IMPLEMENTACIÓN DE UN FIREWALL CONSTRUIDO A PARTIR DE SOFTWARE Y UNA PLACA DE CIRCUITOS COMPACTA O SBC (SINGLE BOARD COMPUTER) EN LA EMPRESA TAIO SYSTEMS DE LA CIUDAD DE POPAYÁN

JUAN SEBASTIAN CHICAIZA PAREJA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERIA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
POPAYÁN
2017

IMPLEMENTACIÓN DE UN FIREWALL CONSTRUIDO A PARTIR DE SOFTWARE Y UNA PLACA DE CIRCUITOS COMPACTA O SBC (SINGLE BOARD COMPUTER) EN LA EMPRESA TAIO SYSTEMS DE LA CIUDAD DE POPAYÁN

JUAN SEBASTIAN CHICAIZA PAREJA

Trabajo de grado para optar el título de Especialista en Seguridad Informática

Línea de Investigación: Infraestructura tecnológica y Seguridad en Redes

Director

JULIO VARGAS
Ingeniero de Sistemas

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERIA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
POPAYÁN
2017

Nota de aceptación

Firma del Director

Firma del Jurado

Firma del Jurado

Popayán, Febrero de 2018

CONTENIDO

pág.

LISTA DE TABLAS

pág.

LISTA DE FIGURAS

pág.

GLOSARIO

Teniendo en cuenta la finalidad de este proyecto que se basa en el desarrollo de un *appliance* de seguridad conformado por una placa de circuito compacta o SBC y *software* libre es necesario aclarar al lector de los conceptos que se van a plasmar en este documento.

Appliance: es un término que se utiliza para describir dispositivos provistos de *hardware* y *software* que tienen una finalidad específica, en nuestro contexto el *hardware* será la SBC y el *software* será el *firewall* de licencia para contenidos libres o GNU. Existen distintos tipos de *appliance*, pero se hace énfasis en el *appliance* de seguridad que incorpora distintas herramientas de monitoreo y detección, que posee características de UTM.

UTM: su sigla en inglés significa *Unified Threat Management* o Gestión Unificada de Amenazas o comúnmente llamado cortafuegos o *firewall* que posee diferentes características y/o servicios que ayudan a la protección de las redes, posee características específicas que son:

- Función de inspección de paquetes
- Antispam
- Función de VPN
- Antiphishing
- Antivirus
- Filtrado de contenidos
- Antispyware
- Detección/Prevención de Intrusos (IDS/IPS)

Los dispositivos UTM son importantes en el momento que se desee proteger el acceso a nuestra red, así mismo tener control del tráfico interno que se genera, ayudándonos en la implementación de políticas de acceso de páginas, puertos, y horarios. Estos dispositivos analizan el tráfico en tiempo real y según sus políticas implementadas brindan o deniegan el acceso ya sea desde la red interna hacia internet o desde internet hacia nuestra red.

Existen muchos fabricantes de estos dispositivos como FortiNet, CISCO, 3COM, etc, pero estos dispositivos requieren licenciamiento adicional para utilizar todas sus funciones.

Firewall: es un sistema que se centra en crear una barreara de seguridad del tráfico de entrada y de salida de una red de datos, permitiendo o denegando el acceso. Actúa a base de políticas o reglas establecidas por quien lo administre. Dichas políticas definen las acciones que se ejecutan al recibir un paquete de datos que debe cumplir con ciertas características, esta herramienta protege la red de servicios y protocolos que puedan suponer una amenaza o generen vulnerabilidades a la seguridad, a esta parte que es aislada por el *firewall* o cortafuegos de le denomina perímetro de seguridad.

SBC (single board computer) o placa de circuitos reducida: es un dispositivo el cual integra todas sus partes en una sola placa procesador, memoria RAM, conectores, etc.

INTRODUCCION

En la actualidad la información se ha convertido en uno de los activos más preciados para las empresas, debido a esto es necesario protegerla o resguardarla creando controles o medidas que permitan garantizar el correcto funcionamiento de la empresa, monitoreando y asegurando la integridad de la información.

Ya que las empresas se han visto en la necesidad de adquirir herramientas que le permitan expandir más sus negocios han adoptado el Internet como un medio esencial y primordial para su funcionamiento, pero no han detectado ni evaluado los riesgos a los que está expuesta su información almacenada en equipos o servidores en forma de documentos, planos, hojas de cálculo o bases de datos, por lo tanto es de suma importancia evitar la pérdida de información, daños en su parque tecnológico tanto *software* como *hardware*.

Para satisfacer dichas necesidades de Seguridad de la Información se han creado dispositivos especializados en el monitoreo del tráfico de red que incorporan diferentes características, siendo muy necesarios en la implementación de un modelo de seguridad y privacidad de la información, controlando el acceso y monitoreando todo tipo de anomalías en una red, de esta manera se genera la propuesta de construcción de un *firewall* de bajo costo, que aportara a la implementación de controles de la seguridad perimetral en la empresa TAIO SYSTEMS adoptando políticas a nivel del *firewall* que aportaran a mejorar la seguridad de los datos, generando un control de tráfico.

Este proyecto consiste en la construcción, documentación y configuración de una herramienta que permitirá crear controles de seguridad perimetral dentro del contexto de acceso y administración de la red, abarcando dentro de esta solución el diseño de las herramientas, métodos y técnicas a utilizar para el levantamiento de la información, para finalmente conformar una propuesta que apoyara a la gestión de seguridad de la información con el fin de mitigar los riesgos. La propuesta será presentada ante la gerencia de la empresa, para su implementación.

1. EL PROBLEMA DE INVESTIGACIÓN

1.1 PLANTEAMIENTO DEL PROBLEMA

En la actualidad las empresas tienen como finalidad ser más competitivas, dentro de sus objetivos tienen planteado prestar un mejor servicio, para satisfacer las necesidades de los usuarios y evitarles grandes desplazamientos innecesarios. Lo anterior debido o basado en el gran crecimiento digital que se ha venido desarrollando desde hace unos años. Es por esta razón que las empresas están en la constante búsqueda de diferentes herramientas que permitan brindar a sus usuarios mejores servicios con ayuda de las tecnologías, y con ello generar una mejor comunicación con los mismos. Sin embargo, muchas veces se deja de lado o se olvidan los riesgos que se pueden originar en un ambiente que no cumpla con la adopción de controles o medidas encargadas de evitar un inadecuado funcionamiento de los procesos y mantener la eficiencia de los mismos, además de eludir pérdidas importantes de dinero, credibilidad de las empresas y aumento en el tiempo de ejecución de proyectos.

"Al 80% de las Pymes de Latinoamérica les preocupa la seguridad, a pesar de ello, el 98% no considera este aspecto como una prioridad dentro de sus organizaciones, indica un estudio elaborado por IDC, y es que no saben cómo están siendo atacadas ni cómo se comportan los códigos maliciosos"[1]

Las soluciones de seguridad existentes para la infraestructura y dispositivos de las empresas, requieren demasiado poder adquisitivo un ejemplo de esto son los *firewalls* UTM usado principalmente para asegurar el área perimetral de la red, que además se encarga de prevenir y proteger los datos y dispositivos, sin embargo, como se mencionó anteriormente, es muy costoso implementarla. Para las Pymes como TAIO SYSTEMS dedicadas principalmente a la Innovación y que actualmente se encuentran en proceso evolutivo este tipo de soluciones son difíciles de adquirir, debido a que no posee el personal idóneo para implementar estas herramientas, no cuenta con los recursos necesarios para comprarlas y mantenerlas, optando por soluciones que no son lo suficientemente efectivas a los riesgos y ataques que se derivan de las vulnerabilidades de una organización expuesta sin la implementación de controles de seguridad y medidas preventivas que permitan resguardar la información.

[1] SÁNCHEZ, Marcelo. 98% de las Pymes de Latinoamérica no invierten en seguridad [citado junio 5, 2016]. Disponible en internet: <https://www.entrepreneur.com/article/258834>

Según Oscar Díaz “el costo de la seguridad es para los negocios el principal obstáculo para resguardar su información debido a que "no se hacen conciencia de que un ataque puede interrumpir la producción, disminuir su rendimiento e incluso deteriorar la reputación de la empresa "[2].

Es importante mencionar que a raíz de este problema han surgido múltiples propuestas o soluciones de *software* libre, sin embargo, las empresas que los adquieren por su condición de “empresa pequeña” no cuenta con los espacios o ambientes controlados con el que puedan asegurar el adecuado y correcto funcionamiento de los equipos en los que pueden ser instalados los cortafuegos, tales como PFSENSE, IPCOP, IPFIRE, CLEAROS, entre otros.

Partiendo de lo anterior es posible afirmar que los delincuentes informáticos prefieren las Pymes ya que presentan una barrera menor para lograr infiltrase en su parque tecnológico, teniendo en cuenta que la información es el activo más importante para cualquier empresa es necesario implementar controles físicos y lógicos que permitan evitar los actos delictivos dentro de las empresas tales como robo, suplantación, modificación y eliminación de la información, generando una necesidad primordial de buscar alternativas que permitan controlar la seguridad informática de la empresa, siendo el mayor problema en las Pymes la falta de adopción de controles de seguridad en cuanto al tráfico de la red de datos de la empresa.

Teniendo en cuenta el contexto planteado anteriormente es posible afirmar que la empresa TAIO SYSTEMS no es ajena a esta situación ya que cuentan con dos canales de internet sin ningún cortafuegos, barrera o herramienta que permita restringir o detener el tráfico no deseado como conexiones entrantes de los atacantes o trafico malicioso desde los equipos que puedan ser infectados, ya sea visitando sitios web infectados, correos electrónicos con virus o simplemente al conectar una memoria USB, creando brechas de seguridad que permitirán que los atacantes puedan efectuar sus actividades ya mencionadas, poniendo en riesgo toda la integridad de la infraestructura TI, bases de datos e información primordial para la empresa TAIO SYSTEMS.

[2] Citado en: seguridad informática costosa para las empresas, 30 marzo 2009. [citado junio 10, 2016] Disponible en internet < http://elempresario.mx/asesoria/seguridad-informatica-costosa-empresas>

1.2 FORMULACIÓN DEL PROBLEMA

¿En qué medida un *Firewall* construido a partir de una placa de circuitos compacta y *software* libre puede mejorar la protección y seguridad de la red de datos de TAIO SYSTEMS?

2. JUSTIFICACIÓN

Para TAIO SYSTEMS como para todas las demás empresas, la información es el activo más importante en todo su marco de negocio. Sin embargo, según certicamara las amenazas cibernéticas crecen a una proporción de 60 %, el presupuesto asignado en las compañías públicas y privadas apenas llega al 10 % del total de los gastos.” [3].

Partiendo de lo anterior es posible afirmar que son muy pocas las empresas que han detectado sus falencias en tema de seguridad y privacidad de la información, adoptando herramientas que garanticen la trazabilidad y continuidad de la empresa, las demás invierten en soluciones que no permiten realizar un verdadero control sobre información esencial para el funcionamiento, exponiendo su infraestructura TI y su parque tecnológico sin tener en cuenta sus vulnerabilidades.

“La seguridad informática es costosa de implementar, pero más costoso es recuperarse de los daños causados por un ataque informático.”[4]

Con este proyecto se busca generar una propuesta que contribuya al control y detección de riesgos o vulnerabilidades que pueda afectar la seguridad de la información de la empresa, el cual permitirá concebir controles de acceso y herramientas que se unificaran en un solo dispositivo, permitiendo la creación de mecanismos y medidas que apoyaran el control del tráfico de datos, que se genera en la infraestructura tecnológica de la empresa.

En la actualidad existen múltiples soluciones que se encuentran en el mercado como FORTIGATE, FIREEYE, CISCO ASA, WATCH GUARD XTM, entre otros, sin embargo estas soluciones pueden llegar a ser muy costosas generando gastos adicionales a futuro como renovación de licencias y mantenimientos específicos, dado la naturaleza de estos dispositivos es necesario mantener un área donde se garantice características definidas por sus fabricantes como refrigeración,

[3] Las empresas en Colombia no invierten en seguridad digital. Revista Semana. 9 de junio de 2016 [citado junio 24, 2016]. Disponible en internet <http://www.semana.com/tecnologia/articulo/colombia-no-invierte-en-seguridad-digital/492724 >.

[4] Mateo, Santos. los ataques informáticos cuestan 11,6 millones al año por empresa. Revista electrónica Enter.co, 1 de noviembre de 2013. [citado junio 24, 2016]. Disponible en internet < http://www.enter.co/chips-bits/enterprise/el-costo-de-los-ataques-informaticos-supera-los-32-millones-de-dolares >.

continuidad de fluido eléctrico y otras especificaciones, por esta razón se ha propuesto construir un *appliance* de seguridad versátil a un bajo costo en relación a otros dispositivos, que apoyara la implementación de controles para mitigar los ataques y riesgos que pueden ocasionar daños o robo a la información, monitoreando el tráfico en la red de las empresa en tiempo real adoptando controles que tendrán como objetivo apoyar al mejoramiento y mantenimiento de un nivel de seguridad de la información en cuanto a la red de datos de la empresa usando herramientas para crear políticas y controles que estarán enfocados en afirmar el mejoramiento del nivel de seguridad lógico de la empresa.

3. OBJETIVOS

3.1 OBJETIVO GENERAL.

Mejorar la seguridad perimetral de la empresa TAIO SYSTEMS mediante un appliance de seguridad de bajo costo construido a partir de *software* libre y una placa de circuitos, y configurado de acuerdo a las características de red organización.

3.2 OBJETIVOS ESPECÍFICOS

- Realizar levantamiento de información con respecto a la infraestructura de la red de la empresa TAIO SYSTEMS
- Diseñar un dispositivo de seguridad según los requerimientos de la empresa TAIO SYSTEMS.
- Implementar el dispositivo en la red de la empresa TAIO SYSTEMS
- Realizar pruebas de funcionamiento y rendimiento del dispositivo para corregir posibles fallos.

4. MARCO DE REFERENCIA

4.1 ANTECEDENTES DE INVESTIGACIÓN

Comprendiendo la gran acogida que tienen las soluciones de libre distribución y sus aportes por todos los miembros de esta comunidad se han presentado múltiples teorías de la utilización de este *software*, a continuación, se hace referencia a algunos proyectos enfocado a la utilización de *software* libre como aporte a la seguridad informática y propuestas para el manejo de SBC (SINGLE BOARD COMPUTER) o placa de circuitos reducida en diferentes ámbitos.

El trabajo realizado por Echeverry, D. (2011), con título *PROPUESTA E IMPLEMENTACIÓN DE UN APPLIANCE DE SEGURIDAD A PARTIR DEL RE-USO TECNOLÓGICO*, como trabajo de grado ingeniería de sistemas, Pereira, Universidad Católica De Pereira. Esta propuesta es una de las que más se asemeja al presente proyecto ya que consiste en desarrollar un *firewall* con la excepción que se conforma a partir de la reutilización de equipos obsoletos y *software* libre llegando así a la construcción de un dispositivo que integra diferentes características.

Otro proyecto que aporta conocimientos y metodologías para el desarrollo de esta propuesta es el realizado por Brito, A y Tirado, J. (2016), titulado *ARQUITECTURA DE UN SISTEMA C4ISR PARA PEQUEÑAS UNIDADES*, ingeniería en electrónica y control, Quito, Escuela Politécnica Nacional, el cual analiza los tipos de SBC disponibles en el mercado para el desarrollo de un robot utilizando características especiales para su funcionamiento.

