



DESIGN AND ASSEMBLY OF A TOPOLOGICAL NETWORK DIAGRAM THAT PROVIDES SECURITY, CONFIDENTIALITY, INTEGRITY AND AVAILABILITY IN THE DATA NETWORK OF THE COMPANY

CONTROLES EMPRESARIALES S. A. S. NEIVA

Jesús D. Quintero-Polanco, Jesús D. Joven-Vega and Martin D. Bravo-Obando

Department of Electronic Engineering, Faculty of Engineering, Surcolombiana University, Neiva, Huila, Colombia

E-Mail: jdavid@usco.edu.co

ABSTRACT

The perimeter security system is a possible method of defense of a network, based on the establishment of security resources in the external perimeter of the network at different levels. This study established a perimeter security system for the company Controles Empresariales SAS - Regional Neiva taking into account the basic pillars of cyber security, Hardization manuals and ISO 27001 standard. Through the identification of different types and brands of Firewall devices, we selected the option that best suited the needs of the Company. The necessary guidelines were established for the design of the topological network diagram, the Firewall was installed, configured and parameterized, the configuration of the interfaces in Software Switch mode in order to be able to differentiate the traffic in the different VLANs. Finally, the network access users were created and the security profiles, the SSL VPNs were established and the equipment of the Company's collaborators were configured, carrying out bandwidth consumption tests, vulnerability analysis and security audit at the system.

Keywords: hardware, VPN, Web GUI, firewall, software, switch.

1. INTRODUCTION

Currently we are living the era of digital transformation, where businesses and especially information have been migrated to digital media, which implies a greater challenge for organizations, in protecting their data (Morales, Toapanta, & Toasa, 2020). In Colombia, at least 187 reports of computer theft are registered per month, the most common through the form of phishing (information fishing), which is a digital crime in which, through emails, people are deceived so that they provide information such as bank codes, identification number, passwords and carry out financial transactions (Unilibre, 2015).

Faced with this need that exists not only in Colombia but worldwide, it generates hardening or bastioning, a process that helps to protect a system or set of computer systems by applying specific security configurations to prevent computer attacks; This process can range from software measures depending on the operating system that the workstations manage, as well as hardware measures that help to protect the periphery of the system and its network in physical terms (Montaña & Duvany, 2017). In addition, firewalls known for their task of protecting the corporate intranet from untrusted users trying to access have been developed, allowing selected communications data to pass from one side of the corporate network perimeter to the other side.

By having Internet firewalls acting as agents for corporations, attackers stop closer to their gateway of origin. This changes the task of the firewall from a defensive to an offensive mode. By having firewalls working together to search and locate or block the attacker at the source gateway, there are several benefits. (Smith, R & Bhattacharya, 1999).

Controles Empresariales S.A.S - Regional Neiva is an important company in the technology sector that provides implementation, operation and support services for technology solutions. In recent years it has had an exponential growth of its activities in the departments of Huila, Tolima and Caquetá, however, it has an obsolete technological infrastructure, it does not have a system that protects the LAN and WAN networks from attacks both external and internal, incidents such as ransomware, Backdoors, among others, the Wifi network has deficiencies because it does not have an independent network of guests from the administrative network, thus causing a security breach towards the information hosted on the different servers of the Company, failing to meet the minimum requirements necessary to provide optimal service.

Companies must have an effective and efficient network design that best suits their needs, always seeking the business balance between profit and cost, following a scalability projection of both human and technological resources. Due to the above, this research proposes to generate the design and assembly of a network topological diagram that provides security, confidentiality, integrity and availability to the data network of the Company Controles Empresariales SAS Regional Neiva and in turn is composed of different subnets according to with the good practices contained in the ISO 270001 standard.

2. METHODOLOGY

2.1 Types of Firewall

To choose the appropriate Firewall, we made 3 comparisons between the three models tested (Table-1) through: 1. their characteristics, 2. the cost of the equipment in datacenter360.com who directly distribute



the three brands. 3. The usability of the application as the ability of the software to be understood, learned and used, for this we turned to g2.com, a page dedicated to making

device and software comparisons in order to guide people when it comes to make a purchase.

Table-1. Firewall model comparison.

