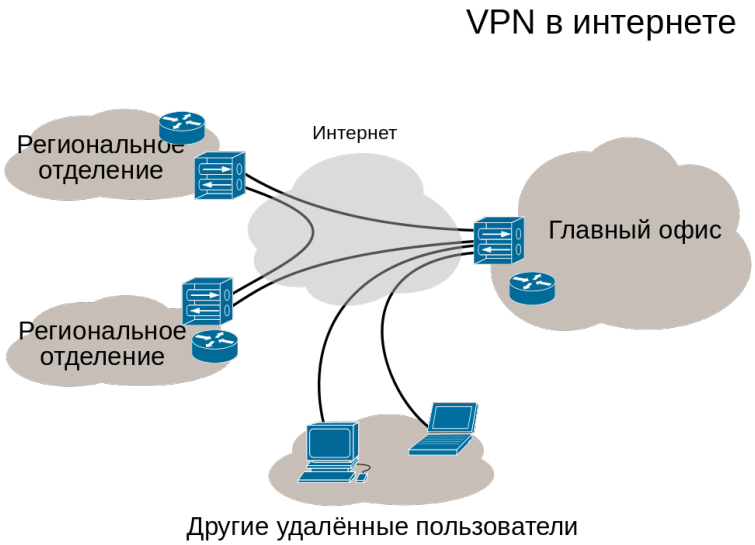
ЗИСОПД
Лекция

Виртуальные частные сети

VPN (Virtual Private Network — виртуальная частная сеть) — обобщённое название технологий, позволяющих обеспечить одно или несколько сетевых соединений (логическую сеть) поверх другой сети (локальной или глобальной). По-другому, это логический канал передачи данных, сконфигурированный на основе существующих физических каналов и обеспечивающий реализацию технологии туннелирования.



В зависимости от применяемых протоколов и назначения, VPN может обеспечивать соединения трёх видов: узел-узел, узел-сеть и сеть-сеть.

Виртуальные частные сети строятся в первую очередь на технологии туннелирования, которая обеспечивает создание условно постоянного соединения между абонентами. Кроме того, необходимо использовать специальные устройства или программное обеспечение, реализующие криптографическое преобразование передаваемых данных.

Для построения виртуальной частной сети необходимо использовать следующие функции оборудования:

1) туннелирование;
2) управление доступом;
3) аутентификация;
4) шифрование.

Классификация виртуальных частных сетей

Существует несколько классификаций виртуальных частных сетей, основанных на особенностях технологий их реализации.

По виду и собственнику каналов

1. ***Истинные частные сети***. Это такая сеть, в которой все оборудование (включая территориальные кабельные системы, коммутирующие устройства, средства управления и т. п.) являются собственностью организации и принадлежат корпоративной сети. Такая виртуальная частная сеть гарантирует, что риск доступа к информации извне, то есть без привлечения сотрудников организации, практически сведен к нулю. Кроме того, в пределах истинной частной сети можно варьировать в широких пределах качество обслуживания и методы шифрования (кроме случаев, когда такая сеть используется для передачи информации, составляющей государственную тайну). *Правила построения*: 1) сеть не должна располагаться на территории, принадлежащей другой организации; 2) весь обслуживающий персонал (ремонт, техподдержка, инфобезопасность) не должен быть внешним.
2. ***Сети на арендованных каналах***. Построены по принципу защищенных виртуальных тоннелей в частично защищенной общей сети. В этом случае техническое и программное обеспечение передачи информации между локальными подразделениями организации берет на себя доверенный провайдер транспортных услуг. *Особенности*:
   a) арендуемые территориальные каналы прокладываются провайдером транспортных территориальных услуг в его первичной сети или сети с интегрированными услугами ISDN;
   b) каналы, связывающие центральную сеть предприятия с сетями филиалов, проходят через мультиплексор, объединяющий каналы всех абонентов в магистральный канал;
   c) коммутация каналов в первичных сетях выполняется только оператором сети;
   d) пропускная способность выделенного каждому конкретному арендатору канала постоянна и заранее оговорена.

   Кроме того, особенностью сети на арендованных каналах является существенное затруднение пассивного анализа трафика. Это происходит из-за того, что провайдер в данном случае не задействован в поддержке криптографических преобразований, и, следовательно, используемое сквозное или канальное шифрование обеспечивает достаточную конфиденциальность.
3. ***Сети на каналах открытого доступа***. В качестве канала передачи используется глобальная сеть пакетной коммутации (Интернет). *Особенности*:
   a) использование неспециализированного оборудования (то есть отсутствие криптомаршрутизаторов);
   b) привлечение к процессу передачи информации большого числа

организаций, функционально, территориально и структурно не ограниченных;

c) использование пакетной коммутации.

