VPN TECHNOLOGY

Mirolyub Tsekov, Nataliya Marinova

VPN ТЕХНОЛОГИЯ

Миролюб Цеков, Наталия Маринова

***Резюме**: Виртуалната частна мрежа (VPN) е станала почти толкова безразсъдно използвана в мрежовата индустрия, колкото и QoS (Quality of service) за описване на широк набор от проблеми и решения, когато самите цели не са правилно формулирани. В този доклад ще се опитаме да дефинираме основите на VPN.*

***Ключови думи**: vpn, мрежа, сървър, услуга, протокол, тунелиране.*

I. Въведение

VPN (виртуална частна мрежа) е услуга, която създава безопасна, криптирана онлайн връзка. Потребителите на интернет могат да използват VPN, за да си осигурят повече поверителност и анонимност онлайн или да заобиколят географско блокиране и цензура. VPN мрежите по същество разширяват частна мрежа в обществена мрежа, което би трябвало да позволи на потребителя да изпраща и получава данни в интернет.

Обикновено VPN се използва в по -малко сигурна мрежа, като например публичния интернет. Доставчиците на интернет услуги (ISP) обикновено имат доста голяма информация за дейностите на клиента. В допълнение, някои незащитени точки за достъп до Wi-Fi (AP) могат да бъдат удобен начин за нападателите да получат достъп до личните данни на потребителя. Потребителят на интернет може да използва VPN, за да избегне тези посегателства върху поверителността.

VPN могат да се използват за скриване на историята на браузъра на потребителя, адреса на Интернет протокола (IP) и географското местоположение, уеб активността или използваните устройства. Всеки в същата мрежа няма да може да види какво прави VPN потребител. Това прави VPN мрежите инструмент за онлайн поверителност.

VPN използва тунелни протоколи за криптиране на данни в изпращащия край и ги декриптира в приемащия. Изходният и получаващият мрежови адреси също са криптирани, за да осигурят по -добра сигурност за онлайн дейности.

VPN приложенията често се използват за защита на предаването на данни на мобилни устройства. Те могат да се използват и за посещение на уебсайтове, които са ограничени по местоположение. Сигурният достъп чрез мобилна VPN обаче не трябва да се бърка с частното сърфиране. Частното сърфиране не включва криптиране; това е просто незадължителна настройка на браузъра, която предотвратява събирането на идентифицируеми потребителски данни.[4]

II. История

VPN технологията е използвана за първи път през 1996 г., когато служител на Microsoft разработи PPTP. Протоколът създаде по-сигурна частна връзка между потребителско устройство и интернет. През 1999 г. спецификацията е публикувана.

В началото на 2000-те VPN мрежите бяха свързани предимно с и използвани от бизнеса. Технологията не беше използвана съвсем от средните онлайн потребители. По това време VPN се използваха от бизнеса за достъп до частни бизнес мрежи. В този случай на използване организациите са имали достъп до фирмени данни отвсякъде, докато изглеждат така, сякаш са в офиса. Стана възможно сигурното споделяне на файлове между различни офиси.

След това стандартите за криптиране започнаха да стават по-мощни и бяха разработени нови протоколи за тунелиране. Тъй като хората започнаха да научават за потенциални онлайн заплахи и проблеми с поверителността, използването на VPN се разшири до индивидуални, домашни потребители. Скандалите за поверителност, като WikiLeaks или отделните изтичания на сигурността от Едуард Сноудън, бяха инжектирани в съвременния дух. Около 2017 г. потребителите на интернет в Съединените щати научиха, че интернет доставчиците могат да събират и продават своята история на сърфиране, а неутралността на мрежата се превърна в концепция, за която гражданите трябва да се борят и на практика загуби.[1]

