6. Виртуални частни мрежи

Гласът, видео сигналите и данните, обикновено изпращани между отдалечени офиси и централни местоположения често изискват ниска латентност и лесно осигуряване, като при това трябва да се осигури и ниска цена. Традиционните решения с WAN (например, наети линии, Frame Relay и ATM) обикновено не отговарят едновременно на всички тези изисквания. За щастие в подобна конструкция попадат множество различни технологии за VPN. Те представляват нов прочит на една доста стара концепция. X.25 пакетно комутиращите мрежи от години осигуряват на компаниите софтуерно дефинирана защитена мрежа в рамките на голяма обществена комутируема мрежа. Обществената комутируема мрежа се притежава и поддържа от телекомуникационен оператор, а потребителите имат средства за достъп. Всеки потребител може да използва мрежата като своя собствена частна мрежа и никога трафика не достига до другите потребители. X.25 мрежата осигурява функционалността на частна мрежа, без разходите по изграждането и поддържането на такава.

VPNs представляват ново приложение на този стар X.25 подход, Основната разлика е, че те използват много по-модерни средства за пренос и мрежови протоколи. Още по-важно, те се използват по различен начин за различни бизнес цели. VPNs са идеални за всяка ситуация, където не е ценово ефективно изграждането на частно притежавана мрежа, например:

- Компания с мобилни служители;
- Малки компании, които не могат да си позволят разходите по изграждането на своя собствена комуникационна мрежа.

VPNs могат да бъдат закупени от телекомуникационен оператор по същия начин, както старата X.25 услуга. Алтернативно, те могат да бъдат създадени чрез използването на съществуваща мрежова инфраструктура като Интернет или обществена комутируема телефонна мрежа с използването на тунелен софтуер.

6.1. Тунелиране

Тунелирането е процес, при който комуникацията се извършва по логическа структура, създадена от друг протокол за комуникация. Това може да реши няколко различни мрежови проблема от необходимостта за

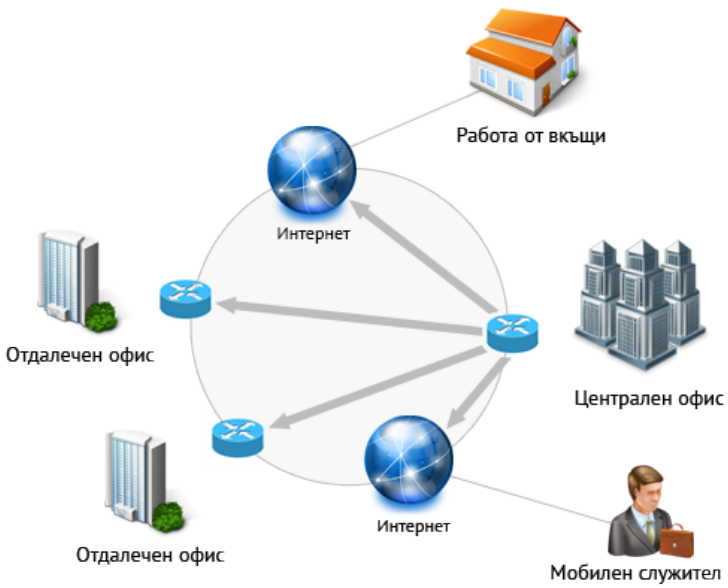
защита на данните по време на техния пренос, до преодоляване на несъвместимостта между протоколи или адресиране.

Тунел е виртуална връзка, която може физически да се разпространи по няколко скока през маршрутизатори. Но от гледна точка на трафика, преминаващ през тунела, преходът от единия край на тунела до другия край изглежда като един скок през маршрутизатор. Независимо от това какви протоколи се използват и каква е цената на тунела, базовата техника е относително постоянна. Обикновено за установяване на връзка към отдалеченото място се използва един протокол, а за енкапсулиране на данни и инструкции за пренос по тунела се използва друг протокол.

