CIYA. Ciencias de la ingeniería y Aplicadas, vol. 8 Nº 2, julio-diciembre de 2024, pp. 75-83

Firewall de una red doméstica en Cisco Packet Tracer: Caso de Estudio

Firewall of a home network in Cisco Packet Tracer: Case Study

Andres Paul Delgado Sornoza[1], Washington Xavier Garcia Quilachamin[2], Mikel Angelo Ubillus Amalla[3]

RESUMEN:

Los avances tecnológicos han permitido la instalación de redes WLAN para la intercomunicación entre dispositivos, lo que a su vez presenta vulnerabilidad de datos confidenciales debido a los ataques cibernéticos , lo cual se considera como una problemática. El propósito de este estudio fue determinar una configuración de firewall adecuado en una red doméstica por medio de la simulación de una red WLAN para evitar posibles conexiones externas sin comprometer la conexión. La metodología empleada se basó en el diseño, análisis de conexiones y simulación de la estructura en una red doméstica, empleando el software Packet Tracer de CISCO para la transferencia de paquetes entre los dispositivos. Posteriormente, se implementó la configuración del Firewall que permitió el bloqueo en la transmisión de datos externos de la red corrigiendo las conexiones en el proceso. Los resultados obtenidos determinaron que la configuración del firewall permitió el bloqueo de tráfico externo no deseado, evitando intrusión mediante el envío de paquetes.

Palabras claves: Firewall, Optimización, Cisco Packet Tracer, Seguridad en la red, Red doméstica

Recibido 15 de noviembre de 2023; revisión aceptada 22 de abril de 2024

ABSTRACT:

Technological advances have allowed the installation of WLAN networks for intercommunication between devices, which in turn presents vulnerability due to cyber-attacks, which is considered a problem in relation to the use of smart devices, as well as the configuration not suitable for the protection of confidential data. The purpose of this study was to determine an appropriate firewall configuration in a home network by simulating a WLAN network to avoid possible external connections that present a cyber threat without compromising the connection. The methodology used was based on the design, analysis of connections and simulation of the structure in a home network, using the CISCO Packet Tracer software in which the behavior of data packet transfer between all devices and Subsequently,

[1] Universidad Laica Eloy Alfaro de Manabí, Manta, Ecuador, e1315255651@live.uleam.edu.ec
[2] Universidad Laica Eloy Alfaro de Manabí, Manta, Ecuador, washington.garcia@uleam.edu.ec
[3] Universidad Laica Eloy Alfaro de Manabí, Manta, Ecuador, e1317892014@live.uleam.edu.ec

the firewall configuration was implemented that allowed data transmission to be blocked between all devices and a series of processes were followed to restrict external data from the network, correcting the connections in the process. The results obtained determined that the firewall configuration allowed the blocking of unwanted external traffic, avoiding intrusion by sending packets.

***Keywords**: Firewall, Optimization, Cisco Packet Tracer, Network security, Home network*

1. INTRODUCCIÓN

Los firewalls desempeñan un papel crucial como salvaguardas de datos y constituyen un componente esencial en la seguridad informática. En el mundo empresarial donde la información fluye constantemente entre las organizaciones y su entorno, existe una serie de riesgos, sea de origen interno o externo, que involucren la integridad de la empresa. Tal como menciona Cortes estas amenazas no cesan en su evolución, lo que destaca aún más la importancia del firewall como el principal mecanismo de defensa y protección en el flujo de información [1].

Debido al vertiginoso avance del Internet, la seguridad en las redes se ha erigido como un tema de primordial importancia en la investigación contemporánea. Ying Zhang argumenta que actualmente los cortafuegos tradicionales no son efectivos contra ataques provenientes desde el interior de la red protegida, lo que constituye una amenaza significativa en el ámbito de la seguridad en línea [2].

La proliferación de dispositivos de Internet de las cosas (IoT) en los hogares ha ampliado la superficie de ataque, lo que hace que sea esencial proteger adecuadamente la red [3].

En la era digital actual, la seguridad de la información se ha convertido en un aspecto fundamental de nuestras vidas cotidianas. Con la creciente interconexión de dispositivos y la creación de redes domésticas cada vez más complejas, la protección de los datos y la privacidad se convierten en preocupaciones prioritarias.

El presente estudio se centra en la optimización del firewall en el contexto de una red WLAN doméstica utilizando la plataforma Cisco Packet Tracer, lo que permitirá determinar el comportamiento de conexión entre dispositivos.

