Tekhnê
January - June 2018, Vol. 15, No. 1, pp. 45 – 53

ISSN 1692-8407

Informatics Security - VPN

Seguridad Informática - VPN

Paola A. Segura
Universidad Distrital Francisco José de Caldas
andreaasegura@gmail.com

Maritza Ramírez F.
Universidad Distrital Francisco José de Caldas
mramirezf@correo.udistrital.edu.co

In the following article, the topic of IT (Information Technology) security will be presented, focusing on everything that concerns the implementation of a VPN in a business environment. The type of VPNs that exist, the protocols, requirements, and uses for which this network is used will be addressed, and then the configuration of one of these networks will be explained. In this way, we will evaluate the level of reliability, performance, and traffic control of a VPN and argue why it is the best current IT security solution for a company.

Keywords: Access, computer security, encryption, networking, VPN

En el siguiente artículo se expondrá el tema de seguridad informática, enfocando su contenido en todo aquello que concierne a la implementación de VPN en un ambiente empresarial. Se abordará el tipo de VPNs que existen, los protocolos, requisitos y usos para los cuales esta red se emplea, para luego explicar la configuración de una de estas redes. De esta forma, evaluar el nivel confiabilidad, el desempeño y el control de tráfico de una VPN y argumentar porqué es la mejor solución actual de seguridad informática de una empresa.

Palabras clave: Acceso, cifrado, redes, seguridad informática, VPN

Article typology: Research

Date manuscript received: December 6, 2017
Date manuscript acceptance: December 15, 2017

Research funded by: Universidad Distrital Francisco José de Caldas.

How to cite: Segura, P., Ramírez, M. (2018). *Informatics Security - VPN*. Tekhnê, 15(1), 45 -53.

Introduction

It will identify the problem and the question to be solved of, why the implementation of a VPN is the best solution in the IT security of a company, and it will give a brief description of the information gap and how it will be solved (Alshalan, Pisharody, & Huang, 2016; Redžović, Smiljanić, & Savić, 2017).

VPNs are created by the need to keep our data safe when surfing the Internet since we are not exempt from the theft of our information and more without realizing it, also born by companies that need to provide their internal network infrastructure to their workers, when they are in places other than the company and at any time and this method allows a safe way (Olver, 2016; Park et al., 2015; Udayakumar, Thooyamani, & Khanaa, 2014).

They also allow accessing public information from anywhere in the world that due to the laws of different countries many contents are blocked and/or censored, thanks to this security system you can visualize that information and keep protected the trace that the user leaves when surfing the internet, the VPNs can be found in paid versions with great features even for those who cannot pay the premium versions there are the free versions that also satisfy that need but with some limitations (Kuroda, 2017; Massis, 2017).

At the end of the day it is nothing more reassuring than knowing that when surfing the Internet no matter what page you are visiting you can be confident that our data will always be safe, such as when making financial transactions, entering social network passwords, credit or debit card keys, making purchases with cards and so on, companies have the reliability that their customers' data and internal company data are not in danger as more and more new methods are created to manipulate the Internet and sabotage its security to get theirs those unscrupulous people who take advantage of unsuspecting users, to steal their personal information (Shunmuganathan, Saravanan, & Palanichamy, 2014).

The main objective of the article which is to inform about the alternative of computer security (VPN), also to create awareness that having computer security is necessary to protect our data and thus increase the implementation of this security system (Liu & Wang, 2014; Salman, 2017).

IT security and VPN

It will be briefly explained what a VPN is and how it works, to understand in an easy and precise way this effective security method.

VPN

A VPN (Virtual Private Network), is a network that allows a secure connection of data through a public or private Internet network being encrypted for security, and no matter where you are running this technology makes it possible to use the Internet from the original location of the server being used. This means that it is possible to use the Internet as if you were present in the region that has the VPN network.

Types of VPN

- **Remote access VPN**. This type of network allows them to connect to the same VPN network through a fixed IP from other remote locations. It is commonly used by companies with workers in other locations different from their headquarters that need to connect to the company's network and its headquarters temporarily.

To access the secure connection, the user must run the application and authenticate with a username and password. This creates the encrypted channel between the computer and the remote network, for a secure data exchange (Amaya, 2016) (Fig. 1).

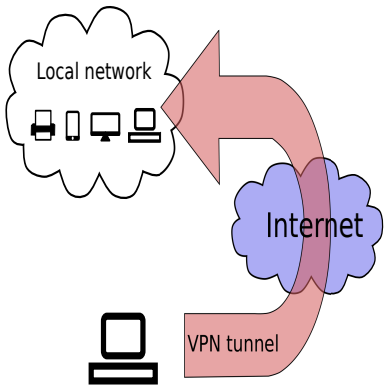

Figure 1. Remote access VPN.