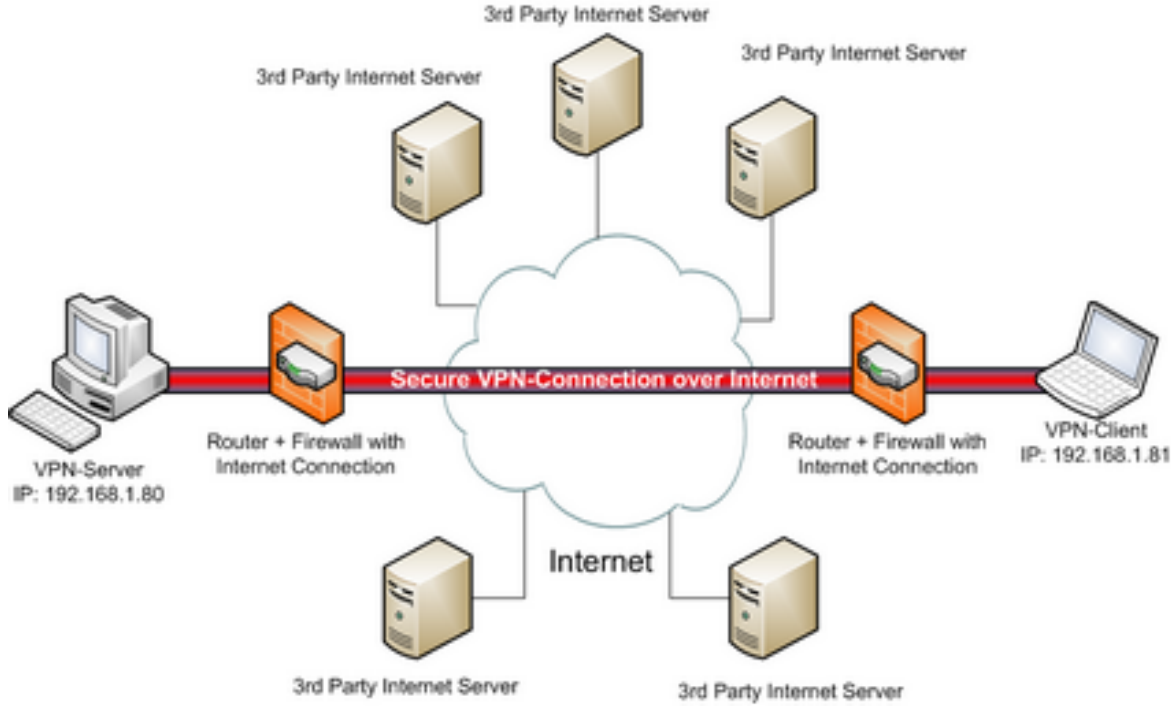
Пример за използването на тунел за преодоляване на несъвместимостта между протоколи и адреси е SIT (Simple Internet Transition) комплекта, придружаващ IPv6. Един от инструментите в този комплект служи за улеснение на миграцията от IPv4 към IPv6 чрез тунел. Двете версии на IP не са директно съвместими. Съвместим та се осигурява чрез тунелирането на IPv4 по IPv6 и обратно.

Тунелирането осигурява и защитата на данните при преминава им през незащитен район, осигурявайки им защитна обвивка. Един от протоколите, създаден специално за тази цел е PPTP.

6.2. Виртуални частни мрежи.



При виртуалните частни мрежи – VPNs (Virtual Private Networks) се изгражда тунел за предаване на съобщенията през глобалната мрежа Интернет. Данните се изпращат чрез глобалната мрежа по модела от тип „от точка до точка" - Point-to-Point (PPP). Това се постига чрез капсулиране на данните и по този начин се създава логическа независима мрежа от местоположението на крайните точки, в които се поддържа автентификация. Предаваните съобщения по тунелите се защитават с криптиране. Криптирането на съобщенията е от голямо значение, в противен случай всеки може да ги прихване по време на пътуването през обществената интернет мрежа между предаващата и приемащата крайна точка на тунела.



VPN технологията позволява да се създаде логическа мрежа, която е независима от местоположението на служителите или клиентите и създава условия за установяване на директна информационна връзка между тях. За разлика от използването на скъпи системи от наети линии, които могат да бъдат използвани само от една организация, VPN мрежата предоставя на организациите еднакви възможности на много по-ниска цена, което е голямо предимство. VPN мрежата работи с криптиран трафик, преминаващ през несигурната интернет среда и е значително евтина алтернатива спрямо използването на наети линии за изграждане на частна мрежа за дадена организация. VPN мрежите се използват за осигуряване на отдалечен достъп до мобилни служители, осигуряване на екстранет мрежа с достъп до нейни

клиенти или за осигуряване на връзка между два офиса в различни местоположения. VPN мрежите използват надеждно защитени тунели, в средата на Internet за връзка между две мрежи и обмен на данни между тях.