Se concluye este estudio con el análisis de tráfico de paquetes obtenidos tanto de transmisión como recepción, anticipando que los resultados obtenidos fueron óptimos para el bloqueo externo.

Objetivo

Mejorar la seguridad de una red doméstica WLAN mediante la implementación de un Firewall simulado en Cisco Packet Tracer, con el fin de garantizar la protección de los dispositivos y datos de la red frente a amenazas externas

2. METODOLOGÍA

Este artículo se fundamenta en la revisión sistemática de la literatura. Para ello se recopilaron, evaluaron y sintetizaron revistas, libros, artículos científicos relacionados con la vulnerabilidad que existe en las redes y simulación de adaptación una red WLAN mediante Packet Tracer. A continuación, se detallan estos procedimientos.

2.1. Procedimiento

El desarrollo de este estudio se lo describe en la Figura 1, el cual está basado en la experimentación simulada y recopilación de la información.

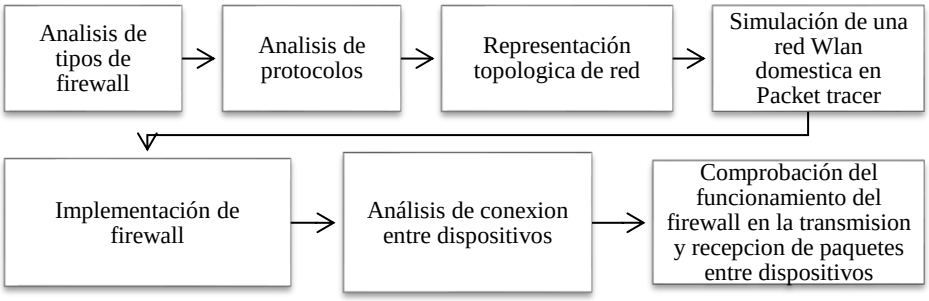

Figura 1. Procedimiento metodológico empleado.

2.2. Tipo de Firewall

Firewall de Inspección de Estados (Stateful Inspection Firewall): Anteriormente conocido como un firewall "tradicional", el firewall de inspección de estados permite el bloqueo de tráfico en función de criterios relacionados con el estado, el puerto y el protocolo. Supervisa todas las actividades desde la apertura de una conexión hasta su cierre, tomando decisiones de filtrado basadas en las restricciones definidas por el administrador y el contexto. Para hacerlo, utiliza información de conexiones previas y paquetes asociados a la misma conexión.

Cheswick menciona que los firewalls desempeñan un papel fundamental en la protección de las redes domésticas contra una variedad de amenazas cibernéticas, incluyendo malware, ransomware y ataques de phishing [4].

Malware: Monje hace referencia al término "malware" o "software malicioso" se utiliza para describir cualquier programa o aplicación informática que, después de infiltrarse en un sistema informático, tiene la intención de causar daño de diversas maneras a dicho sistema (el tipo de daño depende del tipo de malware) de manera deliberada y sin el permiso del usuario, [5].

Phishing: Según Microsoft el phishing tiene como propósito principal obtener información de autenticación de sitios web del usuario, como datos bancarios, cuentas de correo electrónico o perfiles en redes sociales mediante un enlace a través de correo electrónico, que redirige al usuario a un sitio web fraudulento [6].

2.3.Tipos de protocolos

Según Xinzhou, la protección de Firewall funciona en diversos niveles de la arquitectura de red tal y como se muestra en la Ilustración 2, donde se utilizan distintos criterios para restringir el tráfico de red. Esta arquitectura se basa en la suite de TCP/IP [7].

