009. SISTEMA DE SEGURIDAD PERIMETRAL EN UN ENTORNO UNIVERSITARIO

Autores:

Ing. Manuel Ramírez Pírez
Universidad Tecnológica Ecotec.
Docente tiempo completo.
Master en TICs
mramirez@ecotec.edu.ec

Ing. José Gómez Lorentty
Universidad Tecnológica Ecotec.
Administrador de Redes.
Master en TICs
jgomez@ecotec.edu.ec

Resumen

Los ataques a la red y pérdidas de información provocan un alto costo en el desempeño exitoso de una empresa o institución, por ello la implementación de una infraestructura que garantice el control de accesos y protección de los datos es necesaria para lograr la integridad, confidencialidad y seguridad de la información. El presente trabajo de investigación aborda diferentes aspectos relacionados al diseño de seguridad perimetral lógica escalable en un entorno universitario. Mediante un enfoque cualitativo inductivo se recolectaron los datos y experiencias referentes a trabajos similares realizados en universidades y empresas de la región, aspectos que permitieron estudiar y conocer la teoría relacionada al objeto de estudio. El diseño integra cortafuegos de última generación, IDS, IPS y DMZ, para alcanzar una seguridad de alto nivel con redundancia de datos, mejorando la infraestructura tecnológica de la universidad, con un modelo de red robusto y seguro.

Palabras claves: Seguridad perimetral, IDS, DMZ, cortafuegos, seguridad informática

Abstract

Attacks on the network and loss of information cause a high cost in the successful performance of a company or institution, so the implementation of an infrastructure that guarantees access control and data protection is necessary to achieve integrity, confidentiality and security of the information. This research work addresses different aspects related to the design of scalable logical perimeter security in a university environment. Through an inductive qualitative approach, data and experiences related to similar work carried out in universities and companies in the region were collected, aspects that allowed studying and knowing the theory related to the object of study. The design integrates state-of-the-art firewalls, IDS, IPS and DMZ, to achieve high-level security with data redundancy, improving the university's technological infrastructure, with a robust and secure network model.

Keywords: Perimeter security, IDS, DMZ, firewall, computer security

INTRODUCCIÓN

La seguridad de la información ha sido un tema de vital importancia para el sector empresarial y como ente de ella la seguridad perimetral. En los últimos años este concepto ha sufrido algunos cambios y ello ha estado condicionado según (Bohórquez Gutiérrez, 2017)) al incremento de las brechas en las redes, los sistemas operativos, los equipos de uso cotidiano, la evolución de la tecnología, el uso de mecanismos de comunicaciones móviles y el almacenamiento de información en la nube, siendo necesario integral a este concepto los acceso lógicos y físicos.

Esta revolución tecnológica implica problemas de vulnerabilidad que atentan contra la disponibilidad, integridad y seguridad de la información, a esta realidad se une el hecho de que muchas empresas crecen en infraestructura (civil, edificios), personal, inversiones, productos, servicios para sus clientes, pero no invierten en mejorar su seguridad ya sea por desconocimiento, costos o falta de personal con preparación en el área de TI.

Una de las acciones que ayudan a mitigar estos problemas, es establecer una seguridad perimetral lógica afín de poner una barrera o frontera que sea imposible de penetrar entre una red interna y el Internet, para restringir y tener un control sobre los datos que entran y salen de la organización (Díaz C. M., 2013), siendo la principal ventaja permitir al administrador concentrarse en los puntos de entrada, sin olvidar la seguridad del resto de servidores internos de la red, para protegerlos frente a una posible intrusión.

Un estudio reciente publicado por Gemalto, líder mundial en seguridad perimetral plantea que la inmensa mayoría de los profesionales de TI continúan creyendo que la seguridad perimetral es eficaz para mantener a los usuarios no autorizados fuera de sus redes. Sin embargo, las empresas no invierten lo suficiente en tecnología que proteja adecuadamente (Gemalto security, 2017).

Es evidente que para garantizar la seguridad de una forma eficiente es necesario primeramente contar con el apoyo de los directivos, pues son ellos quienes pueden apostar por un cambio con una inversión de infraestructura tecnológica que permita la protección de sus datos.

En este contexto se desarrolla la presente investigación para un entorno universitario que tiene como objetivo diseñar un sistema de seguridad perimetral lógica que garantice un uso correcto de los servicios informáticos, para lograr una red robusta con redundancia de datos a nivel de router y con alta seguridad.

El artículo se organiza de la siguiente forma:
En la primera parte se hace un análisis teórico de los dispositivos y el rol de los mismos en el diseño de un sistema de seguridad perimetral lógica, a fin de tener una idea sobre cual se ajuste a las necesidades de la universidad. Posteriormente se hace una descripción de la infraestructura lógica de la empresa.
En otro apartado se describen los materiales y métodos que sustentan la investigación y finalmente se hace el análisis y discusión de los resultados que en función del diseño que se propone.

Bases teóricas

En este apartado se hace una descripción en base a los elementos que deben tenerse en cuenta para la implementación de un sistema de seguridad perimetral lógica.
Un sistema de seguridad perimetral siempre ha tenido relación directa con los recursos de las redes de computadoras, debido a que desde el comienzo se buscó la unión de los sistemas informáticos para obtener más rendimiento y capacidades.

La seguridad lógica hace referencia a la aplicación de mecanismos y barreras para mantener el reguardo y la integridad de la información dentro de un sistema informático, la seguridad es una herramienta valiosa para cualquier negocio, lo cual conlleva a cuestionarse sobre la manera en que se puede formalizar la intención que tiene la misma en las organizaciones. En el contexto actual cuando se habla de seguridad sobre las TI se definen o establecen desde diversas áreas, tales como la seguridad informática, la seguridad de la información y la Ciberseguridad (Flake, 2017).

