PERIMETER SECURITY FOR DATA NETWORK

Torres Bolaños Rodrigo Javier
Universidad Técnica del Norte
rjtorres@utn.edu.ec

Summary.- The evolution of technology and the constant demand for security have allowed perimeter security systems in networks evolve to provide greater reliability to both internal and external users on transparency and protection of your information to access different services, today there are a number of people who use their knowledge and professional ethics in the wrong way when entering restricted computer networks I caused multibillion-dollar losses worldwide.

This article aims at performing an analysis of the steps and requirements necessary for the design of a system of perimeter security for a network of data.

I. INTRODUCTION

Perimeter security is a method of defense of computer networks, which involves installing communications equipment in which security policies necessary for optimal functioning is established; these teams are placed between the external network and internal network, allowing or denying access to user internal and external to different network services.

The implementation of perimeter security consists of three stages Segmentation Network, Firewall and Intrusion Prevention System IPS. For optimization of technological resources is essential virtualization, this requires a team with excellent physical and logical as this will be installed in software for service virtualization features.

II. PERIMETER SECURITY

"The perimeter security bases its philosophy on the protection of all computer system of a company from "outside" that is compose an armor that protects all sensitive elements of attack within a computer system. This implies that each transmitted packet traffic should be dissected, analyzed and accepted or rejected based on their potential security risk to our network" [1]

For the design of perimeter security system is essential to make an analysis of the current situation of the network thus achieving know which network segments of data need more protection, is to say that network segment must have or not to access permissions to the network or internet services.

Moreover, the use is free software to implement the Firewall and IPS is recommended.

A. Segmentation Network

The first step to the implementation of perimeter security is a correct network segmentation by means of VLANs with its own IP address. Having a record of VLANs and IP used in the network, you can apply policies to each of the segments.

By segmenting the network must take into account the possible growth of the data network, to be able assign an IP address pull that covers both the current situation and the possible growth.

After the network segmentation active network equipment must be configured such as Layer 2 and Switches Routers, Routers absence configuring a Layer Switch 3 is necessary.

Below is showing the necessary settings for the active network

- **Support equipment configuration**

Switch#copy running-config tftp
Address or name of remote host []? A.A.A.A
Destination filename [router01-confg]? router01-config-20120730.bak
!!
830 bytes copied in 0.489 secs (1022 bytes/sec)

- **Equipment name configuration**

Switch>enable
Switch#configure terminal
Switch(config)#hostname NOMBRE
NOMBRE(config)#

- **Password settings**

Switch(config)#enable password PASSWORD-ENABLE
Switch(config)#enable secret PASSWORD-SECRET
Switch(config)#line console 0
Switch(config-line)#password PASSWORD
Switch(config-line)#login
Switch(config-line)#exit
Switch(config)#line vty 0 4
Switch(config-line)#password PASSWORD
Switch(config-line)#login
Switch(config-line)#exit

- **VTP Configuration**

Switch#vlan database
Switch(vlan)#vtp server ó Switch(vlan)#vtp client
Switch(vlan)#vtp domain DOMINIO-VTP
Switch(vlan)#vlan password PASSWORD-VLAN
Switch(vlan)#exit

- **VLANs Create**

Switch#vlan database
Switch(vlan)#vlan NUMERO-DE-VLAN name NOMBRE-DE-LA-VLAN
Switch(vlan)#exit

- **Trunk link configuration**

Switch(config)#interface fastethernet #/#
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk native vlan #-VLAN-NATIVA
Switch(config-if)#switchport trunk encapsulation dot1q
Switch(config-if)#escription NOMBRE-DEL-ENLACE
Switch(config-if)#no shutdown
Switch(config-if)#exit

- **Add ports to VLANs**

Switch(config)#interface fastethernet #/#
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan #
Switch(config-if)#switchport voice vlan #
Switch(config-if)#description DESCRIPCION-DEL-PUERTO
Switch(config-if)#no shutdown
Switch(config-if)#exit

- **IP configuration on the VLANs**

Switch(config)#interface vlan #
Switch(config-if)#ip address A.A.A.A B.B.B.B
Switch(config-if)#no shutdown
Switch(config-if)#exit

- **HSRP Configuration**

Switch(config)#interface vlan #
Switch(config-if)#standby #-NUMERO-DEL-GRUPO ip A.A.A.A
Switch(config-if)#standby #-NUMERO-DEL-GRUPO priority 200
Switch(config-if)#standby #-NUMERO-DEL-GRUPO preempt
Switch(config-if)#exit