- **Point-to-point VPN**. This scheme is used to connect remote offices to the organization's headquarters. The VPN server, which has a permanent link to the Internet, accepts Internet connections from the sites and establishes the VPN tunnel (Cheng, 2007).

In simple terms, a point-to-point VPN creates a virtual bridge that links networks in different locations to connect them to the Internet and maintain secure and private communication between them. They connect to the Internet using the services of their local Internet provider, typically through broadband connections.

- **Tunneling**. Type of communication is encapsulated using an encrypted network protocol to travel over the communication network, precisely creating a tunnel or encrypted communication channel within a computer network. As important information travels encrypted within the communication protocol data unit (PDU), all intermediate nodes participating in the communication will interact with the packet, but only at the end of the communication can the information be unpacked and decrypted for use.

ISSN 1692-8407

In this way, data packets are routed over intermediate nodes that are unable to see the contents of those packets. The tunnel is defined by the endpoints and the communication protocol used, which, among others, could be SSH (Secure Shell) (Cheng, 2007) (Fig. 2).

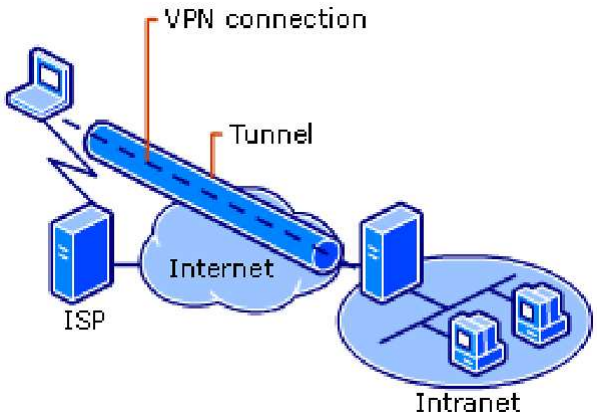

Figure 2. VPN connection.

- **VPN-LAN**. This is a variant of the remote access type but, instead of using the Internet as a connection medium, it uses the same company local area network (LAN) (Cheng, 2007).

It works just like a normal VPN, except within the same local LAN rather than over the Internet. It serves to isolate areas and services from the same internal network. It also serves to enhance the security features of a Wifi wireless network.

- **Firewall-based VPN**. This VPN takes advantage of the firewall's security mechanisms, including restricting access to the internal network, performing address translation, and meeting authentication requirements. The disadvantage of this type of technology is to be able to optimize its performance efficiently without diminishing the applications of the operating system (UNAM, 2017).

Protocols

- **IPsec (Internet Protocol Security)**. It enables improved security through robust encryption algorithms and a more comprehensive authentication system. IPsec has two encryption methods, transport mode, and tunnel mode. It also supports 56-bit and 168-bit (triple DES) encryption.
- **PPTP/MPP**. Technology is developed by a consortium of several companies. PPTP supports various VPN protocols with 40-bit and 128-bit encryption using the Microsoft Point to Point Encryption (MPPE) protocol. PPTP alone does not encrypt information.
- **PPTP/MPP**. Technology is developed by a consortium of several companies. PPTP supports various VPN protocols with 40-bit and 128-bit encryption using the Microsoft Point to Point Encryption (MPPE) protocol. PPTP alone does not encrypt information.
- **Symmetric vs. Asymmetric Encryption (Private Key vs. Public Key)**. Symmetric or private key encryption (also known as conventional encryption) is based on a secret key shared by both parties. The sending party uses the secret key as part of the mathematical operation to encrypt (or cipher) plain text to encrypt text. The receiving party uses the same secret key to decrypt (or unscramble) the ciphertext into plain text. Examples of symmetric encryption schemes are the RSA RC4 algorithm (which provides the basis for Microsoft's Point-to-Point Encryption (MPPE)) (UNAM, 2017), the Data Encryption Standard (DES), the International Data Encryption Algorithm (IDEA), and the US government's proposed Skipjack encryption technology (implemented on the Clipper chip).

Asymmetric or public-key encryption uses two different keys for each user: one is a private key known only to that user; the other is a corresponding public key, accessible to anyone. The private and public keys are mathematically related by the encryption algorithm. One key is used for encryption and the other for decryption, depending on the nature of the communication service being implemented.

