гарантирует, что данные поступают в пункт назначения без изменений с использованием алгоритма хеширования, такого как, Message Digest 5 (MD5) или Secure Hash Algorithm (SHA).
Аутентификация	IPsec использует Internet Key Exchange (IKE) для аутентифкации пользовательских устройств которые могут независимо устанавливать связь. IKE использует несколько типов аутентификации, включая логин и пароль, одноразовый пароль, биометрические данные, предустановленные ключи (PSK) и цифровые сертификаты с использованием алгоритма RSA.
Алгоритм Диффи — Хеллмана	IPSec использует алгоритм DH для предоставления метода обмена публичного ключа между двумя участниками для установления общего секретного ключа. Существует несколько различный групп на выбор от DH 14, 15, 16 и DH 19, 20, 21 и 24. DH1, 2 и 5 сейчас не рекомендуются к использованию.

ТЕХНОЛОГИИ 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 доступны.

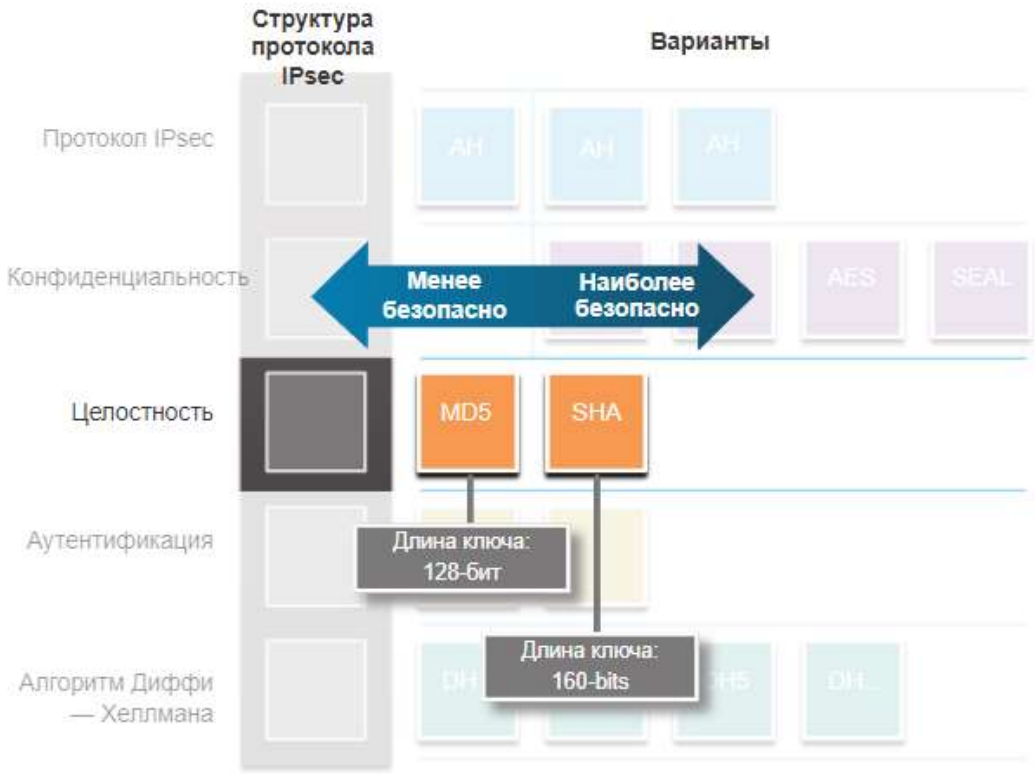


ТЕХНОЛОГИИ IPSEC



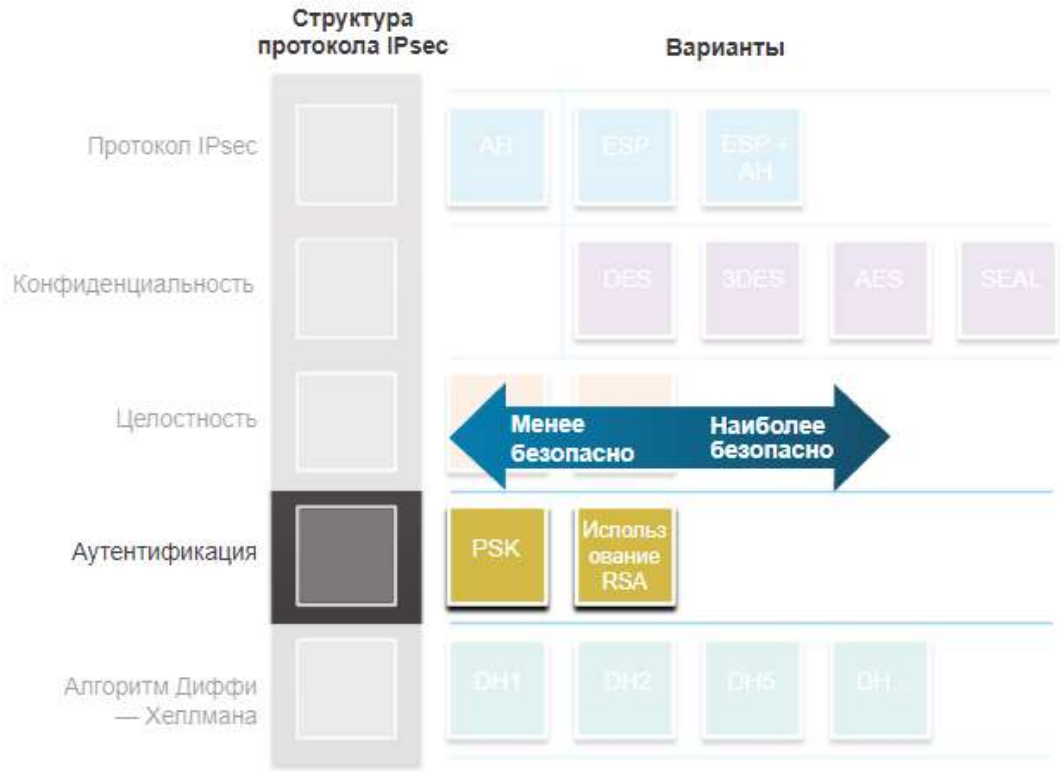
- DES использует 56-битный ключ.
- 3DES - это вариант 56-битного DES. Он использует три независимых 56-битных ключа шифрования на 64-битный блок, что обеспечивает более надежную защиту по сравнению с DES.
- AES обеспечивает более высокую безопасность, чем DES, и вычислительно более эффективен, чем 3DES. 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.

ТЕХНОЛОГИИ IPSEC



- Message-Digest 5 (MD5) использует 128-битный общий секретный ключ. Сообщение произвольной длины и 128-битовый общий секретный ключ объединяются друг с другом и обрабатываются алгоритмом хеширования HMAC-MD5. В результате создаётся 128-битовый хеш-код.
- Secure Hash Algorithm (SHA) использует 160-битный секретный ключ. Сообщение переменной длины и 160-битный общий секретный ключ объединяются и выполняются по алгоритму HMAC-SHA-1. В результате создаётся 160-битовый хеш-код.

