UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE INGENIERÍA EN SISTEMAS, ELECTRÓNICA E INDUSTRIAL

MAESTRÍA EN TELECOMUNICACIONES

TEMA: DESPLIEGUE DE UN HONEYNET BASADO EN REDES DEFINIDAS POR SOFTWARE PARA UN ISP

Trabajo de Titulación previo a la obtención del Grado Académico de Magister en Telecomunicaciones.

Modalidad de titulación “Proyecto de Desarrollo”

Autor: Ing. Rubén Edison Terán Moreano, Mg.

Director: Ing. Víctor Santiago Manzano Villafuerte, Mg.

Ambato-Ecuador

2021

APROBACIÓN DEL TRABAJO DE TITULACIÓN

A la Unidad de Titulación de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial.

El Tribunal receptor de la Defensa del Trabajo de Titulación presidido por la Ingeniera Elsa Pilar Urrutia Urrutia Magíster, e integrado por los señores: Ingeniero Dennis Vinicio Chicaiza Castillo Magíster, e Ingeniero Juan Pablo Pallo Noroña Magister, designados por el Unidad Académica de Titulación de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial de la Universidad Técnica de Ambato, para receptar el Trabajo de Titulación con el tema: "DESPLIEGUE DE UN HONEYNET BASADO EN REDES DEFINIDAS POR SOFTWARE PARA UN ISP", elaborado y presentado por el señor, Ingeniero Rubén Edison Terán Moreano Magíster, para optar por el Grado Académico de Magister en Telecomunicaciones; una vez escuchada la defensa oral del Trabajo de Titulación el Tribunal aprueba y remite el trabajo para uso y custodia en las bibliotecas de la Universidad Técnica de Ambato.

Firmado electrónicamente por:
ELSA PILAR URRUTIA

Ing. Elsa Pilar Urrutia Urrutia Mg.

Presidente y Miembro del Tribunal de Defensa

Firmado electrónicamente por:
DENNIS VINICIO CHICAIZA CASTILLO

Ing. Dennis Vinicio Chicaiza Castillo, Mg.

Miembro del Tribunal de Defensa

Firmado electrónicamente por:
JUAN PABLO PALLO NORONA

Ing. Juan Pablo Pallo Noroña, Mg.

Miembro del Tribunal de Defensa

AUTORÍA DEL TRABAJO DE TITULACIÓN

La responsabilidad de las opiniones, comentarios y críticas emitidas en el Trabajo de Titulación presentado con el tema: "DESPLIEGUE DE UN HONEYNET BASADO EN REDES DEFINIDAS POR SOFTWARE PARA UN ISP", le corresponde exclusivamente a: Ingeniero Rubén Edison Terán Moreano, Autor bajo la Dirección del Ingeniero Víctor Santiago Manzano Villafuerte, Magister, director del Trabajo de Titulación; y el patrimonio intelectual a la Universidad Técnica de Ambato.

Firmado electrónicamente por:
RUBEN EDISON TERAN MOREANO

Ingeniero Rubén Edison Terán Moreano, Magister.

AUTOR

Firmado electrónicamente por:
VICTOR SANTIAGO MANZANO VILLAFUERTE

Ingeniero Víctor Santiago Manzano Villafuerte, Magister.

DIRECTOR

DERECHOS DE AUTOR

Autorizo a la Universidad Técnica de Ambato, para que el Trabajo de Titulación, sirva como un documento disponible para su lectura, consulta y procesos de investigación, según las normas de la Institución.

Cedo los Derechos de mi Trabajo de Titulación, con fines de difusión pública, además apruebo la reproducción de este, dentro de las regulaciones de la Universidad Técnica de Ambato.

Firmado electrónicamente por:
RUBEN EDISON TERAN MOREANO

Ingeniero Rubén Edison Terán Moreano
C.C. 0502074040

ÍNDICE GENERAL

CONTENIDO

PORTADA I

APROBACIÓN DEL TRABAJO DE TITULACIÓN II

AUTORÍA DEL TRABAJO DE TITULACIÓN III

DERECHOS DE AUTOR IV

ÍNDICE GENERAL V

ÍNDICE DE FIGURAS VIII

DEDICATORIA IX

AGRADECIMIENTOS X

RESUMEN EJECUTIVO XI

EXECUTIVE SUMMARY XIII

CAPÍTULO I 1

1.1. INTRODUCCIÓN 1
1.2. JUSTIFICACIÓN 2
1.3. OBJETIVOS 2
1.3.1. General *2*
1.3.2. Específicos *2*

CAPITULO II 3

2.1. ESTADO DEL ARTE 3
2.2. MARCO TEÓRICO 5
2.2.1. Proveedor de servicios de internet (ISP) *5*
2.2.2. Redes definidas por software (SDN) *8*
2.2.3. Funcionamiento de SDN *15*
2.2.4. OpenFlow *15*
2.2.5. Puertos OpenFlow *16*
2.2.6. Componentes de un switch OpenFlow *17*
2.2.7. Controlador SDN *17*
2.2.8. Sistema trampa o señuelo honeypot *23*
2.2.9. Tipos de honeypot *23*
2.2.10. Red trampa o honeynet *24*

CAPITULO III 26

3.1. METODOLOGÍA 26
3.2. UBICACIÓN 26
3.3. EQUIPOS Y MATERIALES 26
3.4. TIPO DE INVESTIGACIÓN 27
3.4.1. Investigación Bibliográfica *27*
3.4.2. Investigación Exploratoria *27*
3.5. PRUEBA DE HIPÓTESIS 27
3.6. POBLACIÓN Y MUESTRA 28

CAPÍTULO IV 29

4.1. DETERMINACIÓN DE SITUACIÓN ACTUAL DE LA INFRAESTRUCTURA DE LA RED DE LA EMPRESA CLICKNET S.A. 29
4.2. ESQUEMA DE IMPLEMENTACIÓN DE LA RED SDN PARA LA EMPRESA CLICKNET 32
4.3. SELECCIÓN DEL CONTROLADOR SDN 34

4.4. IMPLEMENTACIÓN DE LA RED SDN EN UN BANCO DE PRUEBAS. 37
4.5. IMPLEMENTACIÓN DE RED SDN DE LA EMPRESA EN PRODUCCIÓN 42
4.6. IMPLEMENTACIÓN DE HONEYNET EN RED SDN ESTABLECIDA 44
4.7. ANÁLISIS DEL FUNCIONAMIENTO 50
4.7.1 Resultados de implementación de red SDN *50*
4.7.2 Resultados de implementación Honeynet *57*
4.7.3 Incidentes y soluciones *64*
CAPITULO V **67**
5.1. CONCLUSIONES 67
5.2. RECOMENDACIONES 67
BIBLIOGRAFÍA **69**
ANEXOS **71**

ÍNDICE DE TABLA

Tabla 2.2.1. Características de los controladores de Redes Definidas por Software 21
Tabla 3.3.1. Materiales utilizados para el proyecto 26
Tabla 4.1.1.Servidores de data center 29
Tabla 4.1.2 Nodos de comunicación 30
Tabla 4.1.3. Cantidad de equipos existentes de acuerdo a la marca 31
Tabla 4.7.1. Comparación de respuestas a ICMP 54
Tabla 4.7.2. Respuesta de 4 equipos sin SDN 55
Tabla 4.7.3. Respuesta de 4 equipos con SDN 55
Tabla 4.7.4. Comparación en porcentaje de las pruebas 55
Tabla 4.7.5. Comparación de resultados en AB 56

ÍNDICE DE FIGURAS

Figura 2.2.1 Arquitectura de red SDN 15
Figura 2.2.2. Funcionamiento OpenFlow 16
Figura 4.1.1. Organigrama técnico Clicknet 29
Figura 4.1.2. Ejemplo de arquitectura de red de la empresa Clicknet 30
Figura 4.1.3. Porcentaje de dispositivos activos en la red 31
Figura 4.2.1. Red SDN propuesta para toda la infraestructura de la empresa 33
Figura 4.4.1. Esquema de red SDN de prueba en plataforma VirtualBox 37
Figura 4.4.2. Plataforma de prueba con equipos virtuales 38
Figura 4.4.3. Configuración de interfaces de red en routers mikrotik 39
Figura 4.4.4. Menú principal, servicios y protocolos instalados 39
Figura 4.4.5. Router cargado protocolo OpenFlow 40
Figura 4.4.6. Descarga de software para virtualizar el controlador HPE VAN SDN 40
Figura 4.4.7. Configuración de router Mikrotik 41
Figura 4.4.8. Controlador HPE VAN SDN ejecutándose OpenFlow versión 1.0 42
Figura 4.5.1. CPU para controlador HPE VAN SDN 43
Figura 4.5.2. Controlador SDN en producción 44
Figura 4.6.1. Acceso a honeypot Kippo en modo gráfico 48
Figura 4.6.2. Consola gráfica de Dionaea Honeypot 49
Figura 4.6.3. Presentación de servidor T-POT en funcionamiento 50
Figura 4.7.1. Origen y destino de prueba 51
Figura 4.7.2. *Respuesta de servidor sin habilitar OpenFlow* 51
Figura 4.7.3. Iperf como servidor 52
Figura 4.7.4. Prueba de Iperf sin habilitar OpenFlow 53
Figura 4.7.5. Respuesta de servidor habilitado OpenFlow 54
Figura 4.7.6. Prueba de Iperf sin habilitar OpenFlow 56
Figura 4.7.7. Diez contraseñas más usadas 57
Figura 4.7.8. Diez usuarios más usados 58
Figura 4.7.9. Número de conexiones por IP 58
Figura 4.7.10. Clientes SSH más usados 59
Figura 4.7.11. Servicios atacados 59
Figura 4.7.12. Puertos en intento de ataque 60
Figura 4.7.13. Direcciones IP de atacantes 60
Figura 4.7.14. Tablero de control de Suricata 61
Figura 4.7.15. Tablero de Dionaea 62
Figura 4.7.16. Servicios que monitorea T-POT con Dionaea 62
Figura 4.7.17. Vulnerabilidades registradas en Suricata 62
Figura 4.7.18. Alerta de vulnerabilidades 63
Figura 4.7.19. Geografía de los puntos de origen de ataque 64
Figura 4.7.20. Deshabilitar OpenFlow en router Mikrotik 65
Figura 4.7.21. Script para deshabilitar OpenFlow 66
Figura 4.7.22. Tarea que se ejecuta al iniciar el router 66

DEDICATORIA

Dedico este trabajo al ser que siempre guía mi existencia y me lleva de la mano cuando estoy en las peores condiciones, a ti Sr. Jesús.

A mi esposa Elizabeth por el apoyo incondicional desde el primer día de esta maestría, a mi hija Alisson, por preguntar el cómo me va cada día y preguntar cosas que ni ella entiende, a mi hijo Ian por permanecer esperando que termine mi trabajo para que hable con él, a Danna porque cada noche no duerme si no estoy cerca y tampoco quiere que salga de casa.

Al Ingeniero Santiago Manzano por ser la guía académica en este proceso de titulación y convertirse en un amigo a más de ser tutor.

A mi familia, a mis padres que a pesar de no saber lo que hago me felicitan porque saben lo que busco.

Edison Terán

AGRADECIMIENTOS

Agradezco infinitamente a mis padres por inculcarme desde pequeño a alcanzar las metas propuestas.

A mis hermanos, a Magdalena, Gloria, Marlene, Roberto y Sandra, por formar parte de mi existencia y el cariño que me entregan día a día.

A mis cuñados, y cuñadas por formar un vínculo familiar, a mis suegros por entenderme cuando no estoy presente.

A mis sobrinos, porque me ven como un ejemplo a seguir y por eso no desmayo.

Infinitamente a mi esposa y a mis tres amores.

Edison Terán

UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE INGENIERÍA EN SISTEMAS, ELECTRÓNICA E INDUSTRIAL

MAESTRÍA EN TELECOMUNICACIONES

TEMA:

DESPLIEGUE DE UN HONEYNET BASADO EN REDES DEFINIDAS POR SOFTWARE PARA UN ISP

AUTOR: Ingeniero Rubén Edison Terán Moreano

DIRECTOR: Ingeniero Víctor Santiago Manzano Villafuerte, Magíster

LÍNEA DE INVESTIGACIÓN:

- TECNOLOGÍAS, SEGURIDAD Y GESTIÓN DE REDES DE COMUNICACIONES

FECHA: 20 de octubre de 2021

RESUMEN EJECUTIVO

En la actualidad el Internet se ha convertido en un servicio básico en los hogares ecuatorianos y su utilización está creciendo de manera exponencial, por esta razón los proveedores de servicio de Internet o ISPs se encuentran preocupados por solventar la presencia de tráfico de datos dentro de su infraestructura, la raíz de este inconveniente, es que las empresas se han visto en la obligación de incrementar la capacidad en canal dedicado hacia sus clientes a menor costo con el objetivo de acaparar el mercado, sin imaginar que el incremento de suscriptores implica incremento de ancho de banda dentro de su propia red. Para evadir la congestión en la red convencional de la empresa se plantea utilizar el protocolo OpenFlow, sobre dispositivos de la marca Mikrotik, se ejecuta la red definida por software (SDN por sus siglas en inglés), con HPE VAN SDN como orquestador de la nueva topología de red. Se muestran las pruebas realizadas, tanto de velocidad de respuesta de datos como los resultados de rendimiento de ancho de banda.

Al disponer de una nueva tecnología en la red de datos se plantea mejorar la confianza perimetral con sistemas trampa, aplicando y configurando varios honeypots para crear una honeynet (unión de honeypots). Con distribuciones de software como Honeydrive y T-Pot, se describieron todas las herramientas

embebidas en cada una, mostrándose como resultado de la investigación las respectivas pruebas de seguridad y la importancia que implica disponer de un sistema Trampa dentro de un ISP.

UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE INGENIERÍA EN SISTEMAS, ELECTRÓNICA E INDUSTRIAL

MAESTRÍA EN TELECOMUNICACIONES

THEME:

DEPLOYING A NETWORK-BASED HONEYNET DEFINED BY SOFTWARE FOR AN ISP

AUTHOR: Ingeniero Rubén Edison Terán Moreano

DIRECTED BY: Ingeniero Víctor Santiago Manzano Villafuerte, Magíster

LINE OF RESEARCH:

- TECHNOLOGIES, SECURITY AND MANAGEMENT OF COMMUNICATIONS NETWORK

DATE: Oct 20, 2021

EXECUTIVE SUMMARY

Currently the Internet has become a basic service in Ecuadorian homes and its use is growing exponentially, for this reason Internet service providers or ISPs are concerned about solving the presence of data traffic within their infrastructure, the root of this problem, is that companies have been obliged to increase the capacity in the channel dedicated to their customers at a lower cost in order to monopolize the market, without imagining that the increase in subscribers implies an increase in width band within your own network. To avoid congestion in the company's conventional network, it is proposed to use the OpenFlow protocol, on Mikrotik brand devices, the software defined network (SDN) is executed, with HPE VAN SDN as orchestrator of the new Network topology. The tests performed are shown, both for data response speed and bandwidth performance results.

By having a new technology in the data network, it is proposed to improve perimeter trust with honeypots, applying and configuring several honeypots to create a honeynet (union of honeypots). With software distributions such as Honeydrive and T-Pot, all the tools embedded in each one was described, showing as a result of the investigation the respective security tests and the importance of having a Trap system within an ISP.

CAPÍTULO I

1.1. Introducción

La expresión HoneyNet fue adoptada por The Money Project; una organización no lucrativa, fundada por Lance Spitzner. Este grupo está compuesto por expertos en seguridad, cuyo objetivo es aprender las herramientas, tácticas y motivos de los atacantes. [1]

Según [3], las redes SDN (redes definidas por software), son un enfoque arquitectónico que separa el plano de control del plan de datos de una red y se gestiona el flujo de datos mediante un controlador SDN, hoy en día este tipo de sistemas sería de mucha utilidad para los ISPs, con el fin de direccionarse a un solo dispositivo y no en toda una infraestructura.

En el presente se evalúa un proyecto como despliegue de un honeynet basado en redes definidas por software para un ISP, que surge de la necesidad de controlar los dispositivos de manera centralizada sin importar la ubicación y marca de los mismos, a su vez desarrollar un sistema de prevención de ataques hacia la red de interna.

El trabajo de gestión de flujo de datos lo va a llevar un controlador SDN, y de acuerdo a [2], HP SD VAN CONTROLLER se muestra como un controlador que se acopla a las necesidades específicas de una red empresarial, haciendo referencia a condiciones técnicas, económicas y de infraestructura, para la prueba de este controlador se requiere herramientas que indiquen si la red SDN mejora su rendimiento en relación a la red de datos convencional. La red SDN probada en su gran mayoría ha sido virtualizada, por tanto, en el presente proyecto se ejecutará este sistema en un fragmento de red de un ISP para no afectar a la entrega de servicios. Dado los recursos disponibles, se aplica a hardware de marca Mikrotik, y como lo indica [3], poder obtener resultados más cercanos a la realidad.

La seguridad en una red SDN, para [4], es conveniente la utilización de una red trampa o honeynet, la misma que se establece de varios honeypot agrupados entre sí, lo que obliga a este honeynet que debe cumplir como agente de anticipación de intrusos dentro de la infraestructura de red basada en software. En lo que respecta a este tema, [5] hace referencia a que este tipo de red trampa debe disponer de una arquitectura inteligente para poder solucionar el consumo de recursos continuos.

1.2. Justificación

El rendimiento promedio de una infraestructura de red como lo menciona [6], se puede identificar mediante la calidad de servicio (QoS) en una red tradicional de un ISP, de forma cuantitativa se mide la calidad de los servicios de red, considerado en varios aspectos tales como tasas de errores, ancho de banda, rendimiento, retraso en la transmisión, disponibilidad, jitter, etc.

Se considera que los servicios mencionados dependen de los dispositivos y marcas que forman parte de la infraestructura, la propuesta quiere experimentar cambios primordiales en una red SDN, dependiendo del controlador aplicado y poder evidenciar si existe un mejoramiento de los servicios convencionales.

La empresa Clicknet S.A no dispone de ningún sistema que permita evidenciar alertas tempranas ante ataques a la red y mucho menos recopilación de información para analizar y ejecutar soluciones de vulnerabilidades, según [4] un honeynet permitirá captura, recopilación y control de datos, con esta información adquirida se podrá ejecutar métodos o planes de contingencia para solventar problemas de seguridad, como lo solicita el ente regulador del país (ARCOTEL).

La detección de intrusos se hace cada vez más complicada de manejar y alertar, por la proliferación de servicios dentro de una red de datos que son innumerables y que trabajan simultáneamente, para lo cual se utilizará el beneficio que provee el mejoramiento de tecnología de SDN como se evidencia en [7] donde se propone una arquitectura diferente a la tradicional para obtener datos historiales y ejecución de soluciones.

1.3. Objetivos

1.3.1. General

Desplegar un honeynet basado en redes definidas por software para in ISP.

1.3.2. Específicos

- Determinar la situación actual de la infraestructura de red de la empresa Clicknet S.A.
- Implementar una red definida por software en la empresa Clicknet S.A.
- Aplicar una herramienta de seguridad de datos dentro de la infraestructura de red SDN, basado en Honeynet.

CAPITULO II

2.1.Estado del Arte

En la investigación de [8], denominada como "Estudio de factibilidad y diseño de una red inalámbrica ISP, para proveer servicio de internet en las comunidades de la cuenca del Lago San Pablo", la misma que tenía como objetivos realizar el estudio de un diseño técnico de una red inalámbrica ISP, para proveer servicio de internet en las comunidades de la cuenca del Lago San Pablo, mediante un enlace punto multipunto en la que se analizó el estado de arte de las tecnologías de comunicación inalámbrica para enlazar nodos punto a punto y multipunto y diseñó una red con nodos y repetidores de banda ancha de internet para el enlace entre los usuarios finales.

Para el desarrollo de la investigación se usó una metodología que desea plantear una infraestructura con equipos y dispositivos que se utilizan en un ISP. Con un nodo central como estación base ubicados estratégicamente en los alrededores de la cuenca del lago, y así cubrir con internet inalámbrico las zonas rurales de las parroquias; que cuentan con una superficie aproximada de alrededor de 150 km² de la cuenca del lago. Aplicada a 32.056 personas, obtuvo o concluyó con que el estudio planteado es carácter técnico, y económicamente factible, una vez cumplidos todos los requerimientos necesarios que se mencionaron en los apartados correspondientes por cuanto su ejecución es totalmente viable y accesible, con la desventaja que no logra brindar un servicio de última milla, este servicio lo brinda un portador backhaul, dado que para legalizar el nodo principal como secundario de un WISP se lo debe hacer a través de un proveedor de servicios portadores porque estos son los únicos que tienen el permiso para el levantamiento de infraestructura de transmisión de datos y son concesionarios de las frecuencias utilizadas para la transmisión de datos inalámbricos (de acuerdo a reglamentos legales de la ARCOTEL).

En la investigación de [9], denominada como “Implementación de un ISP para mejorar el servicio de internet con la empresa CSED net en el cantón El Carmen provincia de Manabí", la misma que tenía como objetivos el de implementar un ISP para mejorar el servicio de internet con la empresa CSED net en el cantón El Carmen provincia de Manabí con un diseño de un esquema de funcionamiento de un ISP y los lugares favorecidos del mismo en el cantón El Carmen. Para ello se realizó un estudio de mercado aplicado a la población y se realizó una simulación de carga basada en la población y los mejores equipos disponibles para tal efecto, se concluyó con que la

implementación de un ISP, está ubicado en un sector estratégico en la ciudad de El Carmen, obteniendo una factibilidad óptima para realizar enlaces de punto a punto y así brindando un mejor ancho de banda a los clientes última milla que adquieran este servicio. Se presenta un presupuesto mínimo y el estudio de recuperación económica es factible para que se dé la inversión total de la implementación del ISP y así en esta primera fase recuperar la inversión en un mínimo tiempo de 7 meses con el funcionamiento del nodo matriz y nodo secundario a funcionar.

En la investigación de [10] denominada como "Estudio de factibilidad para la creación de un proveedor de servicios de internet con cobertura en la ciudad de Quito", la misma que tenía como objetivos el de identificar al cliente potencial del servicio de internet en la ciudad de quito, la posibilidad de que contrate los servicios, sus deseos y necesidades a fin de determinar la viabilidad de implementar este proyecto de inversión desde el punto de vista del mercado, donde se determinó la demanda del servicio de internet en quito, sector sur y norte. Para esta investigación se usó una metodología cualitativa, siendo la encuesta el principal instrumento aplicado y donde se concluyó con que en la actualidad el servicio de internet se ha vuelto indispensable para el desenvolvimiento de las actividades diarias de una persona. El estudio de mercado determinó que la mayor parte de la población conoce lo que es el servicio de internet y lo utiliza para sus labores diarias sean estudiantiles, de trabajo, entretenimiento o de comunicación.

En la investigación de [11] , denominada como "Diseño de un nodo ISP inalámbrico de banda ancha para la comuna El Azúcar del cantón Santa Elena", la misma que tenía como objetivos diseñar un nodo ISP inalámbrico de banda ancha, mediante un estudio de factibilidad técnica, que permita mejorar el acceso a internet en la comuna El Azúcar del cantón Santa Elena, además de levantar la información necesaria relacionada con el tópico de estudio, mediante entrevistas no estructurada a expertos en el tema y la comunidad en general y simular el radio enlace punto – multipunto en el software radio mobile. En la que uso una metodología a través de un estudio de mercado desde la aplicación de encuestas a la comunidad de El Azúcar aplicada a 308.693 personas y mediante simulaciones para tener una mayor inclusión y entendimiento del problema. Se concluyó que la presente propuesta tecnológica es técnica y financieramente factible una vez realizado todo el estudio y cumplir con los requerimientos necesarios para que en un futuro se ejecute la implementación.

En la investigación de [12], denominada como "Análisis y diseño de una solución

dé red ISP wimax basada en ieee802.16m-2011 para las sedes UDLAPARK y Granados de la Universidad de las Américas en la ciudad de Quito", la misma que tenía como objetivos, diseñar una solución de red de enlace analizando tecnología wimax o fibra óptica para las sedes Granados y UDLAPARK de la Universidad de las Américas en la ciudad de Quito, comparando estas dos tecnologías tanto en su aspecto técnico como financiero, escoger la que mejor se adapta a las necesidades de la institución, en la que se concluyó que la implementación del diseño por fibra es relativamente económica en comparación con el costo mensual que la universidad asume por este tipo de servicio, de esa forma en menos de un año de pago por el servicio, la universidad puede ser la dueña del manejo, transporte y administración de su información entre las dos sedes de estudio.

En la investigación de [13], denominada como "Diseño de una red que provea servicios de internet (ISP) en las cabeceras cantonales Célica y Catacocha de la provincia de Loja", la misma que tenía como objetivos diseño de una red que provea servicios de internet (ISP) en las cabeceras cantonales Célica y Catacocha de la provincia de Loja, en la que se usó una metodología cuantitativa, donde se concluyó con que una vez realizado el proyecto se concluye que es factible la implantación en las cabeceras cantonales de Célica y Catacocha debido al alto grado de posibles clientes según los datos tabulados, además al utilizar estos equipos inalámbricos Mikrotik y Ubiquiti los que le ofertan al usuario el servicio de internet de acuerdo a su economía.

2.2. Marco teórico

2.2.1. **Proveedor de servicios de internet (ISP)**

Los proveedores de servicios de internet o ISPs como indica binlun2018, disponen de redes comerciales convencionales distribuidas dentro de su infraestructura, en este ambiente se despliega varios tipos de tecnologías como, redes de fibra óptica, redes inalámbricas, ADSL, etc. Dentro de esta gran conexión se integran dispositivos enrutadores y conmutadores o switchs los mismos que son gestionados de manera independiente.