Принцип на работа на VPN мрежите

Виртуалните компютърни мрежи използват два вида канали за предаване на данните: комутируеми канали (dial-up) и наети канали от типа „маршрутизатор до маршрутизатор". И за двата типа мрежи се изисква конфигуриране и настройка на мрежите от администратор.

Изграждането на тунел през глобална компютърна мрежа е свързано със създаване на логическа връзка между две крайни точки, в които се поддържа автентификация и криптиране на данните от едната до другата страна. Тунелирането е термин, използван за описание на капсулацията, маршрутизация и декапсулация на пакетите. Капсулирането представлява скриване на оригиналния пакет в нов пакет, който се използва за маршрутизирането през тунела, т.е. в хедъра на новия пакет се задава адреса на крайната точка от тунела, в хедъра на оригиналния пакет се намира адреса на възела получател, който остава криптиран до пристигането му в крайната точка на мрежата.

VPN мрежата позволява на локалните частни мрежи намиращи се в различни географски региони физическо свързване към мрежата на дадена организация посредством VPN сървър. Администраторът на VPN мрежата разрешава на някои от работните станции на локалните мрежи връзка с VPN сървъра. Само потребители, които имат достъп до виртуалната мрежата на организацията могат да ползват защитените ресурси на конфигурираната частна виртуална мрежа. Тези потребители получават акредитивни писма за достъп, а останалите не виждат локалната мрежа и нямат достъп до общите ресурси.

Във VPN мрежите се използват три типа протоколи:

- Тунелни протоколи - понякога означавани като VPN протоколи, те се използват за изграждане на тунели;
- Протоколи за криптиране - означавани като протоколи за сигурност, използват се за криптиране на данните;

- Мрежови/транспортни протоколи - означавани още като LAN протоколи, използват се за комуникация на съобщенията по частната мрежа.

Тунелните протокол капсулират данните така, че хедърите на протоколните единици от оригиналния протокол се обвиват в тунелни капсулиращите хедъри.

Тунелиране на каналния слой на OSI модела

VPN мрежите използват тунелни протоколи, работещи в каналния слой. Тези протоколи осигуряват виртуална връзка от сървъра до клиента. Могат да се използват различни протоколи за изграждане на тунела на каналния слой на възлите от мрежата.

Протоколът Point-to-Point Tunneling Protocol (PPTP) работи на каналния слой на OSI модела. Освен него може да се използват и други тунелни протоколи на този слой, като Layer 2 Forwarding (L2F), който осигурява тунелиране по глобалните компютърни мрежи от стандартите ATM и Frame Relay. За разлика от тунела изграден от протокола PPTP, протоколът L2F поддържа повече от една връзка между крайните абонати. VPN мрежите функциониращи в каналния слой на OSI модела използват и двата протокола (PPTP и L2TP). Протоколът PPTP е по-стар, използва се главно за отдалечен достъп, функционира в режим клиент-сървър. Клиентската част може да бъде отдалечен хост с инсталиран PPTP протокол или сървър за мрежов достъп с разрешение за функциониране на протокола PPTP от страна на доставчика на Интернет. Реализацията на сървърната част може да е рутер, специализиран VPN концентратор или приложен сървър. Протоколът PPTP капсулира PPP пакети в модифицирана версия на протокола GRE (Generic Routing Encapsulation), който ги транспортира през мрежата. Той представлява механизъм за капсулиране на произволен протокол от мрежовия слой към друг такъв протокол. Протоколът PPTP може да се използва за транспортиране на протоколни единици на протоколи като IP, IPX и NetBEUI. Той разчита на автентифициращите механизми на протоколите PPP – PAP (Password Authentication Protocol) и CHAP (Challenge Handshake Authentication Protocol), които не се считат за особено сигурни. Протоколът PAP изпраща паролите като чист текст – т.е. паролите остават незащитени по време на предаване на пакетите по обществената мрежа. Протоколът CHAP е по-сигурен от PAP, той изпраща един вид

„покана” (challenge), на която другата страна трябва да отговори, за да се автентифицира. Microsoft създава разширена версия на протокола CHAP, наречена MS-CHAP. PPTP криптира данните, използвайки 128-битов ключ, който го поставя в най-слабата категория VPN протоколи.