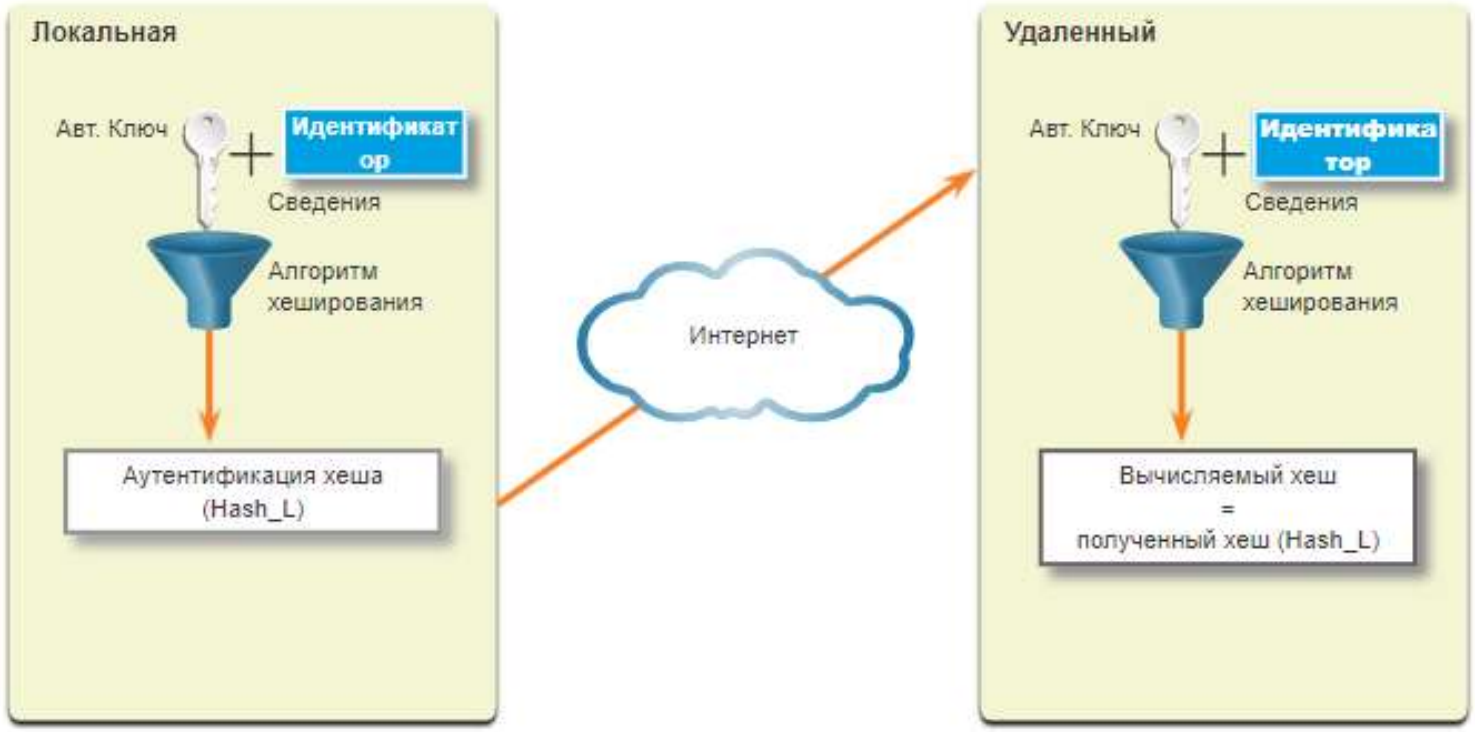
ТЕХНОЛОГИИ IPSEC



- Значение общего секретного ключа (PSK) вводится в каждый узел вручную. PSK объединяется с другой информацией для формирования ключа аутентификации. PSK легко настраиваются вручную, но они плохо масштабируются, потому что каждый узел IPsec должен быть настроен с PSK каждого другого узла, с которым он связывается.
- Аутентификация Rivest, Shamir и Adleman (RSA) использует цифровые сертификаты для аутентификации партнеров. Локальное устройство создаёт хеш-код и шифрует его с помощью своего закрытого ключа. Зашифрованный хеш прикрепляется к сообщению и пересылается на удаленный конец и действует как подпись. На удалённой стороне зашифрованный хеш-код расшифровывается с помощью открытого ключа локальной стороны. Если расшифрованный хеш-код совпадает с расчётным значением, это означает, что подпись является подлинной. Каждый узел должен подтвердить подлинность своего противоположного узла, прежде чем туннель будет считаться безопасным.

ТЕХНОЛОГИИ IPSEC

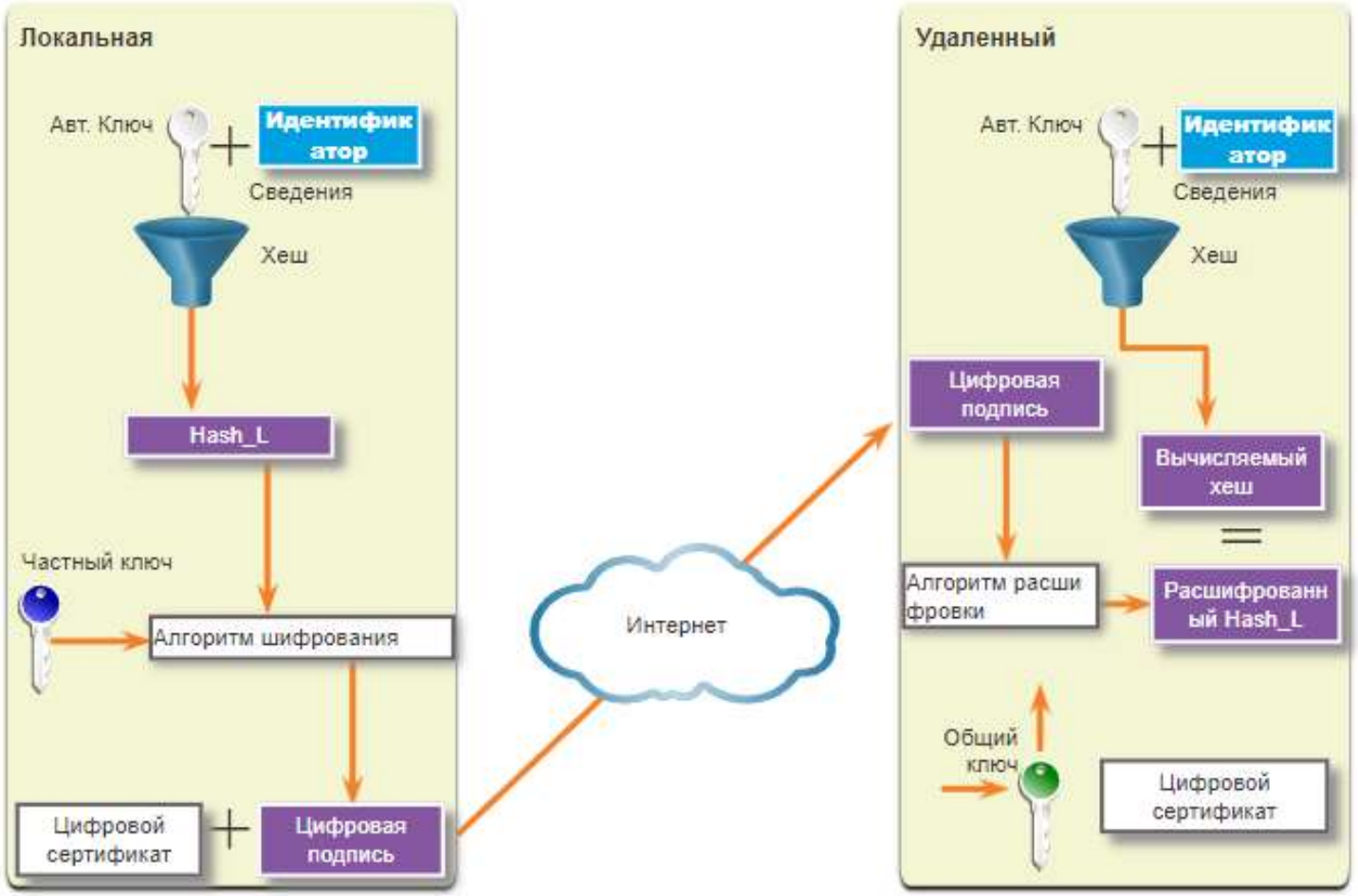
PSK Authentication



На локальном устройстве ключ аутентификации и идентификационная информация отправляются с помощью алгоритма хеширования, чтобы сформировать хеш для локального узла (Hash_L). Затем Hash_L шифруется с использованием личного ключа шифрования локального устройства. Это создает цифровую подпись. Цифровая подпись и цифровой сертификат пересылаются на удаленное устройство. Открытый ключ шифрования для расшифровки подписи включен в цифровой сертификат.

ТЕХНОЛОГИИ IPSEC

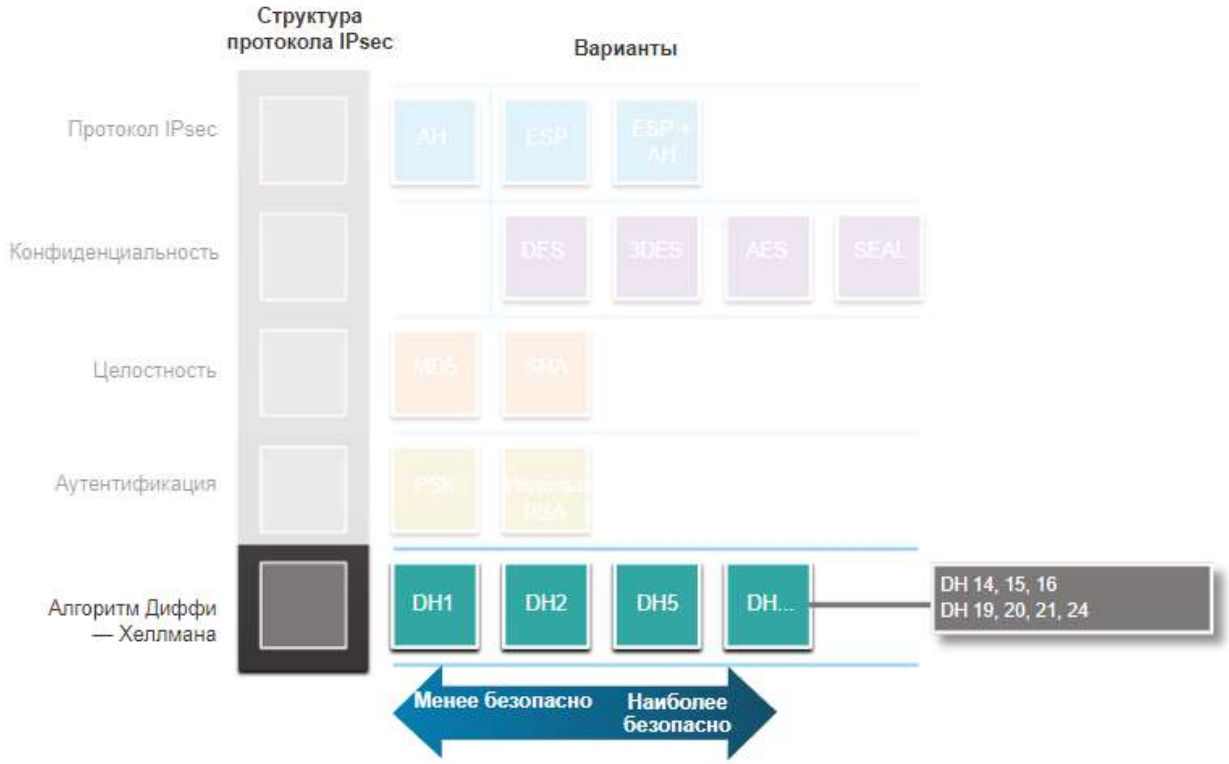
RSA Authentication



ТЕХНОЛОГИИ IPSEC

DH предоставляет возможность двум партнерам установить общий секретный ключ, который знают только они, даже если они обмениваются данными по небезопасному каналу. Варианты обмена ключами DH указаны как группы DH:

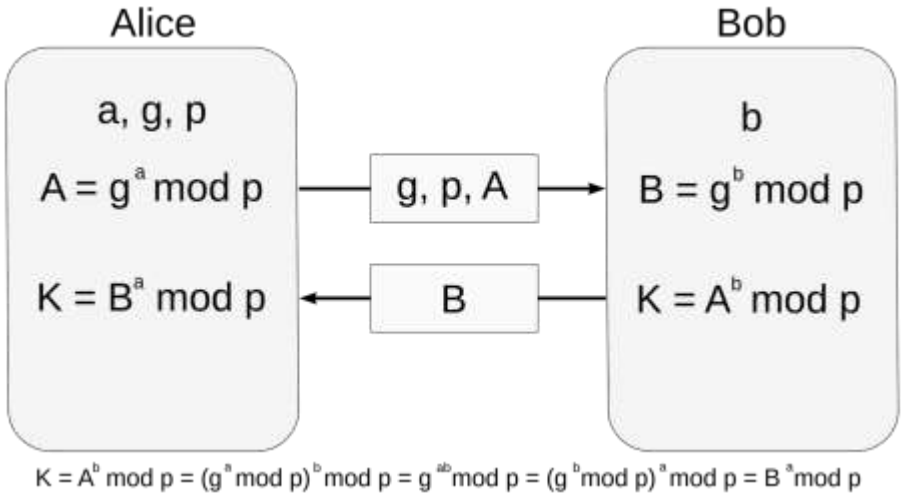
- группы DH 1, 2 и 5 больше не должны использоваться. Эти группы поддерживают размер ключа 768 бит, 1024 бит и 1536 бит соответственно.
- Группы DH 14, 15 и 16 используют ключи больших размеров с 2048 битами, 3072 битами и 4096 битами соответственно и рекомендуются для использования до 2030 года.
- Группы 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. DH группа 24 является предпочтительным шифрованием следующего поколения.

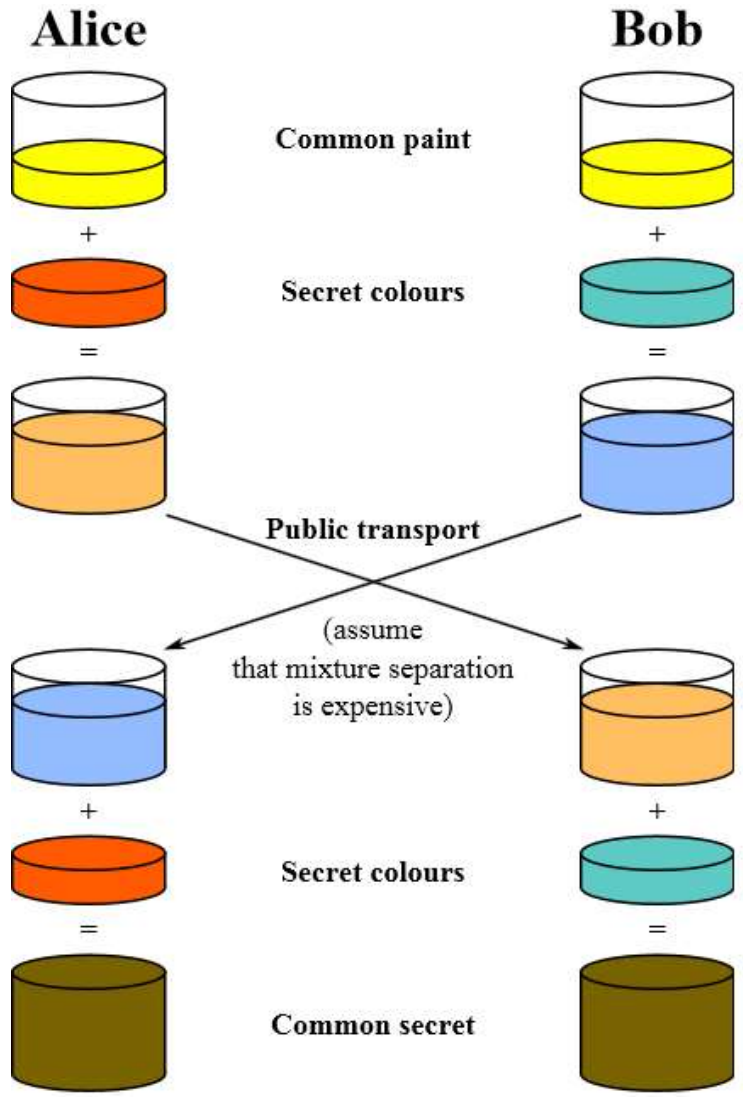


ТЕХНОЛОГИИ IPSEC

Алгоритм Диффи-Хеллмана используется для того, чтобы две стороны могли создать общий **секретный ключ**, его еще называют *«транспортный ключ»*, который затем используется для *шифрования* и *дешифрования* сообщений.

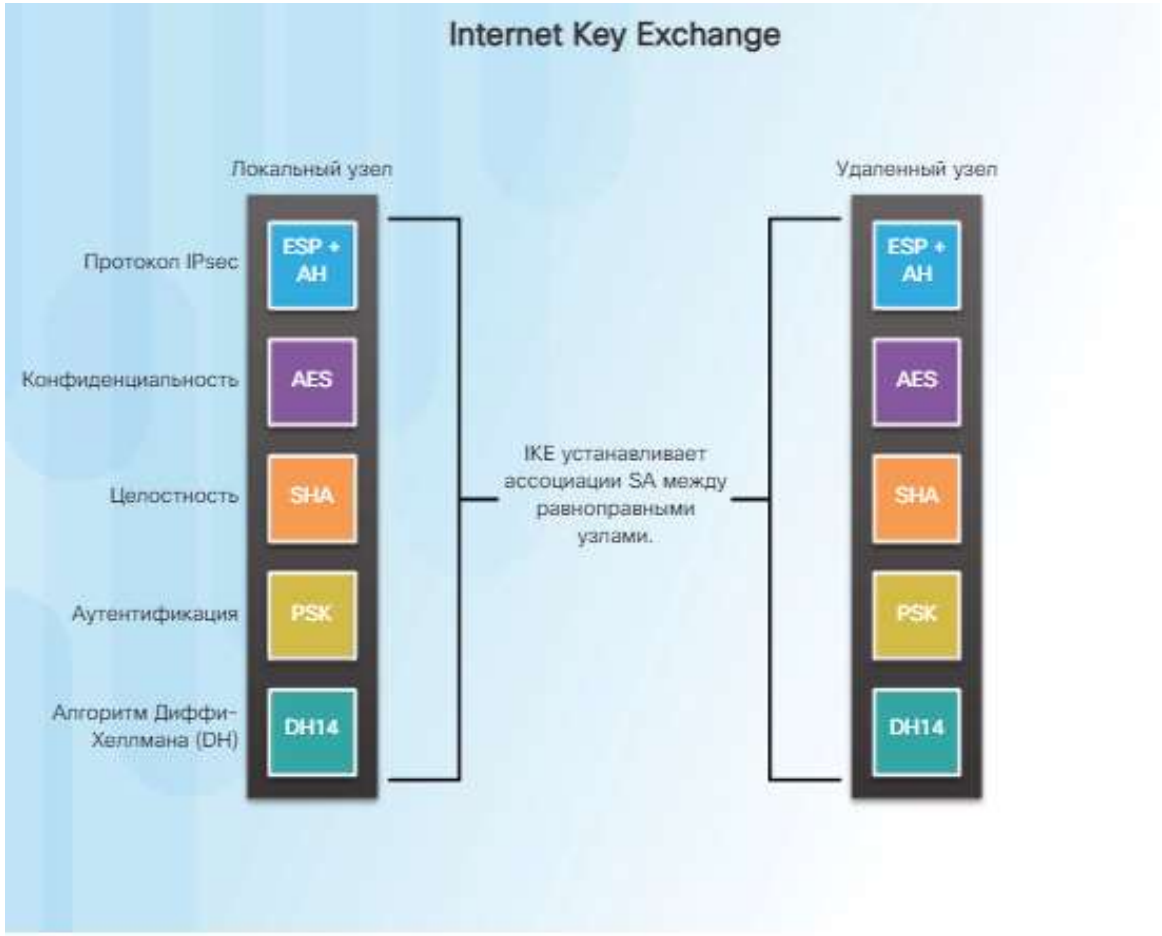
Самое главное - этот ключ создается без прямого обмена им между сторонами.
Принцип работы алгоритм основан на принципе *"сложности вычисления дискретного логарифма"*.





