SocioBrains

ISSN 2367-5721 (online), JOURNAL HOMEPAGE: WWW.SOCIOBRAINS.COM
Publisher: SMART IDEAS – WISE DECISIONS, Ltd., Sofia, Bulgaria

ISSUE 71, JULY 2020

DEVELOPMENT OF A VIRTUAL PRIVATE NETWORK IN COMPUTER NETWORKS AND COMMUNICATION ENVIRONMENTS

Abstract: Nowadays, hiding and encrypting information is one of the most common things. This is where the creation of virtual private networks lies. In this paper the creation of a virtual private network is explained, as well as the characterization of this type of network.

Author information:

Daniel Denev
PhD student
Faculty of Technical Sciences
at Konstantin Preslavsky – University of Shumen
✉ slimshady33@abv. bg
Bulgaria

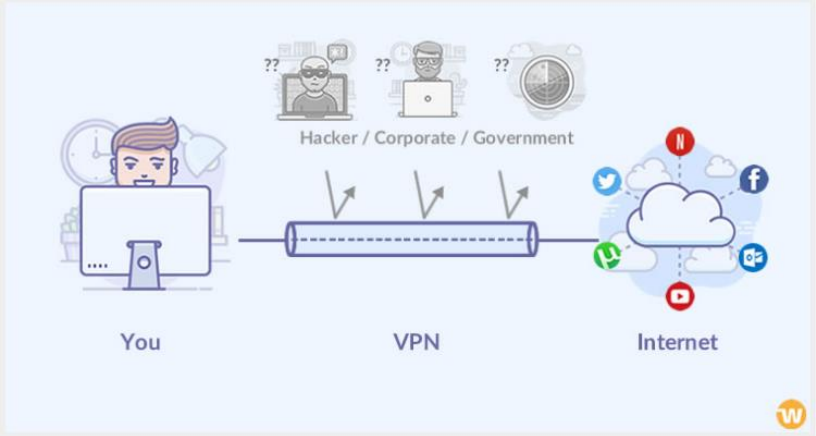
Tsvetoslav Tsankov
Assoc. prof. Eng., PhD
Faculty of Technical Sciences
at Konstantin Preslavsky – University of Shumen
✉ c.cankov@shu.bg
Bulgaria

Keywords:
Communication, Computer Networks, Virtual Private Network.

1. Въведение

Компютърната виртуална частна мрежа (VPN – VirtualPrivateNetwork) е специфична компютърна мрежа, реализираща се чрез технология, при която на потребителите се осигурява отдалечен достъп до локални мрежови ресурси чрез използване на глобалната комуникационна инфраструктура. Адаптирането и оптимизацията на взаимодействието между технически и иновационни процеси и тяхното отражение върху обществото би могло да даде съществен принос за конкурентоспособността и продуктивността на българската икономика [4].

По този начин индивидуален отдалечен потребител (RemoteUsers) или потребител от дадена отдалечена локална мрежа (Remote LAN) може да получи достъп до мрежовите ресурси на друг индивидуален потребител или друга локална мрежа, която се намира на голямо разстояние, като при това комуникацията изглежда така, сякаш свързаните потребители са разположени в една и съща локална мрежа,т. е. сякаш са в непосредствена близост, например в една и съща сграда (фиг. 1).



Фиг. 1. VPN мрежа

VPNмрежите се осъществяват в няколко топологични варианта:

— Host-to-Host;

— Host-to-Site;

— Site-to-Site.

За да се реализира една VirtualPrivateNetwork е задължително да се използват 3 основни технологични условия [1], [2], [3]:

— да се изгради виртуален комуникационен тунел чрез който ще се свързват отдалечените потребители;

— потребителите да получават „Автентикация“, чрез нея ще добиват достъп до отдалечените мрежови ресурси;

— тунелите да притежават криптиращ комуникационен трафик чрез който данните да се криптират и имат конфиденциалност.

