PROPUESTA E IMPLEMENTACIÓN DE LA ARQUITECTURA DE LA RED LAN EN LA EMPRESA ACINOX LAS TUNAS

PROPOSAL AND IMPLEMENTATION OF THE LANTERN ARCHITECTURE IN THE ACINOX LAS TUNAS COMPANY

Carmen María Batista Díaz[1], Zenoyda Lujo Aliaga[1], Libely Victoria Cedeño Galindo [1], Arianna Pérez Céspedes[1], Ricardo Ernesto Pantaleón Fernández[2]
[1]Facultad de Ciencias Técnicas, Departamento de Ingeniería Informática. Universidad de Las Tunas.
[2] Empresa de Aceros Inoxidables ACINOX Las Tunas.
E-mail: [carmenbd, zlujo, lcedeno, ariannapc]@ult.edu.cu, ricardo@acinoxtunas.co.cu

(Enviado Febrero 12, 2018; Aceptado Mayo 05, 2018)

Resumen
La idea que se implementó con el título Propuesta e implementación de una red LAN constituye un medio de trabajo para el mejoramiento del acceso, distribución y procesamiento de información de todos los procesos y de la seguridad informática, que persigue como objetivo favorecer la labor de los especialistas, reduciendo el tiempo de obtener los datos de una manera rápida. Para la elaboración, diseño y puesta en práctica se hicieron encuestas y entrevistas para obtener una búsqueda amplia y variada sobre el conocimiento que poseen los especialistas relacionados con el tema. La propuesta hace un aporte para minimizar las demoras en el acceso a la información, haciendo más eficaz la velocidad de transferencia de datos, además contribuye a la preparación de los especialistas que realizan dicha responsabilidad.

Palabras clave: *Acceso a la Información, Red LAN, Seguridad Informática.*

Abstract
The idea that was implemented with the title Proposal and implementation of a LAN network is a means of working to improve the access, distribution and processing of information of all processes and computer security, which aims to promote the work of specialists, reducing the time to obtain the data in a fast way. For the elaboration, design and implementation, surveys and interviews were conducted to obtain a wide and varied search on the knowledge possessed by the specialists related to the subject. The proposal makes a contribution to minimize delays in access to information, making the speed of data transfer more efficient, and also contributes to the preparation of the specialists who carry out this responsibility.

Keywords**:** *Information Access, LAN Network, Informatics Security.*

1 INTRODUCCIÓN

En el siglo XXI la investigación constituye, sin lugar a dudas, uno de los bienes más preciados. Los desarrollos tecnológicos de la informática han impulsado el surgimiento de la globalización de la indagación, el cual ha elevado considerablemente la importancia de la encuesta para el trabajo de gobiernos, entidades, empresas, organizaciones e instituciones educacionales. Sin embargo, la averiguación en muchos casos, pierde su valor si no cuenta con ciertos factores como la privacidad, la disponibilidad y la integridad. Estos factores solo pueden obtenerse con la implantación de una adecuada política de seguridad adherida a un conjunto de herramientas y estrategias.

Las instituciones empresariales que brindan servicio directamente con la producción como la Empresa ACINOX Las Tunas, necesitan mantener funcionales varios servicios de red permanentemente capaces de monitorizar y controlar procesos remotos para su funcionamiento.

Como parte de su estructura interna ACINOX se dividen en departamentos, los cuales agrupan a los trabajadores y organizan el trabajo. Cada departamento ocupa un importante peldaño en el objetivo final de la empresa, que es producir planchas y palanquillas, así como exportar acero inoxidable.

En esta empresa existe una configuración de red que cumple con los parámetros establecidos por los organismos estatales, pero con el paso del tiempo se han quedado obsoletos.

Al hacer un estudio profundo sobre la seguridad en esta empresa, se comprobó que a pesar de la existencia de una política de seguridad y de varios estudios de la red

para su mejoramiento como la propuesta para la implementación de una red corporativa y la realización de un nuevo plan de seguridad todavía continuaban ocurriendo incidentes que demostraban el incumplimiento de estas medidas y la falta de seguridad que ello derivaba.