ТЕХНОЛОГИИ IPSEC

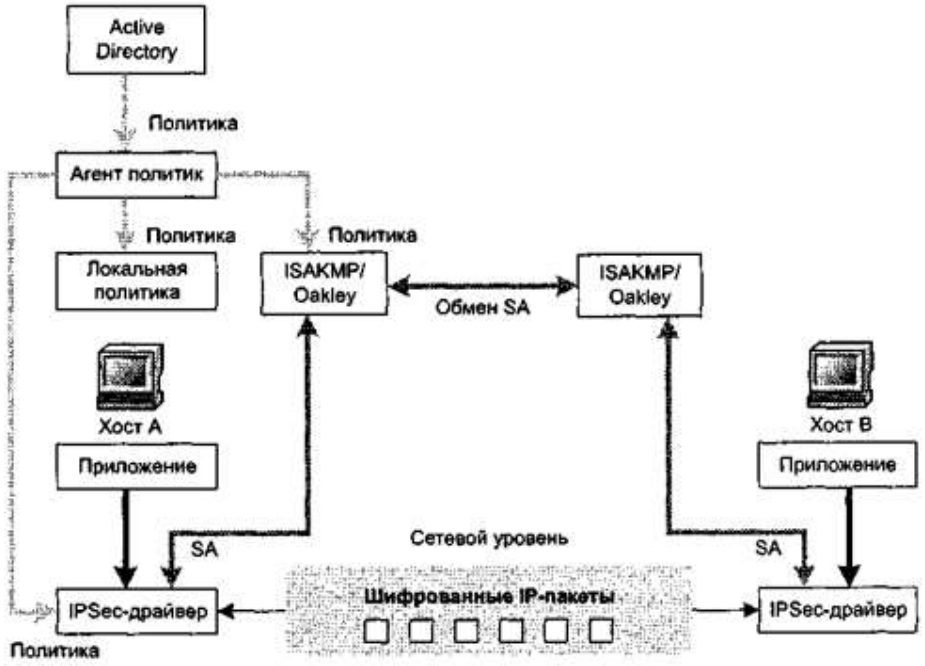
Протокол Internet Key Exchange (IKE) представляет собой стандарт протокола управления ключами. IKE используется вместе со стандартом IPsec.



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. IKE – это гибридный протокол, реализующий протоколы обмена ключами на базе платформы Internet Security Association Key Management Protocol (ISAKMP). ISAKMP определяет формат сообщений, механизм протокола обмена ключами и процесс согласования с целью создания SA для IPsec. IKE реализует части протоколов Oakley и SKEME, но никак не зависит от этих протоколов.

ТЕХНОЛОГИИ IPSEC

- Драйвер IPSEC на компьютере A проверяет список фильтров IP в активной политике на наличие совпадающего адреса или типа трафика исходящих пакетов.
- Драйвер IPSEC предоставляет ISAKMP сведения для начала согласования безопасности с компьютером B.
- Служба ISAKMP на компьютере B получает запрос для согласования безопасности.
- Два компьютера выполняют обмен ключами, устанавливают соответствие безопасности ISAKMP и создают общий секретный ключ.
- Затем компьютеры согласовывают уровень безопасности для передачи данных, устанавливая пару соответствий безопасности IPSEC и ключей для защиты пакетов IP.

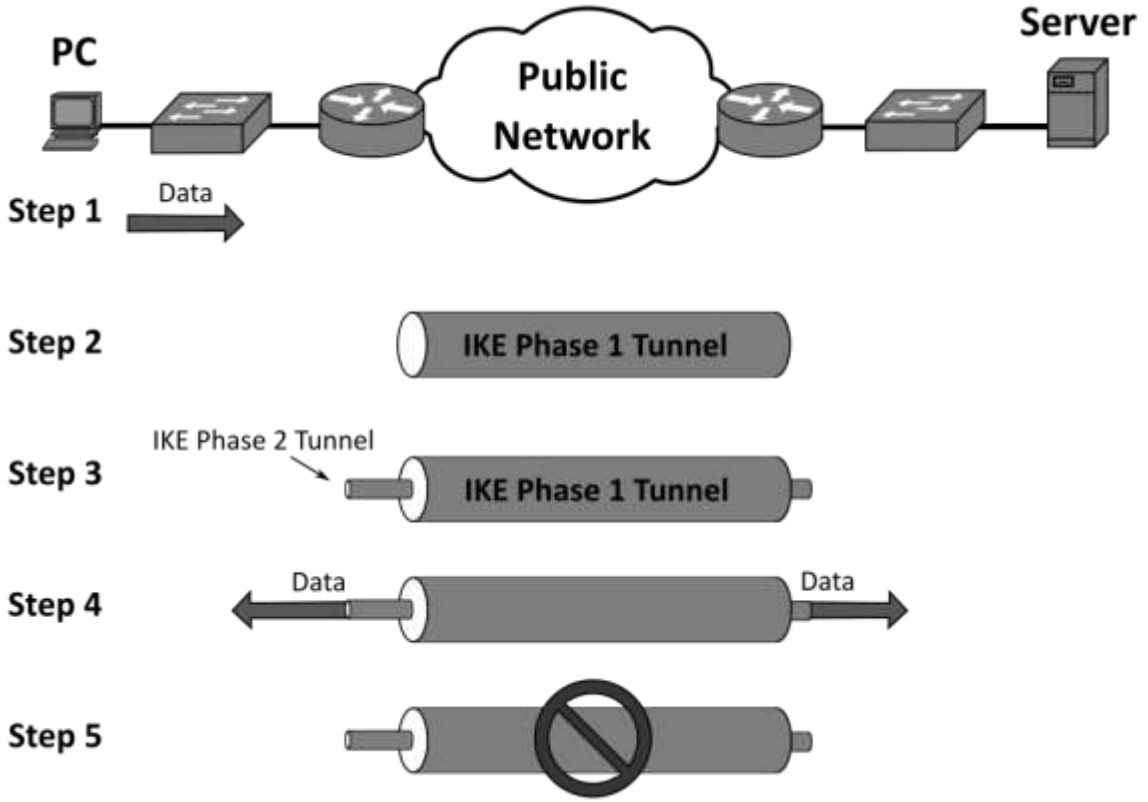


- Используя сопоставление безопасности IPSEC для исходящего трафика и ключ, драйвер IPSEC на компьютере A подписывает пакеты для проверки целостности и зашифровывает пакеты, если было согласовано шифрование.
- Драйвер IPSEC на компьютере A отправляет пакеты на соответствующий тип подключения для передачи на компьютер B.
- Компьютер B получает защищенные пакеты и передает их драйверу IPSEC.
- Используя сопоставление безопасности IPSEC для входящего трафика и ключ, драйвер IPSEC на компьютере B проверяет подпись целостности и, при необходимости, расшифровывает пакеты.
- Драйвер IPSEC на компьютере B передает расшифрованные пакеты драйверу TCP/IP, который передает их в принимающее приложение.