Alejandro Ramos Fraile de la UPM (Universidad Politécnica de Madrid) define la seguridad perimetral como: “Arquitectura y elementos de red que proveen de seguridad al perímetro de una red interna frente a otra que generalmente es Internet”

Por otra parte, la empresa mexicana Multicomp, especialistas en equipos de seguridad informática, define la seguridad perimetral como un concepto emergente que asume la integración de elementos y sistemas, electrónicos y mecánicos, para la protección de perímetros físicos, detección de tentativas de intrusión y/o disuasión de intrusos en instalaciones especialmente sensible”

Resulta claro que hablar de seguridad informática incluye la seguridad física y lógica. En el caso de la seguridad perimetral lógica es aquella que integra deferentes componentes de hardware que configurados correctamente permiten la protección de los datos.

Se pueden establecer diferentes categorías de productos que proporcionan seguridad perimetral (Inteco, 2015), Entre los que se destacan CORTAFUEGOS, VPN e IPS/IDS, estos permiten establecer un perímetro de seguridad y garantizar las comunicaciones seguras para evitar accesos no autorizados y ataques procedentes de redes externas y de Internet.

Los cortafuegos actúan como una herramienta de defensa perimetral que monitoriza el tráfico, lo permite o lo bloquea. En los últimos años, su funcionalidad ha aumentado, y ahora la mayoría de los cortafuegos no solo pueden bloquear un conjunto de amenazas conocidas y hacer cumplir las políticas de listas de control de acceso avanzado, sino que también pueden inspeccionar profundamente paquetes individuales de tráfico y probar paquetes para determinar si son seguros (ComputerWord, 2017)

Los cortafuegos manejan la conectividad por zonas (seguras o no) o bien por niveles de seguridad, los que establece el usuario, según el grado de permisividad que le imponga al equipo. Los cortafuegos sólo deben configurarse según las necesidades o gustos del usuario, cosa que no termina con la instalación. (Rabanales, 2012).

Es evidente entonces que el cortafuego es la primera línea de defensa en una red al permitir el filtrado de los datos, su implementación puede asumir diferentes roles en cuanto al diseño que se decida. Para el filtrado de datos desde el nivel de enlace de datos hasta el nivel de aplicación intervienen diferentes cortafuegos entre los que se destacan:

Cortafuegos de próxima generación (NGFW)
Un Cortafuegos de nueva generación o Next Generation Cortafuegos (NGFW) es un dispositivo de red que integra múltiples funcionalidades de seguridad en una única plataforma, de modo que se simplifican la administración de políticas, se eliminan puntos de fallo, latencias y cuellos de botella incensarios, incrementando la seguridad (Secure it, 2018). Estos cortafuegos integran muchas opciones avanzadas, como son:

- Estar al tanto de cuáles son los activos que corren mayor riesgo con reconocimiento del contexto completo
- Reaccionar rápidamente ante los ataques con automatización de seguridad inteligente que establece políticas y fortalece las defensas en forma dinámica
- Detectar mejor la actividad sospechosa o evasiva con correlación de eventos de terminales y la red
- Reducir significativamente el tiempo necesario desde la detección hasta la eliminación de la amenaza con seguridad retrospectiva que monitorea continuamente la presencia de actividad y comportamiento sospechosos, Incluso después de la inspección inicial
- Facilitar la administración y reducir la complejidad con políticas unificadas que brindan protección en toda la secuencia del ataque.

Este tipo de cortafuegos según cisco proporciona de forma exclusiva protección avanzada contra amenazas antes, durante y después de los ataques.

Cortafuegos Proxy
Es uno de los primeros tipos de dispositivos de cortafuegos, tiene funciones de gateway de una red a otra para una aplicación específica. Los servidores proxy pueden brindar una funcionalidad extra, como seguridad y almacenamiento de contenido en caché, evitando las conexiones directas desde el exterior de la red y mejorando la velocidad de acceso, transparencia para la aplicación de técnicas NAT y proxy inverso instalado en servidores web para controlar el acceso, balancear la carga o aumentar el rendimiento.

Cortafuegos de inspección activa
En la actualidad, a estos tipos de Cortafuegos se los considera un Cortafuegos “tradicional”, permite o bloquea el tráfico en función del estado, el puerto y el protocolo. Este Cortafuegos monitorea toda la actividad, desde la apertura de una conexión hasta su cierre. Las decisiones de filtrado se toman de acuerdo con las reglas definidas por el administrador y con el contexto, lo que refiere a usar información de conexiones anteriores y paquetes que pertenecen a la misma conexión.

Cortafuegos de administración unificada de amenazas (UTM)
*Unified Threat Management, o simplemen*te un dispositivo UTM, combina de manera flexible las funciones de un Cortafuegos de inspección activa con prevención de intrusiones y antivirus. También, a menudo incluye, administración de la nube. Los UTM se centran en la simplicidad y la facilidad de uso. Esto se explica porque al tener

un solo equipo que cumpla varias funciones, la administración y el manejo se consolidan.

Otro elemento a considerar en el diseño de un sistema de seguridad perimetral lógica, son los Sistemas De Detección De Intrusos (IDS). Las sondas IDS son dispositivos que se posicionan offline del flujo de las redes, de manera que reciben una copia del tráfico de cada VLAN (mediante la utilización de TAPs físicos o con la creación de un port mirroring o port span de una VLAN de un switch capaz de hacerlo), siendo ésta una gran ventaja ya que no retardan el flujo del tráfico de producción. Por un interfaz sin pila TCP/IP reciben el tráfico en formato RAW y lo analizan enfrentándolo contra una base de datos de firmas de ataques conocidos, de manera que, a través de otro interfaz, cuando detectan tráfico malicioso, envían señales de alarmas a una base de datos centralizada. La desventaja es que no pueden detener ataques de un único paquete y necesitan de otros dispositivos de red (Router, firewall) para detener un ataque. (Díaz C. M., 2013)

Sistemas De Prevención De Intrusos (IPS).