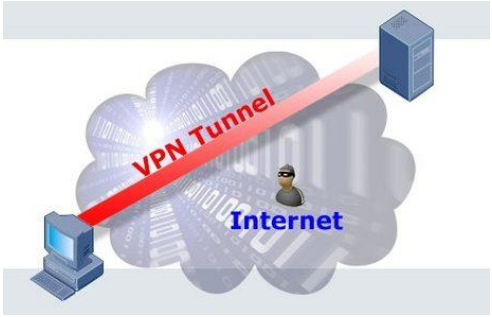
2. Реализиране на VPN комуникация

В единия край на комуникационния „тунел“, най-често в локалната мрежа (LAN) на един потребител има хардуерен или софтуерен VPN сървър. В другия край на „тунела“ имаме потребител, който използва инсталиран клиентски VPN софтуер.

За осъществяване на връзката, тя трябва да бъде инициализирана от потребителя към VPN сървъра, чрез неговия клиентски VPN софтуер. По този начин се изгражда VPN комуникационния „тунел“. Той осигурява обмена между потребителя и сървъра. Обменът се извършва чрез съответен комуникационен протокол.

При комуникация на двете страните в на комуникационния „тунел“ се извършва автентикация. Доста често тя е с потребителско име и парола. При разрешен достъп се оценяват правомощията на даден потребител, предоставянето му на споделени услуги и нивата за достъп до различните мрежови ресурси [1], [2], [3].

След потвърждаване на самоличността и оценката за правомощията на дадения потребител, се извършва криптиране на данните по линията VPN сървър – VPN клиент (фиг. 2).



Фиг.2. Линията VPN сървър – VPN клиент

3. Общи VPN протоколи

Въпреки че съществуват много комуникационни протоколи, има някои основни приложения, които обикновено се поддържат, независимо от марката за VPN услуги. Някои от тях са по-бързи, някои по-бавни, някои по-сигурни, други по-малко. Изборът е на потребителя в зависимост от неговите изисквания (табл. 1).

OpenVPN: Протокол с отворен код, който е със средна скорост, но предлага силна поддръжка за криптиране.

L2TP / IPSec: Това е доста често срещано и предлага прилични скорости, но лесно се блокира от някои сайтове, които не са в полза на потребителите на VPN.

SSTP: Не толкова често достъпни и освен добро криптиране, няма какво да се препоръча.

IKEv2: Много бърза връзка и особено добра за мобилни устройства, предлагайки по-слаби стандарти за криптиране.

PPTP: Много бързо, но през годините е пълен с пропуски в сигурността

Таблица 1. Общи VPN протоколи

Видове	Encryption	Сигурност	Скорост
OpenVPN	256-битова	Най-високото криптиране	Бърза на връзки с висока латентност
L2TP	256-битова	Най-високото криптиране	Бавна и силна зависимо от процесора
SSTP	256-битова	Най-високото криптиране	Бавна
IKEv2	256-битова	Най-високото криптиране	Бърза
PPTP	128-битова	Минимална сигурност	Бърза

4. Модели на VPN и WEB сайтове предлагащи VPN услуги

Съществуват 3 модела за изграждане на VPN мрежи:

— използвайки хардуер (VPN рутери, VPN Firewall);

— използвайки WEB сайтове предлагащи VPN услуги;

— допълнителен софтуер Putty.

В днешно време има много различни типове VPN потребители, следователно те имат различни нужди. Някои потребители се нуждаят от VPN да заобикалят географски ограничения, за да получат достъп до излъчвано съдържание, докато други искат да подсигурят допълнително връзката си докато ползват Wi-Fi. Трети пък използват VPN, за да свалят спокойно торенти в страни и територии, където са изцяло забранени. Тези хора ще трябва да изградят своя домашна мрежа, за да са сигурни, че избраната от тях VPN услуга ще може да задоволи нуждите им.