Los proveedores de servicios de internet (ISP), que comenzaron a surgir a finales de 1980 y principios de 1990, son las empresas y organizaciones que proporcionan acceso a internet y servicios relacionados a los usuarios. Estos proveedores conectan los clientes a los clientes de otros proveedores de servicio por

medio de redes. A menudo, los proveedores de servicio de internet (también llamados proveedores de acceso a internet) son empresas que proporcionan servicios de telecomunicaciones, entre ellos, acceso a las comunicaciones de datos y la conexión telefónica, o incluso acceso a la televisión por cable. La mayoría de las empresas telefónicas funcionan ahora también como proveedores de acceso a internet o proveedores de servicio de internet. Los isp pueden ser comerciales, sin fines de lucro, de propiedad privada o propiedad de la comunidad.

Hay un buen número de diferentes tipos de proveedores de servicio de internet disponibles en la actualidad, que incluyen acceso, buzón de correo, espacio de servidor, tránsito, virtual y gratuito.

ISP de acceso - emplean una variedad de tecnologías para facilitar la conexión de los clientes a su red. Estas tecnologías alcanzan incluir banda ancha o conexión por línea conmutada. Tipos de conexiones permanentes de banda ancha, cable compuesto, servicio de fibra óptica (fios), DSL (digital subscriber line) y satélite. Una cantidad de proveedores de acceso también proporcionan email y servicios de servidores.

ISP de buzón de correo - ofrecen servicios de servidor de buzón de email y servidores de email para enviar, recibir y almacenar email. Muchos ISP de buzón de correo son también proveedores de acceso.

ISP de servidores - ofrecen email, protocolo de transferencia de archivos (ftp), servicios de servidores web, máquinas virtuales, servidores de cloud y físicos.

ISP de tránsito - proporcionan grandes cantidades de ancho de banda necesarias para conectar los ISP de servidores y acceder de manera conjunta a los ISP.

ISP virtuales (ISP) - compran servicios de otros IPSs para permitir a los clientes el acceso a internet.

ISP gratuitos (freenets) - proporcionan servicio de forma gratuita y a menudo muestran anuncios mientras los usuarios están conectados.

Los proveedores de servicio de internet ofrecen una gran variedad de servicios a sus clientes, desde el acceso a internet por cable hasta el acceso a internet por fibra, entre otros. Algunos de estos servicios son el acceso a internet, el registro de nombres de dominio, el alojamiento de nombres de dominio o alojamiento web, el acceso a una conexión dial-up, el acceso por línea alquilada y la comunicación. Como la mayoría sabe, internet es un sistema global de redes de computadoras interconectadas utilizado por miles de millones de personas en todo el mundo. Este sistema de redes está enlazado mediante una amplia variedad de tecnologías electrónicas, de redes ópticas

e inalámbricas [14].

El término proveedor de servicios de internet (ISP) se refiere a una empresa que proporciona acceso a internet tanto a clientes personales como comerciales. Los ISP permiten a sus clientes navegar por la web, comprar en línea, hacer negocios y conectarse con familiares y amigos, todo por una tarifa. Los ISP también pueden proporcionar otros servicios, incluidos servicios de correo electrónico, registro de dominio, alojamiento web y paquetes de navegador. Un ISP también se denomina proveedor de servicios de información, proveedor de servicios de almacenamiento, proveedor de servicios de internet (ISP) o cualquier combinación de los tres en función de los servicios ofrecidos por la empresa.

Un proveedor de servicios de internet (ISP) es una empresa que proporciona acceso web tanto a empresas como a consumidores. Los ISP también pueden proporcionar otros servicios como servicios de correo electrónico, registro de dominio, alojamiento web y servicios de navegador.

El servicio de internet se limitó inicialmente a determinadas agencias gubernamentales y departamentos universitarios. La tecnología se desarrolló para brindar acceso al público en general a través de la *Word Wide Web* a fines de la década de 1980. Los consumidores pudieron obtener acceso limitado a través de algunos ISP, América on line (AOL) como uno de los nombres más reconocibles en ese momento, que usaba conexiones de acceso telefónico a través de una línea telefónica.

El número de ISP aumentó a varios miles a mediados de la década de 1990 y el auge continuó. A medida que las opciones de conectividad aumentaron y las velocidades cambiaron de conexiones telefónicas más lentas, nació la economía de internet. Los proveedores han desarrollado tecnología más avanzada, dando a los clientes acceso de alta velocidad a través de tecnología de banda ancha a través de módems de cable y línea de abonado digital (DSL).

Detrás de todo esto había una red de conexiones multicapa. Los ISP locales vendían el acceso a los clientes, pero pagaban a más ISP por su propio acceso. Posteriormente, los ISP más grandes pagaron a más ISP por el acceso. Los operadores de nivel 1 lideran el camino para llegar a todos los puntos de acceso de la red sin pagar por el acceso. Estas empresas de nivel 1 son propietarias de la infraestructura de su región.

Como se indicó anteriormente, los proveedores de servicios de internet brindan principalmente a sus clientes acceso a internet: proveedores de acceso simple que solo

manejan el tráfico entre el individuo e internet en su conjunto. Pero también se pueden incluir otros servicios en función de la ubicación y la disponibilidad del cliente. Algunos de estos servicios incluyen el servicio de correo electrónico, hospedaje web, Registro de dominio y paquetes de software y navegador. [15]

2.2.2. **Redes definidas por software (SDN)**

Las SDN, según [16], permite separar el plano de control del plano de distribución o forwarding gestionada desde un controlador, al poder tramitar desde un solo lugar, evidencia una arquitectura, dinámica, automatizada, y rentable. También se hace referencia de acuerdo a binlun2018 que el controlador tiene la capacidad de regular y seleccionar el origen de los datos para su proceso dentro de la red SDN, esto implica que SDN admite el control de flujo de datos de acuerdo a la configuración empleada en el gestor, sin importar el tipo de dispositivo que se instale dentro de la infraestructura de red.

De acuerdo a [3], la red de datos dispone de dos recursos, el plano de control que usa información de señalización para ejercer disposiciones de control, el plano de datos se encarga de la entrega de datos hacia los usuarios correspondientes.

De acuerdo a [7], la tecnología SDN excluye la inteligencia propia que dispone cada hardware de las redes de datos tradicionales, esta tecnología separa la información real que se transporta por la capa de datos y la de control, la que establece el cómo, cuándo y dónde va el trayecto de flujo de datos, y como consecuencia cada capa se encuentras automatizadas. En [4], se evidencia las ventajas que se logran presentar en esta nueva arquitectura en relación a las redes convencionales, entre ellas están:

- Gestión centralizada: admite la gestión centralizada en su totalidad, con este detalle se consigue evitar errores de configuración, minimizar riesgos de seguridad, cuellos de botella, etc. Que generan puntos de fallo en una red convencional.
- Agilidad: se consigue asegurar un ancho de banda especifico o calidad de servicio (QOS) con mayor ligereza para acoplarse a las transiciones de la red.
- Bajos costos: en este caso, solo se presentan si los equipos disponen de compatibilidad con protocolo OpenFlow, si es el caso se abaratarían costos de

implementación.

- Programación automática: la red SDN permite a los administradores, se logra generar scripts propios para optimizar y gestionar la red de manera ágil y dinámico.
- Fácilmente programable: al estar separado del plano red, existe la posibilidad de que se pueda programar o configurar con facilidad el plano de control.
- Escalabilidad: de acuerdo a la arquitectura que dispone, existe la facilidad de proyectar o extender una red en gran medida sin que se pierdan sus características.
- Basado en estándares abiertos y proveedores neutrales: al implementar sobre estándares abiertos, se hace más fácil el diseñar esta red y operar, porque todas las órdenes son enviadas por el controlador, en lugar de varios dispositivos de varios proveedores o varios protocolos.
- Seguridad: como la red pertenece a un controlador centralizado, hay poca probabilidad de agujeros de riesgo de seguridad en las configuraciones de los dispositivos SDN.

Las redes definidas por software (SDN) representan un enfoque en el que las redes utilizan controladores basados en software o interfaces de programación de aplicaciones (API) para dirigir el tráfico en la red y comunicarse con la infraestructura de hardware subyacente.

Este enfoque es distinto al de las redes tradicionales, que utilizan dispositivos de hardware dedicados (enrutadores y conmutadores) para controlar el tráfico de la red. Una SDN consigue crear y controlar una red virtual o controlar una red de hardware tradicional mediante el software.

Mientras que la virtualización de red ofrece la posibilidad de segmentar distintas redes virtuales dentro de una red física o de conectar dispositivos de diferentes redes físicas a una red virtual, la red definida por software proporciona una nueva forma de controlar el enrutamiento de los paquetes de datos a través de un servidor centralizado.

Estos son los fundamentos de las SDN: en una SDN (como en cualquier tecnología

virtualizada), el software se encuentra desvinculado del hardware. La SDN separa los dos planos de los dispositivos de red, ya que traslada al software el plano de control que establece dónde enviar el tráfico y deja en el hardware el plano de datos que realmente reenvía el tráfico. Esto significa que los administradores de red que utilizan redes definidas por software pueden programar y controlar toda la red desde un solo panel de control en lugar de hacerlo dispositivo por dispositivo.

La arquitectura típica de SDN se divide en tres partes:

- Las aplicaciones, que comunican las solicitudes de recursos o información sobre la red en su conjunto.
- Los controladores, que utilizan la información de las aplicaciones para decidir cómo enrutar un paquete de datos.
- Los dispositivos de red, que reciben información del controlador sobre dónde mover los datos.

Estos tres elementos suelen encontrarse en diferentes ubicaciones físicas. Los dispositivos de redes virtuales o físicas son los que realmente trasladan los datos a través de la red. Los conmutadores virtuales, que pueden estar integrados en el software o en el hardware, en algunos casos asumen las responsabilidades de los conmutadores físicos y consolidan sus funciones en un único conmutador inteligente. El conmutador comprueba la integridad tanto de los paquetes de datos como de los destinos de las máquinas virtuales y traslada los paquetes.

Las SDN ofrecen toda una serie de ventajas sobre las redes tradicionales, entre ellas:

- Mayor control con una velocidad y flexibilidad superiores: en lugar de programar manualmente varios dispositivos de hardware específicos de un proveedor, los desarrolladores logran controlar el tráfico que fluye en una red con solo programar un controlador basado en software de estándar abierto. Los administradores de red también tienen más flexibilidad para elegir el equipo de las redes, puesto que optan por un protocolo de código abierto para comunicarse con cualquier cantidad de dispositivos de hardware a través de un controlador central.
- Infraestructura de red personalizable: al utilizar una red definida por software, los administradores configuran los servicios de red y asignar recursos virtuales para

cambiar la infraestructura de la red en tiempo real desde una ubicación centralizada. Esto permite que los administradores de red optimicen el flujo de datos en la red, dando prioridad a las aplicaciones que requieren una mayor disponibilidad.

- Seguridad sólida: una red definida por software aumenta la visibilidad de toda la red, lo que proporciona una visión integral de las amenazas a la seguridad. Dada la proliferación de dispositivos inteligentes que se conectan a internet, una SDN ofrece ventajas patentes en comparación con las redes tradicionales. Los desarrolladores pueden crear zonas independientes para los dispositivos que exijan distintos niveles de seguridad o poner en cuarentena al momento cualquier dispositivo con alguna vulnerabilidad para que no pueda infectar el resto de la red.

La diferencia clave entre las SDN y las redes tradicionales es la infraestructura: las SDN están basadas en software, mientras que las redes tradicionales están basadas en hardware. Ya que el plano de control está basado en software, las SDN son mucho más flexibles que las redes tradicionales. Permiten que los administradores controlen la red, cambien los ajustes de configuración, aprovisionen recursos y aumenten la capacidad de la red, todo ello desde una interfaz de usuario centralizada y sin necesidad de añadir más hardware.

También hay diferencias relativas a la seguridad entre las SDN y las redes tradicionales. Gracias a una mayor visibilidad y a la capacidad de definir rutas seguras, las SDN ofrecen una seguridad mejor en muchos aspectos. Sin embargo, puesto que las redes definidas por software hacen uso de un controlador centralizado, protegerlo es crucial para mantener una red segura, puesto que este punto único de fallo representa una posible vulnerabilidad de las SDN.

Aunque la premisa de un software centralizado que controle el flujo de datos en los conmutadores y enrutadores se aplica a todas las redes definidas por software, existen diferentes modelos de SDN.

- SDN abierta: los administradores de red utilizan un protocolo como OpenFlow para controlar el comportamiento de los conmutadores virtuales y físicos en el plano de datos.
- SDN por api: en lugar de utilizar un protocolo abierto, las interfaces de

programación de aplicaciones controlan cómo se desplazan los datos a través de la red en cada dispositivo.

- Modelo de superposición de SDN: otro tipo de red definida por software ejecuta una red virtual sobre una infraestructura de hardware existente, lo que crea túneles dinámicos hasta diferentes centros de datos locales y remotos. La red virtual asigna el ancho de banda en diversos canales y asigna dispositivos a cada canal, de forma que la red física queda intacta.
- SDN híbrida: este modelo combina la red definida por software con los protocolos de red tradicionales en un solo entorno a fin de respaldar las diferentes funciones de una red. Los protocolos de red estándar siguen dirigiendo parte del tráfico, mientras que la SDN asume la responsabilidad de otra parte, lo que permite a los administradores de red introducir la SDN por etapas en un entorno heredado.

Muchos de los servicios y aplicaciones actuales, en especial cuando involucran a la nube, no podrían funcionar sin las SDN. Las SDN permiten que los datos se desplacen fácilmente entre ubicaciones distribuidas, lo que es fundamental para las aplicaciones en la nube.

Además, las SDN permiten desplazar cargas de trabajo rápidamente dentro de una red. Por ejemplo, dividir una red virtual en secciones, mediante una técnica denominada virtualización de funciones de red (NFV), permite a los proveedores de telecomunicaciones trasladar los servicios del cliente a servidores más económicos o incluso a los propios servidores del cliente. Los proveedores de servicios pueden utilizar una infraestructura de red virtual para trasladar las cargas de trabajo desde las infraestructuras de nube privada hasta las de la pública, según sea necesario, y poner a disposición de los clientes nuevos servicios de forma instantánea. Las SDN también facilitan que cualquier red se flexibilice y crezca a medida que los administradores de red añadan o eliminen máquinas virtuales, ya estén en el entorno local o en la nube.

Por último, gracias a la velocidad y la flexibilidad que ofrecen las SDN, es posible dar soporte a tendencias y tecnologías emergentes, como la informática perimetral y el internet de las cosas, que requieren una transferencia de datos rápida y sencilla entre sitios remotos. [17]

Las redes definidas por software (SDN) son un enfoque arquitectónico de la red que permite a la red ser controlada de manera inteligente y central, o "programada", utilizando aplicaciones de software. Esto ayuda a que los operadores gestionen toda la red de manera constante e integral, independientemente de la tecnología de red subyacente.

Corporaciones, operadores y proveedores de servicios se ven rodeados de varias fuerzas competitivas. El crecimiento monumental del contenido multimedia, la explosión de la computación en la nube, el impacto del aumento de uso del móvil y las continuas presiones empresariales para reducir los costos mientras que los ingresos se mantienen fijos están convergiendo para causar estragos en los modelos empresariales tradicionales.

Para mantener el ritmo, muchos de estos jugadores están recurriendo a la tecnología de SDN para revolucionar las operaciones y el diseño de la red.

SDN permite la programación del comportamiento de la red de una manera controlada centralmente mediante aplicaciones de software que utilizan api abiertas. Con la apertura de las plataformas de red generalmente cerradas y la implementación de una capa de control de SDN común, los operadores pueden gestionar toda la red y sus dispositivos de forma consistente, independientemente de la complejidad de la tecnología de red subyacente.

Hay cuatro áreas críticas en las que la tecnología SDN marcan la diferencia para una organización.

1) programabilidad de la red: SDN permite que el comportamiento de la red se controle mediante el software que reside más allá de los dispositivos de red que proporcionan conectividad física. Como resultado, los operadores de red pueden adaptar el comportamiento de sus redes para soportar nuevos servicios e incluso clientes individuales. Al desacoplar el hardware del software, los operadores introducen nuevos servicios diferenciados e innovadores rápidamente, libre de las limitaciones de las plataformas cerradas y patentadas.

2) Centralizar inteligencia y control lógicamente: SDN se basa en topologías de red centralizadas lógicamente, que permiten la administración y el

control inteligente de los recursos de la red. Se distribuyen métodos de control de red tradicional. Los dispositivos funcionan de forma autónoma con un conocimiento limitado del estado de la red. Con el tipo de control centralizado que ofrece una red basada en SDN, la administración, la restauración, la seguridad y las políticas de ancho de banda pueden ser muy inteligentes y optimizados; y una organización obtiene una visión integral de la red.

3) Abstracción de la red: los servicios y las aplicaciones que se ejecutan en la tecnología SDN se abstraen de las tecnologías subyacentes y del hardware que proporcionan conectividad física de control de la red. Las aplicaciones van a interactuar con la red a través de las api, en lugar de las interfaces de administración estrechamente acopladas al hardware.

4) Apertura: las arquitecturas de SDN dan comienzo a una nueva era de apertura, que permite la interoperatividad de proveedores múltiples, así como la promoción de un ecosistema no vinculado a proveedores. La apertura proviene del enfoque de SDN en sí. Las api abiertas soportan una amplia gama de aplicaciones, incluidas la orquestación de la nube, OSS/BSS, SAAS y aplicaciones en red críticas para el negocio. Además, el software inteligente puede controlar el hardware de múltiples proveedores con interfaces de programación abiertas como OpenFlow. Por último, desde el interior de SDN, los servicios de red y las aplicaciones inteligentes pueden ejecutarse dentro de un entorno de software común.

Una ventaja clave de la tecnología de SDN es la capacidad para que los operadores de red escriban programas que utilizan las api de SDN y dan a las aplicaciones el control del comportamiento de la red. SDN permite a los usuarios desarrollar aplicaciones orientadas a la red, monitorear las condiciones de red de forma inteligente y adaptar automáticamente la configuración de la red, según sea necesario. [18]

2.2.3. **Funcionamiento de SDN**

De acuerdo a [3], el plano de control está de nido por un controlador centralizado que está en capacidad de negociar las interfaces físicas a través de api southbound y protocolo OpenFlow, a nivel de aplicación otra api conocido como northbound mejora la gestión de los datos, como se muestra en la figura 2.2.1.

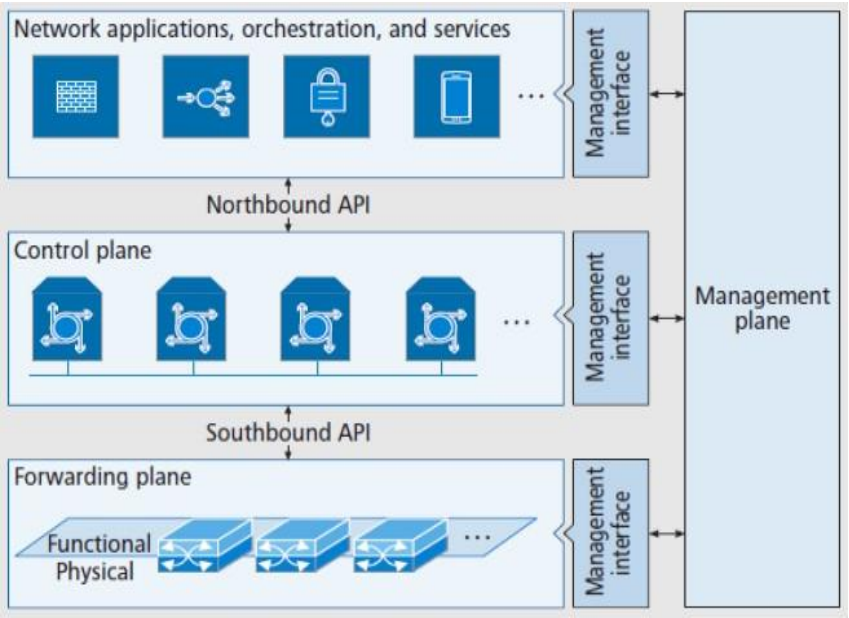


Figura 2.2.1 Arquitectura de red SDN

Fuente: [3]

De acuerdo a [3] la arquitectura SDN se compone de tres capas acceden mediante api.

- Capa aplicación: aquí se encuentran las aplicaciones del administrador o usuario local, es donde se encuentran los servicios.
- Capa de control: otorga la gestión lógica centralizada, ejecuta la supervisión y reenvío de paquetes por medio de una interfaz activa.
- Capa de infraestructura: los instan los dispositivos de red y los elementos que otorgan la conmutación y reenvío de los paquetes.

Como se indicó anteriormente la comunicación entre capas se ejecuta mediante las api.

2.2.4. **OpenFlow**

El protocolo OpenFlow de acuerdo a [19], es uno de los mejores documentados y utilizado para investigación. [3] muestra que OpenFlow es un protocolo standard

de comunicación para la tecnología SDN, de nido entre la capa de control y la capa de fordwarding, este protocolo permite acceso directo y dirección de los equipos físicos y virtuales activos en un concentrador.

Este protocolo permite un intercambio de información entre dispositivos de diferentes fabricantes como se muestra en la figura 2.2.2, admitiendo el control de una red programada de manera independiente de los conmutadores de red.

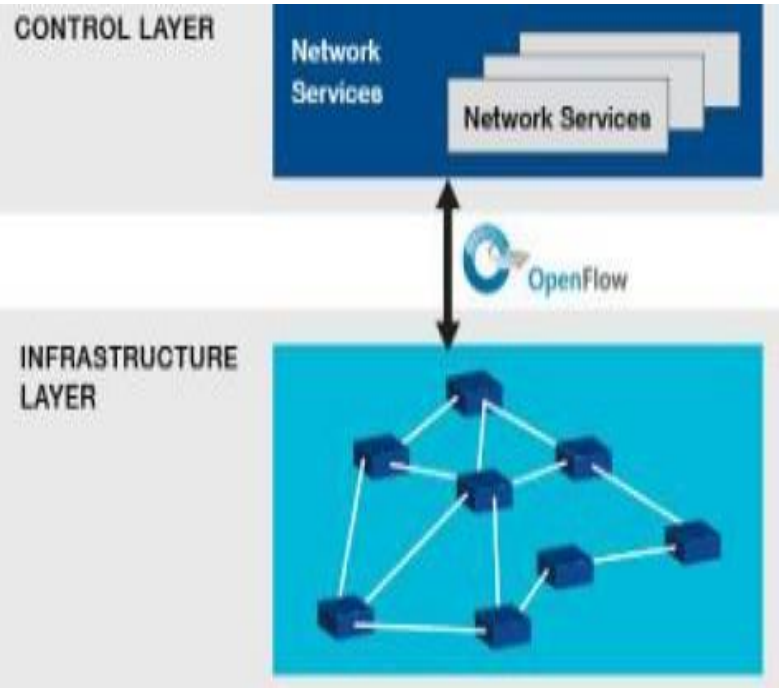


Figura 2.2.2. Funcionamiento OpenFlow

Fuente: [3]

2.2.5. **Puertos OpenFlow**

Para [3] los switch OpenFlow se interconectan a través de puertos OpenFlow, en donde un paquete se traslada de uno a otro de nido por un puerto de salda y un puerto de entrada en el primero y segundo dispositivo respectivamente. Existen tres puertos en OpenFlow, puertos físicos, lógicos y reservados (solo si el equipo soporta este tipo de puertos).

- Puerto físico: se los reconoce como puertos de entrada y de salida, cuando se encuentran en grupo estos puertos se ejecutan como contadores y tienen una etapa de configuración.
- Puerto lógico: estos puertos no se relacionan con los puertos físicos, son

puertos abstractos de nidos en forma de túneles, loopback o conexiones de agregación.

- Puerto reservado: aquí es donde se específica las operaciones de reenvió, ya sea al controlador, una inundación, o reenvío como procesamiento de un conmutador tradicional.

2.2.6. **Componentes de un switch OpenFlow**

En [3], se evidencia que el dispositivo está compuesto por varias tablas de flujos con sus grupos de tablas asignadas respectivamente, en el instante en que un flujo de datos se compara, para aplicar normas de búsqueda de paquetes y distribución.

El controlador gestiona según [3] a los dispositivos por medio del protocolo OpenFlow, el mismo que admite, añadir, actualizar y borrar flujos de ingreso de manera proactiva como reactiva.

2.2.7. **Controlador SDN**

Un controlador en una red SDN hace el papel del cerebro de dicha red, es decir, el punto de gestión estratégico que retransmite información a los conmutadores y enrutadores de debajo (a través del api southbound) y a las aplicaciones y la lógica de negocio encima (a través del api northbound).

La selección de un controlador vuelve importante si se va a realizar un diseño de red SDN [20], por tanto, se debe tomar en cuenta ciertas características como:

- Soporte OpenFlow: se debe tomar en cuenta que versiones de protocolo OpenFlow dispone, así como la posibilidad de migrar a nuevas versiones.
- Virtualización de red: un controlador debe soportar redes virtualizadas disponer de herramientas para que puedan ser gestionadas de manera independiente o aislada por seguridad, todas estas redes SDN deben ser gestionadas de manera centralizada.
- Funcionalidad de la red: el controlador debe disponer de capacidad de tomar decisiones de enrutamiento, así como también de unir parámetros de GoS flujo por flujo. Es importante también que el controlador pueda de unir múltiples caminos desde el origen del flujo a su destino y para segmentar el tráfico de un flujo a través de múltiples enlaces. Esta capacidad elimina la necesidad de

protocolos como STP (spanning tree protocol), y evitar otros protocolos que no son necesarios dentro de esta arquitectura.

- Escalabilidad: para tener en cuenta esta capacidad hay que hacer referencia al número de conmutadores o dispositivos que el controlador pueda soportar. El controlador debe estar en la capacidad de disminuir el impacto de sobrecarga de expansión de red. También debe disponer de capacidad de acaparar múltiples sitios.