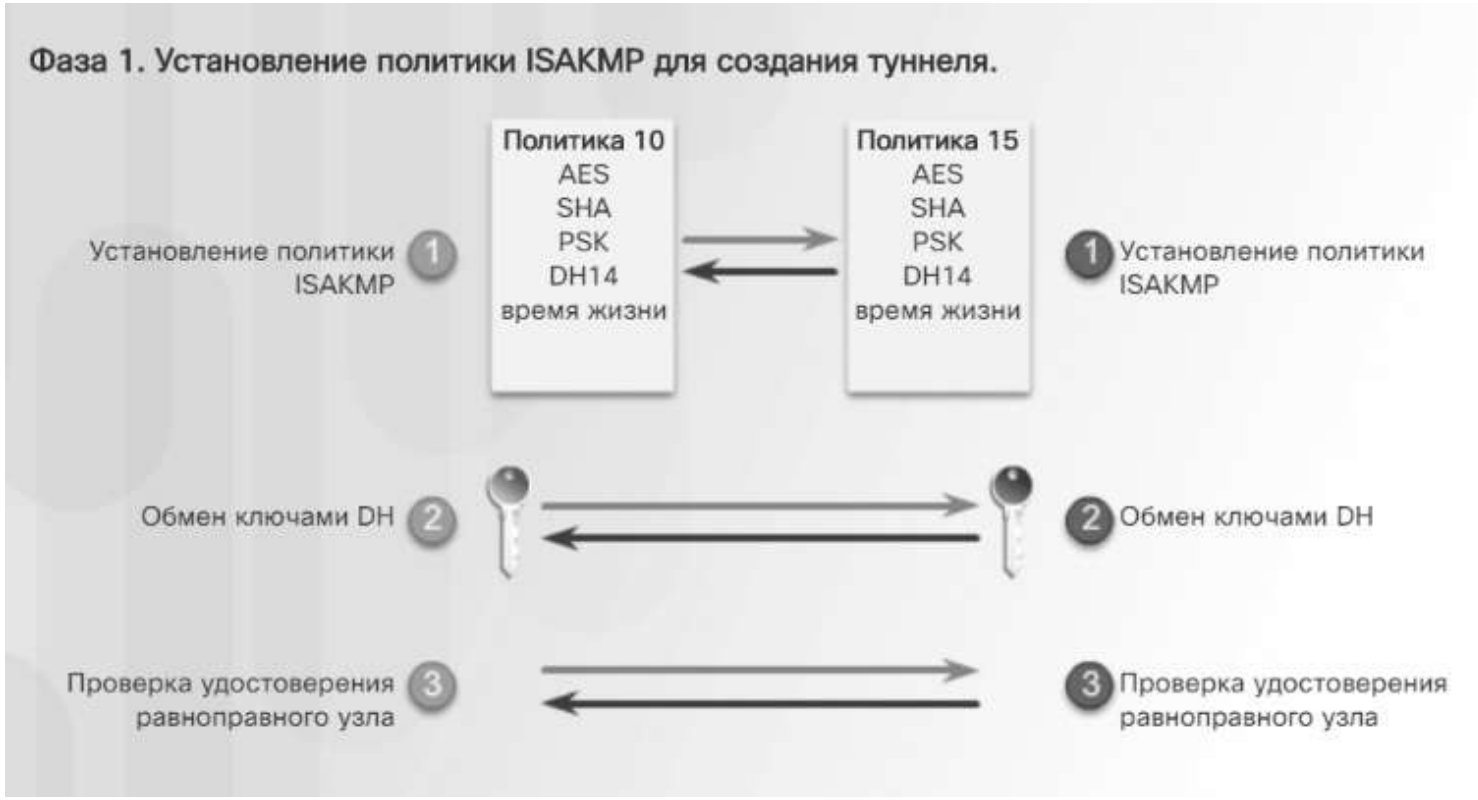
ПРОТОКОЛ IPSEC

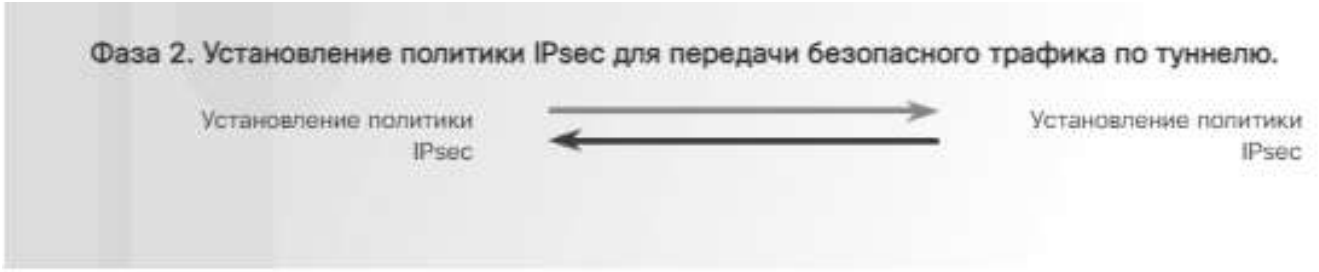
Этапы работы IPsec

1. Первый этап – создания на каждом узле политики безопасности.
2. Второй этап является первой фазой IKE. Её цель — организовать безопасный канал между сторонами для второй фазы IKE. На втором этапе выполняются:
3. Третий этап является второй фазой IKE. Его задачей является создание IPsec-туннеля.
4. Рабочий этап. После создания IPsec SA начинается обмен информацией между узлами через IPsec-туннель, используются протоколы и параметры, установленные в SA.
5. Прекращают действовать текущие IPsec SA.



ПРОТОКОЛ IPSEC





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.

ПРОТОКОЛ IPSEC

Туннельный режим

Туннельный режим IPSec используется для создания безопасного соединения WAN и VPN, использующих Интернет в качестве среды подключения. В этом режиме протоколы IPSec шифруют заголовок и полезную нагрузку IP-пакеты. Таким образом данные, содержащиеся в этом пакете, инкапсулируются внутри дополнительного пакета, который и будет отправлен.

1.Данные передаются с использованием незащищенного IP-пакета с компьютера в частной сети.

2.Когда пакет поступает на маршрутизатор, он инкапсулирует его, используя протоколы безопасности IPSec.

3.Маршрутизатор пересылает пакет на другой конец соединения.

4.Маршрутизатор, принимающий IP-пакет проверяет его целостность.

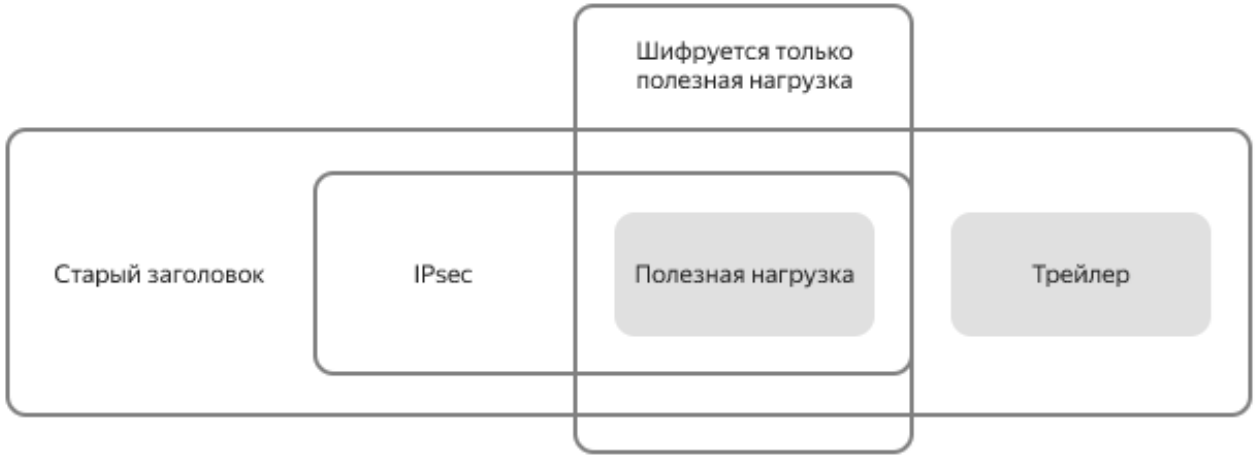
5.Пакет расшифровывается.

6.Данные пакета отправляются на компьютер получателя в частной сети.

ПРОТОКОЛ IPSEC

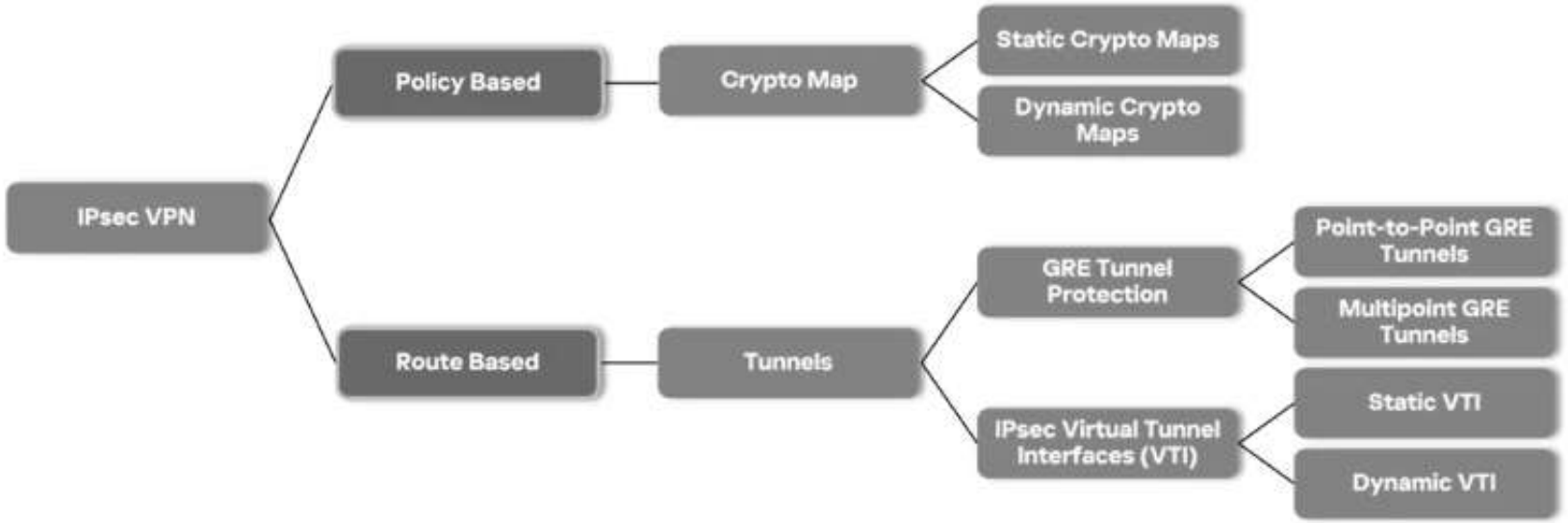
Транспортный режим
Основное отличие транспортного режима от туннельного в том, что в транспортном режиме работы шифруется не весь IP-пакет, а только полезная нагрузка.