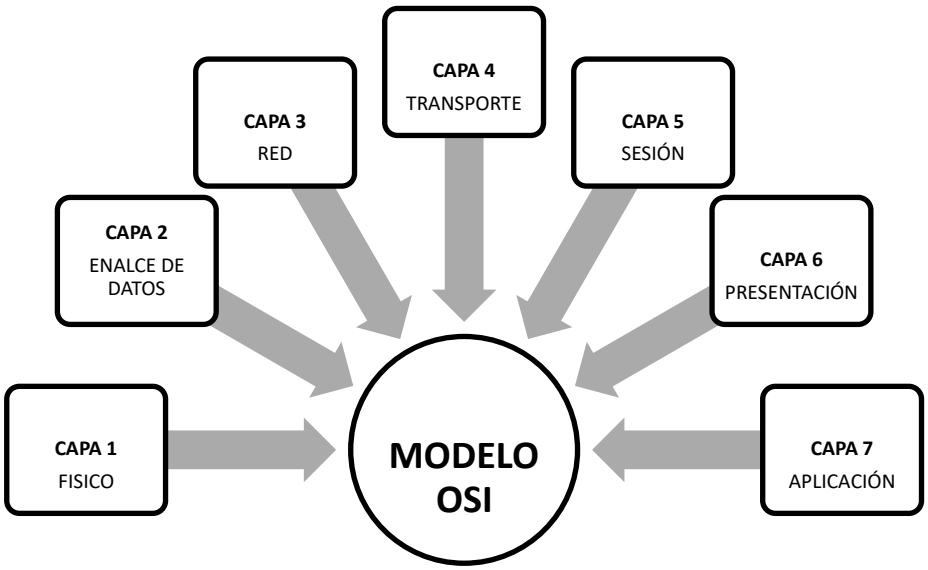

Figura 2. Modelo OSI.

2.4. Topología utilizada.

La topología de estrella es popular en los hogares debido a su simplicidad y facilidad de configuración. Cada dispositivo se conecta directamente al enrutador a través de cables Ethernet o mediante conexiones inalámbricas, tal como se muestra en la Ilustración 3.

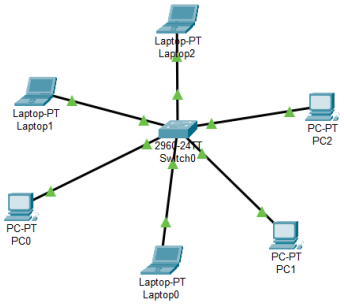

Figura 3. Topología tipo malla.

2.5. Simulador Utilizado.

Cisco Packet Tracer:

Peculea menciona que Cisco Packet Tracer es un potente programa de simulación de red que permite experimentar con el comportamiento de la red, ofrece capacidades de simulación, visualización, creación, evaluación y colaboración y facilita la enseñanza y el aprendizaje de conceptos y tecnologías complejas [8].

Versión de Cisco Packet Tracer: v8.2.1.0118

Tabla 1. Dispositivos Utilizados.

Cantidad	Dispositivos	Modelo
1	***Switch***	*Switch 2960*
1	***Router***	*Router 2901*
1	***access Point***	*Access Point-PT*
4	***Smartphone***	*SMARTPHONE-PT*
1	***PC***	*PC-PT*
1	***Server***	*Server PT*
2	***Laptop***	*Laptop-PT*

En la tabla 1 hace referencia a los dispositivos utilizados en Packet Tracer para la simulación de la red WLan

2.6. Procedimiento de configuración

Se procede a la utilizacion de los equipos mencionados previamente, los cuales incorporan dispositivos inalámbricos de uso diario. Como se representa en la Ilustración 3, se han ubicado siete dispositivos, considerando la configuración típica de equipos en un hogar, que incluyen 2 laptops, 1 PC y 4 smartphones.

La dirección IP asignada al router pertenece a la clase C, una elección común entre las empresas proveedoras de servicios de internet. En este caso, la dirección IP del router es 192.168.1.1, y la máscara de subred está definida por la dirección 255.255.255.0.

Cada dispositivo posee una dirección estática única, que sirve para identificarlo en la red. Esto se debe a que asignar la misma dirección IP a múltiples dispositivos podría ocasionar conflictos y una interferencia entre los dispositivos conectados.

El Access Point proporciona conectividad inalámbrica a los dispositivos mencionados anteriormente