В такой виртуальной частной сети требуется максимально обеспечить автономность средств криптографического преобразования и управления системой в целом, а также использовать ряд стандартизированных решений, в частности, инфраструктуру открытых ключей. Защита информации в такой сети может быть недостаточной. В первую очередь это касается аспекта доступности, который может быть утерян в результате отказов средств коммутации глобальной сети, а также подверженности подобного решения разного рода сетевым атакам.

По способу реализации

1. Сетевые операционные системы со встроенными функциями организации виртуальной частной сети.
2. Маршрутизаторы, межсетевые экраны или коммутаторы.
3. Средства криптографической защиты информации, предназначенные только для организации виртуальной частной сети.

По назначению

1. ***Intranet VPN***. Используют для объединения в единую защищённую сеть нескольких распределённых филиалов одной организации, обменивающихся данными по открытым каналам связи.
2. ***Remote Access VPN***. Используют для создания защищённого канала между сегментом корпоративной сети (центральным офисом или филиалом) и одиночным пользователем, который, работая дома, удаленно подключается к корпоративным ресурсам.
3. ***Extranet VPN***. Используют для сетей, к которым подключаются «внешние» пользователи (например, заказчики или клиенты). Уровень доверия к ним намного ниже, чем к сотрудникам компании, поэтому требуется обеспечение специальных «рубежей» защиты, предотвращающих или ограничивающих доступ последних к особо ценной, конфиденциальной информации.
4. ***Internet VPN***. Используется для предоставления доступа к интернету провайдерами, обычно если по одному физическому каналу подключаются несколько пользователей. Протокол PPPoE/PPPoA стал стандартом в ADSL-подключениях. L2TP был широко распространён в середине 2000-х годов в домовых сетях: в те времена внутрисетевой трафик не оплачивался, а внешний стоил дорого. Это давало возможность контролировать расходы: когда VPN-соединение выключено, пользователь ничего не платит.
5. ***Client/Server VPN***. Он обеспечивает защиту передаваемых данных между двумя узлами (не сетями) корпоративной сети. Особенность данного варианта в том, что VPN строится между узлами, находящимися, как правило, в одном сегменте сети, например, между рабочей станцией и

сервером. Такая необходимость очень часто возникает в тех случаях, когда в одной физической сети необходимо создать несколько логических сетей. Например, когда надо разделить трафик между финансовым департаментом и отделом кадров, обращающихся к серверам, находящимся в одном физическом сегменте. Этот вариант похож на технологию VLAN, но вместо разделения трафика используется его шифрование.

По типу протокола

Существуют реализации виртуальных частных сетей под TCP/IP, IPX и AppleTalk. Но на сегодняшний день наблюдается тенденция к всеобщему переходу на протокол TCP/IP, и абсолютное большинство решений VPN поддерживает именно его. Адресация в нём чаще всего выбирается в соответствии со стандартом RFC5735, из диапазона Приватных сетей TCP/IP.

По уровню сетевого протокола

По уровню сетевого протокола на основе сопоставления с уровнями эталонной сетевой модели ISO/OSI.

1. PPP (Point-to-Point Protocol) используется в качестве универсального канального уровня.
2. PPTP (Point-to-Point Tunneling Protocol) реализует технологии туннелирования на канальном уровне.
3. L2TP (Layer 2 Tunneling Protocol) объединяет протоколы PPTP и L2F (Layer-2 Forwarding).
4. IPSec и SKIP используется для организации туннеля на сетевом уровне;
5. SSL, TLS, SOCKS обеспечивают существование туннеля на уровне представления.

Основные протоколы VPN

Протокол PPP

PPP (Point-to-Point Protocol) — двухточечный протокол (семейство протоколов) канального уровня модели OSI. Обычно используется для установления прямой связи между двумя узлами сети. Обеспечивает аутентификацию соединения, шифрование и сжатие данных. Используется для различных типов физических сетей: нуль-модемный кабель, телефонная линия, сотовая связь и т. д.

