24.03.20

Дисциплина: Организация, принципы построения и функционирования компьютерных сетей

Тема: Типы сетей VPN

Существует несколько разновидностей VPN: Самые распространенные типы — PPTP VPN, Site-to-Site VPN, L2TP VPN, IPsec, SSL, MPLS VPN и Hybrid VPN. Ниже мы рассмотрим их более подробно.

1. PPTP VPN

PPTP VPN — это протокол туннелирования точка-точка. Как видно из названия, PPTP VPN создает туннель и захватывает данные. Это самый распространенный тип VPN. PPTP VPN позволяют подключиться к сети VPN через существующее интернет-подключение. Этот тип VPN прекрасно подходит как для бизнеса, так и для домашнего использования. Для доступа к сети используется пароль. PPTP идеальны для дома и бизнеса, так как они не требуют установки дополнительного оборудования и позволяют обходиться дешевыми и несложными приложениями. PPTP хорошо совместимы с Windows, Mac и Linux.

И хотя PPTP VPN демонстрируют множество преимуществ, не обошлось без недостатков. Главный из них — это то, что протокол PPTP не использует шифрования. Кроме того, основа PPTP — это протокол PPP, что также не обеспечивает высокий уровень безопасности.

2. Site-to-Site VPN

Узел-узел или Роутер-Роутер — это самый распространенный тип VPN в бизнесе. Особенно это характерно для компаний с офисами как в разных частях одной страны, так и в нескольких странах, что позволяет связать все компьютеры в единую сеть. Также они известны как интранет-VPN (VPN по внутренней сети). Другой вариант также возможен. Компании, использующие VPN узел-узел, подключаются к серверам других компаний таким же образом, как и экстранет-VPN. Говоря простым языком, этот тип VPN — своего рода мост, соединяющий сети в разных локациях, обеспечивая безопасное соединение и подключение к интернету.

Как и PPTP, VPN типа узел-узел создает безопасную сеть. Однако, выделенная линия не предусмотрена, так что разные компьютеры компании могут подключаться к сети. В отличие от PPTP, шифрование производится либо при помощи специальных устройств, либо при помощи приложений на обоих концах сети.

3. L2TP VPN

L2TP означает «Протокол туннелирования второго уровня», он был разработан компаниями Microsoft и Cisco. VPN на основе протокола L2TP сочетается с другим протоколом, что обеспечивает более безопасное соединение. При протоколе L2TP формируется туннель между двумя точками подключения L2TP, а также при помощи другого протокола, например IPsec, производится шифрование данных.

L2TP действует подобно PPTP. Главное сходство — отсутствие шифрования и основа на протоколе PPP. Разница же — это защита и сохранность данных. VPN на основе L2TP обеспечивают более безопасное и надежное соединение.

4. IPsec

IPsec — это сокращение, означающее «Безопасность интернет-протокола». IPsec — это VPN-протокол, используемый для того, чтобы обеспечить безопасность в сети. Протокол устанавливает туннель до удаленного узла. Каждая сессия проверяется, пакеты данных шифруются, так что протокол IPsec обеспечивает высокий уровень безопасности соединения. Существует два режима, в которых работает этот протокол. Транспортный и туннельный. Оба служат для защиты передачи данных между разными сетями. В транспортном режиме шифруется сообщение в пакете данных. В туннельном режиме шифруется весь пакет данных. Преимущество использования IPsec заключается в том, что он может быть применен в дополнение к другим протоколам, чтобы повысить защиту сети.

И хотя IPsec — это полезный и удобный протокол, однако основной минус — это долгое время установки клиентских приложений.

5. SSL and TLS

SSL — это протокол защищенных сокетов, TLS — безопасность на транспортном уровне. Они работают как один протокол. Оба используются для создания VPN. В этом подключении веб-браузер работает как клиент, пользователь получает доступ к специальным приложениям вместо всей сети. SSL и TSL используются в онлайн-продажах. SSL и TSL предоставляют защищенную сессию от браузера до сервера с приложением. Браузер легко переключается на SSL, не требуя никаких дополнительных действий со стороны пользователя. Абсолютное большинство современных браузеров уже включает в себя SSL и TSL. SSL-подключение содержит https вместо http в адресе.

6. MPLS VPN

VPN-сервисы с поддержкой технологии многопротокольной коммутации с использованием меток (MPLS) лучше всего использовать для подключений типа сайт-к-сайту. Все потому, что MPLS — это наиболее гибкий вариант с максимум возможностей для адаптации. MPLS основываются на определенных стандартах, используемых для ускорения распределения сетевых пакетов по множеству протоколов. VPN-сервисы с поддержкой MPLS — это системы, представляющие собой VPN-сервисы, настроенные для работы с интернет-провайдерами, когда два или более сайтов могут объединиться между собой, формируя VPN, используя для этого мощности одного и того же интернет-провайдера. Впрочем, самым большим минусом VPN-сервисов с поддержкой MPLS является тот факт, что такую сеть настроить куда сложнее, чем остальные VPN. Сложнее и вносить в нее модификации. Как следствие, услуги VPN-сервисов с поддержкой MPLS обходятся пользователям дороже.

7. Hybrid VPN

Гибридная сеть VPN сочетает в себе MPLS и IPSec. Оба типа используются отдельно на различных узлах. Однако, иногда узел допускает одновременное подключение обоих типов протоколов. Это делается с целью повысить надежность MPLS при помощи IPSec.

IPSec, как уже упоминалось ранее, требуют наличия определенного оборудования. Обычно это роутер или многоцелевое устройство безопасности. При его помощи данные шифруются и образуют VPN-туннель. MPLS используются на канале передачи информации при помощи передающего оборудования.

Для соединения этих двух типов VPN устанавливается шлюз, где устраняется IPSec и производится подключение к MPLS с сохранением безопасности данных.

Гибридные VPN используются компаниями, так как MPLS очень часто не подходит для их узлов. MPLS обеспечивает множество преимуществ по сравнению с общим подключением, однако цена высока. При помощи гибридной сети вы можете подключиться к центральному узлу через удаленный. Гибридные VPN наиболее дорогие, но при этом очень гибкие в настройке.