III. Как работят VPN мрежите?

На най-основното си ниво тунелирането на VPN създава връзка от точка до точка, която не може да бъде достъпна от неоторизирани потребители. За създаване на тунел се използва протокол за тунелиране върху съществуващи мрежи. Различните VPN ще използват различни протоколи за тунелиране, като OpenVPN или протокол за тунелиране на защитени гнезда (SSTP). Използваният протокол за тунелиране може да зависи от платформата, на която се използва VPN, като например SSTP, използвана в Windows OS, и ще осигури криптиране на данни с различна сила. Устройството на крайната точка трябва да работи с VPN клиент (софтуерно приложение) локално или в облака. Клиентът ще работи във фонов режим. VPN клиентът не се забелязва за крайния потребител, освен ако не създава проблеми с производителността.

Използвайки VPN тунел, устройството на потребителя ще се свърже с друга мрежа, скривайки своя IP адрес и криптирайки данните. Това е, което ще скрие личната информация от нападатели или други, които се надяват да получат достъп до дейностите на индивида. Тунелът ще свърже устройството на потребителя с изходен възел на друго отдалечено място, което прави впечатлението, че потребителят е на друго място. Това е показано на фигурата (фиг. №1).

Фиг. №1 – Схема на работа на VPN

VPN свързват историята на търсенията на потребителя с IP адреса на VPN сървъра. VPN услугите ще имат сървъри, разположени в различни географски области, така че ще изглежда, че потребителят може да е от някое от тези места.

VPN мрежите могат да повлияят на производителността по много начини, като скоростта на интернет връзките на потребителите, типовете протоколи, които доставчикът на VPN може да използва и вида на използваното криптиране. В предприятието ефективността може да бъде повлияна и от лошото качество на услугата (QoS) извън контрола на отдела за информационни технологии (ИТ) на организацията.

Превключвателят за убиване е функция за защита в краен случай в някои VPN продукти. Ако VPN връзката бъде прекъсната, превключвателят за убиване автоматично ще изключи устройството от интернет, за да елиминира вероятността от излагане на IP адрес. Има два вида превключватели за убиване:

1. Протоколите за активен убийствен превключвател предотвратяват свързването на устройства към опасни мрежи, когато устройството е свързано към VPN. Освен прекъсвания на сървъра, той е деактивиран, когато не е свързан с VPN.

2. Протоколите за пасивни превключватели са по -сигурни. Те предпазват устройството от свързване с връзки, които не са VPN, дори когато са изключени от VPN сървъра.[3]

IV. За какво се използват VPN?

VPN се използват за виртуална поверителност както от нормалните интернет потребители, така и от организациите. Организациите могат да използват VPN, за да се уверят, че външните потребители, които имат достъп до техния център за данни, са оторизирани и използват криптирани канали. VPN също могат да се

използват за свързване към база данни от същата организация, разположена в различна област.

VPN също могат да се използват за предоставяне на достъп до отдалечени служители, работници на свободна практика и бизнес пътници с достъп до софтуерни приложения, хоствани в собствени мрежи. За да получи достъп до ограничен ресурс чрез VPN, потребителят трябва да бъде упълномощен да използва виртуалната частна мрежа и да предостави един или повече фактори за удостоверяване. Това могат да бъдат пароли, символи за сигурност или биометрични данни.

При сърфиране в мрежата потребителят на интернет може да получи достъп до информация от нападател, включително навици за сърфиране или IP адрес. Ако поверителността е проблем, VPN може да осигури спокойствие на потребителите. Шифроването, анонимността и способността да заобикалят географски блокирано съдържание е това, което повечето потребители намират за ценни в VPN.

