IMPLEMENTACIÓN DE UN SERVIDOR FIREWALL-PROXY BAJO LA PLATAFORMA DE GNU/LINUX PARA LA FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS, A FIN DE LIBERAR PROCESAMIENTO DE LOS EQUIPOS DEL DATA CENTER DE LA UNIVERSIDAD TÉCNICA DEL NORTE

Galo Israel Espinosa Padilla

***Abstract*— The data network of the Technical University of the North is administered by the Directorate of Technological and IT Development, the same that has the management of the network segments of the different dependencies of the institution, including the VLANs of each one of faculties.**

The management of the institutional data network is centralized, leading to congestion of traffic and processing information in a single sector. The project allows to manage the network traffic of each faculty of the Technical University of North in order to optimize access to the Internet service and manage the same independently.

It focused in the first instance on data collection and analysis of the situation, which allowed to clarify doubts that served as a basis to guide the solution better. The design of the project was based on a layered model based on the TCP / IP network architecture.

For the implementation of the solution and the fulfillment of the objectives, it was tried to use tools that are able and need to play with the raised about an operating system that contemplates the criteria of free software.

In this way it was possible to conclude with the implementation of an alternative that allows to administer the internet access service and manage the same according to requirements requested by users.

I. INTRODUCTION

Due to the increase of information flow and processing of the equipment in the computational networks it tends to have congestion points, a firewall is a system that entails us to have greater control in the filtering and routing of the packets that cross a segment of Network and provide some form of sectorization, allowing us to manage traffic more optimally; While the proxy has the functionality of an intermediary, preserving the content requested by the users, accelerating the responses in future requests.

The technical University of the North network is managed and managed in a centralized way, condescending to congest the traffic and processing the information in a single sector, leading to a high processing, no access to services, packet queuing and equipment saturation Of the data center.

The objective is to use mechanisms that allow free processing of the data center equipment through the implementation of a firewall and proxy in each faculty, under the GNU / Linux platform, to help control the content of the information that goes through Each segment of the network.

In order to fulfill the objective, the solution design is presented, taking as reference the TCP / IP network architecture, the process of implementation and functional tests of the project, attempting to point out the conclusions and recommendations to the work carried out.

II. THEORETICAL FRAMEWORK

A. Computational Networks

Computer networks and communication technologies have been developed in such a way that new services and applications have been integrated that allow the evident process and improvement of the transmission of the information through the entities and transmission systems.

There are 4 classifications of computational networks.

CLASSIFICATION:

- Local area networks (LAN).
- Metropolitan Area Networks (MAN).
- Wide Area Networks (WAN).
- Wireless networks

B. Network architecture

The TCP / IP model describes a set of general guidelines for designing and implementing specific network protocols to enable a computer to communicate over a network. TCP / IP provides end-to-end connectivity.

The purpose of the physical layer is to transport a stream of data from one machine to another. It is possible to use several physical media for transmission. Each transmission medium has its own characteristics as; Bandwidth, delay, cost, ease of installation and maintenance [1].

The data link layer prepares the packets to be transported through the local media by encapsulation with header and a trailer to create a frame.

The internet layer takes the packages from the source to the

E. R. Carlosama estudia en la Carrera de Ingeniería Electrónica y Redes de Comunicación, Universidad Técnica del Norte, Ibarra, Ecuador (e-mail: ercarlosama@utn.edu.ec).

destination. Reaching the destination may require many jumps over intermediate routers. Therefore, the network layer is the lowest layer that handles the end-to-end transmission.

The transport layer allows the segmentation of data and provides the control necessary to re-arm these segments in the different communication streams.

Application layer protocols are used by both source and target devices during a communication session.

C. Network Hierarchy

To optimize bandwidth, the network must be organized so that traffic is conserved locally and not unnecessarily propagated to other parts of the network. Using the three-tiered hierarchical design model helps to organize the network [2].

The access layer provides connectivity to the end users, typically it is only made up of access switches.