Comparison Types	Characteristics	Fortinet FG30E	Sophos XG 86	SonicWALL Soho 250
Characteristics of the different Firewall models Tested	Firewall	950 Mbps	3 Gbps	600 Mbps
	IPS	300 Mbps	580 Mbps	250 Mbps
	NGFW	200 Mbps	310 Mbps	275 Mbps
	Threat Protection	150 Mbps	360 Mbps	200 Mbps
Market price	price Dollars	434	350	375
Usability of different Firewall models Tested	Meets requirements	9,2	8,8	8,9
	Easy to use	9,2	9,1	8,1
	Ease installation	8,8	9,0	7,7
	Ease of administration	9,0	8,8	8,0
	Support quality	9,3	8,5	8,1
	Ease of doing business	9,0	8,5	7,8
	Product direction (positive%)	9,8	9,4	6,6

According to the first comparison, the device with the best characteristics is the Sophos XG 86, followed by the Fortinet FG30E and finally the SonicWALL SoHo 250. However, the analysis of more thoroughly and seeking opinions of companies strictly dedicated to the evaluation of Security products such as Gartner, which annually presents a report called "Magic quadrant for network firewall", in 2019 positioned the Fortinet brand for the tenth time in a row as a leading brand in the development of Firewall, placing it above Sophos and SonicWALL.

Based on the three previous evaluation criteria, and the obtained results with Gartner Inc., the Firewall FG30E was chosen. Although it is the most expensive equipment, it is the one that best adapts to the need to supply or connect the different users that are found outside the network, it is also one of the best positioned in the gartner quadrant, and though the Sophos has better IPS than Fortinet, a recent study carried out directly by NSS LABS managed to show that the FORTIGATES have a rate of 99.6% exploit blocking.

2.2 Design of the Network Topology

The first consideration in this process is the implementation of the Firewall UTM-Fortigate 30E security solution, which started from the initial recognition of the Neiva Regional Business Controls network, whose original status is illustrated in Figure-1.

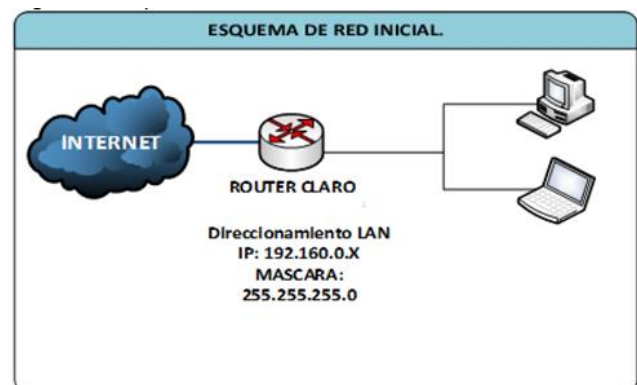


Figure-1. Initial connectivity scheme.

The previously stated information takes as a highlight the fact that a firewall is implemented to prevent unauthorized Internet users from obtaining access to private networks connected to the Internet, and that all network traffic that enters or leaves the local network passes through the firewall, which examines each piece of data and blocks specified in the security criteria; For this reason, it is chosen to choose a perimeter security device to meet the needs of information availability regardless of where the end users are, control of web traffic content in order to make the working day more efficient, give Internet access to external users of the Company without compromising the information hosted on the company's servers, protect the Customer Database from external attacks.

Therefore, the design is illustrated in Figure-2, in this it is proposed to contract 2 internet channels in order



to have channel redundancy and thus solve the service availability problem, in the same way a firewall is added which will be in charge of controlling the incoming and outgoing traffic of the data network. In addition, it is understood that the same equipment is going to be used as a DHCP server and its functions correspond, on the one hand, to the routing of the different requests from the clients that will be in 3 different network segments, this in order to give way to the good practices contained in the ISO 270001 standard; while, on the other hand, it is in charge of managing the users who will access the network through VPN.

