UNIVERSIDAD TÉCNICA DE BABAHOYO

FACULTAD DE ADMINISTRACIÓN, FINANZAS E INFORMÁTICA.

PROCESO DE TITULACIÓN

DICIEMBRE 2024 – ABRIL 2025

EXAMEN COMPLEXIVO DE GRADO O DE FIN DE CARRERA

PRUEBA PRÁCTICA

PREVIO A LA OBTENCIÓN DEL TÍTULO DE:

INGENIERO EN SISTEMAS DE INFORMACIÓN

TEMA:

LOS ATAQUES DE DENEGACIÓN DE SERVICIO (DOS) EN LA SEGURIDAD DE REDES DEFINIDAS POR SOFTWARE (SDN).

ESTUDIANTE:

NIXON JAVIER TIERRA REINOSO

TUTOR:

ING. TOMAS ECHEVERRIA SUAREZ

2024/2025

INDICE

RESUMEN

Las redes definidas por software (SDN) a diferencia de las redes tradicionales centralizan la gestión del tráfico por medio de un único controlador, lo que ha permitido una evolución en la arquitectura de redes. A pesar de las ventajas que posee esta arquitectura de centralización es vulnerable a diversos ataques cibernéticos, de manera especial a los ataques de Denegación de Servicio (DoS), estas amenazas tienen como objetivo saturar la red y afectar la disponibilidad del servicio, comprometiendo la seguridad de la información que se transmite. Esta investigación analiza detalladamente las vulnerabilidades que por naturaleza poseen las redes SDN en sus tres capas fundamentales (aplicación, control y datos), identifica los principales tipos de ataques DoS según sus vulnerabilidades y sus impactos en la infraestructura tecnológica en cada una de las capas de la red.

Adicionalmente se realiza la propuesta de diversas estrategias de detección y mitigación de los ataques DoS encontrados en el estudio, mediante herramientas de monitoreo, autenticación reforzada, balanceo de carga y cifrado de datos. Los resultados obtenidos permiten demostrar que la implementación de medidas de seguridad adecuadas, como sistemas de detección de intrusos (IDS) y controladores distribuidos, reducen considerablemente el impacto de los ataques en redes SDN. En conclusión, se indica que una combinación de enfoques de seguridad multicapa y buenas prácticas de configuración es garantiza la resiliencia y estabilidad de las redes SDN.

PALABRAS CLAVES

Redes definidas por software, amenazas, vulnerabilidades y ataques de denegación de servicio.

SUMMARY

Software-defined networks (SDN), unlike traditional networks, centralize traffic management through a single controller, which has enabled an evolution in network architecture. Despite the advantages of this centralization architecture, it is vulnerable to various cyber attacks, especially Denial of Service (DoS) attacks, these threats aim to saturate the network and affect the availability of the service, compromising the security of the information being transmitted. This research analyzes in detail the vulnerabilities that by nature have SDN networks in its three fundamental layers (application, control and data), identifies the main types of DoS attacks according to their vulnerabilities and their impacts on the technological infrastructure in each of the layers of the network.

Additionally, several strategies for detecting and mitigating the DoS attacks found in the study are proposed, using monitoring tools, strong authentication, load balancing and data encryption. The results obtained show that the implementation of appropriate security measures, such as intrusion detection systems (IDS) and distributed controllers, considerably reduce the impact of attacks on SDN networks. In conclusion, it is indicated that a combination of multi-layered security approaches and good configuration practices ensures the resilience and stability of SDN networks.

KEYWORDS

Software-defined networks, threats, vulnerabilities and denial of service attacks.

PLANTEAMIENTO DEL PROBLEMA

Los ataques de denegación de servicio (DoS) son consideradas una de las mayores amenazas a nivel mundial en la ciberseguridad, sobre todo en las Redes Definidas por Software (SDN), a pesar de sus grandes avances, Las diferentes organizaciones siguen enfrentando el desafío de mitigar este tipo de ataques que podrían llegar a colapsar toda una infraestructura de la red. Las Redes Definidas por Software por su centralización y dependencia de un único controlador son mucho más vulnerables a estos ataques, por esta razón conlleva a incidentes de gran escala que afectan a la disponibilidad de servicios, como las plataformas en la nube, algunos servicios financieros e incluso sistemas gubernamentales, lo que ha causado grandes pérdidas económicas y daños a la reputación de las distintas organizaciones. Sin embargo, ya se ha alcanzado un notable progreso en la implementación de medidas de seguridad para proteger este tipo de redes, pero la falta de estándares globales en ciberseguridad y la evolución de los diferentes ataques cibernéticos representan un desafío persistente.

La adopción de Redes Definidas por Software está creciendo en sectores muy importantes en el Ecuador, como en centro de datos y redes corporativas, pero la seguridad en estas redes aun es deficiente. Diversos estudios han revelado que muchas organizaciones, en especial del sector privado, no cuentan con la protección adecuada contra ataques de Denegación de servicios, debido a la falta de capacitación técnica y de recursos económicos para la implementación de defensas sólidas. Esto ha provocado en que los controladores de las Redes Definidas por Software se han visto saturados por estos tipos de ataques, lo que ha afectado las disponibilidades y los servicios. Aunque las infraestructuras de las Redes SDN han crecido en el país, la falta de estrategias

preventivas a expuesto a las organizaciones a riesgos que podrían perjudicar su eficiencia operativa y comprometer la información, además de reducir la confianza en el uso de este tipo de tecnologías.

En ciudades como Quito y Guayaquil, muchas pequeñas y medianas empresas (PyMEs) han comenzado a implementar Redes Definidas por Software (SDN) para optimizar sus operaciones y reducir costos, pero estas empresas enfrentan serios desafíos en cuanto a la seguridad, debido a la falta de conocimiento y capacitación del personal la limitación de recursos financieros para poder adoptar soluciones de protección contra ataques DoS. Esta carencia de configuraciones de seguridad robustas, más la falta de un monitoreo continuo dejan a las redes SDN vulnerables a ataques que pueden interrumpir sus operaciones, causar pérdidas económicas significativas y afectar la confianza de los clientes en sus servicios. Las PyMEs locales son aún más susceptibles a este tipo de ataques debido a su falta de infraestructura avanzada y se ven seriamente afectadas por los ataques DoS, lo que ha limitado su crecimiento y estabilidad en un entorno tecnológico que es cada vez más competitivo.

JUSTIFICACION

Un análisis profundo de los ataques de denegación de servicio (DoS) en las redes definidas por software es de mucha importancia, esencialmente al enfocarse en las diferentes vulnerabilidades que estas redes presentan en base a su arquitectura centralizada, se examinaran como los ataques DoS afectan la disponibilidad y la estabilidad de este tipo de redes, resaltando a sus controladores centralizados como el punto crítico de las Redes Definidas por Software, además de hacer énfasis en las medidas de seguridad que actualmente se implementan en las empresas, evaluando su efectividad en la mitigación de los riesgos que producen estos ataques.

Por lo tanto, al identificar las brechas de seguridad existentes en las redes SDN, sobre todo en las pequeñas y medianas empresas del Ecuador, permitirá realizar un diagnóstico más preciso de las vulnerabilidades existentes, y con esto mejorar la planificación de seguridad y la reducción de incidente, facilitando la optimización de los recursos, lo que ayudaría a las empresas a alinearse con estándares y regulaciones de seguridad.

Es crucial entender que reducir los riesgos relacionados con los Ataques de Denegación de Servicio (DoS) en las redes definidas por software (SDN) es fundamental para garantizar la continuidad operativa de cualquier empresa y proteger los activos críticos, como son los datos sensibles, la infraestructura tecnológica y los servicios esenciales, lo que posibilita fomentar la adopción segura de las Redes Definidas por Software (SDN) en un entorno digital que cada vez es más complejo y expuesto a las ciber amenazas.

Generar una mayor importancia sobre las vulnerabilidades de las Redes SDN frente a los ataques DoS incentivara a las empresas a implementar medidas de seguridad

más robusta, a diseñar programas de capacitación que estén orientados a mejorar las competencias técnicas del personal responsable de la administración de redes, lo que permitirá hacer frente a las amenazas cibernéticas actuales, además de generar estrategias de protección más eficaces que garanticen la continuidad operativa de las empresas, fomentando así la adopción de este tipo de redes en el futuro y fortalecer la infraestructura del país.

OBJETIVOS

Objetivo General.

- Definir las amenazas y las vulnerabilidades de las Redes Definidas por Software (SDN) frente a los Ataques de Denegación de Servicios (DoS).

Objetivos Específicos.