Durante el estudio del proceso se han podido constatar las siguientes insuficiencias:

- Problemas con un elevado flujo de datos saturando los servidores de comunicaciones en funcionamiento y poniendo en riesgo la seguridad informática de la empresa.
- Inexistencia de una adecuada configuración que permita segmentar la red LAN y regular el tráfico de información, lo cual limita el trabajo en las estaciones de servicio.

Todas estas deficiencias nos llevan a plantearnos como objetivo diseñar e implementar la red LAN en ACINOX Las Tunas para el mejoramiento del acceso, distribución y procesamiento de información de todos los procesos y de la seguridad informática.

2 DESARROLLO

2.1 Definiciones, características y topologías

Una red de computadoras (también llamada red de ordenadores o red informática) es un conjunto equipos (computadoras y dispositivos), conectados por medio de cables, señales, ondas o cualquier otro método de transporte de datos, para compartir información (archivos), recursos (discos, impresoras, programas, etc.) y servicios (acceso a una base de datos, internet, correo electrónico, chat, juegos, etc.). A cada una de las computadoras conectadas a la red se le denomina un nodo [1].

Las redes se pueden clasificar de la siguiente forma:

- **Por alcance**
  Red de área personal (*Personal Area Network*, PAN)
  Red inalámbrica de área personal (*Wireless Personal Area Network*, WPAN)
  Red de área local (*Local Area Network*, LAN)
  Red de área amplia (*Wide Area Network*, WAN)
  Red de área local inalámbrica (*Wireless Local Area Network*, WLAN)
  Red de área local virtual (*Virtual LAN*, VLAN)
- **Por relación funcional**
  Cliente-servidor
  Peer-to-peer
- **Por tecnología**
  Red punto a punto (*point to point*, PtP)
  Red de Difusión (*broadcast*)
  Red multipunto
- **Por servicio o función**
  Red comercial
  Red educativa
  Red para el proceso de datos

La topología de una red es el arreglo físico o lógico en el cual los dispositivos o nodos de una red (e.g. computadoras, impresoras, servidores, *hubs*, *switches*, enrutadores, etc.) se interconectan entre sí sobre un medio de comunicación [1].

Teniendo en cuenta el desarrollo de la investigación se utilizó como tipo de red la Red de Área Local (LAN). Cuyas principales características son [2]:

- La distancia máxima entre los equipos a conectar está en el rango de las centenas de metros.
- La capacidad de transmisión es muy grande, generalmente mucho mayor que la de las redes de área extensa, siendo las velocidades habituales entre 10 y 100 Mbits/s, alcanzando las más rápidas hasta 1 Gbits/s.
- Los componentes que las forman (equipos *hardware* y *software)* son de propiedad particular así como los edificios y locales donde están ubicados dichos componentes, todo lo contrario ocurre con muchas de las redes de área extensa.
- Los errores introducidos en la transmisión de datos son menores que en las redes de área extensa.

Las redes de área local facilitan la comunicación de un gran número de equipos y aplicaciones a las organizaciones en un entorno reducido, mientras que las redes de área extensa interconectan a estas LAN permitiendo el intercambio de información entre sitios que están distantes geográficamente [2].

2.2 Características que debe cumplir una red LAN en empresas

La seguridad informática para las empresas Nacionales e Internacionales es un paso muy importante ya que esta se encarga de la protección de la infraestructura computacional y todo lo relacionado con esta y, especialmente, de la información contenida o circulante.

Para ello existen una serie de estándares, protocolos, métodos, reglas, herramientas y leyes concebidas para minimizar los posibles riesgos a la infraestructura o a la información.

En nuestro país el Esquema Nacional de Seguridad establece medidas tecnológicas para permitir que los sistemas informáticos en las empresas cumplan con unos requerimientos de seguridad acordes al tipo y disponibilidad de los servicios que se prestan.

Atendiendo a las medidas y esquemas de seguridad establecidos para las empresas estatales en Cuba y cumpliendo con las normas internacionales de redes más actuales, se pretende dividir la red en 3 segmentos, uno llamado Externo, aquí están los equipos directos a Internet, como el *router* del proveedor ETECSA, otro

denominado Zona Desmilitarizada (DMZ), donde estarían ubicados los servidores que brindan servicio a la red local e interactúan con el segmento Externo, y por último, el segmento denominado Red Interna (LAN) donde están los servidores que dan servicios exclusivos para la LAN así como las estaciones de los usuarios, ver Fig. 1.

