CAPÍTULO 1

SECURITY OF INFORMATION AND IPSEC VPN

Data de submissão: 25/10/2024 *Data de aceite: 01/11/2024*

Izan Fabrício Neves Calderaro
Masters in Regional Development and Environment (PGDRA), Brazil. Member – Technology Development and Systemic - the Research Group GEITEC/UFRO.

Paulo Henrique Guyss
Graduate in Analyses of System(UFRO), Brazil.

Fabrício Moraes de Almeida
PhD in Physics (UFC), with post-doctorate. Specialist in Systems Analysis and Development (FUNIP). Researcher of the Doctoral Program and a Masters Degree in Regional Development and Environment (PGDRA - UNIR). Leader - Technology Development and Systemic -the Research Group GEITEC-UFRO.

ABSTRACT: The objective of the chapter is: with the rapid evolution of technology, the Internet has become an indispensable tool of contemporary times, and is seen as a world encyclopedia, source of information from various fields of knowledge. It is noteworthy that, as shown by studies, this network is not secure because the present protocols have vulnerabilities to attacks (Denial of Service Attack, DNS poisoning, IP spoofing, etc.). For this security happens, network security protocols are used, such as SSL, SSH, TLS, and between these protocols is the IP Security (known as IPSec), which has stood out more and more for the safety of proof provided, so that will become the standard security protocol, a fact already proposed by US agencies. The main objective is the implementation of IPSec using Ubuntu OS, since it is more flexible for the installation of free codes (as Openswan).

KEYWORDS: VPN; IPSec Protocol; Internet Security; Cryptography; Ubuntu; Operational System.

1 | INTRODUCTION

The leak of information and intelligence on the largest network of all is a fact that is becoming common, although it is worrying. Of millions data has already been proven hacked on the Internet Writing (2014).

Assuming a company has huge data bank with registration through millions of users with names, passwords, emails, short, relevant data. It may seem banal if these data are delivered to those who do

not know what to do with them. However, just as there are experts to defend the Internet, there are experts in attack. Are able to use thousands of email accounts to make attacks on websites, send emails with viruses, use the passwords and users to try to invade other sites Writing (2014).

Hypothetically, imagine that not only are these types of data and the responsibility that the company brings to save them. Imagine also financial data, inventory data, products, targets, plans. All this information in the hands of those who know what to do with them would become a gold mine.

Possible forms of security breach: Destruction of information; Codification or misrepresentation of information; Theft, removal or loss of resources and disruption of services.

The present attacks are varied, but some basic care should be taken not to be totally at the mercy on the Internet: keep the OS updated, keep updated anti-virus and firewalls, create difficult passwords to crack, disable the sharing of resources between computers in unknown networks Cert (2014). These settings can easily block network attacks made by not very experienced users because although they seem basic, obloquy many doors and loopholes that could be used by a hacker.

All this only reaffirms the importance of Network Security in the current context of communications.

And there are many technologies available for this defense, as: SSL: Allows client / server applications can exchange information safely through authentication of the parties involved, Martins (2009). SSL is a widely used type of defense because its implementation is a medium complexity and provides effective defense. SSH: allows virtual access to a server through a terminal, Cybernetx (2011). It can be observed as a secure telnet, since all communication is encrypted. VPN: are point to point connections in private or public networks by the use of tunneling protocols, Microsoft (2014). Although IPSec requires a VPN to work, it is worth noting that both do not mix: are different concepts, because one includes the other. And the IPSec discussed in this case study.

2 | THEORETICAL REFERENCE

At the beginning of the creation of the Internet, there was not much concern for network security issue. While the internet was restricted to scientific and academic circles, security problems were not as boring because there was based control in the ethical use of the network codes, Huitema (1998).

However, the internet turned out to expand, making it the largest union of networks and equipment globally. The main step to the top of network security concerns began when the network was also directed to the private sector, where they began to be attacks and targets of interest.

IP Security is a security platforms developed by the IP Security Protocol Working Group (IPSec) of the IETF (Internet Engineering Task Force) in response to network security challenges.

For understanding the IPSec protocol, one must have the foundation of a whole range of information, from the operation of a computer network, to the communication between devices that use this protocol.

2.1 INTERNET AND CRYPTOGRAPHY

The internet can be defined as a global network (union of several smaller networks), able to reach even the most remote distances, causing a connection is established between all the equipment present in it, no matter the distance, Tanenbaum (2003).

For the connection of such a large scale can be made, we cannot ignore the protocols in no time. Among the major internet protocols, have the TCP / IP protocol (known by that name, but it is a protocol stack). Basically, the idea of this protocol is to assign each computer a different IP address, thus making each single device in their identification.

