Ciencia e Ingeniería
Revista Interdisciplinar de Estudios en Ciencias Básicas e Ingenierías.
Año 2020, Enero- Junio, Vol. (7) N° (1), pp. 28-35. ISSN 2389-9484.
Universidad de La Guajira, Facultades de Ciencias Básicas y Aplicadas e Ingeniería.
La Guajira-Colombia.
Revista en Línea http://revistas.uniguajira.edu.co/index.php/cei

IMPORTANCIA DE LA IMPLEMENTACIÓN DE FIREWALL EN REDES EMPRESARIALES COMO MECANISMO PARA LA PROTECCIÓN DE INFORMACIÓN

IMPORTANCE OF THE IMPLEMENTATION OF FIREWALL IN BUSINESS NETWORKS AS A MECHANISM FOR THE PROTECTION OF INFORMATION

Elias Fernando Mora Bandera y Sara Luz Villero Contreras

1 Ingeniería de Sistemas. Universidad de La Guajira. efmora@uniguajira.edu.co

Recibido : julio 26 de 2019 Aceptado: octubre 20 de 2019

RESUMEN

Los firewalls representan actualmente uno de los elementos de seguridad informática para las redes empresariales debido a las características y cualidades de los mismos en cuanto a la protección de información y datos de las mismas, los cuales son uno de los elementos estratégicos y operativos más sobresalientes para cualquier organización que busque ser competitiva. Ante ello, el presente trabajo investigativo parte de una metodología de revisión de bibliografía y literatura donde se indaga y expone sobre las diferentes consideraciones relacionadas con los firewalls, sus características y tipologías. Así como la implementación de los mismos en diferentes organizaciones variadas entre sí para mostrar la variedad de aplicación que esta herramienta tiene en torno a la seguridad informática. Por último se plasman los resultados, conclusiones y recomendaciones encontradas frente a la temática de firewalls así como las perspectivas y consideraciones frente a nuevos estudios que deben ser tomadas en cuenta para expandir la temática.

Palabras clave: Redes Empresariales, Seguridad Informática, Firewalls, Vulnerabilidad

ABSTRACT

Firewalls currently represent one of the elements of computer security for business networks due to their characteristics and qualities in terms of information and data protection, which are one of the most outstanding strategic and operational elements for any organization seeking to be competitive. Given this, this research work starts from a literature and literature review methodology where it is investigated and expounds on the different considerations related to firewalls, their characteristics and typologies. As well as the implementation of the same in different organizations varied among themselves to show the variety of application that this tool has around computer security. Finally, the results, conclusions and recommendations found regarding the issue of firewalls are reflected, as well as the perspectives and considerations regarding new studies that must be taken into account to expand the issue.

Keyword: Enterprise Networks, Computer Security, Firewalls, Vulnerability

1. INTRODUCCIÓN

Elementos como la globalización y la conectividad, así como el desarrollo efectivo de internet y las redes sociales entre otras tecnologías han causado que la sociedad se encuentra inmersa en toda una red donde la información y la estela de datos que deja cualquier individuo sea un insumo importantísimo para las empresas en torno a elementos como la toma de decisiones y la operatividad diaria de la misma. Ya que sectores como las finanzas, la banca, el e-commerce, entre otras industrias son

funcionales gracias a la data que diariamente se mueve a través de internet, puesto que todo este conjunto de información que a la final resulta ser simples 0 y 1 representan todo un conjunto de elementos que hacen posible la vida moderna (Pérez et al. 2016).