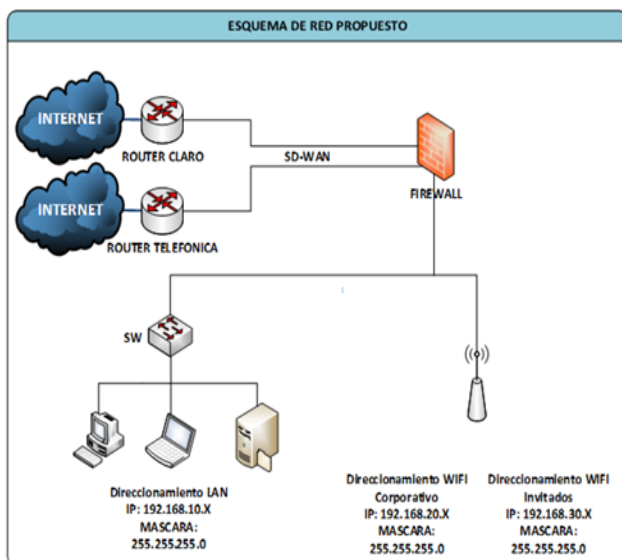


Figure-2. Proposed connectivity scheme.

2.3 Firewall Implementation

The implementation defined for Controles Empresariales S.A.S regional Neiva, is a FortiGate 30E UTM solution to meet all the needs in terms of security and availability of data, applications, servers and end users. The type of solution applied was configured with an SD-WAN, which is served by 2 internet channels from two different ISPs, thus allowing to ensure the availability of the service and at the same time control incoming and outgoing traffic to the data network of the regional. In addition to this, it serves as a VPN terminator to bind services to users outside the network.

2.3.1 Internet services. Internet services are connected to ports "WAN1" and "port1" of the FortiGate 30E

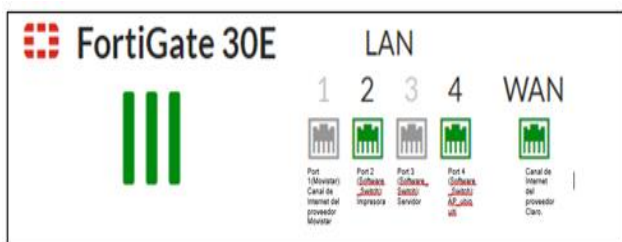


Figure-3. FortiGate 30E physical interfaces.

2.3.2 LAN connection

The LAN addressing of the company controls Empresariales S.A.S regional Neiva was segmented into three different networks. The first network called Red_LAN, is the network for all corporate users connected via Copper; the second network (Wifi_Administrativa), which is for all corporate users connected to the network wirelessly; and the third network called Wifi_Invitados, which is a network created for all external people who go to the office and request an internet connection. The materialization of what has been previously described requires the creation of a Software Switch, which converts the LAN ports of the FG-30E into a layer 3 switch, for this reason, it is seen in table 5 and in Figure-5 that Wi-Fi networks are Tagged by VLANs ID.

Name	Type	Members	IP/Netmask	Administrative Access	DHCP Ranges
Hardware Switch					
SD-WAN Interface		2 Member(s)			
Software Switch					
Red_Lan	Software Switch	lan2, lan4, lan3	192.168.10.254/255.255.255.0	PING, HTTPS, FMG-Access	192.168.10.1-192.168.10.253
Wifi_Invitados	VLAN		192.168.30.254/255.255.255.0	PING	192.168.30.1-192.168.30.253
Wifi_Administra	VLAN		192.168.20.254/255.255.255.0	PING, HTTPS	192.168.20.1-192.168.20.253

Figure-4. Configuration of network interfaces in the LAN Network.

2.3.3 SD-WAN

Members of the SD-WAN. It balances channels to achieve the best performance when directing traffic to the Internet. Since we seek to take full advantage of the SD-WAN functionality and have greater availability in the service, it was necessary to contract redundancy of internet channels by 2 different ISPs. In this case, it is to indicate that the main channel of course is connected to the WAN port and the Lan1 port is connected to the Movistar internet channel. As can be seen in figure 6, the two channels have the same cost, which means that the device will automatically be in charge of sending traffic to the WEB through established SD-WAN rules or evaluating parameters such as Jitter, latency and ping.

2.3.3.1 SD-WAN Rules

The necessity this item is that the different networks go to the internet, for this, 2 rules were created: 1. The 3 networks always go out through the main channel, which is of course, this is because this network has a greater bandwidth than the Movistar network. 2.egla indicates that in the event that the first rule is not met, all users as a contingency must go out to the WAN through the Movistar channel.