Un ejemplo claro de éxito con la implementación de un *firewall* para la protección de una red mediante el uso de un *firewall* libre es el proyecto realizado por Lopez, J. (2010) titulado *DISEÑO DE UN PROTOTIPO QUE PERMITA EVALUAR LA VIABILIDAD DE UN FIREWALL EN REDES SCADA*, ingeniería de sistemas, Bogotá, Fundación Universitaria Konrad Lorenz, el cual usa un *firewall* para la protección de una red privada

Otro trabajo más acercado a esta propuesta es el de Martínez K, Pacheco J (), Zúñiga Titulado *FIREWALL-LINUX: UNA SOLUCIÓN DE SEGURIDAD INFORMÁTICA PARA PYMES (PEQUEÑAS Y MEDIANAS EMPRESAS)*, Universidad Industrial de Santander el cual consiste en la implementación de *firewall* de Linux usando las IPTABLES del sistema creando políticas o controles

Un proyecto a tener en cuenta es el desarrollado o propuesto por Morales C. (2002) titulado *ESTUDIO, DISEÑO E IMPLEMENTACIÓN DE UN FIREWALL*
el cual consiste en la implementación y evaluación de rendimiento de un *firewall*.

Un ejemplo más es el de Du R., Safavi R., Susilo W titulado *Design and Implementation of A Content Filtering Firewall* (Diseño e implementación de un *firewall* de filtrado web) Australia, *University of* Wollongong, el cual tiene como objetivo presentar el diseño e implementación de un *firewall* para hacer control del contenido web de una red.

Este trabajo también es relevante para esta propuesta ya que consiste en el desarrollado por Martinsen P. titulado *Configuration And Implementation Issues For A Firewall System Running On A Mobile Handset*, Queensland *University* of *Technology*, el cual busca implementar un servidor *firewall* para los dispositivos móviles

4.2 MARCO TEÓRICO – CONCEPTUAL

Se ha formulado esta propuesta apoyándose en que un dispositivo de seguridad perimetral, aporta considerablemente a la construcción de un sistema de gestión de seguridad de la información, ya que existen metodologías y buenas practicas que ayudan en la implantación de este sistema como lo son la familia de normas ISO 27000 que son un conjunto de estándares que pueden ser aplicado a cualquier empresa que busque mejorar o implementar una serie de políticas para asegurar su información, para prevenir gran cantidad de riesgo, como lo es la norma ISO 27002 que establece una serie de buenas prácticas describiendo controles y objetivos de control recomendables en cuanto a seguridad de la información pero algunas pymes presentan un gran número de problemas, debido a que no prestan atención a la seguridad de su información, al pensar que los ataques informáticos solo se hacen a o están enfocados a grandes empresas, sumado que no cuentan con un modelo definido de mitigación o tratamiento de riesgos, no poseen controles o medidas de prevención, generando brechas de seguridad que las hacen más vulnerables. En múltiples estudios se ha concluido que las pymes no invierten en seguridad informática, lo que da a entender que las pymes se han descuidado en el tema, facilitando el trabajo para los cyber-delincuentes que están en busca de información, Kevin Haley, director de la unidad de respuesta de seguridad de Symantec, dice que “Las PYMES no están tan preparadas porque piensan que no es necesario y eso las ha dejado vulnerables”, argumento que se base en la falta de recursos de estas empresas, personal idóneo que permita realizar una planeación y gestión debida de la seguridad.

De acuerdo a la preocupación en temas de seguridad de la información han surgido gran cantidad de dispositivos y componentes que ayudan a implementar los controles que una empresa necesita para crear un marco en el cual se involucren gran número de herramientas como control de acceso, detección de intrusos, antivirus entre otros.

En respuesta a esta problemática se han formulado propuestas que pueden ser satisfactorias en materia de construcción de controles, pero que pueden ser inalcanzables para las PYMES por esta razón se ha investigado sobre iniciativas donde se usan microprocesadores en placas de circuitos reducidas, haciendo que el costo de este *hardware* sea más menor en relación a los demás, como los son las SBC. Existen un gran número de modelos y marcas, entre las más reconocidas están RASPBERRY PI, ARDUINO, BANANA PI, BEAGLEBOARD, entre otros. Estos dispositivos utilizan sistemas embebidos y se usan con fines específicos en donde se exige gran demanda de procesamiento para control de procesos o funciones, al indagar más sobre el tema se puede apreciar que la SBC o placa de circuitos reducida RASPBERRY PI se desarrolló con el fin de estimular la educación haciendo un dispositivo robusto de bajo costo en pro de brindar una solución de calidad.

De esta manera se ha propuesto usar un *firewall* llamado IPFIRE que es una variedad de IPCOP solo que usa la arquitectura ARM compatible con la serie de procesadores que usan algunas SBC, este *firewall* brinda gran cantidad de herramientas para implementar controles en una red de datos por tal motivo se ha formulado la propuesta de investigación de construcción y funcionamiento del *appliance* de seguridad tratando de generar respuesta a la problemática de las PYMES ya que no se evidencian estudios en los cuales se pueda comprobar la capacidad que brindan las SBC como dispositivo de seguridad que monitoree y controle el tráfico de datos en tiempo real.

Para desarrollar el trabajo mencionado se basará en teorías y conceptos que se presentan a continuación.

4.2.1 Seguridad Informática. Se entiende como seguridad informática "la disciplina que se ocupa de diseñar las normas, procedimientos, métodos y técnicas, orientados a proveer condiciones seguras y confiables, para el procesamiento de datos en sistemas informáticos."[5] Por esta razón es posible afirmar que la seguridad informática abarca todo lo relacionado con los procedimientos, normativas y herramientas encargadas de asegurar un buen uso de información, además de su confidencialidad e integridad.

Es muy usual encontrar que al hablar de seguridad se entienda esta como a la certeza total de la falta de riesgo o contingencia, sin embargo no es posible tener la certeza total de dicha seguridad, el riesgo es algo que siempre está presente independientemente de las medidas que se tomen, es por ello que es de vital

[5] RÍOS, Julio. Seguridad informática, Disponible en internet < http://www.monografias.com/trabajos82/la-seguridad-informatica/la-seguridad-informatica.shtml >

importancia establecer niveles de seguridad, de esta manera la seguridad informática es un conjunto de técnicas o estrategias que buscan obtener altos niveles de seguridad en los sistemas informáticos, lo cual a su vez, requiere un nivel organizativo.

De igual manera es importante mencionar que la seguridad informática también consiste en asegurar que los recursos del sistema de información (material informático o programas) es decir, garantizar que la información de una organización o empresa sean utilizados, modificados o tratados por el personal que está acreditado y autorizado para hacerlo.

Como se mencionó anteriormente la seguridad informática es una de las divisiones o niveles de la seguridad de la información, que busca la protección de un parque tecnológico, esta parte de la seguridad de la información busca proteger dos aspectos esenciales: la seguridad física y la seguridad lógica, donde la seguridad física enmarca la protección de los medios de distribución y almacenamiento de la información frente a los desastres asociados a daños eléctricos, robos, inundaciones, etc. Y por otra parte La seguridad lógica busca proteger todo aquello comprendido como lógico ya sea sistema operativo, aplicaciones y datos mediante componentes que reduzcan el riesgo de pérdida de información.

La seguridad de la información se divide en seguridad activa la cual se encarga de prevenir, detectar y evitar los daños en los sistemas de información antes que se originen, esto con la ayuda de mecanismos que apoyen la prevención de incidentes como antivirus, *firewall*, contraseñas, entre otros también comprende la seguridad pasiva que abarca los procesos y procedimientos que son requeridos para disminuir las consecuencias de un incidente de seguridad como un sistema de recuperación (*Backups*), sistemas de respaldo, entre otros.

La seguridad informática tiene como deber, establecer normas que aporten o minimicen los riesgos de la información o la infraestructura informática, dichas normas deben incluir restricciones a ciertos lugares, autorizaciones, horarios de funcionamiento, perfiles de los usuarios, denegaciones, protocolos, planes de emergencia y demás características necesarias para lograr un buen o alto nivel de seguridad, logrando minimizar el impacto en el desempeño de los trabajadores y de la entidad.

La seguridad informática se ejecuta para proteger los activos informáticos como la infraestructura computacional, la cual es de gran importancia para el almacenamiento y gestión de la información, esta debe velar por que los equipos funcionen de manera eficaz y adecuada además de anticiparse ante robos, ataques, incendios, entre otros.

Como es notorio en el mundo existen gran cantidad de personas dedicadas a buscar el acceso a los datos de diferentes ordenadores o equipos, este acceso no autorizado puede ocasionar problemas o fallas graves en su mayoría, por ejemplo la perdida de datos, lo cual sucede constantemente y genera grandes problemas porque no siempre es posible recuperar los datos en su totalidad, el robo de información es otro de los grandes riesgos, se puede generar la divulgación de dicha información, lo cual trae consecuencias como demandas.

Es por razones como las anteriormente mencionadas que es de gran importancia contar con seguridad informática dentro de las empresas y tener en cuenta los servicios que esta presta, entre los principales son, primero la confidencialidad la cual básicamente es la capacidad que se tiene para asegurar que solo las personas autorizadas tendrán acceso a cierto tipo de información, este es un aspecto de gran importancia dentro de lo que es la seguridad, ya que representa tener la información privada y de esta manera lograr tener la información y recursos protegidos.

La confidencialidad provee protección a los recursos y de la información en términos del almacenamiento y la información, "Se refiere a la privacidad de los elementos de información almacenados y procesados en un sistema informático, Basándose en este principio, las herramientas de seguridad informática deben proteger el sistema de invasiones y accesos por parte de personas o programas no autorizados. Este principio es particularmente importante en sistemas distribuidos, es decir, aquellos en los que los usuarios, computadores y datos residen en localidades diferentes, pero están física y lógicamente interconectados"[6].

Por otra parte, la autenticidad es otro servicio fundamental de la seguridad informática, además de esto es uno de los más sencillos de asimilar. Este busca verificar la identidad de algo o alguien. Es posible comparar esta con la identificación como la firma personal o las contraseñas si se refiere a un equipo, esta se requiere para generar una prueba en el sistema la cual demuestre que es quien menciona ser, es decir permite verificar la información que la persona ingresa con la información guardada en el sistema. Para realizar la autenticación se utilizan medios como contraseñas o números de identificación los cuales pasan a ser verificados. También mediante tarjetas o pasaportes que permitan comprobar la identidad, o estrategias un poco más complejas como el reconocimiento de voz, retina, huellas dactilares o del rostro.

La integridad es el tercer servicio que debe brindar la seguridad informática, este se refiere principalmente a la validez y constancia de los elementos de información

---

6 REVUELTO, Carlos. Seguridad informática, [citado junio 28, 2016]. Disponible en internet < https://estudiantes.elpais.com/EPE2016/periodico-digital/ver/equipo/3165/articulo/seguridad-informatica >

almacenados y procesados en un sistema. Partiendo de lo anterior es posible afirmar que las herramientas de la seguridad informática están en la tarea de garantizar que los procesos de actualización estén sincronizados y no se dupliquen, asegurando así que se manipulen adecuadamente los datos del sistema. La importancia de este servicio está ligada principalmente en sistemas donde los diferentes usuarios, procesos y equipos compartan la misma información, la integridad va a asegurar y revisar que la información que se transmita mediante cualquier medio no padezca de modificaciones sin la autorización pertinente.

Por último, el control de acceso es otro servicio fundamental, donde se busca limitar y controlar el acceso a los sistemas y aplicaciones, todo esto mediante puentes de comunicación, es decir cuando una organización o entidad busca el control debe inicialmente autenticarse, y con ello lograr que los derechos de acceso sean adaptados de forma individual. “Un control de acceso se ejecuta con el fin de que un usuario sea identificado y autenticado de manera exitosa para que entonces le sea permitido el acceso.”[7]

Uno de los elementos de seguridad informática que cuenta con mayor publicidad es el *firewall*, sin embargo, debe ser uno de los sistemas que cuente con mayor atención.

4.2.2 Problemas de seguridad en PYMES. Debido al gran crecimiento digital las empresas que desean ser más competitivas, han buscado herramientas para prestar mejores servicios con ayuda de las tecnologías, tratando de generar una comunicación directa con sus usuarios, pero muchas veces no se tiene en cuenta los riesgo que se generan en un ambiente sin la adopción de controles o medidas que buscan evitar el mal funcionamiento de los procesos y mantener la eficiencia de los mismos, impidiendo pérdidas importantes de dinero, credibilidad de las empresas y aumento en el tiempo de ejecución de proyectos.

Las actuales soluciones de seguridad existentes para la infraestructura y dispositivos de las empresas, requieren demasiado poder adquisitivo, para las Pymes que actualmente se encuentran en proceso evolutivo lo que genera cierta dificultad para la adquisición de estos dispositivos. Las pymes presentan un gran número de problemas, debido a que no prestan atención a su seguridad al pensar que los ataques informáticos solo se hacen a grandes empresas y no cuentan con un modelo definido ya que al no poseer controles surgen brechas de seguridad que las hacen más vulnerables, como lo expone Mateo Santos en el artículo “LOS

[7] Universidad Nacional Autónoma de México. Fundamentos de Seguridad informática, [citado junio 28, 2016]. Disponible en internet < http://redyseguridad.fi-p.unam.mx/proyectos/seguridad/ServControl.php >

RETOS DE SEGURIDAD PARA LAS PYMES" de la revista ENTER.CO, en donde Diego Gómez Sevilla, gerente de territorio para Pymes menciono "*es que las empresas no invierten en seguridad sino que reaccionan a un ataque*"[8], lo que da a entender que las pymes se han descuidado en el tema, facilitando el trabajo para los cyber-delincuentes que están en busca de información.

De esta manera los delincuentes informáticos prefieren las Pymes ya que presentan una barrera menor para lograr infiltrase en su parque tecnológico, teniendo en cuenta que la información es el activo más importante para cualquier empresa es necesario implementar controles físicos y lógicos que permitan evitar los actos delictivos dentro de las empresas tales como robo, suplantación, modificación y eliminación de la información, generando una necesidad primordial de buscar alternativas que permitan controlar la seguridad informática de la empresa, siendo el mayor problema en las Pymes la falta de adopción de controles de seguridad en cuanto al tráfico de la red de datos de la empresa.

En la actualidad existen múltiples soluciones que se encuentran en el mercado sin embargo estas soluciones pueden llegar a ser muy costosas generando gastos adicionales a futuro como renovación de licencias y mantenimientos específicos, dado la naturaleza de estos dispositivos es necesario mantener un área donde se garantice características definidas por sus fabricantes como refrigeración, continuidad de fluido eléctrico y otras especificaciones.

Al existir tantos riesgos a los que está expuesta la información en medios digitales como robo, falsificación, fraude, divulgación o destrucción entre otras más, conducen a la necesidad de crear o emplear herramientas y controles que garanticen un ambiente confiable, pero conseguir la mejor solución hace parte de muchos factores ya que todas las empresas no poseen las mismas características.

Por esta razón se han creado múltiples enfoques de seguridad que tienen el propósito de aplicar medidas de seguridad en diferentes capas.