Транспортный режим шифрования используется когда между двумя устройствами уже существует IP-связь, но она небезопасна. Например, при передаче IP-пакета от сервера к клиенту.



ТЕХНОЛОГИИ VPN

Настройка IPsec



Порядок следующий:

- Настраиваем фазу 1;
- Задаём PSK;
- Создаём Crypto ACL для отбора интересного трафика;
- Настраиваем фазу 2: Transform Set;
- Создаём Crypto Map, в Crypto Map используем созданные Crypto ACL, Transform Set;
- Затем вешаем Crypto Map на нужный интерфейс;
- Разрешаем входящий трафик ISAKMP, ESP.

ТЕХНОЛОГИИ IPSEC

Кроме этого IPsec обеспечивает **Antireplay** *(все пакеты нумеруются и если пакет уже приходил, то второй пакет с таким же номером будет отброшен).*

•IKE — Самый центровой протокол в IPsec Framework это IKE (Internet Key Exchange). Остальные протоколы работают под его управлением;
Самое первое, IKE должен быть включен для реализации функционала IPsec. Он включен по умолчанию в IOS, но его можно и отключить:

```
Router(config)# no crypto isakmp enable
*Aug 8 10:11:16.283: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is OF
```

Надо проверить и при необходимости включить:

```
Router# show crypto isakmp policy
ISAKMP is turned off
Router(config)# crypto isakmp enable - эта команда также проверяет поддержку
IKE со стороны роутера, если при выполнении возникает ошибка, IOS нужно
апгрейдить
```

ТЕХНОЛОГИИ IPSEC

Существует две версии IKE: IKEv1 (RFC 2409) and IKEv2 (RFC 7296), IKEv2 реализован чтобы обойти ограничения IKEv1 и имеет существенные улучшения по сравнению с первой версией:

- EAP (certificate-based authentication);
- Anti-DoS capabilities;
- Needs fewer messages to establish an IPsec SA.

Параметр	IKEv1	IKEv2
Пропускная способность	Больше	Меньше
EAP — протокол расширяемой аутентификации	Не поддерживается	Поддерживается
MOBIKE — протокол мобильности и многодомности	Не поддерживается	Поддерживается
NAT-T —обход NAT	Не поддерживается	Поддерживается
Выбор между агрессивным и основным режимом	Поддерживается	Не поддерживается
XAUTH — расширенная аутентификация	Поддерживается	Не поддерживается

ТЕХНОЛОГИИ IPSEC

Преимущества IPsec

•Сетевой уровень работы

Основным преимуществом IPSec является то, что он работает на сетевом, а не прикладном уровне. По сути, это означает, что данные шифруются на компьютере-отправителе.

•Безопасность

Протоколы AH и ESP обеспечивают высокий уровень безопасности и приватности.

•Универсальность

Протоколы безопасности IPsec используются для защиты любых типов данных, включая электронную почту, видеоконференции, VoIP и многое другое.

Недостатки и ограничения IPsec

•Сложность настройки и управления

IPSec сложнее, чем альтернативные протоколы безопасности, и его сложнее настроить.

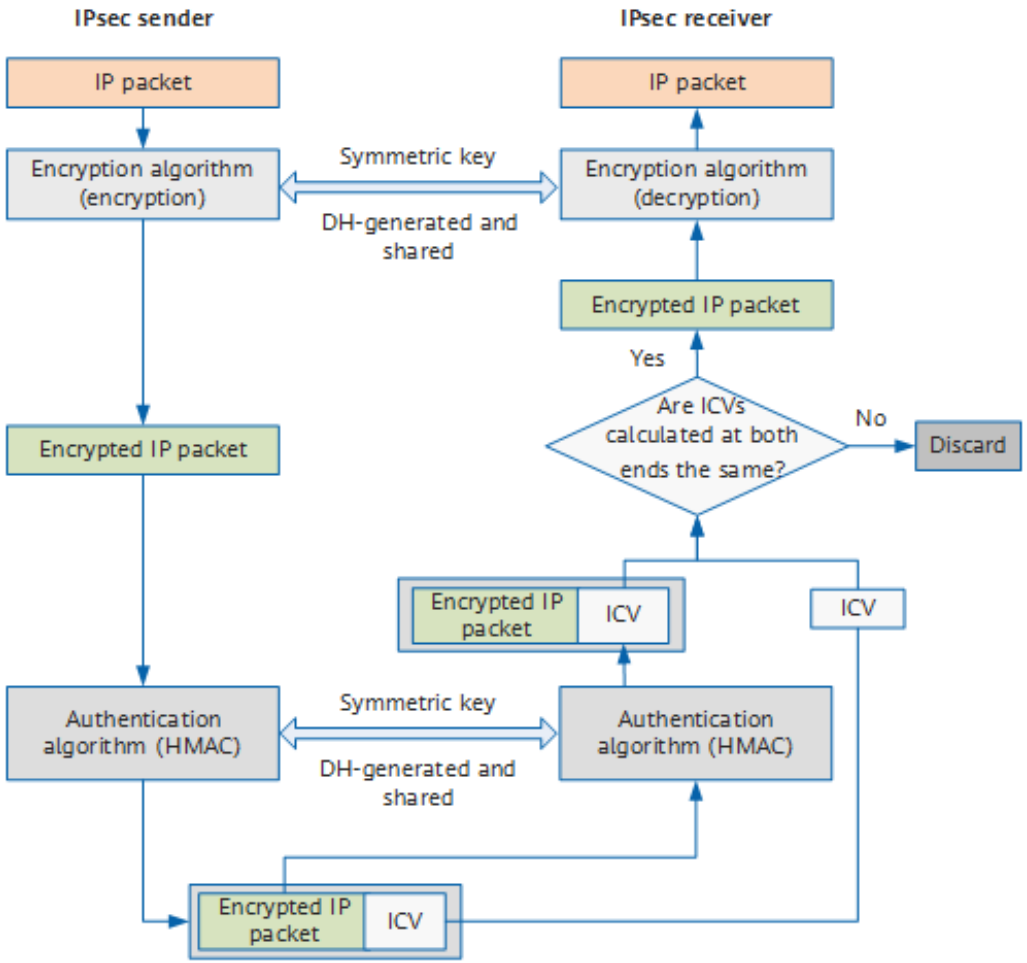
•Возможность проблем совместимости между различными реализациями IPsec

Если разработчики ПО не придерживаются стандартов IPSec, это может привести к проблемам с совместимостью.

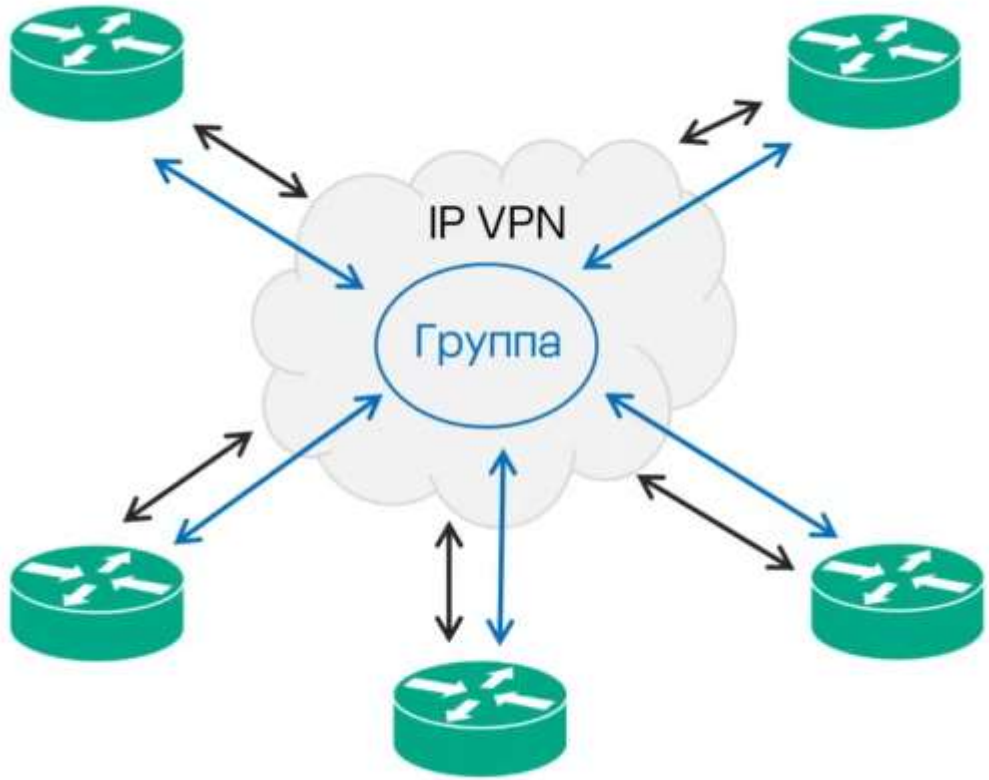
•Влияние на производительность сети

Для шифрования и дешифрования всех данных, проходящих через сервер, требуется довольно много вычислительной мощности.