On the way between the devices over the internet, there are many other elements that can be cited: Network Card (each NIC has a MAC address, thus making impossible the presence of a copy that is undetectable). Modem and Router (The first is capable of processing the signal sent / received from the company that gives Internet services. The second is responsible for understanding what the possible paths for the delivery of data across the network). Dealership Internet service is the company that rents the services to its customers, both domestic and commercial. This is the company that will address the issue of unique addresses for each of which is present on the network. There are many elements that make the Internet work, but the main have been cited. Therefore, all network devices are made by standards and protocols being followed rigidly.

Encryption can be understood as the combination of the Greek words Kryptos and graphein, meaning “Hidden” and “Write”, respectively, Romagnolo (2007). Accordingly, it is a set of rules to be followed by the sender and receiver so that a message can be sent on one hand and be understood by the other. The last idea through it is to protect sensitive data stored on a computer and / or communications made by the internet. The features sought by encryption are well fixed and defined based on Information Security: Integrity, Confidentiality, Authenticity, Availability - Alencar (2011) and In addition, replacement, transposition, Running Key Cipher, Concealment Cipher, Steganography - Fernando (2007).

In addition, a major part of cryptography, algorithms, also has interesting models: DES, AES and 3DES. Recalling that the three algorithms presented are all symmetric key, Oliveira (2006), is now worth highlighting the asymmetric key: Diffie-Hellman, RSA and ElGamal.

2.2 VPN

A prerequisite for understanding the IPSec protocol is how to operate the networks or VPN Virtual Private.

VPNs work with peer to peer connection, whether in private or public networks. In this technique, special protocols are used which is based on TCP / IP, known as tunneling protocols. The idea is really simulate a tunnel, where only the sender and the receiver will know the existing connection.

The motivation behind the VPN is security interests. Large companies that need to communicate with their branch offices need the assurance that their data traveling over the network are not exposed and vulnerable. When used as a kind of “improved firewall” VPNs are known as extranet. Other VPN usage mode is when a user, say the head of the company wants to connect to the network of the same. To virtualize communication with the company, to create a single channel.

To create new connections dedicated to all existing companies and users, the cost is high, so the idea is to use a ready-made infrastructure is feasible. The internet is the cheapest existing means and it is the center for the use of VPNs. Since VPNs do not require special platforms, all already present equipment may be used for its implementation; only installing any software required One Linea (2009).

To emulate this connection, the data is encapsulated with a header. This header is responsible for routing contain important information that is needed to make the data transmission from start to finish. The data that is sent is encrypted, keeping confidentiality.

2.3 IPSEC PROTOCOL

This is a set of standards can ensure secure communication between two computers, even if the information submitted by both are in a medium non-insurance, such as the internet, Battisti (2013). But why use IPSec rather than other security protocols?

IPSec is proving to be the most complete structure to be used in VPNs. While it is true that the other protocols that are evolving are increasingly approaching its features. This causes it to be taken as a reference to equipment manufacturers and will eventually become a standard, Martins (2000). Currently, the Internet, uses the IPv4 standard that has no safety feature. This protocol then, is able to restrict the machines applied to communicate only when it is present. That is, in a given instance, the transfer of a message between two devices will only be possible if both are enabled with IPSec and no one knows the message exchange.

IPSec works with the IP datagrams, characteristic of internet communication by TCP / IP model, it is necessary to understand the structure of this datagram, as the following picture:

Version (4 bits)	Header length (4 bits)	Type of service (8 bits)	Total lenght (16 bits)	
ID (16 bits)			Flag (3 bits)	Fragment lag (13 bits)
Time life (8 bits)		Protocol (8 bits)	Header checksum (16 bits)	
IP source address (32 bits)				
Destination IP address (32 bits)				
Data (32 bits)				

Figure 1: The IP Datagram

Source: Kioskea (2014)

IPSec has several features, among which is worth mentioning: It has various forms of implementation, from the server to routers and firewalls. It can be integrated the TCP/IP through changes on the server. Implementation has BITS (Bump-In-The-Stack), being created on the TCP / IP stack already present. This is the technique commonly used in servers. Implementation features BITW (bump-in-the-Wire) using a dedicated device for encryption. Usually the device is connected to gateways and servers. Diffie-Hellman protocol used to exchange passwords between the pair of devices. For identity assurance those involved, uses public key cryptography to sign the exchanges. For encryption uses DES or 3DES generally. For package authentication, uses MD5 or SHA-1. And to validate the key, uses digital certificates.

Also, IPsec is divided into principal components. AH or Autentication Header, ESP or Encapsulating Security Payload and The IKE or Internet Key Exchange.