Едни от най-популярните VPN доставчици, които не пазят записи за търсещите максимална конфиденциалност са:

— CactusVPN

— CyberGhost

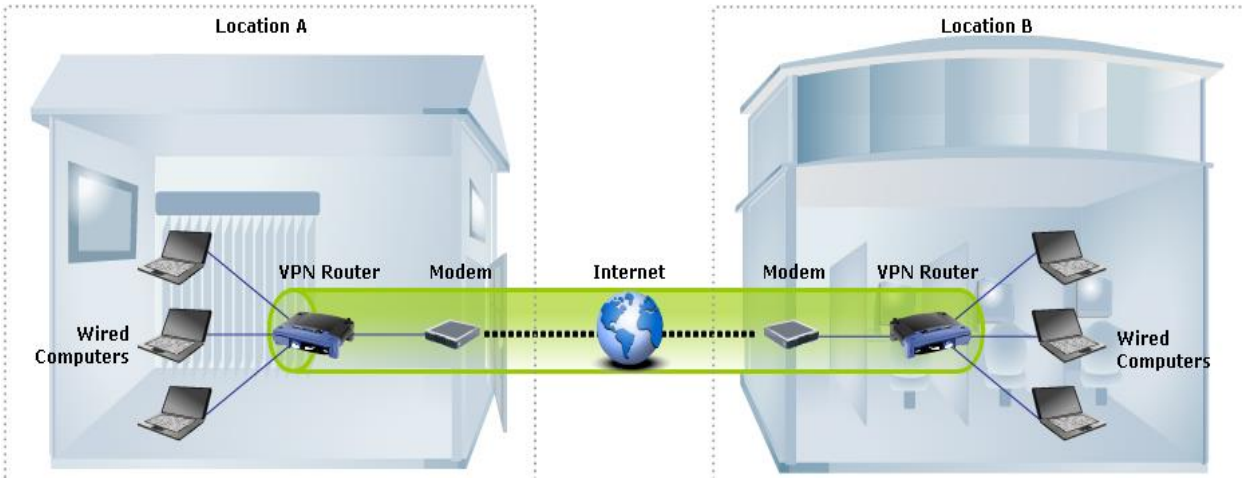
— NordVPN
— TRUST.ZONE
— VPNTUNNEL

5. Изграждане на VPN мрежа с 2 рутера

За пример е изградена мрежа с 2 рутера [5], [6], [7]. Опитната постановка е изобразена на фиг. 3.

Локация А – Рутер 1

Използван е VPN рутер от Linksys. Lan Address-a е от IPv4 тоест,четири 32 битови числа и е 192.168.1.1. Маската на подмрежата (Subnet Mask) е бъде от клас С – 255.255.255.0. Така ще има 24 бита NETID и 8 бита HOSTID. Internet Address-a е IPv4 и е 22.15.160.53. Local IP Address е същия като на LAN мрежата (192.168.1.1). Local secure gateway (Локален защитен шлюз) е 192.168.1.1. (Remote secure gateway). Отдалечен защитен шлюз е 10.100.16.60. Шлюзовете ще се грижат за уникалността на IP да няма машини и с еднакво IP. Encryption (Шифриране) ще е от тип DES, който е най-разпространения тип за шифриране и е с дължина 56 бита, което не е от достатъчните защити в днешно време. Authentication (Автентикация) е от тип PAP Password Authentication Protocol, опростен протокол при който автентикация се осъществява при правилно въведена парола и потребителско име. PFS (perfect forward **Secrecy**) ще бъде Enable – включено за по добра защита. Pre-shared Key (Предварително споделен ключ) ще бъде „MySecretKey“. Inbound And Outbound SPI: 100. Key Management (Управление на ключове) Auto – автоматично. Key Lifetime (Живот на ключа) 3600 секунди. Operating model – Aggressive (Агресивен) 768 бита.