Una de las capas es el perímetro límite, que separa la red interna de las empresas de Internet o de otras redes, una característica de cualquier empresa que posea un canal de Internet, por esta razón en la seguridad perimetral, los *firewalls* son los dispositivos o medidas más usados para la protección de la información. Según ESET[9] los controles más utilizados en las empresas son los *firewall*, en conjunto con los antivirus.

---

[8] MATEO, Santos. , LOS RETOS DE SEGURIDAD PARA LAS PYMES. Revista electrónica ENTER.CO, 7 de mayo de 2013. [citado junio 24, 2016]. Disponible en internet < http://www.enter.co/especiales/enterprise/los-retos-de-seguridad-para-las-pymes/ >

[9] MENDOZA, Miguel, ¿Por qué es necesario el firewall en entornos corporativos?, julio 29, 2014. [citado julio 30, 2016]. Disponible en internet <

4.2.3 Soluciones que brinda el mercado para mejorar el nivel de seguridad de la infraestructura TI. Un *firewall* o cortafuegos, es un *software* o *hardware* utilizado para mantener la seguridad de una red privada. El cortafuegos bloquea el acceso no autorizado o de redes privadas y, a menudo se emplean para evitar que usuarios no autorizados o que usan *software* ilícito tengan acceso a redes privadas conectadas a Internet.

Un servidor de seguridad puede implementarse utilizando *hardware*, *software*, o una combinación de ambos. Un cortafuegos es reconocido como la primera línea de defensa de la información sensible. Para mayor seguridad, los datos pueden ser encriptados.

Los cortafuegos suelen utilizar dos o más de los siguientes métodos:

- El filtrado de paquetes: método que permite permitir o denegar la entrada o salida de paquetes de datos de una red haciendo uso de un conjunto predefinido de reglas de filtrado.

- Application Gateway: La técnica de aplicación de pasarela emplea métodos de seguridad que se aplican a ciertas aplicaciones, tales como Telnet y servidores de transferencia de archivos.
- Circuito a nivel de gateway: Una puerta de enlace a nivel de circuito aplica estos métodos cuando se establece una conexión como el Protocolo de Control de Transmisión y paquetes comienzan a moverse.

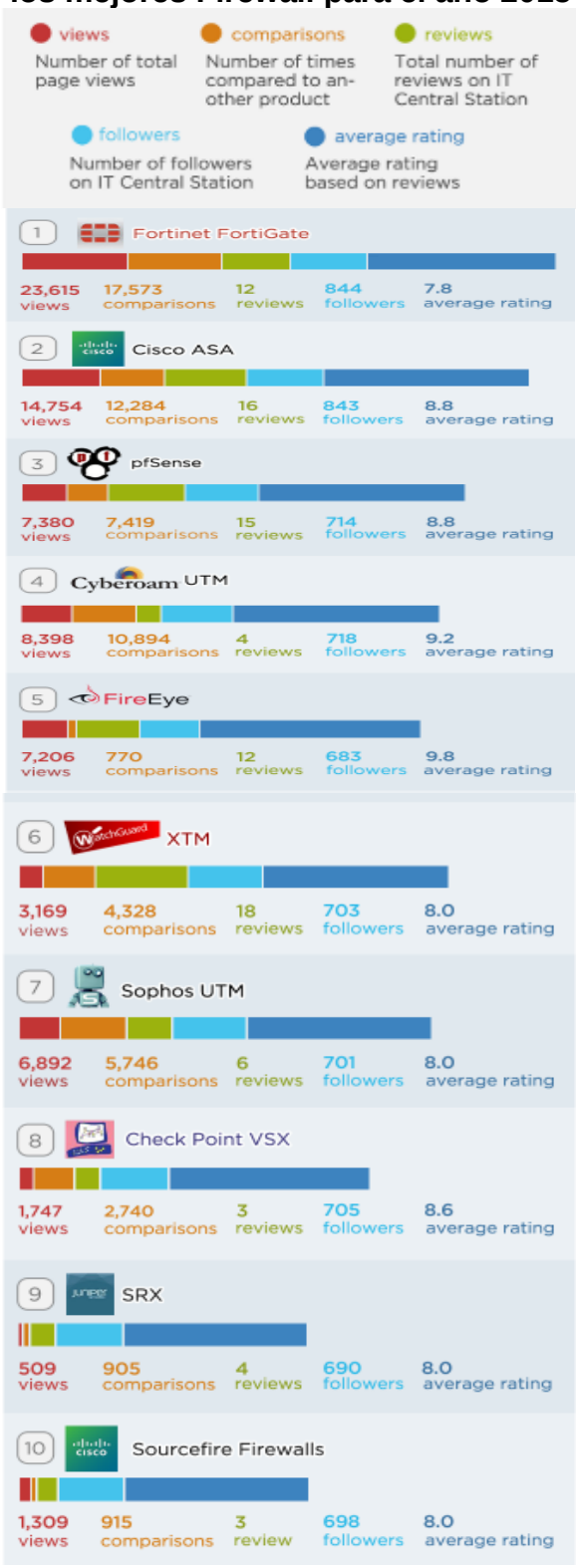
- Servidores Proxy: Los servidores proxy pueden enmascarar direcciones de red reales e interceptar todos los mensajes que entran o salen de una red.

- Inspección de estado o filtrado de paquetes dinámico: Este método compara no sólo la información del encabezado, sino también partes más importantes de datos entrantes y salientes de un paquete. Estos se comparan con una base de datos de información de confianza para los partidos característicos. Esto determina si la información está autorizada

---

https://www.welivesecurity.com/la-es/2014/07/29/por-que-necesario-firewall-entornos-corporativos/ >

Figura 1. Top 10 de los mejores Firewall para el año 2015



Fuente: http://www.itproportal.com/2015/08/21/the-top-enterprise-firewalls-of-2015_

En la anterior figura se logra apreciar unos de los mejores *firewall* libres y de pago, constituidos por *software* o *software* más *hardware*, la evaluación de esta lista de proveedores y marcas se realizó teniendo en cuenta varios aspectos como funcionalidades o características, calificación de los usuarios y adaptación a los nuevos ataques informáticos.

Según el reporte anterior FORTINET es el mejor proveedor de servicios de seguridad con respecto a la protección de redes de datos ofreciendo características como:

- Networking
  Los dispositivos permiten usar varias formas de operación como modo NAT y modo transparente, adicional posee soporte a varios protocolos y servicios como servicio DHCP, soporte DDNS, soporte SNMP, entre otros.

- Antivirus
  El servicio de antivirus se encarga de rastrear eliminar y desinfectar las porciones de código malicioso que entra y sale a la red donde se encuentra implementado, buscando en tiempo real los protocolos de trasmisión de datos HTTP, FTP, SMTP, POP3, IMAP y cualquier otro puerto habilitado dentro de las políticas de seguridad del dispositivo.

- IDS / IPS
  Detección y Prevención de Intrusión es un sistema que se encarga de la detección y prevención automática, y en tiempo real.

- AntiSpam
  La funcionalidad AntiSpam ofrecida por los equipos FortiGate consiste en la aplicación de diferentes filtros sobre el tráfico de intercambio de correo electrónico.

- URL Filtering
  El Servicio de Filtrado Web de Fortinet entrega actualizaciones para regular actividades web mediante la categorización de los sitios y la creación de políticas.

- VPN
  Los equipos FortiGate soportan el establecimiento de Redes Privadas Virtuales basadas en protocolos IPSec y SSL.

Figura 2. Dispositivos de Fortinet

Fuente: https://www.fortinet.com/

"Los equipos de seguridad Fortinet constituyen una nueva generación de equipos de seguridad de muy alto rendimiento que garantizan la protección completa de nuestros sistemas en tiempo real". [10]

Al ser dispositivos tan completos pueden llegar a ser muy caros y su costo de sostenimiento puede incrementar por la adquisición de licencias, por esta y muchas más razones se han creado los *firewall* libres que pueden estar constituidos por *software* libre y *hardware* y pueden ser fácilmente implementados, como lo es PfSense que ofrece grandes características dentro el *firewall*, ya sea adquiriendo el dispositivo y el *software* o descargar de manera gratuita el *software* ofreciendo características como:

- Balanceo de carga: usa múltiples componentes combinado con un método para distribuir las cargas de trabajo a través de varios ordenadores u otros recursos de red, optimizando los canales de internet y mejorando el tiempo de respuesta de los servicios

- Failover: PfSense puede configurarse para redirigir automáticamente el tráfico desde el servidor Web primario a un servidor Web copia de seguridad en el caso de tener algún incidente con el principal.

- Reglas personalizables: firewalls todos tienen reglas, pero pfSense, crea reglas altamente personalizables.

- MAC spoofing de Dirección: es posible escribir en una dirección diferente de la MAC de una interfaz de red, creando la posibilidad de reforzar el ISP servidor DHCP para crear otros segmentos y nuevas direcciones IP.

[10] Fortinet [citado julio 30, 2016]. Disponible en internet < www.fortinet.com >

- VPN: Mayoría de *firewalls* y *routers* soportan redes privadas virtuales (VPN), pero pocos tienen la flexibilidad de PfSense.

Figura 3. Dispositivos de PfSense

Fuente: https://www.pfsense.org/

La importancia de contar con un dispositivo que permita tener control del tráfico en la red radica en que se convierte en un filtro que examina en tiempo real cualquier paquete que sea trasmitido desde dentro de la red de la empresa hacia una red externa o desde una red externa hacia dentro de la red interna, por medio de reglas o políticas que se ajustan a la necesidad de las empresas de acuerdo a sus características, por lo tanto permitir o denegar conexiones evita la propagación de malware a través de la red o accesos no autorizados que generen incidentes de seguridad donde se vea comprometida la integridad, confidencialidad y disponibilidad de la información.

4.2.4 SBC o placa de circuitos reducida. Como se expresa en Blog sobre tecnología UYTec&Games "son placas que contienen todos o la mayor parte de los componentes de una computadora normal y corriente, pero estos están todos integrados dentro de la misma placa base"[11].

Estos dispositivos poseen características parecidas a los computadores de escritorio como memoria, procesador, almacenamiento, entradas y salidas solo que más limitadas haciendo que su costo de producción sea más barato por

[11] UYTec&Games [citado noviembre 28, 2017]. Disponible en internet <https://uytec.wordpress.com/2017/07/05/introduccion-a-las-sbc-computadoras-de-placa-reducida/>

consiguiente más accesible para cualquier persona. Aunque tienen características similares a los computadores son construidos de forma muy diferente, estos dispositivos pueden ser muy limitados ya que elimina características de los equipos de escritorio como cables o conectores específicos y su configuración puede dificultarse, por esta razón usan sistemas operativos embebidos los cuales se usan para metas específicas cumpliendo una función esencial como control de robots, control de procesos o aplicaciones las cuales tienen un uso intensivo de procesamiento.

Hay muchas ventajas de utilizar las computadoras de una sola placa, sus características al estar integradas debido a la construcción del *hardware* la máquina posee ranuras que proporcionan gran cantidad de configuraciones para integrar paneles, sensores y demás *hardware* adicional que se pueda imaginar. Los SBC pueden ser fácilmente producidos, en comparación con los ordenadores personales o portátiles. Ellos son más ligeros en peso, de tamaño compacto, más fiable y más eficiente en el consumo de la energía características que a largo plazo pueden ser beneficiosas en su adquisición, sin embargo, las SBC poseen también limitaciones, ya que su estándar no es compatible con algunos sistemas y su rendimiento puede ser reducido de acuerdo a su fabricante y versión o modelo de placa.

Existen muchas clases de SBC en el mercado como:

Banana Pi: placa similar a la Raspberry Pi, su *hardware* posee un procesador ARM Cortex A7 dualcore, 1GB de memoria RAM DDR3, GPU ARM Mali 400 como algunos teléfonos del mercado.

Figura 4. Placa de circuito compacta Banana Pi

Fuente: http://www.bananapi.org/

BeagleBoard: está producida por Texas Instruments en asociación con Digi-Key. Su procesador es un SoC OMAP3530 basado en ARM Cortex A8, con un DSP TMS320C64x y una GPU PowerVR SGX530 de Imagination Technologies. Tiene ranura SD/MMC, USB, RS-232, jacks, etc. En la placa también se incluye memoria RAM de 256MB y una flash de 256MB.
En el transcurso de su desarrollo surgieron otros modelos derivados con características modificadas como BeagleBone, BeagleBoard-xM y BeagleBone Black.

Figura 5. Placa de circuito compacta BeagleBoard

Fuente: https://beagleboard.org/

Arduino Tian: esta SBC posee módulo WiFi para conexiones, un procesador ARM Cortex M0 de 32 bits y un Qualcomm Atheros AR9342, acompañados de 64MB de RAM, 32 KB de SRAM, 4GB de memoria flash para almacenamiento, conexiones GPIO, salida USB, leds, etc. Esta placa se creó para usarla en el internet para las cosas.

Figura 6. Placa de circuito compacta Arduino Tian

Fuente:http://comohacer.eu

PcDuino: Tiene características como un CPU es una AllWinner A20 1Ghz ARM Cortex A7 dualcore, GPU Mali 400 dualcore, 1GB de RAM, 4GB de memoria flash en placa y posibilidad de ampliarlo con una microSD. Contiene GPIO, ADC, I2C, UART, PWM, HDMI, USB, Ethernet, WiFi, IR, SATA, MIPI integra las mejores características de Raspberry Pi y Arduino.

Figura 7. Placa de circuito compacta PcDuino

Fuente:http://comohacer.eu

Raspberry Pi 1 Model B: este modelo posee características técnicas como un procesador SoC Broadcom BCM2835 con arquitectura ARM, su consumo de energía oscila entre los 300mA (1,5w) hasta los 700mA (3,5w). Posee conexión HDMI, USB MicroSD, 512MB SDRAM, etc

Figura 8. Placa de circuito compacta Raspberry Pi1 B

Fuente:https://www.raspberrypi.org/

Para este proyecto se va a usar la SBC Raspberry Pi por sus características y su alta compatibilidad con sistemas LINUX.

“La Raspberry Pi Foundation trabaja para poner el poder de la toma digital en las manos de personas en todo el mundo, por lo que son capaces de entender y dar forma a nuestro mundo cada vez más digital, capaz de resolver los problemas que son importantes para ellos, y equipado para los trabajos del futuro.”[12]
Este *hardware* tan poderoso y útil fue creado en 2006 pero no fue sacado al mercado sino hasta febrero de 2012, fue desarrollado por un grupo de la Universidad de Cambridge que poseían como misión enseñar las ciencias de la computación a los niños.

[12] Raspberry PI, [citado agosto 10, 2016]. Disponible en internet < www.raspberrypi.org >

“Proporcionamos bajo costo, computadoras de alto rendimiento que usa la gente para aprender, resolver problemas y divertirse. Proporcionamos asistencia y educación para ayudar a más personas acceso a la informática y la toma digital. Desarrollamos recursos gratuitos para ayudar a la gente a aprender acerca de la computación y la forma de hacer las cosas con las computadoras, y capacitar a los educadores que pueden guiar a otras personas a aprender.”[13]

Figura 9. Tabla comparativa de modelos Raspberry Pi.