- Identificar las principales amenazas de Ataques de Denegación de Servicio en infraestructuras vulnerables basadas en Redes Definidas por Software.
- Determinar las vulnerabilidades en la infraestructura de redes SDN que son susceptibles a ataques DoS y el riesgo asociado a cada una.
- Proponer estrategias y recomendaciones para fortalecer las seguridades de las redes definidas por software (SDN).

LINEAS DE INVESTIGACION

Línea de Investigación

Un análisis de los ataques de denegación de servicio (DoS) en redes definidas por software (SDN) se enmarca dentro de la línea de investigación "Sistemas de información y comunicación, emprendimiento e innovación". Debido a que las redes SDN representan un avance tecnológico que transforma la forma en que se gestionan y configuran las redes, al separar la capa de control de la capa de datos.

Este estudio producirá un impacto notable en el desarrollo de soluciones dirigidas a empresas emergentes y emprendedores tecnológicos que están creando herramientas de ciberseguridad especializadas, las que buscan proteger las infraestructuras SDN en sectores claves como las telecomunicaciones, la banca y la salud, contribuyendo al fortalecimiento de la seguridad en áreas críticas de la economía y la sociedad.

Sublínea de Investigación.

La sublínea de Investigación “Redes y Tecnologías inteligentes de Software y Hardware” se relaciona con el desarrollo de infraestructuras tecnológicas avanzadas y seguras, por motivo de que estos ataques DoS saturan los recursos críticos como controladores o switchs de una red SDN, se pone en manifiesto la necesidad de integrar tecnologías inteligentes para poder detectar y mitigar estas amenazas, evolucionando a soluciones avanzadas como la inteligencia artificial, aprendizaje automático y análisis de tráfico en tiempo real para predecir y prevenir estos ataques.

MARCO CONCEPTUAL

Redes Definidas por Software (SDN)

De acuerdo con Amaya et al. (2022), las redes definidas por software (SDN) se presentan con una perspectiva revolucionario en la configuración de las redes, ya que en las redes tradicionales el control se asocia con el hardware, mientras que en las SDN el control se traslada a un software llamado controlador. La novedad de esta arquitectura es la separación de la capa de control y la capa de datos, centralizando la inteligencia de la red en el controlador, los dispositivos de red se encargan únicamente de tareas de conmutación con capacidades reducidas, esto permite una gestión y control más flexibles y precisos, facilitando la modificación de funciones y políticas de tráfico, sin tener que interactuar directamente con cada conmutador. A diferencia de las redes tradicionales, donde los paquetes se procesan de manera uniforme, las redes definidas por software ofrecen la capacidad de adaptar dinámicamente el tratamiento de los paquetes según las necesidades específicas, mejorando significativamente la eficiencia y la adaptabilidad de la infraestructura de red, y esto permite una respuesta más ágil a los requerimientos de las organizaciones.

Controladores.

Controlador SDN.

Según Ruipérez, J. (2021), en las redes definidas por software (SDN), el controlador funciona como el núcleo central de la red, gestiona y distribuye instrucciones a los dispositivos según las demandas de las aplicaciones, está ubicado en la capa de control y entre sus funciones principales esta administrar las entradas de las tablas de flujo, tomar decisiones sobre paquetes inusuales y dirigir el tráfico de la red de manera proactiva o reactiva entre otras instrucciones. En el modo proactivo, las reglas se aplican

de forma inmediata, mientras que, en el modo reactivo, el controlador responde a las solicitudes de flujo de los dispositivos, verificando las políticas antes de enviar las instrucciones correspondientes, permitiendo adaptaciones dinámicas a las condiciones de la red, aunque requiere un equilibrio entre el tiempo de configuración y la capacidad de memoria de los dispositivos para mantener las entradas de flujo. La granularidad del flujo es muy importante para lograr un equilibrio entre flexibilidad, seguridad y escalabilidad. Lo que conlleva a enfrentar un nuevo desafío al seleccionar el diseño de control correcto, al ser variable desde un único controlador hasta múltiples controladores distribuidos para la gestión de diferentes segmentos de la red.

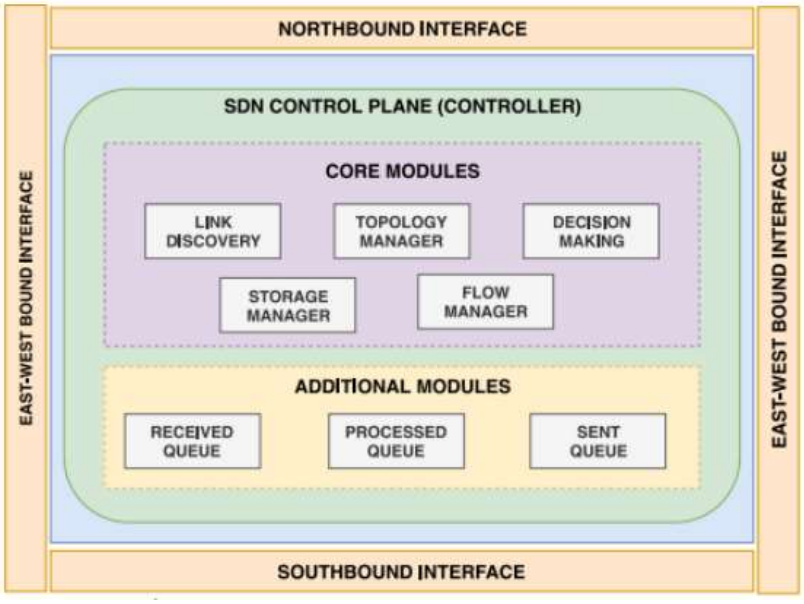

Figura 1: Arquitectura interna del Plano de Control SDN.
Elaborado por: Ruipérez, J. (2021)

Controladores OpenFlow.

Como señala Huawei, (2024) un controlador OpenFlow es el cerebro de la arquitectura SDN y está ubicado en la capa de control para instruir el reenvío de datos a través del protocolo OpenFlow.

Los principales Controladores OpenFlow son:

Controller	Principal Caracterisitcas.
NOX/POX	OpenFlow Controller open-source que proporciona una plataforma para escribir software de control de la red en C++ o Python.
Beacon	Controller basado en Java que soporta operación basada en eventos y multi-hilos.
Trema	Completa plataforma OpenFlow para Ruby/C.
Maestro	Plataforma de control escalable escrita en Java.
SNAC	OpenFlow controlador que usa una interface web para gestionar la web.

Tabla 1: Controladores OpenFlow.
Elaborado por: Roncero, O. (2020)

Amenazas y vulnerabilidades en SDN

Como afirma Becci et al. (2019) en las Redes Definidas por Software, la seguridad representa un desafío crítico debido a la naturaleza centralizada del control y la abstracción de las funciones de red. El controlador SDN funciona como un núcleo centralizado en la red, lo que permite tener multiples ventajas pero también algunas vulnerabilidades que pueden ser aprovechadas por amenazas como ataques dirigidos al mismo controlador, manipulación de las tablas de flujo y debilidades en la comunicación entre la capa de control y la capa de datos, sobre todo a través del protocolo OpenFlow. Dichos ataques se pueden manifestar en muchas formas, como la modificación de reglas de flujo lo que redirige o bloquea el tráfico original, también ataques de denegación de servicio (DoS) y ataques de hombre en el medio (MitM) los cuales interceptan y alteran los datos que se encuentran en tránsito. Por lo cual es necesario fortalecer la seguridad en las redes definidas por software, empleando técnicas de cifrado que protegen las

comunicaciones entre el controlador y los dispositivos de red, junto con políticas de seguridad sólidas que gestionan el acceso y las operaciones dentro de la red. Además, el implementar estrategias de seguridad proactivas y reactivas para reducir los riesgos y garantizar la integridad de las operaciones de red en entornos SDN.

Mecanismos de Seguridad para SDN

Autenticación y autorización

De acuerdo Acosta, O. & Ortega, E. (2023) es importante hacer referencia a la prevención del acceso no autorizado y a la gestión efectiva del acceso, ya que los intentos de accesos no autorizados pueden resultar en la manipulación del flujo de los datos y en cambios de la configuración que pondrían en riesgo la seguridad y la integridad de la red. Para lograr reducir estos riesgos, se debe implementan controles de acceso y sistemas de detección de anomalías que identifiquen el comportamiento inusual en el tráfico de la red, permitiendo una respuesta rápida y proactiva ante amenazas. En las redes definidas por software (SDN), quien gestiona el acceso es el Network Access Control (NAC) que es una herramienta que controla los dispositivos que tienen permiso para conectarse a la red y también a qué recursos tiene permitido acceder una vez conectados. Además, el NAC permite verificar y autenticar los dispositivos antes de permitirles el acceso, lo que asegura que solo aquellos que tienen autorización puedan integrarse a la red, esto permite tener la seguridad de los dispositivos y aplicar políticas de cumplimiento garantizando que los terminales y los usuarios sigan las normativas establecidas.