Фиг. 3. Изглед на разработената VPN мрежа

Локация В – Рутер 2

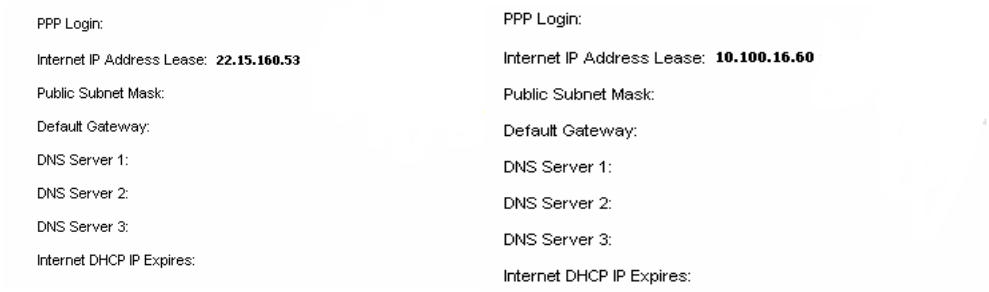
Използван е VPN рутер от Linksys. Lan Address-a е от IPv4 т.е., четири 32 битови числа и е 192.168.2.1. Маска на подмрежата (Subnet Mask) е от клас С – 255.255.255.0. Така има 24 бита NETID и 8 бита HOSTID. Internet Address-a е IPv4 и е 10.100.16.60. Local IP Address ще е същия като на LAN мрежата (192.168.2.1). Local secure gateway (Локален защитен шлюз) е 192.168.2.1. Отдалечен защитен шлюз (Remote secure gateway) е 22.15.160.53. Шлюзовете ще се грижат за уникалността на IP да няма машини и с еднакво IP. Encryption (Шифриране) е от тип DES. Authentication (Автентикация) ще е от тип PAP. PFS (perfect forward security) е Enable – включено за по добра защита. Pre-shared Key е „MySecretKey“. Inbound And Outbound SPI: 100. Key Management Auto – автоматично. Key Lifetime 3600 секунди. Operating model – Aggressive.

Свързване на устройствата заедно

Преди да се свържем с VPN тунел трябва да се уверим, че има активна Интернет връзка между двата маршрутизатора, които ще комуникират. Натискаме клавиша (старт бутона) на Windows 10 в търсачката въвеждаме „cmd“ и отваряме „Command Prompt“. В него пишем ping yahoo.com и натискаме ENTER. Проверяваме раздела Ping Statistics. Трябва да получим няколко последователни еднакви отговора, които ще ни потвърдят връзката на компютъра с Интернет.

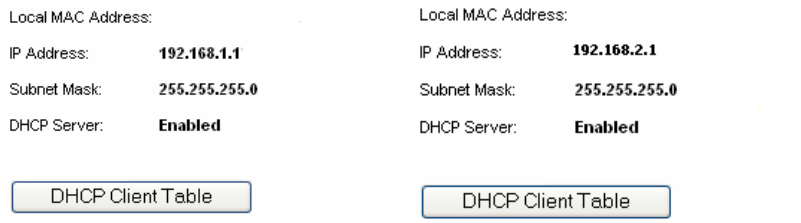
След като се уверим, че има активна Интернет връзка, трябва да проверим настройките на VPN. За да получим достъп до тях, в браузера който използваме въвеждаме IP 192.168.1.1. Отваря се страница в която трябва да се въведе парола. Паролата по подразбиране е admin. След нейното въвеждане влизаме в настройките на Рутер 1. Аналогичен е пътя и за Рутер 2, него го търсим в браузъра с IP 192.168.2.1.

При кликване на Status, след това Gateway обръщаме внимание на Internet/WAN IP address (фиг. 4).



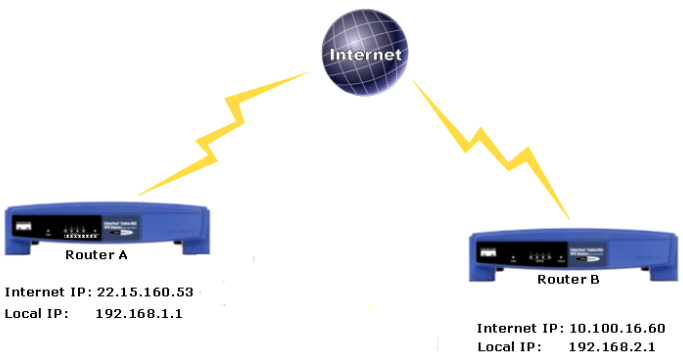
Фиг. 4. Извадки от двата Рутера на Internet/WAN IP address

22.15.160.53 ще бъде Remote Secure Gateway на Рутер 2, а 10.100.16.60 ще бъде Remote Secure Gateway на Рутер 1. На следваща стъпка кликваме Status след това Local Network и обръщаме внимание на IP Address-а (фиг. 5).