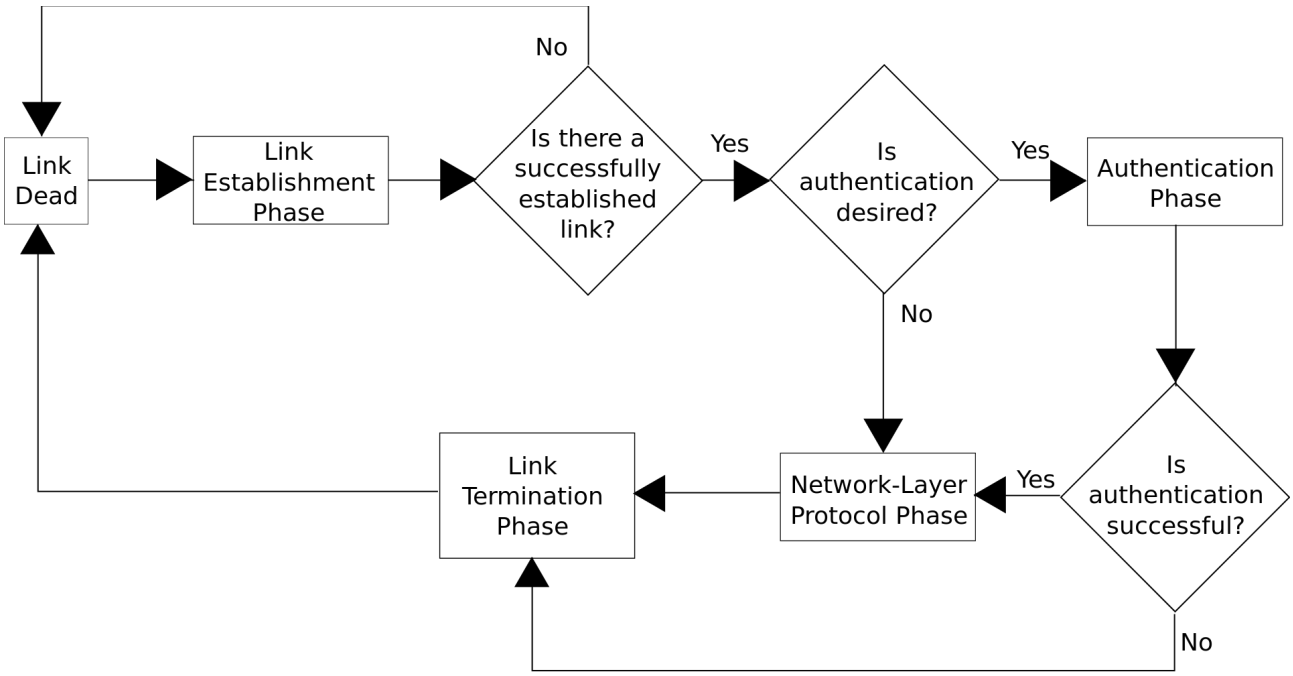
Подвиды протокола PPP:

1. Point-to-Point Protocol over Ethernet (PPPoE) — для подключения по Ethernet, и иногда через DSL.
2. Point-to-Point Protocol over ATM (PPPoA) — для подключения по DSL.

Семейство протоколов PPP:

1) протокол управления линией связи (LCP): для установления, конфигурирования и тестирования информационных каналов;
2) протокол управления сетью (NCP): для установки и конфигурирования различных протоколов сетевого уровня;
3) протоколы аутентификации (PAP, CHAP, EAP),
4) многоканальный протокол PPP (MLPPP).

Протокол PPP при установлении соединения опционально предусматривает процедуру аутентификации. После перехода на сетевой уровень вызывается NCP-протокол, который выполняет необходимую конфигурацию канала.



Фазы установления соединения PPP по RFC 1661:

1. *Link Dead*. Эта фаза наступает, когда связь нарушена либо одной из сторон указали не подключаться (например, пользователь завершил модемное соединение.)
2. *Link Establishment Phase*. В данной фазе проводится настройка Link Control. Если настройка была успешной, управление переходит в фазу аутентификации либо в фазу Network-Layer Protocol, в зависимости от того, требуется ли аутентификация.
3. *Authentication Phase*. Данная фаза является необязательной. Она позволяет сторонам проверить друг друга перед установкой соединения. Если проверка успешна, управление переходит в фазу Network-Layer Protocol.
4. *Network-Layer Protocol Phase*. В данной фазе вызывается NCP для желаемого протокола. Например, IPCP используется для установки IP сервисов. Передача данных по всем успешно установленным протоколам также проходит в этой фазе. Закрытие сетевых протоколов тоже включается в данную фазу.
5. *Link Termination Phase*. Фаза закрытия соединения. Вызывается в случае

ошибок аутентификации, если было настолько много ошибок контрольных сумм, что обе стороны решили закрыть соединение, если соединение неожиданно оборвалось, либо если пользователь отключился.