Протоколът L2TP (Layer 2 Tunneling Protocol) се разглежда, като заместник на PPTP и се счита като по-надежден. Протоколът L2TP също функционира в режим клиент-сървър и подобно на PPTP, L2TP тунелът може да бъде иницииран от отдалечен компютър към LNS (L2TP network server) или от LAS (L2TP-enabled access концентратор) към LNS. L2TP дефинира свой собствен тунелиращ протокол, в зависимост от транспортната среда, като не използва протокола GRE. L2TP може да се използва за функционирането на протоколи от мрежовия слой, различни от IP, но не всички версии го поддържат. L2TP може да използва протоколите PAP, CHAP и EAP за автентикация. L2TP се счита за по-сигурен вариант от PPTP, тъй като IPSec протоколът, който съдържа по-сигурни алгоритми за кодиране, се използва заедно с него. Той също така изисква предварително споделен сертификат или ключ. Най-силното ниво на криптиране на L2TP използва клавиши с 168 битове, алгоритъм за криптиране DES 3 и изисква две нива на удостоверяване.

Тунелиране на мрежовия слой на OSI модела

Тунели могат да се създават и в мрежовия слой на OSI модела, като по този начин се осигуряват IP-базирани виртуални връзки. Те работят чрез изпращане на IP пакети, капсулирани във вътрешността на специфицирани от IETF (Internet Engineering Task Force) протоколни обвивки. Използват се IPSec (IPSecurity), IKE (Internet Key Exchange) методи за автентикация и криптиране, като DES (Data Encryption Standard) и Secure SHA (Hash Algorithm). IPSec може да бъде използван заедно с протокола L2TP, който изгражда тунела, а IPSec криптира данните. По този начин IPSec работи в транспортен режим. Той може също да бъде използван и в тунелен режим, при който осигурява тунела. Една важна особеност е тази, че IPSec може да капсулира само IP пакети. L2TP може да осигурява капсулиране на IPX (Internetwork Packet Exchange) пакети и на пакети на други протоколи по IP мрежа. Някои от шлюзовете не поддържат VPN мрежи, базирани на L2TP или PPTP, като в този случай за осигуряване на тунела се използва IPSec. Тези тунелите обикновено работят от шлюз до шлюз.

VPN изградени на мрежовия слой на OSI модела обикновено са такива мрежи, използващи IP протокола като протокол от мрежовия слой. VPN от мрежовия слой използват комуникациите MPLS (Multiprotocol Label Switching) и IPSec.

MPLS обикновено се предлага като тип връзка site-to-site VPN услуга от ISP. Доставчикът построява частна IP-базирана мрежа и предлага връзка на множество клиенти между техните местоположения в мрежата. Технологията позволява на отделни клиенти да гледат на MPLS услугата като на частна IP мрежа свързваща различните им местоположения. По този начин се предлагат на клиентите предимства като частните мрежи от каналния слой, като при стандартите Frame Relay и ATM, но с възможност за лесното управление на мрежите от мрежовия слой. Тъй като MPLS функционира чрез частна IP-базирана мрежа вместо Internet, доставчикът може да предостави обособени нива на услугите на своите клиенти: QoS (Quality of Service – качество на услугите) и SLA (Service-level Agreements – споразумения за нивата на услугите). MPLS е базирана на частна мрежа на определен доставчик, достъпността на услугата е ограничена до обхвата, в който функционира доставчика.

Изисквания към VPN мрежите

Необходимо да се осигури контролиран достъп на отдалеченото мрежово решение до ресурсите и информацията на организацията, тъй като се разрешава се на отдалечения клиент да се свързва към ресурсите на локалната мрежа. Решението трябва да позволява на отдалечените офиси да се свързват един с друг, да споделят ресурси и информация, да се осигурява цялостност и неделимост на данните при преминаването им през Интернет. VPN решението трябва да отговаря на следните изисквания:

- Автентификация на потребителя – проверка на идентичността на VPN клиента, ограничаване на VPN достъпа само на упълномощени потребители;
- Управление на адресите;
- Криптиране на данните - данни трябва да се пренасят криптирани през Интернет;
- Управление на ключовете за криптираните данни.