The distribution layer interconnects the access layer to the core layer. Redundant links are spelled out to distribute access level information.

The core layer represents a high-speed backbone between scattered networks.

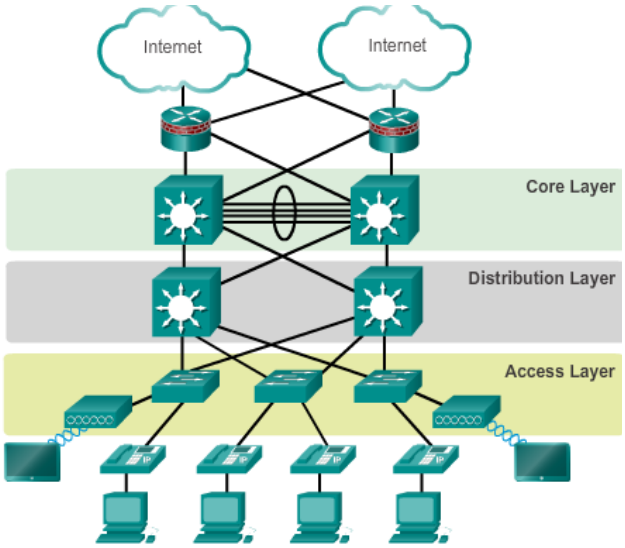

Fig. 1 Hierarchical network design

D. Firewall-Proxy

A firewall is a trusted entity that sits to separate sensitive areas within a computer network. The firewall is configured with a set of rules that depend on the security policies of the organization, which determine what network traffic will be allowed to pass and which will be blocked or rejected [3].

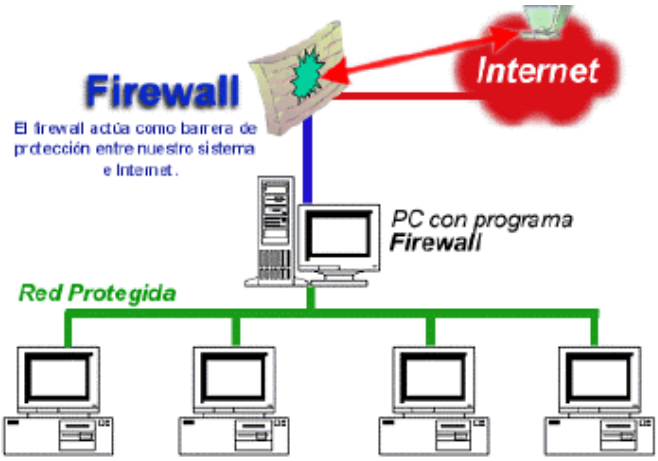

Fig2. Schematic of a Firewall.

A proxy allows other computers to connect to a network indirectly through it. When a computer in the network wants to access an information or resource, it is actually the proxy that performs the communication and then transfers the result to the initial equipment [4].