2.3.4 Local users



The task of the step considered here is the creation of local users in the firewall, in this sense, it was necessary to collect the MAC information of each computer because the firewall was configured in such a way that to assign DHCP it must recognize the address physical of the equipment that is trying to connect, in case the MAC is not recognized, what the device does, is to block all the traffic coming from that device.

2.3.5. DHCP Reservation

The important aspect when configuring the firewall and the DHCP Server is that there are computers such as servers, printers, APs, among others, which must always keep the same IP address. It is precisely in compliance with these aspects that Figure-5 shows that the firewall needs a unique comparison criterion on each computer, in this case the MAC address, to carry out the IP reservation.

2.3.6 Firewall policies

The routing policies are executed in the different networks (see Figure-6), and they occur once the DHCP is ready for the different users. Not before, without giving clarity that the policies in this type of device are applied in a hierarchical order, that is, from top to bottom.

Address Assignment Rules

Type	Match Criteria	Action	IP
MAC Address	MAC address: 60:eb:69:d5:4e:9d	Reserve IP	192.168.10.201
MAC Address	MAC address: 50:46:5d:32:d4:e8	Reserve IP	192.168.10.1
MAC Address	MAC address: a0:d3:c1:81:4f:ac	Reserve IP	192.168.10.200
Implicit	Unknown MAC Addresses	Assign IP	

Figure-5. General scheme of policies implemented in the Fortigate 30E.

The policies of rules of the Network of the company Controles Empresariales S.A.S regional Neiva. Are the following:

The first group of routing policies exposes two rules, the first whose ID is 8, its objective is to allow the lan network to see all the servers of the Any desk application, and thus be able to access any computer on the lan network through this tool when required; the second is the output of data from the Red_Lan to the internet, in which 4 enabled security profiles are observed, whose sole purpose is to restrict the content of the network and thus prevent users from browsing malicious pages, with sexual content, among others.

The Second Group of routing policies basically allows users contained within the group Lan_Administrativa and who belong to the Lan Network to see the users of the network Wifi_Administrativa The third group of routing policies allows users to connect through the vpn ssl access only the computers that are in the Red_Lan

The fourth group of routing policies mainly allows users contained within the Wifi_Administrativa group to see the users of the Red_Lan network

The fifth group of routing policies has three rules, namely: the first rule with ID 7, allows the Wifi_Administrativa network to see all the servers of the Any desk application, in order to allow connection to any computer on the lan network by middle of this tool; the second is the output of data from the Wifi_Administrativa to the internet, in which 4 enabled security profiles are observed, whose sole purpose is to restrict the content of the network and thus prevent users from browsing malicious pages, with sexual content, among others .

The last policy, no less important, is in charge of allowing mobile devices to navigate to the Internet with the restrictions contained in the general security profiles. the rule with Id 4, which was created to allow the guest Wi-Fi_Network to see only the Server where the unify network controller administration console is installed, because if this does not happen the captive portal created for this network will not It would work. The Routing policy with ID number 3 is responsible for the output of traffic to the Internet from the Wi-Fi network for guests, in this it is shown that the security profiles are enabled by default. The rule with ID 0, this one is in charge of blocking any type of routing that does not classify in the previous policies.

2.3.7 Security profiles-UTM

FortiGate combines a set of security features to protect networks from different threats. These features when included within a single security appliance are known as Unified Threat Management (UTM). These functionalities can be applied through profiles, which are called within the policy at the time they are to be used; the features included in UTM are the following, which are set out below:

- Antivirus
- Application control
- SSL inspection
- Web filtering
- Intrusion prevention system (IPS)

Antivirus is the security profile in charge of blocking all viruses from protocols such as HTTP, SMTP, POP3, IMAP, FTP, CIFS among others, as shown in figure 20. Once the profile finds a malicious file, it sends it to Fort sandbox, which through advanced threat protection determines if the file contains any type of malicious program.

The configuration of the application control security profile made it necessary to analyze the company's business core and take into account the different levels of hierarchy between users; due to this two



profiles were configured (App_Directivos and App_Generales).

