SEGURIDAD PERIMETRAL PARA LA RED DE DATOS

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

Resumen.- La evolución de la tecnología y la constante demanda de seguridad han permitido que los sistemas de seguridad perimetral en redes evolucionen para ofrecer una mayor confiabilidad a los usuarios tanto internos como externos sobre la transparencia y protección de su información para el acceso de diferentes servicios, hoy en día existen un sin número de personas que usan sus conocimientos y ética profesional de una forma incorrecta al ingresar a redes informáticas restringidas ocasionado pérdidas multimillonarias alrededor del mundo.

Éste artículo tiene como objetivo realizar un análisis de los pasos y requerimientos necesarios para el diseño de un sistema de Seguridad Perimetral para una red de Datos.

I. INTRODUCCIÓN

La seguridad perimetral es un método de defensa de las redes informáticas, en el que consiste instalar equipos de comunicaciones en los que se establece las políticas de seguridad necesarias para su óptimo funcionamiento; estos equipos se los coloca entre la red externa y la red interna, permitiendo o denegando el acceso a los usuarios internos y externos a los diferentes servicios de la red.

La implementación de seguridad perimetral consta de tres etapas Segmentación de la Red, Firewall y un Sistema de Prevención de Intrusos IPS. Para la optimización de recursos tecnológicos es indispensable la virtualización, esto requiere un equipo con excelentes características físicas y lógicas ya que en éste será instalado el software para la virtualización de servicios.

II. SEGURIDAD PERIMETRAL

"La seguridad perimetral basa su filosofía en la protección de todo sistema informático de una empresa desde "fuera" es decir componer una coraza que proteja todos los elementos sensibles de ser atacados dentro de un sistema informático. Esto implica que cada paquete de tráfico transmitido debe ser diseccionado, analizado y aceptado o rechazado en función de su potencial riesgo de seguridad para nuestra red" [1]

Para el diseño del sistema de seguridad perimetral es indispensable realizar un análisis a la situación actual de la red logrando así saber cuál de los segmentos de red de datos necesitan más protección, es decir que segmento de red debe tener o no permisos para acceder a los servicios de red o internet.

Además se recomienda la utilización se software libre para la implementación del Firewall e IPS.

A. Segmentación de Red

El primer paso para la implementación de la seguridad perimetral es realizar una correcta segmentación de red por medio de VLANs con su respectivo direccionamiento IP. Al tener un registro de las VLANs y de las IPs utilizadas en la red, se puede aplicar las políticas a cada uno de los segmentos.

Al segmentar la red hay que tomar en cuenta el posible crecimiento de la red de datos, para poder asignar un pull de direcciones IP que cubra tanto la situación actual como el posible crecimiento.

Luego de la segmentación de red hay que configurar los equipos activos de red como son los Switchs capa 2 y los Routers, de no existir Routers es necesario la configuración de un Switch capa 3.

A continuación se muestra las configuraciones necesarias para los equipos activos de red:

- **Respaldar la configuración del Equipo**

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)

- **Configurar el nombre en cada Equipo**

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

- **Configuración de contraseñas**

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

- **Configuración del protocolo VTP**

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

- **Crear VLANs**

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

- **Configuración del enlace troncal**

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

- **Agregar puertos a las 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

- **Configuración de IP en las 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

- **Configuración de HSRP**

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

- **Habilitar funciones capa 3 en el Switch**

Switch(config)#ip routing

- **Configurar STP en los equipos**

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

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

- **Configuración del default Gateway**

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

- **Configuración del servidor DHCP**

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

- **Configuración de SSH**

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

- **Configuración de ruteo en el Switch**

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

- **Configuración de MOTD**

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

- **Encriptación de contraseñas**

Switch(config)#service password-encryption

- **Guardar las configuraciones**

Switch#copy running-config startup-config

B. Virtualización

Para la optimización de los recursos, es necesario la virtualización de servicios, para ello es necesario contar con un equipo de buenas prestaciones tecnológicas. En el mercado existen varios software destinados a la virtualización de servicios de diferentes marcas y propietarios, pero también existe software libre que es orientado a la virtualización.