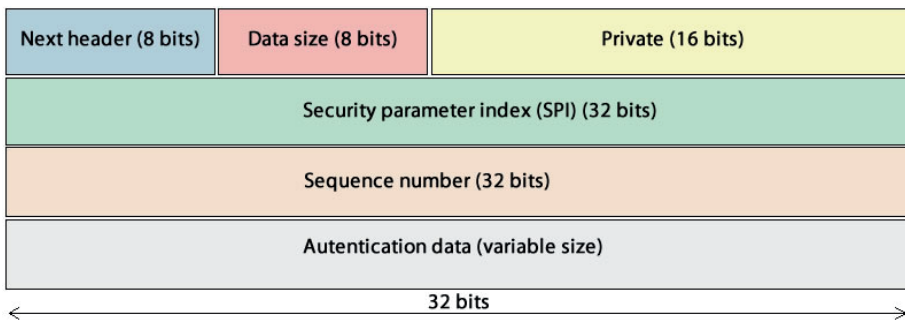

Figure 2: *Authentication Header*

Source: Andreoli (2008)

The Authentication Header is responsible for authentication, checking which computers will communicate using IPSec. It is also used to verify data integrity, realizing that the data has not been altered or corrupted during transport. It is also your responsibility

to prevent replay attacks, which is the attack in which captured packets are sent to the destination, trying a form of entry. His form of defense is the header itself, as it contains important information such as the status of the package has been received or not. The information contained in the header is the following: ID, size, security parameters, sequence number and data authentication. The AH is not encrypted.

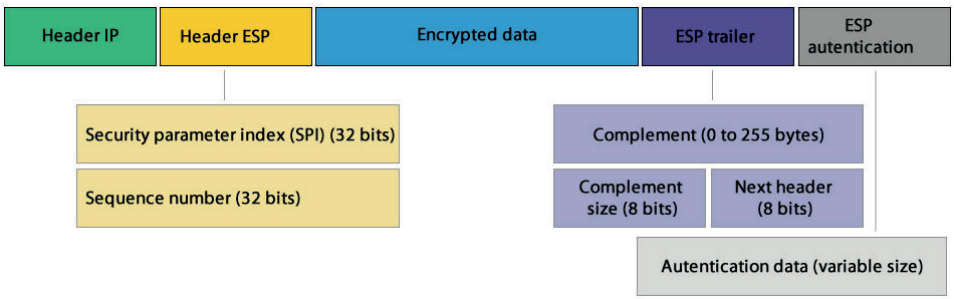

Figure 3: *Encapsulating Security Payload*

Source: Andreoli (2008)

The Encapsulating Security Payload is responsible for encryption, and does so with the packets before transmission. Therefore, even if the package is intercepted, nothing will be revealed. Only the equipment with the cryptographic key is to be able to read the packages and understand them. The information is divided into blocks and each block is encrypted by a block cipher. Therefore, it is almost impossible to find only tentatively.

The Internet Key Exchange is responsible for negotiating the connection parameters, such as session keys. Provides means for the parties to negotiate what protocols or algorithms are used to ensure the customer's identity on server. Ensures the exchange of messages that have keys securely Battisti (2013).

Soon after adding the functions of AH and ESP, sure there are changes in the structure of IP packets, which would then follow this pattern:

IPSec is also the issue of Security Association, Security Association. This association is an agreement between the connections of the entities on how they transmit the safety information. Therefore, every connection is from one side to the other, or both at the same time require an AS for each action.

Finally, IPSec works in two modes: Transport and Tunnel.

In transport mode, it is mainly used to provide service to upper-layer protocols. Its use is generally made to client-server. The information of the transport layer is encrypted by entering a new IP header. It is widely used in structures that already implement IPSec.

In tunnel mode, it provides a lot of protection to IP packet. To do this, each packet is individually applying headers, and encryption rules. Widely used in structures that do not implement IPSec, such as the Internet (in the case of this study), Andreoli (2008).

And this is how IPSec is able to make a statement that would be vulnerable in a safe and away from concerns connection.