Basic VPN requirements

Typically, when implementing a remote network solution, a company needs to facilitate controlled access to company resources and information. The solution must allow roaming or remote clients to connect to LAN resources, and the solution must allow remote offices to connect to share resources and information (router-to-router connections). Besides, the solution must ensure the privacy and integrity of data as it travels over the Internet. The same concerns apply in the case of sensitive data traversing a corporate internal network (Microsoft, 2017).

Therefore, a VPN solution should provide at least all of the following:

- **User authentication**. The solution must verify the identity of the VPN client and restrict VPN access to authorized users only. It must also provide audit and accounting records to show who accessed what information and when.
- **Addressing**. The solution must assign a VPN client address on the intranet and ensure that private addresses are kept private.
- **Data encryption**. Data transported on the public network must be unreadable to unauthorized customers on the network.
- **Password management**. The solution must generate and update encryption keys for the client and server.
- **Multi-protocol support**. The solution must handle common protocols used on the public network.

Deployment

The de facto standard protocol is IPSEC, but there are also PPTP, L2F, L2TP, SSL/TLS, SSH, etc. Each with its advantages and disadvantages in terms of security, ease, maintenance, and types of clients supported.

Currently, there is a growing line of products related to the SSL/TLS protocol, which tries to make the configuration and operation of these solutions more friendly.

Hardware solutions almost always offer higher performance and ease of configuration, but do not have the flexibility of software versions. Within this family, we have products from Fortinet, Sonic WALL, Watch Guard, Nortel, Cisco, Linksys, Nets creen (Juniper Networks), Symantec, Nokia, U.S. Robotics, D-link, Mikrotik, etc.

Software VPN applications are the most configurable and are ideal when interoperability problems arise in previous models. The performance is lower and the configuration more delicate, because it adds the operating system and the security of the computer in general (Eumed, 2017).

User administration

When selecting a VPN technology, it is important to consider administrative issues. Large networks need to store directory information on a per-user basis in a centralized data store or directory service, so that administrators and applications can add, modify, or query this information. Each access or tunnel server could maintain its own internal database of per-user properties, such as names, passwords and dial-up permission attributes. However, because it is administratively prohibitive to maintain multiple user accounts on multiple servers and keep them up to date at the same time, most administrators set up a master account database on the main domain controller or directory server, or on a RADIUS server.

Common uses

The objective of this section is to specify the most common applications given by common users and corporations of a bureaucratic nature, it should be clarified, with completely different purposes (Jacinto, Martínez, & Martínez, 2015).

The first of these is the leap in geographical restrictions. In many cases, there is content whose availability is very restricted because it is only accessible in certain countries. Given this situation, any user with Internet access can use VPN connections that are provided by mobile applications, browser plug-ins, or programs developed for computers whose software facilities to alter the connection network, Windows or Linux-based systems, for example. And through this VPN connection, give the device from which the procedure has performed the IP of a proxy located in the desired country.

Second is data privacy when surfing on a public Wi-Fi network. It is very common to find open networks in places such as airports, cafes, and shopping malls, which, although they fulfill their function and provide access to the network, are not at all secure, since they lend themselves to users intercepting information. This problem is avoided when using a VPN connection since it allows the person to use it to hide private data, such as credit card information, and so on.

Finally, but the most relevant point, given that it is one of the greatest interest to the article, is its use in the area of corporations. While it is true that access to a certain company's database requires a password, this is visible to anyone who uses the same network as the first person in question (Montiel, Jacinto, & Martínez, 2016). This is where the use of VPNs becomes almost essential in the case of multinationals, or companies with franchises that require coordinating people who are a considerable distance away, since it is viable to use the Internet for the transfer of data and information, safely. Because VPN connections allow the encryption of such information, either the password mentioned in the first place or confidential data belonging to the company.

Methodology

This part of the article will explain in detail how we will solve the problem, what software and materials will be used. In this case, the methodology will be tested on a LAN and WAN simulator called Packet Tracer from CISCO and on computers with Windows operating system.

Site-to-site VPN

The following explains the basic tasks for configuring IP-based Virtual Private Networks (VPNs), site-to-site, and IP-based extranets on a Cisco 7200 Series router using generic routing encapsulation (GRE) and IPSec tunneling protocols. Basic security, network address translation (NAT), encryption, Cisco IOS weighted equal queuing (WFQ), and extended access lists for basic traffic filtering are configured (Fig. 3).