Протоколы аутентификации:

- ***PAP (Password Authentication Protocol)*** — протокол простой проверки подлинности, предусматривающий отправку имени пользователя и пароля на сервер удалённого доступа открытым текстом (без шифрования). PAP передает незашифрованные ASCII коды по сети и поэтому крайне небезопасен, поскольку пересылаемые пароли можно легко читать в пакетах, которыми обмениваются стороны в ходе проверки подлинности. Обычно PAP используется только при подключении к старым серверам удалённого доступа на базе UNIX, которые не поддерживают никакие другие протоколы проверки подлинности.
- ***CHAP (Challenge Handshake Authentication Protocol)*** — протокол аутентификации с косвенным согласованием. Является алгоритмом проверки подлинности и предусматривает передачу не самого пароля пользователя, а косвенных сведений о нём. Аутентификация узла выполняется путём трехэтапной процедуры согласования:
    1. После установления PPP-соединения и одобрения обеих сторон на подключение по CHAP-протоколу аутентификатор отправляет на узел CHAP-пакет Challenge (вызов), который содержит в себе открытый ключ.
    2. Узел на основе полученного открытого ключа и своего секрета, вычисляет хеш с помощью алгоритма хеширования MD5 и отправляет CHAP-пакет Response (отклик), содержащий в себе вычисленный хеш.
    3. Аутентификатор сравнивает полученное значение хеша со своим расчётом ожидаемого значения хеша. Если значения совпадают, то проверка подлинности считается успешной. При отличающихся значениях происходит разрыв соединения.

  Через различные промежутки времени аутентификатор посылает новый запрос узлу, и шаги 1-3 повторяются.
- ***EAP (Extensible Authentication Protocol)*** — протокол аутентификации, который часто используется в беспроводных сетях и соединениях точка-точка. Впервые описан в RFC 3748 и обновлён в RFC 5247. Используется для выбора метода аутентификации, передачи ключей и обработки этих ключей подключаемыми модулями называемыми методами EAP. Существует множество методов EAP, как определенных вместе с самим EAP, так и выпущенных отдельными производителями. В процессе аутентификации можно выделить три основных участника процесса:
    1. *Аутентификатор* (authenticator) — участник процесса требующий провести аутентификацию.
    2. *Узел* или *клиент* (peer) — участник процесса который будет аутентифицирован.
    3. *Сервер аутентификации* (authentication server) — участник процесса способный по некоторым данным от узла аутентифицировать его.

Процесс аутентификации происходит следующим образом:

1. Аутентификатор отправляет EAP-запрос для начала аутентификации клиента с указанием метода аутентификации (EAP-TLS, EAP-PSK, ...).
2. Клиент посылает аутентификатору EAP-ответ.
3. Аутентификатор посылает запрос серверу аутентификации, передавая информацию о том, какой метод аутентификации используется.
4. Сервер аутентификации запрашивает у клиента необходимую информацию через аутентификатор, выполняющий роль посредника.
5. Клиент отвечает серверу, передавая запрашиваемую информацию. Пункты 4 и 5 повторяются до тех пор, пока сервер аутентификации не примет решение о разрешении доступа, запрете или ошибке.
6. Сервер аутентификации посылает аутентификатору пакет сообщающий о успехе или сбое аутентификации.
7. Аутентификатор посылает клиенту EAP пакет с кодом соответствующим ответу сервера аутентификации (успех или ошибка).

Протокол PPTP

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. PPTP помещает кадры PPP в IP-пакеты для передачи по глобальной IP-сети, например Интернет. PPTP может также использоваться для организации туннеля между двумя локальными сетями. PPTP использует дополнительное TCP-соединение для обслуживания туннеля.

PPTP работает, устанавливая PPP сессию с противоположной стороной с помощью протокола Generic Routing Encapsulation. Второе соединение на TCP-порту 1723 используется для инициации и управления GRE-соединением. PPTP сложно перенаправлять за сетевой экран, так как он требует одновременного установления двух сетевых сессий. PPTP-трафик может быть зашифрован с помощью MPPE (Microsoft Point-to-Point Encryption), который использует RSA+RC4. Для аутентификации клиентов могут использоваться различные механизмы, наиболее безопасные из них — MS-CHAPv2 и EAP-TLS.

PPTP удалось добиться популярности благодаря тому, что это первый протокол туннелирования, который был поддержан корпорацией Microsoft (использована лицензированная реализация от Cisco). Все версии Microsoft Windows, начиная с Windows 95 OSR2, включают в свой состав PPTP-клиент, однако существует ограничение на два одновременных исходящих соединения. В Linux-дистрибутивах полная поддержка MPPE появилась в ядре 2.6.13 (2005 год). Официально поддержка PPTP была начата с версии ядра Linux 2.6.14.