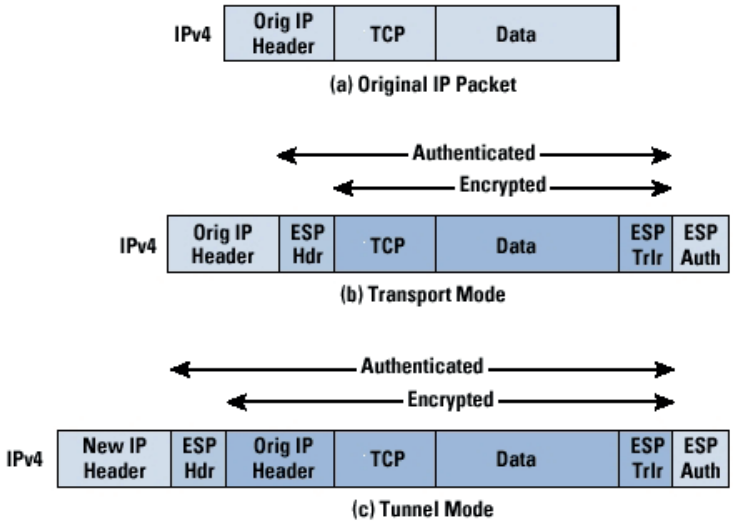

Figure 4: The new package IPSEC

Source: Andreoli (2008)

3 | METHODOLOGY

To achieve the goals specified in this project, the following steps will be taken into consideration:

The case study: The case study method or monographic method allows, through the analysis of isolated cases or small groups, to understand certain facts, Rodrigues (2005). The case study it is a methodological approach especially proper research when trying to understand, explore or describe events and complex contexts in which are simultaneously involved several factors. In this case is to show the efficiency of IPSec VPN Protocol in protecting a host-host connection with Ubuntu version 4.14.

The literature: According to Rodrigues (2005) "is the production from already published material, consisting mainly of books, journal articles and currently of material available on the Internet." Therefore, it uses materials already developed in the area under study or deepen. Likewise can be done independently or compose a greater part of research. The literature "is the basic procedure for monographic studies for which one seeks the state of the field of art on a given theme." Wire (2010). In this study, shown a brief history of events that led to the existence of IPSec on the Internet and makes use of knowledge already explored in previous implementations.

Experimental research: Consists of determining an object of study, select the variables that would be able to influence it, define the forms of control and observation of the

effects that can produce variable object in Rodrigues (2005). Therefore, the goal is to build hypotheses from the analysis of the problem and understand the factors that influence the result. Analyzing the possible problems and linking to their possible solutions, establishing the relationships of cause and effect. From this it is possible to evaluate the results. The present study attempts to test from the implementation that IPSec is an extremely safe and effective protocol, able to meet the required demand on the Internet through the Ubuntu system.

4 | INSTALATION OF THE IPSEC

To understand the IPSec will in communication, here are some concepts, then.

The study was conducted considering the client as branches (smaller) and the server as an array (highest). The idea for the progress of the company always grow, is the exchange of information, both of subsidiaries to the parent (sales quantity, necessary items, cancellations, profit, etc ...) as the matrix for affiliates (new products, change price targets, new formulas, etc ...). The information that travels, then, are valuable because the company's own life depends on this information. And that is exactly what many seek on the Internet. With the current growth of companies that come to dominate the world market, many others want the secret of success, trying to illicit means to achieve. One alternative is to attack by computer networks.

As explained earlier, it would be impossible for a company with dozens of branches have to create its own network, for the very infrastructure would be too costly. This company may be spread across the globe. However, the internet also has the feature of this company: is spread across the globe.

IPSec provides, then, that companies use the Internet to make the exchange of information between their equipment and may transfer the information more smoothly as possible, ensuring the safety and integrity.

Combined with these understandings, it is possible to proceed to the IPSec configuration itself.

For the implementation of IPSec within the Ubuntu version 14.04 system, the installation of Openswan platform is required. Openswan is a production staff apart, formalizing an IPSec standard to be used. Among the productions that exist, Openswan to fit better in the case study, it is easier to pass through NAT and Firewall, and has an important feature: the data compression.

For the full operation of the Protocol, both parties (client and server), need Openswan installed because it will deal with certificates and files needed for correct communication.

Its installation in Ubuntu system is simple, using the system default:

~$ sudo apt-get -y install openswan

After confirming the files and procedures, installation of Openswan is complete.

5 | CONFIGURATION OF THE IPSEC

With that done both at headquarters and in its subsidiaries, the first step has been taken: find a standard IPSec.