Sistema de Detección de Intrusos (IDS)

Una herramienta fundamental en la seguridad de redes es el Sistema de Detección de Intrusión (IDS) que en servidore y hosts se localiza en el borde de la red. Identificar

una amenaza a la seguridad de la red implica enfrentar un doble desafío, en primer lugar, detectar flujos de tráfico sospechoso y, en segundo lugar, es determinar si esos flujos son normales o poseen anomalías. Al diseñar un IDS es importante saber dónde debe localizarse, cómo detectara las amenazas, qué tipo de amenazas detectara, qué herramientas de detección son las más apropiadas para detectar las amenazas seleccionadas, etc, Becci et al. (2020).

Tipos de IDS según el grado de conocimiento de las amenazas.

Como señala Mishra et al. (2019) las amenazas se dividen en conocidas y desconocidas, basadas en la cantidad de información disponible sobre ellas. Las amenazas desconocidas, como los ataques del día cero, suelen ser difíciles de detectar debido a que no se asocian con vectores de ataque claramente identificables y las amenazas conocidas pueden ser identificadas a través del análisis de especificaciones, datos estadísticos y protocolos, y mediante la búsqueda en bases de datos especializadas.

Amenazas Desconocidas

Las IDS son diseñadas para detectar anomalías en la red, está compuesto de sistemas que detectan patrones anormales e indican comportamientos inusuales que se realicen en la red, por tal motivo durante la fase de aprendizaje de la máquina, se registra en ella el comportamiento normal de la red, creando un perfil que se comparara con el flujo estándar y así identificar las posibles amenazas, lamentablemente aunque es un método efectivo para la detección de anomalías también suele generar una gran cantidad de falsos positivos. Los auto-codificadores que son redes neuronales artificiales son considerados, aprenden de manera no supervisada las características principales del flujo de datos, resultando especialmente útiles cuando las características del conjunto de datos son amplias, complejas y desconocidas, Gu et al. (2019)

Amenazas Conocidas.

Según Nanda et al. (2020) las IDS basado en firma investiga patrones que coinciden con amenazas previamente identificadas y documentadas en bases de datos como listas negras o en historiales de ataques anteriores. Aunque es efectivo para identificar ataques bien establecidos y reconocidos, falla en detectar ataques nuevos o aquellos no registrados previamente en estas bases de datos.

Resiliencia del controlador

La capacidad para resistir amenazas de un controlador en las redes definidas por software es muy importante para su estabilidad y seguridad, ya que permite proteger estos controladores contra ataques dirigidos y fallos imprevistos, es esencial la implementación de estrategias proactivas, las que deben tener como fin optimizar la ubicación de los controladores principales y de respaldo, y reducir el impacto de estos ataques específicos a nodos, mejorando en gran manera la capacidad de recuperación ante fallos que podrían presentarse. Este enfoque garantiza que, si existiera un controlador comprometido, otros puedan asumir sus funciones sin interrumpir el servicio de la red, asegurando así la continuidad y confiabilidad del sistema, según lo afirma Mycek et al. (2021).

Desde el punto de vista de Bhuiyan et al. (2023) es fundamental implementar un enfoque proactivo en la gestión de la seguridad del controlador SDN, que se limite a reaccionar ante incidentes, identifique y prevenga posibles vulnerabilidades, y vectores de ataque antes de que ocurran. Este enfoque preventivo fortalece la resiliencia del sistema y garantiza la protección de la red, otra estrategia es diversificar los controladores mediante el uso de diferentes instancias y modelos puede ayudar a aumentar la protección ante ataques y fallos, permitiendo a las redes SDN adaptarse y manejar las amenazas, permitiendo la continuidad del servicio y reduciendo la ventana de vulnerabilidad

Las SDN plantean nuevos desafíos que las redes tradicionales no poseen y a medida que estas redes se implementen gradualmente, se pronostica que aparezcan más retos de seguridad que serán necesario abordar. Las vulnerabilidades en las SDN se enfocan principalmente en sus tres capas o planos (aplicación, control y datos), según Báez, J., (2021).

Las principales amenazas en las capas de SDN son las que se presentan a continuación:

Capa	Amenaza	Descripción
Aplicación	Falta de Autenticación y autorización.	No posee mecanismos de autenticación y autorización para las aplicaciones.
	Inserción de reglas de flujo fraudulentas.	Aplicaciones malintencionadas pueden generar reglas de flujo falsas.
	Falta de control de acceso.	Difícil de implementar el control de acceso en aplicaciones de terceros.
Control	Ataques DoS	Su naturaleza visible, su gestión centralizada y sus recursos limitados traen ataques DoS.
	Acceso no autorizado al controlador.	Falta de mecanismos convincentes para imponer el control de acceso.
	Escalabilidad y disponibilidad.	El centralizar el controlador produce problemas de escalabilidad y disponibilidad.
Datos	Reglas de flujos fraudulentas	La capa de datos es más susceptible a las reglas de flujo fraudulento.
	Ataques de inundación	Las tablas de flujo de los conmutadores almacenan un número limitado de reglas de flujo.
	Secuestro del Controlador.	La seguridad del controlador es fundamental para la capa de datos.
	Ataques TCP-Level	TLS (Transport Layer Security) es susceptible a ataques de nivel TCP.
	Ataques Man in the Middle	Debido al uso opcional y complejidad de TLS.

Tabla 2: Principales amenazas en los Planos SDN.
Elaborado por: Báez, J., (2021)

Ataques de Denegación de Servicio (DoS)

De acuerdo con Dong et al. (2019) un ataque de denegación de servicio (DoS) es la coordinación de muchos dispositivos distribuidos en varias ubicaciones llamados

“bots” o “zombis”, estos forman parte de una red controlada de manera remota por un atacante, los dispositivos antes mencionados son utilizados para la ejecución de ataques masivos que son dirigidos a un objetivo específico. El objetivo principal de estos ataques es sobrecargar los recursos de la red, suspendiendo totalmente su funcionamiento, provocando que los usuarios legítimos no puedan acceder a la red.

La distribución de los dispositivos que se utilizaran para el ataque es muy importante para lograr ampliar la escala y la eficacia del ataque, además esto dificulta su detección y mitigación. Los bots son herramientas que son utilizadas para la ejecución del ataque y su gestión depende de la arquitectura de los mecanismos de comando y control de la botnet, los cuales pueden estar basados en protocolos como IRC, HTTP, DNS o redes P2P (peer-to-peer), Tamayo, J., (2023).

Clasificación de ataques DoS:

Desde el punto de vista de Manso et al. (2019) los ataques DoS se categorizan según su criterio, lo cual es importante para entender cómo se ejecutan los diferentes ataques, hacia que recurso es dirigido y que estrategia de defensa se puede implementar.

Las formas en que se realiza un ataque varía dependiendo de la técnica a utilizar y el objetivo a donde está dirigido. Los ataques pueden ser clasificados en tres categorías principales:

Por la técnica de ataque.

Los ataques por su técnica son Ataques de Inundación que utilizan un volumen excesivo de tráfico para sobrecargar la red o los recursos del servidor, estos incluyen inundaciones SYN, inundaciones UDP, e inundaciones HTTP; otro es el ataque de Agotamiento de Recursos que apunta a consumir recursos críticos del sistema como CPU, memoria, o conexiones disponibles, un ejemplo de este es el ataque Slowloris; finalmente

el ataques de Amplificación que se aprovecha de la funcionalidad de los servidores para amplificar la cantidad de tráfico enviado a la víctima, como los ataques de reflexión DNS o NTP, como afirma Manso et al. (2019).

Por el número de fuentes.

Según Katz, O. & Black, J. (2022) existen dos tipos de ataques según el número de fuentes, el ataque DoS simples que es cuando el ataque proviene de una sola fuente, e intenta saturar los recursos de la red de la víctima; y los ataques DDoS (Distributed Denial of Service) que a diferencia del DoS este posee múltiples fuentes a través de una red de bots, estos se coordinan para lanzar un ataque masivo y simultáneo hacia la victima, lo que complica su detección y mitigación.

Por la capa del modelo OSI que atacan.

Existe el ataque a la Capa de Aplicación (Capa 7) que esta dirigido directamente a las aplicaciones, intenta agotar los recursos que son específicos a la aplicación, como a las sesiones web; el ataque a la Capa de Transporte (Capa 4) son como los ataques SYN, que abusan del protocolo TCP para consumir recursos del servidor; y el ataque a la Capa de Red (Capa 3) que incluye ataques como ICMP flood, que pueden afectar la infraestructura de toda la red, según Deb, R. & Roy, S. (2022).

Por la visibilidad del ataque.