Fuente: http://comohacer.eu/wp-content/uploads/comparativa-raspberry-pi.png

En esta imagen de una tabla de comparación se puede encontrar todos los modelos de las placas que ha desarrollado Raspberry Pi hasta junio de 2016, a menudo las SBC son confundidas como MiniPC pero la realidad es que no es así, ya que poseen características distintas, ya que las SBC pueden funcionar con sistemas operativos embebidos, permitiendo explotar al máximo su funciones empleado pequeñas cargas con respecto a otros sistemas o equipos.

[13] Raspberry PI, [citado agosto 10, 2016]. Disponible en internet < www.raspberrypi.org >

5. METODOLOGÍA

5.1 TIPO DE INVESTIGACIÓN

El presente estudio es de carácter descriptivo, con enfoque cuantitativo y cualitativo. Se realizará un análisis cualitativo de la red de datos del edificio donde se encuentra ubicada la empresa TAIO SYSTEMS, con el fin de definir las posibles falencias que conllevaron a la problemática actual. La investigación explicativa permitirá analiza, las causas y las consecuencias derivadas de la falta de control de tráfico de datos.

La investigación tomará un enfoque cualitativo ya que el proyecto estará basado en el estudio de las características de un *Firewall* construido a partir de un *software* libre y una placa de circuitos compacta y un enfoque cuantitativo realizado por medio de pruebas de funcionamiento al dispositivo implementado.

5.2 DISEÑO DE INVESTIGACIÓN

5.2.1 Métodos de observación. La técnica a utilizar es el método de análisis, que se realizará con la recolección de información del nivel de seguridad informática de acuerdo a los controles implementados en la empresa, encontrando de esta manera, las principales falencias en el marco de seguridad de la entidad que impide o pone en riesgo la protección de los datos y dispositivos a nivel perimetral, para lograr entender los efectos positivos que se tienen en la red con el uso de un dispositivo de seguridad perimetral, se desarrollara el estudio y análisis de las propuestas que han realizado diferentes personas, buscando así mejorar o controlar el tráfico de una red en una empresa por medio de soluciones de seguridad como un *firewall open source*.

Se realizarán visitas a la empresa TAIO SYSTEMS en la ciudad de Popayán y se hará un registro fotográfico, análisis y diagnóstico de los controles de red implementados con el fin de evidenciar las condiciones actuales en las que se encuentra la empresa en cuanto a seguridad informática.

Se registrarán datos observados, se interpretarán y se elaborarán conclusiones de acuerdo al análisis de dicha información.

Partiendo de las problemáticas identificadas, que no permiten un adecuado nivel de seguridad se propondrá la implementación de un *appliance* que apoye y aporte al mejoramiento de la seguridad perimetral de la empresa.
La investigación se llevará a cabo en 4 etapas:

Etapa 1. Interpretativa

Para la recolección de la información se parte del análisis de:

- Contextualización de la problemática actual de la seguridad informática.
- estudio de un firewall (funcionamiento y análisis)
- investigación de la placa de circuitos compacta RASPBERRY PI1.
- Networking (Trabajo de red)

Etapa 2. Trabajo de campo.

- Levantamiento de la información y análisis de la topología de red de la empresa para identificar sus principales falencias.
- Análisis visual y registro fotográfico del estado de la red de la empresa.
- Estudio de los factores positivos de la red de la empresa TAIO SYSTEMS
- Diagnóstico del estado de la red de datos de la empresa

Etapa 3. Propositiva:

Proponer una *appliance* que aporte al mejoramiento de la seguridad perimetral de la red de datos de la empresa, definiendo reglas dentro del dispositivo para apoyar a mejorar el control de acceso de la red.

Etapa 4: pruebas.

Realizar pruebas del funcionamiento del *appliance*.

5.3 FUENTES DE INFORMACIÓN

En la investigación se utilizarán fuentes de información mixta (primaria, secundaria y terciaria):

- Fuentes primarias: Se obtendrá información por medio del diseño de técnicas e instrumentos para conseguir datos de forma directa

- Fuentes secundarias: se tomarán como referentes estudios científicos, trabajos de grado, páginas con trayectoria científica y academia en internet, revistas indexadas y libros especializados.

- Fuentes terciarias: Se tomarán como referentes guías físicas y virtuales que contienen información sobre las fuentes secundarias. (índices, directorios guías, bibliografías, catálogos)

5.4 MATERIALES

Es de suma importancia poseer conocimientos acerca de *networking*, funcionamiento y configuración de *Firewall*, así como de diseño de políticas, protocolos y gestión de riesgos o vulnerabilidades, también es necesario conocer sobre las vulnerabilidades de los sistemas y técnicas de *hacking* ético para realizar pruebas de intrusión a los sistemas.

Dentro de los materiales para la construcción del *appliance* es necesario contar con una placa de circuitos reducida RaspBerry PI1, un adaptador de Ethernet USB, *Firewall* IPFire, patch cord o cables UTP, memoria SD de 8 GB y un adaptador de voltaje de 5V.

5.5 PLAN DE PRUEBAS

Para este plan se ha propuesto conformar un laboratorio con el fin de recrear algunos de los servicios de los que dispone la empresa hacia internet de tal forma, poder trabajar y realizar ataques en un ambiente seguro.

Este plan se propone analizar 3 tipos de servicios que usa la empresa TAIO SYSTEMS, que serán recreados e implementados dentro de la red interna (LAN) del *Firewall*, generando reglas para su acceso desde la red externa (WAN) mediante puertos específicos que usan los protocolos.

Dentro de este proyecto se ha planteado documentar los resultados obtenidos a partir de la evaluación o detección de vulnerabilidades que puedan ser atacadas por herramientas o *software* especializado en la ejecución de un *pentest*, pero ya que no es el objetivo esencial del proyecto solo se documentara algunas de las fases. ESET SECURITY en su artículo “*Penetration* Test, ¿en qué consiste?”, plantea que las fases de un *pentest* están comprendidas de la siguiente forma:

- **Fase de reconocimiento**
- **Fase de escaneo**
- **Fase de acceso**

De esta forma, el alcance de este plan se limitará a la Identificación de los puntos a evaluar como los servicios, protocolos configurados en el ambiente de pruebas en el cual se ejecutarán las pruebas de intentos de entrada y explotación de posibles vulnerabilidades, de las cuales posteriormente se consolidará un resumen de los resultados obtenidos.

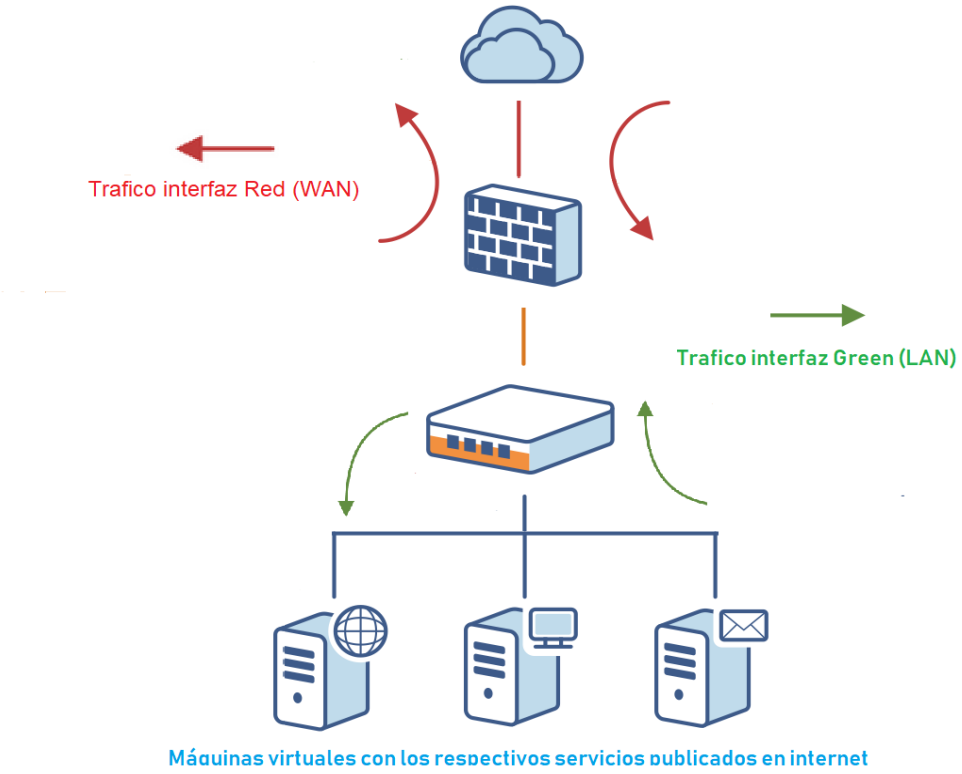
Dentro del contexto de *hacking* ético en el cual se desea realizar las pruebas de penetración existen 3 tipos de Pruebas según el libro titulado "Hacking Ético 101. Cómo hackear profesionalmente en 21 días o menos!" expresados de la siguiente manera:

> Black box hacking También llamado hacking de caja negra. Esta modalidad se aplica a pruebas de intrusión externas. Se llama de este modo porque el cliente solamente le proporciona el nombre de la empresa a auditar al consultor por lo que éste obra a ciegas, la infraestructura de la organización es una caja negra para él.
>
> Gray box hacking o hacking de caja gris. Esta modalidad suele utilizarse como sinónimo para referirse a las pruebas de intrusión internas. pero, algunos auditores también le llaman gray-box-hacking a una prueba externa en la cual el cliente proporciona información limitada sobre los equipos públicos a ser auditados. Ejemplo: un listado con datos como la dirección IP y el tipo, función del equipo (router, web-server, *firewall*, etc.).
>
> White box hacking. Este es el denominado hacking de caja blanca, aunque en ocasiones también se le llama hacking transparente. Esta modalidad se aplica a pruebas de intrusión internas solamente y se llama de esta forma porque la empresa cliente le da al consultor información completa de las redes y los sistemas a auditar.[14]

Teniendo en cuenta lo anterior, las pruebas realizadas se basan en el tipo de prueba de Caja Gris, ya que se tiene conocimiento previo de las direcciones de los equipos de red, pero se realizará escaneos para detectar servicios y protocolos vulnerables.

[14] ASTUDILLO, Karina. Hacking Ético 101. Cómo hackear profesionalmente en 21 días o menos!. Create Space, July 7, 2016. p. 12-13.

Figura 10. Esquema de red propuesto



Fuente: Autor del trabajo

El anterior diagrama plantea el esquema de red que se trabajara para realizar los ataques hacia el *firewall* y servicios, para esta actividad se instalaran los siguientes servicios.

Tabla 1. Descripción de servicios usados por la empresa

Nombre del Servicio	Puerto	Descripción del Servicio
FTP	21	Protocolo de transferencia de archivos por sus siglas en ingles File Transfer Protocol o FTP
SSH	22	Servicio de acceso remoto por consola, por sus siglas en ingles Secure Shell
HTTPD Apache	80	Servicio para publicación de páginas, aplicaciones, etc

Fuente: Autor del trabajo

6. DESARROLLO DEL PROYECTO

La empresa TAIO SYSTEMS ha apoyado varios proyectos relacionados con el desarrollo del prototipo del *firmware* como una empresa de consultoría y desarrollo independientes. TAIO SYSTEMS se dedica a la investigación y desarrollo de sistemas embebidos y móviles orientado a crear una cultura de investigación aprendido y aplicado en la academia los conocimientos adquiridos.

Figura 11. Empresa TAIO SYSTEMS

Fuente: http://google.com.co/maps

La empresa se encuentra ubicada en la ciudad de Popayán y como se puede apreciar en la anterior imagen la compañía no cuenta con una construcción grande para llevar a cabo sus funciones por esta razón, poseen una infraestructura de red de topología en cascada en la cual, poseen un canal de internet de la empresa EMTEL S.A.E.S.P y es recibida por un *switch* encargado de distribuir el canal entre las estaciones de trabajo y los demás dispositivos de red de la infraestructura tecnológica de la empresa.

De acuerdo a la investigación realizada se logró identificar, que la red está configurada con direcciones IP estáticas con el fin de mejorar la identificación de

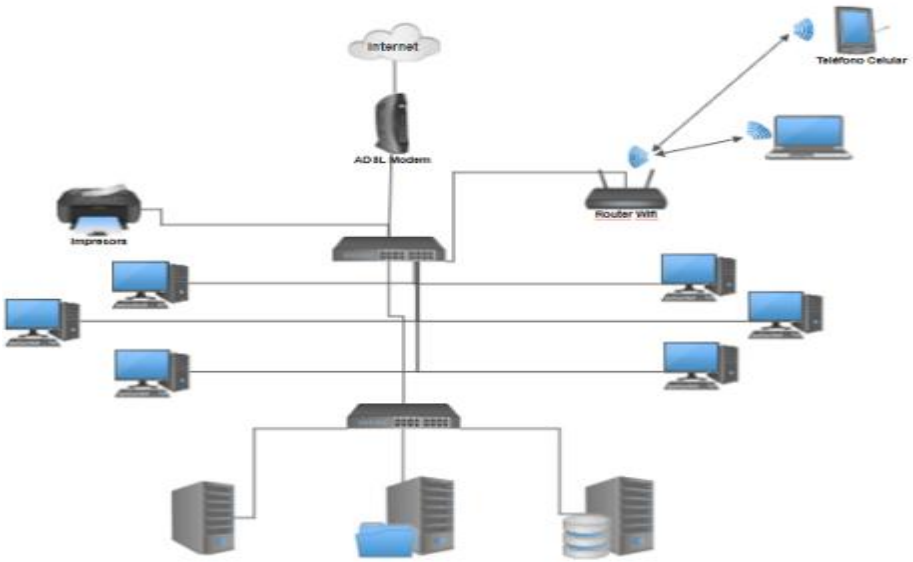
los equipos en la red de la empresa y el servicio de DHCP para los equipos esta deshabilitado, con el fin de conservar y controlar las direcciones IP dentro de la red interna.

Su infraestructura aloja algunos servicios que han dispuesto hacia internet que, aunque son de uso personal pueden ser intervenidos por cualquier *software* malicioso o atacante, que desee causar algún daño en la red o equipos. Dentro de ellos están los servicios de VPN, FTP y servicios web ya que poseen una página institucional en un servidor local.

Adicionalmente de los servicios demandados y en busca de proteger los datos y equipos de la infraestructura tecnológica de la empresa, se hará uso de las herramientas que provee el *firewall*, optimizando la calidad del servicio de internet, y configurando el acceso mediante políticas que permitan generar controles a los usuarios que no tengan privilegios sobre la red definidas por el personal de soporte de la empresa.

Los ingenieros de TAIO SYSTEMS no han realizado la implementación de ningún control físico o lógico para su red, haciéndola vulnerable y deficiente en cuento al uso del canal de internet sin contar con políticas o controles para su administración, no obstante, los equipos cuentan con algunas medidas de prevención como antivirus, *firewall* del sistema operativo y usuarios con autenticación mediante contraseñas.

Figura 12. Esquema de red actual de TAIO SYSTEMS



Fuente: Autor del trabajo

Para la aplicación del proyecto en la empresa TAIO SYSTEMS en primera instancia se plantea la instalación y configuración del *firewall* IPFIRE donde se debe realizar la descarga de la imagen del sistema o *firewall*. La versión actual del sistema es IPFire 2.19 - Core Update 107 hasta la fecha de elaboración e implementación del proyecto.