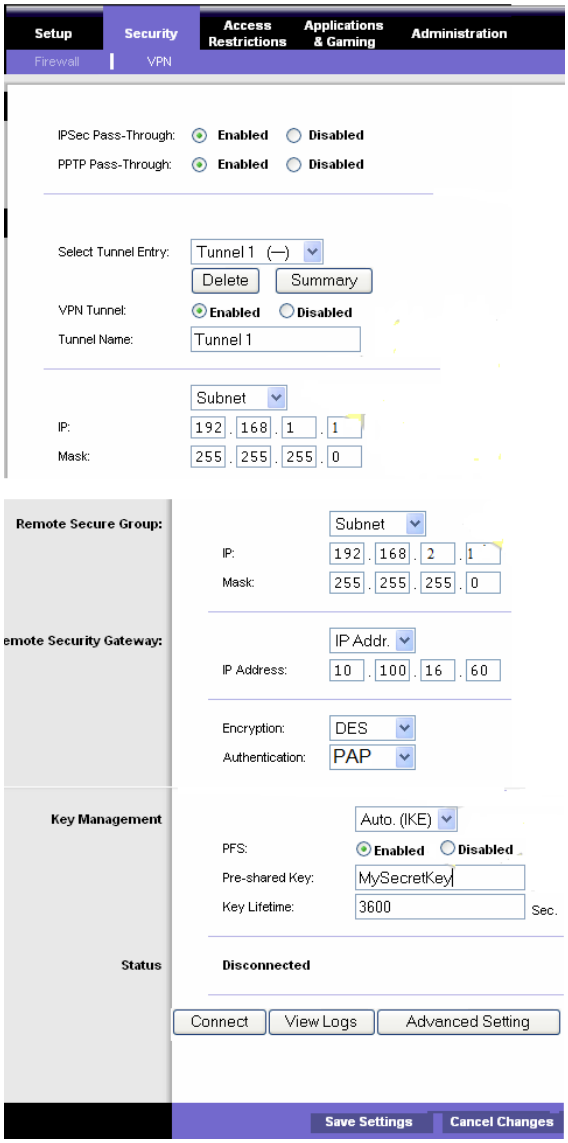
Фиг. 5. Извадки от двата Рутера на IP address

192.168.1.1 ще бъде Local Secure Group за Рутер 1, както и Remote Secure Group за Рутер 2, а 192.168.2.1 ще бъде Local Secure Group за Рутер 2, както и Remote Secure Group за Рутер 1. За по-голяма сигурност отново се проверяват Local IP Address-ите на двата рутера да са различни. Забелязва се до тук, че Local IP Address на Рутер 1 ще бъде Remote Secure Group IP на Рутер 2 (фиг. 6).