- **Enable layer 3 functions on the switch**

Switch(config)#ip routing

- **STP configuration**

SwitchPrincipal(config)#spanning-tree vlan 1 root primary
SwitchPrincipal(config)#exit

SwitchSecundario(config)#spanning-tree vlan 1 root secundary
SwitchSecundario(config)#exit

- **Default Gateway configuration**

Switch(config)#ip default Gateway A.A.A.A

- **DHCP server configuration**

Switch(config)#ip dhcp pool NOMBRE-DEL-POOL
Switch(dhcp-config)#network A.A.A.A B.B.B.B
Switch(dhcp-config)#default-router A.A.A.C
Switch(dhcp-config)#dns-server D.D.D.D
Switch(dhcp-config)#exit
Switch(config)#ip dhcp excluded-address A.A.A.A A.A.A.X

- **SSH configuration**

Switch(config)#ip ssh authentication-retries #
Switch(config)#ip ssh time-out #
Switch(config)#ip shh versión #
Switch(config)#line vyt 0 4
Switch(config-line)#transport input ssh telnet
Switch(config-line)#exit

- **Routing on Switch configuration**

Switch(config)#ip route A.A.A.A B.B.B.B C.C.C.C

- **MOTD configuration**

Switch(config)#banner motd &MENSAJE-A-DESPLEGAR&
Swtich(config)#exit

- **Encryption password**

Switch(config)#service password-encryption

- **Save the settings**

Switch#copy running-config startup-config

B. Virtualización

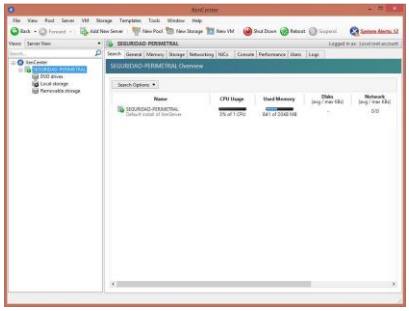
For optimization of resources, it is necessary virtualization services, it is necessary to have a team of good technological features. In the market there are several software for virtualization services of different brands and owners, but there is also free software which is oriented virtualization.

In this section the use of XEN-Server, which is based on open source software and is oriented network service virtualization is suggested. XEN-Server complies with many features virtualization server owners, but it can be accessible for any user to be Free Software.

Besides XEN-Server, there is software XEN-Center which is an application that all virtualized servers that are installed and configured on the corporate network is administered.

Below is the display screens shown XEN-Server.

a) Screen presentation of XEN-Server & XEN-Center.



b) Screen presentation of XEN-Center

C. Firewall

Firewall implementation is done by using the IP-Tables making settings on the console of CentOS operating system, but there is a graphical method in which the user can configure the necessary parameters and graphical interface which includes the commands are used to configure the Firewall in their respective scripts, this is done using Shorewall and Webmin.

- **Shorewall**

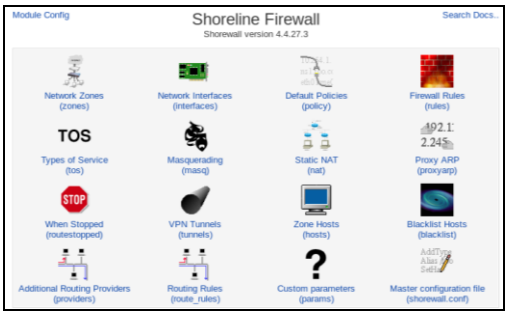
"A high-level tool for configuring Netfilter. You describe the requirements for firewall, Gateway using the entries in the configuration file set. Shorewall reads those configuration files and with the help of iptables, iptables-restore, and other utilities and configures Netfilter subsystem Linux Network" [2]

- **Webmin**

It is a web-based interface for managing Linux system, allowing users easy interaction between him and the functionality of the operating system by

eliminating the need to manually edit configuration files, in this case will allow easy handling of Firewall Shorewall.