In addition, what has been done with the directive and general App is specified, as follows:

- App Directivos. The APP_Directivos required the restriction of 3 browsing categories (Game, P2P and Proxy) as evidenced in Figure-6, because they are categories that are not necessary when fulfilling the functions of the position, the other 15 categories they were placed in Monitoring mode, which is a mode that accepts all traffic, but generates logs.

App Generals. In the case of APP_Generals, 5 browsing categories were restricted (Game, P2P, Proxy, video / Audio and social. media) as shown in figure 6. In the case of social networks, an exception was made to the WhatsApp application so that allow users to send text messages, voice memos, files and make calls

This point is oriented to meet one of the needs of the Requirements for the Design of the Network Topology. Thus, it was necessary to configure the SSL-VPN to give access to the different corporate users being outside the Business controls network Web filtering is a special security feature of the UTM Firewall that is responsible for viewing and controlling the end-user traffic to the Internet; this service is categorized into 6 main groups, which in turn have different subcategories.

Likewise, it should be emphasized that the objective of web filtering is to optimize internet service, execute computer security locks and considerably reduce idle browsing by end users. 2 security profiles were created (Nav_Directivos, Nav_General). To increase the security levels of the VPN within the configuration, we changed the default connection port, in the same way the range of specific IPs allowed by the device was modified and only users created locally were accepted. 10 users were created for the different corporate officers

2.4 Implementation of the UAP-AC-LR Management Server

The fulfillment of all the needs of the requirements for the Design of the Network Topology, in Controles Empresariales S.A.S regional Neiva implied installing an administration Software called Unifi Network Controller, in order to manage two networks called (Wifi_administrativa, Wifi_Guests). These networks are tagged in their traffic by VLAN, and have two different authentication security systems, the first of them has Wpa2 Security encryption and the second is managed by a Hotspot who requests Authentication voucher every time you want make use of it.

2.4.1 Server to install

The "Unifi Network Controller" tool, a PC was prepared with Windows 10, Core i7 processor, 8.00 Gb RAM, 64-bit operating system, x64 processor.

This application is in charge of configuring and adopting all the Unifi access points, and it is used to

manage them centrally, as well as to monitor them in the event of a failure in the system, a situation that is illustrated in Figure-6.

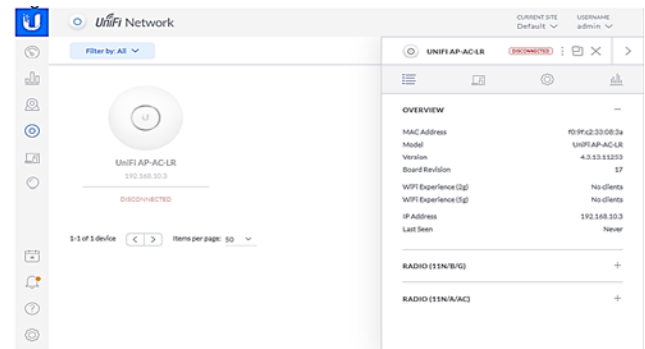


Figure-6. Unifi network controller management console.

2.4.2 Unifi network controller

Once the Aps Controller called Unifi Network was installed, the configuration process began, for this, two networks were configured. In the case of the Administrative Wifi, it was labeled with VLAN 200 because as indicated in section 4.3. Lan connection. The firewall will manage that network through that VLAN. WPAPSK was assigned as security encryption for when the administrative staff required to connect to this network, additionally, to have a better performance of the WiFi network it was necessary to activate the Combine name functionality, which means that the Ap will be able to support 2GHz and 5GHz networks with the same SSID.

For the Wifi_Ivitados, it was necessary to activate the Guest Network to work through a captive portal (Hotspot), which means that every time an external person is going to connect to this network and try to navigate, the controller will automatically do so. Redirect to a portal where you will require a voucher, this in order to make the administration easier and that this network is completely transparent to the Wifi_Administrativa. tagged with VLAN 300 because as indicated in section 4.3. Lan connection. The firewall will manage that network through that VLAN. Additionally, to have a better performance of the WiFi network it was necessary to activate the Combine name functionality, which means that the Ap will be able to support 2GHz and 5GHz networks with the same SSID.