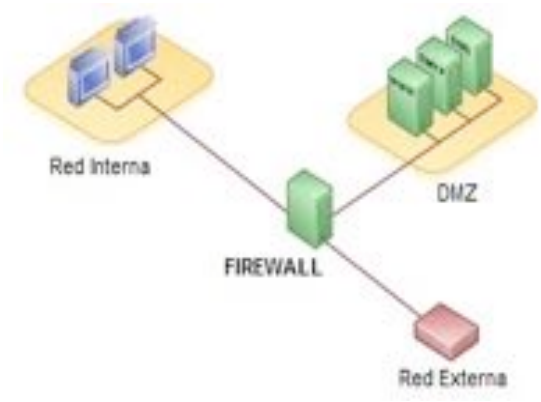

Figura 1 Diagrama de una red que utiliza una DMZ [4].

La zona DMZ se usa habitualmente para ubicar servidores que es necesario que sean accedidos desde fuera, como servidores de correo electrónico, web y DNS (*Domain Name System* - Sistema de Nombres de Dominio). Y es precisamente estos servicios alojados en estos servidores los únicos que pueden establecer tráfico de datos entre la DMZ y la red interna, por ejemplo, una conexión de datos entre el servidor *web* y una base de datos protegida situada en la red interna [3].

2.3 Situación actual en la Empresa ACINOX Las Tunas

La estructura de red en la Empresa ACINOX Las Tunas a lo largo de los años ha aumentado considerablemente, hasta el límite que hoy en la misma intervienen cuatro servidores y alrededor de 200 estaciones de trabajo, sin embargo el enlace con el proveedor que es ETECSA cuenta con un único nivel de seguridad que es un servidor firewall con dos interfaz de red, pero realmente con las características y el desarrollo de las redes actuales no se cumplen con las expectativas de seguridad que se requieren.

La red LAN de esta empresa posee más de 100 estaciones con acceso pleno a internet y más de 200 cuentas de correo electrónico con salida Internacional, estos servicios se brindan a través de un solo servidor de comunicaciones, con limitaciones serias en la calidad del servicio que reciben los usuarios.

Demasiado tráfico en la red para un solo servidor que presta varios servicios, limitándose el flujo de trabajo para las distintas áreas. Solucionar esto requiere pasar a niveles superiores en cuanto a la segmentación de la red, más ahora que se introdujeron nuevos ordenadores vinculados al control directo del proceso de producción, por tanto; es imprescindible pasar a otro nivel de seguridad en una red de este tipo que por un lado tiene estaciones con acceso pleno a Internet y por otro lado estaciones conectadas directamente al proceso tecnológico.

Trabajar con la referida configuración de un único firewall conlleva un elevado nivel de riesgo ante la proliferación de virus y ataques que pueden venir desde Internet hacia la red local, de ahí, la recomendación de lograr cambiar el nivel de seguridad que hoy está establecido. Para ello se prevé una nueva segmentación de la red (Fig. 2 y Fig. 3), así como la instalación y configuración de un nuevo servidor *Firewall*, el cual solo cumpla esa función dentro de la estructura de red, pasando el resto de los servicios a otros servidores.

La implementación de los servicios que se requieren se prevé hacerlo utilizando servidores profesionales adquiridos recientemente, utilizando preferentemente entornos de virtualización, para garantizar un mecanismo eficiente de salvas de seguridad y la rápida puesta en marcha ante contingencias, lográndose en la empresa un ambiente de trabajo más eficiente y seguro en el uso de las Tecnologías de la Información y las Comunicaciones (TIC), y por sobre todas las cosas, pasando a un nivel de seguridad informática que cumpla con las exigencias actuales.