For the Firewall, you must configure several files which are edited areas of our network interfaces and firewall rules that allow or deny access to different services.



c) Setup screen Shoreline Firewall

The configuration files that should be avoided for the Firewall and which are performed by Shoreline Firewall are:

- **Network Zones**

Represent the networks that connect to the firewall, to implement perimeter security 4 zones are established:

fw.- Represents the firewall to implement own system

dmz.- Represents the DMZ where the servers.

local.- Represents the intranet.

net.- Represents th output to Internet.

Zone ID	Parent zone	Zone type	Comment
dmz		IPv4	Hacia la DMZ
local		IPv4	Hacia la Red Local
net		IPv4	Hacia Internet
fw		Firewall system	

d) Setup Zones on Shoreline

- **Network Interfaces**

Are all interfaces installed on the server to be configured to implement security rules in the Firewall University all three interfaces Ethernet 10/100/1000 needed and are distributed in the following way.

eth0.- This interface link connects to the Internet.

eth1.- This interface link connects to the DMZ

eth2.- This interface link connects to the

Interface	Zone name
eth2	local
eth1	dmz
eth0	net

e) d) Network Interfaces configured in ShorelineInterfaces de red configuradas en Shoreline

- **Default Policies**

They are default policies to be configured in Firewall, because it is used policy everything that is not specifically permitted is denied, you should deny all transmissions between different zones that are created in the Firewall Server, these policies are the last to be analyzed within the Firewall settings, it first analyzes the firewall rules and everything that is not allowed in these rules will be denied by these policies. There is also a default policy that states deny traffic from any source to any destination that is analyzed at the end of all Firewall Rules and Policies Default.

Source zone	Destination zone	Policy
dmz	net	DROP
dmz	local	DROP
dmz	Firewall	DROP
net	dmz	DROP
net	local	DROP
net	Firewall	DROP
local	net	DROP
local	dmz	DROP
local	Firewall	DROP
Any	Any	DROP

f) Setup default policies in Shoreline

- **Firewall Rules**

Using the Firewall Rules different security policies where the origin, destination, the communication port is specified and sets whether or not to allow access is created. Upon being launched the Firewall Server these rules are the first to be analyzed and if necessary that there is no policy shall that which specifies the Default Policies that is refuse everything.

To configure the Firewall Rules shall take into account the ports needed by each of the services it provides and requires the computer network and access only to those ports are allowed.

Safety rules used are those described below in general..

- ✓ From the Internet to the DMZ to the Intranet and only the necessary ports for each of the services are enabled
- ✓ From the DMZ to the Internet and Intranet only the necessary ports for each of the services are enabled.
- ✓ From the Intranet to the DMZ and to the Internet only the necessary ports for each server are enabled, and serve the same settings for each of the interfaces of the local area firewall.
- ✓ You should only enable certain equipment for access to the Firewall.

- **Dinamic NAT**

The NAT helps translate Private Public IPv4 addresses to IPv4 is why you must configure the necessary rules for the different internal network segments pull out by the public IPv4 addresses assigned to it. An internal NATEO performed due to the existence of the DMZ since it must have a different IP network address rest.

D. Intrusion Prevention System

To install the Intrusion Prevention System or IPS software platform used under Open Source Suricata which is the evolution of Snort, these software functionality meet IDS / IPS.

Proceed to the configuration of several parameters that are in the settings file Suricata. To access the settings file type in the console:

nano etc/suricata/surucata.yaml

The values to be set in this configuration file are:

- **max-pending-packets**

This represents the number of packets that can be processed simultaneously, this depends on the capabilities of the server computer that hosted the IDS / IPS Suricata.

max-pending-packets:2000

- **action-order**

Indicates the order of the action that occurs when a match with one of the rules, set forth the actions are: pass, drop, reject and alert; and you are already set by default..

action-order:
-pass
-drop
-reect
-alert

- **outputs**

First of all you must configure the directory where the output of alert events are saved through:

default-log-dir: /var/log/suricata

Then proceed to the output configuration of alerts. To record based alerts online; which are stored in a file where each alert occupies a line of the same showing a brief description of the alert, the time at which the alert and IP addresses coming activated; should be enabled by enabled: yes, you must add a filename name: fast.log must be configured so that when you restart the IDS / IPS does not over-write the file using append: yes and given a size MB with limit: 32, as follows

-fast:
enabled:yes
filename:fast.log
append:yes
limit:32

The output alerts by barnyard2 which is done by means of the unified alerts is very important when you want to send all alerts or events detected by the IDS / IPS Suricata towards external database. It is enabled by enabled: yes, it is assigned a filename name: unified2.alert and is given a file size in MB limit: 32, as shown below::

- unified2-alert:
enabled: yes
filename: snort.unified2
limit: 32

The outputs of the HTTP events are written to the file http.log which should enable it by means of enabled: yes and verify its filename name: http.log

- http-log:
enabled: yes
filename: http.log

The output to syslog, which is the standard for sending records generated in a data network it should enable or disable as follows.