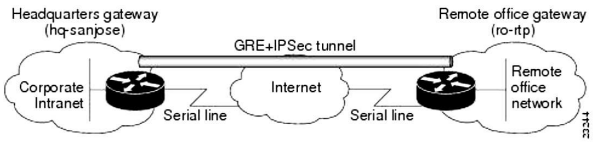

Figure 3. Site-to-site VPN business scenario.

Fig. 4 shows the physical elements of the scenario. The Internet provides the central interconnecting fabric between the central office and the remote office routers. Both the headquarters and the remote office use a VPN gateway.

The GRE tunnel is configured on the first serial interface in slot 1 of the chassis (serial 1/0) of the central and remote

ISSN 1692-8407

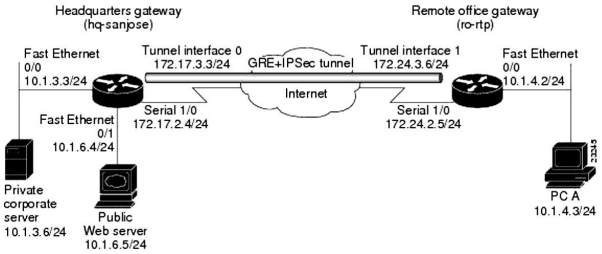

Figure 4. Physical elements of the site-to-site VPN scenario.

office routers. The configuration steps in the following sections are for the headquarters router unless otherwise noted.

Extranet scenario

The extranet scenario presented in Fig. 5 is based on the site-to-site scenario by providing a business partner with access to the same headquarters network. In the Extranet scenario, the site and trading partner are connected through a secure IPSec tunnel and the trading partner only has access to the site's public server to perform various IP-based networking tasks, such as placing and managing product orders.

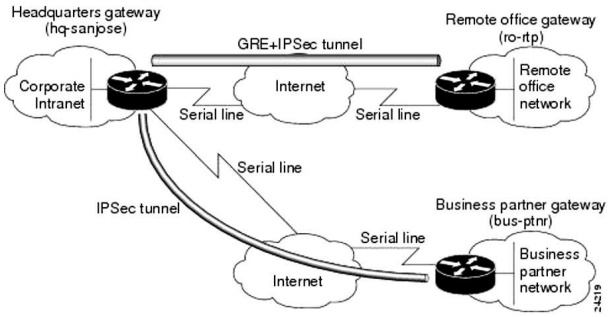

Figure 5. Extranet VPN business scenario.

The configuration steps in the following sections are for the headquarters router unless otherwise noted.

Tunnel configuration

The tunnel provides a way to encapsulate packages within a transport protocol. Tunneling is implemented as a virtual interface to provide a simple interface for configuration. The tunnel interface is not tied to specific *passenger* or *transport* protocols but is an architecture designed to provide the services needed to implement any standard point-to-point encapsulation scheme. Since tunnels are point-to-point links, you must configure a different tunnel for each link.

• **GRE Tunnel**. GRE is capable of handling multiprotocol transport and IP multicast traffic between two sites, which have only IP multicast connectivity. The importance of using tunnels in a VPN environment is based on the fact that IPSec encryption only works in IP multicast frames.

Network redundancy (resilience) is an important consideration in the decision to use GRE tunnels, IPSec tunnels, or tunnels using IPSec over GRE. GRE can be used in conjunction with IPSec to pass routing updates between sites on an IPSec VPN.

To configure a GRE tunnel between the central office and the remote office routers, you must configure a tunnel, source, and destination interface at the central office and the remote office routers. To do this, complete the following steps starting in global configuration mode.

Paso 1	hq-sanjose(config)# **interfaz tunnel 0** **hq-sanjose (cdnfig-if) # dirección IP 172.17.3.3 255.255.255.0**
Paso 2	hq-sanjose(config-if)# **fuente del túnel 172.17.2.4 255.255.255.0**
Paso 3	hq-sanjose(config-if)# **destino del túnel 172.24.2.5 255.255.255.0**
Paso 5	hq-sanjose(config)# **túnel de interfaz 0** **hq-sanjose (config-if) # no shutdown** % LINK-3-UPDOWN: Interface Tunnel0, estado cambiado Para arriba
Paso 6	hq-sanjose(config-if)# **salir** **hq-sanjose (config) # ip route 10.1.4.0 255.255.255.0 tunnel 0**

• **Set up a different shared key**. Because pre-shared keys were specified as the authentication method for policy 1 in the *Configuring IKE Policies* section (the policy that will also be used on the partner router) complete the following steps on the home router and the partner router:

• **Step 1**: Establish the identity of each Internet Security Association and Key Management Protocol (ISAKMP) peer. Each peer identity must be established in its hostname or by its IP address. By default, a peer identity is set to your IP address. In this scenario, you only need to complete this task on the business partner router.