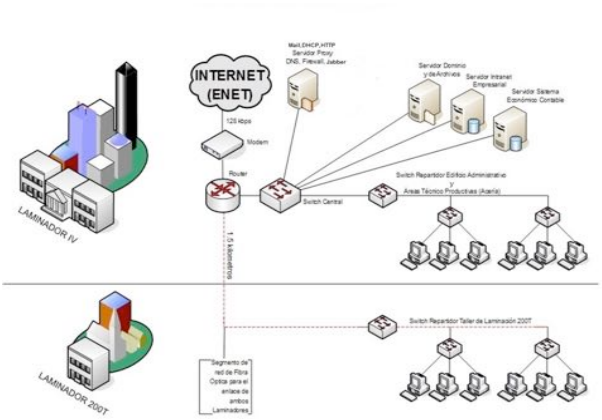

Figura 2 Diagrama de la configuración de red anterior

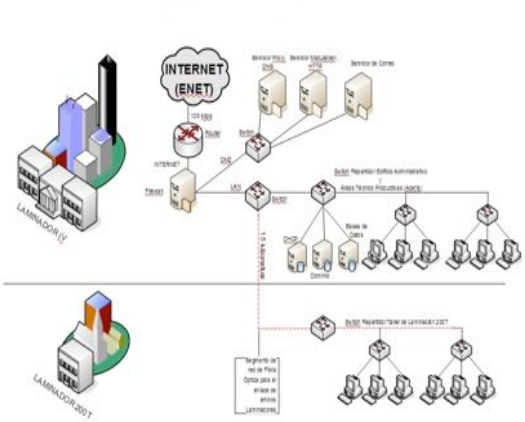

Figura 3 Diagrama de configuración de red actual.

Entre las principales ventajas y desventajas podemos encontrar las siguientes:

Desventajas:

- La configuración del servidor Firewall solo establece y regula el tráfico entre dos zonas (Internet y LAN) con una única interfaz de red utilizando enmascaramiento IP, lo cual está obsoleto y expone a la red LAN a inadecuadas condiciones de seguridad.
- En el servidor Firewall coexisten otros servicios, como el DNS, Mail, DHCP, HTTP, *Jabber* y el *Proxy* lo cual limita el trabajo de las estaciones en caso de problemas en el mismo.
- La política de salvas de seguridad en los servidores no garantiza la reactivación de los servicios en un tiempo breve.

Ventajas:

- La empresa cuenta con un servidor Firewall que establece y controla el tráfico entre zonas (Internet, DMZ y LAN), utilizando para ello tres interfaces de red a tono con las configuraciones de seguridad actuales y garantizando mayor seguridad ante posibles amenazas.
- Se utiliza un equipo exclusivamente como servidor Firewall, sin que estén implementados en este otros servicios, resultando más fácil reponerse ante problemas que puedan surgir.
- La utilización de la plataforma de virtualización PROXMOX no solo optimiza el uso de recursos, sino que además facilita la utilización de una política de Salvas de Seguridad (salvas periódicas y automáticas de las máquinas virtuales) que permite reponerse rápidamente y con el mínimo costo de operaciones en caso de contingencias.

2.2 Implementación de los mecanismos de seguridad

Para la implementación de la red se utilizaron como herramientas de seguridad la LAN, las cuales se distinguen por poseer pequeñas dimensiones que no superan los 10 Km.

Se caracterizan principalmente en cuanto al medio de transmisión utilizado y por sus topologías. El medio de transmisión es por donde circula la información. Se utilizaron par de cables trenzados, cable coaxial y fibra óptica.

Otras de las herramientas que se tuvo en cuenta fueron los topologías de las redes, la cual de define como la distribución de cada estación en relación a la red y a las demás estaciones, determina dónde pueden colocarse las estaciones de trabajo, la facilidad con que se extenderá el cable y el corte de todo el sistema de cableado. Las que se utilizaron fueron bus, anillo, estrella, árbol y trama. Todas estas herramientas fueron de mucha utilidad para la implementación de la red.

Como mecanismo o estrategia de seguridad se utilizó un *firewall* o cortafuego el cual es utilizado para separar, en cuanto a seguridad se refiere, una computadora o subred del resto, protegiéndola así de servicios y protocolos que desde el exterior puedan suponer una amenaza a la seguridad.

Los tipos de cortafuegos que se utilizaron: encaminador que filtra paquetes, pasarela con dos tarjetas de red, cliente, encaminado, (pc, *router*), subred protegida (DMZ).