2.4.3 Guest Control

To carry out the Guest control configuration previously configured in the Wi-Fi_guest Network, it was necessary to configure the following parameters:

- Guest Policies. Within the policies of the guest portal it was defined that the authentication to the portal would be through a Hotspot, in the same way it was established that the maximum time that a person could be connected to the hotspot would be 8 Hours, it was enabled that when a person needs to connect to the network, they are redirected to a URL with HTTPS security and encryption configured on the server.



- Hotspot. Following this, we proceeded to enable the Hotspot authentication by means of vouchers.
- Voucher Customization. In the case of Vouchers, its functionality was enabled that cancels templates with personalized changes, that is, it will generate a voucher with a default template.
- Portal Customization. Once the configuration was finished, we proceeded to customize the entire access interface that is shown to the invited user at the time of validation in the captive portal. For this, it was chosen that the template was going to be Angular JS since it is more stable than the legacy JSP. The title of the page "Portal Controls Empresariales" was established and as a security policy the terms of service box was enabled. In the same way, the portal was customized with 2 languages (English and Spanish). The company logo was attached and the company's corporate colors were selected.
- Vouchers. Likewise, from the portal, several vouchers were generated that allow guest users to navigate to the internet, an example of this can be seen in Figure-7.

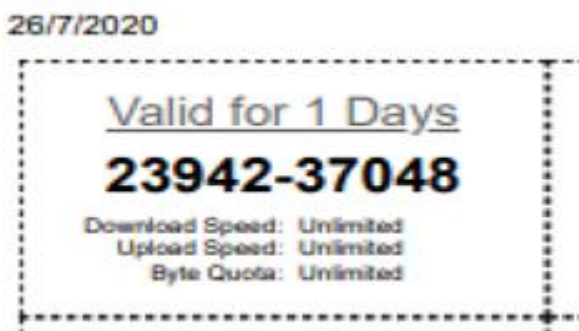


Figure-7. Voucher that validates the guest user and allows him to navigate to the internet.

3. RESULTS

3.1 Vulnerability Analysis

Vulnerability is defined as a weakness or risk in the security of the system, which can compromise the confidentiality, integrity and availability of the information. To carry out this test, a tool called Nessus was used, which is a security program specifically designed to scan vulnerabilities in different operating systems. The first test was run in a network topology lacking a firewall, where the ISP router is the one who is directly in charge of routing all traffic to the WAN and vice versa, as shown in Figure-8.

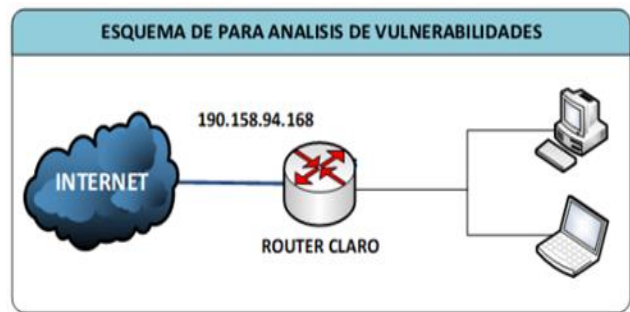


Figure-8. Scheme for vulnerability analysis.

A particular feature of this software gives a score to each risk based on CVSS (Common Vulnerability Scoring System) V3.0., And turn each vulnerability with a CVE (Common Vulnerabilities and Exposures), which is a list where each vulnerability or exposure found annually is recorded, and in which each reference has a CVE-ID identification number.

The test result found 2 critical vulnerabilities, 1 vulnerability with high risk, 14 with medium risk, 3 with low risk and 38 informational.

The second test carried out was with the network topology shown in Figure-9. This topology includes the firewall and in turn, the ISP router becomes in bridge mode in order to give it total control over the IP. Post static to the Firewall.