• **Step 2**: Specify the shared keys in each pair. Note that a given pre-shared key is shared between two pairs. On a given pair, you can specify the same key for sharing with multiple remote pairs; however, a more secure approach is to specify different keys for sharing between different pairs.

• **Create extended access lists using access list numbers**. To create an extended access list that denies and allows certain types of traffic, completes the following steps starting in global configuration mode (table 1).

VPN configuration in Windows 10

This part of the article will explain in detail how we will solve the problem, what software and materials will be used. Whether it's for business or personal use, you can connect to a VPN (a virtual private network) on your Windows 10 PC. A

Table 1
Extended access lists.

	Mando	Propósito
Paso 1	`hq-sanjose(config)# access-list 102 deny tcp any alguna`	Defina la lista de acceso 102 y configure la lista de acceso para denegar todo el tráfico TCP.
Paso 2	`hq-sanjose(config)# access-list 102 deny udp any alguna`	Configure la lista de acceso 102 para denegar todo el tráfico UDP.
Paso 3	`hq-sanjose(config)# access-list 102 permiso ip cualquiera`	Configure la lista de acceso 102 para permitir todo el tráfico IP.

VPN connection can help provide a more secure connection to your company's network and the Internet.

To connect to a VPN, you need a VPN profile on your PC. You can either create a VPN profile on your own or set up a professional account to get a company VPN profile.

- Create a VPN profile. If you do not have a VPN profile on your Windows 10 PC, you will need to create one. If it's for work, look for the VPN settings or a VPN application on the company's intranet site when you're at work, or contact the company's technical support staff. Select the Start button, and then select **Settings > Network and Internet > VPN > Add a VPN connection**.
- Under Add a VPN connection, do the following. Under VPN Provider, choose Windows (integrated). In the Connection box, type a descriptive name (for example, my Personal VPN) for the VPN connection profile. This is the name of the VPN connection that you should look up in the server names or the address box when you want to connect. Enter the VPN server address.
- Under VPN Type, choose the type of VPN connection you want to create. You will need to know what type of VPN connection the company or the VPN service uses, in this case, the Point-to-Point Tunneling Protocol (PPTP) will be used, but the steps for L2TP/IPSec with pre-shared key are very similar, and you should have no problem following them.
- Under Login Information Type, choose the type of login information (or credentials) you will use. This information can be a user name and password, a one-time password, a certificate, or a smart card if you connect to a VPN at work. Enter your username and password in the appropriate boxes (optional).
- Select Save. If you need to edit the VPN connection information or specify additional settings, such as the proxy settings to be used for the VPN connection, choose the VPN connection, then Advanced.
- Connect to a VPN. Once you have a VPN profile, you can log in. At the far right of the taskbar, select the Network icon Select the VPN connection you want to use, and then do one of the following depending on what happens when you select the VPN connection.
- If the Connect button is displayed below the VPN connection, select Connect. If the VPN is opened in Settings, select the VPN connection, and then select Connect. If prompted, enter your user name and password or other login information. When you are connected, the name of the VPN connection will display *Connected* below.
- To quickly check if you're connected to the VPN while performing tasks on your computer, select the Network icon on the far right of the taskbar, and then see if the VPN connection indicates *Connected* below it.

Testing

It is taken into account in the accounts and results taken from the population of the United States because of the facility and complete information that this country is a superpower.

Data filtering

The latest statistics show a steady trend of increasing data leakage around the world (Fig. 6 (Greenberg, 2017)).

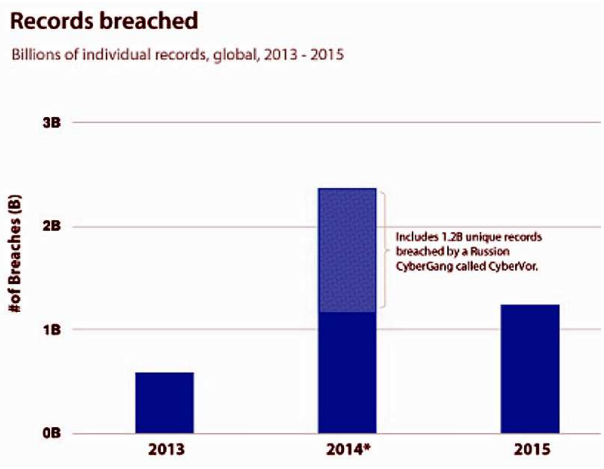

Figure 6. Records breached (Greenberg, 2017).