Como afirma Tamayo, J., (2023) hay ataques de Volumen Alto que son fácilmente detectables debido al enorme volumen de tráfico generado; y ataques de Bajo Volumen que son más sigilosos y diseñados para no ser detectados fácilmente, enfocándose en técnicas que consumen recursos de manera sutil.

Por su persistencia.

Esta categoría posee Ataques Persistentes que continúan durante un período prolongado y pueden evolucionar en intensidad o técnica; y ataques No Persistentes que son esporádicos o de corta duración, a menudo destinados a probar la capacidad de respuesta de un sistema o su infraestructura de defensa, Correa et al. (2020).

Por el tipo de impacto.

Según Kumar, M. & Bhandari, A. (2023) estos son ataques de Depleción que intentan consumir recursos hasta que se agotan; y los ataques de Disfunción que buscan alterar el comportamiento normal de la red o de los sistemas para crear un impacto negativo, sin necesariamente agotar los recursos.

Ataques DoS en las Redes Definidas por Software.

Según Saurabh et al. (2022) durante un ataque, se envía un volumen significativo de paquetes de datos a uno o varios dispositivos (hosts) dentro de la red. Si las direcciones IP de origen de estos paquetes están falsificadas (algo común en este tipo de situaciones), el conmutador no podrá encontrar una coincidencia en su tabla de flujo y se verá obligado a redirigir los paquetes al controlador. Esta acumulación de paquetes que son de usuarios legitimo y de usuarios maliciosos dirigidos por el atacante, saturan los recursos de comunicación, procesamiento y almacenamiento del controlador SDN, agotando estos recursos y provocando un caos, incluso existiendo redundancia de controladores, estos enfrentaran el mismo problema, por la gran cantidad de paquetes que se deben gestionar.

Estos ataques pueden dirigirse a cualquier de las 3 capas de las redes definidas por software, por lo tanto estos ataques se pueden clasificar en tres categorías según la capa a la que ataquen: Ataques de denegación de Servicio a la Capa de Aplicación, Ataques de Denegación de Servicios a la Capa de Control y Ataques de Denegación de Servicios a la Capa de Control. El objetivo común de estos ataques es lograr saturar la red con una gran

cantidad de paquetes sin importar a que capa sea dirigida el ataque, estos ataques pueden ser ICMP, TCP. Esta inundación de tráfico malicioso busca sobrecargar los recursos de la red y comprometer su funcionamiento normal, Ahuja et al. (2020)

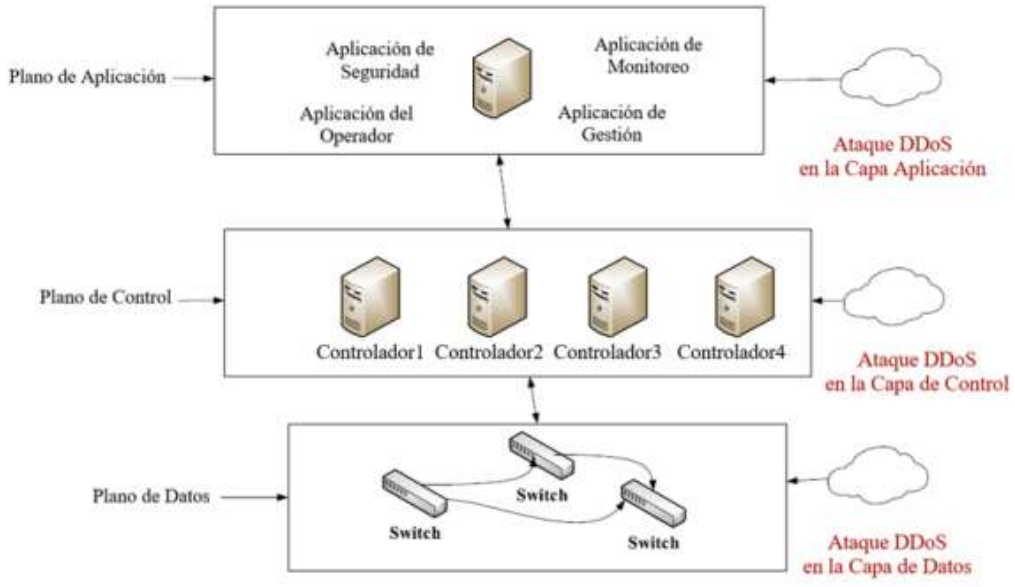

Figura 2: Ataques DoS en SDN.
Elaborado por: Dong et al. (2019)

Vulnerabilidades y Amenazas DoS a la capa de Aplicación SDN.

Según Adil et al. (2024) indica que los ataques de denegación de servicio (DoS) dirigidos a la capa de aplicación de una red definida por software tienen como objetivo principal las aplicaciones y la interfaz de programación de aplicaciones (API) northbound de las redes definidas por software. La separación que se producen entre las diferentes aplicaciones SDN normalmente no es muy clara, por lo que un ataque DoS que está dirigido a una aplicación especifica podría de manera indirecta afectar a otras aplicaciones que no eran el objetivo inicial. Estos ataques establecen conexiones TCP completas con el servidor del objetivo y luego lo inunda con una gran cantidad de solicitudes HTTP, saturando el ancho de banda disponible por el tráfico malicioso que se genera, ya que es

difícil diferenciarlos del tráfico legitimo por su bajo perfil y lenta ejecución. Por lo cual estos ataques a la capa de aplicación se han convertido en herramientas altamente efectivas para que los atacantes causen daños significativos a sus víctimas en la actualidad.

Citando a Ramos, D., (2021) indica varias vulnerabilidades y ataques DoS que podría enfrentar la capa de aplicación en las redes definidas por software:

Vulnerabilidades.

Ofrece interfaces de programación de aplicaciones llamados APIs, las cuales permiten interactuar al controlador con aplicaciones externas.

Es susceptible a ataques de inyección como SQL, XSS, etc., ante una validación errónea de entradas pasadas por los usuarios o bien por parte de las aplicaciones.

Esta capa se convierte en vulnerable a ataques si tiene configuraciones incorrectas o inseguras.

Aparte de que las APIs de la capa de aplicación son unas interfaces fundamentales para la comunicación entre el controlador y las aplicaciones, constituyen un objetivo muy frecuente para ataques de denegación de servicio (DoS).

Amenazas.

Existen ataques DoS que inundan las diferentes APIs con varias solicitudes, consiguiendo abrumar al controlador y por consiguiente haciendo que el servicio sea inaccesible para usuarios legítimos,

Hay ataques que envían datos malformados o excesivos para lograr explotar la falta de validación y así causar desbordamientos que consuman los recursos.

Se producen ataques que explotan las configuraciones incorrectas o inseguras desencadenando condiciones DoS y deshabilitar las medidas de seguridad.

Hay ataques que dirigidos específicamente a las APIs del controlador SDN con el único objetivo de sobrecargarlo y que el controlador deje de responder a las solicitudes que son legítimas.

Vulnerabilidades y Amenazas DoS a la capa de Datos SDN.

El conmutador OpenFlow y su tabla de flujo pueden convertirse en objetivos de un ataque de denegación de servicio (DoS), ya que contienen información crítica relacionada con la administración, el control de acceso y la transmisión de datos. El conmutador OpenFlow posee un almacenamiento limitado y no puede almacenar todas las reglas de flujo necesarias, por lo cual, al enviar una gran cantidad de paquetes desde varias direcciones desconocidas en un corto tiempo, el controlador entenderá que debe crear nuevas reglas para estos paquetes y las agregará a la nueva tabla de flujos. Esto provoca que la tabla se sature rápidamente, quedando sin espacio para registrar nuevas reglas. Como resultado, se interrumpe la transmisión del tráfico legítimo, afectando gravemente el funcionamiento de la red, según Dong et al. (2019).

Según Katz, O. & Black, J. (2022) la memoria caché de flujo también es vulnerable a los ataques de denegación de servicio (DoS). Cuando un conmutador recibe un paquete a través de un puerto de entrada, busca una coincidencia en la tabla de flujo. Si una coincidencia es encontrada, el paquete es reenviado de manera directa desde la memoria cache al puerto de salida que corresponde, pero si no es encontrada ninguna coincidencia este paquete es enviado al controlador, el cual responde con un mensaje que

definirá las reglas de envió de paquetes y los tiempos de activación de estas reglas, el conmutador acusa el recibido, procesa el paquete y almacena las reglas en la memoria cache de la tabla de flujo, la cual servirá para gestionar futuros envíos de paquetes más eficientemente. Al realizarse un ataque DoS se envían una gran cantidad de paquetes por medio de nodos maliciosos, estos paquetes son dirigidos al conmutador y almacenados en la memoria cache, esperando la respuesta del controlador con las reglas de flujo, por lo cual es esta gran cantidad de paquetes maliciosos saturara el búfer del conmutador lo que impedirá que los paquetes legítimos puedan ser procesados y transmitidos, comprometiendo en gran manera el funcionamiento eficiente de la red.