- Rendimiento: hace referencia a la cantidad de números de flujos que es capaz de pasar en un enlace de datos con relación a un dispositivo convencional de red de datos (switch), si es capaz de pasar más cantidad es mejor su rendimiento. Los flujos de datos dentro de una red SND, se puede configurar de dos maneras, proactivas o reactivas.

- Programación de red: gracias a las entradas que dispone un controlador se puede aplicar configuración específica para aplicar varias funcionalidades. Como ejemplo se indica la capacidad de redirigir el tráfico y la posibilidad de emplear filtros sofisticados de paquetes.

- Confiabilidad: el controlador debe disponer de capacidad de encontrar múltiples caminos desde el origen hasta el destino y esto lo realiza solo si se controla de manera continua la topología de la red. Como dispone de varios caminos si uno de ellos faltare, el servicio no será interrumpido.

- seguridad de la red: para proporcionar seguridad en el controlador debe dispone de la capacidad de soportar la autenticación y autorización. Debe disponer de una instigación ante una sospecha de ataque.

- monitorización centralizada y visualización: un controlador debe ser capaz de usar los datos obtenidos por el protocolo OpenFlow e identificar los problemas de la red y de esta forma realizar cambios en la infraestructura cuando se presenten. Debería disponer de monitoreo el controlador con algún protocolo como por ejemplo SNMP.

- fabricantes de controladores SDN: en la actualidad existen numerosas empresas fabricando dispositivos que soportan redes SDN y por ende compatibles con el protocolo OpenFlow, en consecuencia, estos fabricantes

deben implementar sus servicios SDN y el controlador debe ser capaz de mantenerse al día con este servicio.

- Soporte de plataformas: debe convenir que el controlador pueda correr bajo varios sistemas operativos, es decir debe ser multiplataforma y más si es bajo plataformas de código abierto.
- Procesamiento: un controlador funciona con procesos múltiples y monoprocesos, todo depende de la capacidad de su procesamiento, por tanto, es bueno aplicar un controlador de procesos múltiples en redes empresariales y monoproceso en redes pequeñas.

Se dispone de herramientas para la evaluación de controladores de red SDN basados en pruebas de rendimiento, escalabilidad, disponibilidad y seguridad.
Entre las herramientas para la evaluación de los controladores SDN, para [20], se despliega dos herramientas muy efectivas las cuales son:

Cbench cbench (controler benchmarker) se utiliza para monitorear controladores OpenFlow por medio de la generación de eventos, esta herramienta emula número configurables de switch OpenFlow los que se comunican con el controlador para medir aspectos de rendimiento y latencia. Básicamente cada switch envía mensajes al controlador, espera que las respuestas sean apropiadas y registra estadísticas de la diferencia de tiempo entre los pedidos y respuestas, así como otras características de desempeño.

Hcprobe escrita en haskell, dispone de escenarios para pruebas de control, tiene la capacidad de emular una gran cantidad de switch y host conectados a un controlador. Se puede con esta herramienta de unir patrones para generar mensajes OpenFlow, perfiles de tráfico entre otras cosas. Dispone de características como:

- generación de paquetes y tablas de red.
- Ejecución de lenguaje de alto nivel.
- presencia de una api para proyectos personalizados.
- un lenguaje específico de dominio embebido (EDSL) para la instauración de pruebas.

De acuerdo a [21] , mediante un análisis metodológico se procede a elegir un controlador que tenga prestaciones para un servicio empresarial, el mismo que se muestra en la tabla 2.2.1.

Tabla 2.2.1. Características de los controladores de Redes Definidas por Software

Características	Meridian	Rosemary	ONIX	HiperFlow	SMart-Light	Fleet	ElastiCon	NOX (-MT)	POX	Maestro	Pane	Open MUL	Open IRIS	Beacon	Active Fabric Controller	Trema	Programable Flow	Disco	Yanc	Beehive	RUNOS	LOOM	IBM SDN VE	Faucet	Open Contrail Controller	North Star	Blue Planet SDN Controller	Ryu NOS	Floodlight	HP SDN VAN Controller	ONOS	OpenDaylight	Big Network Controller	Cisco Open SDN Controller (APIC)	Huawei SDN Agile Controller
V. OpenFlow	V 1.0, 1.3	V 1.0, 1.3	V 1.0	V 1.0	v 1.3			V 1.0	V 1.0, 1.1, 1.2	V 1.0	V 1.0	V 1.0, 1.3, 1.4	V 1.0, 1.1, 1.2, 1.3	V 1.0	v 1.3	V 1.0, 1.3	V 1.0, 1.3	V 1.0	V 1.0, 1.1, 1.2, 1.3	V 1.0, 1.1, 1.2	V. 1.0, 1.3	V 1.3, 1.4	V 1.0, 1.3	V 1.3				V 1.0, 1.2, 1.3, 1.4, 1.5	V 1.0, 1.1, 1.2, 1.3, 1.4, 1.5	V 1.0, 1.3	V 1.0, 1.3	V 1.0, 1.3, 1.4	V 1.0, 1.1, 1.2, 1.3, 1.4, 1.5	V 1.0, 1.3	V 1.0
API (Sur)	OpenFlow	OpenFlow, XMPP	OpenFlow, OVSDB, IS-IS, OSPF	OpenFlow	OpenFlow		TCP	OpenFlow, TCP, SNMP	OpenFlow, TCP, OVSDB	OpenFlow, TCP	OpenFlow, MPLS, 4D	OpenFlow, OVSDB, OF-Config, Netconf	OpenFlow, OVSDB, SNMP, BGP, PCEP, LISP	OpenFlow API (OpenFlow), TCP, Beacon Datapath API	OpenFlow, TCP	OpenFlow, TCP	OpenFlow, TCP	OpenFlow, OSPF, BGP, RSVP	OpenFlow, LLDP	OpenFlow	OpenFlow, BGP	OpenFlow	OpenFlow, PCEP, BGP, LISP, DOVE (Distributed Overlay Virtual Ethernet)	OpenFlow, BGP, LACP, ARP	BGP, Netconf, SNMP, XMPP (Canalde Control de Vrouter),	BGP, ISIS, OSPF, PCEP, Netconf	OpenFlow, MPLS, Netconf, SNMP, BGP	OpenFlow, Netconf, Vrrp, Netflow, OF-Config, OVSDB, Sflow	OpenFlow, Indigo Agent and Oxygent (Agente con libreérias y lenguajes para accedera múltiples Switch)	OpenFlow, L3 Agent, L2 Agent	OpenFlow, Netconf, PCEP, OVSDB, BGP, P4, TL1, SNMP	OpenFlow, OVSDB, SNMP, PCEP, BGP, YANG, IISP, NETCONF client, SNMP, COAT, LACP, Cisco Opflex, CAPWAP, OF-Config, P4, SXP, USC, PCMM, COPS	OpenFlow, BGP, OSPF	OpenFlow, Cisco Opflex, Netconf, BGP-LS, PCEP, OVSDB	OpenFlow, Netconf, PCEP, BGP-LS, SNMP, IGP, OVSDB
API (Norte)	REST API	REST API	NVP, NBAPI, ONIX NIB API		REST API	REST API	REST API	REST API	Pythonic (REST API)	REST API	REST API	REST API	REST API	REST API, REST WS	REST API	REST API	REST API	REST API	REST API , File System	REST API, JAVA RCP	REST API	JSON	SDN-VE North API (REST API)	REST API	REST API	REST API	REST API	REST API	REST API, Java, RPC, Quantum	REST API, Java API (OSGI)	REST API, OSGI framework	REST API, Java API (OSGi), Restconf, XMPP, Maven	REST API, Java	REST API	REST API
Interfaz	WEB GUI	CLI	GUI		CLI			CLI WEB, GUI (Python, QT4)	WEB GUI (Python,QT4)	CLI, WEB GUI	CLI	CLI, WEB GUI	CLI, WEB GUI	CLI, WEB GUI	WEB GUI	CLI	CLI, GUI	GUI	CLI	CLI	CLI, WEB GUI	CLI	CLI, WEB GUI	CLI, WEB GUI	CLI, WEB GUI	WEB GUI	CLI	WEB CLI, GUI básica	CLI, WEB GUI	GUI (Shell)	CLI, WEB GUI	CLI, WEB GUI	CLI, WEB GUI	WEB GUI	CLI, WEB GUI
Aplicación Enrutamiento			Enrutamiento					Enrutamiento, STP básico, OpenRoads (integración con redes fijas y móviles)	Enrutamiento, Balanceo de carga, STP, DHCP, NAT, ARP	Enrutamiento, STP		PRISM APP (enrutamiento), NAT	Enrutamiento, Balanceo de carga	IRouting Engine interface (Enrutamiento), Balanceo de carga	Enrutamiento, Balanceo de carga, DHCP, QoS, Optimización de trafico	Enrutamiento	Enrutamiento, Calidad de Servicio			Enrutamiento	Enrutamiento, NAT, DHCP, QoS		Enrutamiento, Balanceo de carga, STP	Enrutamiento	Enrutamiento, Balanceo de carga	Enrutamiento, Balanceo de carga	Enrutamiento	Enrutamiento, Calidad de servicio, STP	Enrutamiento, Virtual Switch, Balanceo de carga, Calidad de servicio, NAT, Balanceador de costos, DHCP, Proxy ARP, QoS, SE-Floodlight, HAND (Controlador de red basado en métricas)	Enrutamiento (SPF)	Enrutamiento	Enrutamiento (SPF), Balanceo de carga	Enrutamiento, Virtual Switch, Calidad de servicio, Balanceo de carga, VLAN, NAT	Enrutamiento, Balanceo de carga	Enrutamiento, NAT, Calidad de servicio, Balanceo de carga
Aplicación Medición	Monitoreo, Topología	Gestión de recursos	Monitoreo, Topología		Topología			Monitoreo, Topología	Monitoreo, Topología	Monitoreo, Topología		Topología, Gestión de estadísticas	Monitoreo, Topología	Monitoreo, ITopology interface (Topología)	Monitoreo, Topología	Monitoreo, Topología	Monitoreo, Topología	Monitoreo, Topología	Monitoreo, Topología	Monitoreo	Monitoreo, Topología, Gestión de estadísticas		Monitoreo, Topología, Gestión de estadísticas, eventos y rendimiento		Monitoreo, Gestión de estadísticas	Monitoreo, Topología, Gestión de estadísticas	Gestión de estadísticas, Automatizaci ón de uso recursos	Monitoreo, Topología	Monitoreo, Topología	Monitoreo, Topología	Monitoreo, Topología	Monitoreo, Topología, Gestión de estadísticas y equipos	Monitoreo, Topología, Gestión de estadísticas	Monitoreo, Topología, Gestión de estadísticas	Monitoreo, Topología, Gestión de ancho de banda y de trafico
Aplicación Seguridad		Aislamiento y Monitoreo de aplicaciones, Control de acceso y autenticación, Firewall	Gestión de fallos, VPN, VLAN, Ethane aplication (Seguridad en redes empresariales)	WheelFS (Gestión de fallos)	Zookeper (Consistencia de la información de la red)	Autenticación de controlador, Gestión de fallos, Seguimiento del comportamie nto de los controladores		Autenticación de usuario, FortNox (resuelve conflicto de reglas)	Firewall	Autenticacióónde equipos, Hipervisor			Firewall, Gestión de fallos	Firewall, VM Security, Open VPN, Recuperación de redes, Sistemas de protección, VLAN OpenVAS (escáner de vulnerabilidad es)	VLAN, Autenticación de Usuario, Gestión de fallos, Recuperación de redes	VLAN	VLAN, VPN	Gestión de fallos	SSHFS (Seguridad acceso remoto); WheelFS (Consistencia en la distribución de reglas)	Gestión de fallos	Autenticacióny control de usuarios, Firewall, VPN		Autenticación y control de usuarios, VPN, VLAN, Gestión de fallos	Autenticación y control de usuarios	VLAN, Firewall, Eth VPN, Gestión de fallos y re-enrutamiento de paquetes	Gestión de fallos, Autenticación de Usuario, VPN	Seguimientode aplicaciones	Firewall, Gestión de fallos, VLAN, Snort (detección de intrusos)	ACL, Firewall, Autenticación , autorización y seguimientode aplicaciones, Detección de anomalías, VLAN, Gestión de fallos	Autenticación de usuario y de aplicaciones, Sistemas de protección (2n+1), ACL	Gestión de fallos	Autenticación, autorización y limitación de Administrador es de red	Gestión de fallos, Autenticación de usuario, Seguimiento de aplicaciones	Autenticacióny seguimientodel comportamie nto de usuario	IP sec VPN, Autenticació n y control de usuarios; Gestión de fallos
Integración (Nube y Virtualización)	OpenStack, IBM Smart Cloud Provisioning		DVS (Virtualizació n de la red)					OVN (framework de virtualización)	OVS (Open Virtual Switch)			OpenStack		OpenStack, Open Nèbula	OpenStack, NFV	OpenStack	OpenStack, Center Virtual Machine Manager (Microsoft)				OpenStack		OpenStack	NFV	OpenStack, CloudStack, Amazon Web Services, OpenNFV	OpenStack	Cloud, NFV	OpenStack	OpenStack	OpenStack	OpenStack, OPNFV	OpenStack, OPNFV, ONAP	OpenStack, Nutanix	OpenStack, OPNFV, ONAP	OpenStack, NFV
No. Flujos Soportados		10 M/s	2.2 M/s	30 m/s	367 m/s			5.3 M/s (NOX-MT), 30 m/s (NOX Classic)	35 m/s	4.8 M/s		2.7 M/s	5 M/s	13.8 M/s	160 m/s		200 m/s			200 m/s	8 M/s								20 mil/s	2.5 M/s	2.3 M/s	1 M/s	106 m/s	2.5 M/s		300 m/s
Código Abierto	Si	No	No	No	Si			Si	Si	Si	Si	Si	Si	Si	No	Si	Si	No	No	Si	Si	Si	No	Si	Si	No	No	Si	Si	No	Si	Si	No	No	No
Sistemas Operativos	Basados en Cloud	Linux		Linux	Linux			Linux (Ubuntu, Debian, Redhat, Gentoo)	Linux, MAC OS, Windows	Linux, MAC OS, Windows	Linux, MAC OS	Linux	Linux, MAC OS, Windows	Linux, MAC OS, Windows, Android móvil	Linux	Linux	Linux	Linux	Linux	Linux	Linux	Linux	Linux	Linux	Linux	Linux		Linux, Windows, Android, MAC OS	Linux, MAC OS, Windows	Linux	Linux, MAC OS, Windows	Linux, MAC OS, Windows	Linux	Linux	Linux
Multihilos	Si	Si	No	Si	Si			Si (NOX-MT)	No	Si		Si	Si	Si		Si	Si	Si		Si	Si	Si	Si	Si	Si			Si	Si	Si	Si	Si	Si	Si	Si
Consistencia	No	Alta	Alta	Débil	Alta	No	Débil	No	No	No	Media	No	Alta	No	Media	No	Alta	Débil	Débil	No		Alta				No			No	Débil	Alta	Débil	Media	Débil	
Ambientes de Uso	Redes pequeñas, Infraestructura en la nube,	Redes empresariale s, Data center	Redes empresariales, Data center, Infraestructura en la nube	Redes pequeñas,	Redes pequeñas	Redes pequeñas	Redes pequeñas	Redes empresariales	Redes pequeñas	Redes empresariale s, Data center	Redes pequeñas	Redes empresariales, Data center, infraestructura en la nube	Redes empresariales	Redes empresariales, Infraestructura en la nube	Redes empresariales, Infraestructura en la nube	Redes empresariales, Data center, Infraestructura en la Nube	Redes empresariales, Data center, Infraestructura en la Nube	Redes empresariales	Redes pequeñas	Redes pequeñas	Redes empresariales, Data center, Infraestructura en la Nube	Redes pequeñas	Redes empresariales, Infraestructura en la nube	Redes pequeñas	Redes empresariales, Infraestructura en la nube	Redes empresariales, Infraestructura en la nube	Redes pequeñas, Infraestructura en la nube	Redes pequeñas, Data center, Infraestructura en la nube	Redes empresariales, Data center, Infraestructura en la Nube	Redes empresariales, Infraestructura en la nube	Redes empresariales, Data center, Infraestructu ra en la nube	Redes empresariales, Data center, infraestructura en la nube	Redes empresariales, Infraestructura en la nube	Redes empresariales, Infraestructura en la nube	Redes empresarial es, Infraestruct ura en la nube
Distribuido o Centralizado	Centralizado	Centralizado	Distribuido plano	Distribuido plano	Distribuido Plano	Distribuido jerárquico	Distribuido	Centralizado	Centralizado	Centralizado	Distribuido plano	Distribuido	Distribuido jerárquico	Centralizado	Distribuido jerárquico	Centralizado	Centralizado	Distribuido plano	Distribuido plano	Distribuido jerárquico	Distribuido plano	Distribuido plano	Centralizado	Distribuido	Distribuido		Centralizado	Centralizado	Distribuido	Distribuido Plano	Distribuido plano	Distribuido	Distribuido plano	Distribuido
T. a Fallos	No	No	Si	Si	Si	No	Si	No	No	No	Si	No	Si	No	Si	No	No	Si	Si		Si	Si	No	No	Si	Si	Si	No	No	Si	Si	Si	Si	Si
Fabricante	IBM T. J. Watson Research Center	SRI International	Nicira Networks, NTT OSRG y Google	Universidad de Toronto	Universidad de Lisboa	Carnegie Mellon University		Nicira Networks, Universidad de Stanford	Nicira Networks	Universidad de Rice	Universidad de Brown	Open Mul Fundation	ETRI	Universidad de Stanford	Dell	NEC Labs	NEC Labs	Thales Community and Security	Universidad de Colorado	Universidad de Toronto	ARCCN, Universidad estatal de Moscú	AGH Universidad de Ciencia y Tecnología, Polonia	IBM	Universidad de Wikato, Nueva Zelanda	Juniper Networks	Juniper Networks	Ciena Inc	NTT OSRG, VA Linux	Big Switch Networks (Proyecto Floodlight)	Hewlett Packard	ON Lab	Fundación Opendaylight (Múltiples fabricantes)	Big Switch Networks	Cisco Sistems	Huawei Tecnologies

Documentación	Pobre	Pobre	Pobre	Pobre	Pobre	Pobre	Pobre	Buena	Buena	Buena	Pobre	Pobre	Buena	Buena	Buena	Buena	Buena	Pobre	Pobre	Pobre	Alta	Pobre	Buena	Buena	Pobre	Buena	Buena	Alta	Alta	Alta	Alta	Alta	Alta
Licencia		Propietario	Propietario	Propietario	GPLv2L			GPLv3	GPLv3	LGPLv2.1	BSD 3.0	GPLv2	Apache 2.0	GPLv2	Propietaria	GPLv2	GPLv2	Propietaria	Propietaria	Apache 2.0	Apache 2.0	apache 2.0	Propietaria	Apache 2.0	Apache 2.0	Propietaria	Propietaria	Apache 2.0	Apache 2.0	Propietaria	Apache 2.0	EPL V1.0	Propietaria	Propietaria	Propietaria
Lenguaje	Java	C	on, C++,Java	C++	Java		Java	C++	Python	Java	Haskell	C	Java	Java	Linux	C, Ruby	C, Ruby	Java	C, C++	C++, C, ython, Go (Beehive)	C++	Erlang	Java	Python	++, Java,Python			Python	Java	Java	Java	Java	Java	Java	Java
Versión	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0		1.0	2.08	1.0		1.0	5.0	1.1		1.0	2.0			1.2	1.0			1.3	1.2	2.7.16	1.10.0	1.3	4.7	1.2	3.0
Pagina	No tiene	No tiene	No tiene	No tiene	No tiene	No tiene	No tiene	https://github. com/noxrepo/ nox- classic/wiki	https://noxrep o.github.io/pox- doc/html	http://zhengc ai.github.io/m aestro- platform	http://pane.cs .brown.edu	tp://www.op enmul.org	tps://openiri s.etri.re.kr	https://openfl ow.stanford.e du/display/Be acon/Home.html	https://www.d ell.com/learn/ co/es/cobsdt1 /networking?s =bsd&~ck=mn	https://trema. github.io/trema	https://www.n ecam.com/PFlow	http://anr- disco.ens- lyon.fr	https://github. com/ngn- colorado/yanc	https://github. com/kandoo/ beehive- netctrl	https://arccn. github.io/runos	https://github. com/FlowFor warding/loom	https://www.ib m.com/servic es/network/so ftware- defined	https://faucet. readthedocs.i o/en/latest/int ro.html ; https://github. com/faucetsd n/faucet	http://www.op encontrail.org	https://www.ju niper.net/doc umentation/e n_US/northst ar3.0.0/inform ation- products/path way- pages/3.0/nor thstar-user- guide.html	https://www.bl ueplanet.com	rp://osrg.git hub.io/ryu	http://www.pr ojectfloodlight .org	http://h17007. www1.hpe.co m/us/en/netw orking/library/i ndex.aspx?ca t=sdn#.XIsD WShKg2w	tps://onosp roject.org	https://www.op endaylight.org	https://www.bi gswitch.com/t ags/big- network-controller	https://www.ci sco.com/c/en/ us/products/cl oud-systems-management/ open-sdn-controller/ind ex.html	https://e.hu awei.com/e s/products/e nterprise-networking/ sdn- controller
Actualización Pagina	N/A	N/A	N/A	N/A	N/A	N/A	N/A	2012	2015	2015	2013	2015	2015	2017	2019	2017	2016	2017	2016	2016	2016	2016	2018	2019	2019	2019	2019	2017	2018	2019	2019	2019	2019	2019

Fuente: [21]

2.2.8. **Sistema trampa o señuelo *honeypot***

Para [5] un honeypot (tarro de miel en inglés) o sistema trampa es una herramienta de seguridad informática desplegado en una red de datos y dispuesto a ser atacado, con el fin de obtener información del atacante y utilizar estos datos para la toma de decisiones ante la presencia de incidentes. Pero la función específica es atraer y analizar intrusiones ejecutados por bots o hackers, es tratar de conocer sus modelos de ataque, componer diccionarios para acumular las palabras que ejecutan los atacantes. Se podría resumir diciendo que se conoce al personaje hostil y su perfil.

Un honeynet podría ser un dispositivo sencillo como un dispositivo informático que analice el flujo de datos entrante y saliente hacia el internet u otra red privada, el que cuenta con vulnerabilidades del sistema operativo en algún protocolo, programa o cualquier otro módulo para de esta forma llamar la atención del atacante.

Estos dispositivos cubren varios servicios que los atacantes escogen para realizar su ejecución, estos servicios de interés para los atacantes son, ftp, http, smb, mysql, etc. Y existe nuevas opciones de servicios en nuevos sistemas trampa, estos dispositivos no solo están diseñados para protegerse de un posible ataque, sino para servir de señuelo invisible al atacante. Existen tres tipos de honeypot dependiendo de la interacción, baja, media y alta, cada una de estas dispone de características definidas.

2.2.9. **Tipos de honeypot**

Honeypot de investigación estos honeyports se ejecutan con recursos educativos y para realizar demostraciones de investigación, el n de estos es el estudio de patrones de amenazas e intrusiones de todo tipo. La mayoría de estos dispositivos son generados para recolectar información de los atacantes. Con esta información recogida se evidencia el tipo de amenazas y cómo funcionan, así también ganar terreno a los bandidos cibernéticos. [22]

Honeynet de producción son dispositivos generados para proteger entidades organizacionales en ambientes reales. Son equipos que se encuentran en funcionamiento 365 días del año, cada vez van ganando más confianza de por las

herramientas de detección que pue- den ofrecer y el complemento que prestan a la seguridad de la red. Se puede observar los sistemas que usan los intrusos o la explotación que realizan, pero es casi imposible que se pueda aprender cómo se comunican entre sí o de qué forma se desarrolla las herramientas utilizadas en el ataque. [22]

Honeypots por su nivel de interacción se basan en el nivel de libertar que dispone el atacante con el equipo honeypot, por tanto, mientras más tiempo de interacción exista más información se consigue obtener del ataque.

- honeypots de baja interacción: estos equipos emulan servicios y sistemas operativos, la libertad del atacante está limitada al nivel de emulación. Son fáciles de implementar y su riesgo es casi nulo. Un ejemplo de estos equipos puede ser un servidor ftp que está habilitado con el puerto 21 y que disponga de algún usuario habilitado o algún comando activo, pero que no existe riesgo por estar enlazado a un servidor irreal. La desventaja es que la información también es limitada por el hecho de disponer de un servicio básico. [22]
- honeypot de alta interacción: la implementación de estos equipos trampa son más complejos ya que requieren la utilización de sistemas operativos y servicios reales corriendo sobre hardware real. Es decir, si se quiere un desplegar un honeynet hay que hacerlo sobre un servidor Linux que ejecute un servidor ftp como ejemplo, este se convierte en un servidor ftp real. En estos honeynet se captura gran cantidad información que revele el modo de operación del atacante ya que el atacante se encuentra con un sistema real y por tal razón se consigue analizar todas las actividades que realiza sobre este equipo. [22]

2.2.10. **Red trampa o honeynet**

Para [5], un honeynet es como una red de sistemas trampa o honeypot, que compone de software y hardware, es usado como un recurso de seguridad cuyo valor reside en un sistema o red que se está probando, atacando o comprometiendo, con el n de distraer la atención del atacante y evidenciar su estrategia de irrupción.

Un honeynet debe cumplir dos requerimientos básicos, debe ser realmente útil y

debe proporcionar información valiosa. [1]

CAPITULO III

3.1.Metodología

La presente investigación es de tipo experimental, con diseño cuantitativo y explicativo, aplicando técnica comprobatoria, observación in situ y análisis técnico sobre la información de datos que se involucran en la implementación de una honeynet y las herramientas necesarias para su aplicación práctica sobre una red SDN.

3.2.Ubicación

El presente trabajo fue desarrollado en la ciudad de Ambato, ubicado en el centro Sur de la Ciudad. Para realizar la investigación se escogió a la empresa proveedora de servicios de Internet (Clicknet S.A debido a las prestaciones que entrega la empresa de probar en su infraestructura de red.