Los sistemas de prevención de intrusos son el tercer eslabón que se necesita para armar un diseño de seguridad perimetral. IPS extendió las soluciones IDS al agregar la capacidad de bloquear amenazas además de detectarlas y se convirtió en la opción de implementación dominante para las tecnologías IDS / IPS.

Un Sistema de Prevención de Intrusiones (IPS), según Palo Alto Networks, es una tecnología de seguridad de red y prevención de amenazas que examina los flujos de tráfico de red para detectar y prevenir exploits de vulnerabilidad. Los exploits de vulnerabilidades a menudo vienen en forma de entradas maliciosas a una aplicación o servicio de destino que los atacantes usan para interrumpir y obtener el control de una aplicación o máquina. Después de una explotación exitosa, el atacante puede deshabilitar la aplicación de destino, o puede acceder a todos los derechos y permisos disponibles para la aplicación comprometida

El IPS a menudo se ubica directamente detrás del Cortafuegos y proporciona una capa complementaria de análisis que selecciona negativamente el contenido peligroso. A diferencia de su predecesor, el Sistema de Detección de Intrusos (IDS), que es un sistema pasivo que escanea el tráfico e informa sobre amenazas, el IPS se coloca en la ruta de comunicación directa entre el origen y el destino, analizando activamente y tomando acciones automáticas en todos flujos de tráfico que ingresan a la red. Específicamente, estas acciones incluyen:

- Enviar una alarma al administrador
- Dejar caer los paquetes maliciosos
- Bloquear el tráfico desde la dirección de origen
- Restableciendo la conexión

Como componente de seguridad en línea, el IPS debe funcionar de manera eficiente para evitar la degradación del rendimiento de la red. También debe funcionar rápido porque las exploraciones pueden ocurrir casi en tiempo real. El IPS también debe detectar y responder con precisión, a fin de eliminar las amenazas y los falsos positivos, es decir, los paquetes legítimos se interpretan mal como amenazas.

Los nuevos equipos IPS se los conoce con la abreviación de NGIPS (Next Generation Intrusion Prevention System) por sus siglas en inglés.

Los sistemas de prevención de intrusos de próxima generación (NGIPS por sus siglas en inglés), cumplen todas las funciones de un IPS tradicional, pero adicional a estos los NGIPS deben:

- Proporcionar una amplia cobertura de protocolos de red: Esto con la finalidad de identificar un ataque de amplio alcance
- Tener conciencia contextual: En otras palabras, información sobre el ambiente de la red que ayudará a evaluar eventos de intrusión y decisiones de bloqueo
- Proporcionar conciencia del contenido: Al hacer capaz de identificar archivos, y los tipos de archivos (extensiones .doc, .pdf, .jpg, entre otras)

Concluyendo, un (NGIPS) debe ser capaz de mantener un constante rastreo de las aplicaciones y de los usuarios, esto con el fin de facilitar y hacer más agiles las investigaciones para identificar a los atacantes. Un NGIPS deberá tener una serie de métodos avanzados para poder detectar oportunamente las amenazas avanzadas. Habilitando reactivamente la identificación de cargas que se reciben en la red y decidir si lo envía a algún dispositivo integrado de seguridad (integración con Sandboxing Analysis) o si lo administra con servicios en la nube.

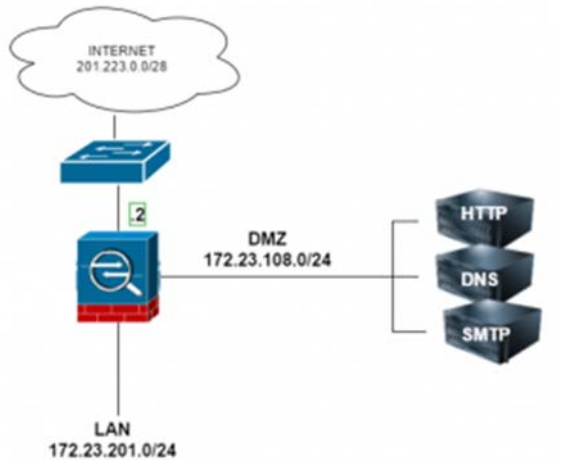
Zona desmilitarizada (DMZ)

Una zona desmilitarizada (DMZ). es una subred separada por los cortafuegos que presta servicios generales, internos y externos. La DMZ no puede acceder a la red interna, protegiéndola de ataques del exterior. Se sitúan en ella servidores accesibles desde Internet (web, correo, DNS, etcétera).

La configuración de una DMZ se debe realizar con mucho cuidado pues como plantea (Colomés, 2015) el problema está cuando la compañía tiene servidores locales que deben ser accesibles desde Internet y el administrador de redes o encargado de la infraestructura se comienza a preguntar cómo y donde los instalará. En tal sentido, Colome analiza tres casos:

1. Servidores instalados fuera de la red
2. Servidores instalados en la LAN
3. Servidores en la DMZ

El tercer caso y coincidiendo con el autor brinda una mayor seguridad al permitir una interfaz nueva y una subred independiente, pero siempre interna, que controla mejor el acceso a los servidores.



En la figura se aprecia que la DMZ es una subred independiente, separada de la LAN y de Internet, con ello se puede configurar el firewall para crear reglas específicas de seguridad y NAT que permitan el tráfico proveniente de Internet solamente hacia esa zona. El NAT estático estaría asociado entre las IP públicas y las IP asignadas a cada servidor en la DMZ. Así, si un hacker vulnera la seguridad de uno de los servidores, este no tendría acceso a la red LAN corporativa.