From there, IPSec becomes a gift service in Ubuntu 14.04 system. This service can be checked with the command:

~$ sudo ipsec verify

This command will show the current state of the IPSec service in the system. An example is the following image, withdrawal of implementation made:

```
Checking your system to see if IPsec got installed and started correctly:
Version check and ipsec on-path                                 [OK]
Linux Openswan U2.6.23/K2.6.32-318-ec2 (netkey)
Checking for IPsec support in kernel                            [OK]
NETKEY detected, testing for disabled ICMP send_redirects       [FAILED]

  Please disable /proc/sys/net/ipv4/conf/*/send_redirects
  or NETKEY will cause the sending of bogus ICMP redirects!

NETKEY detected, testing for disabled ICMP accept_redirects     [FAILED]

  Please disable /proc/sys/net/ipv4/conf/*/accept_redirects
  or NETKEY will accept bogus ICMP redirects!

Checking for RSA private key (/etc/ipsec.secrets)               [OK]
Checking that pluto is running                                  [OK]
Pluto listening for IKE on udp 500                              [OK]
Pluto listening for NAT-T on udp 4500                           [OK]
Two or more interfaces found, checking IP forwarding            [FAILED]
Checking for 'ip' command                                       [OK]
Checking for 'iptables' command                                 [OK]
Opportunistic Encryption Support                                [DISABLED]
```

Figure 5: Test of the service IPSec

Source: The Author

It can be noticed that the service was identified as installed, however some checks without error. NETKEY *detected, testing is disabled ICMP accept_redirects:* This error indicates the inability of the IP address routing in front of one interface to another (private to public or public to private). To correct this multiplicity of interfaces, there is a file created with *Openswan* called sysctl.conf (*system control*). This file contains a number of settings for the direction of the IP address. Four lines need to be added in this document for the IP

routing work properly.

net.ipv4.conf.all.send_redirects = 0
net.ipv4.conf.all.accept_redirects = 0
net.ipv4.conf.default.send_redirects = 0
net.ipv4.conf.default.accept_redirects = 0

The installation of *Openswan* makes several files are installed. All are important, but it is worth noting that some are essential and need to be configured so that the connection is established: *ipsec.conf:* this is the main file where the basic settings such as IP type of class, type of NAT, among others; *ipsec.d/nameofconnection.conf:* file with settings for the connection to be established, encryption, mode, etc; *ipsec.secrets:* this file is set to pre-shared key. This key is the minimum requirement for the two machines know to identify, ie, is the "password" connection; *Security Group:* For the connection to be established IPSec, some ports need to be addressed and released by the firewall. These doors can be opened in the Security Group. The doors need to be opened are the UDPs 500 and 4500. In the case of our implementation, Ubuntu 14.04 has left those liberated doors.

For the IPSec service to work with the changes, you must control it in Ubuntu through the commands:

~$ sudo service ipsec stop
~$ sudo service ipsec start

And the first for the IPSec service and the second begins again.

The main configuration file *ipsec.conf* brings a number of interesting parameters for the connection: *Config setup* - command that starts the document setup.

Virtual_private = %v4:172.16.0.0/12, %v4:192.168.0.0/16, %v4:10.0.0.0/8, %v4!10.1.1.0/24: this command shows the possibility of acceptance of connections. It is very important that the IP class types to be specified accurately. In the above case, applied to the study, is covering the IP that the branches will be able to own.

Protostack=auto: specify the type of "core" protocol to be used. The self is the pattern that is usually the most used because it is able to handle with ease firewalls.

Nat_transversal=*yes*: is important to have the characteristic of "transpose" connections through the firewall. When one of the two ends is behind a firewall, it is important that the NAT is enabled, as it is able to convert local and public IP addresses and vice versa (MICROSOFT, 2014).

The file *ipsec.d/nameofconnection.conf* is the connection configuration file created specifically for an address. The server, for example, will have several files of this, one for each branch. Already the branch only keep the array configuration.

Conn *%nameofconnection:* is the connection name that you want to put. Is not very important at the time of connection, although it is important for the matrix, especially, record the name of each connection of its branches, as if existing in large quantities, is dangerous cause confusion.

Type = tunnel: as IPSec tunneling works with, this must be specified in this file, so that the connection is established tunnel.

Authby = secret:. Various types of authentication are supported by IPSec However, in this case, the secret sets the authentication type to Pre-Shared Key, or pre-shared key (explained below).

Auto = start: this is only a specification so that the routes are created automatically when the IPSec tunnel is created.

IKE: sets out the types of algorithms used in phase 1 communication (establishment). In our example, the standard to which was ike = aes256-sha1. The encryption used will be explained later.

Phase2alg: establishes the algorithms used in phase 2 communication (packet switching), which was also followed the pattern phase2alg = aes256-sha1.

Left = EndereçoIPDaFilial: the left side or left, down the IP address of one of the branches. It is important that this address is correct, because the connection is impossible without it.

Right = EndereçoIPDaMatriz: the right hand or right, down the public IP address (the address is the Matrix).

Leftsubnet and rightsubnet: it is important to know the sub-network covered the tunnel. Often, this value is arbitrary, although it needs to be cohesive (no use putting the subnet that does not cover its own IP address). Here are placed subnetworks. Left indicating the branch and Right indicating the Matrix.