3.3.Equipos y Materiales

Los equipos y materiales utilizados para el despliegue de la investigación lo muestra la tabla 3.3.1.

Tabla 3.3.1. Materiales utilizados para el proyecto

Equipos y materiales	**Valor (USD)**
Equipos	$1500
Software	$250
Materiales	$300
Gastos varios	$400
Total	$2450

Fuente: Elaborado por el Investigador

3.4. Tipo de Investigación

3.4.1. Investigación Bibliográfica

El trabajo se inclinó hacia la metodología de investigación bibliográfica ya que la información adquirida para la implementación se ha encontrado de manera dispersa en varios artículos científicos, publicaciones, trabajos de titulación de maestrías, libros, manuales de fabricantes y desarrolladores.

3.4.2. Investigación Exploratoria

Se definió el trabajo como de investigación exploratoria ya que inicia desde un ámbito general de dos tecnologías para llevar a una realidad determinada. Adicional se encuentra con escasos estudios previos al tema, hasta la fecha no se ha encontrado pruebas realizadas con arquitecturas de red físicas, la mayor parte de investigaciones han sido con dispositivos virtualizados o de laboratorio.

3.5. Prueba de hipótesis

El presente proyecto de investigación, por su naturaleza «Despliegue de un honeynet basado en redes definidas por software para un ISP», le hace referencia a una modalidad exploratoria. En la investigación se hizo referencia a las tecnologías «Honeypot y SDN» son relativamente nuevas con el objetivo de mejorar las tecnologías tradicionales los mismos que continúan en fase de desarrollo basado en seguridad y redes definidas por software, la relación entre estas dos tecnologías convierte en un proyecto relativamente nuevo.

El trabajo de investigación intentó evaluar los beneficios que se adquiere de cada una de ellas; bajo un ambiente controlado se realizó un análisis experimental para la obtención selecta sobre la interacción, gestión y control de manera unificada para obtener debilidades o beneficios en tiempo real, y con dispositivos ya en funcionamiento.

Hipótesis

De acuerdo a (Sampieri H 1997 Pág. 13) los estudios de género exploratorio se efectúan, normalmente cuando el objetivo es examinar un tema o problema de

investigación poco estudiado o no abordado antes y por lo tanto carecen de hipótesis.

Variables

Ya que este proyecto de investigación no dispuso de hipótesis, no es posible considerar variables de operacionalización.

3.6. Población y muestra

Siendo el presente trabajo de investigación, no fue necesario definir población y muestra. Los resultados que se obtienen en el proceso de prueba se han considerado para el estudio y desarrollo.

CAPÍTULO IV

4.1. Determinación de situación actual de la infraestructura de la red de la empresa Clicknet S.A.

De acuerdo a [23], Clicknet es una empresa de Telecomunicaciones, creada en la provincia de Cotopaxi en el año de 2011, con el objetivo de brindar servicios de Internet y Transmisión de Datos para hogares y empresas.

Actualmente la oficina Matriz se encuentra en la ciudad de Ambato, provincia de Tungurahua, dirección: Antonio José de Sucre y Juan Montalvo, Edificio Criollo 3er Piso. posee cobertura en las provincias de Cotopaxi, Tungurahua, y Pastaza.

Clicknet dispone de un organigrama departamental (técnico) cómo el que se muestra en la figura 4.1.1.

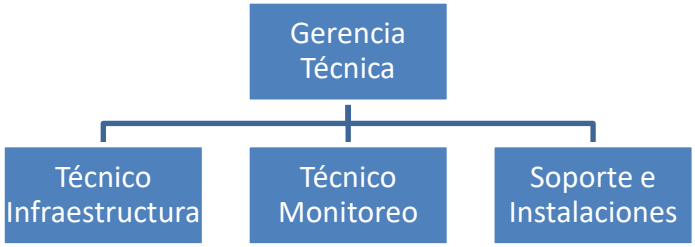


Figura 4.1.1. Organigrama técnico Clicknet

Fuente: Elaborado por el investigador

La infraestructura de equipamiento depende de su importancia y uso, dentro del data center se dispone de servidores como de muestra en la tabla 4.1.1

Tabla 4.1.1.Servidores de data center

DESCRIPCIÓN SERVIDOR	IMPORTANCIA
Servidor Monitoreo	Alta
Servidor de Gestión de red	Alta
Servidor de Base de datos y Aplicaciones	Alta

Fuente: Elaborado por el investigador

Estos servidores se encuentran ubicados en un Centro de Datos en la ciudad de

Ambato.

La distribución del servicio en las diferentes ciudades hace que se disponga de varios nodos de comunicaciones, como se indica en la tabla 4.1.2.

Tabla 4.1.2 Nodos de comunicación

Provincia	Ciudad
Cotopaxi	Latacunga
Tungurahua	Ambato
Tungurahua	Píllaro
Tungurahua	Patate
Pastaza	Puyo
Pastaza	10 de Agosto

Fuente: Elaborado por el investigador

La arquitectura de red en cada ciudad es similar de modo jerárquico, es decir: Núcleo, Distribución y Acceso, se dispone de equipos en un 99% de marca Mikrotik, es decir desde el router de frontera hasta equipo final o de cliente.

En su totalidad, los routers de borde, routers de núcleo, routers de distribución, routers de acceso, switchs y suscriptores, son de marca Mikrotik, a excepción de la última milla en fibra óptica que es de marca Huawei (trabajan en capa 2, con *VLANs*).

La topología estrella usada en todas las ciudades en la que se brinda el servicio es la que se muestra en la figura 4.1.2.

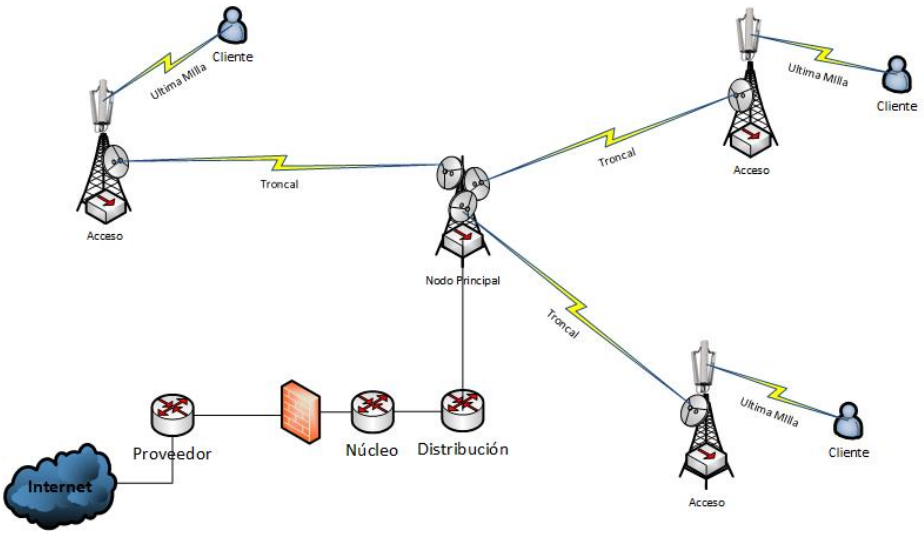


Figura 4.1.2. Ejemplo de arquitectura de red de la empresa Clicknet

Fuente: Investigador

La distribución interna se ejecuta con equipos de radio o enlaces de fibra hacia los nodos, los equipos utilizados para la transmisión entre nodos es equipos de radio

Mikrotik, y con fibra directamente con tranceivers de cobre a óptico y conectados entre routers, la interconexión entre nodos para un sistema de gestión se presenta por medio de túneles de datos hacia el Data Center de Ambato, los enlaces de Internet se presentan en cada nodo principal de cada ciudad por medio de un proveedor.

Se dispone de un estudio anterior [23] para la gestión de la red en la cual se evidencia que los dispositivos utilizados en su mayoría son de marca Mikrotik, por tanto, se confirma lo indicado en el trabajo citado, ya que se encontró en su mayoría la marca referida para el transporte de datos. En la tabla 4.1.3 se muestra la cantidad de equipos que existe actualmente dentro de la infraestructura.

Tabla 4.1.3. Cantidad de equipos existentes de acuerdo a la marca

Marca	Ciudad	Cantidad
Mikrotik	Latacunga	72
Huawei	Latacunga	1
Mikrotik	Ambato	78
VSOL	Ambato	1
Mikrotik	Píllaro	82
Huawei	Píllaro	1
Mikrotik	Patate	40
VSOL	Patate	1
Mikrotik	Puyo	32
VSOL	Puyo	1

Fuente: elaborado por investigador

En su totalidad se dispone de 302 dispositivos RouterOS, 2 Huawei (OLT) y 2 VSOL (OLT), que ratifica en un 99% de equipos de la marca Mikrotik.

Figura 4.1.3. Porcentaje de dispositivos activos en la red

Fuente: Investigador

Basándose en los datos anteriores se debe implementar una red definida por software que es uno de los objetivos del presente proyecto, ajustada en la marca de equipos encontrados.

4.2.Esquema de implementación de la red SDN para la empresa Clicknet

Al contar con dispositivo *core* y de distribución de la marca Mikrotik en cada una de las ciudades se propuso el siguiente esquema de conexión para desplegar la red SDN (ver figura 4.2.1).

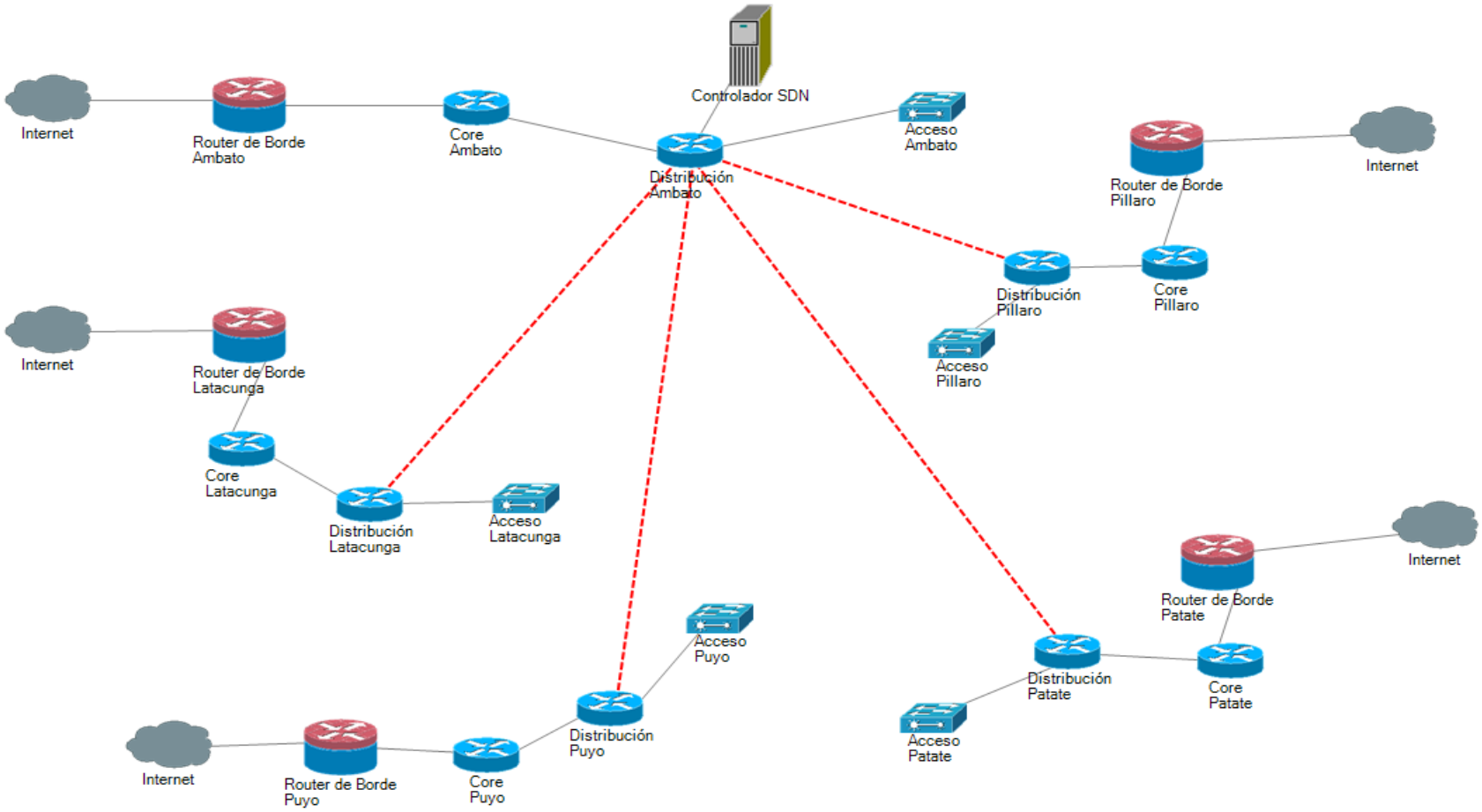


Figura 4.2.1. Red SDN propuesta para toda la infraestructura de la empresa

Fuente: Investigador

4.3. Selección del Controlador SDN

En referencia a la tabla 2.2.1, y de acuerdo a [21] se selecciona el controlador SDN de HPE Virtual Application Networks (VAN) porque, proporciona un punto de control unificado en una red habilitada para SDN, lo que simplifica la gestión, el aprovisionamiento y la orquestación. Esto permite la entrega de una nueva generación de servicios de red basados en aplicaciones. También proporciona interfaces de programación de aplicaciones (API) abiertas para permitir a los desarrolladores crear soluciones innovadoras para vincular dinámicamente los requisitos comerciales con la infraestructura de red a través de programas Java personalizados o interfaces de control RESTful de propósito general. El controlador VAN SDN está diseñado para funcionar en entornos de campus, centros de datos o proveedores de servicios. Las principales características de este controlador según [24] son:

Procesamiento de flujo proactivo. - Permite redes SDN altamente escalables y con orquestación centralizada.

Procesamiento de flujo reactivo. - Permite el monitoreo dinámico de nuevos flujos o puntos finales.

Interfaz gráfica de usuario (GUI). - Facilita la administración del controlador y la documentación de API.

API en dirección norte. - Aprovecha la interfaz extensible RESTful HTTPS del controlador, proporcionar una representación abstracta de la red OpenFlow subyacente y permitir que las aplicaciones externas que se ejecutan por encima del controlador ejerzan un control deliberativo a nivel empresarial sobre la red.

Proporcionar los servicios necesarios para admitir una plataforma de gestión completa como HPE Intelligent Management Center (IMC)

API nativas. - Permitir que las aplicaciones Java se ejecuten dentro del controlador como una colección de paquetes OSGi que permiten el procesamiento de paquetes y eventos de alto rendimiento.

Arquitectura escalable. - Utiliza marcos de base de datos escalables y resistentes, lo que permite la expansión más allá de un solo controlador independiente a un clúster de alta disponibilidad; basado en sistemas de base de datos en memoria de código abierto, incluidos Hazelcast (para una coherencia

estricta), Cassandra (para una coherencia eventual) y una base de datos relacional PostgreSQL, los datos persistentes se pueden compartir entre varios controladores para ofrecer un enfoque de escalamiento horizontal para el control de grandes o redes exigentes.

Alta disponibilidad. -Proporciona un modelo de consistencia activa "2n + 1", que permite que tres controladores administren subconjuntos individuales de la red mientras comparten una vista de red común; la falla de un componente de control genera una respuesta rápida por parte del clúster para proporcionar operaciones de red continuas.

Seguridad del controlador. - Brinda seguridad en múltiples niveles; HTTPS se utiliza para la API REST, y la autenticación de usuarios y aplicaciones se realiza mediante el servicio de identidad de Keystone; Las comunicaciones de controlador a conmutador están aseguradas a través del protocolo de cifrado Transport Layer Security (TLS), como se especifica en el estándar OpenFlow.

Módulo de servicio de enlace. - Utiliza mensajes LLDP para descubrir enlaces físicos entre conmutadores en el dominio de control y supervisa los cambios de estado del puerto y notifica a las aplicaciones sobre cambios de eventos de enlace; También es capaz de identificar enlaces de múltiples saltos donde los dispositivos que no son OpenFlow separan segmentos de red controlados.

Módulo de servicio de topología. - Crea un gráfico de red basado en información del servicio de enlace; identifica puertos, calcula la ruta más corta entre nodos y crea un árbol de transmisión, evitando bucles de red; En versiones futuras, este módulo habilitará servicios de múltiples rutas.

Módulo de servicio del administrador de nodos. - Supervisa paquetes ARP, DHCP e IP desde puertos de borde; permite que el módulo proporcione una memoria caché de direcciones MAC e IP para cada punto final, lo que proporciona la identificación de dispositivos o usuarios conectados a la red.

Módulo de servicio de ruta. - Utiliza la información del nodo y los servicios de topología para programar una ruta L2 unidireccional de extremo a extremo a través del dominio de control para nuevos flujos de red; elimina direcciones de origen desconocido y admite inundaciones para destinos desconocidos; puede desactivarse para el procesamiento normal de paquetes, o ser reemplazado por un programa más sofisticado según lo desee el programador de la aplicación.

Servicio de diagnóstico de ruta. - Valida rutas de red y genera paquetes de

prueba específicos del protocolo (ICMP, DHCP, UDP, TCP, etc.) que se pueden insertar en la red y observar en varios conmutadores a lo largo de la ruta; esto proporciona a los administradores de red la funcionalidad de ruta de rastreo.

Interfaz de control OpenFlow. - Utiliza un enfoque generalizado en la interfaz en dirección sur del controlador para procesar mensajes OpenFlow1.0 y 1.3; esto proporciona un mecanismo eficiente e intuitivo para monitorear y programar varios componentes de la red y para procesar nuevos mensajes de flujo; Los paquetes se traducen en un conjunto de tipos de datos enriquecidos por el controlador, lo que permite que las aplicaciones Java consuman o creen mensajes o paquetes fácilmente. Los controladores Netconf y SNMP en dirección sur también están disponibles.

Procesamiento de paquetes flexible. - Permite un híbrido de procesamiento de paquetes OpenFlow y normal con la arquitectura HP SDN; las listas de control de acceso se aprovisionan de forma centralizada, por ejemplo, mientras que las decisiones de reenvío L2 o L3 se pueden tomar utilizando protocolos de red estándar; Esto permite que los conceptos de SDN se apliquen de manera incremental a la red, comenzando con la aplicación de la política de red y extendiéndose al reenvío basado en excepciones, agregando valor sin reemplazar la conmutación o el enrutamiento tradicionales.

En [21]**,** con base a resultados dentro de un proceso de cálculo de prioridad, se determina como HPE SDN VAN Controller, uno de las mejores opciones para ejecutar como un controlador que mejor se adapta a las necesidades empresariales.

De acuerdo a [25]la multinacional Hewlett Packard, es miembro de ONF, esta sigue una arquitectura de red semejante a la definida por la organización mencionada, ha desarrollado su propio software controlador, para el desarrollo del concepto en aplicaciones y servicios de SDN llamado HP VAN SC (HP Virtual Aplication Networks SDN Controller), dicho controlador es compatible con OpenFlow y varias API´s para que se puedan comunicar entre capas de la arquitectura. Adicional ha generado una tienda de aplicaciones para entregar diversas soluciones para redes SDN, ejecutadas por los mimos desarrolladores de HP, estos cuentan con la herramienta de desarrollo de uso libre de nombre HP SDK (HP SDN Developer Kit), con esto se trata de conseguir compatibilidad con HP SDN VAN, esta herramienta se menciona que dispone de programas API’s ya

desarrollados que disponen de documentación, guías de programación, ejemplos de código y entornos para poder simular pruebas de funcionamiento.

El controlador HPE VAN SDN está diseñado para funcionar en una variedad de entornos informáticos, incluidos campus, centro de datos, proveedor de servicios, nube privada y nube pública. [26]

Según [27] en Mikrotik se consigue aplicar este tipo de redes con el uso del protocolo OpenFlow, este protocolo se presenta únicamente en versión 1.0, en la parte documental indica que este protocolo en los dispositivos RouterOS es de prueba, adicional se debe tener cuidado de no deshabilitar el acceso al dispositivo al configurar OpenFlow, de lo contrario no se podrá acceder nuevamente a este equipo. Por lo mencionado anteriormente mikrotik solo dispone de protocolo OpenFlow en versión 1.0. y HPE VAN SDN tiene soporte versión 1.0 y 1.3.

4.4. Implementación de la red SDN en un banco de pruebas.

Para la implementación de la red SDN se procedió con la ejecución en equipos virtualizados para probar su funcionamiento antes de ingresar a una red en producción, como se muestra en la figura 4.4.1.

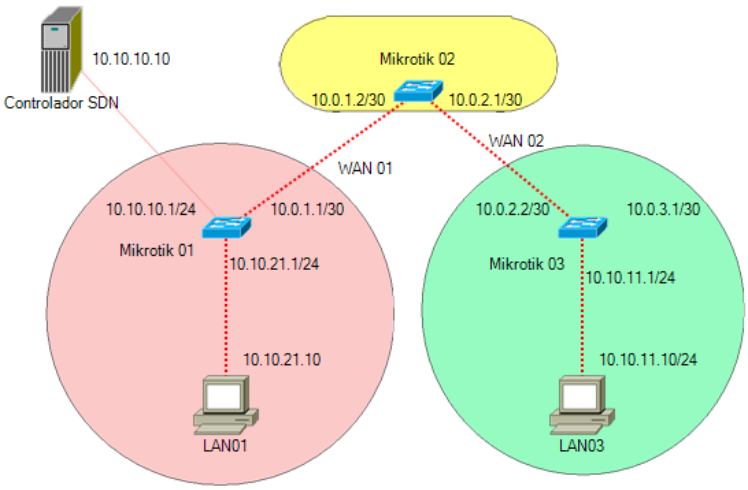


Figura 4.4.1. Esquema de red SDN de prueba en plataforma VirtualBox

Fuente: Elaborado por investigador

Se utilizó para pruebas, software multiplataforma de virtualización bajo

Virtualbox, el mismo que permite arquitecturas x86/amd64, de acuerdo a [23] mikrotik dispone de imagen VDI compatible. Una vez levantado los equipos mikrotik se debe cargar el paquete OpenFlow de manera independiente para disponer del protocolo indicado y poder iniciar con la configuración de la red SDN.

Se ejecuta pruebas sobre una laptop HP con sistema operativo Windows 10, se obtiene el paquete VDI de Mikrotik (https://mikrotik.com/download) para levantar en la plataforma de virtualización. Se designa cuatro routers mikrotik y un controlador HPE VAN SDN, de igual forma se descargar el controlador en la página de HP Aruba (My Networking h10145.www1.hpe.com), en versión OVA para importar como máquina virtual.

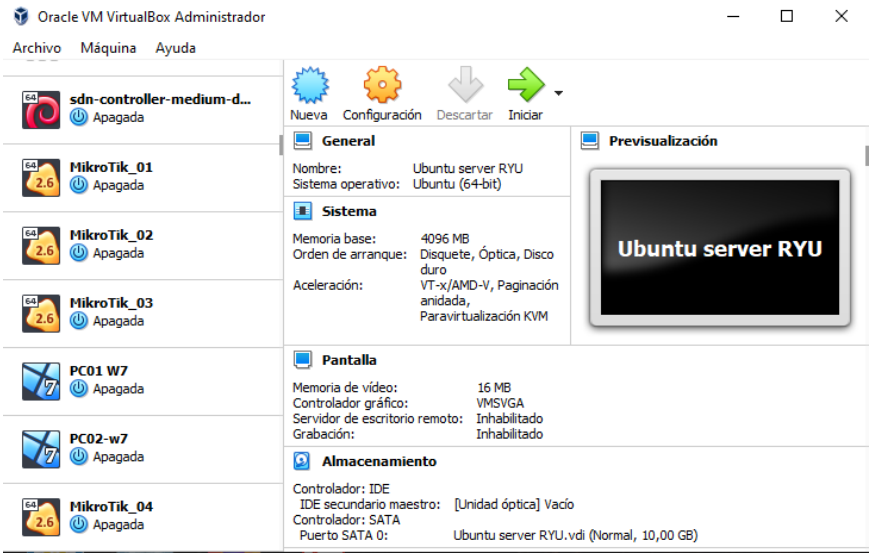


Figura 4.4.2. Plataforma de prueba con equipos virtuales

Fuente: elaboración propia

Cada router mikrotik (virtual) se configura con una interfaz de red para disponer de conexión directa con el equipo físico y se levante con una dirección IP por DHCP del router del que depende la laptop de prueba, para poder gestionar los equipos; otra interfaz para la interconexión entre routers, otra interfaz para conectar el equipo que se hace como cliente y una interfaz para conectar el controlador (en un solo router), como se muestra en la figura 4.4.3.