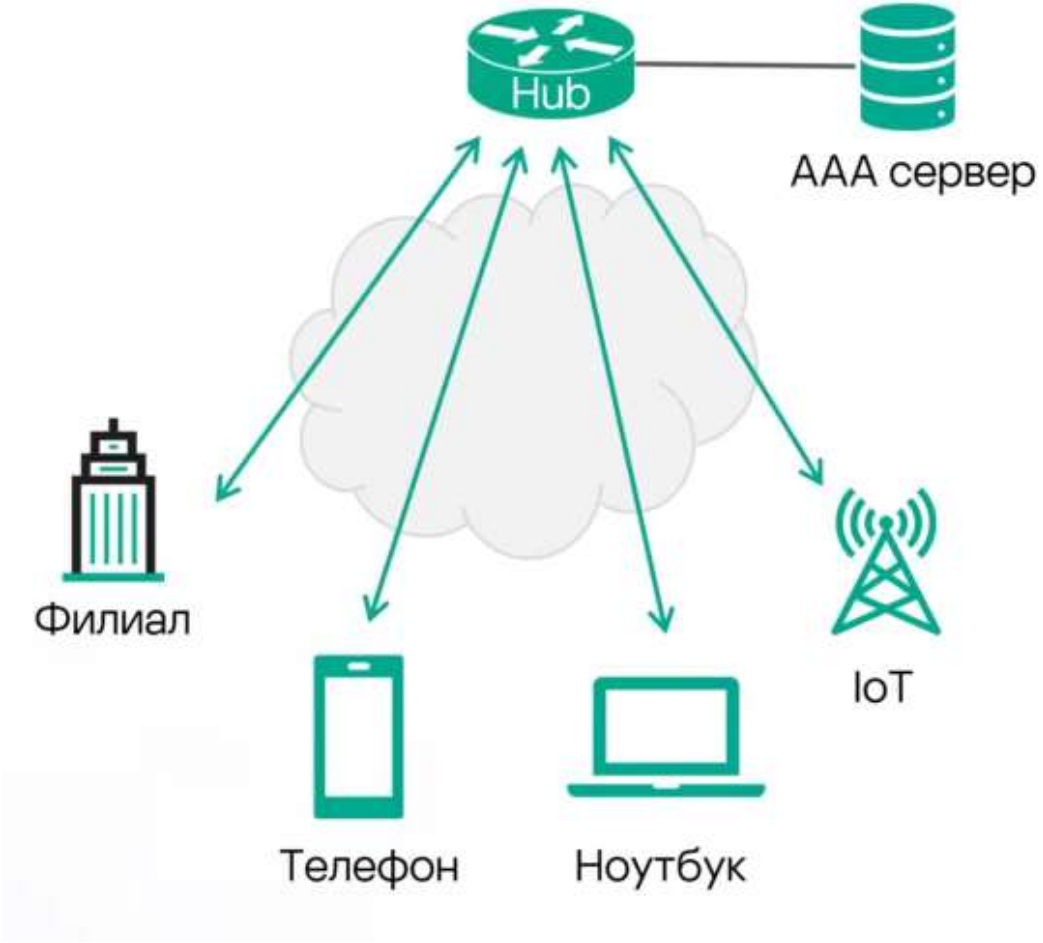
ТЕХНОЛОГИИ IPSEC



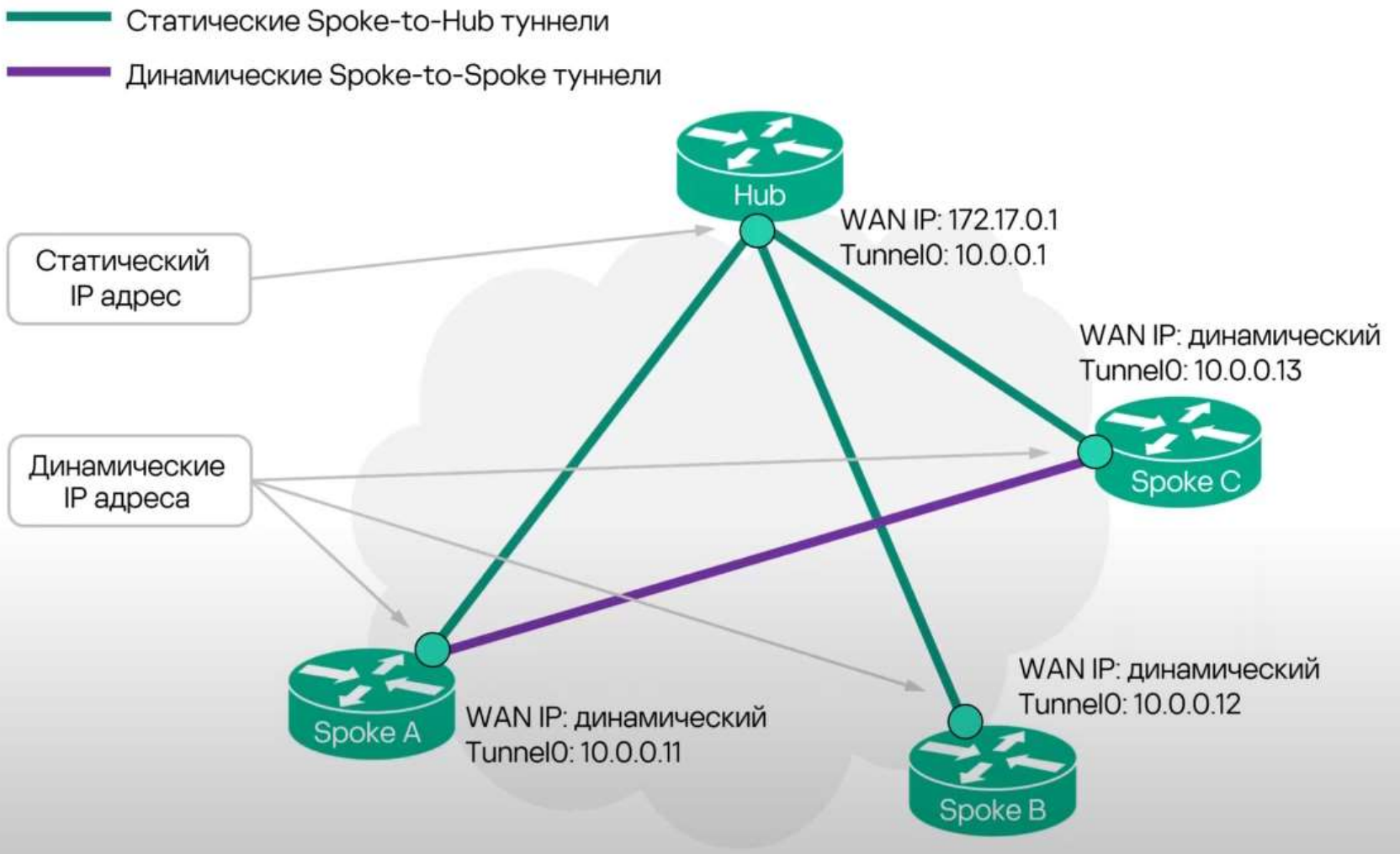
ТЕХНОЛОГИИ IPSEC



ТЕХНОЛОГИИ IPSEC

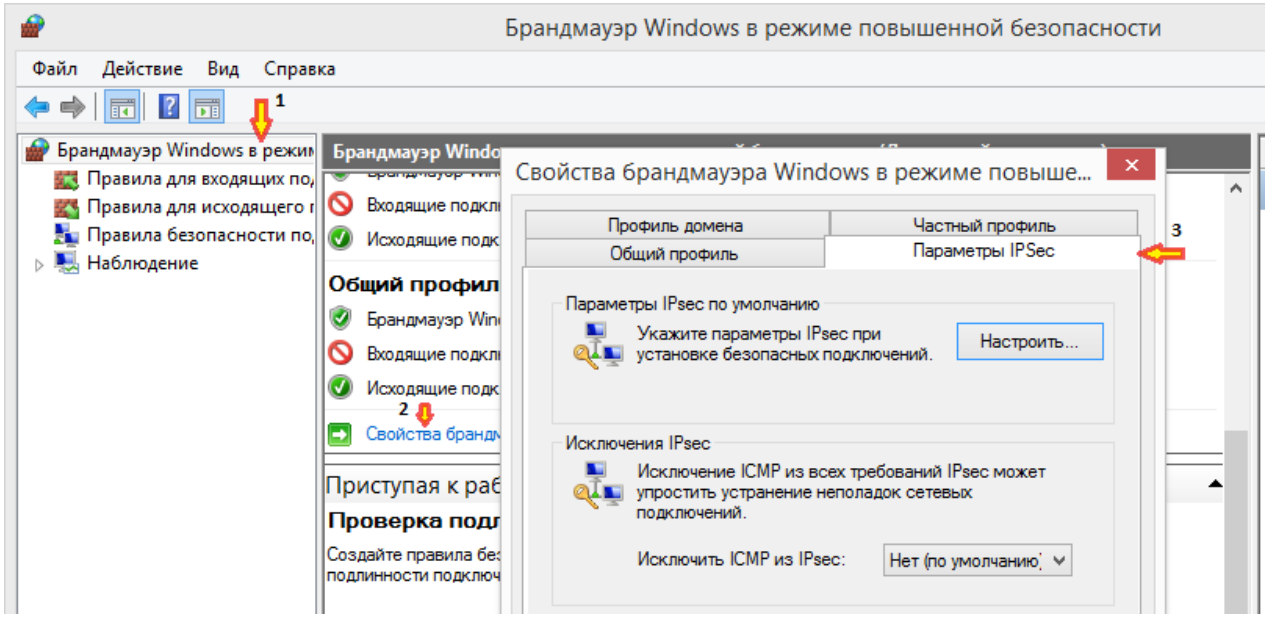


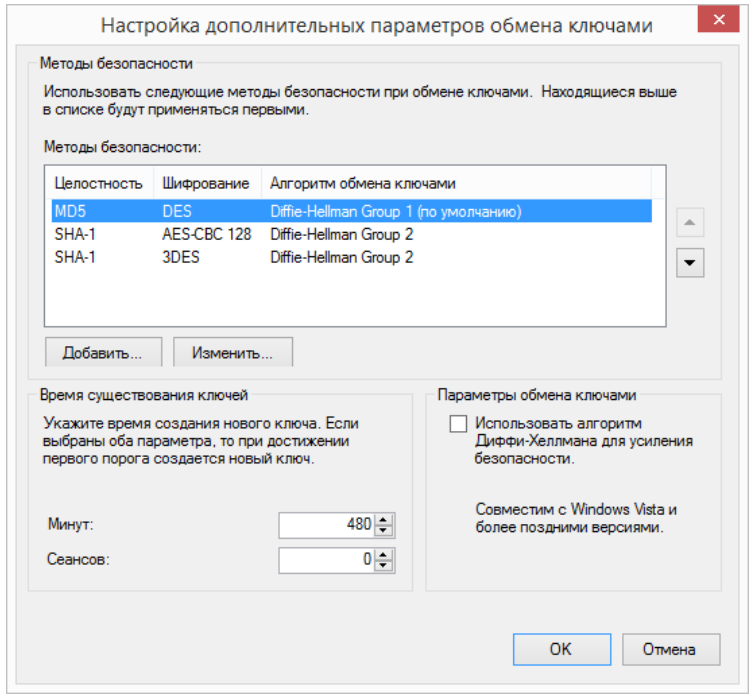
ТЕХНОЛОГИИ IPSEC



ТЕХНОЛОГИИ IPSEC

Задействовать встроенную в ОС Windows функциональность IPSec. Запустить системную консоль управления оснасткой брандмауэра с повышенной безопасностью wf.msc.





Пример создания подключений IPSec средствами операционной системы Windows https://help.keenetic.com/hc/ru/articles/115001906769-Пример-создания-подключений-IPSec-средствами-операционной-системы-Windows

Настройка туннеля IPsec IKEv1 типа «сеть-сеть» между ASA и маршрутизатором с Cisco IOS https://www.cisco.com/c/ru_ru/support/docs/security-vpn/ipsec-negotiation-ike-protocols/119425-configure-ipsec-00.html

ТЕХНОЛОГИИ IPSEC

Кроме этого IPsec обеспечивает **Antireplay** *(все пакеты нумеруются и если пакет уже приходил, то второй пакет с таким же номером будет отброшен).*

•IKE — Самый центровой протокол в IPsec Framework это IKE (Internet Key Exchange). Остальные протоколы работают под его управлением;
Самое первое, IKE должен быть включен для реализации функционала IPsec. Он включен по умолчанию в IOS, но его можно и отключить:

```
Router(config)# no crypto isakmp enable
*Aug 8 10:11:16.283: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is OF
```

Надо проверить и при необходимости включить:

```
Router# show crypto isakmp policy
ISAKMP is turned off
```

Router(config)# crypto isakmp enable - *эта команда также проверяет поддержку IKE со стороны роутера, если при выполнении возникает ошибка, IOS нужно апгрейдить*

ТЕХНОЛОГИИ IPSEC

Существует две версии IKE: IKEv1 (RFC 2409) and IKEv2 (RFC 7296), IKEv2 реализован чтобы обойти ограничения IKEv1 и имеет существенные улучшения по сравнению с первой версией:

- EAP (certificate-based authentication);
- Anti-DoS capabilities;
- Needs fewer messages to establish an IPsec SA.

Параметр	IKEv1	IKEv2
Пропускная способность	Больше	Меньше
EAP — протокол расширяемой аутентификации	Не поддерживается	Поддерживается
MOBIKE — протокол мобильности и многодомности	Не поддерживается	Поддерживается
NAT-T —обход NAT	Не поддерживается	Поддерживается
Выбор между агрессивным и основным режимом	Поддерживается	Не поддерживается
XAUTH — расширенная аутентификация	Поддерживается	Не поддерживается

ТЕХНОЛОГИИ IPSEC

Преимущества IPsec

•Сетевой уровень работы

Основным преимуществом IPSec является то, что он работает на сетевом, а не прикладном уровне. По сути, это означает, что данные шифруются на компьютере-отправителе.

•Безопасность

Протоколы AH и ESP обеспечивают высокий уровень безопасности и приватности.

•Универсальность

Протоколы безопасности IPsec используются для защиты любых типов данных, включая электронную почту, видеоконференции, VoIP и многое другое.