Materiales y métodos

Para llegar al diseño que se propone se siguen una serie de pasos que permiten conformar una idea del trabajo a realizar se siguen los siguientes pasos

1. Se hace un estudio de los trabajos relacionados al objeto de estudio a fin de conocer sus principales aportes en la investigación que se presenta
2. Descripción del diseño que existía antes de la aplicación del nuevo diseño, detallando los dispositivos que intervienen en la configuración y la funcionalidad de los dispositivos intermedios en esa configuración
3. Seleccionar de los dispositivos y configuración en la red, en función del análisis realizado anteriormente y de la funcionalidad de los mismos en el diseño que se propone.
4. Instalación de los Cortafuegos

Principales aportes relacionados al objeto de estudio

A continuación, se describen algunos aportes citados en diferentes fuentes que abordan la seguridad perimetral lógica, y que son relevantes para la presente investigación.

En (Díaz Y. , 2017) se plantea un diseño de seguridad perimetral con LDAP, en el modelo propuesto, el perímetro está formado por las máquinas virtuales, las cuales están bajo un entorno de red interna y pueden interactuar con otras redes. En la arquitectura se propone cortafuegos y DMZ, instalación de anti spam, antivirus, segmentación de servicios y VPN. El proyecto demuestra las ventajas y capacidad para una fácil administración de cuentas de usuario y control de acceso a diferentes directorios, bajo autenticación controlada dentro de la red de área computacional.

Por su parte (Díaz C. M., 2013), propone un proyecto, en el que se utilizan Cortafuegos, IDS e IPS (Sistemas de Detección de Intrusos) Antivirus de correo, Proxys Servidores de DNS, Servidores radius, Servidor de NTP, Sistemas de gestión de ancho de banda, Sistema de monitorización de equipos y Sistemas de realización de backups, con este diseño el autor logra una red escalable, tolerante a fallos eficiente y segura.

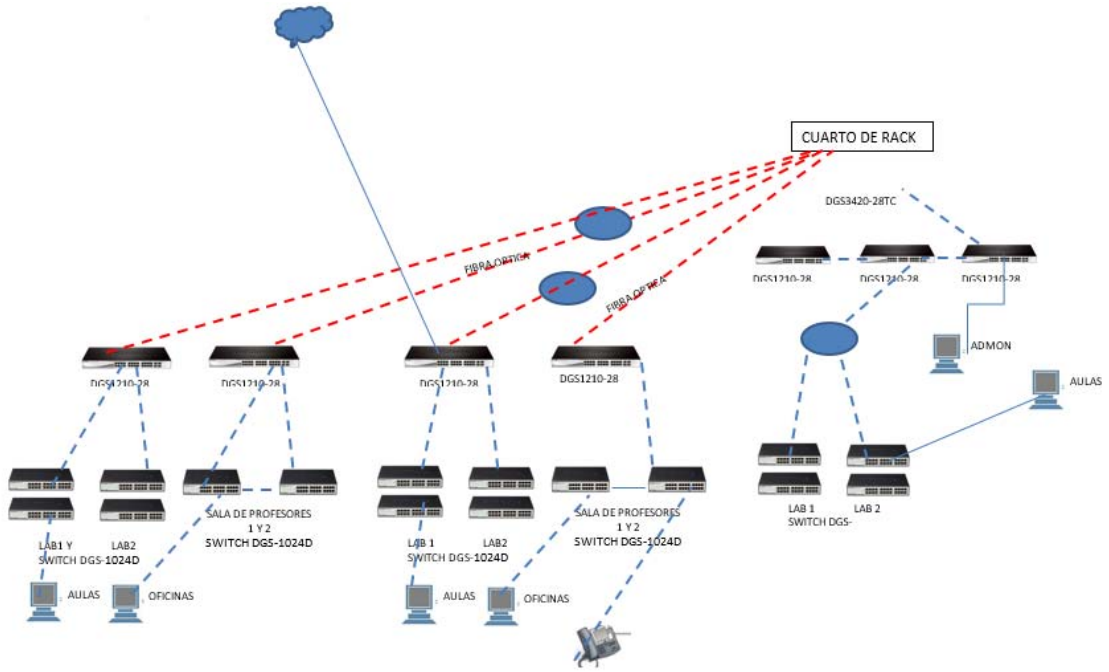
Otro trabajo es el presentado por (González, 2017), el mismo implementa un sistema de seguridad perimetral en un entorno de prueba virtualizado con doble capa de firewall, sistema de protección de intrusos (IPS), un correlador de eventos de seguridad o SIEM para realizar búsquedas forenses y aumentar la detección con este proyecto se logra alcanzar un sistema de seguridad con una inversión mínima en infraestructura.

Un estudio similar es realizado por (Constante, 2016), el autor propone un diseño de red Cortafuegos NGFW de nueva generación (CheckPoint 4800 o Palo Alto 3020) lo que permite proporcionar una protección superior en el área perimetral, de esta forma cubre el nivel físico y de enlace de datos hasta la capa 4 (transporte) del modelo OSI, de ataques externos.

Adicionalmente (Gonzales, 2012) plantea un diagrama con tres zonas de seguridad, zona de internet, zona DMZ donde se ubica el servidor anti spam y el concentrador VPN SSL.y zona Interna. De esta forma se conecta la red de datos de la empresa, considerando como tal, los servidores internos, equipos de red y computadoras de los usuarios.

Diseño anterior de la Lan

La red de computadoras a protegerse al momento de iniciar los trabajos se encuentra montada según se presenta en la figura



En este gráfico se evidencia claramente que la infraestructura local (router o equipo wifi), está conectada directamente al router del proveedor de internet. El router de la LAN, no tiene seguridad alguna, una sola red da servicios a las áreas administrativas, docentes, aulas, biblioteca y laboratorios, siendo una red plana

Haciendo un análisis a nivel de capa física, el medio de transmisión es híbrido, con fibra óptica y par trenzado, o fibra óptica y enlace inalámbrico. Este último utiliza protocolo de encriptación de datos como WPA.