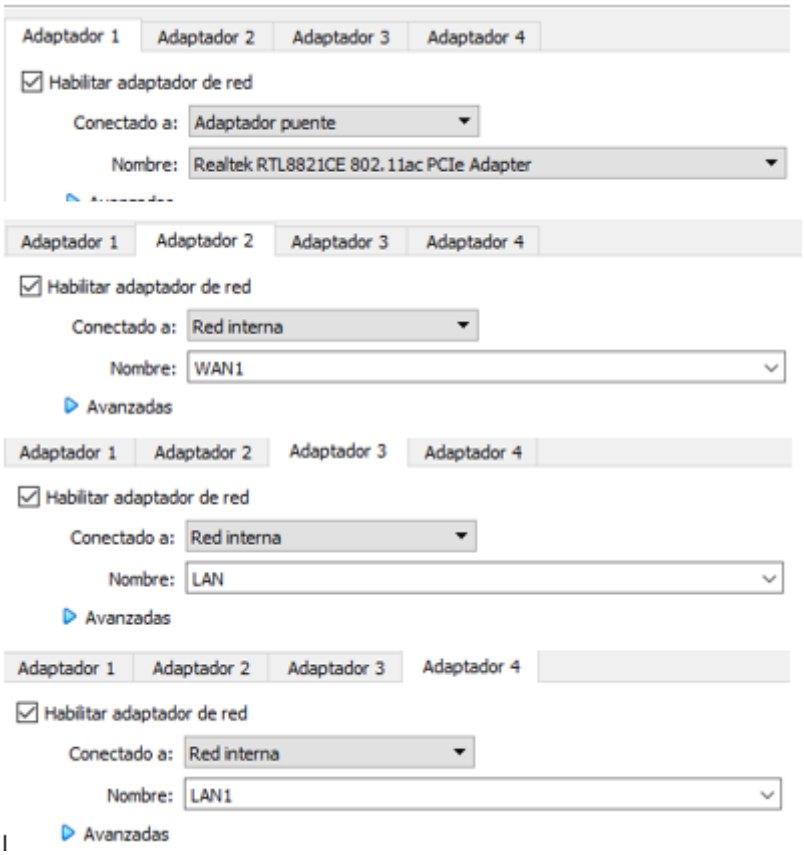


Figura 4.4.3. Configuración de interfaces de red en routers mikrotik

Fuente: elaboración propia

Una vez arrancado el sistema operativo del router mikrotik, no se dispone del protocolo OpenFlow, se observa en el menú izquierdo de los dispositivos.

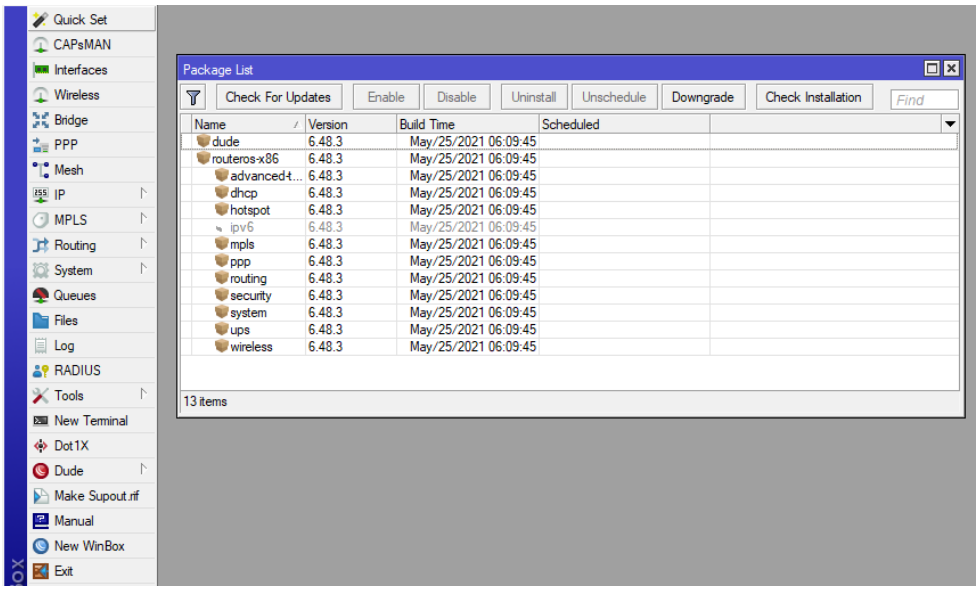


Figura 4.4.4. Menú principal, servicios y protocolos instalados

Fuente: Elaborado por el investigador

Para la descarga del paquete que contiene el protocolo OpenFlow, hay que

hacerlo desde la página web de la marca del equipo, se copia en el router, se reinicia y se dispone en el menú principal el protocolo como se muestra en la figura 4.4.5.

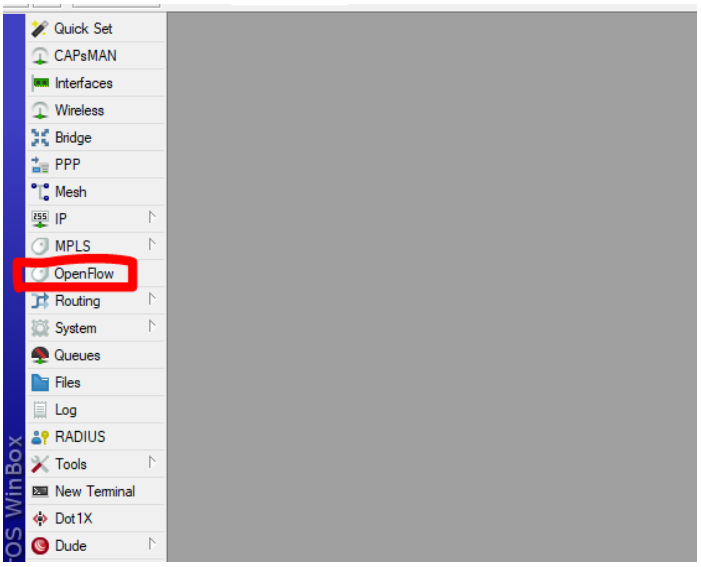


Figura 4.4.5. Router cargado protocolo OpenFlow

Fuente: Elaborado por el investigador

De la misma forma se dispone de versión OVA para el controlador encargado de orquestar la red (HPE VAN SDN) descargado directamente de la página de Aruba HPE como se muestra en la figura 4.4.6.

Figura 4.4.6. Descarga de software para virtualizar el controlador HPE VAN SDN

Fuente: Elaborado por el investigador

Una vez virtualizados los equipos, se configura direccionamiento IP estático en cada router, controlador y PCs, se ejecuta enrutamiento en todos los routers y se levanta el protocolo OpenFlow de manera ordenada a los routers para no quedar desconectado de la red.

El direccionamiento IP se establece como se muestra en la figura 4.5, hay que tomar en cuenta que una vez ejecutado la red SDN se mantienen los protocolos de una red normal, como es enrutamiento, control de AB, QoS, etc. Para habilitar los puertos con protocolo OpenFlow se procede como en la figura 4.4.7, tomando en cuenta la IP del controlador y habilitando los puertos que se requieren que hablen OpenFlow.

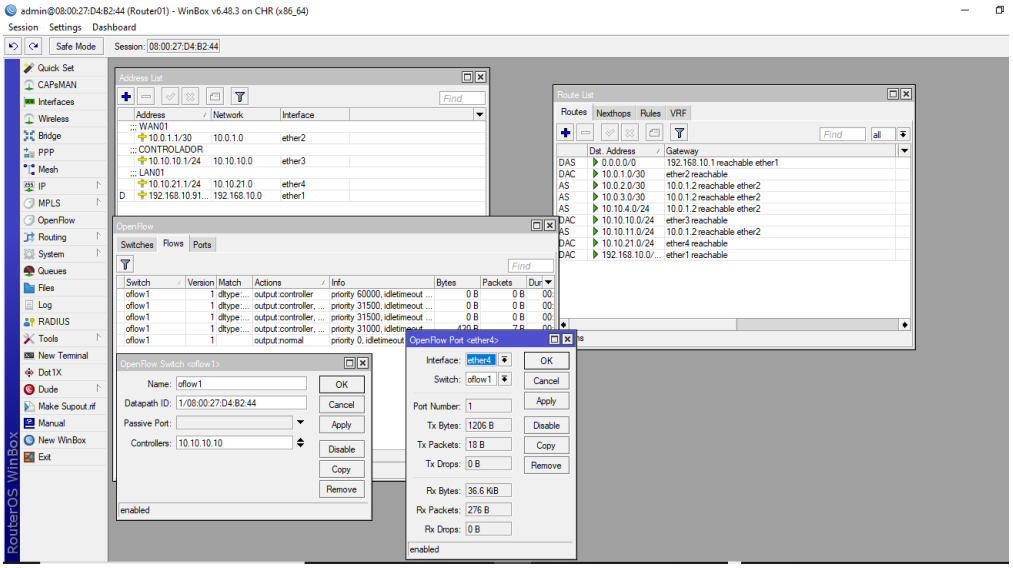


Figura 4.4.7. Configuración de router Mikrotik

Fuente: investigador

Se aprecia en la figura anterior la configuración completa del router, como: direccionamientos IP, configuración de switch OpenFlow, enrutamiento estático, y se observa la generación de flujos que se presentan por el controlador activo. Este controlador se ejecuta bajo plataforma Linux virtualizado que se levanta de manera automática sin previa configuración extra, aparte del direccionamiento IP que requiere para conectarse a la red. Una vez levantado todo, se accede vía IP y puerto 8443 y protocolo https para visualizar la estructura de la red SDN como se evidencia en la figura 4.4.8. que se lo realizó desde la máquina virtual implementada como cliente final.

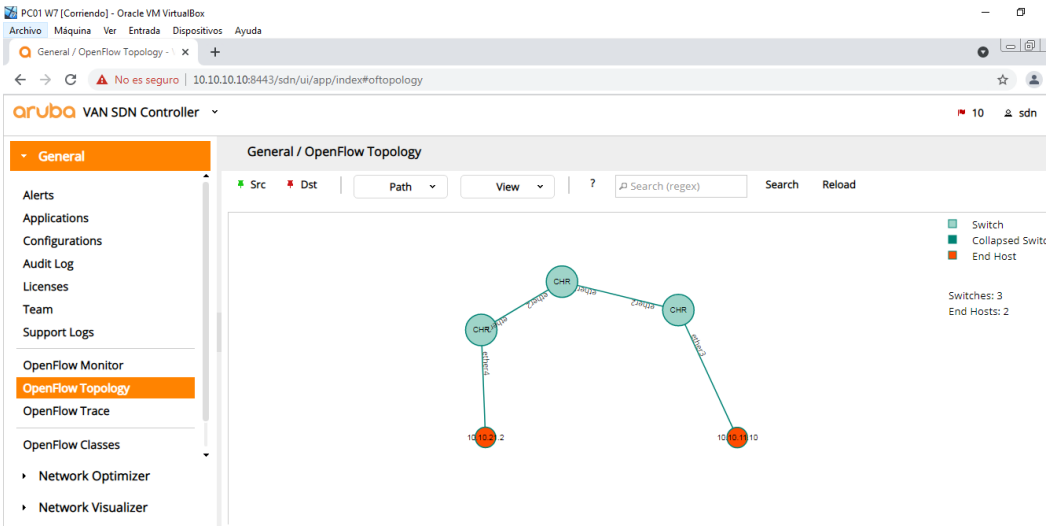


Figura 4.4.8. Controlador HPE VAN SDN ejecutándose OpenFlow versión 1.0

Fuente: investigador

4.5. Implementación de red SDN de la empresa en producción

Una vez puesto en marcha la red SDN bajo una plataforma de dispositivos de la marca mikrotik, se escoge de manera delicada bajo la red de producción de la ciudad de Ambato, los equipos que forman parte de esta red son, router de core, distribución y switchs de acceso.

Para el despliegue se requirió equipamiento físico para el servidor que hace de controlador. Se escogió un CPU que contenga Windows 10 con plataforma VirtualBox de las siguientes características.

- Nombre del SO Microsoft Windows 10 Pro
- Versión 10.0.19043 Compilación 19043
- Fabricante del SO Microsoft Corporation
- Fabricante del sistema BIOSTAR Group
- Modelo del sistema H110MHC
- Tipo de sistema x64-based PC
- Procesador Intel(R) Core (TM) i3-7100 CPU @ 3.90GHz, 3912 Mhz, 2 procesadores principales, 4 procesadores lógicos

- Versión y fecha de BIOS American Megatrends Inc. 5.12, 14/2/2017
- Versión de SMBIOS 3.0
- Versión de controladora integrada 255.255
- Modo de BIOS UEFI
- Memoria física instalada (RAM) 20,0 GB
- Memoria física total 19,9 GB
- Memoria física disponible 10,6 GB
- Memoria virtual total 22,9 GB
- Memoria virtual disponible 13,6 GB
- Espacio de archivo de paginación 3,00 GB
- 2 tarjetas de red físicas 10/100/1000 Realtek y TP-Link

La figura 4.5.1, muestra físicamente el equipo que se asignó para que cumpla con la función de controlador.

Figura 4.5.1. CPU para controlador HPE VAN SDN

Fuente: Elaborado por el investigador

Las características de la máquina virtual para el controlador SDN se presentan con:

- Sistema Operativo Debian 64 bits
- 4 procesadores

- 16 GB en RAM
- 150 GB de Disco Duro
- 1 tarjeta de red física asignada para esta máquina

Una vez implementado el servidor y realizado las pruebas de comunicación entre los dispositivos de la red y el mismo, se levantó OpenFlow de manera ordenada en cada uno de los routers y swichs. Se ha tomado un fragmento de la red para realizar pruebas de funcionamiento.

En la figura 4.5.2, se aprecia la interacción entre el controlador y los dispositivos con protocolo OpenFlow levantados también su topología, puertos conectados, modelo de dispositivos, macaddress, e IP. Adicional se grafica la ruta que siguen los paquetes de un punto inicial a otro. Para acceder al entorno visual, basta escribir la IP del servidor, con el puerto 8443 y protocolo https.

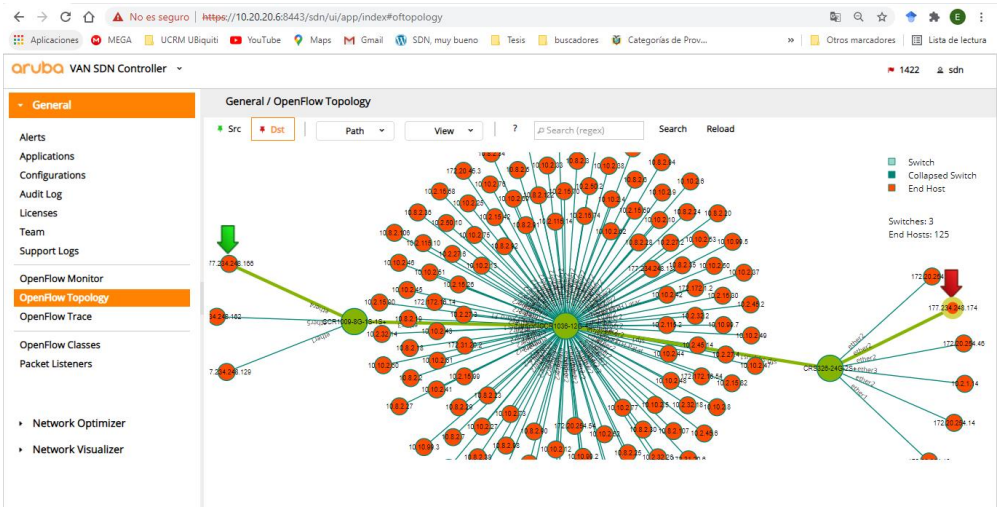


Figura 4.5.2. Controlador SDN en producción

Fuente: Elaborado por el investigador

4.6. Implementación de Honeynet en red SDN establecida

Dentro de esta topología se está tomando en cuenta el router de borde mismo que entrega el servicio de Internet por medio de sus IPs públicas hacia la red de distribución, en este segmento es donde se debe analizar los posibles riegos de ataque externo hacia los dispositivos internos que quieran degradar el servicio, según historial encontrado dentro de la empresa se ha evidenciado de forma regular este tipo de incidencias.

Ya que la empresa no dispone de equipamiento que realice seguridad perimetral especializada en su borde por el costo que implica adquirirlo, se han mantenido bloqueando puertos y dominios (IPs) por medio del firewall que dispone el equipo mikrotik, el hecho es que no existe un dispositivo que alerte a que puerto están intentando atacar y desde donde están dirigidos estos ataques (IPs), se complica la funcionalidad óptima en la red cuando el equipo se vuelve vulnerable al no disponer de alertas tempranas antes de correr algún riesgo. Cómo se menciona en el capítulo 2, un honeypot es una herramienta de la cual se puede extraer información y apoyar de manera directa a la implementación del firewall y hacer más robusta su seguridad. En este apartado se va mostrar el despliegue de un honeynet en el segmento de la red en producción levantada con SDN y apoyar al listado de puertos e IPs de las que hay restringir para mantener un servicio óptimo.

Para la implementación se procedió con la adquisición de otro CPU en el cual se estructuró un sistema operativo con Windows 10 y plataforma de virtualización VirtualBox, el equipo referido ofrece las siguientes características.

- Nombre del SO Microsoft Windows 10 Enterprise LTSC
- Versión 10.0.17763 compilación 17763
- Fabricante del SO Microsoft Corporation
- Nombre del sistema DESKTOP-02Q2RSR
- Tipo de sistema PC basado en x64
- SKU del sistema To be filled by O.E.M.
- Procesador Intel(R) Core (TM) i7-3770 CPU @ 3.40GHz, 3401 Mhz, 4 procesadores principales, 8 procesadores lógicos
- Versión y fecha de BIOS Intel Corp. BEH6110H.86A.0109.2012.1221.1455, 21/12/2012
- Versión de SMBIOS 2.7
- Versión de controladora integrada 255.255
- Fabricante de la placa base Intel Corporation

- Producto de placa base DH61CR
- Versión de la placa base AAG14064-210
- Rol de plataforma Escritorio
- Capa de abstracción de hardware Versión = "10.0.17763.168"
- Memoria física instalada (RAM) 16,0 GB
- Memoria física total 15,8 GB
- Memoria física disponible 14,4 GB
- Memoria virtual total 18,2 GB
- Memoria virtual disponible 16,8 GB
- 3 interfaces de red 10/100/1000 GB
- 2 discos de 2 TB y 4 TB respectivamente

Como se mencionó en el capítulo 2, honeynet es un grupo de honeypots dentro de la misma red, trabajando de manera simultánea para apoyar a la seguridad de la infraestructura, se implementó dos servicios honeypot, uno es adquirido en plataforma virtual con extensión OVA y otro es adquirido como versión ISO desde su página web, estos dos honeypot están aprovechando los recursos de la máquina física cada uno con su interfaz física y dirección IP pública respectivamente. Los dos honeypot se han probado en interfaz web para apreciar de manera más ordenada los resultados. Los servidores que se usaron para estas pruebas son los siguientes: HoneyDrive3 (https://sourceforge.net/projects/honeydrive/) y TPOT (https://github.com/telekom-security/tpotce), el primero se obtiene en fuente virtual y el segundo en ISO. Algo que hay que tomar mucho en cuenta es que la interfaz por donde escuchen estos servidores debe estar configurado en modo promiscuo.

HoneyDrive. - Es una herramienta de software en plataforma virtual con Xubuntu Desktop el mismo que dispone de varios paquetes de software honeypot, tiene utilidad para agrupar varios servicios con el objeto de analizar, visualizar y procesar los datos que ingresan a su entorno, como ejemplo de estos servicios Kippo y Dionaea. Hay muchas funciones más que son de provecho para la integridad en

las redes de Telecomunicaciones, se podría decir también que es una distribución en Linux que congrega varias herramientas para montar un honeypot rápidamente.

Existen servicios integrados o herramientas dentro de Honeydrive como: Ntop, EtherApe, Nmap, Wireshak, ClamAV, entre otros que sirven para análisis de vulnerabilidades.

EL servidor que hace como honeypot está en su máquina virtual con las siguientes características:

- Sistema Operativo: Xubuntu Desktop 12.04.4 LTS i386
- Disco de almacenamiento: 80GB VMDK
- Memoria: 6 GB
- 2 procesadores
- 1 interfaz ethernet 10/100/1000 Realtek

Dispone de IP pública conectado directamente al router de borde, al levantar este servidor se dispone de una interfaz gráfica de escritorio en el cual hay que configurar antes de arrancar el servicio.

Honeydrive tiene bien marcado de resultados con dos de los honeypot de los tantos que dispone, como es Kippo y Dionaea.

Kippo. – Según [28], es un honeypot de correlación media, diseñado para el análisis de ataques SSH. Dispone de capacidad de almacenar los intentos de nombre de usuario y contraseña que utiliza los atacantes, tanto de fuerza bruta como de diccionario.

La forma de ejecutar este honeypot para que inicie el almacenamiento de información es mediante dos reglas, dentro de consola de comandos en el servidor Honeydrive, para acceder a la información se realiza mediante la dirección en cualquier navegador web ip-servidor/kippo-graph, como se muestra en la Figura 4.6.1.

```
$ cd /opt/kippo/
$ ./start.sh
```

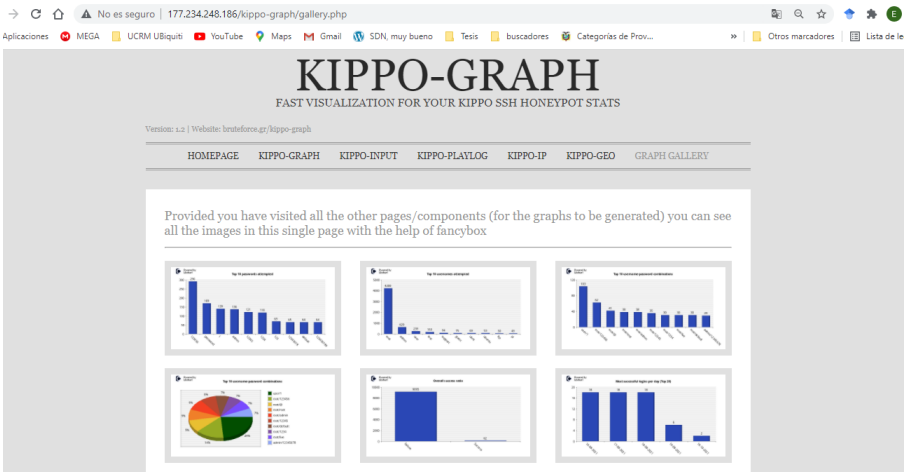


Figura 4.6.1. Acceso a honeypot Kippo en modo gráfico

Fuente: Elaborado por el investigador

Dionaea. – De acuerdo a [29], es una herramienta de software desarrollado con el fin de abstraer malware y analizarlo posteriormente. Para mitigar que se exploten bugs en su software la herramienta reduce los privilegios, de manera que las actividades que requieran privilegios elevados sean ejecutadas por un proceso hijo creado previamente, esto no asegura, pero al menos complica la tarea de explotación que se genera por los atacantes.

El principal protocolo de trabajo es SBM, pero también habilita otros servicios en diferentes puertos como http por el puerto 80, ftp por el puerto 21 y tftp por el 69.

Para ejecutar el servicio de Dionaea se debe ejecutar varias reglas en consola de comandos del servidor Honeydrive.

cd /opt/dionaeaFR

python manage.py collectstatic

python manage.py runserver ip-servidor:8090

Una vez ejecutadas las reglas anteriores se accede a la consola gráfica mediante cualquier navegador, escribiendo la IP del servidor y el puerto establecido como se muestra en la figura 4.6.2.

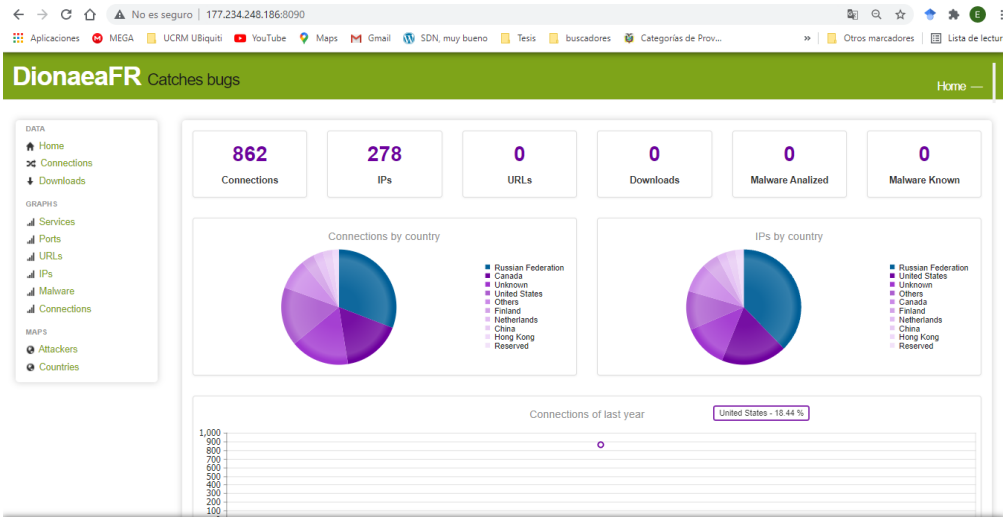


Figura 4.6.2. Consola gráfica de Dionaea Honeypot

Fuente: Elaborado por el investigador

T-POT. – Según [30] T-pot, es un honeypot multiplataforma de código abierto, bajo el sistema operativo Debian (Stretch), es un de las herramientas más exitosas y adecuadas en código abierto, debido a su sencilla configuración, bajo mantenimiento, ventanas y paneles de control de fácil uso. Es un software o conjunto de computadores con la única intención de cautivar atacantes, con la simulación de sistemas sensibles o débiles para los ataques. Así también se considera una herramienta para aplicarlo en seguridad informática, que recoge información de los atacantes y sus técnicas. Este software se utiliza como señuelo para distraer a los atacantes de las máquinas más importantes de la red de datos y advertir previamente al administrador de una incidencia, además de consentir un análisis en profundidad del atacante, durante y después de la arremetida al honeypot.

EL servidor que contiene este honeypot está en una máquina virtual con las siguientes características:

- Sistema Operativo: Xubuntu Desktop 12.04.4 LTS i386
- Disco de almacenamiento: 80GB VMDK
- Memoria: 6 GB
- 2 procesadores
- 1 interfaz ethernet 10/100/1000 Realtek

En la figura 4.6.3, se observa el tablero de todos los honeypots integrados dentro de la herramienta T-POT.