Considerando la problemática expuesta en ACINOX Las Tunas y según el resultado de los estudios y la búsqueda de información más actual asociada a la seguridad informática de la empresa, se considera que lo más adecuado es pasar a trabajar en un esquema donde se segmente la red, participando en dicha segmentación un servidor *Firewall* que encamine los paquetes entre las diferentes subredes, para esto se utilizó *Endian Firewall.* Se utilizó un servidor *Firewall* con distribución basada en GNU/LINUX. La principal ventaja es que es una solución totalmente *Open Source* patrocinada por *Endian* es un *software* libre (también tiene versión de pago que incluye soporte y *hardware),* especializada en *Firewal*l, ruteo y gestión unificada de amenazas (Fig. 4). También puede utilizarse para otros servicios tales como: *Proxy*, antivirus, servidor VPN, servidor DHCP [4].

Figura 4 ENDIAN Firewall [5].

Para aplicar estas estrategias se utilizaron como mecanismo de seguridad *Promox* Virtual la cual es una plataforma de virtualización, basada en sistemas de código abierto, disponible bajo licencia GPLv2, para la implementación de máquina virtuales utilizando los entornos *OpenVZ* y KVM. *OpenVZ*, es una tecnología de virtualización, basada en el núcleo de Linux, que permite, a un servidor físico, ejecutar múltiples instancias de sistemas operativos aislados.

El entorno ofrece al administrador una interfaz *web* de gestión, lo cual es cómodo y no requiere instalar nada. Incluye conexión remota a la consola de cada una de las máquinas virtuales alojadas, además de permitir la

creación, arranque y parada de las distintas máquinas virtuales.

2.3 Virtualización con PROXMOX

PROXMOX Virtual Environmentes Proxmox es un **Hypervisor de tipo 1** también conocido como nativo, *unhosted o bare metal* (sobre metal desnudo) por lo que el software de proxmox se ejecuta directamente sobre el *hardware* del equipo físico. Proxmox es una solución completa de virtualización de servidores que implementa dos tecnologías de virtualización: KVM (*Kernel-based Virtual Machine)* y OpenVZ. En la Fig. 5 podemos observar su entorno *Web*.

OpenVZ,: Virtualización basada en contenedores para LINUX. Proxmox nos permite ejecutar múltiples *instancias* de sistemas operativos aislados sobre un único servidor físico, consiguiendo con esto mejoras en el rendimiento, escalabilidad, densidad, administración de recursos dinámico [6].

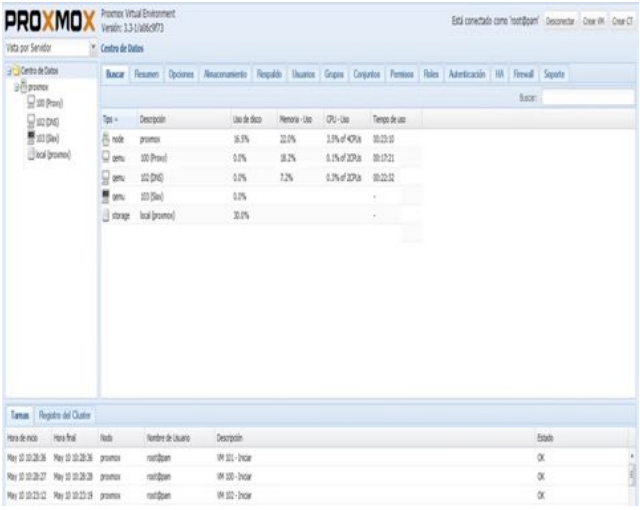

Figura 5 Entorno *Web* de PROMOX con máquinas virtuales.

De esta manera podemos apreciar en la Fig. 6 la implementación de *Endian Firewall*, donde se definieron las interfaces de redes WAN, LAN y DMZ, mostrando el gráfico de procesos que brinda toda la información del tráfico, tanto de entrada como de salida de todos los servicios implementados.

Figura 6 Implementación de ENDIAN *Firewall*.