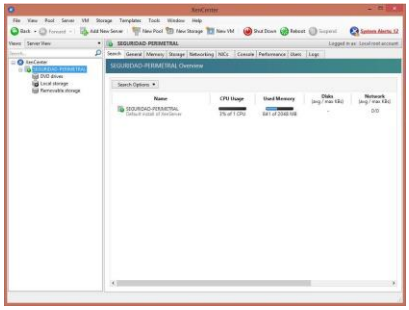
En este apartado se sugiere la utilización de XEN-Server, el cual es un software basado en open source y que está orientado a la virtualización de servicios de red. XEN-Server cumple con muchas características de los servidores de virtualización propietarios, pero puede ser accesible para cualquier usuario al ser Software Libre.

Además de XEN-Server, existe el software XEN-Center el cual es una aplicación con la que se administra todos los servidores virtualizados que se encuentren instalados y configurados en la red empresarial.

A continuación se muestran las pantallas de presentación de XEN-Server

a) Pantalla de presentación de XEN-Server

y XEN-Center.



b) Pantalla de presentación de XEN-Center

C. Firewall

La implementación del Firewall se lo realiza mediante la utilización de las IP-Tables realizando configuraciones en la consola del sistema operativo CentOS, pero existe un método gráfico en el cuál, el

usuario puede configurar los parámetros necesarios y la interfaz gráfica es la que incluye los comandos que se emplean para la configuración del Firewall en sus respectivos scripts, esto se lo realiza mediante Shorewall y Webmin.

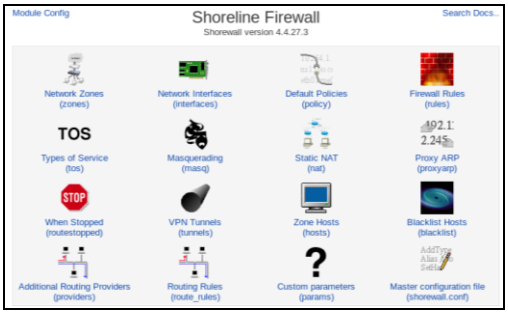
- **Shorewall**

"Una herramienta de alto nivel para configurar Netfilter. Usted describe los requisitos de firewall, Gateway usando las entradas en el conjunto de archivos de configuración. Shorewall lee los archivos de configuración y con la ayuda de iptables, iptables-restore, y las demás utilidades configura Netfilter y el subsistema de la red de Linux" [2]

- **Webmin**

Es una interfaz basada en web para la administración del sistema Linux, permitiendo al usuario una fácil interacción entre él y las funcionalidades del sistema operativo eliminando la necesidad de editar manualmente los archivos de configuración, en este caso permitirá un fácil manejo del Firewall Shorewall.

Para el funcionamiento del Firewall, se deben configurar varios ficheros en los cuales se encuentran editadas las zonas de nuestra red, las interfaces del firewall y las reglas que permitirán o denegarán el acceso a los diferentes servicios.



c) Pantalla de configuración de Shoreline Firewall

Los archivos de configuración que se deben editar para el funcionamiento del Firewall y que se los realiza mediante Shoreline Firewall son:

- **Network Zones**

Representan las redes que se conectarán al firewall, para la implementación de seguridad perimetral se establecen 4 zonas:

fw.- Representa al sistema propio del firewall a implementar.

dmz.- Representa a la DMZ donde se encuentran los servidores.

local.- Representa la intranet.

net.- Representa la salida a 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) Zonas configuradas en Shoreline

- **Network Interfaces**

Son todas las interfaces instaladas en el servidor y que se configurarán para la implementación de las reglas de seguridad, en el Firewall de la Universidad se necesita tres interfaces todas ellas Ethernet 10/100/1000 y se encuentran distribuidas de la siguiente manera.

eth0.- En esta interfaz se conecta el enlace hacia el internet.

eth1.- En esta interfaz se conecta el enlace hacia la DMZ

eth2.- En esta interfaz se conecta el enlace hacia la intranet.

Interface	Zone name
eth2	local
eth1	dmz
eth0	net

e) Interfaces de red configuradas en Shoreline

- **Default Policies**

Son políticas por defecto que se deben configurar en Firewall, debido a que se utiliza la política de todo lo que no es específicamente permitido se niega, se deben negar todas las transmisiones entre las diferentes zonas que se crean en el servidor Firewall, éstas políticas son las últimas en ser analizadas dentro de la configuración del Firewall, primero se analiza las Firewall rules y todo lo que

no se encuentre permitido en dichas reglas será denegado por estas políticas. También existe una política por defecto que indica Negar el tráfico desde cualquier origen hacia cualquier destino que se analiza al finalizar todas las Firewall Rules y las Default Policies.