The *ipsec.secrets* file is responsible for keeping the pre-shared keys, previously mentioned in connection configuration file (just above). The structure of your setting is to store IP pairs and the keys to the communication of each pair. For the matrix it is a very interesting structure, because although you can use the same key for all communications with the command:

%*ANY* %*ANY* : PSK: “SecretKeyToCommunication”

In terms of communication, this is not so sure. The main idea is to put the IP pairs for each branch and put each key individually. Thus one example would be:

%IPDaFilial1 %IPDaMatriz : PSK: “SecretKeyToBranch1AndMatrix”
%IPDaFilial2 %IPDaMatriz : PSK: “SecretKeyToBranch2AndMatrix”

It is also worth noting that the branch must have the same key of the matrix, because otherwise, when the tunnel is closed, the branch will not be able to see the matrix and no other network equipment.

After establishing these settings, everything is almost ready.

For all parameters to be actually established, you must restart the IPSec service in branches and in the matrix. For this we use the sudo command *service ipsec restart*.

Now that everything is restarted, it is necessary to establish the connection. To do so, the command is used:

~$ sudo ipsec auto –up %nameofconnection

This command starts the branch connection in particular to the Matrix. The message displayed after establishing the connection is:

“apd” #3: STATE_QUICK1: initiate
“apd” #3: STATE_QUICK2: sent QI2, IPSec SA established tunnel mode

This indicates a successful connection. IPSec has been properly set up and ready for the transfer of files you want.

6 | CONNECTION TEST

After the tunnel established branch to the Matrix, becomes clearly visible IPSec protocol efficiency To test if there is a branch with the established IPSec service can ping other machines on the network except the Matrix.:

Ping %AddressIPOfAnotherHostOnTheNetworkOnTheInternet

Clearly this test after the reply packets that will improve the response time. This is because the tip Branch will try to get the equipment with the same pre-shared key. How not find this equipment, the packages will be jumping router in router, until the maximum number of hops is reached.

Any other established test show that the branch machine with the active IPSec connection cannot be found unless one making the search has pre-shared key.

Conclusive implementation of images;

There have been changes in the outcome of IPsec Verify command:

```
Checking your system to see if IPsec got installed and started correctly:
Version check and ipsec on-path                                 [OK]
Linux Openswan U2.6.38/K3.13.0-24-generic (netkey)
Checking for IPsec support in kernel                            [OK]
 SAref kernel support                                           [N/A]
 NETKEY:  Testing XFRM related proc values                      [OK]
    [OK]
    [OK]
Checking that pluto is running                                  [OK]
 Pluto listening for IKE on udp 500                             [OK]
 Pluto listening for NAT-T on udp 4500                          [OK]
Checking for 'ip' command                                       [OK]
Checking /bin/sh is not /bin/dash                               [WARNING]
Checking for 'iptables' command                                 [OK]
Opportunistic Encryption Support                                [DISABLED]
```

Figure 6: Output for command IPSec Verify

Source: The Author

The SystemCrontrol.conf file has its public-private IP fixed redirection:

```
net.ipv4.ip_forward=1

net.ipv4.conf.all.accept_redirects = 0

net.ipv4.conf.all.send_redirects = 0

net.ipv4.conf.default.send_redirects = 0
net.ipv4.conf.eth0.send_redirects = 0

net.ipv4.conf.default.accept_redirects = 0
net.ipv4.conf.eth0.accept_redirects = 0
```

Figure 7: File sysctl.conf

Source: The Author

The Ipsec.conf file has all the appropriate adjustment commands and covering the network and correct subnets:

```
config setup
        nat_traversal=yes
        virtual_private= %v4:172.16.0.0/12, %v4:192.168.0.0/16, %v4:10.0.0.0/8, %v4!10.1.1.0/24:
        protostack=auto

include /etc/ipsec.d/*.conf
```

Figure 8: File ipsec.conf

Source: The Author

The individual connection handled by *Ipsec.d /nameofconnection.conf* brings all the correct parameters used in the implementation of server and local client:

```
conn  Filial1

        type=tunnel
        authby=secret
        auto=start
        ike=aes256-sha1
        phase2alg=aes256-sha1
        left=10.0.106.45
        right=10.0.106.82
        leftsubnet=10.0.106.1/18
        rightsubnet=10.0.106.1/18
```

Figure 9: File ipsec.d/connection_name.conf

Source: The Author

The Ipsec.secrets file covers symmetric encryption password used in the connection: is:

```
%10.0.106.45      %10.0.106.82 : PSK: "chavesecreta2014"
```