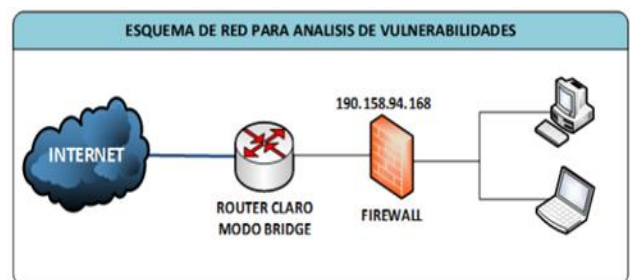


Figure-9. Network topology implemented for vulnerability analysis with the firewall mounted.

The test result details that the critical vulnerabilities disappeared, as well as the high and low ones, the average vulnerabilities decreased considerably from 14 to 6, and the informative notes decreased from 38 to 33. With this test it was shown that the Firewall helps to close existing security gaps in the network, which are sometimes imperceptible to network administrators. In addition, it shows that the security level of the network went from being in a critical state to a medium state that can continue to be improved by intervening the network equipment, and making the respective updates and recommendations.

3.2 Bandwidth Consumption

One of the existing problems in the regional recipient of the project was the bandwidth of the internet channel, as shown in Figure-10; the channel always lived saturated causing all users to present failures when using



corporate tools such as Teams, Microsoft dynamic 365, among others.

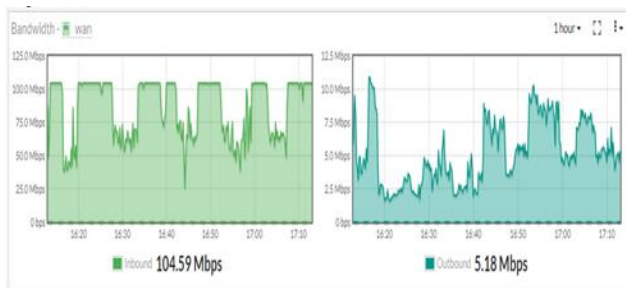


Figure-10. Network bandwidth consumption before applying security policies.

Once the security profiles were applied (Application Control, web filtering, ssl inspection and the antivirus filter), the bandwidth consumption was considerably reduced, as can be seen in Figure-11, the bandwidth consumption happened to be an average of 30 Mb, which means that users' leisure time also decreased, thus increasing office productivity.

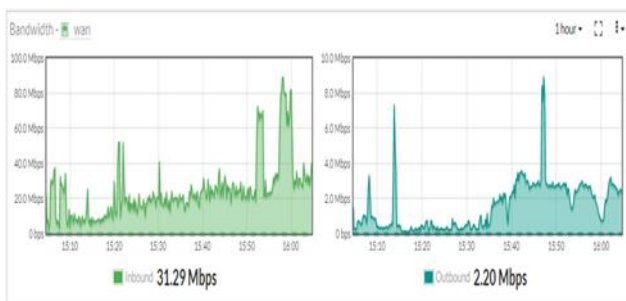


Figure-11. Network bandwidth consumption after applying security policies.

Hack-Inn SAS, a leading security company specialized in information security and cybersecurity, certifies that once the exhaustive review of the vulnerability analysis carried out in the company Controles Empresariales SAS regional Neiva was carried out, the risk level dropped considerably given that the firewall solved the critical, high and part of the media levels, which is why a certificate is issued that these actions closed the security gaps that had been presented, forming a preventive barrier from possible attacks on the network centralized access to files stored on the server without having to be on the same network.

4. CONCLUSIONS

The study focused on the design and assembly of a network topological diagram that provides confidentiality, integrity and availability, in addition to meeting existing needs in the company's data network.

Finding that the application of security profiles helps greatly to increase the productivity of users, as well as to make adequate use of the bandwidth of the Internet channel.

Furthermore, conducting vulnerability scans provides valuable information that network administrators can use to close security breaches.

Installing perimeter security systems helps to correct weak security problems in the network, thus reducing the risk of losing valuable information for the normal development of the company's commercial activities.

Vpn SSL substantially assist users when they are off the network, thus providing centralized access to files stored on the server without having to be on the same network.

5. RECOMMENDATIONS

Keep the Firmware of the equipment updated to the latest version since in this FortiIOS improvements are included and the antivirus signature base is updated, IPS.

Backup copies of the FG-30E equipment configuration must be made periodically in case some eventuality happens in which you see forced to do a total system restore.

Do not open unnecessary ports that may involve network security.