Según Velasquez, M. (2020) destaca ciertas vulnerabilidades que poseen las redes definidas por software ante ataques DoS:

Vulnerabilidades.

OpenFlow es el protocolo estándar utilizado para la comunicación entre el controlador SDN y la capa de datos, por lo cual es susceptible a ataques si no está correctamente implementado o configurado.

Los conmutadores en una red SDN tienen una capacidad limitada en sus tablas de flujo, que es donde se almacenan las reglas de enrutamiento, por lo cual cuando estas tablas se llenan, no pueden procesar nuevos flujos de manera eficiente y esto podría ser explotado maliciosamente.

Los dispositivos en la capa de datos son los responsables de manejar y reenviar paquetes basados en las reglas establecidas por el controlador, por lo cual un volumen excesivo de paquetes, sobre todo si estos no coinciden con ninguna regla predefinida, debe ser procesado y potencialmente reenviado al controlador para su análisis.

Al existir una gestión deficiente de la seguridad y configuraciones erróneas en la capa de datos pueden dejar abiertas vulnerabilidades que facilitan los ataques de DoS.

Amenazas.

Se sobrecarga el conmutador enviando flujos de comandos OpenFlow corruptos, produciendo una denegación de servicio por el agotamiento de los recursos.

Impedimento de que se procese tráfico legitimo por el procesador al saturar las tablas de flujo con entradas inútiles, esto degrada el rendimiento de la red o incluso parando su funcionamiento en su totalidad.

Sobrecargar los conmutadores y el controlador al inundar la red con trafico que requiera procesamiento manual del controlador, esto resulta en la disminución del funcionamiento o hasta que la red pueda fallar completamente.

Existen ataques que interrumpen directamente el flujo de datos, como ataques ARP poisoning, inundación de puertos, y otros métodos que alteran directamente el comportamiento normal de los dispositivos de la capa de datos.

Vulnerabilidades y Amenazas DoS a la capa de Control SDN.

Citando a Dong et al. (2019) el controlador es quien toma las decisiones sobre el envío y reenvió de paquetes basándose en las reglas de flujo, por tal razón al recibir una gran cantidad de tráfico desde varias fuentes, se produce una inundación al controlador y que tiene como resultado la caída de la red, siendo este el principal objetivo de los ataques DoS en la capa de control. El conmutador al detectar un nuevo paquete y este no tiene reglas en la tablas de flujo, es enviado al controlador, quien toma la desecion Cuando un conmutador en el plano de datos detecta un nuevo paquete y no encuentra una regla existente en la tabla de flujo que corresponda con la información de dicho paquete, se

envía al controlador todo el paquete o una parte de su encabezado para que tome una decisión, adicional si esto se realiza cuando existe un tráfico de red elevado puede llevar a consumir una gran cantidad de ancho de banda.

Lo primero en verificar es que la red donde se va a realizar el ataque sea SDN, ya que, a diferencia de las redes tradicionales, donde las tablas de reenvío ya están preconfiguradas y no se necesita tiempo adicional para para procesar nuevos paquetes, mientras que en las redes SDN el controlador genera una nueva entrada de flujo para cada paquete entrante, añadiendo tiempo extra al primer paquete comparado con los siguientes. Al conocer esto los atacantes usan herramientas de escaneo para detectar variaciones en los tiempos de respuestas entre el primer y los siguientes paquetes, Ahuja et al. (2020).

Como opina Mantilla et al. (2022) existen varios ataques que son realizados hacia vulnerabilidades específicas de la capa de control:

Vulnerabilidades.

Los controladores SDN son el cerebro de la red, por lo cual tienen una capacidad limitada de procesamiento y memoria, entonces un volumen excesivo de solicitudes o comandos, puede sobrecargar rápidamente estos recursos.

La interfaz norte del controlador SDN es la que permite la comunicación con las aplicaciones de red y con los servicios de alto nivel, por lo cual si esta interfaz no está protegida adecuadamente podría ser un punto vulnerable para ataques.

El realizar una implementación deficiente de mecanismos de autenticación y validación de solicitudes en el controlador puede permitir que entidades no autorizadas accedan y manipulen la configuración de la red.

La comunicación entre el controlador y los dispositivos de red se produce a través de la interfaz sur, si no posee un cifrado o protocolos de seguridad robustos en estas comunicaciones podría ocurrir intercepción o manipulación de los datos.

Amenazas.

Un ataque puede inundar el controlador con peticiones falsas o innecesarias, agotando los recursos computacionales y causando retrasos o fallos en el procesamiento de comandos legítimos.

Un ataque con tráfico malicioso dirigido a la interfaz norte podría desbordar al controlador, interrumpiendo su operatividad.

Se puede insertar reglas maliciosas que podrían bloquear o redirigir el tráfico legítimo, que producirían alteraciones en el comportamiento de la red.

Es posible introducir comandos para interceptar o alterar las instrucciones que se envían a los diferentes dispositivos de la red, llevando a un agotamiento de la red.

Estrategias de Detección y Mitigación de ataques DoS en la capa de Aplicación SDN

Citando a Albarracín-Estrada et al. (2022) recomienda aplicar ciertas estrategias de detección y de mitigación sobre ataques que pueda enfrentar la capa de aplicación en redes definidas por software:

Una importante estrategia de detección es implementar sistemas de monitoreo que logren detectar anomalías en las tasas de tráfico hacia las APIs para así identificar posibles ataques de inundación, y para lograr mitigar estos ataques también se puede utilizar firewalls de aplicación web (WAF) y Gateway para APIs y lograr limitar las solicitudes y con esto protegerse contra ataques de inundación.

Una estrategia importante para lograr detectar ataques DoS es el usar herramientas de detección de intrusos (IDS) para lograr identificar ataques de inyección de datos maliciosos, además para lograr contrarrestar estos ataques también es importante asegurar una validación estricta en todos los puntos de entrada y así lograr rechazar datos malformados y excesivos que pueden causar daño a los recursos.

Una estrategia importante para detectar ataques es realizar auditorias de configuración y cumplimiento de seguridad de manera regular y con esto lograr identificar configuraciones incorrectas o inseguras, y una estrategia para lograr mitigar ciertos tipos de ataques es lograr establecer procesos de gestión de configuración segura, incluyendo revisiones automáticas y pruebas de penetración.

Una estrategia que logra detectar ataques en las APIs es utilizar herramientas de análisis de tráfico para lograr detectar patrones anormales de solicitud a la API y poder reconocer un ataque, mientras que una estrategia para evitar estos ataques es implementar Gateway de APIs para limitar la tasa de solicitudes y lograr verificar la autenticidad e integridad de todas las solicitudes de APIs que lleguen al controlador.

Estrategias de Detección y Mitigación de ataques DoS en la capa de Datos SDN.

Desde el punto de vista de Manso et al. (2019) existen varias estrategias que pueden detectar y contrarrestar ataque que pueden ir dirigido a la capa de datos:

Implementar sistemas de detección de anomalías que monitoreen los mensajes OpenFlow en busca de patrones inusuales; mientras que una estrategia para mitigar estos ataques es aplicar cifrado y autenticación en todas las comunicaciones OpenFlow asegurando la integridad de los datos.

Otra estrategia de detección es monitorear la tabla de flujo en los dispositivos SDN, lo cual permite detectar rápidamente cuando se acerque a su capacidad máxima; y para lograr contrarrestar ataques a la tabla de flujo es importante implementar políticas de limpieza automática y gestión dinámica para optimizar el uso de espacio libre en las tablas de flujo.

Una estrategia para detectar ataques de inundación de paquetes es usar técnicas de análisis de tráfico que detecten incrementos abruptos en el volumen de paquetes: y para lograr mitigar estos ataques puede configurarse mecanismos de limitación de tasa de datos en los conmutadores SDN y lograr controlar el número de paquetes enviados al controlador.

Una estrategia muy importante para detectar ataques por una posible seguridad inadecuada de las SDN es realizar auditorías de seguridad regulares y escaneos de vulnerabilidad para identificar estas configuraciones inadecuadas; mientras que para que estos ataques no sucedan podría desarrollarse políticas de seguridad estrictas, asegurando su cumplimiento mediante herramientas automatizadas.

Estrategias de Detección y Mitigación de ataques DoS en la capa de Control SDN.