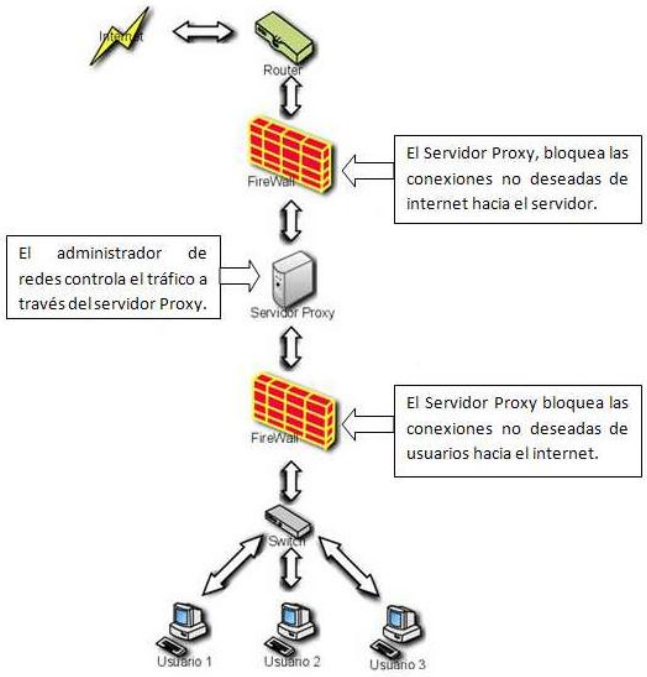

Fig3. How a proxy server works

E. Design

The first part of the design starts with the logic diagram, This model details the network topology without wiring installation details. It is a basic route map

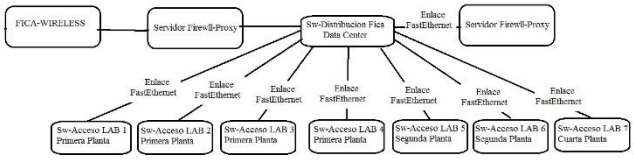

Fig4. FICA-UTN Logical Diagram

Layer 2 design details how many switch ports are being used and the speed at which each works measured in bits per second.

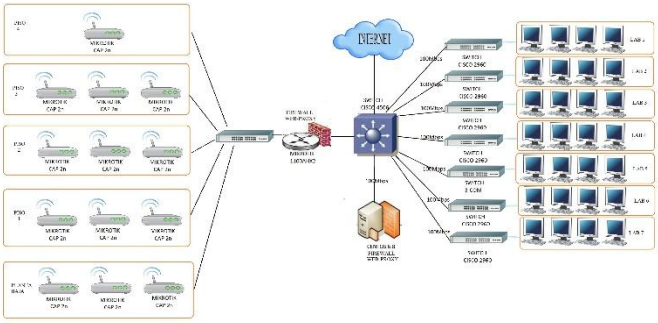

Fig5. Layer 2 Diagram Firewall-Proxy FICA

Layer 3 design details how the VLANs of laboratories of the Faculty of Engineering in Applied Sciences (FICA) were created. These subnets allow communication between segments based on Layer 3 addresses or IP addresses. For security, the addressing shown in this section only refers to the last octet; The first three octets are represented by letters x, y.

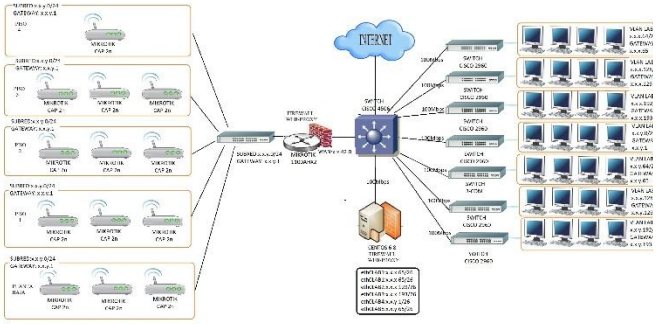

Fig6. Layer 3 Diagram Firewall-Proxy FICA

F. Implementation.

Virtual Interfaces VLAN's.

The VLANs are all the interfaces installed in the server and that will be configured for the implementation of the security rules in the Firewall.

Nombre	Tipo	Dirección IP	Máscara de red
eth0	Ethernet	172.17.41.250	255.255.254.0
eth0:64	Ethernet (Virtual)	172.17.40.65	255.255.255.192
eth0:128	Ethernet (Virtual)	172.17.40.129	255.255.255.192
eth0:192	Ethernet (Virtual)	172.17.40.193	255.255.255.192
eth0:410	Ethernet (Virtual)	172.17.41.1	255.255.255.192
eth0:4164	Ethernet (Virtual)	172.17.41.65	255.255.255.192
lo	Loopback	127.0.0.1	255.0.0.0

Fig7. Configured Network Interfaces.

IPTABLE POLICIES AND RULES

Policies are geared towards denying all traffic Input, Output y Forward.

