Universidad Mariano Gálvez de Guatemala

Sede Villa Nueva

Catedra: Seminario de Tecnologías de Información.

Catedrático: Inga. Shirley Gómez

Firewall

Integrantes

Nombre	Carnet
Brandon Roberto Morales Canil	5190-16-2875
Hilmer Ademar Serrano Alonzo	5190-16-6874
Luis Fernando Ixpatá Chen	5190-16-11176
Hardee Rolando Peña	5190-08-13799
Josevictor Emanuel Samayoa	5190-13-11406

Contenido

Introducción

¿Qué tan seguros y confiables son los sitios web que visitan diariamente miles de niños al día, que contenido pueden estar viendo mientras navegan por diferentes páginas web?

Muchas de las páginas que son visitadas por niños pueden tener ciertos enlaces o hipervínculos con contenido no apropiado o no apto para su edad. Es por eso que como grupo hemos decido implementar ciertas restricciones y configuraciones con la ayuda de varias herramientas, donde las páginas que sean visitadas puedan estar libres de anuncios inapropiados, sin contenido ilícito, o también poder evitar que gente con malas intenciones roben información importante de otras personas.

Planteamiento del Problema

Un firewall, también llamado cortafuegos, es un sistema cuya función es prevenir y proteger a nuestra red privada, de intrusiones o ataques de otras redes, bloqueándole el acceso. Permite el tráfico entrante y saliente que hay entre redes u ordenadores de una misma red.

Actualmente en Guatemala adquirir un firewall es sumamente costoso ya que no solo implica el costo del equipo físico sino el licenciamiento y diferentes funcionalidades que puede ofrecer este dispositivo de seguridad, para los hogares, colegios y pequeñas empresas les es difícil adquirir estos servicios por los altos costos.

Los costos de los dispositivos que se manejan hoy día van desde los Q7,000.00 hasta los Q53,000.00 además es necesario adquirir un licenciamiento y soporte los cuales tienen un costo adicional (Guatemala, s.f.).

Formulación del Problema

¿Es importante disponer de un firewall en una casa, centro educativo o pequeña organización?

Objetivo General

Analizar la importancia e implementación de la seguridad en una red doméstica, educativa o empresarial.

Objetivos Específicos

- Conocer las características principales de los Firewalls, tales como su concepto, ventajas y desventajas, tipos de firewalls y las arquitecturas más utilizadas en la actualidad.
- Evaluar los costos que conlleva la adquisición e implementación de un firewall.
- diseñar la arquitectura del firewall a implementar, tanto como las políticas de seguridad para la utilización en esta implementación.
- Realizar pruebas que depuren la configuración del servidor cortafuego desde el otro extremo de la red local.

Hipótesis

¿Una de las vulnerabilidades que pueden presentar los Firewall’s en Linux pueden ser por una mala configuración ya sea en el software o hardware, que pueden ser perjudiciales para el sistema?

¿Si la escuela tiene fugas de seguridad en su firewall, y no lleva un adecuado funcionamiento de control de su firewall se puede comprobar que sus configuraciones no son adecuadas para dicha red donde se implementará?

Justificación

La justificación está orientada a indicar por qué deberían utilizarse recursos para el desarrollo de la tesis. Para su planteamiento, en el caso de Ecuador, se recomienda que se justifique en base a las líneas de investigación de la universidad y el Plan Nacional de Desarrollo del país.