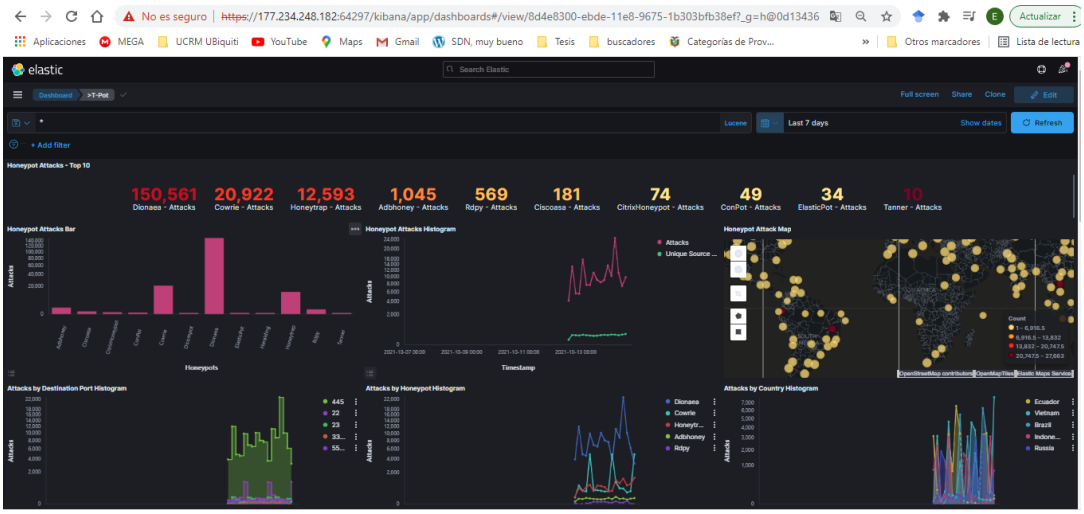


Figura 4.6.3. Presentación de servidor T-POT en funcionamiento

Fuente: Elaborado por el investigador

4.7. Análisis del funcionamiento

4.7.1 Resultados de implementación de red SDN

En este apartado se hace referencia a las ventajas de implementar un honeynet dentro de una red SDN para la empresa Clicknet S.A. Como se mencionó la empresa dispone en su mayoría de equipos de la marca mikrotik, que únicamente soportan protocolo OpenFlow en versión 1.0, este particular impone a que el controlador sea compatible con versión 1.0 de OpenFlow por tal razón HPE SDN VAN fue seleccionado. La red SDN se estableció dentro de un segmento de red para mantenerlo a prueba, dentro de este segmento se incluyó a equipo de borde, núcleo y distribución para realizar pruebas de rendimiento, tanto en respuesta continua (icmp) como rendimiento en la transferencia de datos desde una oficina hacia los servidores de servicios.

Las pruebas se realizaron en un segmento de red que integre la oficina de la empresa y el nodo de servidores que se encuentran en diferentes puntos. El objetivo es percibir las ventajas disponibles al

integrar estos dispositivos a una red SDN para esto se arma un circuito como el de la figura 4.7.1.

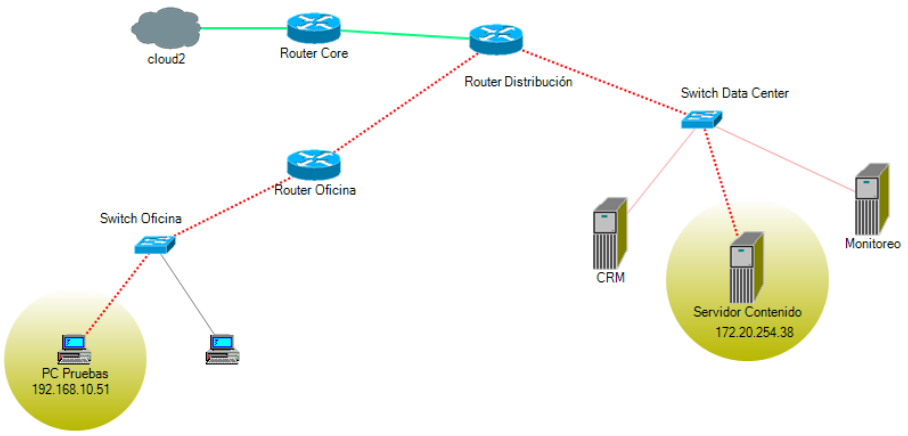


Figura 4.7.1. Origen y destino de prueba

Fuente: Elaborado por el investigador

Para el proceso de prueba de respuesta ICMP o ping, se realiza desde la consola de comando de Windows de la portátil con la IP 192.168.10.51 hacia un servidor en el data center con la IP 172.20.254.38, este servidor está habilitado para que responda las peticiones de ping.

Se procede con la prueba de ping sin habilitar OpenFlow y se obtiene el resultado que se muestra en la figura 4.7.2.

```
64 bytes from 172.20.254.38: icmp_seq=201 ttl=126 time=2.88 ms
64 bytes from 172.20.254.38: icmp_seq=202 ttl=126 time=2.44 ms
64 bytes from 172.20.254.38: icmp_seq=203 ttl=126 time=3.30 ms
64 bytes from 172.20.254.38: icmp_seq=204 ttl=126 time=2.62 ms
64 bytes from 172.20.254.38: icmp_seq=205 ttl=126 time=2.67 ms
64 bytes from 172.20.254.38: icmp_seq=206 ttl=126 time=3.15 ms
64 bytes from 172.20.254.38: icmp_seq=207 ttl=126 time=3.11 ms
64 bytes from 172.20.254.38: icmp_seq=208 ttl=126 time=2.51 ms
64 bytes from 172.20.254.38: icmp_seq=209 ttl=126 time=3.43 ms
64 bytes from 172.20.254.38: icmp_seq=210 ttl=126 time=2.62 ms
64 bytes from 172.20.254.38: icmp_seq=211 ttl=126 time=3.04 ms
64 bytes from 172.20.254.38: icmp_seq=212 ttl=126 time=5.65 ms
64 bytes from 172.20.254.38: icmp_seq=213 ttl=126 time=4.63 ms
64 bytes from 172.20.254.38: icmp_seq=214 ttl=126 time=3.75 ms
64 bytes from 172.20.254.38: icmp_seq=215 ttl=126 time=2.87 ms
64 bytes from 172.20.254.38: icmp_seq=216 ttl=126 time=4.99 ms
64 bytes from 172.20.254.38: icmp_seq=217 ttl=126 time=2.88 ms
64 bytes from 172.20.254.38: icmp_seq=218 ttl=126 time=2.54 ms
64 bytes from 172.20.254.38: icmp_seq=219 ttl=126 time=3.18 ms
64 bytes from 172.20.254.38: icmp_seq=220 ttl=126 time=2.42 ms
64 bytes from 172.20.254.38: icmp_seq=221 ttl=126 time=4.10 ms
64 bytes from 172.20.254.38: icmp_seq=222 ttl=126 time=2.54 ms
64 bytes from 172.20.254.38: icmp_seq=223 ttl=126 time=4.79 ms
64 bytes from 172.20.254.38: icmp_seq=224 ttl=126 time=3.70 ms
64 bytes from 172.20.254.38: icmp_seq=225 ttl=126 time=2.29 ms
^C
--- 172.20.254.38 ping statistics ---
225 packets transmitted, 225 received, 0% packet loss, time 224552ms
rtt min/avg/max/mdev = 2.124/2.979/9.857/0.897 ms
```

Figura 4.7.2. *Respuesta de servidor sin habilitar OpenFlow*

Fuente: Elaborado por el investigador

Al momento de estar sin levantar el protocolo OpenFlow, se aprovecha para realizar una prueba de ancho de banda bajo la misma ruta entre el equipo de oficina con Windows 10 y el servidor del Data Center también con Windows 10, para esto se usa una herramienta conocida con el nombre de Iperf, este software se lo obtiene en archivo comprimido, al descargar hay que descomprimirlo una vez desempaquetado se debe usar bajo línea de comandos, este software se utiliza como servidor tal se muestra en la figura 4.7.3.

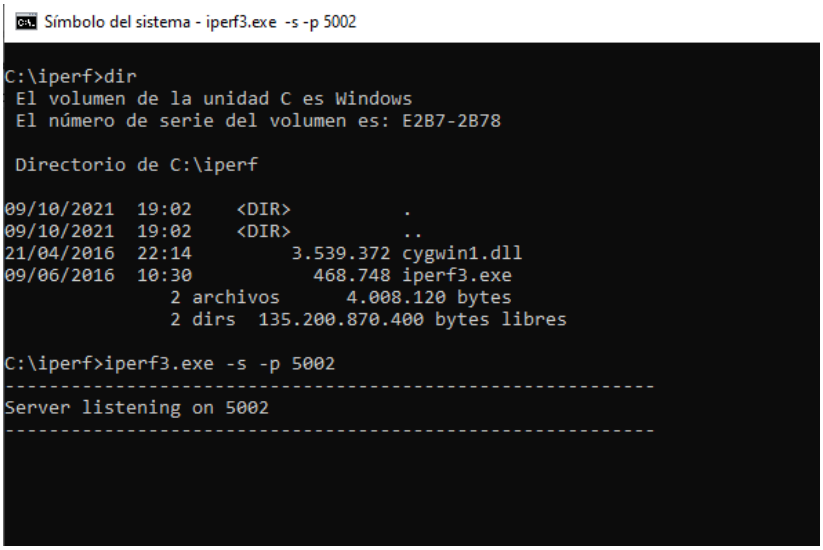


Figura 4.7.3. Iperf como servidor

Fuente: Elaborado por el investigador

Los comandos se ejecutan dependiendo de lo que se requiere, en este caso “-s” indica que va a funcionar como servidor, “-p” indica el puerto de escucha que va a disponer a cualquier cliente que se conecte, en este caso sería puerto 5002.

Para iniciar la prueba en el equipo cliente se ejecuta el comando similar, en este caso la diferencia es que se ejecutará como:

C:\iperf>iperf3.exe -c 172.20.254.38 -p 5002

Donde “-c” implica que es un cliente, la dirección IP es la del servidor al que se va a conectar y “-p” el puerto con el que debe conectarse al servidor.

El resultado de la prueba sin habilitar OpenFlow en los dispositivos de la ruta que se requiere hacer pruebas, es decir, desde el cliente con IP 192.168.10.51, hasta el servidor de contenido con IP 172.20.254.38 utilizando la herramienta, se aprecia

en la figura 4.7.4.

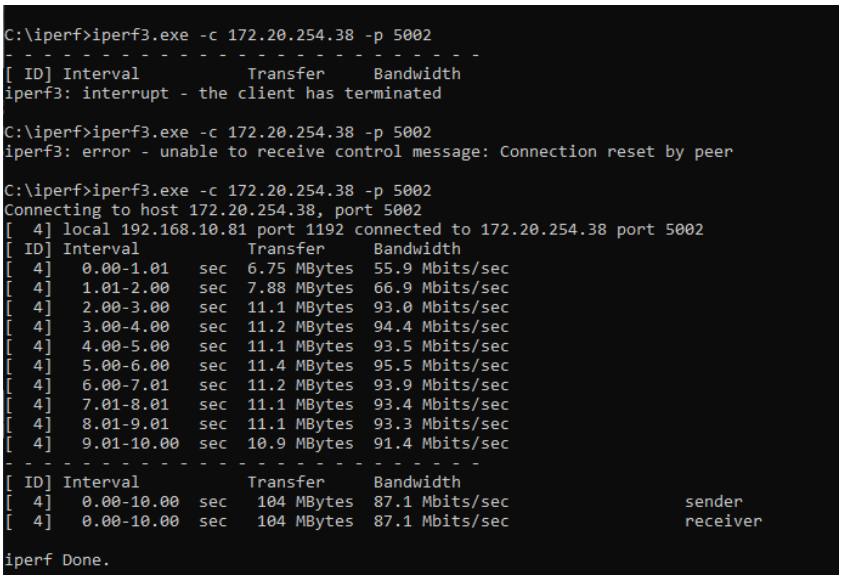


Figura 4.7.4. Prueba de Iperf sin habilitar OpenFlow

Fuente: Elaborado por el investigador

En el gráfico anterior se determinó que el ancho de banda sin establecer una red SDN se dispone de una velocidad de transmisión de 87,1 Mbps de subida y 87,1 de bajada, que es un promedio determinado en otros computadores de prueba.

Se procedió a levantar el servicio del protocolo OpenFlow en los dispositivos establecidos con anterioridad, la misma ruta y las mismas pruebas. Entonces se ejecuta las instrucciones dentro de la consola de comandos con el protocolo ICMP, como se muestra en la figura 4.7.5.

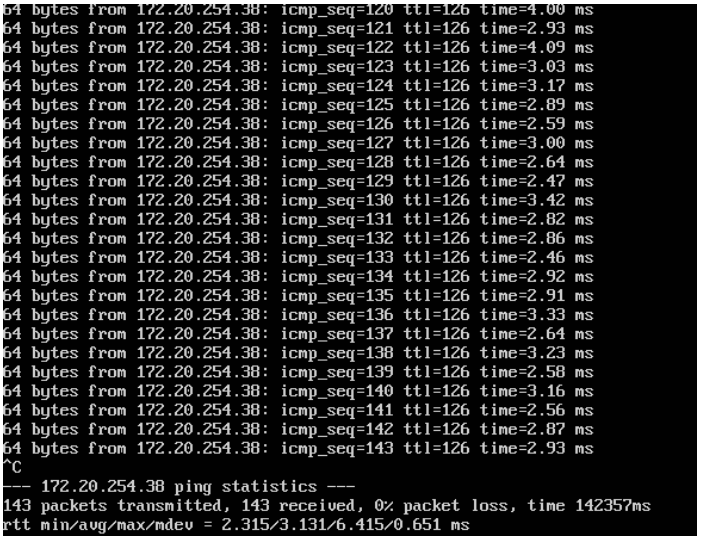


Figura 4.7.5. Respuesta de servidor habilitado OpenFlow

Fuente: Elaborado por el investigador

Luego de esta prueba se dispone del resultado desde la misma máquina con 143 paquetes enviado y 143 paquetes recibidos, un tiempo mínimo de respuesta de 2,315 ms, una media de 3,131 ms y un máximo de 6,415 ms.

Con la tabla 4.7.1, Se compara los resultados obtenidos antes y después de levantar el protocolo OpenFlow.

Tabla 4.7.1. Comparación de respuestas a ICMP

PING	Sin SDN	Con SDN
Mínimo	2,124	2,315
Promedio	2,979	3,131
Máximo	9,857	6,415

Fuente: Elaborado por el investigador

Directamente no se evidenció una diferencia abismal, en los dos eventos no existe perdida de paquetes, pero la diferencia tanto en valor mínimo y promedio son similares, más no los valores máximos que cambian de una forma pronunciada. Aplicando porcentaje se logra considerar una disminución de tiempos de retardo máximos.

$$100\% \rightarrow 9{,}857$$
$$x \rightarrow 6{,}415$$

$$x = 34{,}91\ \%$$

De este resultado se manifiesta que el rendimiento de respuesta en valores máximos desde un dispositivo de cliente a otro que hace de servidor, ha mejorado en un 34,91%, al habilitar el protocolo OpenFlow en la red.

Para obtener más información se procede con la medida desde otros cuatro computadores dentro de la misma red de la oficina hacia el servidor de contenido, se obtiene los valores que se muestran en la tabla 4.7.2. antes de habilitar el protocolo OpenFlow.

Tabla 4.7.2. Respuesta de 4 equipos sin SDN

	Mínimo	Medio	Máximo
Prueba 01	2,124	2,979	9,857
Prueba 02	2,131	2,827	9,123
Prueba 03	2,158	2,923	9,854
Prueba 04	2,112	2,664	9,796
Prueba 05	2,176	2,981	9,123

Fuente: Elaborado por el investigador

Luego de habilitar el protocolo OpenFlow se obtiene otros valores para ser comparados con el primero, se muestra en la tabla 4.7.3.

Tabla 4.7.3. Respuesta de 4 equipos con SDN

	Mínimo	Medio	Máximo
Prueba 01	2,315	3,131	6,415
Prueba 02	2,146	3,121	6,234
Prueba 03	2,111	2,979	6,345
Prueba 04	2,146	2,634	6,129
Prueba 05	2,119	2,875	6,234

Fuente: Elaborado por el investigador

Finalmente, se dispone del cuadro comparativo en la tabla 4.7.4, que en sus valores mínimo y medio no existe mucha variación no así en sus valores máximos donde se evidencia la mejoría en el tiempo de respuesta.

Tabla 4.7.4. Comparación en porcentaje de las pruebas

	Mínimo	Medio	Máximo
Prueba 01	-9%	-5%	35%
Prueba 02	-1%	-10%	32%
Prueba 03	2%	-2%	36%
Prueba 04	-2%	1%	37%
Prueba 05	3%	4%	32%

Fuente: Elaborado por el investigador

Al estar levantado la red SDN, se realizó otra medida, en este caso es el ancho de banda desde el computador en oficina, con IP 192.168.10.51 hasta el servidor

172.20.254.38 que se utilizó con pruebas de ping, se aplicó la herramienta Ipref, pero esta vez como cliente.

C:\iperf>iperf3.exe -c 172.20.254.38 -p 5002

Los resultados que se muestran en la figura 4.7.6, representa el resultado de ancho de banda o tráfico de datos que logran transitar por la ruta con protocolo OpenFlow o red SDN.

```
C:\iperf>iperf3.exe -c iperf.scottlinux.com -p 5201
iperf3: error - unable to receive control message: Connection reset by peer

C:\iperf>
C:\iperf>iperf3.exe -c 172.20.254.38 -p 5002
Connecting to host 172.20.254.38, port 5002
[  4] local 192.168.10.81 port 5134 connected to 172.20.254.38 port 5002
[ ID] Interval           Transfer     Bandwidth
[  4]   0.00-1.00   sec  11.1 MBytes  93.0 Mbits/sec
[  4]   1.00-2.00   sec  11.0 MBytes  92.5 Mbits/sec
[  4]   2.00-3.00   sec  11.1 MBytes  93.4 Mbits/sec
[  4]   3.00-4.00   sec  11.1 MBytes  93.1 Mbits/sec
[  4]   4.00-5.00   sec  11.1 MBytes  93.3 Mbits/sec
[  4]   5.00-6.00   sec  11.0 MBytes  92.1 Mbits/sec
[  4]   6.00-7.00   sec  10.8 MBytes  90.3 Mbits/sec
[  4]   7.00-8.00   sec  11.1 MBytes  93.3 Mbits/sec
[  4]   8.00-9.00   sec  11.1 MBytes  93.5 Mbits/sec
[  4]   9.00-10.00  sec  11.1 MBytes  93.1 Mbits/sec
- - - - - - - - - - - - - - - - - - - - - - - - -
[ ID] Interval           Transfer     Bandwidth
[  4]   0.00-10.00  sec   111 MBytes  92.8 Mbits/sec                  sender
[  4]   0.00-10.00  sec   111 MBytes  92.7 Mbits/sec                  receiver

iperf Done.

C:\iperf>
```

Figura 4.7.6. Prueba de Iperf sin habilitar OpenFlow

Fuente: Elaborado por el investigador

En la tabla 4.7.5, se presentan los valores obtenidos de las pruebas realizadas, para elaborar una comparación de resultados.

Tabla 4.7.5. Comparación de resultados en AB

	Sin SDN	**Con SDN**
Upload	87,1	92,8
Download	87,1	92,7

Fuente: Elaborado por el investigador

La tabla anterior permite distinguir que existe una diferencia de rendimiento en ancho de banda, comparando valores, se tiene que de subida hay una mejoría de 6,54% y de bajada 6,42% en el canal de datos de prueba.

100% → 87,1
x → 92,8

x = 6,54 %

100% → 87,1
x → 92,7

x = 6,42 %

4.7.2 Resultados de implementación Honeynet

En este apartado se analiza los beneficios al implementar una honeynet dentro de una red de datos con herramientas de software. Cómo se comentó con anterioridad una honeynet es la unión de varios honeypot en una misma red, por tanto, se implementó dos servidores bajo plataforma Linux y cada una de estos contienen varios honeypots embebidos. Los honeypots implementado son:

Honeydrive. - Este software contiene varios honeypot incluidos y varias herramientas visuales.

Kippo. – Con esta herramienta se alcanza monitorear y observar los ataques al protocolo ssh con puerto 22, se encontró: contraseñas más usadas y aplicadas en el intento de ataque como se muestra en la figura 4.7.7.

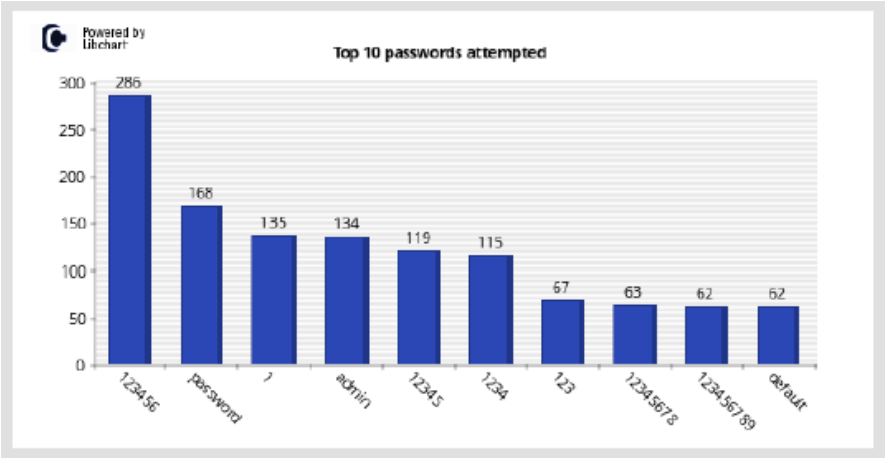


Figura 4.7.7. Diez contraseñas más usadas

Fuente: Elaborado por el investigador

Se logra obtener también los intentos de ingresar al servidor con un usuario específico, como se muestra en la figura 4.7.8, el honeypot entrega la información de estos usuarios en figura de barras verticales.

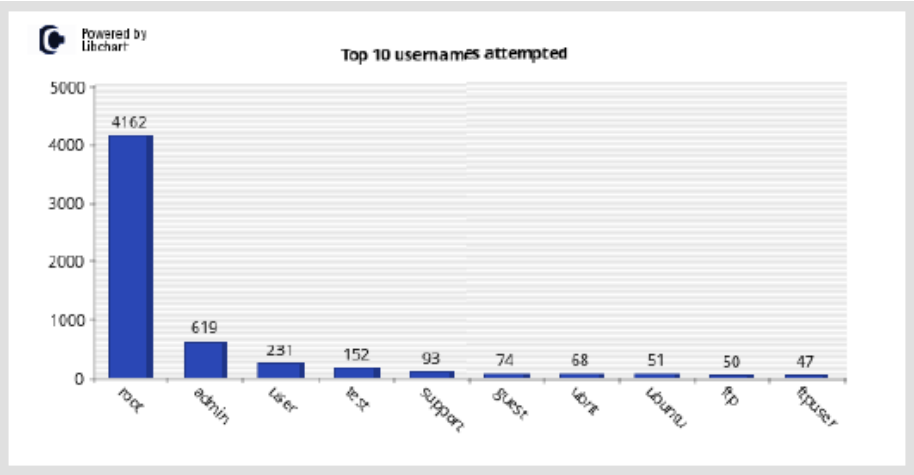


Figura 4.7.8. Diez usuarios más usados

Fuente: Elaborado por el investigador

Número de conexiones por IP en un gráfico en modo pastel para los intentos de acceso en la figura 4.7.9.

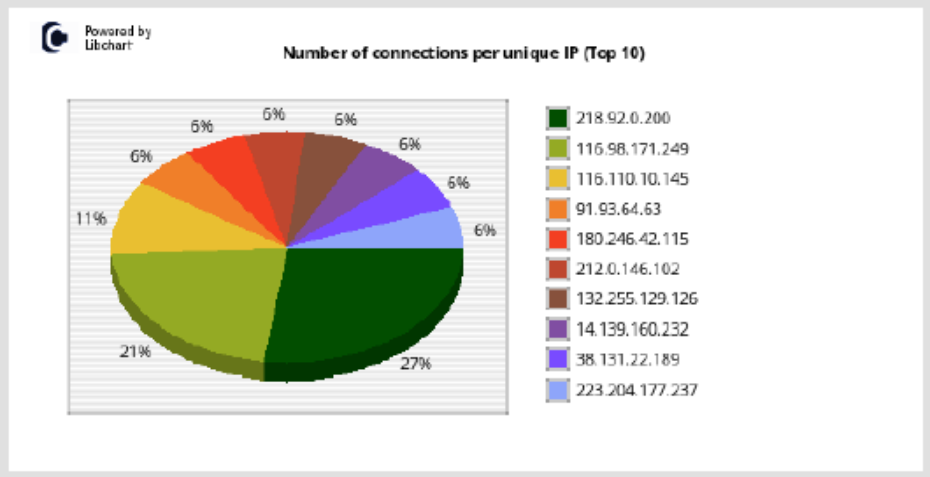


Figura 4.7.9. Número de conexiones por IP

Fuente: Elaborado por el investigador

Se muestra también información de los clientes ssh que se han usado para la prueba de ataques como se muestran en la figura 4.7.10 donde se aprecia sus nombres.

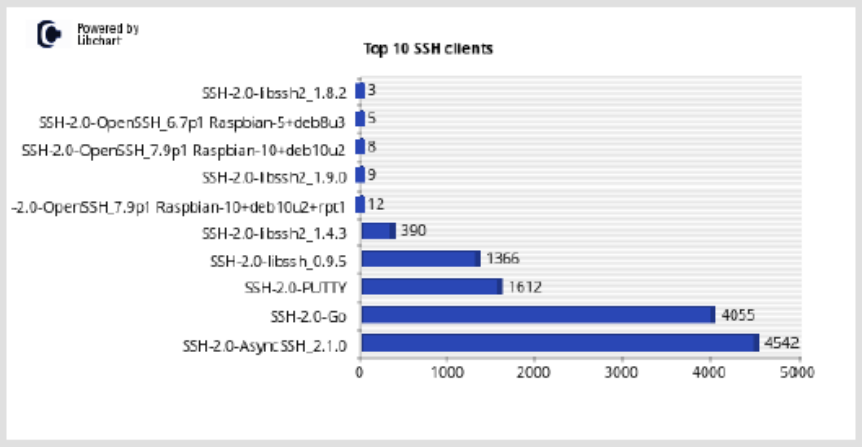


Figura 4.7.10. Clientes SSH más usados

Fuente: Elaborado por el investigador

Al observar la gran cantidad de información que entrega esta herramienta, se convierte en un colaborador muy eficiente para contrarrestar los ataques desde fuera de nuestra red.