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) Configuración de Default Policies en el Shoreline

- **Firewall Rules**

Mediante las Firewall Rules se crea las diferentes políticas de seguridad en donde se especifica el origen, el destino, el puerto de comunicación y se establece si se permite o no el acceso. Al momento de estar en marcha el servidor Firewall estas reglas son las primeras en ser analizadas y dado el caso que no exista una política se realizará lo que especifica las Default Policies es decir se negará todo.

Para la configuración de las Firewall Rules se tendrá en cuenta los puertos que necesita cada uno de los servicios que presta y necesita la red informática y se permitirá el acceso solo a dichos puertos.

Las reglas de seguridad empleadas se las describe a continuación en forma general.

✓ Desde la Internet hacia la DMZ y hacia la Intranet solo se habilitarán los puertos necesarios por cada uno de los servicios.

✓ Desde la DMZ hacia la Internet y la Intranet sólo se habilitarán los puertos necesarios por cada uno de los servicios.

✓ Desde la Intranet hacia la DMZ y hacia la Internet sólo se habilitarán los puertos necesarios por cada uno de los servidores, y la misma configuración servirá para cada una de las interfaces de la zona local del firewall.

✓ Se debe habilitar solamente a determinados equipos para el acceso hacia el Firewall.

- **Dinamic NAT**

El NAT ayuda a traducir las direcciones IPv4 Privadas a IPv4 Públicas es por ello que se debe configurar las reglas necesarias para que los diferentes segmentos de red interna salgan por el pull de direcciones IPv4 públicas que tiene asignado. Además se realiza un NATEO interno debido a la existencia de la DMZ y a que ésta debe tener un direccionamiento IP diferente al resto de la red.

D. Sistema de Prevención de Intrusos

Para la instalación del Sistema de Prevención de Intrusos o IPS se utiliza el software bajo plataforma de Open Source Suricata el cual es la evolución de Snort, estos software cumplen la funcionalidad de IDS/IPS.

Se debe proceder a la configuración de varios parámetros que se encuentran en el archivo de configuraciones de Suricata. Para acceder al archivo de configuraciones digite en la consola:

nano etc/suricata/surucata.yaml

Los valores que se deben configurar dentro de este archivo de configuración son los siguientes:

- **max-pending-packets**

Esto representa el número de paquetes que puede procesar al mismo tiempo, esto depende de las capacidades del equipo servidor donde se encuentra alojado el IDS/IPS Suricata.

max-pending-packets:2000

- **action-order**

Indica el orden de la acción que ocurre cuando se establece una coincidencia con una de las reglas establecidas, las acciones son: pass, drop, reject y alert; y vienen establecidas por defecto.

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

- **outputs**

Antes de todo se debe configurar el directorio en donde se guardarán la salida de los eventos de alertas mediante:

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

Luego se procede a la configuración de la salida de alertas. Para el registro de las alertas basadas en línea; las cuales se guardan en un archivo donde cada alerta ocupa una línea del mismo mostrando una descripción breve de la alerta, la hora en la que se activó la alerta y las direcciones IPs de las que proviene; se debe habilitar mediante enabled:yes, se debe agregar un nombre filename:fast.log, se debe configurar para que al momento de reiniciar el IDS/IPS no se sobre-escriba el archivo mediante append:yes y se le da un tamaño en MB con limit:32, de la siguiente manera

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

La salida de alertas mediante barnyard2 que se lo realiza por medio de las alertas unified, es muy importante para cuando se desea enviar todas las alertas o eventos detectados por el IDS/IPS Suricata hacia una base de datos externa. Se habilita mediante enabled:yes, se le asigna un nombre filename:unified2.alert y se le da un tamaño al archivo en MB limit:32, como se muestra a continuación:

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

Las salidas de los eventos HTTP se graban en el archivo http.log en el cual se debe habilitarlo por medio de enabled:yes y verificar su nombre filename:http.log.