Cada edificio consta con dos laboratorios, en cada uno de ellos están instalados dos switches marca Dlink modelo DGS-1024D de 24 puertos de 10/100/1000 no gestionables, en la sala de docentes se encuentra uno de iguales características. Estos dispositivos se conectan a un panel central de cada edificio a 2 Switch acceso

DGS1024D y estos a su vez por fibra óptica al Bloque B, con el Switch de distribución DGS3420-28TC. En este local también se ubican 3 Switch de acceso DGS1210-28 para la conexión de los laboratorios del edificio B.

En base a la infraestructura de red y el diseño actual del campus se detectan algunas deficiencias que comprometen el desempeño de la misma.

- No existe un servidor de puerta de enlace (Proxy) y dominio que permita establecer permisos a los usuarios de la red.
- No hay configuración de VLAN a nivel de Switch para separar la red o un switch de capa 3 para enrrutar las redes y de esa manera separarlas de manera lógica.
- La clase de red implementada en todo el campus es Clase C) para el edificio D y Clase C para el resto de los edificios, debido a que hay un router intermedio recibiendo una clase nateada. Para la red de Wifi si es clase B por el rango de ip que se maneja.
- La red no está segmentada, lo que hace que aumente considerablemente el tráfico de broadcast y colisiones en la red.
- La seguridad de la red está en un nivel muy bajo o nula y no se puede administrar, además de no ser administrable, no es escalable.
- El diseño de red es no jerárquico imposibilitando la redundancia, lo que hace que el servicio sea deficiente y no permita la escalabilidad de la red.

Análisis y discusión de resultados.

Para obtener un modelo robusto y escalable se opta por un modelo que permita cubrir las necesidades a nivel de seguridad del negocio, infraestructura y de la información.

Este proyecto se desarrolló en varias fases teniendo en cuenta los tiempos en que se ejecutó y los cambios que fueron necesario ir realizando en el diseño inicial. Lo primero que se requiere para el diseño es la integración de un Cortafuegos que se encargue de controlar el acceso entrante y saliente de los servicios de internet. El cortafuego controla los accesos que vienen desde Internet y entran a la red, de igual manera hace un filtrado hacia los DMZ. De esta manera, las conexiones desde la red interna y la externa a la DMZ estarán permitidas, mientras que las conexiones desde la DMZ solo se permitan a la red externa, así también, los equipos en la DMZ no pueden conectar con la red interna, de esta forma se tiene un nivel más de seguridad.

Las aplicaciones que serán consumidas, o que tendrán consumo masivo, desde internet son:

- Servidores Web
- Servidores Endpoint
- DNS externos

Diseño ideal

En el diseño de seguridad perimetral ideal, los autores consideran en base a los estudios realizados el uso de cortafuegos NGFW, IDS, IPS y DMZ.

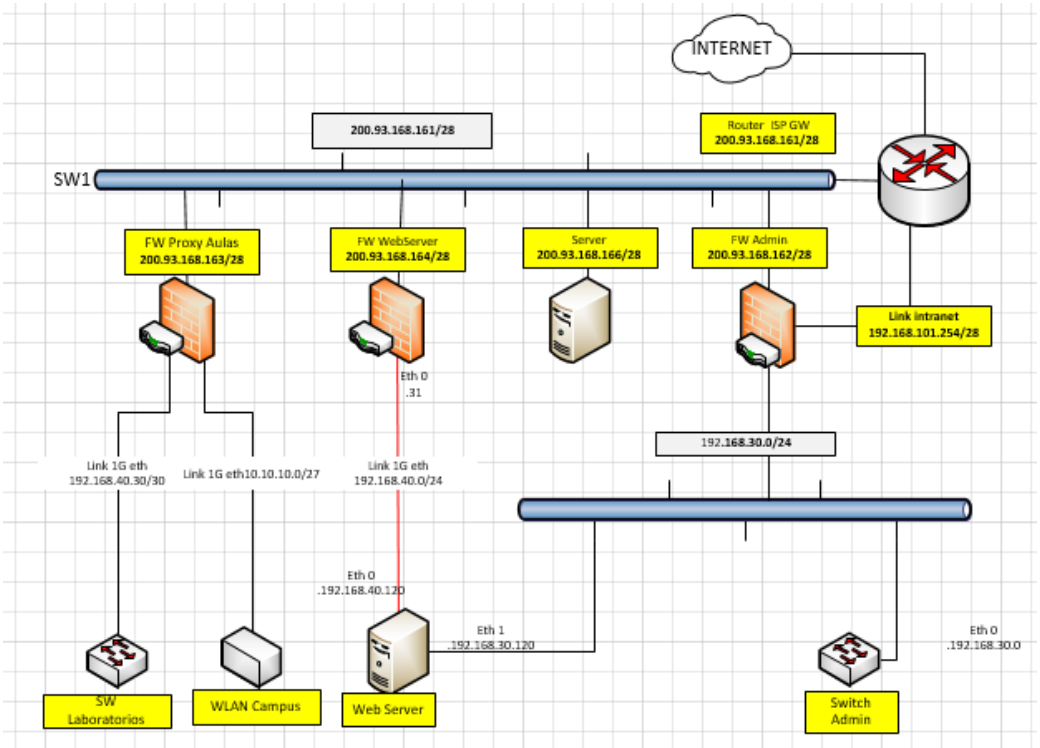
En la primera parte del gráfico se muestran dos Cortafuegos, de esta forma se busca tener redundancia. Esta primera barrera es un Cortafuegos Appliance NGFW que, además de tener la lógica y los accesos de las DMZ, también tiene los siguientes servicios:

- IDS: Para enviar alertas de las amenazas detectadas
- IPS: Defenderá el perímetro de los ataques o software maliciosos que encuentre el IDS
- Conexión VPN: Permitirá a los usuarios establecer una conexión virtual a la red de la empresa, sin tener que estar físicamente ahí
- Control de ancho de Banda
- Proxy/URL Filtering
- Proteccion de Seguridad:
    - Anti DDoS
    - Reputación Web y de IP
    - Black List and White
- Antivirus
- Seguridad en capa 4 y capa 7 (modelo OSI): Se protege la capa de transporte y de aplicación para evitar los ataques conocidos como *denegación de servicios*

La lógica y los accesos de las DMZ están publicados en el primer Appliance NGFW. Adicional, aisladas y separadas de cada una:

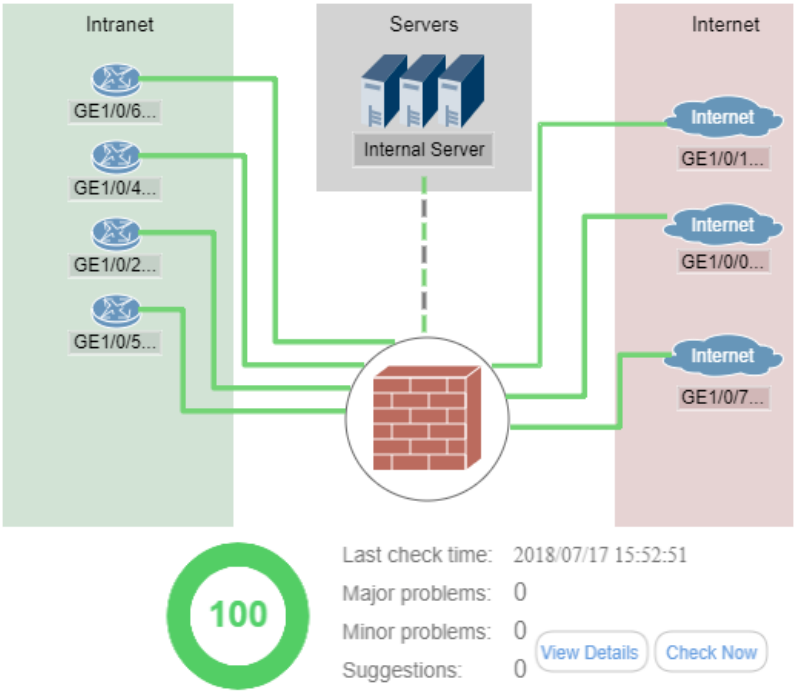
- DMZ 1: DMZ-Server
- DMZ 2: DMZ – VPN
- DMZ 3: DMZ - Guest

Luego, el NGFW, se conecta con la consola de IDS, la cual está en constante escaneo de las cargadas recibidas y enviará las alertas correspondientes para tomar las acciones necesarias.

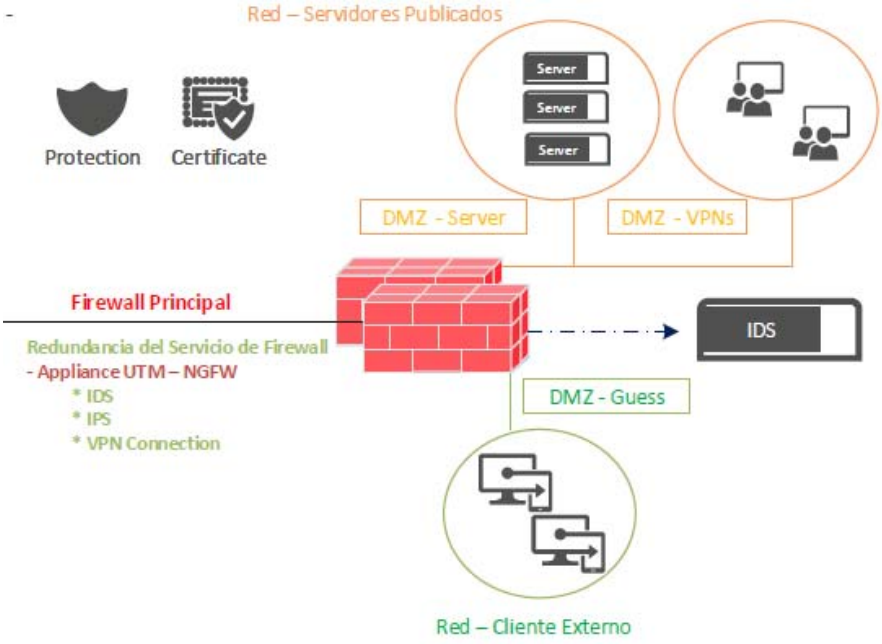


Diseño de la DMZ

En el gráfico siguiente se puede apreciar la configuración de la DMZ, la cual se conecta a una interface pública mediante la interface GE 1/0/1, mientras que internamente se ha configurado una interface desmilitarizada en la Lan tomando una interface GE1/0/6 donde se conecta el web server para que responda las peticiones que vienen desde internet y sean contestadas sin ningún tipo de bloqueo.



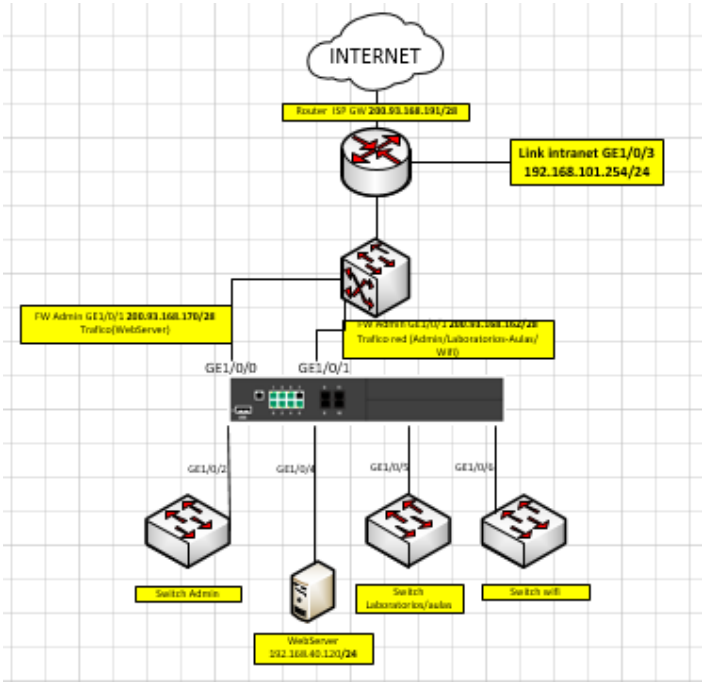
Se deben tomar en cuenta ciertas políticas de seguridad para la red interna ya que al estar dentro de la infraestructura cualquier intensión de intromisión desde esa red DMZ debe ser bloqueada, cualquier tipo de petición sospechosa debe ser rechazada utilizando una lista de control de acceso.