Figure 10: File ipsec.secrets

Source: The Author

This is, without authorization for network monitoring tests, the power of the ping command has become the savior of equipment in connection test:

```
sudo ipsec auto -- up Filial1
117 "apd" #3: STATE_QUICK1: initiate
004 "apd" #3: STATE_QUICK2: sent QI2, IPSec SA established tunnel mode

ping 10.0.106.30
response from 10.0.106.30: packet loss, destination unreachable host

ping 10.0.106.82
response from 10.0.106.82: bytes=32 time=3ms TTL=64
response from 10.0.106.82: bytes=32 time=2ms TTL=64
response from 10.0.106.82: bytes=32 time=3ms TTL=64
response from 10.0.106.82: bytes=32 time=1ms TTL=64
```

Figure 11: Output of test for ping

Source: The Author

Thus, the IPSec protocol is active and ready to work. As seen in the picture above, when the ping command is used in equipment outside the network or do not have the communication key, packets cannot be delivered to the recipient.

In addition, however, it is necessary to understand some cryptographic concepts mentioned above. AES256: is the current standard advanced content encryption using symmetric key. The bytes are represented by polynomials. The operations for encryption are complex and require high throughput. And SHA1: Standard US government to hash encryption (header) that uses 160 bits and is considered strong Lambert (2004).

7 | CONCLUSION

It is shown, after implementation, the IPSec protocol efficiency in communication activity. Companies can take advantage of the protocol reliability in communications. Insecure networks such as the internet or go through little-known structure, could no longer be targets or to be feared by companies for use with full assurance that communication would produce the desired results. IPSec achieves all the objectives to what is proposed. So is chosen among others to be set as the default protocol of the future.

Although it looks like only a temporary fix while IPv6 is not enough, is not the way IPSec should be seen as it is a great power solution to be implemented. While the market has yet to decide the actual date of implementation of IPv6, IPSec becomes the largest support rod for a reliable connection. It is also important to note that IPSec will not be forgotten when IPv6 become the standard as it is implemented in this course, and the knowledge you still need to understand how it works.

In addition, it is recommended to host-gateway and gateway-gateway attempt. The implementation made in this study proved that IPSec is an important shield for a well protected on the Internet work. This implementation was done using the notions point-to-point. It is suggested that the next attempt to prove the usefulness and reliability of a host-gateway - talking mother with a network, where there is more than one branch equipment (equipment vs local network - LAN) and also in a gateway-gateway - various equipment Mother in talking to various equipment in branch (LAN vs LAN).

REFERENCES

ALENCAR, André. (2011) 'Princípios Básicos da Segurança da Informação' [online] www.vestcon.com.br/artigo/principios-basicos-da-seguranca-informacao-mnemonico-dica).aspx (Accessed 20 Setember 2014).

ANDREOLI, Andrey Vedana. (2008) 'IP Security (IPSEC)' [online] http://www.pop-rs.rnp.br/~berthold/etcom/redes2-2000/trabalhos/ipsec.html (Acessed 01 October 2014).

BATTISTI, Julio. (2013) TCP/IP – Teoria e Prática em Redes. Alpha Institute, Saint Maria, Brazil.

BATISTA, Thais, et al. (2010) 'Segurança em Redes de Computadores – Aula 10 – IPSEC e SSL' [online] http://www.metropoledigital.ufrn.br/aulas_avancado/web/disciplinas/seg_redes/aula_10.html (Accessed 01 October 2014).

BEZERRA, Romildo Martins. (2008) A Camada de Rede. Version 0.3, Cefet, Bahia, Brazil.

BORGES, Fábio, et al. (2011) VPN: Protocolos e Segurança. National Laboratory for Scientific Computing, Rio de Janeiro, Brazil.

CERT. (2014) 'Cartilha de Segurança para Internet' [online] http://cartilha.cert.br/redes (Accessed 09 Setember 2014).

COUTINHO, Antônio Abílio da Costa, et al. (2011) IPSec (Internet Protocol Security). Niterói: School of Engineering – Federal University Fluminense, Brazil.

CYBERNETX**.** (2011) 'O que é e como usar SSH' [online] http://www.cybernetfx.com/clientes/knowledgebase.php?action=displayarticle&id=71 (Accessed 25 Setember 2014).

DAS, Kaushik. (2012) 'IPv6 – The Next Generation Internet' [online] http://ipv6.com/articles/general/ipv6-the-next-generation-internet.htm (Accessed 01 October 2014).

DIGITAL, Olhar. (2013) 'Brasil é lider em computadores infectados por vírus que roubam dados bancários' [online] http://olhardigital.uol.com.br/olhar2013/?m=bus brasil-e-o-lider-em-computadores.html (Accessed 18 December 2014).