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

La salida a syslog, el cual es el estándar para envío de los registros que se generan en una red de datos se lo debe habilitar o deshabilitar de la siguiente manera.

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

- **stats**

Muestra las estadísticas que se generan en el motor del IDS/IPS Suricata, se las debe habilitar mediante enabled:yes, agregar un nombre al archivo filename:estadísticas.log, indicar el tiempo en el cual se refreseca la generación de las estadísticas en segundos interval:5 y especificar si se desea sobreescribir el archivo o no append:yes.

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

- **Motor de Detección de Alertas**

El motor de detección de las alertas crea grupos internos de todas las firmas de seguridad, y tomando en cuenta que hay varias firmas de seguridad que no serán utilizadas para todo el tráfico de la red, es necesario crear los grupos de

firmas para optimizar el rendimiento y procesamiento del motor de detección. La desventaja es que si se crean varios grupos baja el rendimiento de los procesadores, a menos que el servidor donde se encuentre alojado tenga grandes capacidades, según la OISF si se va a procesar un troughput superior a 200 MB y el servidor posee grandes prestaciones, es recomendable configurar varios grupos dando así un perfil alto en el performance del motor de detección de alertas, como por ejemplo:

detect-engine:
-profile:high

- **Afinidad de los CPU**

Cuando se posee un servidor con varios procesadores, se debe aprovechar la característica de multi-threading, en la cual se permite asignar uno o varios procesadores a los diferentes hilos que ejecuta Suricata. Si se asigna varios procesadores para un hilo se pueden elegir el modo de trabajo de los mismos ya sean "balanced" para repartir el procesamiento entre todos los procesadores del hilo o "exclusive" para asignar un procesador específico al hilo. La configuración se lo hará de la siguiente manera.

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

- **Definición de la red**

Para que el motor del IDS/ISP Suricata comience a analizar el tráfico se debe agregar las redes a las cuales se encuentra conectado.

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"

Luego de haber realizado las configuraciones necesarias en el archivo suricata.yaml es necesario puentear las interfaces de red, ya que Suricata analizará el tráfico que pase por él.

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

También se debe agregar una regla en las IP-Tables para que se envié el tráfico a las colas que el motor IDS/IPS Suricata lee.

- A FORWARD -i eth0 –j NFQUEUE

Finalmente para ejecutar Suricata como IPS se debe ejecutar el comando

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

III. METODOLOGÍA DE POLITICAS DE SEGURIDAD

Hoy en día la información que transcurre por la red de datos así como la automatización de los servicios prestados es reconocida como un activo valioso para la entidad, es por ello que se requiere contar con estrategias tecnológicas que permitan el control y administración de los datos de manera efectiva.

Con la presentación de la presente metodología de Seguridad Perimetral, donde se incluyen las políticas de administración y gestión de todos los componentes de redes y comunicaciones; la organización pretende establecer conductas del buen uso de la red de datos a todo el personal

universitario, logrando así reducir a un mínimo los ataques informáticos y en caso de suceder uno, solucionarlo de manera eficiente y efectiva.

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

Se deben cumplir requisitos para tener una completa seguridad de la información en la red.

- ✓ Identificación.- Se denomina identificación al momento en que el usuario se da a conocer al sistema.
- ✓ Autenticación.- Es la verificación de que el individuo que se ha identificado al sistema, es seguro.
- ✓ Control de Acceso.- Es la administración correcta de los usuarios que acceden a los servicios de red.
- ✓ Disponibilidad.- Se refiere que los servicios que se ofrecen dentro de la red, estén operativos al 100% del tiempo y en caso de fallas tengan un tiempo de recuperación rápido.
- ✓ Confidencialidad.- Trata sobre la protección de la información que los usuarios seguros cursan dentro de la red de datos ante usuarios no autorizados.
- ✓ Integridad.- Es la protección de los datos y transmisiones contra las alteraciones no autorizadas o accidentales que pueden ocurrir dentro de la red.
- ✓ Responsabilidad.- Es realizar un seguimiento y almacenamiento de todas las actividades seguras, accidentales y no autorizadas que se den dentro de la red.

- **Glosario de términos**

Para la comprensión de las políticas de seguridad es necesario el entendimiento de los siguientes términos.