Como señala Gómez, S. (2020) resalta la importancia de aplicar estrategias de detección y mitigación para los ataques DoS en la capa de control en las redes definidas por software:

Una estrategia importante para detectar amenazas es implementar monitoreo de rendimiento en tiempo real, para la detección de aumentos anormales en la carga de trabajo; además una estrategia de mitigación es implementar técnicas de balanceo de carga y controladores distribuidos.

Una estrategia para detectar ataques a la interfaz norte es analizar y filtrar el tráfico desde y hacia esta interfaz para lograr identificar patrones de tráficos sospechosos; además también es posible contrarrestar estos ataques reforzando la seguridad de la interfaz con autenticaciones robustas y cifrado en la comunicación.

El implementar soluciones de análisis de comportamiento para identificar actividades no autorizadas es una estrategia eficiente para la detección de ataques; mientras que reforzar los mecanismos de autenticación y validación en todas las interfases del controlador.

Una estrategia para detectar ataques a las comunicaciones dentro de la capa de control realizar intercepciones en el tráfico para inspeccionar y validar los mensajes entre el controlador y los dispositivos; además el asegurar todas las comunicaciones utilizando protocolos de cifrado permitirá contrarrestar ataques.

MARCO METODOLOGICO

El presente trabajo tiene un enfoque correlacional, ya que analiza fundamentalmente la relación existente entre las vulnerabilidades de las redes definidas por software (SDN) y los ataques de denegación de servicios (DoS) en materia de seguridad. El enfoque de este estudio permite describir y sustentar en su complejidad los diferentes patrones de correlación obtenidos, ofreciendo un análisis detallado del conjunto de variables que determinan los varios factores que pueden estar influyendo en los ataques a las vulnerabilidades de las redes SDN.

Alcance de la Investigación

Su alcance descriptivo permite clasificar, recopilar y presentar información que se obtengan de diversas fuentes relevantes como sitios web, libros, revistas y otros materiales, esto permitirá conocer las principales vulnerabilidades que posee la red SDN y las amenazas que puedan existir en base a estas deficiencias, además de revisar la efectividad de las estrategias de detección y mitigación que se podrían implementar para contrarrestar estas amenazas.

Técnicas e Instrumentos de Recolección de Datos

Se utilizarán técnicas como:

- Revisión documental: Análisis de documentación técnica, artículos científicos y estudios previos sobre ataques de denegación de servicio (DoS) a las redes definidas por software (SDN).

Diseño de la Investigación

Este estudio esta desarrollado bajo un diseño no experimental, al no manipular variables de manera directa, más se analizarán en un contexto natural, permitiendo

establecer la relación entre los ataques DoS y la efectividad de las estrategias de seguridad sugeridas para las redes SDN.

También es importante indicar que el estudio se categoriza longitudinal, ya que la recolección de los datos será realizada en un periodo de tiempo específico.

RESULTADOS

Se determino en base a la bibliografía estudiar las vulnerabilidades que poseen cada una de las capas que tienen las redes definidas por software como lo son la capa de aplicación, la capa de datos y la capa de control, encontrando varias vulnerabilidades en cada una de estas capas y de la misma manera varios ataques que se podrían realizar usando como referencia estas debilidades de las redes definidas por software.

Como resultados se encontraron vulnerabilidades en cada una de las capas de las SDN como interfaces expuestos, validación de entradas deficientes, errores de configuración y riesgos de DoS a las APIs en la capa de aplicación, también vulnerabilidades en el protocolo OpenFlow, tablas de flujos limitadas, inundación de paquetes y gestión de la seguridad inadecuada en la capa de datos, y en la capa de control se encontraron debilidades como la capacidad limitada del procesamiento, una interfaz norte expuesta, falta de autenticación y validación por parte del controlador, y comunicaciones no seguras entre el controlador y los dispositivos de la red definida por software.

En base a estas vulnerabilidades encontradas en cada una de las capas se realizó un análisis para determinar que ataques podrían realizarse y como afectarían a cada capa, encontrando diversos ataques DoS que afectarían de manera critica a las redes definidas por software, como ataques de inundación HTTP, ataques de exceso de conexiones a las APIs, ataques de inyección que provocan colapsos en el servicio, ataques a las configuraciones de la SDN, y ataques de inundación específicos a las APIs en la capa de aplicación.

En la capa de datos también se encontraron ataques que afectarían a las redes SDN como ataques de envió de flujos de comandos OpenFlow corruptos, ataques DoS para

saturar las tablas de flujos, ataques de inundación al tráfico para sobrecargar los conmutadores y ataques ARP poisoning para la interrupción del flujo de datos.

Además, existen ataques como inundación al controlador, ataques a la interfaz norte para desbordar el controlador, ataques de alteración al comportamiento de la red causando bloqueo en el tráfico legítimo y ataques de intercepción que alteran las instrucciones enviadas a los dispositivos produciendo un agotamiento en los recursos.

Adicionalmente, se lleva a cabo un análisis de diversas estrategias diseñadas para detectar y mitigar estos tipos de ataques. Este análisis se fundamenta en la identificación y explotación de las vulnerabilidades presentes en las redes definidas por software y mencionadas en este estudio.

DISCUSION DE RESULTADOS

Se expone los resultados por medio de tablas que describen las vulnerabilidades y amenazas que afectan a cada una de las capas de las redes definidas por software, adicionalmente se sugieren estrategias que pueden detectar y mitigar estas amenazas.

CAPA	VULNERABILIDAD	AMENAZAS (ATAQUES)	DETECCION	MITIGACION
CAPA DE APLICACIÓN	Interfaces Expuestas	Ataques de inundación HTTP, Ataques de exceso de conexiones simultaneas a las APIs	Implementar un sistema de gestión de seguridad de la información (SIEM) que centralice los registros y alertas de todas las API expuestas.	Establecer un proxy de API que actúe como intermediario entre los usuarios y el controlador SDN.
	Validación de Entrada Deficiente	Ataques de inyección que envían grandes cantidades de datos maliciosos para provocar un colapso o cierre de servicios.	Configurar sistemas de detección de intrusos (IDS) para identificar y alertar sobre patrones de inyección conocidos o anomalías en las cargas de las solicitudes hacia el controlador.	Aplicar una rigurosa validación de todas las entradas en el controlador SDN utilizando listas blancas (permitiendo solo tipos de datos específicos), desinfección de entradas, y validación de longitud y formato.
	Errores de Configuración	Ataques que explotan configuraciones de red mal configuradas para sobrecargar el controlador o los dispositivos de red.	Utilizar herramientas de automatización de configuración como Chef o Ansible para realizar auditorías continuas de la configuración.	Desarrollar scripts que se ejecuten periódicamente para revisar las configuraciones de todos los dispositivos SDN en busca de configuraciones inseguras.
	Riesgo de DoS a la API	Ataques de inundación específicos a la API que utilizan técnicas como inundaciones SYN o Peticiones GET/POST masivas.	Configurar un IDS para monitorear específicamente el tráfico de la API.	Utilizar un API Gateway como Kong o Amazon API Gateway que incluya capacidades de limitación de tasa (rate limiting).
				Implementar cachés para las respuestas de las APIs más frecuentemente y reducir la carga en el controlador SDN durante picos de demanda o ataques DoS.

Tabla 3: Resultados en la capa de aplicación.
Elaborado por: Nixon Tierra.

La tabla que se muestra anteriormente resume de manera eficaz las vulnerabilidades clave, las amenazas asociadas y las estrategias de detección y mitigación

para la capa de aplicación en redes definidas por software, ya que, al centralizar la gestión del control de la red, exponen puntos críticos que pueden ser explotados a través de diversas vulnerabilidades. Las amenazas que se identificaron como los ataques de inundación HTTP, los ataques de exceso de conexiones simultaneas a las APIs, inyecciones de datos maliciosos y la explotación de configuraciones que están mal configuradas pueden dañar la red seriamente sobre todo su funcionalidad y el rendimiento, estos ataques generalmente sobrecargan al controlador hasta llegar a la interrupción total del servicio.

Se proponen estrategias de detección y mitigación para la prevención y respuesta a los ataques enviados, estrategias como implementar sistemas de monitoreo SIEM o IDS para la detección de anomalías y vigilancia continua del tráfico, el uso de herramientas de automatización para gestionar las configuraciones y mantener la red en estado seguro, previniendo explotaciones de configuración a través de las vulnerabilidades de configuración. También es importante mencionar el uso de gestores de llamadas (APIs Gateway) para limitar y controlar el acceso a las APIs, e implementar técnicas de balanceo de carga y caching para las APIs con más demandas, estas estrategias mitigan los ataques DoS y aseguran que el controlador pueda manejar eficientemente las solicitudes legitimas, incluso durante condiciones de alta carga.