PPTP был объектом множества анализов безопасности, в нём были обнаружены различные серьёзные уязвимости. Известные относятся к используемым протоколам аутентификации PPP, устройству протокола MPPE и интеграции между аутентификациями MPPE и PPP для установки сессионного ключа.

Оборудование для организации защищенных VPN

Криптомаршрутизатор или криптошлюз — аппаратно-программный комплекс криптографической защиты трафика данных, голоса, видео на основе шифрования пакетов по протоколам семейства IPsec при установлении соединения, соответствующий требованиям к средствам криптографической защиты информации (СКЗИ) ФСБ России и обеспечивающий базовую функциональность современного VPN-устройства.

Базовый функционал современного VPN-устройства:

1) конфиденциальность и целостность потока IP-пакетов;
2) маскировка топологии сети за счет инкапсуляции трафика в защищённый туннель;
3) прозрачность для NAT;
4) аутентификация узлов сети и пользователей;
5) унификация политики безопасности для мобильных и «внутренних» пользователей (динамическое конфигурирование корпоративных IP-адресов для удаленных пользователей «внутри VPN»).

Криптошлюзы представлены как в сегменте VPN устройств, так и в сегменте унифицированных устройств (UTM) объединяющих несколько средств безопасности в одном.

Отличие криптошлюзов от обычных VPN маршрутизаторов заключается в том, что они работают на основе протокола IPSec и обеспечивают защиту информации, передаваемой по каналам связи, используя алгоритмы, которые отвечают требованиям российских криптографических стандартов (ГОСТ 28147-89, ГОСТ Р 34.10-2001 и др.).

Программное обеспечение для организации VPN

OpenVPN

OpenVPN — свободная реализация технологии виртуальной частной сети (VPN) с открытым исходным кодом (GPL) для создания зашифрованных каналов типа точка-точка или сервер-клиенты между компьютерами. Позволяет устанавливать соединения между компьютерами, находящимися за NAT и сетевым экраном, без необходимости изменения их настроек. Создана Джеймсом Йонаном (James Yonan). Для обеспечения безопасности управляющего канала и потока данных OpenVPN использует библиотеку OpenSSL. OpenVPN используется в операционных системах Solaris, OpenBSD, FreeBSD, NetBSD, GNU/Linux, Apple Mac OS X, QNX, Microsoft Windows, Android, iOS.

Аутентификация:

1. Предустановленный ключ — самый простой метод.

2. Сертификатная аутентификация — наиболее гибкий в настройках метод.
3. С помощью логина и пароля — может использоваться без создания клиентского сертификата (серверный сертификат всё равно нужен).

После установки успешного VPN-подключения IP-адрес клиента изменяется на IP-адрес сервиса OpenVPN.

Главным недостатком OpenVPN является низкая производительность при большом числе работающих через него устройств.

Hamachi (LogMeIn Inc.)

Hamachi — программное обеспечение, предназначенное для построения VPN. Чаще всего Hamachi-сети используются для соединения серверов с серым IP и клиентских компьютеров. Любые приложения, которые работают через локальную сеть, могут работать через сети Hamachi, при этом передаваемые данные будут защищены, и обмен между ними осуществляется в стиле peer-to-peer либо через серверы компании.

Организация VPN основана на протоколе UDP. В такой сети узлы для установления соединения между собой используют третий узел, который помогает им обнаружить друг друга. Передача информации может производиться непосредственно между узлами. При этом взаимодействующие узлы могут находиться за NAT или фаерволом.

Чаще всего используется игроками для игры в старые игры по интернет. Обычно при отсутствии частного IP адреса. Также может использоваться для удаленного управления при использовании Windows-based инфраструктуры.

WireGuard

Новое открытое (GPLv2) приложение и одноименный протокол, запускаемый как модуль ядра Linux. Предполагается, что он обеспечит большую производительность, чем IPsec и OpenVPN. Использует современную криптографию: Noise protocol framework, Curve25519, ChaCha20, Poly1305, BLAKE2, SipHash24, HKDF и т.д. Основан на протоколе UDP.

Список источников

1. Материалы с сайта wikipedia.org
2. Методы и средства криптографической защиты информации: Учебное пособие / О. Н. Жданов, В. В. Золотарев; СибГАУ. – Красноярск, 2007. – 217 с.
3. Telecommunication technologies — телекоммуникационные технологии / Ю. А. Семенов. URL: http://book.itep.ru/1/intro1.htm
4. WireGuard — прекрасный VPN будущего? / supervillain. С сайта Habr.com. URL: https://habr.com/ru/post/432686/