- ✓ Administrador de Red.- Persona capacitada y especializada en gestionar los recursos de red informática.
- ✓ Cableado Estructurado.- Tendido de cables de par trensado, coaxial y fibra óptica, debidamente certificado y etiquetado.
- ✓ Cuarto de Comunicación.- Es el área dedicada al alojamiento exclusivo de equipos informáticos asociado al cableado de telecomunicaciones.
- ✓ Dirección IP.- Es una etiqueta numérica compuesta por cuatro números enteros entre 0 y 255 el cual es único e identifica al equipo dentro de la red.
- ✓ DMZ.- Zona desmilitarizada, sector de la red donde se encuentran alojados los servidores.
- ✓ LAN.- Red de área local.
- ✓ SSID.- Service Set Identifier, nombre asignado a una red Wireless.
- ✓ Subred.- Porcion de la red, que constituye una nueva red lógica.
- ✓ Usuario.- Persona que utiliza los recursos de la red de datos, previo a su autenticación y registro dentro del sistema.
- ✓ WAN.- Red de área global.

- **Comité organizacional**

La presente metodología para la seguridad informática será estructurada por ingenieros en Sistemas Informáticos y Redes de Comunicación, de la Dirección de Desarrollo Tecnológico e Informático (DDTI) de la Universidad Técnica del Norte, la estructuración de este comité es planteada por el Director del DDTI y está compuesta por:

- ✓ Director de Desarrollo Tecnológico e Informático UTN
- ✓ Jefe de Proyectos, DDTI UTN

- ✓ Jefe de Asistencia al Usuario, DDTI UTN
- ✓ Administrador de Redes y Comunicaciones DDTI UTN

El comité organizacional deberá revisar y actualizar una vez al año presentando las propuestas de corrección mediante oficio institucional al comité calificador.

- **Comité calificador**

La presente metodología para la seguridad informática debe ser aprobada por la máxima autoridad, el Honorable Consejo Universitario (HCU), para su implementación y difusión a la comunidad universitaria.

- **Alcance**

Estas políticas de seguridad se aplicarán en cada una de las dependencias Universitarias, y a todo el personal Universitario, cualquiera que sea su situación contractual, la dependencia en la que trabaje y el nivel de tareas que realice. En caso del no cumplimiento de este documento, el HCU será quien tome las acciones pertinentes según la gravedad.

- **Objetivos**

Los objetivos que se deben cumplir son:

- ✓ Administrar y proteger toda la Información de la Universidad Técnica del Norte, conjuntamente con los equipos tecnológicos utilizados para su procesamiento.

- ✓ Mantener las Políticas de Seguridad Perimetral actualizada y operativa de acorde a las necesidades que genere la red de datos institucional.

- ✓ Definir las acciones para la correcta valoración, análisis y evaluación de los resultados.

- **Políticas**

En el presente documento se determinan las políticas de seguridad perimetral, siendo este el resultado del análisis de los datos obtenidos en la auditoría de red y en base a los servicios que brinda la red universitaria, este es un primer paso para la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI).

De la red de datos

- ✓ La red WAN tendrá un rango de direcciones IP de la siguiente subred: 190.95.196.192/27.
- ✓ La red DMZ tendrá un rango de direcciones IP de la siguiente subred: 10.24.8.0/24
- ✓ La red LAN se encuentra divida en dos subredes, una para los administrativos y otra para acceso de estudiantes y laboratorios.
- ✓ La subred LAN de administrativos tendrá un rango de direcciones IP de la siguiente subred: 172.16.0.0/16
- ✓ La subred LAN de estudiantes y laboratorios tendrá un rango de direcciones IP de la siguiente subred: 172.17.0.0/16

De los cuartos de comunicaciones

- ✓ El cuarto de comunicaciones es el principal componente de la red universitaria de datos.
- ✓ El acceso al cuarto de comunicaciones es restringido y solamente autorizado por el Administrador de Redes y Comunicaciones.
- ✓ Todos los equipos que posean servicios de red, deben encontrarse alojados en el cuarto de comunicaciones.
- ✓ En cada una de las facultades existen cuartos de comunicación, donde se alojan equipos de acceso a la red.
- ✓ El cuarto de comunicaciones deben poseer aire acondicionado de acorde a las dimensiones del mismo.
- ✓ El cuarto de comunicaciones debe poseer un sistema de ventilación acorde a las dimensiones del mismo.