– syslog:
enabled: no
facility: local5
format: "[%i] — "
level:info

- **stats**

Displays statistics generated in the engine of IDS / IPS Suricata, they should be enabled through enabled: yes, add a name to the filename: estadísticas.log, indicate the time at which the generation of statistics cool in seconds interval: 5 to specify whether you want to overwrite the file or append: yes..

- stats:
enabled: yes
filename: estadisticas.log
interval: 5
append: yes/no

- **Scanning Engine AlertsAlertas**

The detection engine alerts creates internal groups of all security firms, and considering that there are several security firms will not be used for all network traffic is necessary to create groups of firms to optimize performance and processing scan engine. The disadvantage is that if several groups are created low performance processors, unless the server where staying has great capabilities, according to OISF whether to prosecute than 200 MB troughput and the server has great benefits, it is advisable to configure multiple groups giving a high profile in the scan engine performance alerts, such as:

detect-engine:
    -profile:high

- **CPU Affinity**

When a server with multiple processors it exists, must take advantage of multi-threading feature, which lets you assign one or more processors to different threads running Suricata. If multiple processors assigned to a thread can choose how to work the same whether "balanced" to distribute processing across all processors of the thread or "exclusive" to assign a specific processor in a row. The configuration will be as follows..

Cpu_affinity:
    -management_cpu_set:
        cpu:[5-7]
    -receive_cpu_set:
        cpu:[all]
    -decode_cpu_set:
        cpu:[0, 1]
        mode:"balanced"

- **Network definition**

For the engine of IDS / ISP Suricata start analyzing traffic should add the networks to which it is connected.

vars:
    address-groups:

HOME_NET: "[192.168.1.0/24, 10.20.0.0/16, 172.20.0.0/16]"
EXTERNAL_NET:any
HTTP_SERVERS:"$HOME_NET"
SMTP_SERVERS:"$HOME_NET"
SQL_SERVERS:"$HOME_NET"
DNS_SERVERS:"$HOME_NET"

TELNET_SERVERS:"$HOME_NET"

After completing the necessary settings in the file is necessary to bridge suricata.yaml network interfaces as Suricata analyze the traffic passing through it.

brctl addbr br0
brctl addif br0 eth1
brctl addif br0 eth0

ip li set br0 up
ip li set eth1 up
ip li set eth0 up

You must also add a rule in the IP-Tables for traffic sent to queues that the IDS / IPS engine reads Suricata.

- A FORWARD -i eth0 –j NFQUEUE

Finally to run Suricata as IPS must run the command

suricata –c /etc/suricata/suricata.yaml -q id_cola

III. SECURITY POLICIES METHODOLOGY

Today the information that passes through the data network and automation of services provided is recognized as a valuable asset to the entity is why it is necessary to have technological strategies for the control and management of data effectively.

With the introduction of this methodology Perimeter Security, where political administration and management of all network components and communications are included; the organization intends to establish good behaviors network usage data to all university staff, achieving minimize computer attacks happen and if one fix efficiently and effectively.

- **Sobre la seguridad perimetral de la red**

Requirements must be met for complete information security in the network.

- Identification.- ID is called when the user is made known to the system.

- Authentication.- is verification that the individual has been identified to the system is safe.

- Control Access.- is the proper administration of users accessing network services.

- Availability.- mean that the services offered within the network are operating at 100% of the time and in case of failure have a fast recovery time

- Confidentiality.- Explains protection insurance information users enrolled within the data network from unauthorized users.

- Integrity.- is the protection of data transmissions against unauthorized or accidental alteration that may occur within the network.

- Responsibility.-'s track and secure storage of all accidental and unauthorized activity within the network den activities.

- **Glossary of Terms**

To understand security policies necessary understanding of the following terms.

- Manager Red.- trained and specialized in managing the resources of computer network Person.

- Structured.- Cabling Cabling, duly certified braided pair, coaxial and fiber optics and labeling.