Data privacy and national security

Certain data are analyzed that have reference to the problem, the little privacy that can be had when connecting to the Internet, the attack in San Bernardino, California, United States, on December 2, 2015, was analyzed where it was questioned why the iPhone that was involved with the attack was not unblocked by Apple but the FBI had to intervene, where it makes you question more about how secure the internet network you use is and how easily our information or more importantly, state information can be stolen and that your government is not doing enough on the cyber front to deal with terrorism (Fig. 7).

As new technologies come out, this one benefits us as it harms us if it is in the wrong hands and so we have the need

ISSN 1692-8407

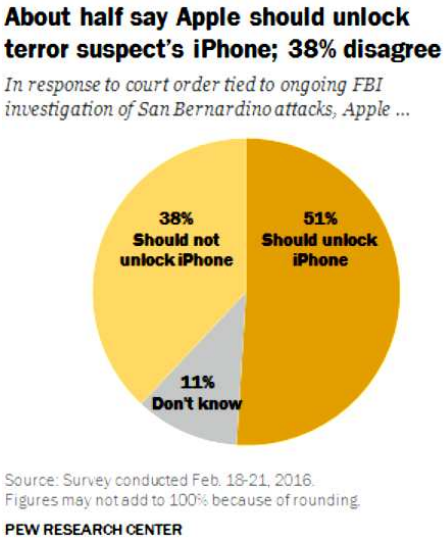

Figure 7. Apple unlock iPhone (Center, 2017).

to protect ourselves more and more from such attacks and in this case at a computer security level, by accessing a separate server for internet use, VPNs become a good option for the security of your data and make it much more difficult for hackers or third parties to record data online.

Frequency of VPN use

According to the data, people use VPNs at least once a week (Fig. 8).

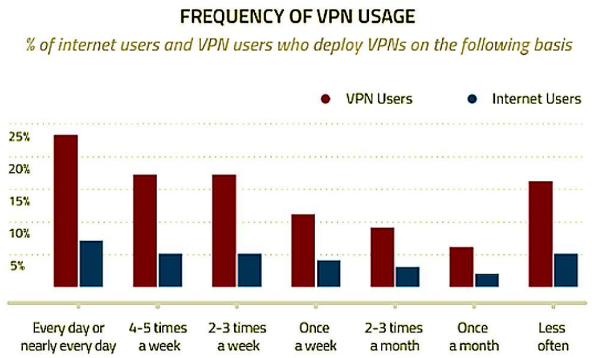

Figure 8. Frequency of VPN usage (Young, 2017).

Main consumers of VPN use

Asia and the Middle East remain the largest consumers of VPNs (Fig. 9).

Anonymous navigation

Anonymous browsing is used to protect our data when surfing the net since it hides the computer's IP to leave no

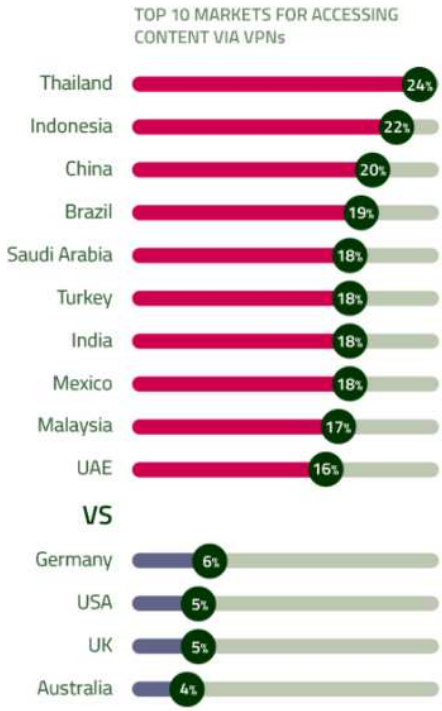

Figure 9. Top 10 markets for accessing content via VPNs (Mander, 2017b).

trace of what is done on the Internet, and for this purpose, VPNs are implemented. Among the countries that most use this method are Saudi Arabia and Vietnam, among others (Mander, 2017a).

Lack of confidence in privacy

NTIA analysis shows that as you use more devices in your home, you are more likely to become a victim of information theft via the Internet (Fig. 10) (Rafi, 2017).

By far the most frequent concern, shared by 63 percent of online households, was identity theft. Other common concerns include credit card or bank fraud, data collection or tracking by online services, loss of control over personal data, data collection or tracking by the government, and personal security threats (Fig. 11) (Rafi, 2017).