Фиг. 6. Връзка между рутери и Интернет

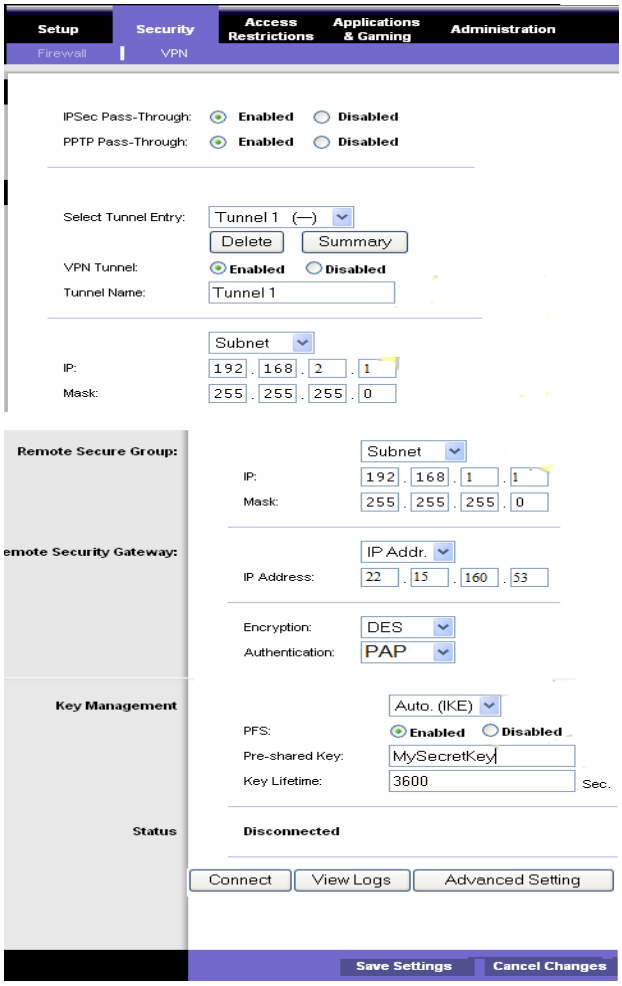
След онагледяването на Рутерите и сверяването на техните Internet IP address-и и LAN IP address-и преминаваме към конфигурирането на Рутер 1. За тази цел от браузера чрез въвеждане на IP 192.168.1.1 отваряме настройките на Рутер1, отключваме ги с парола admin. Когато се отворят кликваме Security и след това VPN. Първо селектираме Tunnel entry, който искаме да създадем. В нашия случай това ще е Tunnel 1. Чрез опцията VPN Tunnel избираме Enabled за да активираме тунела. От разширяващата опция Tunnel Name може да наименуваме как да се казва дадения тунел. В случая го наименуваме Tunnel 1. Преминаваме към следващата настройка на Subnet и IP Address. В тези полета се въвеждат стойности. В този случай се въвежда Subnet с Mask 255.255.255.0 и IP 192.168.1.1. Опциите Remote Secure Group и Remote Secure Gateway подлежат на следните настройки. В Remote Secure Group се въвежда Subnet с Mask 255.255.255.0 и IP 192.168.2.1, а в Remote Secure Gateway IP 10.100.16.60, защото това е IP на отдалечения защитен шлюз. Под Encryption, избираме ниво на шифриране, под което искаме да работи нашия тунел. В случая ще е от тип DES, който е най-разпространения тип за шифриране и е с дължина 56 бита. Преминаваме и през Authentication(Автентикация), тя ще е от тип PAP (Password Authentication Protocol), опростен протокол при който автентикация се осъществява при правилно въведена парола и потребителско име. PFS (Perfect Forward Secrecy) ще бъде Enable, което ще гарантира, че първоначалната ключова размяна и предложенията на IKE са защитени. Под Pre-shared Key (Предварително споделен ключ) ще въведем „MySecretKey“, но може да се въведе каквото и да е име, спрямо желанието на всеки потребител. Key Lifetime (Живот на ключа) ще заложим 3600 секунди. Това е периода, в който искаме ключът да бъде „жив“ и използваем в тунел, като след изтичане на времевия интервал бива унищожен. След всички промени натискаме бутона Save Settings за да запаметим всички настройки по Рутер 1 (фиг. 7).