Avoid at all costs the use of Tools such as Team Viewer, any desk or any other type of software that may compromise in any way the perimeter security of the company.

REFERENCES

- BELCIC, Iván. ¿Qué es el malware? Avast [online], 2019. Obtenido de: <https://www.avast.com/es-es/c-malware>
- CASTRO, Paul. Qué es Hardening. Blog Smartekh [Online], 2012. Obtenido de: <https://blog.smartekh.com/que-es-hardening>
- CEFIRE. Corta fuegos. CEFIRE. [Online], s.f. Obtenido de: http://cefire.edu.gva.es/pluginfile.php/1072694/mod_resource/content/2/33_cortafuegos.html#:~:text=Cortafuegos,Ocultar&text=Los%20cortafuegos%20tambi%C3%A9n%20pueden%20ser,conectadas%20a%20Internet%20%20especialmente%20intranets.
- CISCO. Cómo funcionan las redes privadas virtuales. CISCO [Online], 2008. Obtenido de: https://www.cisco.com/c/es_mx/support/docs/security-vpn/ipsec-negotiation-ike-rotocols/14106-how-vpn-works.html
- COSIO, Ernesto. Modelado de una arquitectura de red definida por Software (SDN) para el aprovisionamiento de recursos utilizando Cross- Layer Desing (CLD). México, Centro de Investigación Científica y de Educación Superior de Ensenada - CICESE, 2017. Obtenido de: <https://207.249.117.38/jspui/bitstream/1007/898/1/Formato%20Tesis%20-%20Ernesto%20Cosio%202009-02-2017%20biblioteca.pdf>



DÍAZ, Igor. Implementación del sistema video vigilancia IP para mejorar la seguridad de activos en una Universidad Pública. Perú, Universidad Peruana de los Andes. 2018. Obtenido de: <http://173.244.209.199/bitstream/handle/UPLA/831/DIAZ%20HUARANCCA%20Igor%20Alexi.pdf?sequence=1&isAllowed=y>Fortinet.

Las intrusiones maliciosas se transforman, y también lo hace FortiGateIPS Remediation. Fortinet. 2018. Obtenido de: <https://www.fortinet.com/blog/business-and-technology/fortinet-and-ngips>Fortinet.

Port forwarding. Fortinet Document Library [Online], s.f. Obtenido de <https://docs.fortinet.com/document/fortigate/6.0.0/cookbook/186598/port-forwarding>

Fortinet. What is a Firewall? Types of Firewalls and How they Work. What is a Firewall. Fortinet [online], 2020. Obtenido de <https://www.fortinet.com/resources/cyberglossary/firewall>

Grooten, Martijn y Luca, Adrian. VBWeb Comparative Review-Winter 2020. VirusBulletin. [Online]. 2020. Obtenido de: <https://www.virusbulletin.com/virusbulletin/2020/01/vb-web-comparative-review>

KAUR, Rajpreet, Hils, Adam, D' Hoinne, Jeremy and Watts, John. Cuadrante mágico para firewalls de red. Obtenido de: <https://www.gartner.com/doc/reprints?id=1-1OIMIBCY&ct=190919&st=sb>

Molenaar, Rene. Cisco IOS NAT Port Forwarding. NetworkLessons [Online], s.f. Obtenido de: <https://networklessons.com/cisco/ccie-routing-switching/cisco-ios-nat-port-forwarding#:~:text=NAT%20port%20forwarding%20is%20typically,to%20host%20on%20the%20inside>

SUÁREZ, David. Redes WAN definidas por Software SD-WAN. España, Universidad Abierta de Cataluña, [Online], 2020. Obtenido de: <http://openaccess.uoc.edu/webapps/o2/bitstream/10609/116386/8/astifrTFG0620memoria.pdf>

TALLER DE INGENIERIA EN SOFTWARE (s.f.). Evaluación de las aplicaciones web. Obtenido de: <https://sites.google.com/site/talleringsoftware/unidad-6-verificacion-y-validacion-de-aplicaciones-web-1>

Oracle. El servidor DHCP. [Online], Oracle s.f. Obtenido de: https://docs.oracle.com/cd/E24842_01/html/820-2981/dhcp-overview-14a.html