En la segunda parte del diseño, como protección adicional, se coloca otro Appliance NGFW o UTM luego del IDS para filtrar las amenazas detectadas por el IDS. Este Appliance tiene una conexión a una consola SYSLOG que almacenará los eventos que se presenten. El segundo NGFW - UTM está conectado a una consola IPS de Siguiente Generación (NGIPS), la cual, a su vez estará conectada a la consola SYSLOG, pero que a diferencia del UTM (el cual almacena información), el NGIPS extrae información de la consola para prevenir una posible filtración del UTM.

La NGIPS estará conectada al switch de la red local de los usuarios (Network – Lan Users), a su vez, estará conectado un Servidor Endpoint de Antivirus al mismo switch. De esta manera, el Endpoint recibirá las definiciones de del NGIPS y actuará preventivamente.

El Endpoint será la última barrera de protección antes de ingresar a las Vlans de los usuarios. Garantizando una red más segura. El Endpoint también tendrá una lógica de filtrado web, que a su vez enviará estas definiciones a los dispositivos de prevención. Con esto se logra que la navegación realizada por los equipos de los usuarios tenga seguridad, principalmente para el departamento de finanzas, quienes constantemente acceden a páginas de entidades financieras.



La tercera parte se utiliza un tercer Appliance NGFW – UTM. Este se conecta a la red de servicios (Network – LAN Core – Services) y a la red de aplicaciones (Network – LAN Application).

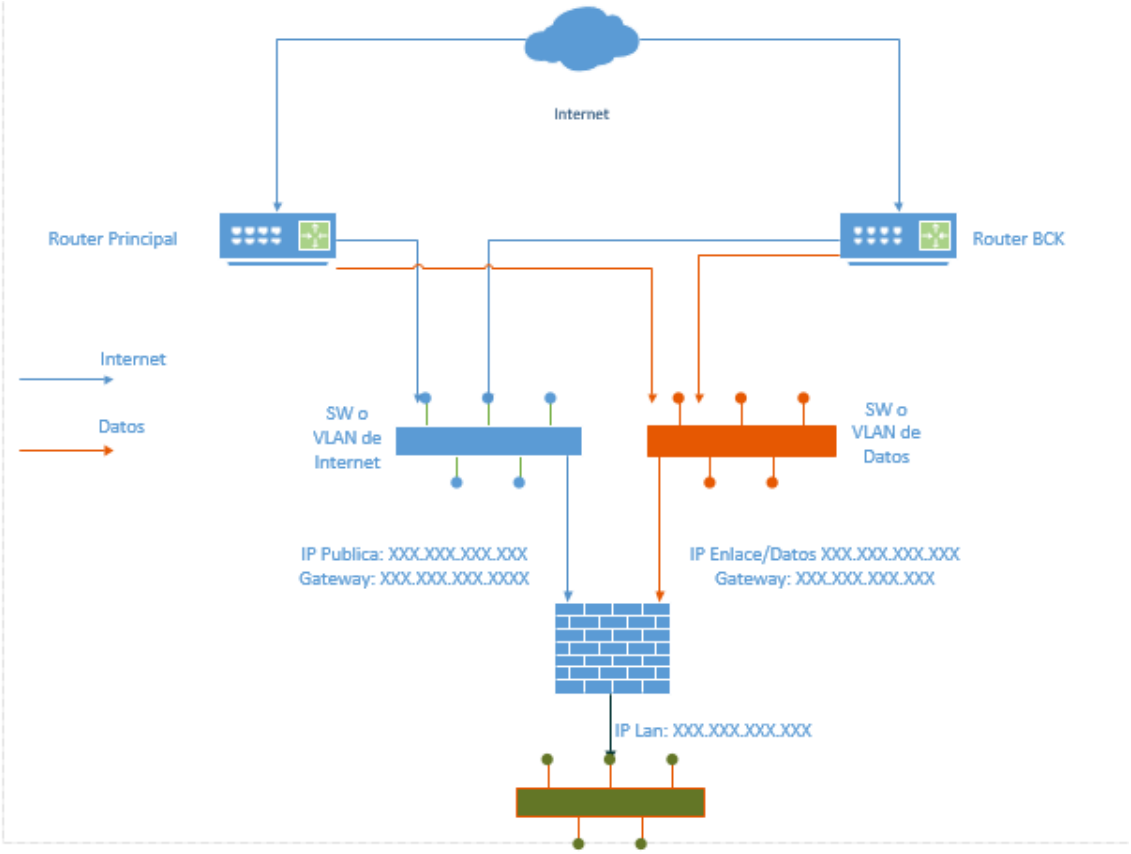
El tercer Appliance se pondrá entre la red de servicios / la red de aplicación y la red de usuarios. De este modo, cuando la red de usuarios quiera consumir servicios de las aplicaciones, llegarían a este tercer Cortafuegos. Es por tanto, que este último equipo controla lo que las aplicaciones necesiten para consumir servicios.