Es necesario aclarar que la arquitectura de los procesadores de la placa de circuitos que se desea usar es una arquitectura ARM.

Figura 13. Raspberry Pi1 y componentes del Appliance

Fuente: Autor del trabajo

De acuerdo a la anterior imagen se puede apreciar que la placa de circuitos reducida solo posee una interfaz de red ethernet, es indispensable adicionar o conectar una interfaz por USB, para reducir en gran medida el tiempo de respuesta del *firewall* a través de las diferentes interfaces.

Dentro del análisis de la red de TAIO SYSTEMS se logró establecer que los equipos de red no poseen puertos de conexión de Gigabit, por lo tanto, manejan velocidad de 100 Megabits para la comunicación de todo el parque tecnológico de la empresa, por esta razón se optó por instalar un adaptador de red Ethernet de la misma velocidad de los equipos en la placa de circuitos reducida, de esta manera los componentes del dispositivo se representan en la siguiente imagen.

Figura 14. Appliance propuesto para TAIO SYSTEMS

Fuente: Autor del trabajo

Para realizar la instalación del *firewall* es necesario grabar la imagen del *software* en un medio de almacenamiento que la placa de circuitos pueda identificar, para ello se hace uso de aplicaciones o *software* libre que permitan hacer que una memoria y una imagen con extensión del archivo en ".img" (formato de versión de IPFire para dispositivos con arquitectura AMR) sean reconocidas por el sistema para la instalación en algún medio de almacenamiento.

En la pantalla inicial de instalación se puede apreciar las herramientas que incorpora la imagen o instalar directamente en algún medio de almacenamiento que posea la SBC.

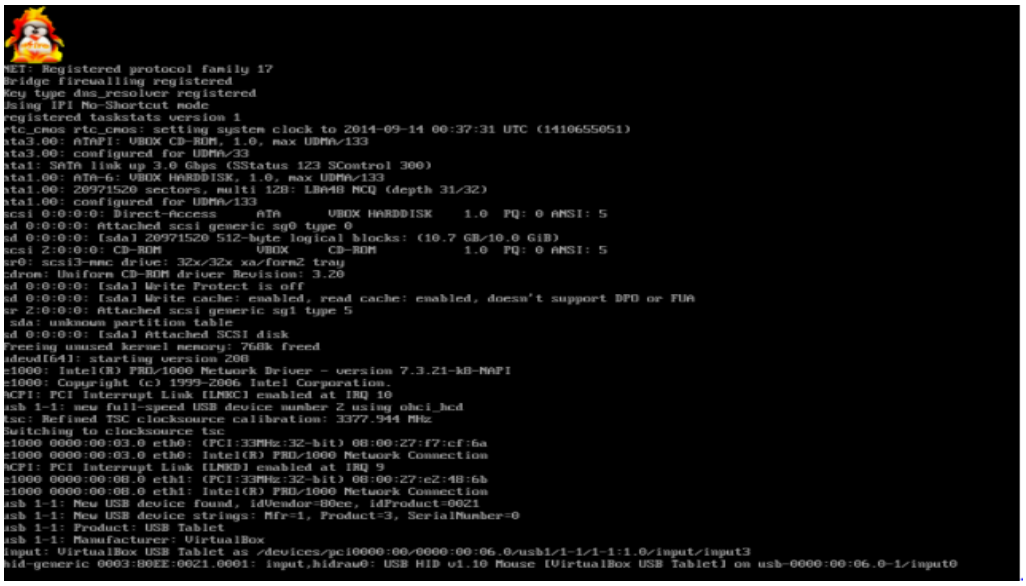
Figura 15. Instalación de IPFire

Fuente: Autor del trabajo

La anterior imagen presenta la pantalla inicial del proceso de instalación del *firewall* en el dispositivo de almacenamiento, para este proyecto se optó por trabajar con la última versión disponible hasta la fecha para procesados con arquitectura ARM.

En el momento de iniciar la instalación, el *firewall* comienza a cargar todos los componentes necesarios, como se presenta en la siguiente imagen.

Figura 16. Instalación de IPFire



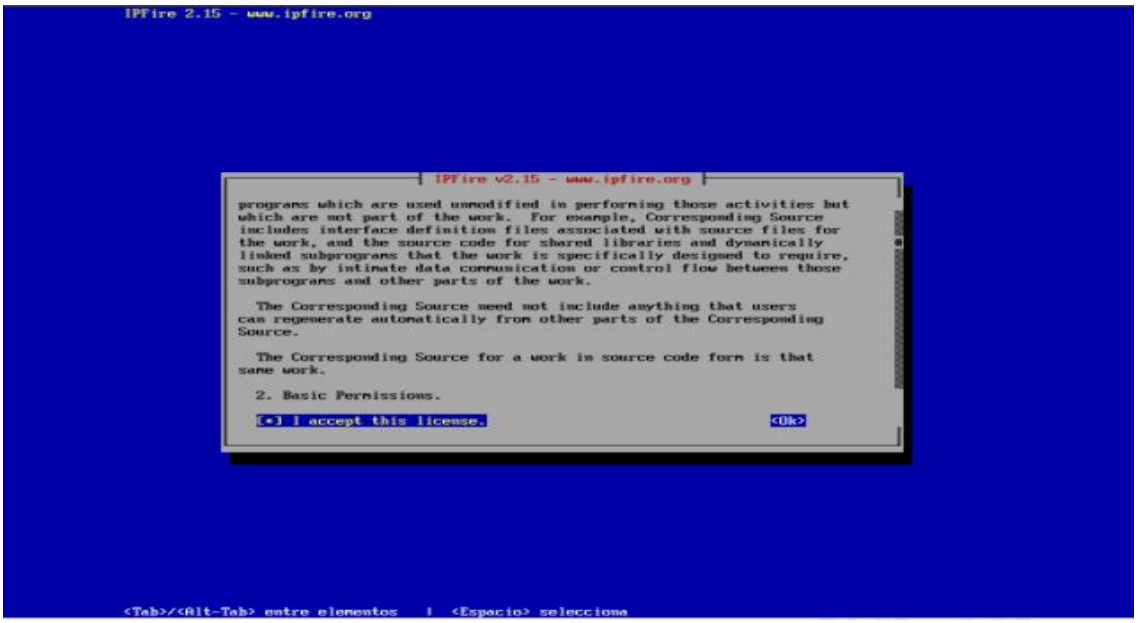
Fuente: Autor del trabajo

A continuación, es necesario seguir con los pasos indicados por el asistente de instalación como se presenta en las siguientes imágenes, seleccionando idioma y aceptando los términos de la licencia y condiciones del *firewall*.

Figura 17. Instalación de IPFire

Fuente: Autor del trabajo

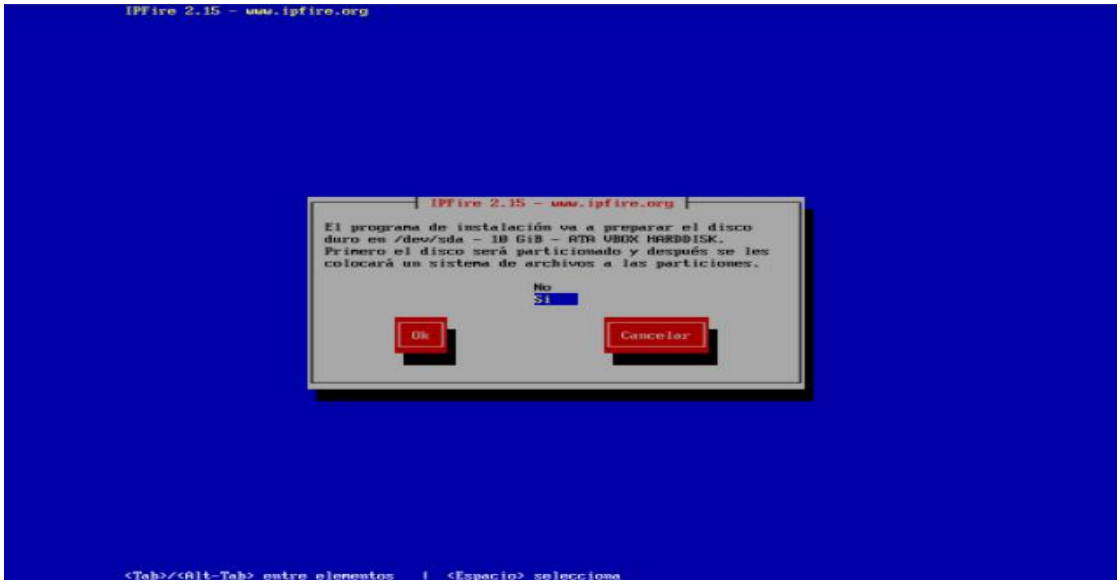
Figura 18. Instalación de IPFire



Fuente: Autor del trabajo

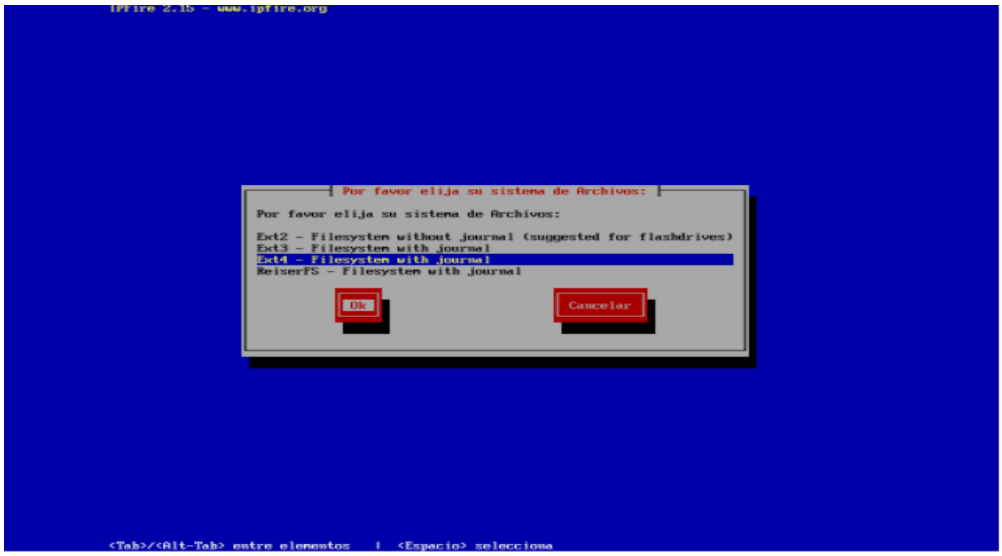
La siguiente imagen permite apreciar el mensaje de advertencia de eliminación de archivos y partición del disco para continuar la instalación del *firewall*

Figura 19. Instalación de IPFire



Fuente: Autor del trabajo

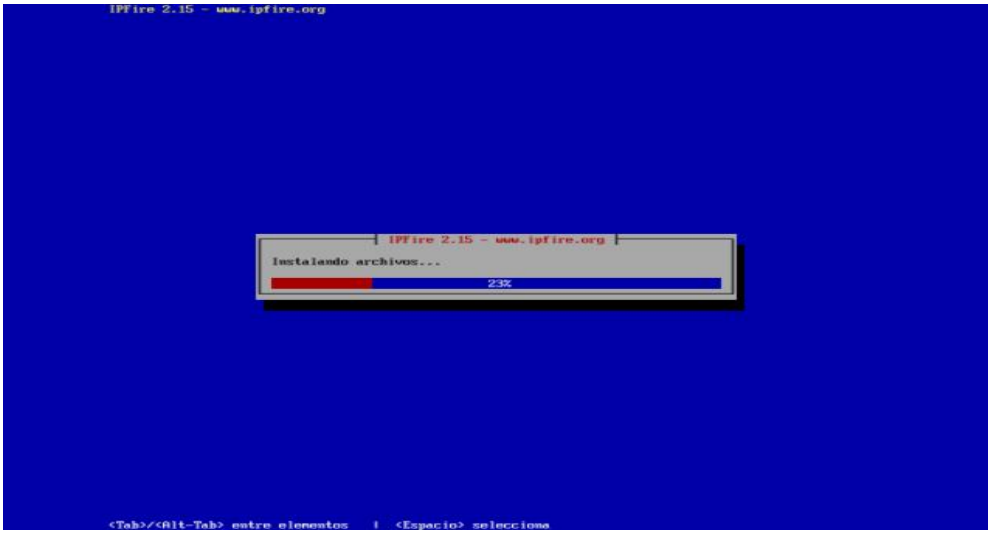
Figura 20. Instalación de IPFire



Fuente: Autor del trabajo

La anterior imagen muestra el tipo de sistema de archivos usado para el almacenamiento del *firewall* que en este caso es Ext4 para mejorar el rendimiento del dispositivo, en el momento de instalar los archivos en el medio de almacenamiento presenta el porcentaje de finalización, como se evidencia en la siguiente imagen.

Figura 21. Instalación de IPFire



Fuente: Autor del trabajo

Figura 22. Instalación de IPFire

Fuente: Autor del trabajo

La imagen anterior es presentada una vez el proceso de instalación ha terminado y se procede a ejecutar configuración básica del *firewall* como es la selección del teclado, zona horaria, nombre y dominio presentado en las siguientes imagenes.

Figura 23. Instalación de IPFire

Fuente: Autor del trabajo

Figura 24. Instalación de IPFire

Fuente: Autor del trabajo

En la siguiente imagen se evidencia el proceso de asignación de contraseña para el usuario del *firewall* con los privilegios más extensos.

Figura 25. Instalación de IPFire

Fuente: Autor del trabajo

La siguiente imagen pauta el mismo proceso de asignación de contraseña, pero para el usuario credo para administrar la interfaz web del *firewall*.

Figura 26. Instalación de IPFire

Fuente: Autor del trabajo

Es preciso saber el funcionamiento de un *firewall* o conocer las funciones básicas de algún otro, ya que este, al igual que muchos *firewalls*, permite configurar varios tipos de interfaces de red enmarcadas en el sistema de IPFire con colores distintos permitiendo la comulación de los equipos con diferente direccionamiento detrás de cada interfaz.

Se puede optar por diferentes tipos de configuración para crear controles adicionales que permitan mejorar la seguridad de la información dentro de una infraestructura de red como la creación de DMZ y otras interfaces de red, pero en el estudio realizado en el levantamiento de la información en la empresa TAIO SYSTEMS, la configuración de red y los equipos o servidores no están preparados para usar o comunicarse a través de diferentes segmentos de red.

Por esta razón se configuran dos interfaces de red LAN – WLAN con el fin de crear políticas que permitan detectar y monitorear los paquetes de información que entran y salen de la red como se muestra en las siguientes imágenes.