Ante esto, es claro que la información y los datos toman un valor sumamente crucial e importante por lo cual la protección de los mismos se convierten en una prioridad para las organizaciones y empresas, ya que si dichos datos cayeran en manos equivocadas los resultados o estragos pueden ser sumamente desastrosos, puesto que se puede prestar para realizar acciones fraudulentas en caso de tratarse de información personal o financiera que son las más delicadas actualmente, pero también se debe entender que no se trata solo del tratamiento de los datos externos que las empresas reciben de sus usuarios, sino también los datos internos de las mismas los cuales son cruciales para su operación y representan en muchos casos un activo estratégico de la misma, ya que existe todo un conjunto de información sensible en torno a desarrollo de productos, investigaciones de mercado, elementos de planeación estratégica, entre otros datos que son cruciales para cualquier empresa y que denotan lo importante que es desarrollar mecanismos los cuales permitan asegurar esta información de todas las partes mal intencionadas que quieran acceder a la misma (Zambrano & Valencia, 2017).

Es de entender, que al estas empresas al estar conectadas a la red, los niveles de seguridad y riesgos de robo de información tienden a aumentar puesto que peligros como virus informáticos, hackers, y violaciones de seguridad de manera remota se pueden dar con mayor facilidad a diferencia de que la información se encontrara en medios físicos como documentos o medios magnéticos.

Es allí entonces, que la seguridad informática dentro de las redes empresariales se vuelve un elemento clave e imprescindible para cualquier organización, por lo cual a día de hoy se han desarrollado una serie de protocolos de protección de datos y encriptación de información con el fin de brindar la mayor seguridad posible a las organizaciones en sus tareas diarias de transmisión de información. Denotando así la importancia de establecer protocolos para la implementación de sistemas de seguridad orientados a la protección de los datos, ante esto se debe entender que las as principales características que un sistema de seguridad tiene o brinda a las empresas tanto naturales como jurídicas en el proceso de transmisión de información y los pilares en el que se fundamentan los mismos son:

• Confidencialidad. Se trata de asegurar que sólo los usuarios autorizados puedan accesar a la información.
• Integridad. Esta busca asegurar que el archivo original no ha sufrido cambios. Dicho archivo puede ser de carácter privado o público.
• Autenticación. Esta ayuda a comprobar y veracidad de la identidad del autor de la información

Uno de estos elementos o tecnologías que ayudan a la protección de la información son los firewalls o contrafuegos, que no son más que una herramienta de software o hardware que filtra todas las conexiones que ingresan a la red interna de la organización o que se dirige hacia el exterior de la misma (Bravo & Barrera, 2020).

Estos firewalls, encargan de supervisar todo el tráfico de red y donde tienen permisos para identificar y bloquear el tráfico no deseado que sea detectado como posible

intromisión de conexiones no autorizadas o maliciosas, y es que la importancia de esta herramienta de seguridad informática se basa en que operan como un filtro que examina todos los paquetes que se dirigen hacia la red corporativa y comparan la información del encabezado con reglas previamente establecidas (Cortés, 2016).

Ante esto, la presente investigación busca abordar todo un conjunto de elementos relacionados con los firewalls, en cuanto a sus características, tipos y condiciones, así como también los niveles de seguridad que ofrecen y la importancia de la implementación de los mismos dentro de las redes empresariales con el fin de constituir un mecanismo efectivo para la protección de la información de dichas organizaciones.

2. MATERIALES Y MÉTODOS

Al tratarse de un artículo de revisión bibliográfica se habla de unidades de análisis las cuales son artículos científicos y publicaciones las cuales guardan una estricta relación con el tema de estudio que para este caso es el de los firewalls, redes empresariales y seguridad informática, ahora para la selección de los mismos se tuvo en cuenta los parámetros de la metodología ToS en cuanto a nivel de importancia, número de veces referenciado, y calificación del articulo con lo que se dio el proceso de estructuración y se procedió al análisis de los mismos (Codina, 2018).

Instrumentos

Para el caso de los instrumentos se utilizó el archivo generado por la mitología ToS el cual fue procesado con Microsoft Excel para determinar los artículos de mayor a menor importancia, luego de esto se procedió a detallar la información que compartía elementos comunes entre los diferentes artículos para con ello delimitar los conceptos encontrados y partir a la construcción de los mismos teniendo como referente 3 elementos claros que son: definición, características y aplicación de los firewalls en torno a la protección de la información, esto se detalla de manera mucho más clara a continuación donde se define el procedimiento seguido para dichas actividades.