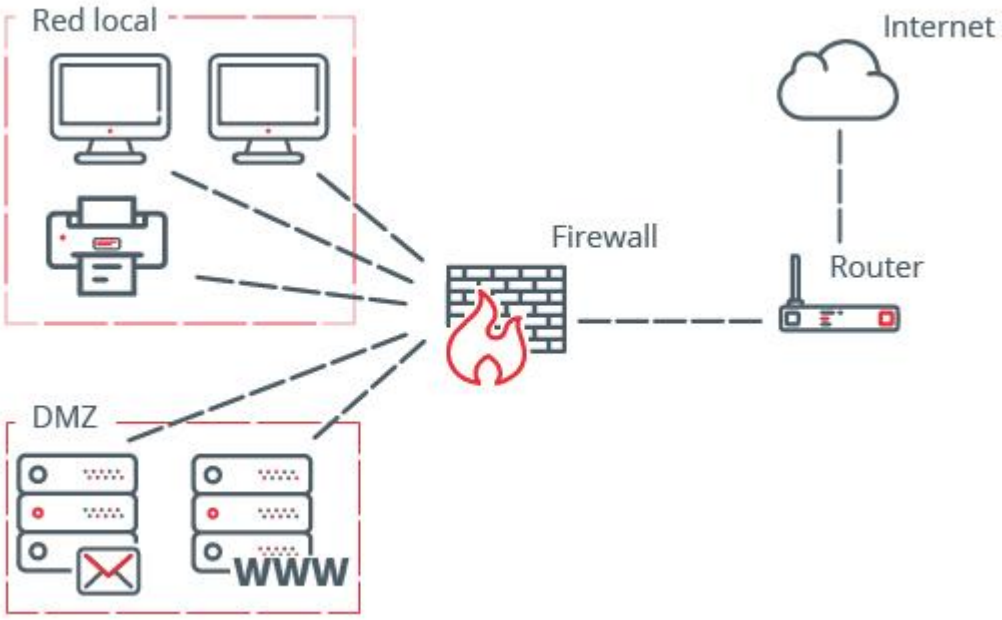
En esta investigación, queremos mostrar la importancia de la seguridad informática en las redes locales y externas; especialmente en la implementación de firewalls, porque esto nos permite controlar mejor el tráfico de datos a través de permisos, de manera que solo aquellos que tienen permitido ingresar a cualquier red Para acceso.

Hay muchos ejemplos de este problema en la actualidad. Un ejemplo es el llamado ataque de denegación de servicio (DDos), que ataca a servidores de PC con diferentes IP; en lo que respecta a los virus, solía hacerlo sin un firewall. es abrir puertos y atacar fácilmente por piratas informáticos. En nuestra era moderna cuando nos ocupamos del ancho de banda, diferentes empresas que brindan estos servicios a cada usuario han adquirido enrutadores con firewalls integrados para poder controlar los puertos que deben abrirse para diferentes funciones.

Todos estos problemas están controlados por firewalls, porque nos ayuda a evitar que cualquier intruso robe o deshabilite la información de algún usuario, ya sea con tarjeta de crédito o pago por Internet, estas son las funciones que implementan estos firewalls.

Definición básica de Firewalls

Un firewall es un sistema que permite ejercer políticas de control de acceso entre dos redes, tales como la red LAN privada e Internet, que es una red pública y vulnerable. El firewall define los servicios que pueden accederse desde el exterior y viceversa. Los medios a través de los cuales se logra esta función varían notoriamente, pero en principio, un firewall puede considerarse como: un mecanismo para bloquear el tráfico y otro para permitirlo. Un firewall constituye más que una puerta cerrada con llave al frente de la red. Es un servicio de seguridad particular.



Los firewalls son también importantes porque proporcionan un único punto de restricción, donde se pueden aplicar políticas de seguridad y auditoría. Un firewall proporciona al administrador de la red, datos, información acerca del tipo y cantidad de tráfico que ha fluido a través del mismo y cuántas veces se ha intentado violar la seguridad. De manera similar a un sistema de circuito cerrado de TV, un firewall no

sólo bloquea el acceso, sino también monitorea a aquellos que están merodeando y ayuda a identificar los usuarios que han intentado violar su seguridad.

Funcionalidades básicas de los Firewalls

Dentro de sus funcionalidades se destacan las siguientes:

- Bloqueo de paquetes que se originan en un determinado rango de IP, puertos, dominios, direcciones de correo, etc.
- Bloqueo de paquetes formados por determinados protocolos o aplicaciones.
- Bloqueo de paquetes que sean reconocidos como firmas de ataques a sistemas o redes.

  Herramienta de análisis del comportamiento de sistemas y de red.
- Herramienta de análisis forense.
- Sistemas de defensa contra virus, gusanos y spam.
- Bloqueo de virus, gusanos, Troyanos y malware en general.
- Bloqueo del uso de la red que protegen como origen de ataques.

Arquitectura de Firewalls

Son las diferentes formas de combinar y conectar los dispositivos que forman los firewalls, como son los enrutadores, Switches, proxies, los hosts bastión y las redes perimetrales.

Las diferentes arquitecturas dependen del grado de seguridad que se requiera implementar, y tiene que ver también con el costo permitido para diseñar el Firewall.

Arquitectura de Host de doble acceso

En esta arquitectura la red está protegida perimetralmente por un solo Firewall, que protege la red interior de la red exterior en el caso típico de conexión a internet y que tiene instalada dos tarjetas de red.