Nombre de red: WIFI-DELGADO **PASSWORD:**123xxxxxxx

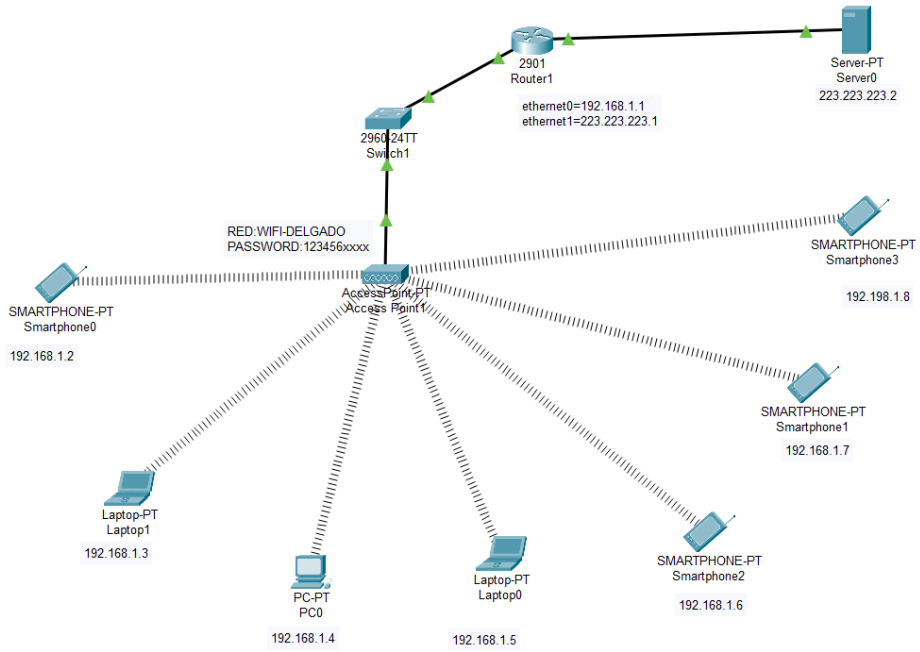

Figura 4. Diseño de Red.

Tabla 2. Lista de Dispositivos.

Dispositivos	***Modelo***	***Direccion IP***
Switch	*Switch 2960*	-
Router	*Router 2901*	*192.168.1.1*
access Point	*AccessPoint*	*192.168.1.1*
Smartphone0	*smartphone-pt*	*192.168.1.2*
Laptop1	*smartphone-pt*	*192.168.1.3*
PC-0	*PC-PT*	*192.168.1.4*
Laptop0	*Laptop-pt*	*192.168.1.5*
Smartphone 2	*smartphone-pt*	*192.168.1.6*
Smartphone1	*smartphone-pt*	*192.168.1.7*
Smartphone3	*smartphone-pt*	*192.168.1.8*
Server	*Server PT*	*233.223.223.2*

En la Tabla 2 se presenta una enumeración de los dispositivos empleados, identificados mediante direcciones IP estáticas de clase C distintas, destinadas a la identificación única de cada dispositivo en la red.

Durante la ejecución del comando ping desde el servidor hacia una computadora o portátil, se confirma la existencia de conexión. Este fenómeno se debe al flujo de tráfico externo que dirige paquetes hacia los dispositivos. En consecuencia, es necesario definir las políticas del firewall para determinar qué tráfico externo se permite ingresar a la red. Además, es necesario especificar que la información transmitida alcance únicamente el router y no se extienda hasta

el servidor externo, con el propósito de salvaguardar la privacidad y evitar la divulgación de información personal.

La configuración de políticas de firewall se realiza en el router, que se define en CLI (Interfaz de Línea de Comando) para permitir o denegar el tipo de tráfico.

Tabla 3. Prueba de conexión entre dispositivos.

Direccion IP 1	Direccion IP 2	Received/Send	Lost %	Tiempo promedio
223.223.223.2	*192.168.1.4*	*4/4*	*0%*	*11 ms*
223.223.223.2	*192.168.1.3*	*4/4*	*0%*	*11 ms*
192.168.1.5	*192.168.1.1*	*4/4*	*0%*	*14 ms*
192.168.1.4	*192.168.1.8*	*4/4*	*0%*	*19 ms*
192.168.1.2	*192.168.1.1*	*4/4*	*0%*	*13 ms*
192.168.1.2	*223.223.223.2*	*4/4*	*0%*	*12 ms*
192.168.1.6	*192.168.1.1*	*4/4*	*0%*	*14 ms*

En la Tabla 3 se evidencia la interconexión entre dispositivos, donde se constata que los paquetes de 32 bytes son transmitidos y recibidos con un tiempo promedio de envío, sin que se registre pérdida alguna en la entrega de paquetes.

3. ANÁLISIS DE RESULTADOS

Al comprobar que, tras realizar la prueba de ping, ningún paquete se pierde, por lo tanto, se procede a realizar una prueba de ping individual a los dispositivos conectados inalámbricamente para envío de paquetes a un servidor externo, simulando ser un servidor extraño y potencialmente peligroso.

Dando como resultado el bloqueo de la recepción de paquetes.

Tabla 4. Prueba de conexión entre dispositivos con firewall en funcionamiento.