De los servidores

- ✓ Todos los servicios que presta la universidad a

su personal administrativo y estudiantil, se encuentran alojados en servidores dentro del Cuarto de Comunicaciones.
- ✓ Cada servidor debe ser administrado por el personal capacitado de la Dirección de Desarrollo Tecnológico e Informático.
- ✓ El acceso a la administración de los servidores es restringido y exclusivo de quien lo administra.
- ✓ Se debe respaldar la información una vez al mes.

De la seguridad informática

- ✓ Se asignará una cuenta de acceso a todos los usuarios de la red institucional, siempre y cuando se encuentre registrado en el sistema integrado de la Universidad.
- ✓ Se permitirá el uso de internet a todos los usuarios dentro de la red de datos universitaria.
- ✓ Se permitirá el acceso a los servidores de la red universitaria a todos los usuarios dentro y fuera de la red de datos universitaria.
- ✓ Se bloquearan las peticiones de acceso a puertos que no utilicen los servicios que presta la red de datos universitaria.
- ✓ Se monitoreará una vez al mes los puertos habilitados en cada uno de los servidores de la red universitaria.
- ✓ En caso de existir ataques a la red se bloquearán las IPs de origen del ataque.
- ✓ Se bloqueará el acceso a redes sociales dentro del campus universitario.
- ✓ Se habilitará el uso de redes sociales previa autorización del señor rector de la Universidad Técnica del Norte.
- ✓ La longitud minima de caracteres permitidos en una contraseña se establece en 6, los cuales tendrán una combinación alfanumérica entre mayúsculas y minúsculas.
- ✓ La longitud máxima de caracteres permisibles en una contraseña se establece en 12.

De la red cableada

- ✓ Todos los puntos de acceso a la red de datos deben ser registrados y aprobados por el Administrador de Redes y Comunicaciones.
- ✓ Todos los equipos de red deben utilizar IP estática correspondiente a su respectiva VLAN.
- ✓ La IP de los equipos conectados a la red cableada serán registradas por el Administrador de Red.
- ✓ El cambio de dirección IP debe ser autorizada y realizada por el Administrador de Redes y Comunicaciones o su delegado.
- ✓ Se deben conectar equipos de red, previa autorización del Administrador de Redes y Comunicaciones.
- ✓ Los equipos conectados a la red cableada pertenecen al lugar de trabajo, no al personal que desempeña en dicho lugar.
- ✓ El equipo del usuario conectado a la red cableada, está sujeto a monitoreo, pruebas de penetración y auditorías de seguridad.
- ✓ No visitar sitios web pornográficos o de contenido ilícito.
- ✓ Cualquier equipo que represente un riesgo de seguridad para la red de comunicaciones del campus universitario, podrá ser desconectado de la red y la persona que tenga registrado el equipo será notificado.
- ✓ Se debe respaldar la información de los equipos activos de red una vez al mes.
- ✓ Cualquier situación que no se pueda resolver con usuarios referente al sistema de red cableado, será referida al DDTI ubicado en el Edificio Central de la UTN específicamente al Área de Redes y Comunicaciones para tomar la decisión que sea necesaria.

De la red inalámbrica

- ✓ El mantenimiento de la seguridad de la red inalámbrica de la universidad requiere métodos que aseguren que sólo los usuarios autorizados puedan tener acceso al mismo. De tal manera, el equipo debe tener las seguridades físicas necesarias para evitar que se vean afectados los servicios de la red inalámbrica.
- ✓ Todos los puntos de acceso deben de ser registrados y aprobados por el administrador de la Red.
- ✓ La instalación, administración y uso de los