VPN мрежи за отдалечен достъп

Използването на VPN за осигуряване на отдалечен достъп до потребители е най-често използвания метод за изграждане. Реализацията може да бъде усложнена от фактори като: използване на различни операционни системи и протоколите, които са инсталирани от страната на клиентите.

VPN клиентът трябва да може да използва протоколи, поддържани от VPN сървъра - тунелни, мрежови и транспортни протоколи както и протоколи за криптиране. След инсталиране и конфигуриране на компонентите на VPN, се установява връзката. Редът за изграждане и пускане в експлоатация на такава мрежа е следният:

- Мобилният потребител набира локален ISP (Internet Server Provider) доставчик и влиза с потребителски акаунт и парола, за да изгради интернет връзка, ако клиентът използва наета или постоянна връзка. При наличие на постоянна интернет свързаност тази стъпка се пропуска.
- Клиентът изпраща заявка за свързване със сървъра за отдалечен достъп, конфигуриран да приема VPN връзки, като използва IP адреса му.
- Потребителят трябва да се автентифицира в частната мрежа, за да му се разреши определен достъп и права.

Когато към част от LAN мрежата на организацията или на определеното нейно звено се разреши достъп на отдалечени потребители по VPN връзка, тогава създаваме виртуален частен екстранет. Един от основните проблеми е защитата на останалата част от вътрешната мрежа от външен достъп. Създава се отделна подмрежа за екстранет мрежата, а останалата част от LAN мрежата се скрива зад защитна стена, за да може да и се осигури необходимата защита.

VPN връзки между филиални офиси

При свързването на различни офиси се използва виртуална частна мрежа във VPN конфигурация от тип маршрутизатор-маршрутизатор. VPN сървърът може да функционира като маршрутизатор с разрешено IP препращане.

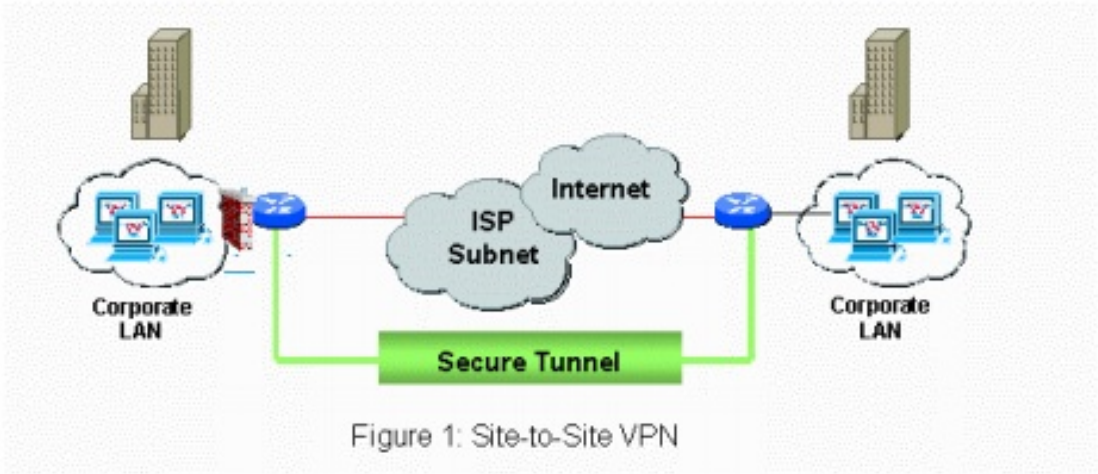


Figure 1: Site-to-Site VPN

VPN връзки от типа маршрутизатор-маршрутизатор може да бъде конфигурирани така, че единият маршрутизатор да действа като клиент и да инициира връзката, а другият да функционира като VPN сървър. По този начин се реализира еднопосочна връзка и представлява добър избор за постоянни връзки. При двупосочната връзка всеки от маршрутизаторите може да инициира връзката. В този случай и двата маршрутизатора трябва да имат постоянна връзка към Интернет и трябва да бъдат настроени като LAN и WAN маршрутизатори.