Dionaea. - Esta herramienta también dispone de información que apoyará a impedir los ataques a dispositivos de manera temprana, los datos que se disponen se muestran en las figuras respectivas.

Esta herramienta dispone de varias ventajas entre ellas mostrar los servicios que están siendo atacados como se observa en la figura 4.7.11.

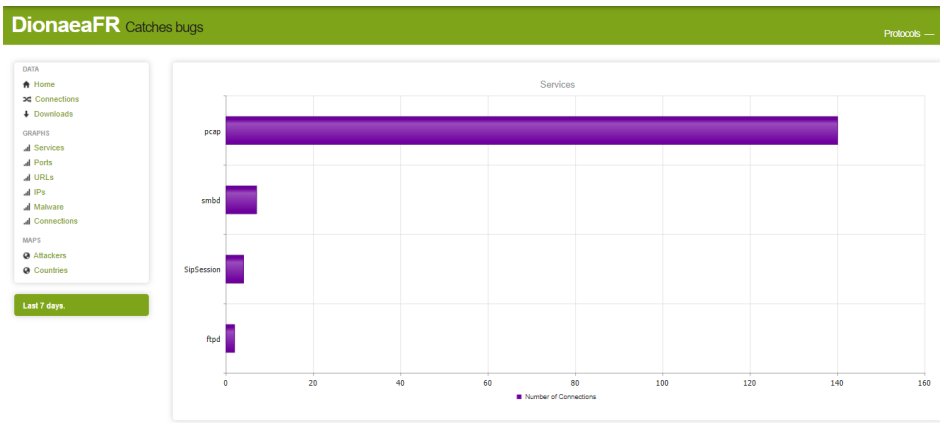


Figura 4.7.11. Servicios atacados

Fuente: Elaborado por el investigador

En la figura se refleja el número de ataques a cada uno de los servicios, que a su vez son los más apetecibles al momento de una intrusión. Se aprecia también el puerto al que el intruso está intentando vulnerar como se muestra en la figura 4.7.12.

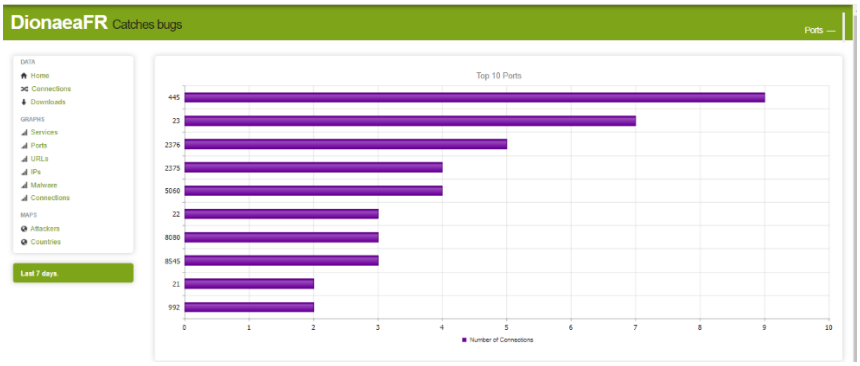


Figura 4.7.12. Puertos en intento de ataque

Fuente: Elaborado por el investigador

La parte interesante de esta herramienta es la captura de las direcciones IPs que de forma intensa acometen a este servidor como se muestra en la figura 4.7.13.

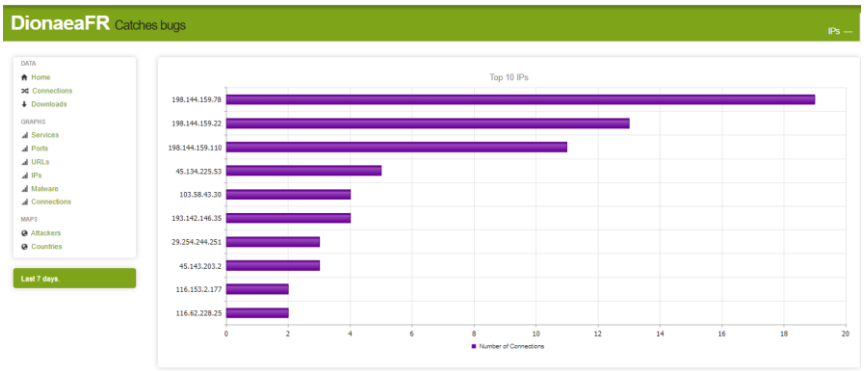


Figura 4.7.13. Direcciones IP de atacantes

Fuente: Elaborado por investigador

T-POT. - Este honeypot o herramienta también dispone de honeypots integrados, como:

- Dionaea
- Cowrie
- Honeytrap
- Adbhoney
- Ciscoasa
- Rdpy
- CitrixHoneypot

- ConPot
- ElasticPot
- Tanner

A este software se lo conoce como el más completo, por la cantidad de honeypots que contiene y la cantidad de información que se consigue de este servicio. Cada honeypot realiza su trabajo al mismo tiempo y captura ataques que se ejecuta hacia el servidor.

Se mirar desde una IP el ataque a un puerto, servicio o exploit que se utiliza, porque también dispone de IDS (Intrusion Detection System) en este caso es como se muestra en la figura 4.7.14. Suricata es un motor de red de alto rendimiento IDS, IPS y seguridad de red.

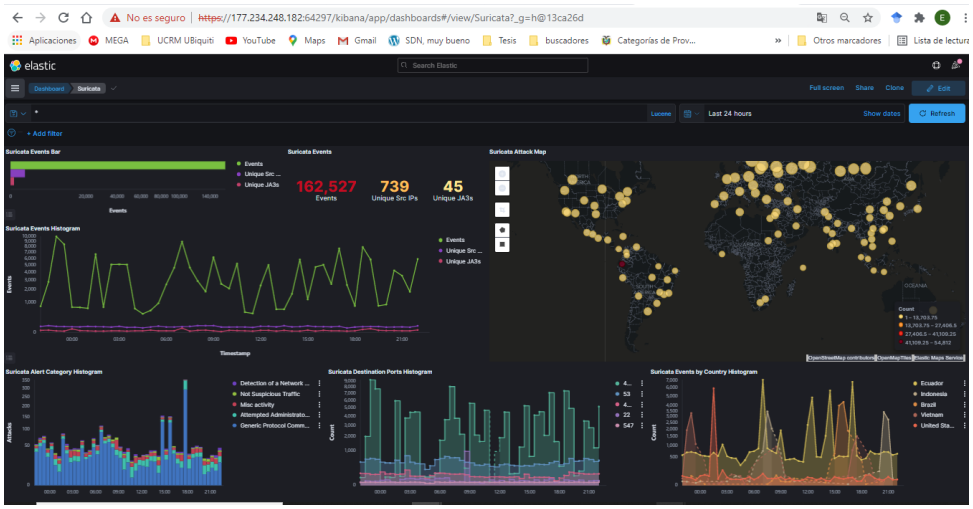


Figura 4.7.14. Tablero de control de Suricata

Fuente: Elaborado por investigador

Hay que rescatar que este honeypot o herramienta dispone también de software similar de Honeydrive, que es Dionaea como se muestra en la figura 4.7.15.

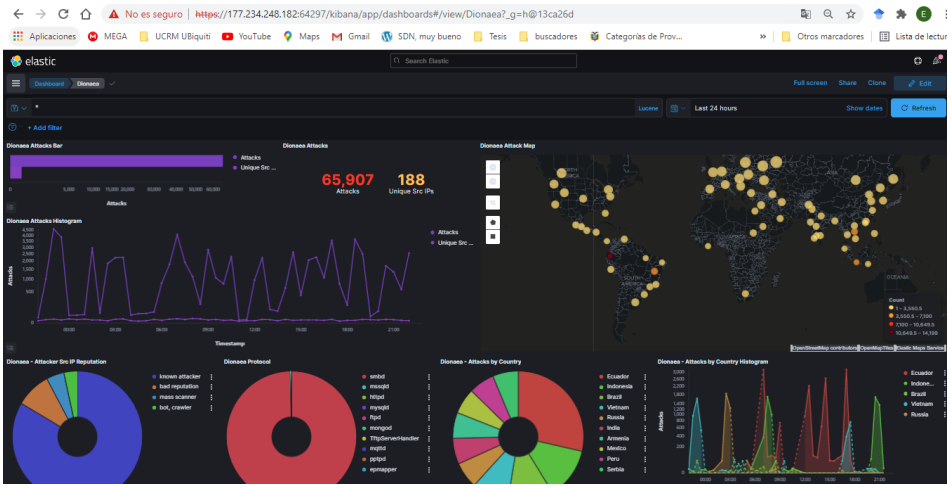


Figura 4.7.15. Tablero de Dionaea

Fuente: Elaborado por investigador

Estos dos hoyneypot coinciden es esta aplicación y también coinciden en los datos que logran rescatar e incluso T-POT lo supera, como se muestra en la figura 4.7.16.

Figura 4.7.16. Servicios que monitorea T-POT con Dionaea

Honeydrive y T-POT coinciden en varios servicios que rastrean en ataques, pero T-POT supera con Suricata, al poder incluso revisar los ataques con el tipo de exploit que intenta romper el atacante la vulnerabilidad existente, como se muestra en la figura 4.7.17.

Figura 4.7.17. Vulnerabilidades registradas en Suricata

Fuente: Elaborado por el investigador

Estas vulnerabilidades vienen registradas con un Link de color azul que permite revisar que tipo de explotación realizada por el atacante, como es general se observa el top 10 en la figura 4.7.18.

Figura 4.7.18. Alerta de vulnerabilidades

La información que presenta este honeypot es considerablemente alta como los histogramas que presentan alertas, ataques, ciudades, clientes ssh, tipo de contenido en http, etc. Muestra hasta el mapa geográfico de donde parten los ataques como se muestra en la figura 4.7.19.

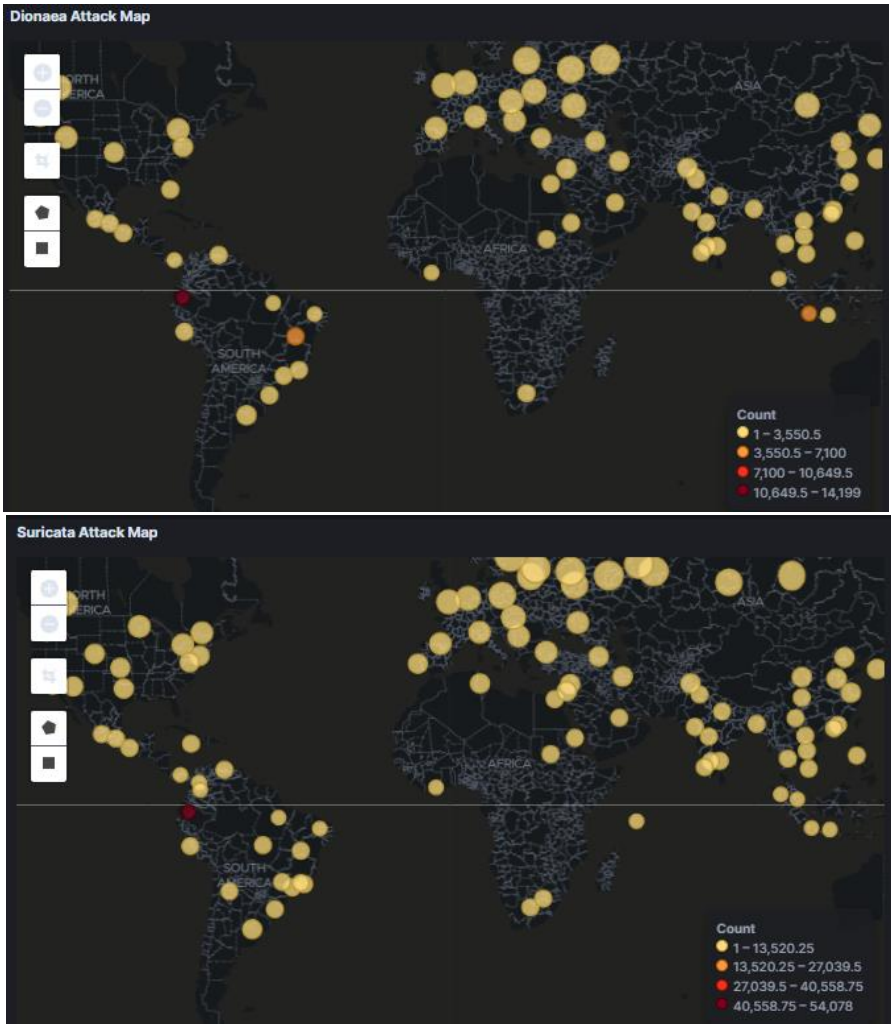


Figura 4.7.19. Geografía de los puntos de origen de ataque

Fuente: Elaborado por el investigador

4.7.3 Incidentes y soluciones

En este trabajo se presentó un gran inconveniente que ya fue mencionado al inicio de este capítulo, cuando de presentar errores dentro de los RouterOS, se quedan aislados completamente de la red, lo que provoca caídas en enlaces de producción, se evidenció en el desarrollo de este proyecto. Una vez que el equipo queda fuera, la única forma de recuperarlo es deshabilitando tanto la conexión con el controlador como los puertos asignados para hablar OpenFlow de manera manual como en la figura 4.7.20.

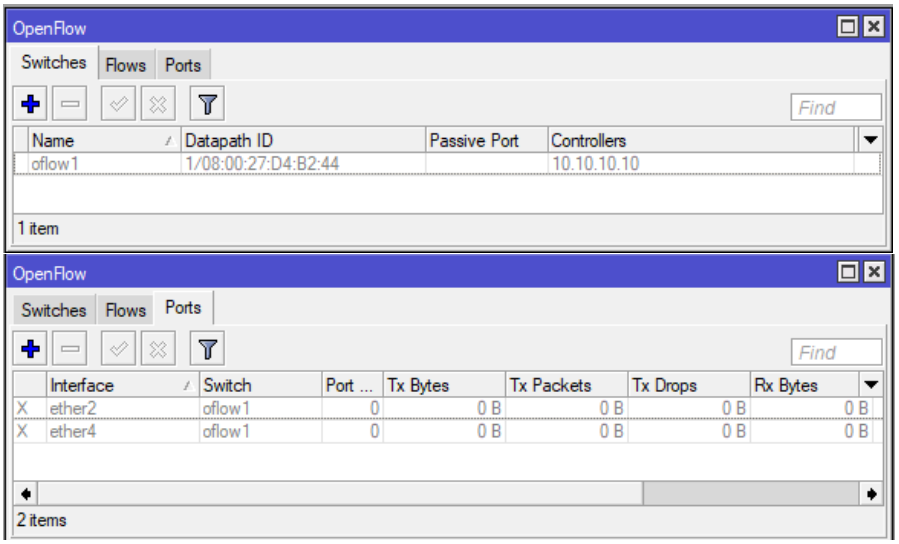


Figura 4.7.20. Deshabilitar OpenFlow en router Mikrotik

Fuente: Elaborado por el investigador

Al disponer de equipos que se encuentran fuera de la ciudad y requieren ser integrados nuevamente a la red de manera inmediata ya que los clientes pierden el servicio, se generó dentro del RouterOS un script que permita deshabilitar los flujos de OpenFlow, pero para que sea automático, se utilizó la herramienta de "whatchdog", este último es un sensor de respuesta, es decir que se configura este con una IP a la que siempre debe responderle el equipo, de no ser el caso este automáticamente envía a reiniciar. Al momento de reiniciar se ejecuta el script que deshabilite el protocolo, es decir que cada que se reinicia el equipo se deshabilita OpenFlow y se recupera los equipos sin tener configuración de protocolo mencionado. El script creado se muestra en la figura 4.7.21.

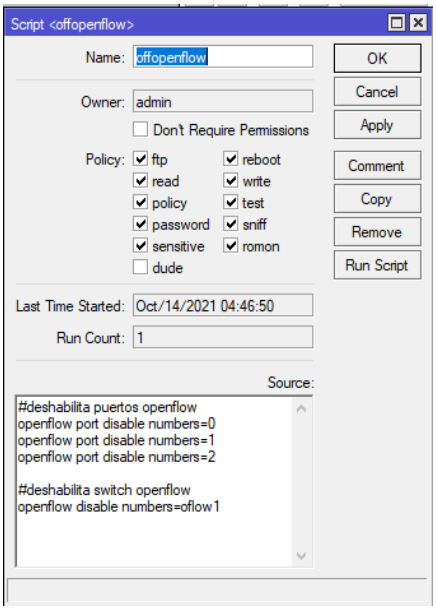


Figura 4.7.21. Script para deshabilitar OpenFlow

Fuente: Elaborado por el investigador

Aquí se deshabilita los puertos que sean necesarios, y se los guarda con un nombre, este nombre se utiliza en el servicio de "scheduler", que son tareas programadas, esta tarea se ejecuta siempre que reinicie el equipo, la regla es bastante sencilla en entorno visual se presenta en la figura 4.7.22.

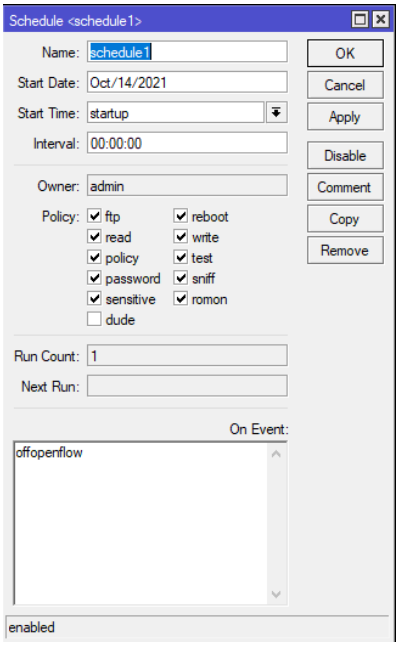


Figura 4.7.22. Tarea que se ejecuta al iniciar el router

Fuente: Elaborado por el investigador

CAPITULO V

5.1. Conclusiones

- La empresa no dispone de seguridad perimetral especializado, los equipos Mikrotik hacen de firewall, ya que poseen esta característica, el presente trabajo permitirá alertar los ataques que un RouterOS no consigue, la información que genere la honeynet anticipará para que se bloquee los puertos que son atacados con frecuencia, desde que direccionamiento IP o dominio, así como también los servicios vulnerables, ante posibles incidentes.
- Se ha evidenciado que una red SDN es escalable y compatible con una red convencional, ya que se probó el servicio luego de levantar el protocolo, y las configuraciones que estaban establecidas en los equipos no hubo necesidad de cambiarlos, servicios como: enrutamientos estáticos, dinámicos, QoS, control de ancho de banda, entre otros.
- El uso de un controlador que depende de una marca complicó poder utilizar funcionalidades como: filtrado de flujos de datos, seguridad en toda la red SDN, monitoreo, obtención de información de la red, porque cada APP adicional requiere licencia de muy alto costo para poder ampliar el funcionamiento.
- Se comprobó que el protocolo OpenFlow permite trabajar bajo un túnel de datos establecido, en este caso se podría, ampliar la red SDN hacia todas las ciudades donde existiría interconexión remota.

5.2. Recomendaciones

- Un dispositivo RouterOS dispone de muchas ventajas en este caso hasta de protocolo OpenFlow, para realizar pruebas se recomienda que se realice en laboratorio ya que Mikrotik indica que la versión de OpenFlow 1.0 es para experimentar el servicio. El fabricante aún no dispone de fecha para mejorar su versión de OpenFlow.
- Se recomienda revisar que tipo de bases de datos utilizan estos servidores

que conforman la honeynet con el fin de automatizar o generar una interfaz que automatice que IPs, que servicios, que puertos son atacados día a día y permanecer protegidos de mejor forma.

- La implementación de los honeynet se ejecutó en la parte perimetral, sería muy alentador probar estas herramientas de software en ambientes de red interna para verificar si existen ataques de parte de los usuarios del servicio.
- Se recomienda adquirir o buscar otra solución para controlador que maneje protocolo OpenFlow 1.0 y sea de libre distribución, con el fin de realizar cambios a necesidad de la empresa sin incrementar gastos adicionales.

Bibliografía

[1] Federación de Enseñanza CCOO de Andalucía, «HoneyNets, una desconocida en la seguridad informática,» 2009. [En línea]. Available: https://www.feandalucia.ccoo.es/docu/p5sd6337.pdf.

[2] C. J. Quimbayo Rodríguez, «Propuesta metodológica para la selección de controladores de redes SDN a nivel empresarial,» Universidad Santo Tomás, Colombia, 2020.

[3] J. L. G. R. Farfán, INTEGRACION DE REDES IP UTILIZANDO SDN, Buenos Aires, Argentina, 2017.

[4] W. H. Sukwha Kyung, «Design and Implementation of Next-Generation Honeynet via SDN,» de *National Science Foundation*, 2017.

[5] X. Meng y Z. Zhao, «An intelligent honeynet architecture based on software defined security,» *IEEE,* 2017.

[6] C. E. Minda Gilces y R. Pacheco Villamar, «Aplicación de Balanceo De Carga Dinámico Para,» *Revista lbérica de Sistemas y Tecnologías de Información*, 2019.

[7] R. Bahman, H. Kevin W, F. Carol y K. Andrzej, «A virtualized honeynet system based on network softwarization,» *IEEE,* 2018.

[8] J. Yacelga, «Estudio de factibilidad y diseño de una red inalámbrica ISP, para proveer servicio de internet en las comunidades de la cuenca del Lago San Pablo,» 2017. [En línea]. Available: http://repositorio.puce.edu.ec/handle/22000/13691.

[9] M. Pinza y F. Cañizares, «Implementación de un ISP para mejorar el servicio de internet con la empresa CSED net en el cantón el Carmen de la provincia de Manabí,» 2018. [En línea]. Available: https://dspace.uniandes.edu.ec/handle/123456789/7563.

[10] W. Machasilla, «Estudio de factibilidad para la creación de un ISP con cobertura en la ciudad de Quito,» 2014. [En línea]. Available: http://repositorio.espe.edu.ec/xmlui/bitstream/handle/21000/8168/T-ESPE-047852.pdf?sequence=1&isAllowed=y.

[11] J. Tomalá, «Diseño de un nodo para ISP de banda ancha para la comuna El Azucar de Santa Elena,» 2016. [En línea]. Available: https://repositorio.upse.edu.ec/xmlui/bitstream/handle/46000/3485/UPSE-TET-2016-0005.pdf?sequence=1&isAllowed=y.

[12] S. Betancourt y C. Morales, «Análisis y diseño de una solución de red ISP WIMAX basada en IEEE802.16M-2011 para las sedes UDLAPARK y Granados de la Universidad de las Américas en la ciudad de Quito,» 2016. [En línea]. Available: http://www.dspace.uce.edu.ec/handle/25000/6868.

[13] W. Abad, «DISEÑO DE UNA RED QUE PROVEA SERVICIOS DE INTERNET (ISP) EN LAS CABECERAS CANTONALES CÉLICA Y CATACOCHA DE LA PROVINCIA DE LOJA,» 2015. [En línea]. Available: https://dspace.unl.edu.ec/jspui/bitstream/123456789/11127/1/Abad%20Ayabaca%2c%20Walter%20Fernando.pdf.

[14] Xfinity Discovery Hub, «¿Qué es un Proveedor de Servicio de Internet (ISP)?,» 29 Mayo 2021. [En línea]. Available: https://es.xfinity.com/hub/internet/internet-service-providers.

[15] Traders.Studio , «Proveedor de servicios de Internet (ISP),» 25 Marzo 2021. [En línea]. Available: https://traders.studio/proveedor-de-servicios-de-internet-isp/.

[16] Binlun, 2018. [En línea].

[17] VMWARE, «Redes definidas por software,» 28 Mayo 2020. [En línea]. Available: https://www.vmware.com/es/topics/glossary/content/software-defined-networking.html.

[18] Ciena, «¿Qué es SDN?,» 9 Septiembre 2017. [En línea]. Available: https://www.ciena.com.mx/insights/what-is/What-is-SDN_es_LA.html.

[19] S. Asadollahi, G. Bhargavi y M. Sameer, «Ryu controller's scalability experiment on software de ned networks.,» *IEEE,* pp. 1-5, 2018.

[20] A. García, C. Rodríguez, C. Anías y C. Casmartiño, «Controladores SDN, elementos para su selección y evaluación.,» *Revista telemática,* vol. 13, pp. 10-20, 2014.

[21] Q. R. C. Julio, «PROPUESTA METODOLÓGICA PARA LA SELECCIÓN DE CONTROLADORES DE REDES SDN A NIVEL EMPRESARIAL,» 2020.

[22] S. Espín, Desarrollo de un honeypot para la monitorización y prevención de ataques., 2017.

[23] T. M. R. Edison, «IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE RED DE DATOS PARA LA TOMA DE DECISIONES DE LA EMPRESA CLICKNET S.A.,» 2016.

[24] H. Aruba, «Controlador HPE VAN SDN,» [En línea]. Available: https://support.hpe.com/hpesc/public/docDisplay?docId=emr_na-c03967699.

[25] C. J. Rodríguez, «Propuesta metodológica para la selección de controladores de redes SDN a nivel empresarial.».

[26] Tech Support HP, «Introduction to the HPE VAN SDN Controller,» nº https://techhub.hpe.com/eginfolib/networking/docs/sdn/sdnc2_7/5200-0910prog/content/c_sdnc-pg-intro.html, 2021.