FERNANDO, Rubens. (2007) 'Criptografia de Dados – Origem e Evolução' [online] http://imasters.com.br/artigo/6360/seguranca/criptografia-de-dados-parte-01-origem-e-evolucao (Accessed 29 Setember 2014).

FIGUEIREDO, Iria Luppi. (2013) 'História das redes de computadores.' [online] http://www.oficinadanet.com.br/post/10123-historia-das-redes-de-computadores (Accessed 18 Setember 2014).

FIO, Faculdades Ourinhos. (2010) 'Manual de Normas para Elaboração de Projetos e Monografias' [online] http://fio.edu.br/manualtcc/co/7_Material_ou_Metodos.html (Accessed 20 Setember 2014).

GLOBO, Jornal O. (2014) 'Internet em Explosão' [online] http://oglobo.globo.com/s

ociedade/tecnologia/internet-em-explosao-13441261 (Accessed 18 December 2014).

GODINHO JUNIOR, L. (2004) Análise da Utilização do IPSec como Garantia de Segurança na Comunicação em Redes TCP/IP**.** Palmas, São Paulo, Brazil.

HUITEMA, Christian. (1998) IPv6: The New Internet Protocol. Upper Saddle River: Prentice Hall.

KIOSKEA, Et all. (2014) 'O protocolo IP' [online] http://pt.kioskea.net/contents/276-o-protocolo-ip (Accessed 24 Setember 2014).

LAMBERT, Jorge De Albuquerque. (2004) Cifrador Simétrico de Blocos. Master's degree thesis, course of master's degree in system of computation. Institute Military of Engineering, Rio de Janeiro, Brazil.

MARTINS, Dêner Lima Fernandes. (2000) Redes Privadas Virtuais com IPSec. UNB, Brasília, Brazil

MARTINS, Elaine. (2009) 'O que é SSL' [online]. http://www.tecmundo.com.br/seguranca/1896-o-que-e-ssl-.htm (Accessed 29 Setember 2014).

MICROSOFT. (2014) 'O que é NAT?' [online] http://technet.microsoft.com/pt-br/library/cc753373(v=ws.10).aspx (Accessed 29 Setember 2014).

MICROSOFT. (2014) 'O que é VPN?' [online] http://technet.microsoft.com/pt-br/library/cc731954%28v=ws.10%29.aspx (Accessed 29 Setember 2014).

NASCIMENTO, Edmar. (2010) 'Introdução à Redes de Computadores' [online] http://www.univasf.edu.br/~edmar.nascimento/redes/Introducao_Redes.pdf (Accessed 20 Setember 2014).

OLIVEIRA, Ronielton Rezende. (2006) Criptografia tradicional simétrica de chave privada e criptografia assimétrica de chave pública: análise das vantagens e desvantagens. Graduate work in Cryptography and Security Network, Niterói, Federal University Fluminense, Brazil.

ONE LINEA. (2009) 'O que é VPN?' [online] http://www.onelinea.com.br/pdfs/bto-vpn.pdf (Accessed 29 Setember 2014).

REDAÇÃO. (2014) 'Especialistas preveem aumento de riscos de segurança com chegada de 4G no Brasil' [online] http://corporate.canaltech.com.br/noticia/4g/Especialistas-preveem-aumento-dos-riscos-com-chegada-do-4G-no-Brasil (Accessed 01 October 2014).

REDAÇÃO. (2013) 'Relembre os maiores vazamentos de informação de 2013' [online] http://corporate.canaltech.com.br/materia/seguranca/Relembre-os-maiores-vazamentos-de-informacao-de-2013 (Accessed 01 October 2014).

RODRIGUES, Maria das Graças Villela. (2005) Metodologia da Pesquisa. EsAO, Rio de Janeiro, Brazil.

ROMAGNOLO, Cesar Augusto. (2007) 'O que é criptografia?' [online] www.oficinadanet.com.br/artigo/443/o_que_e_criptografia (Accessed 25 Setember 2014).

SANTOS, Luiz Carlos. (2002) 'Redes de Computadores e TCP/IP – modelo OSI e TCP/IP' [online] 2002. http://www.abusar.org.br/ftp/pitanga/Aulas/a01_modelos.pdf (Accessed 20 Setember 2014).

SOUZA, Wendley. (2010) 'Segurança em Redes de Computadores' [online] http://www.brasilescola.com/informatica/seguranca-redes.htm (Accessed 01 October 2014).

TANENBAUM, A. S. (2003) Redes de Computadores, 4th ed., Campus, São Paulo, Brazil.