- iptables -P INPUT DROP
- iptables -P OUTPUT DROP
- iptables -P FORWARD DROP

Input

• All traffic originating from the loopback interface is accepted, allowing you to process tasks that originate in the system.
  - iptables -A INPUT -i lo -j ACCEPT

• Traffic is accepted that is related and established, this allows the transit of data that is requested by the clients of the laboratories.
  - iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT

• Traffic to the SSH port is allowed.
  - iptables -A INPUT -p tcp --dport 22 -j ACCEPT

• Traffic is allowed to Webmin.
  - iptables -A INPUT -p tcp --dport 10000 -j ACCEPT

• ICMP traffic allowed
  - iptables -A INPUT -s $SUBREDLABS -p icmp -j ACCEPT

• Incoming traffic is accepted by port 80 either udp or tcp
  - iptables -I INPUT -p tcp -m state --state NEW -m tcp --dport 80 -j ACCEPT
  - iptables -A INPUT -p udp -m state --state NEW --dport 80 -j ACCEPT
  - iptables -A INPUT -p tcp -m state --state NEW --dport 80 -j ACCEPT

• Traffic that is addressed to the proxy port is accepted
  - iptables -A INPUT -s $SUBREDLABS -p tcp --dport 3128 -j ACCEPT

Output

• All Loopback traffic allowed
  - iptables -A OUTPUT -o lo -j ACCEPT

• All established traffic allowed
  - iptables -A OUTPUT -m state --state NEW,ESTABLISHED -j ACCEPT

Forward

• Related traffic is allowed and established
  - iptables -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT

• SSH traffic is allowed.
  - iptables -A FORWARD -p tcp --dport 22 -j ACCEPT

• Traffic destined for the file server is allowed.
  - iptables -A FORWARD -s $SUBREDLABS -p tcp --dport 139 -j ACCEPT
  - iptables -A FORWARD -s $SUBREDLABS -p tcp --dport 445 -j ACCEPT
  - iptables -A FORWARD -s $SUBREDLABS -p udp --dport 137 -j ACCEPT
  - iptables -A FORWARD -s $SUBREDLABS -p udp --dport 138 -j ACCEPT

• DNS server queries are allowed from the Laboratories VLAN.
  - iptables -A INPUT -s $SUBREDLABS -m state --state NEW -m tcp -p tcp --dport 53 -j ACCEPT
  - iptables -A INPUT -s $SUBREDLABS -m state --state NEW -m udp -p udp --dport 53 -j ACCEPT

REGLAS PROXY

To implement the rules in the Proxy you have to establish the ports and network work in which the server will act.

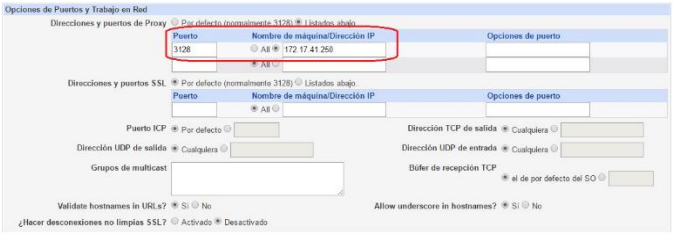

Fig8. . Proxy Address and Communication Port

CONTROL DE ACCESO

Six access control lists have been implemented each of which represents the VLAN of each laboratory.