dispositivos de la red inalámbrica debe estar de acuerdo con las especificaciones y normas de redes inalámbricas y con las políticas implantadas en la universidad.
- ✓ El SSID debe estar configurado para que sea identificado con la universidad.
- ✓ Ningún individuo debe conectar ni instalar cualquier equipo de comunicaciones a la red sin la previa autorización del administrador.
- ✓ Las comunicaciones inalámbricas no proveen codificación de los datos transmitidos. La protección de los datos es responsabilidad del usuario.
- ✓ No se debe permitir ni fomentar el uso de la red inalámbrica para utilizar los sistemas administrativos de la Universidad donde se transmiten o reciben datos confidenciales.
- ✓ El equipo del usuario conectado a la red inalámbrica, está sujeto a monitoreo, pruebas de penetración y auditorías de seguridad.
- ✓ Cualquier equipo que represente un riesgo de seguridad para la red de comunicaciones del campus universitario, podrá ser desconectado de la red y la persona que tenga registrado el equipo será notificado.
- ✓ Cualquier situación que no se pueda resolver con usuarios referente al sistema de red inalámbrica, será referido al DDTI ubicado en el Edificio Central de la UTN específicamente al Área de Redes y Comunicaciones para tomar la decisión que sea necesaria.

De la red telefónica

- ✓ Los usuarios que poseen teléfonos IP, son responsables del buen uso del mismo.
- ✓ Existen 4 niveles de prioridad telefónica: General, Apoyo, Asesoría y Ejecutivo.
- ✓ Todos los usuarios tienen prioridad para llamadas en la categoría General.
- ✓ Para habilitar permisos superiores a la categoría General, debe ser autorizada por la máxima autoridad universitaria.
- ✓ El equipo telefónico pertenece al puesto de trabajo, no al personal que labora en el mismo.
- ✓ Los usuarios deben hacer buen uso del servicio telefónico.
- ✓ Los usuarios se hacen responsables de la clave de seguridad
- ✓ La clave de seguridad para llamadas esta compuesta de 4 dígitos seguidos de la tecla numeral.

Del correo electrónico

- ✓ El servicio de correo electrónico es un servicio gratuito para todo el personal administrativo, docente y estudiantil de la Universidad Técnica del Norte.
- ✓ El correo electrónico es de exclusivo uso académico y administrativo
- ✓ El Administrador de Correo Electrónico se reservará el derecho de monitorear las cuentas de usuario que presenten un comportamiento inadecuado.

De la seguridad física

- ✓ El cableado estructurado de la Universidad Técnica del Norte debe estar certificado.
- ✓ El cableado estructurado de la Universidad Técnica del Norte debe estar etiquetado.
- ✓ Cada cuarto de equipos debe encontrarse cerrado y el acceso debe ser autorizado por el Administrador de redes y Comunicación.
- ✓ Cada cuarto de equipos debe poseer un sistema de aire acondicionado.
- ✓ Cada cuarto de equipos debe poseer alarmas de alerta de incendios.
- ✓ Cada cuarto de equipos debe poseer extintor contra incendios.
- ✓ Cada cuarto de equipos debe poseer sistema contra incendios.
- ✓ Cada cuarto de equipos debe poseer UPS.
- ✓ Cada cuarto de equipos debe poseer circuitos de energía eléctrica redundante.
- ✓ Cada cuarto frio debe tener cámaras de vigilancia.

Del personal universitario

- ✓ El usuario es responsable de mantener sus contraseñas en secreto.
- ✓ El usuario es responsable del uso y acceso a los

servicios de la red Universitaria.

- ✓ No proporcionar datos personales por medio de correo o teléfono.
- ✓ Se prohíbe la excesiva o abusiva navegación por Internet con fines extra laborales.
- ✓ Se prohíbe la transmisión de información confidencial a personal que no labore en la Universidad Técnica del Norte

IV. CONCLUSIONES

La seguridad informática es indispensable para las redes de datos de la actualidad, debido al crecimiento agigantado de las comunicaciones globales también crece la necesidad de cuidar toda la información que se genera y se transmite alrededor del mundo. El sistema de seguridad perimetral ayuda a los administradores de red a proteger la información que circula por la red empresarial de una manera más eficiente, gracias a la combinación de diferentes funcionalidades que pertenecen a la misma como el Firewall, IDS e IPS.

REFERENCIAS

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

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

Autor

Torres Bolaños Rodrigo Javier

Ingeniero en Electrónica y Redes de Comunicación, ha realizado estudios sobre IPv6, VoIP, Networking, Fibra Óptica, Seguridad en Redes, Cableado Estructurado y Video Vigilancia. Miembro IEEE desde el 2009, miembro IEEE Young Profesional desde el 2013. Actualmente se desempeña como Administrador de Redes y comunicaciones en la Dirección de Desarrollo Tecnológico e Informático de la Universidad Técnica del Norte.