Privacy and security concerns change users' online behavior

According to the survey conducted in 2015, for fear of information and identity theft online made 45% of users surveyed refrain from making financial moves, make purchases, and even give controversial opinions in social networks and 30% of users were obtained to do at least 2 of these actions (Fig. 12) (Rafi, 2017).

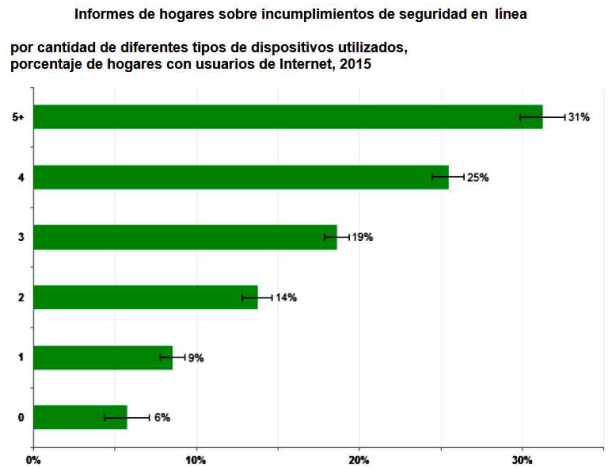

Figure 10. Household reports of online security breaches (Rafi, 2017).

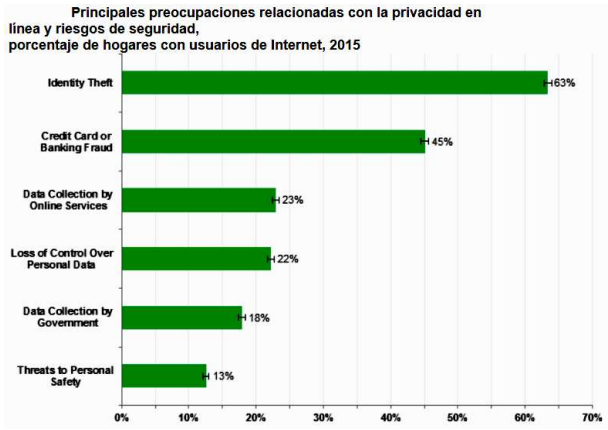

Figure 11. Key online privacy concerns and security risks (Rafi, 2017).

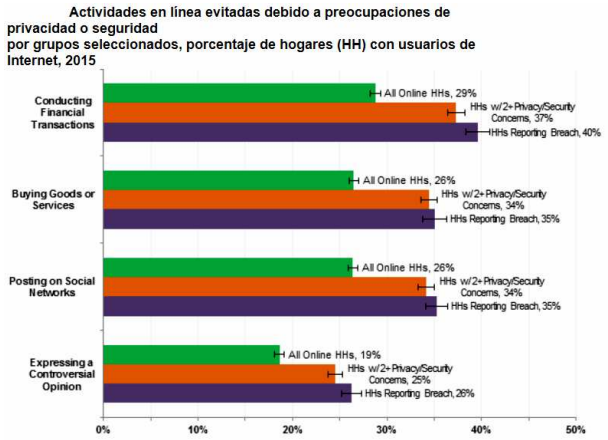

Figure 12. Online activities avoided due to privacy or security concerns (Rafi, 2017).

Be prepared for a cyber attack on companies and organizations

Insecurity matters, private organizations, and companies, a threat to their information is much more sensitive than to the common population, and it goes beyond how prepared they are for such threats, it is estimated that 62% of companies do not have a plan to these incidents.

Only 37% of respondents, most of them in the heavily regulated financial services industry, have a fully operational incident response plan. Three in ten have no plan at all, and of these, almost half do not believe they need one (Burg, 2017).

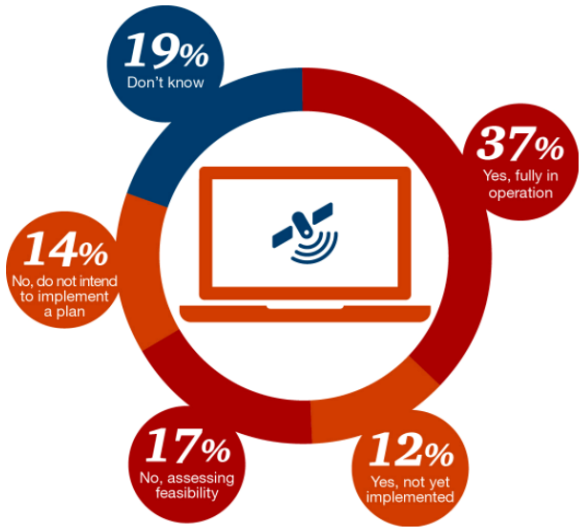

Figure 13. Concept on the use of online security (Burg, 2017).