Figura 27. Instalación de IPFire

Fuente: Autor del trabajo

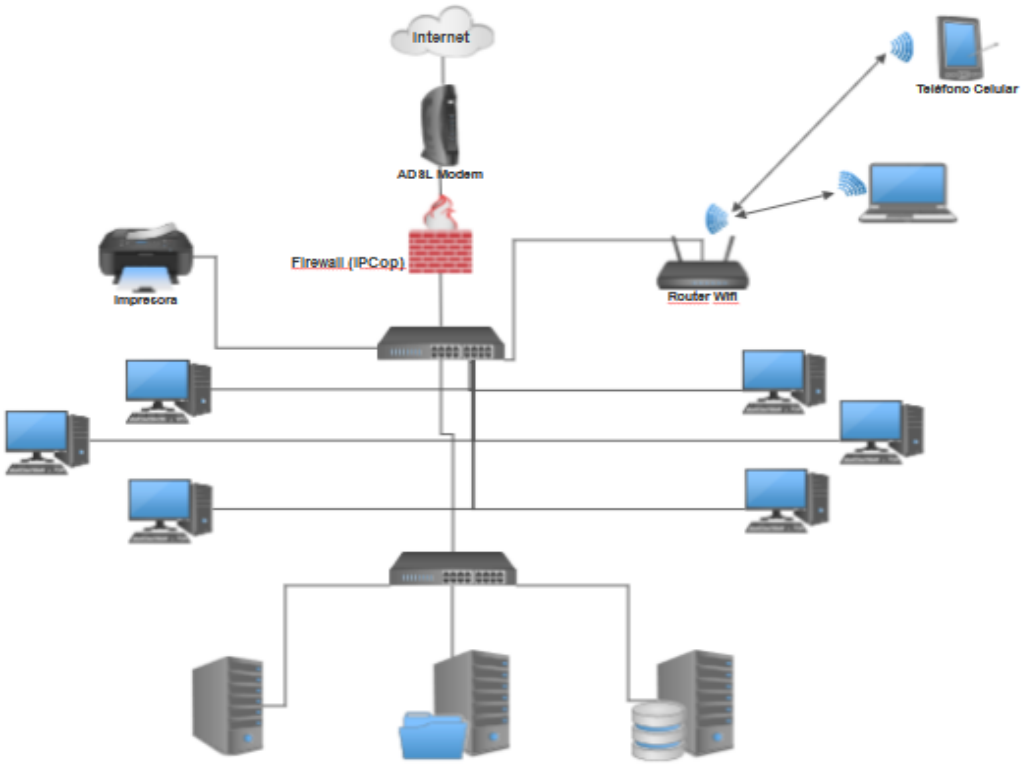
Figura 28. Instalación de IPFire

Fuente: Autor del trabajo

Es necesario realizar el proceso de asignación de tarjetas de red para crear configuraciones separadas, con el fin de crear el esquema de red propuesto.

En la siguiente imagen se generó un diagrama de la red para logra ver de una forma gráfica la configuración del *firewall* para controlar el tráfico de las dos imágenes

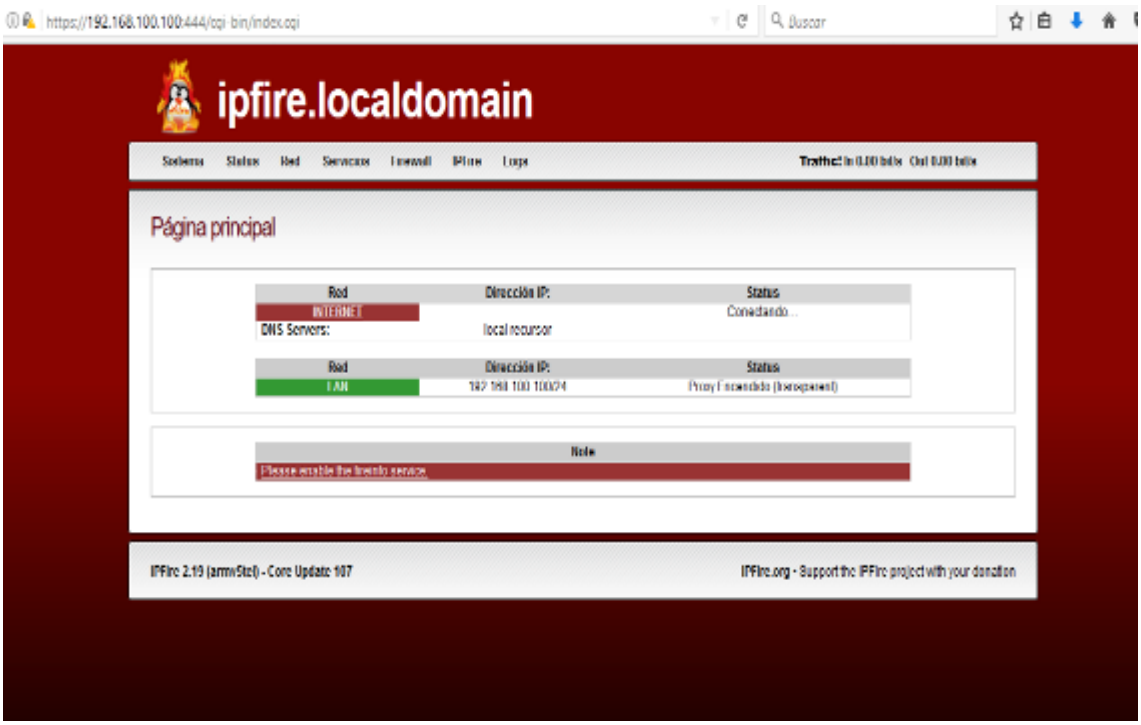
Figura 29. Esquema de red propuesto para la empresa



Fuente: Autor del trabajo

De acuerdo al análisis realizado en la empresa TAIO SYSTEMS se optó por configurar el *appliance* con sus dos respectivas interfaces de red, tal como se muestra en la imagen anterior, de tal forma que todo el tráfico de datos que salen y entran a la red (LAN), pueda ser monitoreado por el dispositivo permitiendo un análisis en tiempo real de los paquetes de información permitiendo o denegando las conexiones por los protocolos habilitados en las reglas de *firewall*.

Figura 30. Estado inicia de la interfaz web del firewall

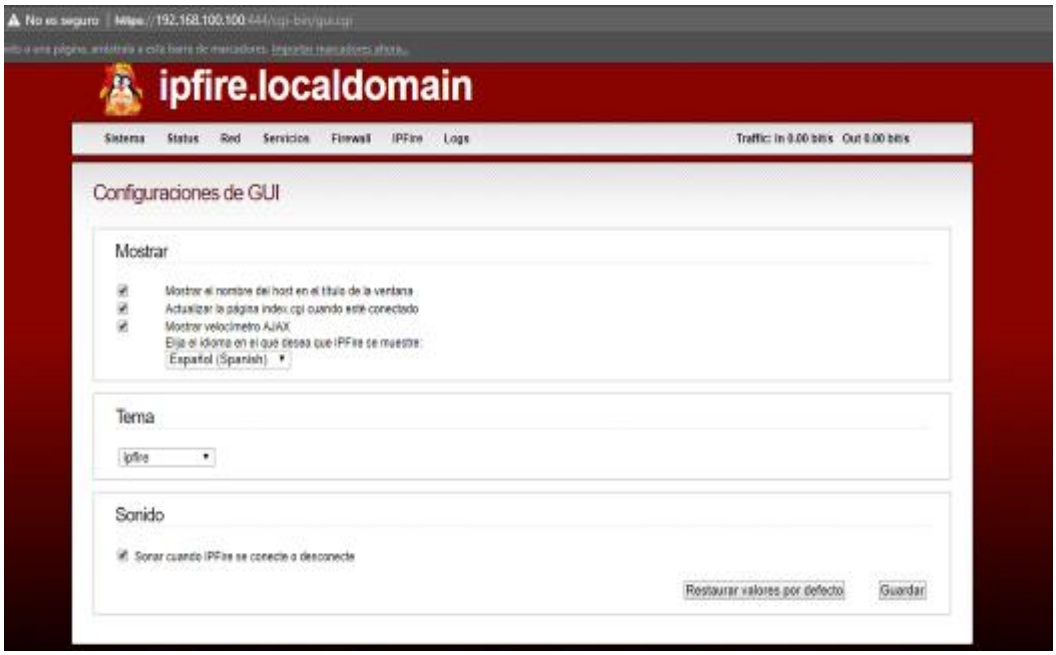


Fuente: Autor del trabajo

En la imagen anterior se puede evidenciar las interfaces de red configuradas previamente, la interfaz de red roja es la red WLAN y la interfaz verde es la red LAN del dispositivo.

Se cambia configuración de idioma de la interfaz gráfica para mejorar su administración.

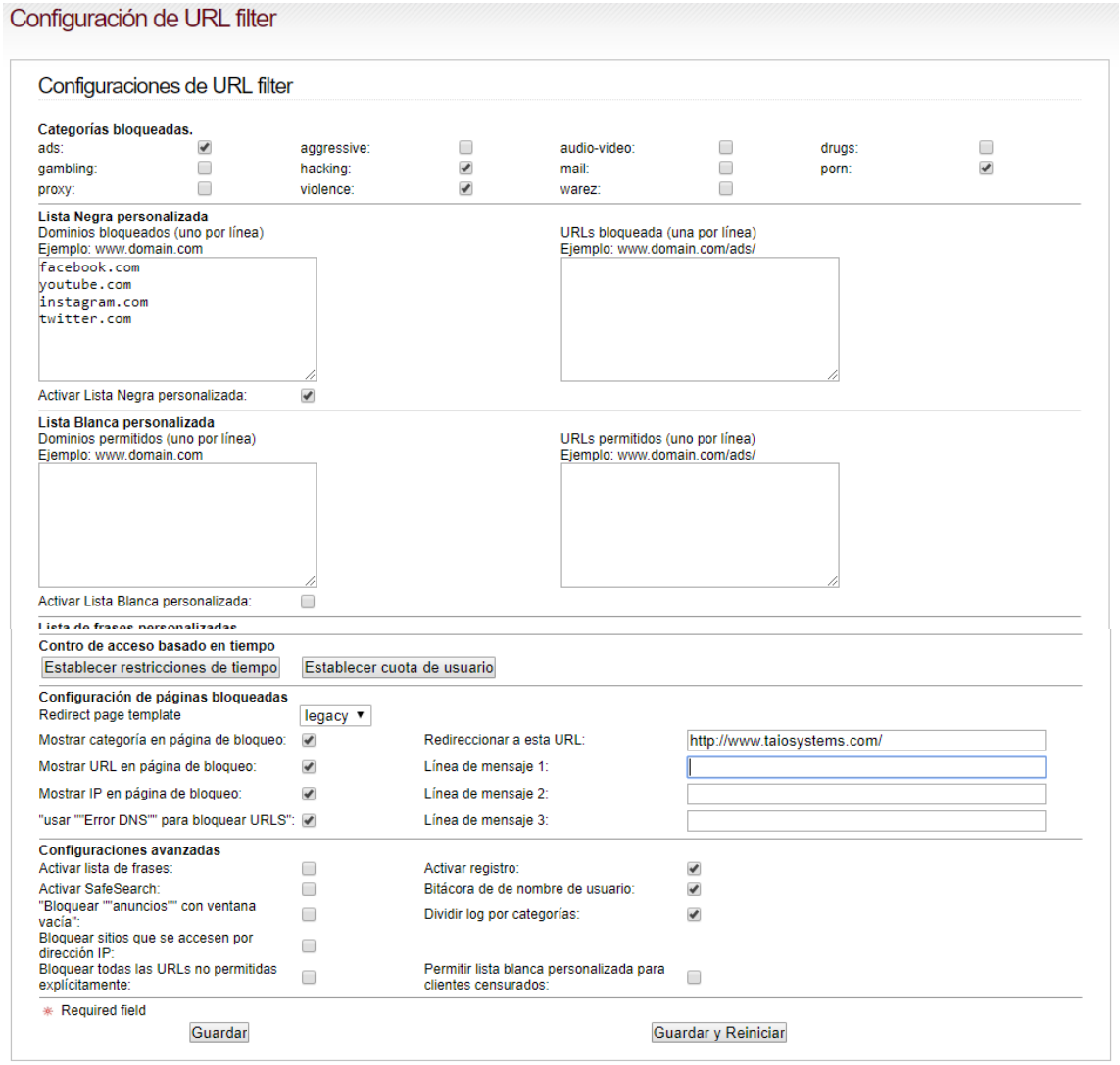
Figura 31. Cambio de idioma



Fuente: Autor del trabajo

Dentro de la interfaz web de IPFire se encuentra unas listas en el menú superior para facilitar la navegación y administración como se evidencia en la anterior imagen, estas listas poseen el acceso a configuración de los servicios como OpenVPN, Sistema de Detección de Intrusiones, URL filter o filtro de contenido, *Firewall*, entre otros.

Figura 32. Configuración del filtro de contenido



Fuente: Autor del trabajo

En el servicio o herramienta del URL Filter, se estableció bloquear contenido innecesario y páginas que pueden afectar al rendimiento de las actividades de la empresa, como se ve en la imagen anterior. Adicionalmente es habilitado el servicio de monitoreo y redirección de los sitios no autorizados, ayudando al administrador de red a monitorear el tráfico y las anomalías que puedan presentarse en los equipos y los usuarios mejorando así el tiempo de respuesta ante cualquier eventualidad que requiera la revisión de los sitios visitado por algún equipo que pueda ser infectado o posea una puerta trasera.

Figura 33. Configuración del sistema de detección de intrusos

Fuente: Autor del trabajo

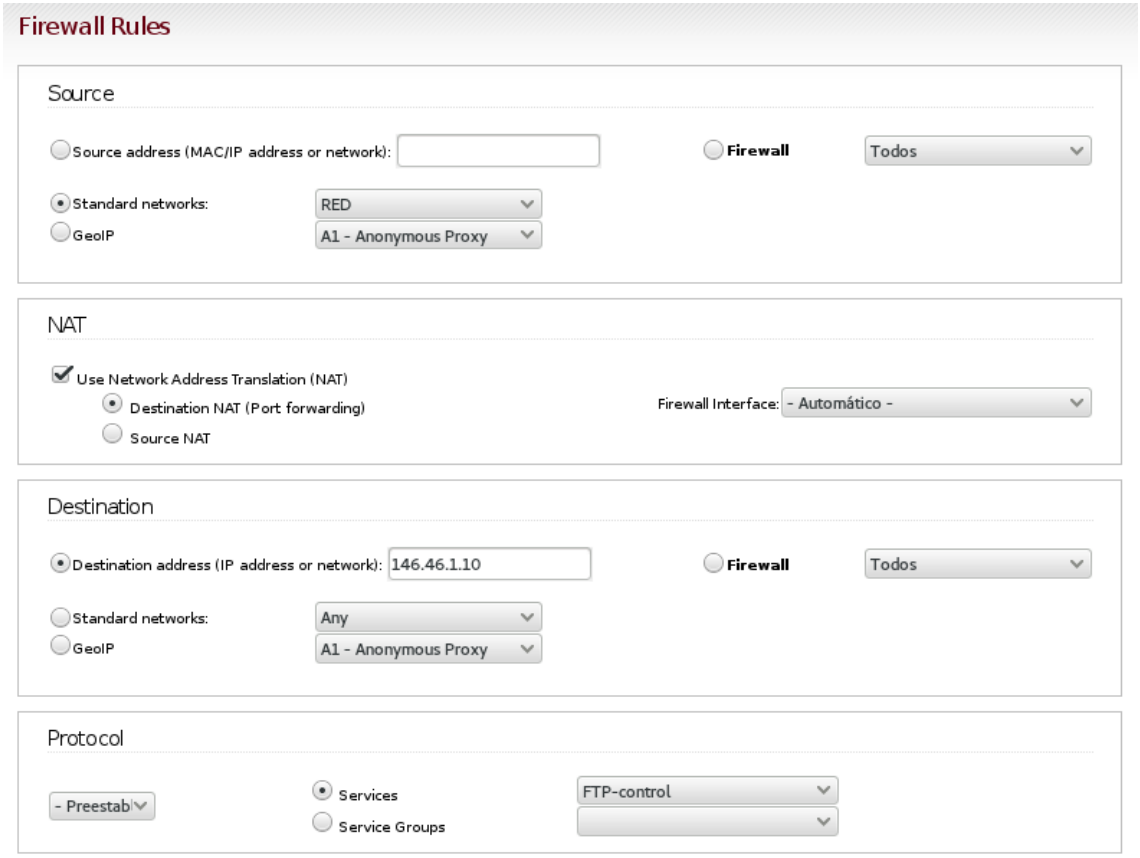
Para el sistema de detección de intrusos basado en Snort se activa como se muestra en la anterior imagen, este servicio se activa para las dos interfaces de red ya que esta herramienta permitirá monitorear el tráfico que entra o sale del dispositivo. Para activar el servicio de actualización de las reglas del sistema de detección de intrusos fue necesario realizar el registro de un usuario, ya que sin este registro no podrá ser generado el código que permitirá actualizar y mejorar el rendimiento del sistema de detección de intrusos.