Procedimiento

De manera más extensa se establece que para la consecución de los objetivos de la investigación se parte de la revisión de literatura con relación a la temática expuesta a través de conceptos claves además de otros elementos que dan forma a la investigación.
Luego de la consecución de la información se pasa a un proceso de selección y depuración donde se escogen solo las fuentes de información que tengan un aporte bastante significativo para el estudio contribuyendo a la generación de contenido de calidad.

Finalmente, el paso siguiente es el análisis y abstracción de la información de estas fuentes seleccionadas con lo que se procede a la articulación y construcción del informe investigativo donde se plasman los resultados obtenidos, así como las conclusiones más sobresalientes a cerca de la temática abordada.

Fuentes

Las fuentes de información son totalmente secundarias a través de una revisión de bibliografía y fuentes de datos se pretende recolectar la información necesaria para llegar a una serie de conclusiones y consideraciones acerca de los firewalls y la

protección de información, esto a través de la consulta de bases de datos, artículos científicos, noticias y demás fuentes de información accesada.

3. RESULTADOS Y DISCUSION

La seguridad informática y la protección de los datos dentro de la redes empresariales, representan actualmente uno de los campos más importantes dentro de las ciencias de la computación, ya que el volumen e importancia de la información jamas había tenido tanta relevancia como lo es actualmente para las empresas, de igual manera la alta exposición de la misma a posibles acciones que buscan hacerse de manera ilegal con la información también suponen un reto para los administradores de redes de comunicación en internet.

Ahondando en dicha hipótesis, se propuso el estudio de los firewalls como estrategia de seguridad para la protección de la información, ya que como es de recordar un firewall una herramienta de software o hardware que filtra todas las conexiones que ingresan a la red interna de la organización o que se dirige hacia el exterior de la misma (Bravo & Barrera, 2020).

Para comprender dicha importancia, se realizó todo un conjunto de actividades de recolección de información en fuentes de información científicas las cuales ayudaran a demostrar a través de las implementaciones y casos de estudio la verdadera efectividad de los firewalls y las características más relevantes a cerca de los mismos dentro de la función de la protección de la información y datos para las redes empresariales.

Es así entonces, que se describe en primera medida la operatividad de los firewalls los cuales según el estudio de (Almeida & Herrera, 2019) estos funcionan como un filtro que examina todos los paquetes que se dirigen hacia la red corporativa y compara la información del encabezado con reglas previamente establecidas. Es así entonces que, si la dirección IP y el puerto son válidos de acuerdo con las reglas, el paquete es entregado, en caso contrario se desecha. La misma operación es realizada con los paquetes que son enviados desde interior hacia Internet.

Este funcionamiento, aunque sencillo es bastante efectivo puesto que al firewall desechar los paquetes que no están permitidos y en consecuencia evitar conexiones que no son válidas de acuerdo a las reglas, se puede evitar de manera acertada la propagación de códigos maliciosos a través de la red, accesos no autorizados o posibles intrusiones de terceros a la red corporativa que busquen infiltrarse en la misma con el fin de acceder a la información y/o sabotear la operatividad de la red (Ekos, 2017).

Estos resultados y la efectividad de los mismos han permitido que aun incluso después de más de 20 años de nacimiento los firewalls sigan siendo altamente utilizado en el entorno corporativo y es que según un estudio de seguridad informática en Latinoamérica, el 76% de los ejecutivos de 14 países de esta región cuentan con una solución de este tipo; lo que ubica al firewall en el segundo lugar de los controles de seguridad más utilizados, después de los antivirus (Palo Alto Networks, 2013). Lo que convierte a los firewalls en una de las herramientas de protección de información y seguridad informática con mayor relevancia dentro de las redes empresariales de información.