CAPA	VULNERABILIDAD	AMENAZAS (ATAQUES)	DETECCION	MITIGACION
Capa de Datos	Vulnerabilidad de Protocolo OpenFlow	Ataques de envíos de flujos de comandos OpenFlow corruptos para sobrecargar el conmutador.	Utilizar herramientas como Flowmon para detectar anomalías en tiempo real en los flujos OpenFlow para detectar patrones de tráfico inusual.	Implementar TLS en las conexiones OpenFlow entre el controlador y los dispositivos para proteger la red de la manipulación de datos.

	Tabla de Flujo Limitada	Ataques DoS que saturen las tablas de flujo con entradas inútiles para impedir al conmutador procesar tráfico legitimo.	Configurar alarmas en el sistema de gestión de red, como PRTG Network Monitor para crear alertas cuando el uso de la tabla de flujo exceda un umbral especifico.	Uso de algoritmos de expiración de flujos en el controlador SDN que periódicamente revisa y elimina entradas de flujo que no se han utilizado recientemente.
	Inundación de Paquetes	Ataques que inundan la red con tráfico que requiere procesamiento manual por parte del controlador, sobrecargando tanto los conmutadores incluso al propio controlador.	Integración de herramientas de análisis de tráfico como Wireshark para monitorizar y alertar sobre aumentos significativos en el tráfico de red que son indicativos de una inundación de paquetes.	Establecimiento de límites de tasa en Cisco IOS con políticas de control de tráfico que limiten la cantidad de paquetes por segundo dirigidos hacia el controlador.
	Configuración y Gestión de Seguridad Inadecuada	Ataques que interrumpan directamente el flujo de datos, como ataques ARP poisoning e inundación de puertos.	Empleo de herramientas como Nessus y OpenVAS para llevar a cabo auditorías automáticas de la configuración de red, y localizar las configuraciones inseguras.	Implementación de Ansible para desplegar y verificar las configuraciones de seguridad de todos los dispositivos SDN, asegurando la validación con las políticas de configuración de seguridad existentes.

Tabla 4: Resultados en la capa de datos. Elaborado Nixon Tierra.

Se expone un análisis exhaustivo de las vulnerabilidades que ofrece la capa de datos de las redes SDN, pudiendo identificar las amenazas que pueden afectar a cada una de las vulnerabilidades existentes, y las posibles formas para su detección y mitigación.

Las redes definidas por software están propensas a los ataques DoS, estas pueden comprometer la funcionalidad y seguridad de la red muy severamente, estas vulnerabilidades que se presentan en la capa de datos, como las limitación de los protocolos OpenFlow, la sobrecarga de las tablas de flujo, la inundación de paquetes y la inadecuada configuración de seguridad, producen en la red interrupciones y perdidas de datos, por este motivo las estrategias de detección y mitigación como el monitoreo en tiempo real, la gestión automática de configuraciones y el fortalecer las comunicaciones entre dispositivos, son importantes para contrarrestar los anteriores ataques mencionados.

Implementar estas medidas protege a la red contra interrupciones del servicio, asegurando el rendimiento óptimo y la escalabilidad de la infraestructura SDN, manteniendo así la integridad y la eficiencia operativa de la red.

CAPA	VULNERABILIDAD	AMENAZAS (ATAQUES)	ESTRATEGIAS	
			DETECCION	MITIGACION
Capa de Control	Capacidad Limitada de Procesamiento	Un ataque puede inundar el controlador con peticiones falsas o innecesarias, agotando los recursos computacionales y causando retrasos o fallos en el procesamiento de comandos legítimos.	Uso de herramientas de monitoreo como Zabbix o Nagios que pueden configurarse para alertar cuando los recursos de CPU o memoria del controlador superan umbrales críticos, indicando potencial actividad de DoS.	Implementación de un clúster de controladores SDN que distribuya la carga entre múltiples nodos, usando soluciones como OpenDaylight u ONOS que soportan configuraciones de alta disponibilidad y escalabilidad.
	Interfaz Norte Expuesta	Ataques dirigidos a la interfaz norte para desbordar el controlador con tráfico malicioso o solicitudes de configuración alteradas, interrumpiendo la operatividad de las aplicaciones de red.	Configurar un IDS como Snort, que pueda personalizarse para monitorizar específicamente la interfaz norte y detectar cualquier tráfico anómalo o malicioso.	Aplicar tecnologías como TLS para cifrar la comunicación entre el controlador y las aplicaciones externas, y uso de OAuth para gestionar las autorizaciones de manera segura.
	Falta de Autenticación y Validación en el Controlador	Se pueden producir ataques que alteren el comportamiento de la red, insertando reglas maliciosas que pueden redirigir o bloquear el tráfico legítimo.	Uso de soluciones avanzadas de seguridad cibernética que empleen IA para detectar cambios inusuales en la configuración de la red que no correspondan con el patrón habitual de uso.	Implementación de autenticación multifactorial y controles de acceso basados en roles utilizando soluciones de gestión de identidades como Keycloak o FreeIPA.
	Comunicaciones No Seguras entre Controlador y Dispositivos de Red	Un ataque puede interceptar o alterar las instrucciones enviadas a los dispositivos de red, al introducir comandos que podrían llevar a un mal funcionamiento de la red o incluso a un agotamiento de los recursos.	Instalar gateways de inspección de paquetes para verificar la autenticidad de mensajes OpenFlow.	Implementar un IPSec o un SSL/TLS para lograr cifrar el tráfico que existe entre el controlador y los dispositivos de red.

Tabla 5: Resultados en la capa de control.
Elaborado por: Nixon Tierra.

Se muestran las vulnerabilidades en la capa de control de las redes SDN, conjuntamente con las amenazas y las estrategias para su detección y mitigación. Estas vulnerabilidades, si no se abordan adecuadamente, pueden comprometer la integridad, seguridad y rendimiento de toda la red. Las amenazas como la sobrecarga del controlador por peticiones falsas, el desbordamiento de la interfaz norte, la manipulación de la autenticación y la interceptación de las comunicaciones pueden llevar a interrupciones significativas, pérdida de control sobre la red y potencialmente un colapso total del sistema.

Las amenazas pueden debilitar muy gravemente las redes SDN, afectando directamente a su núcleo de operaciones que es el controlador, una sobrecarga a este recurso podría ralentizar el procesamiento de los comandos legítimos, esto afecta la capacidad de la red para responder a las necesidades operativas. Los ataques a la interfaz norte interrumpen la operatividad de la red que dependen del controlador para la gestión del tráfico. Los ataques dirigidos a la interfaz norte pueden interrumpir la operatividad de las aplicaciones de red que dependen del controlador para la gestión del tráfico y la configuración de la red. La falta de autenticación y validación adecuada puede permitir la inserción de reglas de tráfico maliciosas, comprometiendo la seguridad de los datos y el funcionamiento de la red y las comunicaciones no seguras entre el controlador y los dispositivos de red pueden ser explotadas para interceptar o alterar instrucciones críticas, poniendo en riesgo toda la infraestructura de la red.

Por lo cual las estrategias de detección y mitigación propuestas son esenciales para contrarrestar estos riesgos. La utilización de herramientas de monitorización de red como: Zabbix o Nagios, sistemas de detección de intrusiones como Snort, puede ser clave para la detección y respuesta antes las actividades sospechosas o maliciosas antes de que puedan cause estragos. La implementación de soluciones avanzadas de seguridad

ciberseguridad, como la autenticación multifactorial y el cifrado de comunicaciones, fortalece la seguridad en los puntos críticos, asegurando que solo las entidades verificadas puedan acceder y operar dentro de la red. La adopción de estas medidas, combinada con una gestión rigurosa y la implementación de políticas de seguridad, es crucial para asegurar que las redes SDN funcionen de manera óptima y segura, manteniendo la integridad, disponibilidad y eficiencia del servicio de red.

CONCLUSIONES.

Se identificaron varios tipos de ataques DoS que aprovechan las vulnerabilidades de las redes SDN, como la saturación del controlador SDN, ataques dirigidos a la interfaz norte y la explotación de debilidades en la autenticación y validación de solicitudes.

Se exponen las vulnerabilidades que tiene cada capa de las SDN, observando como aquellas se pueden ver comprometidas por un atacante en cuanto a debilitar la red, es decir, configuraciones inseguras, debilidades en la gestión de la tabla de flujo, interfases críticas expuestas, etc.

La propuesta de estrategias de detección y mitigación para cada tipo de vulnerabilidad como la implementación de IDS, el uso de tecnologías de balanceo de carga y controladores distribuidos y el fortalecimiento de los protocolos de autenticación.

El documento también permite una mayor comprensión de cómo pueden utilizarse las vulnerabilidades de las redes SDN para debilitar una red a raíz de los ataques DoS, en particular la implementación de soluciones de seguridad de múltiples capas y configuraciones que protejan estas infraestructuras críticas. La centralización del control de las redes SDN implica a su vez eficiencia y flexibilidad.