Para tener un mayor control y seguridad de los datos de la empresa, se contrata un servicio de Cloud Anti Spam, esta sería la primera línea de la defensa de toda la red

de datos, ya que estaría conectada entre los equipos de los proveedores de internet, y al primer Appliance NGFW – UTM.

RouterISP Redundante

Con vista a brindar una mayor seguridad en cuanto a la continuidad de negocio, es tomado en cuenta una alta disponibilidad o redundancia en los routers de ISP, esto permite tener el servicio de internet de manera constante, en el caso de haber una caída por el lado del enlace principal se sufriría una pérdida del servicio de internet por menos de 5 minutos ya que existen dos conexiones al ISP desde internet con un un enlace Backup



Adicionalmente se configura un enlace de datos por medio de una VPN creada por el ISP para la comunicación con otra sucursal o campus. Se agrega un switch entre los router y el firewall, en este switch se han creado VLans para separar ambas redes la de internet y la de datos.

En cada VLan se conectan los routers y a su vez la conexión hacia el firewall, ambas conexiones funcionan dependiendo de la disponibilidad, teniendo como prioridad el enlace declarado como principal. De igual manera en el enlace de datos, las interfaces de cada router en la cual está configurado el enlace de datos llega a la VLan asignada y de esta VLan una conexión al firewall el cual internamente o lógicamente tiene las Rutas estáticas para enlazarse a las sucursales o campus correspondientemente.

CONCLUSIONES

- De acuerdo al estudio realizado, partiendo de la búsqueda de la bibliografía relacionada al tema de investigación, se pudo determinar que metodología utilizar para poder elaborar un diseño de seguridad perimetral escalable.
- El uso de cortafuegos appliance NGFW agrega a la red servicios de extras de seguridad perimetral lo que permitió a la universidad mejorar los servicios que brinda con una mayor eficiencia y seguridad.
- El diseño de una dmz separada de la Lan permite el tráfico solamente hacia esa zona, dando mayor seguridad ante un posible ataque.
- La implementación de un Router ISP redundante permitió mantener el servicio de internet de manera constante brindando mayor calidad en los servicios.
- El diseño de un sistema seguridad perimetral controlada por Cortafuegos a lo largo de la red de la universidad, aseguran un uso eficiente de los recursos tecnológicos.
- El diseño permite la redundancia en los servicios hacia internet logrando un uso eficiente de todos los recursos de la red.

BIBLIOGRAFÍA

Bohórquez Gutiérrez, M. A. (2017). *Diseño de un sistema de seguridad perimetral en las instalaciones del consorcio expansión PTAR Salitre, Sede Bogota DC.* Recuperado el 25 de agosto de 2018, de https://repository.ucatolica.edu.co/handle/10983/15322

Colomés, P. (5 de 12 de 2015). *Redes Cisco.net*. Recuperado el 23 de agosto de 2018, de http://www.redescisco.net/sitio/2015/12/05/que-es-la-dmz/

ComputerWord. (18 de octubre de 2017). *Seguridad*. Recuperado el 20 de agosto de 2018, de http://www.networkworld.es/seguridad/que-es-un-firewall

Constante, M. B. (10 de agosto de 2016). *http://repositorio.puce.edu.ec*. Obtenido de http://repositorio.puce.edu.ec/bitstream/handle/22000/11158/BonillaAlejandra_SeguridadPerimetralADS.pdf?sequence=1

Díaz, C. M. (2013). *Implantación de un sistema de seguridad perimetral.* Recuperado el 20 de agosto de 2018, de Archivo digital UPM: http://oa.upm.es/22228/1/PFC_CARLOS_MANUEL_FABUEL_DIAZ.pdf

Díaz, Y. (diciembre de 2017). *Proyecto de grado.* Recuperado el 25 de agosto de 2018, de http://repository.poligran.edu.co: http://repository.poligran.edu.co/bitstream/handle/10823/1070/ProyectoDeGrado_PrototipoModeloSeguridadPerimetralLDAP.PDF?sequence=1&isAllowed=y

Estrada, A. C. (2016). *Seguridad en Redes.* Madrid: opensource.

Gemalto security. (11 de julio de 2017). Recuperado el 25 de agosto de 2018, de https://www.gemalto.com/press/pages/cuidado-con-la-brecha-un-estudio-de-gemalto-revela-que-las-empresas-confian-demasiado-en-mantener-a-raya-a-los-hackers.aspx

Gonzales, J. L. (10 de agosto de 2012). *http://tesis.pucp.edu.pe/repositorio*. Recuperado el 25 de julio de 2018, de http://tesis.pucp.edu.pe/repositorio/bitstream/handle/123456789/1448/VALENZUELA_GONZALES_JORGE_ARQUITECTURA_SEGURIDAD_PERIMETRAL.pdf?sequence=1

González, R. C. (16 de julio de 2017). *Los sistemas de seguridad perimetral y principales vectores de ataque web*. Recuperado el 20 de agosto de 2018, de http://openaccess.uoc.edu/webapps/o2/bitstream/10609/52986/6/rperezgonTFG0716mem%C3%B2ria.pdf

Inteco. (noviembre de 2015). *Instituto Nacional de Tecnlogías de la Comunicación.* Obtenido de Cátalogo de empresas y soluciones de seguridad TIC: https://www.incibe.es

Rabanales, H. R. (20 de mayo de 2012). *http://biblioteca.usac.edu.gt*. Recuperado el 22 de agosto de 2018, de http://biblioteca.usac.edu.gt/tesis/08/08_0236_EO.pdf

Romaní, I. O. (20 de julio de 2017). Obtenido de http://www.catastro.meh.es/documentos/publicaciones/ct/ct61/61_4.pdf

Secure it. (20 de agosto de 2018). *Seguridad perimetral lógica.* Obtenido de https://www.secureit.es/sistemas-de-seguridad-it/seguridad-perimetral-logica/