Недостатки и ограничения IPsec

•Сложность настройки и управления

IPSec сложнее, чем альтернативные протоколы безопасности, и его сложнее настроить.

•Возможность проблем совместимости между различными реализациями IPsec

Если разработчики ПО не придерживаются стандартов IPSec, это может привести к проблемам с совместимостью.

•Влияние на производительность сети

Для шифрования и дешифрования всех данных, проходящих через сервер, требуется довольно много вычислительной мощности.

ТЕХНОЛОГИИ VPN

Аутентификация

Данное действо производится перед всеми другими.

Роутер должен подтвердить другому роутеру свою подлинность для участия в IPsec туннеле.

Возможности: Общий, вводимый вручную, секретный ключ PSK (Pre Shared Key), Сертификаты RSA.

Рекомендуется: Сертификаты RSA.

Аутентификация на основе общего ключа PSK происходит так: к ключу прикладывается определённая несекретная информация, известная и общая для обоих роутеров, высчитывается хеш, отправляется второму роутеру. Второй роутер повторяет процедуру для своего ключа и сравнивает хеши. Совпадение хешей означает совпадение общих ключей и как результат — подлинность, приславшего сообщение роутера. Потом второй роутер повторяет процедуру. В результате оба роутера подтвердили свою подлинность друг-другу.

```
R1(config-isakmp)# authentication ?
pre-share Pre-Shared Key
rsa-encr Rivest-Shamir-Adleman Encryption
rsa-sig Rivest-Shamir-Adleman Signature
```

ТЕХНОЛОГИИ IPSEC

Шифрование

Применяется *симметричное шифрование,* то есть такое, где ключ для шифрования и расшифровки один и тот же. Оно менее устойчиво ко взлому чем ассиметричное, но только симметричное шифрование технически доступно для больших объёмов передаваемых пользовательских данных, так как использует относительно низкую утилизацию CPU устройства. *Рекомендуется AES.*

```
R1(config-isakmp)# encryption ?
3des Three key triple DES
aes AES - Advanced Encryption Standard.
des DES - Data Encryption Standard (56 bit keys).
```

ТЕХНОЛОГИИ IPSEC

ТЕХНОЛОГИИ VPN

Эволюция VPN: от IPsec до SD-WAN
https://www.youtube.com/watch?v=iFj1mk6tcvc

Как маленькие ошибки могут оборачиваться большими уязвимостями
https://www.youtube.com/watch?v=VbzRKMAKw_U

Разбор полетов. Kaspersky SD-WAN реальные кейсы
https://www.youtube.com/watch?v=xnWT48pyNVM

Шпоры по сертификатам X.509
https://habr.com/ru/articles/346798/

Введение в TLS для ~~практиков~~ Патриков (часть 1)
https://habr.com/ru/companies/plesk/articles/502604/

Настраиваем IPsec-туннель между офисами на оборудовании Mikrotik
https://interface31.ru/tech_it/2022/01/nastraivaem-ipsec-tunnel-mezhdu-ofisami-na-oborudovanii-mikrotik.html

Настройка Site-To-Site IPSec VPN на Cisco
https://wiki.merionet.ru/articles/nastrojka-site-to-site-ipsec-vpn-na-cisco/?ysclid=ln4a5m8y1d83542449