Figura 34. Configuración de las reglas del firewall

Fuente: Autor del trabajo

Dentro del *firewall* del sistema se configura el acceso previo por puertos específicos para el uso de las aplicaciones y las conexiones desde el exterior teniendo en cuenta la IP publica de la empresa que se encuentra en el router que trasmite la señal hacia la interfaz configurada, identificada con el color rojo en el *appliance*

Figura 35. Configuración de la regla para acceso al servicio FTP desde internet



Fuente: Autor del trabajo

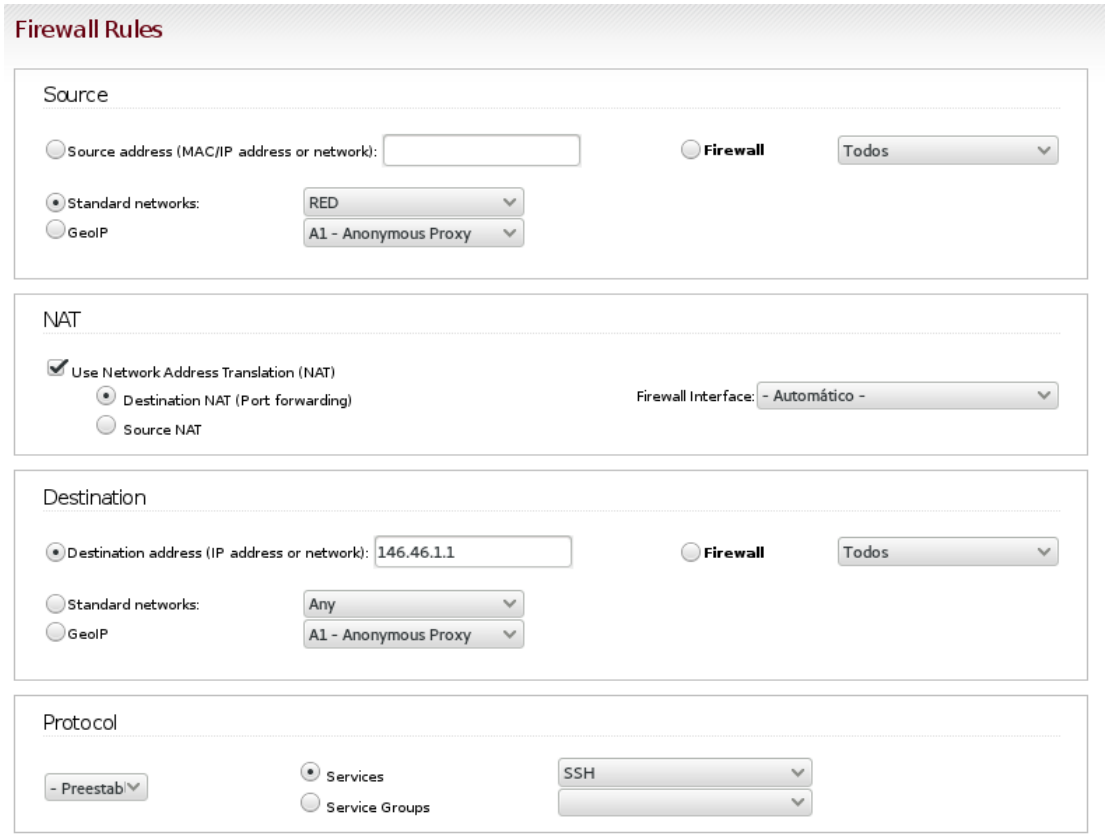
Como se evidencia en la anterior imagen mediante la creación de la regla para el tráfico por el servicio FTP se permitirá los paquetes que provengan a través de la interfaz roja o WLAN, hacia la interfaz verde o LAN permitiendo el acceso a través del puerto 21 que es el que usa el servicio FTP configurado en el servidor de la empresa y en el ambiente de pruebas quedando de la siguiente manera como se muestra en la siguiente imagen.

Figura 36. Regla de acceso FTP activada en el firewall

Fuente: Autor del trabajo

La siguiente imagen permite ver la creación de la regla que tiene como objetivo dentro de la configuración del *firewall,* permitir el acceso a las direcciones provenientes de la interfaz roja (WAN) por el puerto 21, re direccionando el tráfico a la interfaz verde (LAN) a la dirección especifica del servidor destinado a la transferencia de archivos FTP.

Figura 37. Configuración de la regla para acceso al servicio SSH desde el internet



Fuente: Autor del trabajo

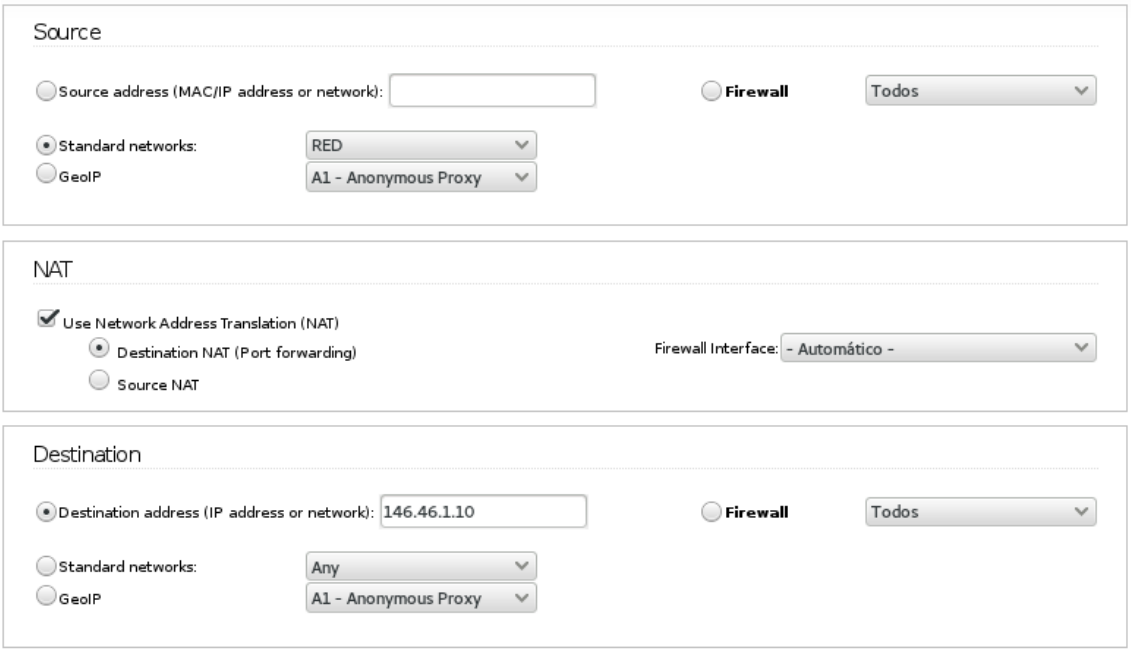
Esta regla permitirá re direccionar el trafico entrante desde internet por el puerto 22 hacia un servidor configurado para tener acceso por el mismo puerto dentro de la red interna del *firewall*, permitiendo el acceso por consola desde internet, como se evidencia en la siguiente imagen.

Figura 38. Regla de acceso SSH activada en el firewall

Fuente: Autor del trabajo

La siguiente imagen permite ver el proceso de creación de la regla que autorizara el trafico http a través del puerto 80 proveniente de la interfaz roja re direccionada a la interfaz verde

Figura 39. Configuración de la regla para acceso al servicio HTTP desde el internet



Fuente: Autor del trabajo

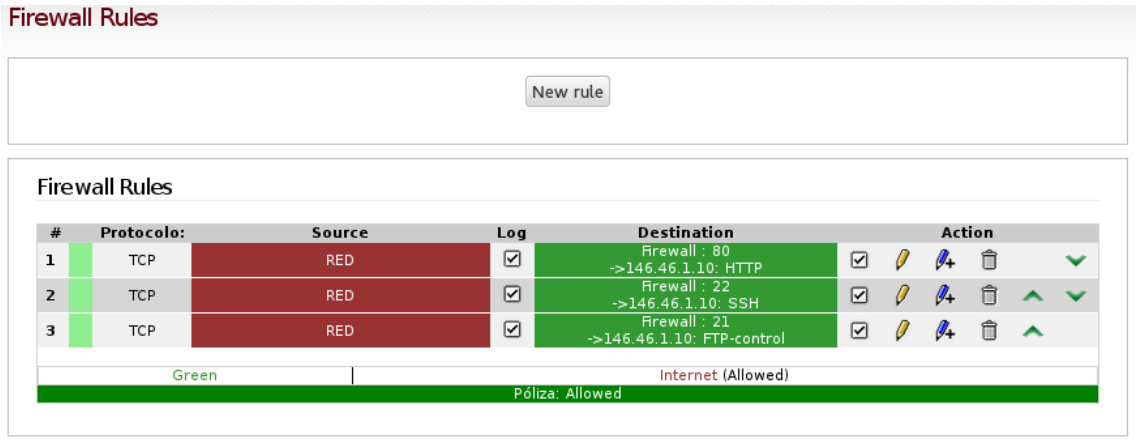
Al finalizar la creación de la regla, permite modificar o eliminar la regla como se muestra en la siguiente imagen.

Figura 40. Regla de acceso HTTP activada en el firewall

Fuente: Autor del trabajo

De esta manera se cuanta con el conjunto de reglas que permitirán el trafico especifico a través del dispositivo.

Figura 41. Reglas del firewall para permitir el tráfico hacia la red interna

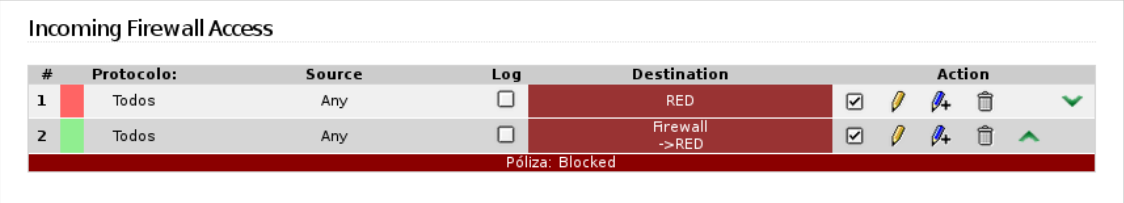


Fuente: Autor del trabajo

Se crearon las respectivas reglas dentro del *firewall* para permitir el re direccionamiento del tráfico a través de los puertos 80, 22 y 21. Estas reglas conforman el grupo de reglas del *firewall* por esta razón es necesario crear las reglas para denegar o aceptar el tráfico de datos que entra o sale del dispositivo y así ayudar a mejorar la seguridad de la información a nivel de seguridad perimetral.

Teniendo en cuenta que las comunicaciones del firewall deben estar bloqueadas por completo excepto las creadas específicamente para los servicios http, ssh y ftp debe generarse las políticas o reglas de entrada de trafico al dispositivo

Figura 42. Reglas del firewall para bloquear el tráfico hacia la interfaz roja



Fuente: Autor del trabajo

La anterior imagen permite evidenciar el conjunto de reglas de entrada creadas que genera las instrucciones para que el *firewall* interprete que, todo el tráfico que apunta hacia la interfaz roja (WAN) este bloqueado por defecto y sea denegado o redirigido, el cual será re direccionado mediante las reglas del *firewall* especificando los puertos de entrada.

6.1 FASE DE RECONOCIMIENTO

Dado que la empresa pública algunos de sus servicios en internet dentro de su página web es posible encontrar su dirección IP Publica en donde se encuentran publicados sus servicios.

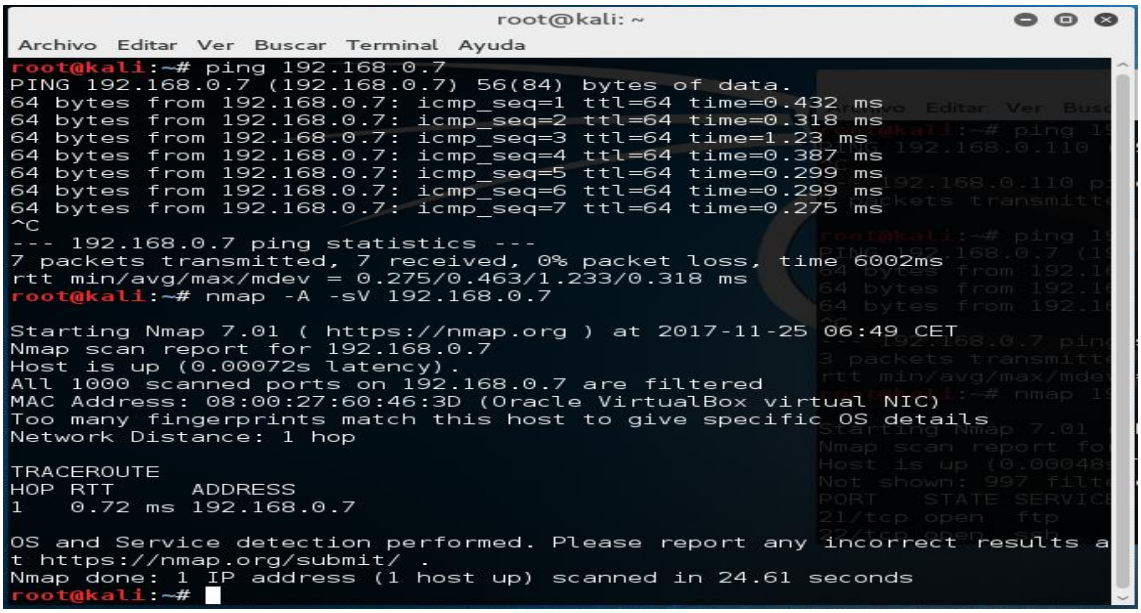
Dado que se cuenta con la dirección IP el siguiente paso es proceder a escanear las vulnerabilidades para realizar un posible modelado de amenazas.