Nombre	Tipo	Coincidiendo con...
manager	Protocolo URL	cache_object
localhost	Dirección de Cliente	127.0.0.1/32 ::1
to_localhost	Dirección de Servidor Web	127.0.0.0/8 0.0.0.0/32 ::1
SUBREDLAB1	Dirección de Cliente	172.17.40.64/26
SSL_ports	Puerto URL	443
Safe_ports	Puerto URL	80
Safe_ports	Puerto URL	21
Safe_ports	Puerto URL	443
Safe_ports	Puerto URL	70
Safe_ports	Puerto URL	210
Safe_ports	Puerto URL	1025-65535
Safe_ports	Puerto URL	280
Safe_ports	Puerto URL	488
Safe_ports	Puerto URL	591
Safe_ports	Puerto URL	777
CONNECT	Método de Petición	CONNECT
SUBREDLAB2	Dirección de Cliente	172.17.40.128/26
SUBREDLAB3	Dirección de Cliente	172.17.40.192/26
SUBREDLAB4	Dirección de Cliente	172.17.41.0/26
SUBREDLAB7	Dirección de Cliente	172.17.41.64/26
Restringidos	Expresión Regular URL	-i facebook
LABS	Dirección de Cliente	172.17.40.0/23
snmppublic	Comunidad SNMP	public

Fig9. Proxy access control list

G. Functional tests.

USING THE PROXY FOR INTERNET ACCESS

You can verify that a request is made to the Facebook website but the response is always made by the Firewall-Proxy server implemented

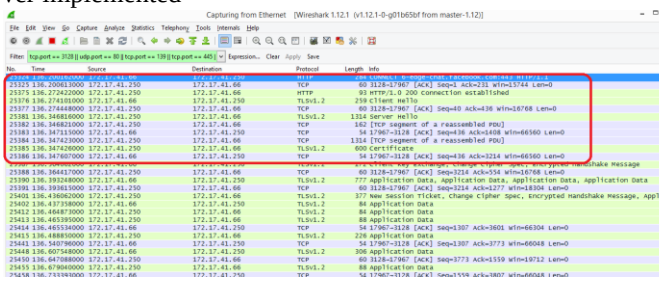

Fig10. Traffic responding to the proxy

ACCESS TIMES

You can check that the access times are reduced due to the use of the proxy server.

The test method is presented by loading a website without addressing to the proxy and another with address to the server.

Fig. 11 Load Time for a Website

GENERATOR OF REPORTS SARG

The SARG report generator is a free development tool that was implemented in the proxy presents us details in graphical form and in times of the amount of Bytes that have been transported by the network.

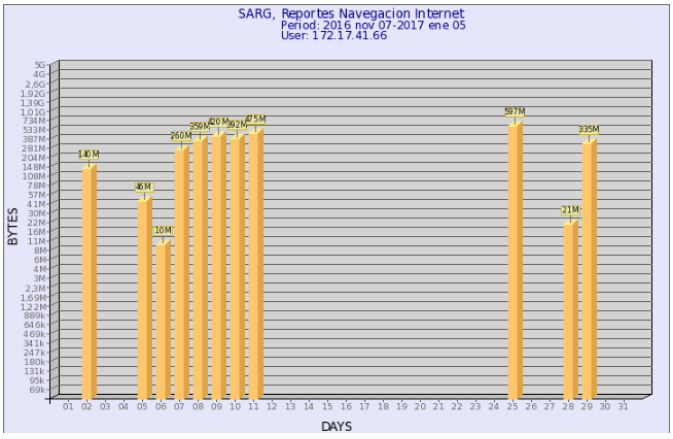

Fig. 12 SARG Chart Generator.

EQUIPMENT PROCESSING

For this test of operation is taken like experimental scene with the following details:

- It is performed in a laboratory with 34 teams.
- Processing is measured in Fica's data center distribution switch.
- The processing of the distribution equipment with the Firewall-proxy server is measured and the other measurement is performed without the Firewall-proxy server.
- Two measurements are taken: one in normal hours of use of the laboratories of 14:50 pm for 20 minutes and another in a schedule where the processing of the equipment can be recorded in a schedule where there is not much data traffic 20:30 Mp for 15 min. In both cases we tried to generate as much traffic as possible.