Ahora, se debe resaltar que existen diferentes tipos de firewalls los cuales responden a necesidades y características propias de las empresas entres los que sobresalen los firewalls de cortafuegos de filtrado de paquetes, los cuales se ocupan de tomar decisiones de procesamiento basadas en direcciones de red, puertos o protocolos. En general, son muy rápidos porque no hay mucha lógica detrás de las decisiones que toman (Martinez, 2017). Así mismo también se encuentran los de puerta de enlace a nivel de circuito, estos operan en la capa de transporte de los modelos de referencia de Internet o OSI y, como su nombre lo indica, implementa el filtrado a nivel de circuito en lugar del filtrado a nivel de paquete (Arismendy, Suta & Parra, 2019).

De igual manera, se resalta el firewall de inspección con estado, como su nombre lo indica realiza un seguimiento del estado de la conexión, en donde los puertos se pueden abrir y cerrar dinámicamente si es necesario para completar una transacción (Gandur & Wadin, 2015).

Ahora, por otra parte también es claro que aunque los firewalls tradicionales siguen siendo funcionales su nivel de seguridad ha disminuido en cierto grado debido al conocimiento de la funcionalidad de los mismos y al desarrollo de herramientas de ataques por parte de los hackers o personas mal intencionadas para burlar dichos protocolos de filtrado establecidos por los firewalls, es por ello que a raíz de esto se ha desarrollado el concepto de nueva generación de firewalls o NGFW los cuales ofrecen mayores niveles de seguridad y confiabilidad para las organizaciones y las redes empresariales dentro de los procesos de protección de sus datos.

La clave de esta protección generada por la nueva generación de firewalls se basa en garantizar la inspección de todos los bytes de cada paquete. Adicionalmente, estas metodologías de revisión y protección de información han de mantener el rendimiento elevado y la baja latencia para que las redes con alto tráfico sigan funcionando óptimamente y no se vean saturadas o limitadas por la operatividad más estricta de los nuevos modelos de firewalls implementados (Cortés, 2016).

Un ejemplo de ello es el estudio adelantado por (Morales, Toapanta & Toasa, 2020) el cual consistió en la implementación de un firewall de nueva generación de tipo perimetral bajo un modelo de virtualización para de la implementación de un firewall perimetral permitió incrementar la eficacia en el control de accesos y protección de los equipos y sistemas tecnológicos existentes en la institución donde se implementó dicho firewall mostrando así la efectividad del mismo y es que la estrategia de cuidar la información mediante el uso de un firewall perimetral, cumple con la protección de la misma, asegurando la integridad, confidencialidad y disponibilidad que son los tres pilares de la seguridad de la información (Chacón, 2018)

Por otra parte, el estudio adelantado por (Guijarro & Yépez, 2018) en el cual se da la implementado un firewall con una red DMZ la cual es una subred que está detrás del firewall pero que está abierta al público que provee servicios como WEB, EMAIL o FTP (Muñoz & Rivas, 2015). El estudio concluyo que el uso del firewall evito que la red sea expuesta en caso de un ataque externo; además se logró la mitigación de malware que provenían de la red interna por parte de los usuarios o proveniente de internet a través de páginas web maliciosas o correos con contenido no deseado. Usando el método planteado en este artículo se pudo comprobar el valor de aplicar defensa en profundidad en las redes empresariales.

Finalmente el estudio de (Quezada, 2016) el cual consistió en la implementación de un firewall para la protección de datos en un área específica de la escuela politécnica de ecuador y el cual arrojo resultados significativos pero a la vez el autor resaltan dentro de las conclusiones más significativas que un firewall por más bien configurado, no es la solución global para los problemas de seguridad; es la base para implementar políticas de seguridad, pero se debe complementar con otros mecanismos que fortalezcan la acción de éste, como son: un IDS, un dispositivo de seguridad de contenido, antivirus, antispam, otras prácticas como el respaldo y el cifrado de información, soluciones de doble autenticación y hasta soluciones de seguridad para dispositivos móviles, cuando éstos son utilizados para acceder a la red corporativa(Mendoza, 2016).