En la Fig. 7 se puede apreciar el uso extensivo del referido servidor al medir el tráfico en la interfaz de red. Las Figs. 8, 9 y 10 muestran el tráfico de datos en el servidor PROXMOX (servicio DNS y *proxy*), el servidor de correo (*mail)* y en el servidor *Firewall* (interfaz de red de la zona DMZ).

2.4 Validación de la efectividad del sistema

Se aplicó en todas las provincias con el objetivo de validar su efectividad. A través de la interacción con la herramienta permitió establecer un cronograma automático de salvas de seguridad, lo cual permitió en breve tiempo recuperarse ante una determinada contingencia.

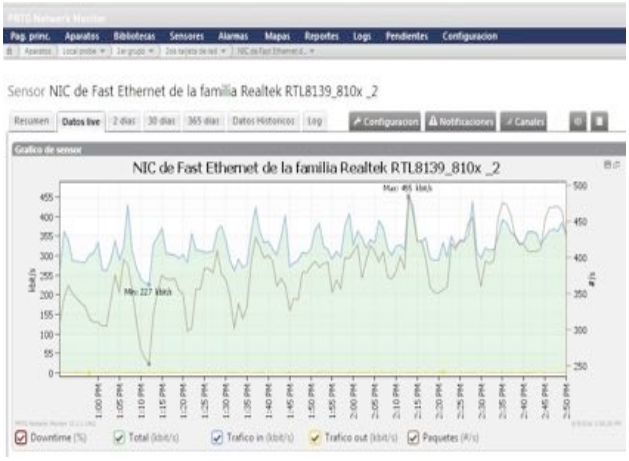

Figura 7 Tráfico del servidor.

Fue admitido por el personal de la institución, especialistas del Departamento de Informática con plena conciencia de su importancia para mantener funcionales varios servicios de red permanentemente capaces de monitorizar y controlar procesos remotos para su funcionamiento así como en el cumplimiento de los parámetros de seguridad informática.

Se motivó a trabajadores de la institución a la utilización de medios informáticos en la aplicación de la herramienta. Se ha generalizado a nivel provincial en los diferentes municipios de nuestra provincia.

Esta investigación forma parte del proyecto Aplicación de Sistemas Informáticos para la gestión de procesos de la Universidad de Las Tunas.

Figura 8 Tráfico de datos servidor PROXMOX.

Figura 9 Tráfico de datos servidor Mail.

Figura 10 Tráfico de datos servidor Firewall.

3 CONCLUSIONES

Posibilitó que la empresa contara con un servidor *Firewall* que estableciera y controlara el tráfico entre zonas (internet, DMZ y LAN), utilizando para ello tres interfaces de red a tono con las configuraciones de seguridad actuales y garantizando mayor seguridad ante posibles amenazas.

Se utilizó un equipo exclusivamente como servidor *Firewall*, sin que estuvieran implementados en este otros servicios, resultando más fácil reponerse ante problemas que pudieran surgir.

La utilización de la plataforma de virtualización PROXMOX facilitó el uso de una política de salvas de seguridad (salvas periódicas y automáticas de las máquinas virtuales), que permitió reponerse rápidamente y con el mínimo costo de operaciones en caso de contingencias.

4 REFERENCIAS

[1] Cáceres Alvarado, L. (2011). Redes de Computadoras. Manual. UNASAM. Recuperado de: https://electronicahz.webcindario.com/pdf/manual_redes_v2.7.pdf.

[2] Pascual Viñé, J. C. (2000). Introducción a la telemática y a las redes de datos. Telefónica de España, pp. 109-110.

[3] Digital Guide. (2016). Zona desmilitarizada. Recuperado de: https://www.1and1.es/digitalguide/servidores/seguridad/en-que-consiste-una-zona-desmilitarizada-dmz/.

[4] Quasar Software (2012). Endian Firewall community (2012). Recuperado de: http://www.quasarbi.com/endian.html.

[5] GreenRoot. (2012). Endian Firewall Configuración y Administración. Recuperado de: http://donjuanblogo.blogspot.com/2012/05/endian-firewall-configuracion-y.html.

[6] Ochoa, S. (2015). Proxmox: Instalación y Puesta a Punto. Recuperado de : https://administradoresit.wordpress.com/instalacion-proxmox/.