RECOMENDACIONES.

Se recomienda la implementación de un programa de formación continua para el personal de TI con un enfoque en las nuevas tendencias en los Ataques de Redes Definidas por Software, así como en las tácticas de mitigación adecuadas para tal tipo de ataque. Esto incluye talleres regulares y simulacros de ataque para preparar al equipo para responder de manera rapida.

Se recomienda hacer auditorías de seguridad y análisis de vulnerabilidad periódicos, con las herramientas correspondientes, específicas para las Redes Definidas por Software, que puedan detectar configuraciones inseguras y vulnerabilidades explotables de las correspondientes configuraciones.

Se aconseja establecerá un marco de políticas de seguridad específico para SDN que incluya directrices claras sobre la configuración de seguridad, gestión de cambios, y respuestas a incidentes. Así mismo, adoptar soluciones tecnológicas como firewalls de nuevas generación y sistemas de prevención de intrusiones (IPS) apropiados para implementados de las arquitecturas SDN.

Que exista una colaboración permanente con los desarrolladores de plataformas SDN, investigadores en seguridad y los organismos de estándares como manera ir mejorando las capacidades de detección y mitigación de ataques de denegaciones de servicios en las Redes Definidas por Software. Fomentar la adopción de estándares de seguridad abiertos y el intercambio de información sobre amenazas para fortalecer colectivamente la resiliencia de las Redes Definidas por Software frente a los ataques cibernéticos.

REFERENCIAS

Amaya Fariño, L. M., Arroyo Pizarro, J. F., Jaramillo Infante, M., Tumbaco Reyes, A., & Mendoza Morán, B. (2022). SDN Redes Definidas por Software usando MiniNet. Revista Científica y Tecnológica UPSE, 9(1). https://doi.org/10.26423/rctu.v9i1.489

Ruipérez Cuesta, J. (2021). Seguridad en Redes definidas por software (SDN) (Trabajo Final de Grado, Universitat Politècnica de València). Escuela Técnica Superior de Ingeniería de Telecomunicación. https://www.etsit.upv.es

Becci, G., Morandi, M., & Marrone, L. A. (2019). Seguridad en la virtualización de redes definidas por software: revisión por dimensión a virtualizar. En 48 Jornadas Argentinas de Informática e Investigación Operativa (JAIIO). Universidad Nacional de La Plata. https://sedici.unlp.edu.ar/handle/10915/88673

Huawei (2024). ¿Qué es OpenFlow? - Conceptos Básicos | programabilidad. https://forum.huawei.com/enterprise/intl/es/thread/%C2%BFQu%C3%A9-es-OpenFlow-Conceptos-B%C3%A1sicos-Programabilidad/748398411205459968?blogId=748398411205459968

Roncero Hervás, O. (2020). Software Defined Networking (Trabajo Final de Grado, UNIVERSITAT POLITÈCNICA DE CATALUNYA). Master en Ingeniería de Telemática. https://upcommons.upc.edu/bitstream/handle/2099.1/21633/Memoria.pdf

Acosta González, O. S., & Ortega Avila, E. A. (2023). Análisis sistemático de modelos de seguridad y control de acceso en arquitectura SDN para la detección de anomalías (Trabajo de titulación, Universidad Politécnica Salesiana). Sede Guayaquil. Carrera de Computación.

Becci, G., Morandi, M., & Marrone, L. A. (2020). Diseño de sistemas de detección de intrusión en redes definidas por software: revisión basada en machine learning. En 49 Jornadas Argentinas de Informática e Investigación Operativa (JAIIO). Universidad Nacional de La Plata. https://sedici.unlp.edu.ar/handle/10915/121984

Mishra, P., Varadharajan, V., Tupakula, U., & Pilli, E. S. (2019). A detailed investigation and analysis of using machine learning techniques for intrusion detection. IEEE Communications Surveys & Tutorials, 21(1), 686-728. https://doi.org/10.1109/COMST.2018.2847722

Gu, Y., Li, K., Guo, Z., & Wang, Y. (2019). Semi-supervised K-means DDoS detection method using hybrid feature selection algorithm. IEEE Access, 7, 64351-64365. https://doi.org/10.1109/ACCESS.2019.2917532

Nanda, S., Zafari, F., DeCusatis, C., Wedaa, E., & Yang, B. (2020). Predicting network attack patterns in SDN using machine learning approach. In 2016 IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN) (pp. 167-172). https://doi.org/10.1109/NFV-SDN.2016.7919493

Bhuiyan, Z. A., Islam, S., Islam, M. M., Ullah, A. B. M. A., Naz, F., & Rahman, M. S. (2023). On the (in)Security of the Control Plane of SDN Architecture: A Survey. IEEE Access, 11. https://doi.org/10.1109/ACCESS.2023.3307467

Mycek, M., Pióro, M., Tomaszewski, A., & de Sousa, A. (2021). Optimizing primary and backup SDN controllers' placement resilient to node-targeted attacks. En 2021 17th International Conference on Network and Service Management (CNSM) (pp. 397-401). Izmir, Turkey. https://doi.org/10.23919/CNSM52442.2021.9615578

Báez Cheza, J. E. (2021). Metodología de detección y mitigación de ataques DDoS en entornos SDN basado en la norma ISO/IEC 27001 para mejorar la seguridad en

el plano de control (Trabajo de investigación de maestría, Universidad Técnica del Norte). Instituto de Postgrado, Maestría en Telecomunicaciones.

Dong, S., Abbas, K., & Jain, R. (2019). A Survey on Distributed Denial of Service (DDoS) Attacks in SDN and Cloud Computing Environments. IEEE Access, 7, 80813–80828. https://doi.org/10.1109/ACCESS.2019.2922196

Tamayo Portero, J. O. (2023). Detección de ataques de denegación de servicio activados mediante botnets en redes definidas por software. Trabajo de titulación previo a la obtención del grado de Magíster en Software con mención en Seguridad, Escuela Politécnica Nacional, Facultad de Sistemas, Unidad de Titulación. https://bibdigital.epn.edu.ec/bitstream/15000/24870/1/CD%2013552.pdf

Manso, P., Moura, J., & Serrão, C. (2019). SDN-based intrusion detection system for early detection and mitigation of DDoS attacks. Inf., 10(3), 1-17. https://doi.org/10.3390/info10030106

Katz, O., & Black, J. (2022, junio). *Akamai DNS Traffic Insights Threat Report*. Akamai DNS Traffic Threat Report. Recuperado de https://www.akamai.com/resources/research-paper/akamai-dns-traffic-insights-threat-report

Deb, R., & Roy, S. (2022). A comprehensive survey of vulnerability and information security in SDN. Computer Networks, 206. https://doi.org/10.1016/j.comnet.2022.108802

Correa, J., Imbachi, J., & Botero, J. (2020). Security in SDN: A comprehensive survey. Journal of Network and Computer Applications, 159. https://doi.org/10.1016/j.jnca.2020.102595

Ahuja, N., Singal, G., & Mukhopadhyay, D. (2020). DDOS attack SDN dataset. Journal of Physicochemical Problems of Mineral Processing, 1. https://doi.org/10.17362/JXPFCJ64KR.1

Kumar, M., & Bhandari, A. (2023). DDoS detection in ONOS SDN controller using Snort. En J. Choudrie, P. Mahalle, T. Perumal, & A. Joshi (Eds.), ICT with intelligent applications (pp. 155-164). Springer Nature Singapore.

Saurabh, K., Kumar, T., Singh, U., Vyas, O. P., & Khondoker, R. (2022). NFDLM: A lightweight network flow based deep learning model for DDoS attack detection in IoT domains. En 2022 IEEE World AI IoT Congress (AIIoT 2022) (pp. 736-742). https://doi.org/10.1109/AIIoT54504.2022.9817297

Adil, M., Midha, S., Srivastav, V. K., & Kavita. (2024). Detection and prevention of DoS attack in VANET using artificial neural network. En 2024 IEEE 1st Karachi Section Humanitarian Technology Conference (KHI-HTC) (pp. 1-7).

Albarracín-Estrada, A., Soto-Duran, D. E., Gil-Herrera, J., & Vargas-Agudelo, F. A. (2022). Análisis de ataques DoS en redes de datos basadas en hardware y software. Revista Ibérica de Sistemas e Tecnologias de Informação, (E47), 262-275.

Ramos Suavita, D. J. (2021). Análisis de vulnerabilidades a nivel de seguridad en redes SDN para los planos de control y plano de datos. Trabajo de grado, Ingeniería en Telecomunicaciones, Universidad Militar Nueva Granada, Facultad de Ingeniería, Bogotá, D.C., Colombia.