Ante esto, es claro que aunque los firewalls incluso los de nueva generación ofrecen todo un conjunto de soluciones para la seguridad de la información en cada una de las capas de las redes empresariales, estos deben ser complementadas con protocolos de encriptado y seguridad además de otras herramientas que también ayudan al mejoramiento de la seguridad de los datos con el fin de brindar una protección integral de la información para las empresas.

4. CONCLUSIONES

Sin duda alguna los beneficios que se obtienen a través de la implementación de los firewalls dentro de las empresas son diversos, debido a la alta aplicabilidad de los mismos y su fácil configuración per efectividad, ante esto se convierte en la primera opción o barrera de protección para los datos de cualquier empresa. Por lo cual es fundamental el entendimiento de la aplicación de los mismos dentro de los diferentes niveles operativos de las organizaciones.

Es de resaltar, también que al existir toda una gran variedad de estas herramientas en cuanto a sus protocolos de funcionamiento así como de las características que los mismos tienen para ofrecer, las organizaciones y redes empresariales deben ser capaz de detectar cuáles son los tipos de firewall que más convienen para ellos, puesto que el tipo de necesidad y requerimientos difiere en diversos aspectos que van desde el nivel de seguridad, la operatividad, los costos, la configuración entre otras variables que son diferentes entre cada una de las industrias donde estos pueden ser aplicables, ya que las necesidades de empresas del sector financiero son totalmente diversas a las necesidades de empresas productoras o de educación.

Es por ello, que el primer paso para una efectiva implementación de los firewalls dentro de cualquier empresa es la identificación de las necesidades y capacidades que dichas empresas tienen, puesto que si no se puede incurrir en bajos niveles de eficiencia o de economía sin mencionar la vulnerabilidad a la exposición de riesgos debido a que no se utilizan las tecnologías o topologías que son propias para cada industria o sector de negocio, además de dejar a un lado el aprovechamiento de la diversificación ofrecida por los firewalls y sus cambios a lo largo de los años que han sabido responder de manera más que efectiva a las necesidades de seguridad que se han creado a lo largo del desarrollo tecnológico de la sociedad y el aumento del volumen de los datos que a diario son trasmitidos.

Así mismo, se debe entender que los firewalls al ser un desarrollo tecnológico en el área de software se encuentran expuesto a un ritmo de cambio bastante álgido que trae nuevos beneficios, mejoras y características por lo que las empresas deben adoptarlas y estar a la vanguardia de las mismas si de verdad quieren desarrollarse dentro de un ambiente seguro que brinde confiabilidad en el procesamiento de su información y datos, estas deben estar siempre atenta a los cambios que se presentan en la tecnología de firewalls e ir actualizándose en conjunto con la misma.

Esto debido a que las mejoras presentadas buscan generalmente brindar mayor seguridad y robustez a los nuevos problemas de seguridad detectados, puesto que de la misma manera en que se desarrolla la ciberseguridad también crecen las amenazas y los nuevo nuevos retos en cuanto a la protección de la información, por lo que en todo momento se deben estar estableciendo y mejorando los protocolos y mecanismos de protección de información, puesto que las vulneralidades aumentan y no todas pueden ser atacadas de manera efectiva, por lo que se deben redoblar esfuerzos para brindar en la mayor medida posible dichos elementos de protección.

Finalmente, en términos investigativos relacionados con el trabajo adelantando se recomienda adelantar un proceso practico de implementación el cual ayude a comprobar y validar lo postulado teóricamente durante todo el texto, a través de situaciones de casos reales o simulaciones validadas las cuales generen una serie de resultados

Es por ello que el fortalecimiento de la seguridad informática dentro de las redes empresariales es un tema que se debe trabajar de manera ardua aprovechando las facilidades que elementos como la globalización y la cooperación internacional ofrecen para los diferentes países en cuanto a la adopción de nuevos protocolos y técnicas mucho más efectivas y escalables para los sistemas informáticos y la validación de la autenticidad de la información y sus remitentes

5. REFERENCIAS BIBLIOGRAFICAS

Almeida, C. A. T., & Herrera, L. R. (2019). La ciberseguridad en el ecuador, una propuesta de organización. Revista de Ciencias de Seguridad y Defensa, IV(7), 156–169

Arismendy Sánchez, J. L., Suta Rincón, J. V., & Parra Martínez, C. F. (2019). Implementación de una herramienta de Firewall y Proxy para el control de las comunicaciones desde un entorno de red.