Direccion IP 1	*Direccion IP 2*	*Send/Received*	*Loss %*	*Tiempo*
223.223.223.2	*192.168.1.4*	*4/0*	*100%*	*7150 MS*
223.223.223.2	*192.168.1.3*	*4/0*	*100%*	*7220 MS*
192.168.1.5	*192.168.1.1*	*4/0*	*100%*	*11 MS*
192.168.1.4	*192.168.1.8*	*4/4*	*0%*	*18 MS*
192.168.1.2	*192.168.1.1*	*4/0*	*100%*	*13 MS*
192.168.1.2	*223.223.223.2*	*4/0*	*100%*	*12 MS*
192.168.1.6	*192.168.1.1*	*4/0*	*100%*	*14 MS*

En la tabla 4, se ejecutaron evaluaciones idénticas de conectividad entre dispositivos mientras el firewall estaba configurado para obstruir el tráfico. La observación revela que el servidor con la dirección IP 223.223.223.2 intenta establecer conexión con un dispositivo específico. El servidor emite un paquete dirigido hacia el router, pero este último, al bloquear el tráfico externo, impide que el proceso de comunicación se complete internamente. Por lo tanto, aunque los paquetes son enviados, el destinatario rechaza la solicitud de conexión.

ICMP (Protocolo de Mensajes de Control de Internet), que se utiliza principalmente para el control y la gestión de mensajes y errores en las comunicaciones de red, especialmente en el protocolo de Internet (TCP/IP).

Al realizar las pruebas de conexión entre dispositivos, se comprueba que la comunicación interna no se ha visto afectada tras el bloqueo de tráfico, solo se vio involucrado el tráfico externo.

La observación en la recepción de paquetes entre dispositivos señala la incidencia de perdida. Para validar la existencia de conexión en el proceso de recepción de paquetes, se procede a realizar una medición durante un intervalo de 4 segundos. Si este período excede los 4 segundos, indica un mal funcionamiento. En consecuencia, se ha concluido que existe una conexión válida entre los dispositivos cuando se cumple con un tiempo de respuesta apropiado, mientras que, en el servidor, los tiempos de respuesta superan el límite temporal establecido.

4. CONCLUSIONES

- La eficacia del Firewall demostró ser efectiva al bloquear el tráfico externo, tal como se observa en la tabla 4, donde se registró una perdida del 100% en los intentos de conexión desde el servidor externo (IP 223.223.223.2) hacia otros dispositivos internos de la red
- A pesar del bloqueo del tráfico externo, la comunicación interna entre dispositivos no se mostró afectada, como se evidencia en las mediciones de perdidas y tiempos de respuesta.
- El ICMP fue crucial para monitorear la conectividad y validar la efectividad del firewall en el manejo de paquetes, lo que permitió identificar y bloquear intentos de comunicación no autorizados, protegiendo la red de posibles amenazas.
- Sin embargo, es crucial reconocer que el entorno tecnológico está en constante evolución, lo que implica la aparición continua de nuevas vulnerabilidades y amenazas en la red. En este sentido, la implementación de un firewall eficaz no es un fin en sí mismo, sino más bien el comienzo de un ciclo de mejora continua en la seguridad cibernética.

5. BIBLIOGRAFÍA

1. Cortes D, Firewalls de nueva generación: La seguridad informática vanguardista. 2016. [Tesis de Grado]. Universidad Piloto de Colombia.
3. Oviedo, B. Visualizador de tráfico de red de comunicación basada en la Arquitectura TCP/IP, 2020, Retrieved from http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S2218-36202019000200193.
4. Kaylani Bochie, , Vista do Detecção de Ataques a Redes IoT Usando Técnicas de Aprendizaje Profundo. Retrieved from, 2020 https://sol.sbc.org.br/index.php/sbseg/article/view/19242/19071.
5. Monje, R.. Seguridad informática y el malware. Universidad Piloto de Colombia, 2017.
2. Cheswick, W. R., Bellovin, S. M., & Rubin, A. D. Firewalls and internet security: Repelling the Wily Hacker. Addison-Wesley Professional, 2003.
3. Estrada, A. Protocolos Tcp/Ip De Internet. Revista Digital Universitaria, 2002.https://www.revista.unam.mx/vol.5/num8/art51/sep_art51.pdf
6. Muelaner, J. Opciones de protocolo de la capa de aplicación para la funcionalidad M2M e IoT. DigiKey, 2021. Retrieved from https://www.digikey.com/es/articles/application-layer-protocol-options-for-m2m-and-iot-functionality.
7. Proaño, M.. Propuesta de aplicaciones futuras en hogares digitales utilizando el protocolo IPv6". repositorio.puce.edu.ec, 2014.
8. Smartekh. Informe de Amenazas IoT 2020, (2020). Recuperado el 27 de septiembre de 2023, de https://info.smartekh.com/hubfs/IoT/Informe%20de%20Amenazas%20IoT%202020.pdf