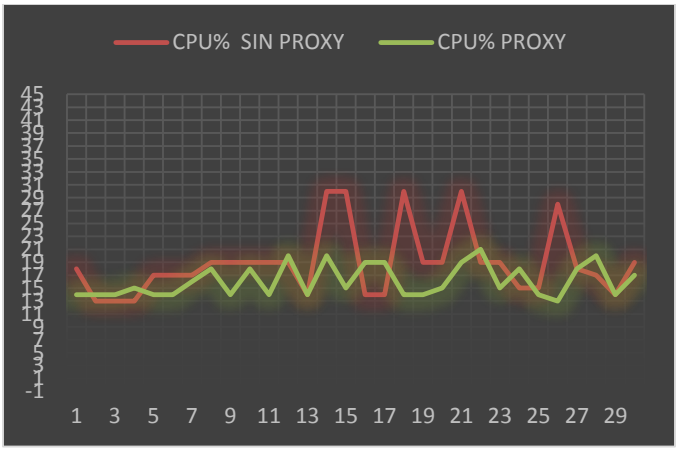

Fig. 13 Consumo de Procesamiento Sw-Dist. con servidor Firewall-Proxy y sin Firewall Proxy escenario 1.

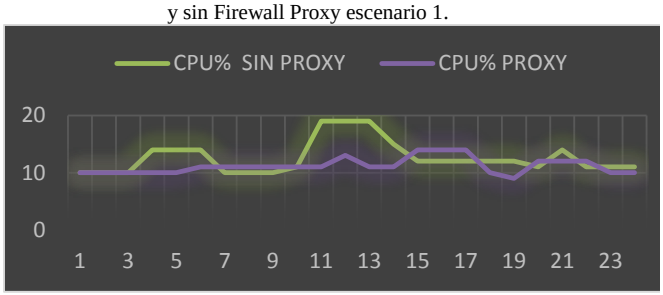

Fig. 14 Consumo de Procesamiento Sw-Dist. con servidor Firewall-Proxy y sin Firewall Proxy escenario 2.

III. CONCLUSIONS

• The Firewall-Proxy server was installed on the CentOs operating system, which complies with the concepts of freedom, and was implemented in the Faculty of Engineering in Applied Sciences, verifying the time savings of web page responses and verifying the decrease of Processing of the same Data Center equipment that is affected in increasing the CPU utilization percentage of the Firewall-Proxy server.

• The documentation of the theoretical bases, allowed to clarify doubts about the process that was taken into account for the development of the project, it was concluded that for the design it was essential to take as reference the TCP / IP network architecture, which supported the determination of Requirements, error detection, error correction, testing and maintenance in the Firewall-Proxy server implementation process.

• The creation of subnetworks in the VLAN of laboratories allowed the autonomous management of each laboratory, which has achieved a specific objective within the project development, controlling access to the internet service as well as the management of websites to which You want to access.

• The policies and rules assigned to the Firewall were defined based on the needs of each Faculty, considering the internal regulations for the use of

• laboratories and in accordance with the institutional policies managed by the data network administrator, this facilitated the assignment of rules of entry, exit and routing in the server, as well as the documentation of established policies.

• It is advisable to dimension the hardware according to the needs and functions that it must carry out, and to consider an IEEE 29148 standard for the choice of a software, since in this way it will be possible to obtain a clear vision of which requirements are necessary, as Structure and which actors will be part of the system.

IV. REFERENCIAS

[1] A. S. &. W. Tanenbaum, Redes decomputadoras, Pearson New International Edition, 2012.

[2] C. N. Academy, «Exploracion de la red,» 2015.

[3] J. Esparza Morocho, Implementacion de un Firewall sobre plataforma Linux, Quito, 1013.

[4] L. G. &. V. T. G. A. Arévalo Galárraga, nalisis, diseño e implementación de un software prototipo de firewall y servidor proxy, 2010.

V. BIOGRAFÍAS

Galo I. Espinosa P. Was born in Ibarra, Ecuador, on April 27, 1990. His primary education was in the Educational Unit, Hermano Miguel “La Salle” ” He graduated as a computer technician and studied electronics and communication networks in the Facultad de Ingeniería en Ciencias Aplicadas (FICA) University of Technology of the city of Ibarra - Ecuador.