Bravo Indacochea, G. E., & Barrera Landires, F. A. (2020). Auditoría de seguridad informática en la red de datos de una empresa utilizando como mecanismo de hacking ético el sistema operativo kali linux previo a la propuesta de implementación del firewall PFSENSE y correlacionador de eventos SIEM (Doctoral dissertation, Universidad de Guayaquil. Facultad de Ciencias Matemáticas y Físicas. Carrera de Ingeniería en Networking y Telecomunicaciones).

Cadavid, J. A. P. (2010). Criptografia y la Proteccion a la Informacion Digital, La. Rev. Prop. Inmaterial, 14, 59.

Cano, J. J., & Almanza, A. (2020). Estudio de la evolución de la Seguridad de la Información en Colombia: 2000-2018. Revista Ibérica de Sistemas e Tecnologias de Informação, (E27), 470-483.

Chacón Barbosa, J. (2018). Evidencia digital: procedimientos y protocolos a la luz de los pilares de la seguridad de la información.

Codina, L. (2018). Revisiones bibliográficas sistematizadas: procedimientos generales y Framework para ciencias humanas y sociales.

Cortés Aldana, D. G. (2016). Firewalls de nueva generación: la seguridad informática vanguardista (Bachelor's thesis, Universidad Piloto de Colombia).

Delgado, V., & Palacios Hielscher, R. (2006). Introducción a la Criptografía: tipos de algoritmos.

Ekos, G. (2017). CW 301 - Seguridad. Retrieved September 9, 2019, from Revista datta website: http://revista.datta.com.ec/publication/ebd17345/mobile/?alt=1

Gandur, F., & Wadin, J. (2015). Firewalls a la vanguardia (Bachelor's thesis, Universidad Piloto de Colombia).

Guijarro-Rodríguez, A. A., Yepez-Holgin, J. M., Peralta-Guaraca, T. J., & Zambrano, M. C. O. (2018). Defensa en profundidad aplicado a un entorno empresarial. Revista Espacios

Martínez, C. V. (2017). Firewalls. Gaceta Instituto de Ingeniería, UNAM, 1(114), 21-21.

Mendoza Zambrano, M. M. (2016). Propuesta de implementación de las tecnologías NFV y SDN y su utilización en la red de comunicaciones (caso de estudio UTM) (Master's thesis, PUCE).

Morales, F., Toapanta, S., & Toasa, R. M. (2020). Implementación de un sistema de seguridad perimetral como estrategia de seguridad de la información. Revista Ibérica de Sistemas e Tecnologias de Informação, (E27), 553-565.

Muñoz, M., & Rivas, L. (2015). Estado actual de equipos de respuesta a incidentes de seguridad informática. RISTI-Revista Ibérica de Sistemas e Tecnologías de Informação, 1-15

Palo Alto Networks. (2013). «Guía para compradores de Firewalls,» PAN_BG_090513_ES, Santa Clara.

Pérez Morfi, D., Nuñez Paula, I., & Font Graupera, E. (2016). Globalización y desarrollo local, una propuesta metodológica de gestión de información y el conocimiento. Economía y Desarrollo, 157(2), 107-119.

Quezada Ayala, A. E. (2016). Estudio y diseño de un sistema de seguridad utilizando firewall para la red de datos de la Ex-Facultad de Ingeniería Eléctrica (Bachelor's thesis, QUITO/EPN/2002).

Zambrano, S. M. Q., & Valencia, D. G. M. (2017). Seguridad en informática: consideraciones. Dominio de las Ciencias, 3(3), 676-688.