- Communication.- room is the area dedicated to unique lodging computers associated with telecommunications cabling.

- IP.- address is a numerical label consists of four integers between 0 and 255 which is unique and identifies the computer within the network.

- DMZ.- Demilitarized Zone, sector network where servers are housed.

- NWL.- Local Area Network.

- SSID.- Service Set Identifier assigned to a Wireless network name.

- Subnet.- Portion of the network, which is a new logical network.

- USER.- person who uses the network resources data, prior to authentication and registration within the system.

- WAN.- Global Area Network.

- **Organizational Committee**

This methodology for information security will be structured by engineers in Information Systems and Communication Networks, Directorate for Technological Development and Computer (DDTI) of the Technical University of the North, the structuring of this committee is raised by the Director of DDTI and is composed of:

- Director of Technology Development and Computer UTN
- Project Manager, DDTI UTN
- Head of User Support, DDTI UTN
- Networking and Communications Manager DDTI UTN

The organizational committee shall review and update once a year presenting proposals for correction by institutional office the rating committee.

- **Qualifier committee**

this methodology for information security must be approved by the highest authority, the Honorable University Council (HCU), for implementation and dissemination to the university community.

- **Scope**

these security policies are applied in each of the University dependencies, and the entire University staff, whatever their contractual status, dependence on working and the level of his tasks. In case of non-compliance with this document, the HCU who will take appropriate action depending on the severity.

- **Objetives**

The objectives to be met are:

- Manage and protect all information from the Technical University of the North, together with technological equipment used for processing.

- Keep updated and operative in accordance with the needs generated by institutional data network Perimeter Security Policy.

- Define actions for the correct assessment, analysis and evaluation of results.

- **Policies**

This paper perimeter security policies are determined, this being the result of analysis of data from network auditing and based on the services provided by the university network, this is a first step in implementing a Management of Information Security System (ISMS).

From the data Network

✓ The network will have a range of WAN IP

address subnet as follows: 190.95.196.192/27.
- ✓ The DMZ network will have a range of IP addresses subnet as follows: 10.24.8.0/24
- ✓ The LAN network is divided into two subnets, one for administration and one for student access and Laboratories.
- ✓ The administrative LAN subnet will have a range of IP addresses subnet as follows: 172.16.0.0/16
- ✓ The student LAN subnet and laboratories have a range of IP addresses subnet as follows: 172.17.0.0/16

From the communications romos

- ✓ The communications room is the main component of university data network.
- ✓ Access to communications room is restricted and only authorized by the Network Manager and Communications.
- ✓ All equipment having network services, they must be housed in the communications room.
- ✓ In each room there are faculties of communication, where teams of network access are housed.
- ✓ The communications room must have air conditioning according to the dimensions.
- ✓ The communications room must have a ventilation system according to the dimensions.

From the servers

- ✓ All services provided by the university to its administrative and student staff, are hosted on servers in the communications room.
- ✓ Each server must be administered by trained Directorate of Staff Development and Computer Technology.
- ✓ Access to server management is restricted and exclusive to who manages it.
- ✓ It should support the information once a month.

Computer security

- ✓ Be assigned a login for all users of the corporate network, as long as you are logged in integrated University system.
- ✓ Internet use for all users within the network of university data is allowed.
- ✓ Access to the university network servers all users inside and outside the university network data is allowed.
- ✓ Requests for access to ports that do not use the services provided by the university data network is blocked.
- ✓ Be monitored once a month enabled ports on each of the servers in the university network.
- ✓ In case of network attacks the source of the attack IPs are blocked.
- ✓ Access to social networks within the campus was locked.
- ✓ The use of social networks prior authorization rector of the Technical University of North will be enabled.
- ✓ The minimum length of characters allowed in a password is set to 6, which will have an alphanumeric combination case sensitive.
- ✓ The maximum length of allowable characters in a password is set to 12

Wired network

- ✓ All access points to the data network must be registered and approved by the Network Manager and Communications.
- ✓ All network equipment must use static IP corresponding to their respective VLAN.
- ✓ The IP of the connected to the wired network equipment will be recorded by the Network Administrator.
- ✓ The IP address change must be authorized and conducted by the Networking and Communications Manager or his delegate.
- ✓ Must be connected network equipment, prior authorization of Networking and Communications Manager.
- ✓ The equipment connected to the wired network belong to the workplace, not the staff performing therein.
- ✓ The user equipment connected to the wired network, is subject to monitoring, penetration testing and security audits.
- ✓ Not visit pornographic or illicit content websites.