Възможността за заобикаляне на блокирано съдържание от друга държава, например, може да бъде изключително полезна за журналистите. Например, ако има вероятност дадена държава да блокира интернет съдържание от чуждестранни организации, журналистите биха могли да използват VPN, за да изглеждат така, сякаш са в тази държава.[4]

V. VPN протоколи

VPN протоколите осигуряват подходящо ниво на сигурност за свързаните системи, когато основната мрежова инфраструктура сама по себе си не може да го осигури. Няколко различни протокола могат да се използват за защита и криптиране на данни. Те включват следното:

- IP защита (IPsec)
- Слой със защитени гнезда (SSL) и защита на транспортния слой (TLS)
- Протокол за тунелиране от точка до точка (PPTP)
- Протокол за тунелиране на слой 2 (L2TP)
- OpenVPN

Предимствата от използването на VPN включват следното:

- възможност за скриване на IP адреса на потребителя и историята на сърфиране;
- защитени връзки с криптирани данни;
- заобикаляне на гео-блокирано съдържание; и
- затруднявайки рекламодателите да насочват реклами към физически лица.

Предизвикателствата при използването на VPN обаче включват следното:

- Не всички устройства могат да поддържат VPN.
- VPN мрежите не защитават от всяка заплаха.
- Платените VPN мрежи са по -надеждни и сигурни опции.

- VPN може да забави скоростта на интернет.
- Анонимността чрез VPN има някои ограничения - например все още може да се направи отпечатък от браузъра.

Всяко устройство, което осъществява достъп до изолирана мрежа чрез VPN, представлява риск от пренасяне на зловреден софтуер в тази мрежова среда - освен ако в процеса на VPN връзка няма изискване за оценка на състоянието на свързващото устройство. Без проверка за установяване дали свързващото устройство отговаря на политиките за сигурност на организацията, нападателите с откраднати идентификационни данни могат да получат достъп до мрежови ресурси, включително комутатори и рутери.
Освен VPN, експертите по сигурността препоръчват на мрежовите администратори да обмислят добавяне на софтуерно дефинирани периметърни (SDP) компоненти към своята инфраструктура за защита на VPN, за да се намалят потенциалните повърхности на атака. Добавянето на програмиране на SDP дава на средните и големите организации възможността да използват модел с нулево доверие за достъп както до локални, така и до облачни мрежови среди.[4]

VI. Видове VPN

Мрежовите администратори имат няколко възможности, когато става въпрос за разполагане на VPN, които включват следното:

- VPN за отдалечен достъп

Клиентите за отдалечен достъп се свързват към VPN шлюз сървър в мрежата на организацията. Порталът изисква устройството да удостовери самоличността си, преди да предостави достъп до вътрешни мрежови ресурси. Този тип обикновено разчита на IPsec или SSL за защита на връзката.

- VPN от сайт на сайт

За разлика от това, VPN от сайт на сайт използва шлюзово устройство за свързване на цяла мрежа на едно място с мрежа на друго място. Устройствата с краен възел в отдалеченото място не се нуждаят от VPN клиенти, защото шлюзът обработва връзката. Повечето VPN сайтове към сайт, свързващи се през интернет, използват IPsec. Също така е обичайно те да използват връзки за многопротоколно превключване на етикети (MPLS) на превозвача, а не публичния интернет като транспорт за VPN от сайт до сайт. Възможно е да има или Layer 3 свързаност (MPLS IP VPN) или Layer 2 (виртуална частна локална мрежова услуга), работещи през базовите транспортни връзки.

- Мобилен VPN

В мобилна VPN сървърът все още се намира на ръба на мрежата на организацията, което позволява защитен тунелен достъп от удостоверени, оторизирани клиенти. Мобилните VPN тунели обаче не са свързани с физически IP адреси. Вместо това всеки тунел е свързан с логически IP адрес. Този логически IP адрес остава на мобилното устройство. Ефективната мобилна VPN предоставя непрекъснато

обслужване на потребителите и може да превключва между технологии за достъп и множество публични и частни мрежи.

- Хардуерен VPN

Хардуерните VPN предлагат редица предимства пред софтуерно базирани VPN. Освен че предлагат подобрена сигурност, хардуерните VPN мрежи могат да осигурят балансиране на натоварването за големи натоварвания на клиенти. Администрирането се управлява чрез интерфейс на уеб браузър. Хардуерният VPN е по-скъп от софтуерния. Поради цената, хардуерните VPN мрежи са по - жизнеспособни за по -големия бизнес. Няколко доставчици предлагат устройства, които могат да функционират като хардуерни VPN.