Фиг. 7. Настройки на Рутер 1

Приключвайки с настройването на Рутер 1 преминаваме към Рутер 2. Неговата настройка е почти идентична с тази на Рутер 1 с минимални разлики. Отново чрез браузера чрез въвеждане на IP 192.168.2.1 отваряме настройките на Рутер 2, отключваме ги с парола admin. Когато се отворят отново кликваме Security и след това VPN. Селектираме Tunnel entry, който искаме да създадем. В нашия случай това ще е Tunnel 1. Чрез опцията VPN Tunnel избираме Enabled за да активираме тунела. От разширяващата опция Tunnel Name може да наименуваме как да се казва дадения тунел. В случая го наименуваме Tunnel 1. Преминаваме към следващата настройка на Subnet и IP Address. В дадения случай въвеждаме Subnet с Mask 255.255.255.0 и IP 192.168.2.1. Опциите Remote Secure Group и Remote Secure Gateway подлежат на следните настройки. В Remote Secure Group въвеждаме Subnet с Mask 255.255.255.0 и IP 192.168.1.1, а в Remote Secure Gateway IP 22.15.160.53, защото това е IP на отдалечения защитен шлюз. Под Encryption, избираме ниво на шифриране, под което искаме да работи нашия тунел. В моя случай ще е от тип DES, отново както в Рутер 1. Преминаваме и през Authentication(Автентикация), тя ще е от тип PAP (Password Authentication Protocol), PFS (Perfect Forward Secrecy) ще бъде Enable – това ще гарантира, че първоначалната ключова размяна и предложенията на IKE са защитени. Под Pre-shared Key (Предварително споделен ключ) ще въведем „MySecretKey“, отново както на Рутер 1. На Живота на ключа ще заложим

3600 секунди, идентично като на Рутер 1. След всички промени натискаме бутона Save Settings за да запаметим всички настройки по Рутер 2 (фиг. 8).



Фиг. 8. Настройки на Рутер 2

След найстройването и на Рутер 2 натискаме появилия ни се вече активен бутон Connect и свързваме двата рутера. След свързването им получаваме изградения тунел и нашата нова активна VirtualPrivateNetwork мрежа.

6. Заключение

VPN обезпечава свързаността на вашия компютър към Интернет, за да се уверите, че всички данни, които сте получили или изпратили са криптирани и скрити от любопитни погледи. Виртуалната частна мрежа създава защитена връзка към мрежа, през обществена такава (Интернет), или през частна мрежа, собственост на Интернет доставчик. Всяка голяма компания, корпорация или правителствена агенция използва VPN технология, за да предостави на потребителите си надеждно защитена връзка към дадена частна мрежа. Има много VPN доставчици в уеб пространството, през които може да се свърже потребител към сървър срещу месечна такса от около $5-$10, ако искате да криптирате личните си данни и онлайн активност.

References:

1. **Boyanov, P., Hristov, Hr., Fetfov, O., Trifonov, T., 2017.** Educational simulation the local area network of academic departments with securely configured FTP server. International Scientific Online Journal, www.sociobrains.com, Publ.: Smart Ideas - Wise Decisions Ltd, ISSN 2367-5721, Issue 31, March, Bulgaria, 2017, pp. 146-154.
2. **Boyanov, P., Stoyanov, St., Hristov, Hr., Fetfov, O., Trifonov, T., 2017.** Routing information security in the local area network of academic departments using an enhanced distance vector routing protocol – EIGRP. A refereed Journal Scientific and Applied Research, ISSN 1314-6289, vol. 11, pp. 35-46.
3. **Boyanov, P., Stoyanov, St., Hristov, Hr., Fetfov, O., Trifonov, T., 2017.** Security routing simulation the local area network of academic departments using a link-state routing protocol – OSPF. A refereed Journal Scientific and Applied Research, ISSN 1314-6289, vol. 11, pp. 47-58.
4. **Dyankov, P., 2020.** Trends in the development of the metalworking industry. International scientific refereed online journal with impact factor, Issue 69 May, c. 37-40, ISSN 2367-5721.
5. **URL:** https://www.namecheap.com/vpn/how-does-vpn-virtual-private-network-work/
6. **URL:** https://vpnoverview.com/vpn-information/what-is-a-vpn/
7. **URL:** https://www.cisco.com/c/en/us/solutions/small-business/resource-center/security/how-to-setup-a-vpn.html#~steps-to-setup-a-vpn