- ✓ Any team that represents a security risk to the communications network of the university campus, may be disconnected from the network and who has registered the team will be notified.
- ✓ Should support asset information network equipment once a month.
- ✓ Any situation that can not be resolved with users regarding the network system wiring, shall be referred to DDTI located in the central building of the UTN specifically to Area Networking and Communications to make the decisions needed.

Wireless Network

- ✓ Maintaining the security of the wireless network of the university requires methods to ensure that only authorized users can access it. Thus, the computer must have the physical security necessary to prevent affected the services of the wireless network.
- ✓ All access points must be registered and approved by the administrator of the network.
- ✓ Installation, administration and use of the devices on the wireless network must be in accordance with the specifications and standards of wireless networks and the policies implemented in college.
- ✓ The SSID must be configured to be identified with the university.
- ✓ No individual should connect or install any communications equipment to the network without the prior consent of the administrator.
- ✓ Wireless communications not provide coding of the data transmitted. The protection of data is the responsibility of the user.
- ✓ No permit or encourage the use of the wireless network to use the administrative systems of the University where confidential data transmitted or received.
- ✓ The user's computer connected to the wireless network, is subject to monitoring, penetration testing and security audits.
- ✓ Any team that represents a security risk to the communications network of the university campus, may be disconnected from the network and who has registered the team will be notified.
- ✓ Any situation that can not be resolved with users regarding the wireless network system, be referred to DDTI located in the central building of the UTN specifically to Area Networking and Communications to make the decisions needed.

Telephone network

- ✓ Users with IP phones, are responsible for good use.
- ✓ There are 4 levels of priority phone: General, Support, Consulting and Executive.
- ✓ All users have priority calls in the General category.
- ✓ To enable higher than the General category permissions must be authorized by the highest university authority.
- ✓ The telephone equipment belongs to the job, not the staff working in it.
- ✓ Users should make good use of telephone service.
- ✓ Are solely responsible for the security key are made
- ✓ The security key for calls is composed of four digits followed by the pound key.

E-mail

- ✓ The email service is a free service for all administrative, faculty and students of the Technical University of North staff.
- ✓ Email is unique academic and administrative use
- ✓ Manager Email the right to monitor user accounts submit inappropriate behavior will be reserved.

Physical security

- ✓ Structured Technical University Northern wiring must be certified.
- ✓ Structured Technical University Northern wiring must be labeled.
- ✓ Each equipment room must be closed and access must be authorized by the - Administrator Network and Communication.
- ✓ Each equipment room must have an air conditioning system.

- ✓ Each equipment room must have fire alarms alert.
- ✓ Each equipment room must have fire extinguisher.
- ✓ Each equipment room must have fire protection system.
- ✓ Each room should have UPS equipment.
- ✓ Each equipment room must have redundant power circuits.
- ✓ Each cold room should have surveillance cameras.

Del personal universitario

- ✓ The user is responsible for keeping passwords secret.
- ✓ The user is responsible for the use and access to the University network.
- ✓ Do not provide personal information through email or phone.
- ✓ Excessive or abusive Internet browsing with non-work purposes is prohibited.
- ✓ Transmission of confidential information to staff who do not labor in the Universidad Tecnica del Norte is prohibited

IV. CONCLUSIONS

Computer security is essential for data networks today due to the gigantic growth of global communications so does the need to protect all the information that is generated and transmitted around the world. The perimeter security system helps network administrators to protect information flowing through the enterprise network more efficiently, thanks to the combination of different features that belong to the same as Firewall, IDS and IPS.

REFERENCES

[1] E. Taboada Gómez, *Ponencia Seguridad Perimetral en Redes*, Mundo Internet 2005

[2] C. Cruz Rincón, *Guía Ubuntu Server Español*, 2013

Author

Torres Bolaños Rodrigo Javier

Electronics and Communication Networks Engineer, has conducted studies on IPv6, VoIP, Networking, Fiber Optic, Network Security, Structured Cabling and Video Surveillance. IEEE member since 2009, Young Professional IEEE member since 2013. He currently serves as Manager of Networking and Communications in the Department of Computer Technology and Development of Universidad Tecnica del Norte.