- VPN уред

Устройство за VPN, известно още като устройство за VPN шлюз, е мрежово устройство с подобрени функции за сигурност. Известен също като SSL VPN уред, той е рутер, който осигурява защита, оторизация, удостоверяване и криптиране за VPN.

Динамична многоточкова виртуална частна мрежа (DMVPN)

DMVPN обменя данни между сайтове, без да е необходимо да преминава през VPN сървър или рутер на централата на организацията. DMVPN създава мрежова VPN услуга, която работи на VPN рутери и концентратори на защитна стена. Всеки отдалечен сайт има рутер, конфигуриран да се свързва с устройството на централата на компанията (хъб), осигуряващ достъп до наличните ресурси. Когато са необходими две спици за обмен на данни помежду си - например за гласово IP (VoIP) телефонно обаждане - спицата ще се свърже с хъба, ще получи необходимата информация за другия край и ще създаде динамичен IPsec VPN тунел директно между тях.[4]

VII. Доставчици и продукти на VPN

VPN услугите се предлагат като безплатни или платени опции. Опциите за платени доставчици обаче се препоръчват по -често от безплатните. Някои доставчици на VPN, сред многото, включват следното:

- NordVPN съдържа силна колекция от защитни функции с голяма колекция от сървъри. NordVPN има функции като връзки с браузъра Tor за анонимно сърфиране в мрежата, като същевременно поддържа силна позиция по отношение на поверителността на клиентите.
- VPN за частен достъп до интернет е приложение за iOS и Android, което може да поддържа до 10 различни едновременни връзки. Той обаче не предлага твърде много по отношение на допълнителни функции и инструменти за поверителност. Все пак обикновено се счита за добра VPN услуга.
- ExpressVPN е VPN услуга с голям и разнообразен набор от разпределени сървъри. Той има силни практики за поверителност и информация, фокусирани върху сигурността и предлага допълнителни функции, като

например разделено тунелиране. Той също така използва протокола OpenVPN.[5]

VIII. Как да изберем VPN

VPN мрежите са законни в Съединените щати, но потребителите и организациите трябва да проверят дали са законни в определени държави. Много VPN предлагат изключително сходни технологии, така че може да е трудно да изберете кой VPN ще работи най -добре. Платените VPN услуги са по -доверени и включват повече функции за сигурност. Уважаемите VPN услуги ще бъдат наясно с тяхната сигурност, техните силни и слаби страни и тяхната прозрачност, като например ще пуснат одити на трети страни. Допълнителните VPN функции включват разделено тунелиране, достъп до мрежата Tor или връзки с много магазини.

След като хората разгледат добавените функции и намерят услуга, която смятат, че ще им свърши работа, е добра идея да започнете с краткосрочен абонамент. Много доставчици предлагат безплатни пробни версии на платените си версии. Някои безплатни пробни версии могат да включват ограничение за това колко данни могат да бъдат използвани.[5]

References

1. Charlie Scott, Paul Wolfe and Mike Erwin," Virtual Private Networks ", Second Edition January 1999.

2. Martin W. Murhammer, Orcun Atakan, Zikrun Badri, Beomjun Cho Hyun Jeong Lee, Alexander Schmid, " A Comprehensive Guide to Virtual Private Networks, Volume III: Cross- Platform Key and Policy Management", November 1999 .

3. How Virtual Private Networks Work by Jeff Tyson http://computer.howstuffworks.com/vpn.htm

4. Virtual Private Networks by Shamod Lacoul http://www.slidefinder.net/V/Virtual_Private_Networks_Shamod_Lacoul/32104518

5. Roy Hills, " Common VPN Security Flaws", January 2005.