При връзката маршрутизатор-маршрутизатор, маршрутните таблици и на двата маршрутизатора трябва да бъдат конфигурирани с необходимите маршрути, за да препращат пакети през връзката. Маршрутите могат да бъдат добавени ръчно или може да бъде използван протокол за динамична маршрутизация, ако интерфейсът за набиране има постоянна връзка.

Класификация на VPN мрежите

VPN мрежата може да бъде реализирана софтуерно или хардуерно. Софтуерно-базираните VPN мрежи включват използването на разгледаните по-горе тунелните протоколи. Тази категория може да бъде разделена допълнително на продукти на независими производители и VPN софтуер, поддържан от операционната система. Очевидното предимство на последните е тяхната ниска цена. Няма допълнително заплащане, а VPN решенията, включени в модерните операционни системи са достатъчни за нуждите на много организации.

VPN софтуерните продукти на независимите производители обикновено предлагат допълнителни възможности и разширяват използваемостта на VPN, като често осигуряват повече опции за сигурност и в някои случаи по-лесно реализиране. Някои софтуерно-базирани VPN мрежи позволяват да се предават данни в тунела на базата на протокола или IP адреса. Този тип филтриране обикновено не е достъпен при хардуерно-базираните продукти. Продуктите на независимите производители включват Safeguard VPN, Checkpoint SVN (Secure Virtual Networking) и NetMAX VPN Suite за операционна система Linux.

Хардуерно-базираните VPN мрежи се произвеждат от компании като Shiva, 3Com и VPNet Technologies. Поддръжката на VPN е вградена в маршрутизаторите на Cisco, както и в маршрутизаторите на други компании. NTS Tunnel-Builder осигурява сигурни VPN комуникации за Windows, NetWare и Macintosh. Такива производители като Raptor Systems предлагат VPN мрежи, базирани на защитни стени, които са комбинирани със средства за сигурност. Хардуерните VPN мрежи могат най-общо да бъдат категоризирани в следните две групи:

- Базирани на маршрутизатори - VPN решения представляващи маршрутизатори с възможности за криптиране. Те предлагат по-добра производителност на мрежата и като цяло са по - лесни за инсталиране и използване;
- Базирани на защитна стена - осигуряват допълнителни мерки за сигурност, като сигурна автентификация и детайлно логване. Базираната на VPN защитна стена има възможност да преобразува адреси. Производителността и може да бъде проблем, макар че в някои реализации хардуерните криптиращи процесори решават тази задача.

Надеждност и сигурност на VPN мрежите

Надеждността на една система се определя от надеждността на най-слабия и елемент. Ето защо не е необходимо да се атакуват използваните криптографски алгоритми. Достатъчно е да се атакува един от компонентите на системата. Надеждността на една система зависи от:

- Условията и външната среда, в която тя работи;
- Режима на работа;

- Надеждност на елементите, от които тя е изградена;
- Вътрешната ѝ структура;
- Възстановимостта на съставните и части след отказ.

Сигурността на VPN има три компонента:

- • Автентификация на клиентите;
- • Оторизация на клиентите;
- • Криптиране на данните.

Автентификацията на VPN клиента включва проверката за истинност на самоличността на машината и на потребителя, който инициира VPN връзката. Автентификацията може да бъде осъществена на нивото на машината. Например, когато една VPN връзка, базирана на Windows 2000, използва IPSec за L2TP VPN мрежа, сертификатите на машините се обменят като част от изграждането на IPSec асоциация за сигурност. Потребителят може да бъде автентифициран с помощта на един от няколкото метода за автентификация, като Extensible Authentication Protocol (EAP), Challenge Handshake Authentication Protocol (PAP) или Shiva PAP (SPAP).

Оторизация означава зададените ограничения, на базата на които на едни потребители се предоставя достъп до VPN, а на други се отказва.

Криптирането служи за защита на данните във VPN мрежи. Могат да бъдат използвани най-различни технологии за криптиране. Много VPN реализации позволяват да се избере метода на криптиране, който трябва да бъде приложен. Криптирането осигурява сигурност на данни, които пътуват по VPN мрежата. Без тази сигурност данните биха могли лесно да бъдат прехванати, докато се предават по обществената мрежа.