Una ventaja de este tipo de arquitectura es que el host trabaja hasta capas más altas que los enrutadores y puede realizar un filtrado de paquetes más elaborado. Una desventaja que comprometen el host en el caso de una mala configuración del mismo se da cuando el atacante tiene entrada libre a la red; esta arquitectura tiende a ser compleja en la configuración por el cual lo hace mucho más vulnerable.

El tener este tipo de arquitectura no significa sencillez en la definición de políticas de seguridad ya que a veces las conexiones desde fuera hacia dentro, hay que realizar políticas para las distintas aplicaciones y protocolos.

Su utilización puede ser en:

- Pequeña cantidad de tráfico dirigido a Internet.
- El tráfico dirigido a Internet no crítico.

- No ofrecer servicios a usuarios de Internet.
- La red protegida sin contener datos muy importantes.

Desarrollo del proyecto

Herramientas a Utilizar:

- Hardware:
  - Raspberry PI 4
  - Raspberry PI Case
  - Micro SD (Mínimo 32GB)
  - Switch Cisco 8 Puertos (Administrable)
  - Patchcore Categoria 7 Marca Panduit
- Software:
  - Sistema operativo Windows 10
  - Sistema operativo Linux Distribuciones (Ubuntu, Xubuntu, Debian, PF - Sense, Raspbian.
  - Herramientas adicionales (Pi Hole, IP-Tables , UFW, SSH, NMAP).

Como primer punto cada miembro del equipo se documentará y ampliará sus conocimientos en distintas distribuciones Linux ya que es necesario conocer el manejo de ficheros de configuración por los requerimientos que el proyecto necesita, será necesario contar con un diagrama o mapa lógico como arquitectura para ir

desarrollando por etapas todas las herramientas embebidas que formaran el dispositivo tomando en cuenta hardware y software.

Se trabajará en un ambiente de pruebas en donde procederemos a crear máquinas virtuales las cuales llevarán distintos sistemas operativos para poder validar la compatibilidad al 100%, se instalarán las herramientas específicas para cada equipo de prueba haciendo una emulación a nivel usuario sin seguridad, con esto se obtendrá un Feedback del consumo esto nos servirá para que en el momento de poner en marcha la configuración tengamos métricas e información que podremos analizar y verificar los intentos de ingreso, links maliciosos, anuncios no deseados, etc.

Es necesario recalcar que todas estas pruebas serán realizadas en una red interna en donde contamos con un segmento de ip limitada, este dispositivo se deberá configurar como parte de los DNS para que todos los equipos anclados a la red apunten a esa dirección ip y que el funcionamiento sea el correcto.

Switch administrable

El switch será utilizado de manera física y lógica para la implementación del prototipo, la característica de administración nos permitirá a cada integrante del equipo poder visualizar y aplicar configuraciones de seguridad en los puertos y al ingreso a la consola de gestión, será posible aplicar una segmentación en la red si es necesario a través de diferentes vlan (virutal local area network) logrando con esto agregar más seguridad ya que a través de la segmentación se hacen separaciones de dominios de colisión, adicional es posible administrar el equipo remotamente.

Planificación del desarrollo del proyecto

En el siguiente link podrá acceder a la planificación del proyecto:

https://umgt-my.sharepoint.com/:x:/g/personal/jsamayoac2_miumg_edu_gt/EWaLIJOBWyhBl7GLxVFV8IEBxUkFJTBgoTyuaT-hhQWihg?e=MXCPJL

Alcance

Se tiene previsto realizar este proyecto en un plazo de 3 meses el cual será implementado en el Colegio Mentes Positivas el 30 de octubre del 2021, inicialmente presentaremos un prototipo de forma virtual el cual será presentando el 4 de septiembre, durante el mes de septiembre y octubre estaremos trabajando en la versión final incluyendo hardware y software.

Conclusión

Para realizar este proyecto se consultó documentación como referencia en la implementación del servidor firewall en Linux, con esto logramos obtener conocimientos tanto de software como de hardware durante este trabajo de investigación.

Al momento de lograr la implementación obtenemos la experiencia para configurar un firewall, la creación de usuarios, roles, grupos para un consumo controlado a nivel usuario. Según las medidas de seguridad para el firewall será configurado con bloqueos de sitios web maliciosos.

Bibliografía

Guatemala, C. (s.f.). *Conectividad Guatemala*. Obtenido de Conectividad Guatemala: https://conectividad.com.gt/firewall-60f-1-ano-de-soporte/