Conclusion of the analysed data

With these data it is demonstrated the great necessity to implement a safe and reliable method at the time of speaking of computer science security, to anticipate this type of incidents and if it is at the level of the common population, it will be possible to be estimated at the level of companies, since as they have managed to intervene in the computer science security of the nation the gravity of the subject is noticed, and one of the main objectives of the companies is to have a good handling of data of its clients and the information that there handle.

Currently, it has been demonstrated that the use of VPNs is one of the best options for computer security and many providers offer this service, and why not also the use of VPNs at the personal level, and as shown above is not so difficult to install on computers and there are also free VPN service providers that explain step by step their installation.

Conclusions

The use of virtual private networks is currently presented as a good alternative for companies because through tunneling provides confidence and certainty that at all times

ISSN 1692-8407

communications are reliable, also thanks to the technology provided by the VPNs can obtain considerable economic savings by reducing the costs of data transmission since it is not necessary to use a dedicated line very expensive, on the contrary, allows you to use a public network such as the Internet.

References

Alshalan, A., Pisharody, S., & Huang, D. (2016). A survey of mobile vpn technologies. *IEEE Communications Surveys and Tutorials*, *18*(2), 1177-1196.

Amaya, C. (2016). *Tipos de redes vpn y cómo funcionan: ¿ya sabes cuál usar?*

Burg, D. (2017). *Cybercrime.* (PWC)

Center, P. (2017). *More support for justice department than for apple in dispute over unlocking iphone.* (People Press)

Cheng, R. (2007). *Lost connections.* (The Wall Street Journal)

Eumed. (2017). *Red privada virtual.*

Greenberg, R. (2017). *Vpn use and data privacy stats for 2017.* (VPN Mentor)

Jacinto, E., Martínez, F., & Martínez, F. (2015). Minimalist identification system based on venous map for security applications. In C. M. Falco & X. Jiang (Eds.), *Seventh international conference on digital image processing (ICDIP 2015).* SPIE.

Kuroda, T. (2017). A combination of raspberry pi and softether vpn for controlling research devices via the internet. *Journal of the Experimental Analysis of Behavior*, *108*(3), 468-484.

Liu, M., & Wang, X. (2014). Inuences of ip fragment on ethernet over udp tunnel vpn and the solution. *Journal of Computational Information Systems*, *10*(6), 2397-2404.

Mander, J. (2017a). *15 trends for 2015: Generation v.*

Mander, J. (2017b). *Thai and indonesian internet users most likely to access content via vpns.*

Massis, B. (2017). Vpns in the library. *Information and Learning Science*, *118*(11-12), 672-674.

Microsoft. (2017). *Technet.*

Montiel, H., Jacinto, E., & Martínez, F. (2016). Implementation of lightweight encryption algorithm based on 32-bit embedded systems. *International Journal of Applied Engineering Research*, *11*(23), 11409-11413.

Olver, N. (2016). A note on hierarchical hubbing for a generalization of the vpn problem. *Operations Research Letters*, *44*(2), 191-195.

Park, P., Ryu, H., Hong, G., Yoo, S., Park, J., & Ryou, J. (2015). A service protection mechanism using vpn gw hiding techniques. *Lecture Notes in Electrical Engineering*, *339*, 1053-1062.

Rafi, P. (2017). *Lack of trust in internet privacy and security may deter economic and other online activities.* (NTIA)

Redžović, H., Smiljanić, A., & Savić, B. (2017). Performance evaluation of software routers with vpn features. *Telfor Journal*, *9*(2), 74-79.

Salman, F. (2017). Implementation of ipsec-vpn tunneling using gns3. *Indonesian Journal of Electrical Engineering and Computer Science*, *7*(3), 855-860.

Shunmuganathan, S., Saravanan, R., & Palanichamy, Y. (2014). A light weight source-end defense architecture to protect ipsec vpn service from spoofing attack. *Information (Japan)*, *17*(9B), 4545-4565.

Udayakumar, R., Thooyamani, K., & Khanaa. (2014). Deploying site-to-site vpn connectivity: Mpls vs ipsec. *World Applied Sciences Journal*, *29*(14), 6-10.

UNAM. (2017). *VPN.*

Young, K. (2017). *1 in 5 are weekly vpn users.*