[27] Mikrotik, «OpenFlow,» 12 Febrero 2018. [En línea]. Available: https://wiki.mikrotik.com/wiki/Manual:OpenFlow. [Último acceso: 2021].

[28] P. S. M. CELMIRA, «ANALISIS Y DISEÑO DE UNA ARQUITECTURA DE RED,» de *Universidad Técnica de Machala*, Machala, 2020.

[29] V. E. Maya, *Detección de incidentes informáticos utilizando Honeypots,* Santa Clara, Cuba: Universidad Central “Marta Abreu” de Las Villas, 2014.

[30] S. M. Z. U. Rashid, «Know Your Enemy: Analysing Cyber-threats,» *IEEE* , 2019.

[31] G. Alvarez, Seguridad en redes ip. Análisis de un sistema conectado a internet, Universidad autónoma de Barcelona, 2003.

[32] J. Ngbinlun, T. S. Chin, L. Ching, Z. Yuso y K. Rizaluddin, «Challenges and direction of hybrid SDN migration in isp networks.,» *IEE,* pp. 60-64, 2018.

[33] G. Borja y C. Ortín, Seguridad y rendimiento en redes híbridas SDN, 2016.

[34] HP Support, «HPE VAN SDN Controller Software - Overview,» 2021. [En línea]. Available: https://support.hpe.com/hpesc/public/docDisplay?docId=emr_na-c03967699.

[35] F. Ávila, «Estudio de Factibilidad Técnica,» 2018. [En línea]. Available: http://opac.pucv.cl/pucv_txt/txt-6000/UCC6148_01.pdf.

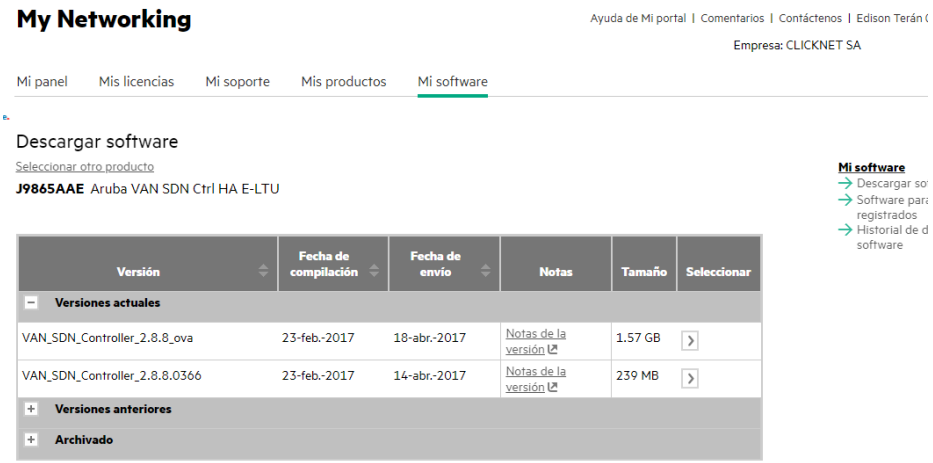
ANEXOS

Instalación de controlador SDN

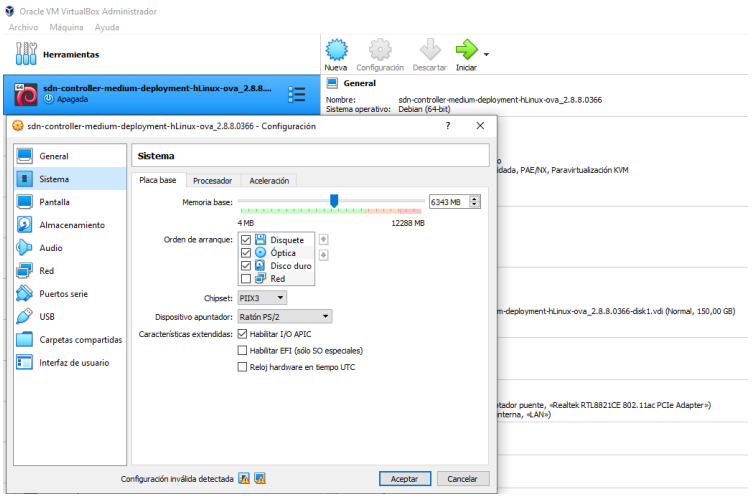
Para la instalación del controlador SDN se procede con la preparación de la máquina virtual, ya que dispone de la capacidad de trabajar con plataforma virtual.

Se prepara el equipo contenedor, en el caso de este proyecto se usó Windows 10.

De la página de HP Aruba se procede a descargar el archivo desde My Networking de HP: h10145.www1.hpe.com, antes hay que registrarse para poder obtener el software.

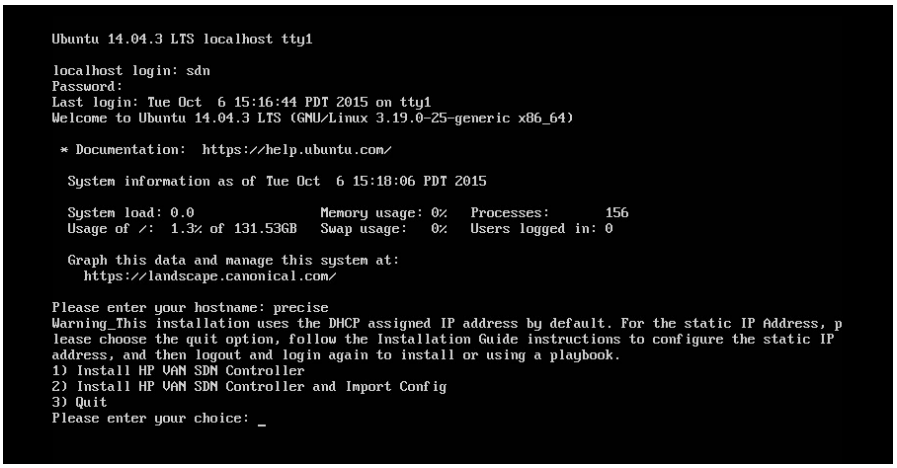


En la plataforma de virtualbox se importa la máquina virtual y se levanta el servicio.

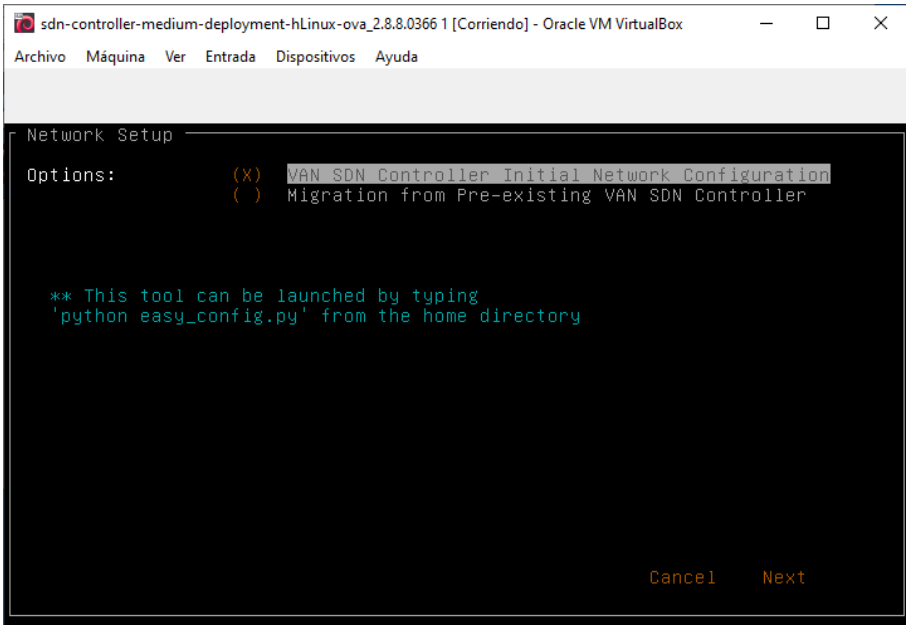


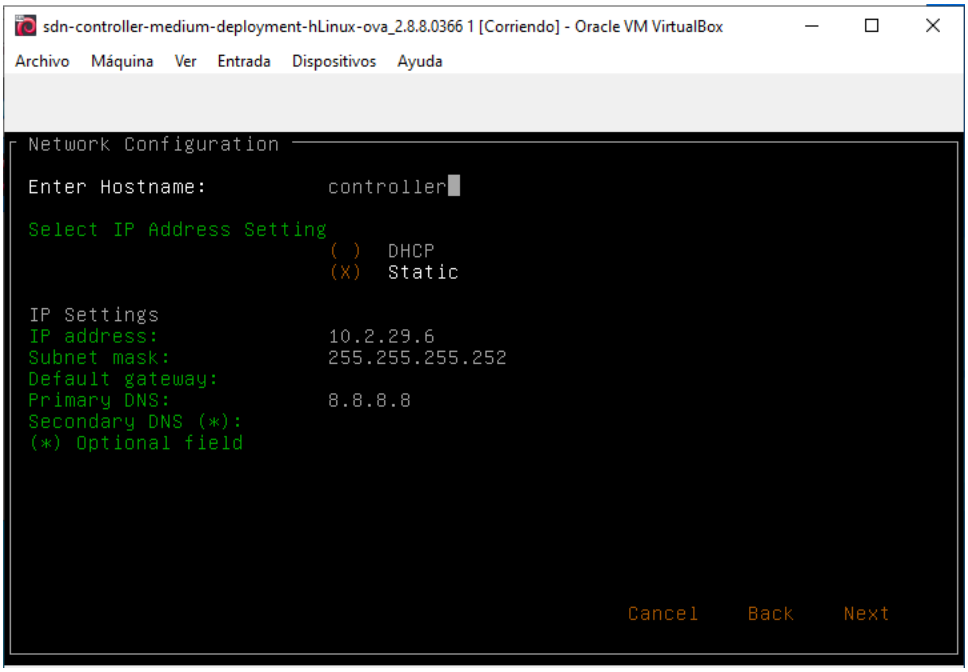
Levantado el servicio nos solicita el User y passswd, que por defecto es sdn y

skyline respectivamente.

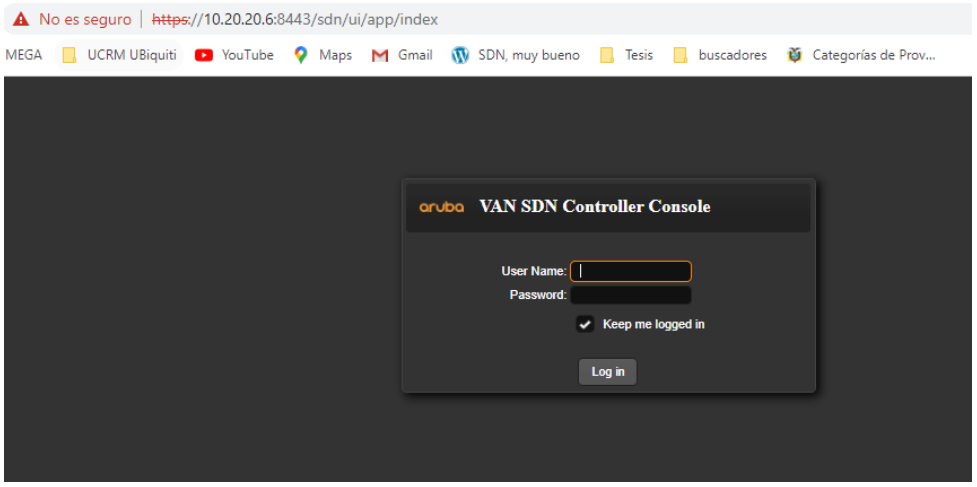


Solicita la configuración de la IP con la que luego se pueda acceder vía web, se debe configurar una IP estática para poder ingresar al servicio.





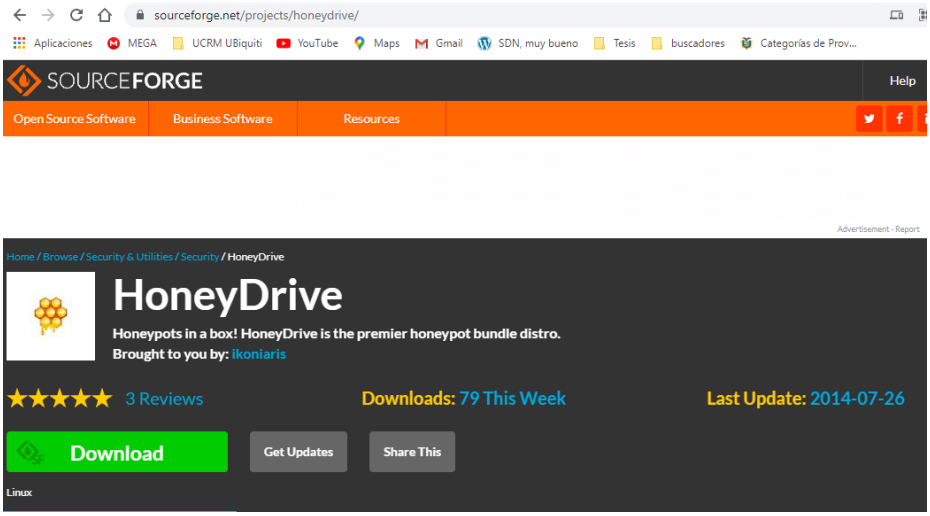
Una vez establecida la IP se ingresa con user y passwd, dirección IP y puerto.



Instalación de Honeypot Honeydrive

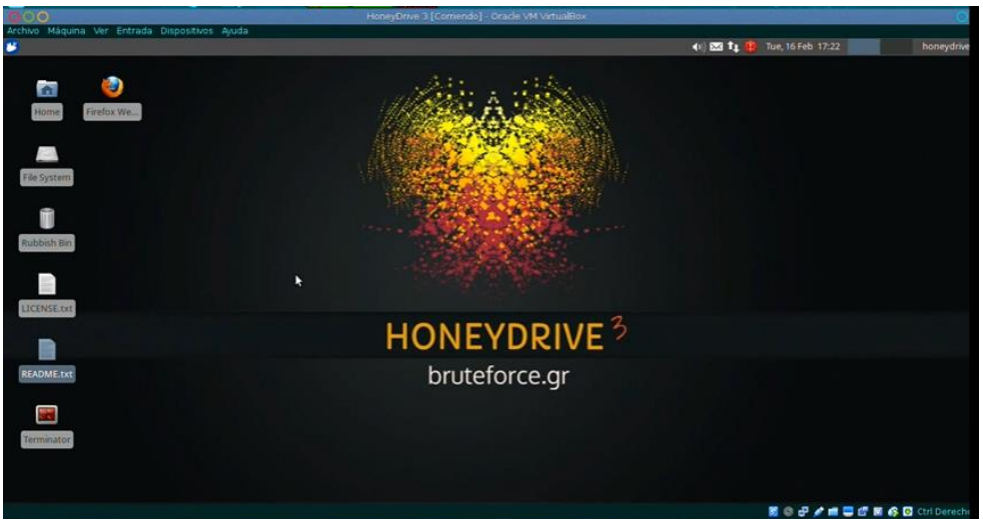
Este software viene en fichero OVA, el mismo que trabaja en plataforma virtual.

El paquete de descarga de este software se obtiene de: https://sourceforge.net/projects/honeydrive/, como se muestra en la figura.



Después de descargar el archivo, simplemente tiene que importar el dispositivo virtual a su administrador de máquina virtual. El software de virtualización recomendado es Oracle VM VirtualBox.

Esta herramienta es en entorno gráfico como se muestra.



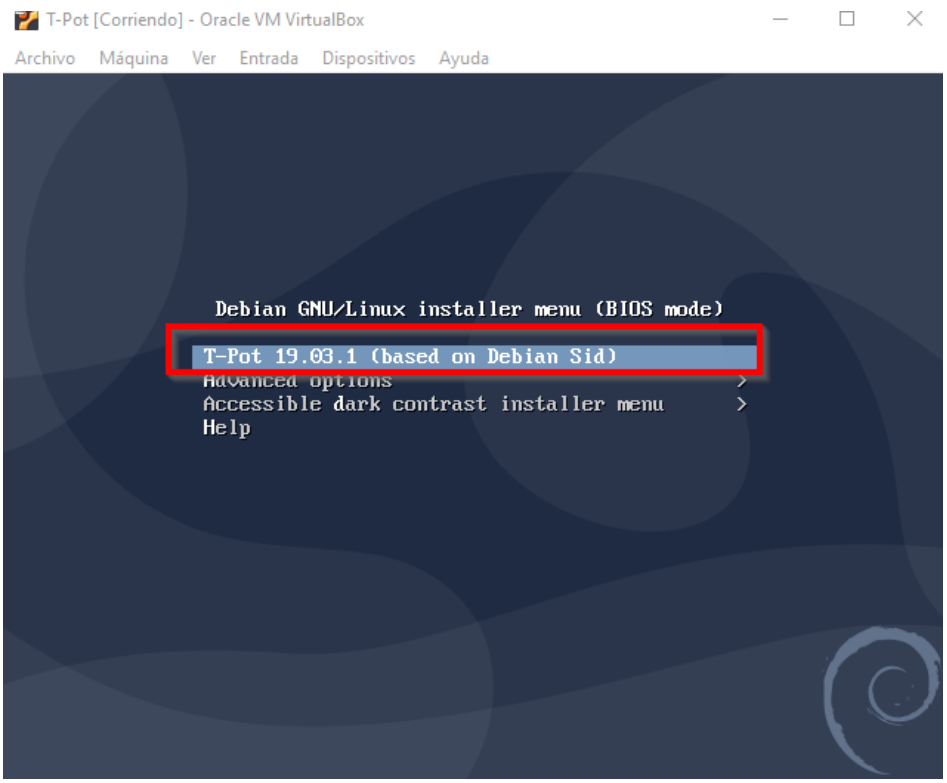
Se accede directamente por medio de navegadores web, por IP y puertos o dominios elegidos.

Instalación de T-POT

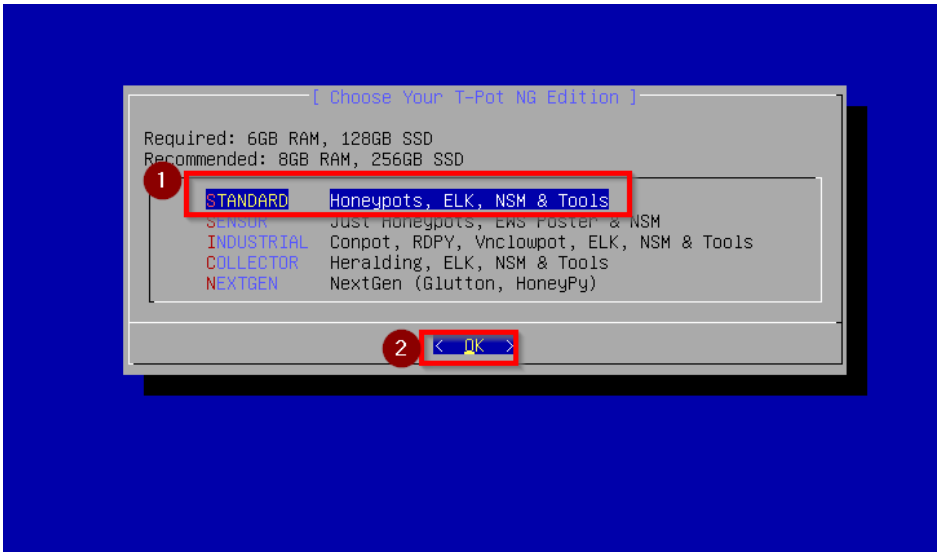
Este software es el más completo de los honeypots, lo primero que hay que hacer es descargarse el ISO desde https://github.com/stackfire/tpotce, hay que instalar desde cero, se aplica también bajo máquina virtual con virtualbox.

Se instala como una máquina de linux, que permite escoger que se quiere instalar

en este caso T-POT.



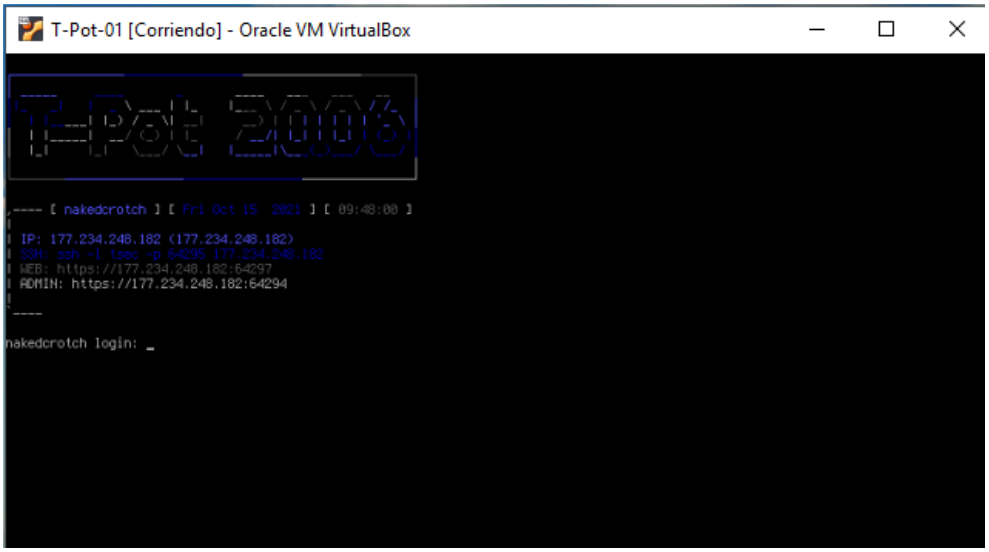
Luego se consulta que tipo de honeypot se requiere instalar.



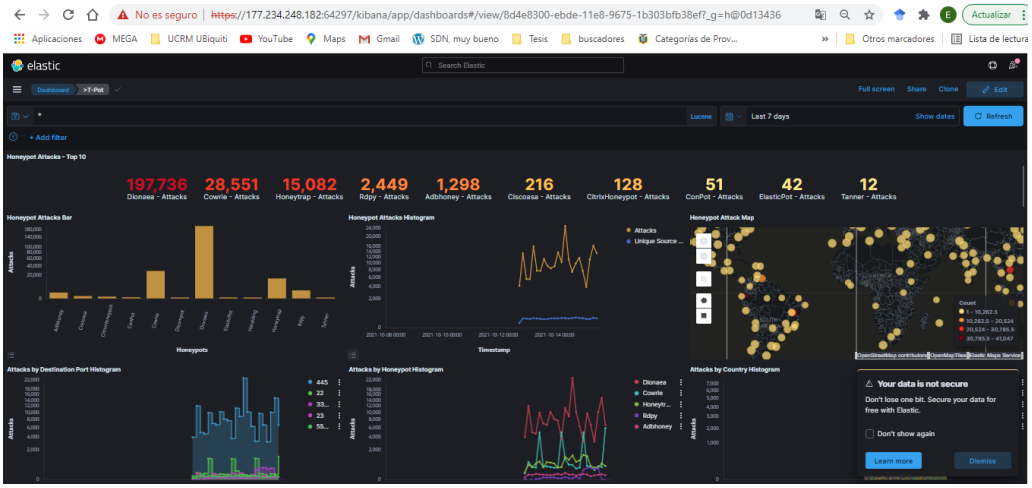
Se elige Estándar.

Solicita la aplicación de usuario y contraseña para poder acceder al sistema y también a los recursos de T-POT.

Finalmente nos muestra la página principal del CLI como se muestra.



Con todo listo se inicia el monitoreo y análisis la cantidad de ataques que recibe un servidor vulnerable, en este caso este software señuelo.



Configuración básica de un Router Mikrotik

La configuración básica de un router para levantar el servicio de OpenFlow una vez cargado el paquete al sistema del RouterOS, es el que viene a continuación.

oct/15/2021 22:05:55 by RouterOS 6.48.3

software id =

#

```
#
#
/interface wireless security-profiles
set [ find default=yes ] supplicant-identity=MikroTik
/openflow
add controllers=10.10.10.10 datapath-id=1/08:00:27:D4:B2:44 disabled=no name=\
    oflow1
/snmp community
set [ find default=yes ] authentication-password=clickdata \
    encryption-password=clickdata name=clickdata write-access=yes
/ip address
add address=10.10.10.1/24 comment=CONTROLADOR interface=ether3 network=\
    10.10.10.0
add address=10.0.1.1/30 comment=WAN01 interface=ether2 network=10.0.1.0
add address=10.10.21.1/24 comment=LAN01 interface=ether4 network=10.10.21.0
/ip dhcp-client
add disabled=no interface=ether1
/ip dns static
add address=3.210.237.154 name=upgrade.mikrotik.com
/ip route
add distance=1 dst-address=10.0.2.0/30 gateway=10.0.1.2
add distance=1 dst-address=10.0.3.0/30 gateway=10.0.1.2
add distance=1 dst-address=10.10.4.0/24 gateway=10.0.1.2
add distance=1 dst-address=10.10.11.0/24 gateway=10.0.1.2
```

```
/openflow port
add disabled=no interface=ether2 switch=oflow1
add disabled=no interface=ether4 switch=oflow1
/snmp
set enabled=yes
/system identity
set name=Router01
/system package update
set channel=long-term
/system scheduler
add name=schedule1 on-event=offopenflow policy=\
    ftp,reboot,read,write,policy,test,password,sniff,sensitive,romon \
    start-time=startup
/system script
add dont-require-permissions=no name=offopenflow owner=admin policy=\
    ftp,reboot,read,write,policy,test,password,sniff,sensitive,romon source="#\
    deshabilita puertos openflow\r\
    \nopenflow port disable numbers=0  \r\
    \nopenflow port disable numbers=1\r\
    \nopenflow port disable numbers=2\r\
    \n\r\
    \n#deshabilita switch openflow\r\
    \nopenflow disable numbers=oflow1\r\
    \n\r\
    \n"
/system watchdog
```

```
set watch-address=10.0.1.2
```