Teniendo en cuenta que todas las pruebas se van a realizar en entornos controlados, se asignara una IP estática a la tarjeta de red Roja (WAN)

6.2 FASE DE ESCANEO

Mediante el uso de la herramienta NMAP y un equipo conectado a la interfaz roja, se logró establecer que, con estas reglas el ping hacia la dirección IP de la interfaz roja está habilitado pero la detección de puerto no está permitida como se puede ver en la siguiente ilustración.

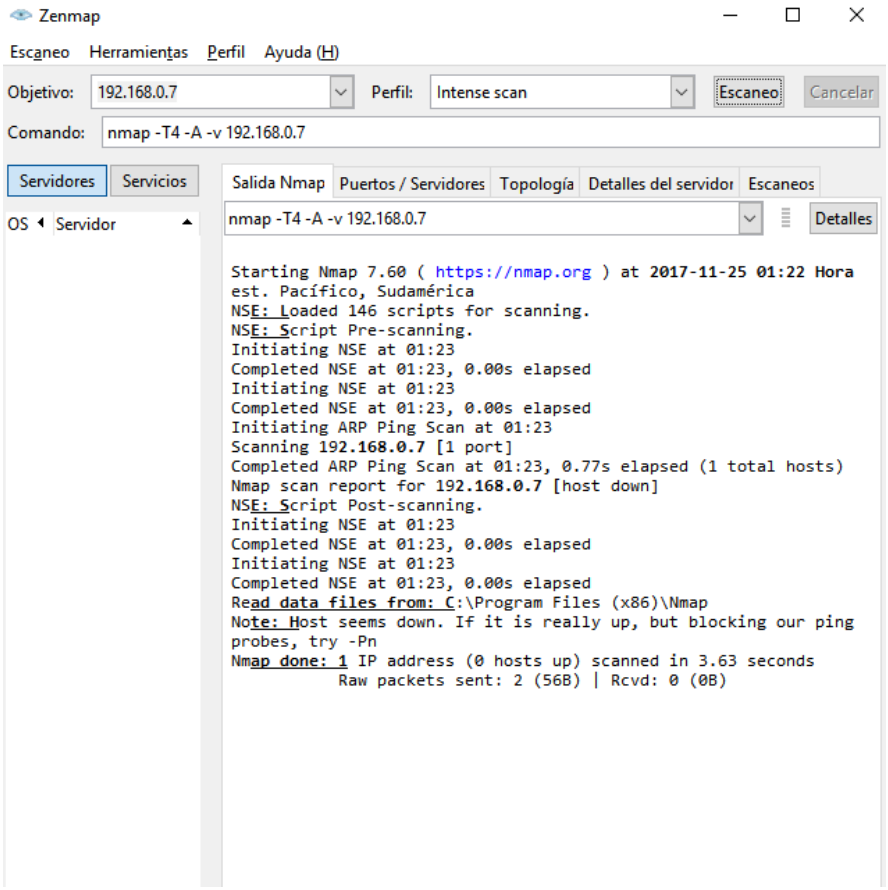
Figura 43. Escaneo de puertos con las reglas del firewall activas



Fuente: Autor del trabajo

Este proceso de escaneo de puertos fue realizado desde diferentes terminales o equipos conectados a la misma red de la interfaz roja del dispositivo de seguridad perimetral, arrojando el mismo resultado.

Figura 44. Escaneo de puertos desde otra terminal

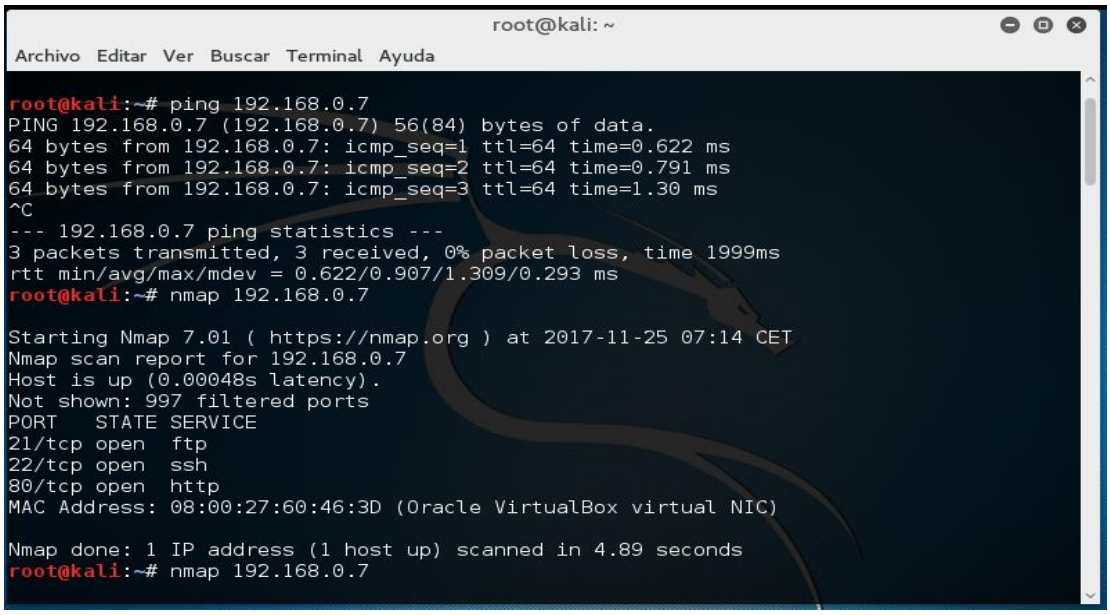


Fuente: Autor del trabajo

Como se evidencia en la anterior imagen las reglas del *firewall* desactivadas permitirían a cualquier equipo escanear los puertos habilitados en el *firewall* logrando así obtener información esencial para realizar ataques enfocados a vulnerar la seguridad de la empresa.

Los resultados del escaneo de puerto sin las reglas del tráfico de datos desactivadas muestran los puertos habilitados en el dispositivo.

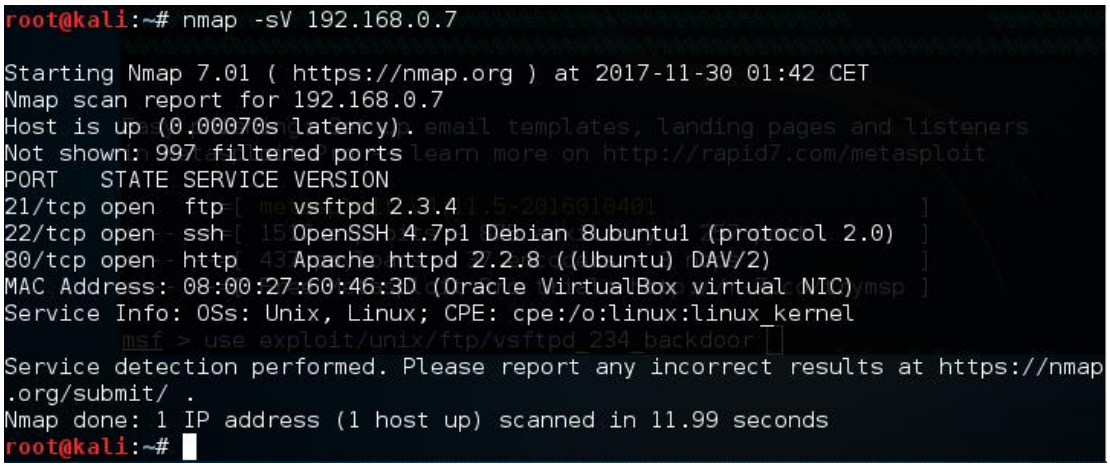
Figura 45. Escaneo de puertos sin reglas activas



Fuente: Autor del trabajo

En la anterior imagen se logra evidenciar que los puertos se encuentran activos y corresponden a los servicios implementados en las reglas del dispositivo por esta razón es indispensable mantener un adecuado uso de las reglas de entrada de tráfico a través de la interfaz de red roja

Figura 46. Escaneo de servicios de los puertos



Fuente: Autor del trabajo

Usando el comando nmap –sV y la IP que se desea escanear es posible observar la versión de cada uno de los servicios publicados como se puede observar en la anterior imagen. Para realizar un modelado de las vulnerabilidades que se pueden usar para explotar las fallas de los servicios o la máquina, es de aclarar que sin las reglas desactivadas este reconocimiento no es posible ejecutar.

Tabla 2. Descripción de las versiones de los servicios usados por la empresa

Nombre del Servicio	Puerto	Versión	Descripción del Servicio
FTP	21	vsftp 2.3.4	Protocolo de transferencia de archivos por sus siglas en ingles File Transfer Protocol o FTP
SSH	22	OpenSSH 4.7	Servicio de acceso remoto por consola, por sus siglas en ingles Secure Shell
HTTPD Apache	80	Apache httpd 2.2.8	Servicio para publicación de páginas, aplicaciones, etc

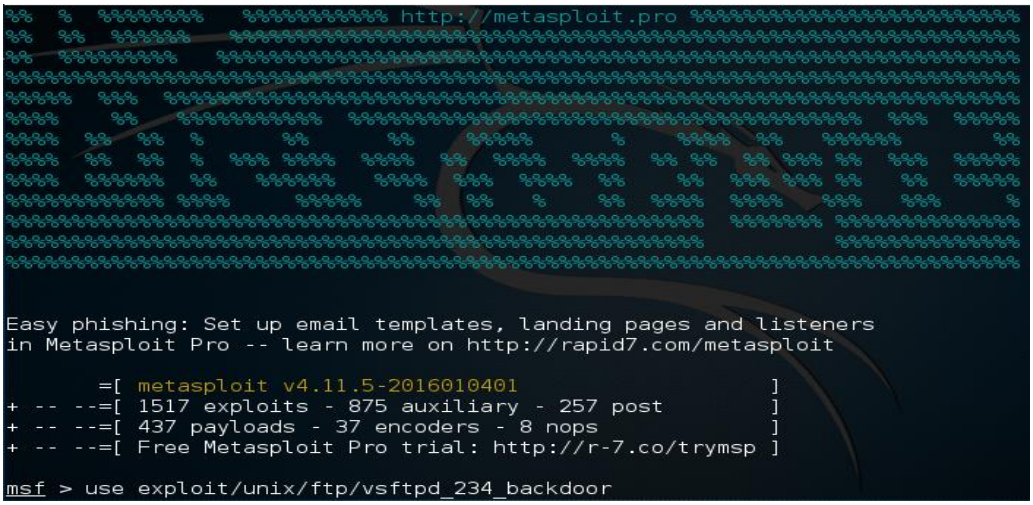
Fuente: Autor del trabajo

6.3 FASE DE ACCESO

Mediante el análisis de vulnerabilidades que se realizó a la dirección IP del dispositivo se logró establecer los tipos y versiones de los servicios publicados en los equipos, por esta razón se usó un *exploit* para tratar de acceder al servicio de forma no autorizada.

Haciendo uso de la herramienta METASPLOIT se realizó la búsqueda del *exploit* correspondiente a los servicios encontrados.

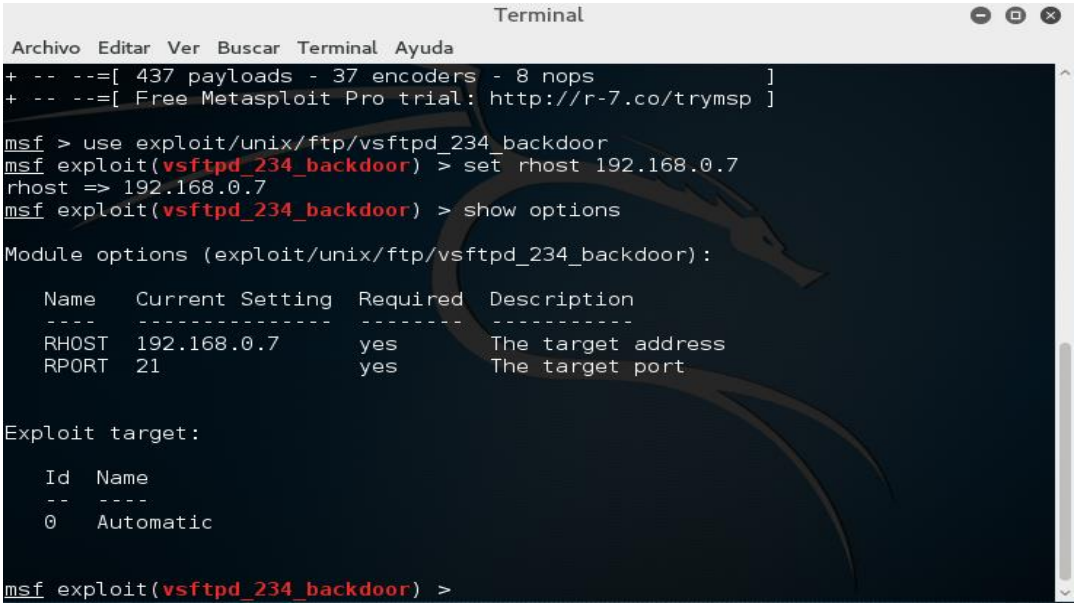
Figura 47. Exploit usado para vulnerar puerto 21



Fuente: Autor del trabajo

Mediante la búsqueda se logró obtener, un exploit adecuado para el servicio FTP, el cual fue ejecutado agregando la dirección IP de la víctima o dispositivo el cual publica los servicios.

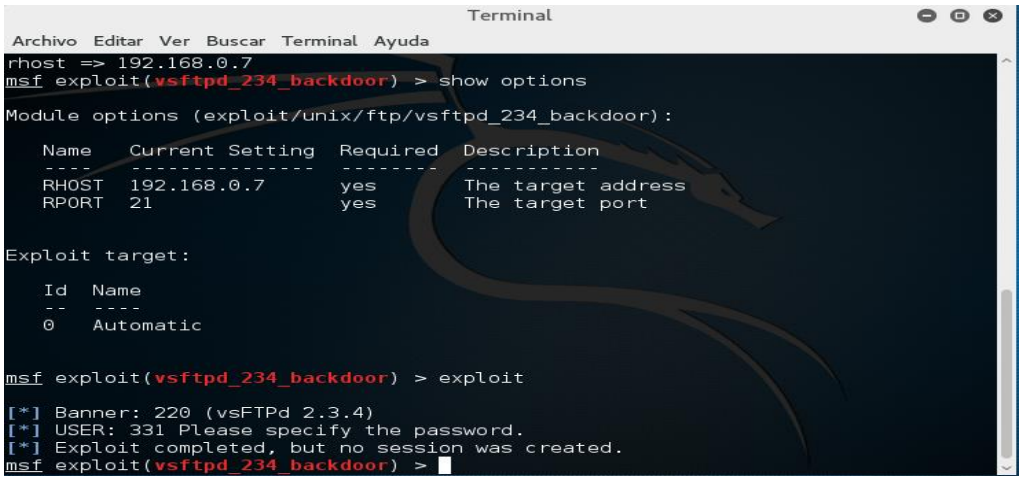
Figura 48. Opciones de exploit para ftp



Fuente: Autor del trabajo

Como se puede comprobar en la siguiente imagen al ejecutar el exploit no se obtuvo ningún éxito al tratar de ingresar por uno de los servicios al sistema ya que la sesión de conexión no pudo ser creada.

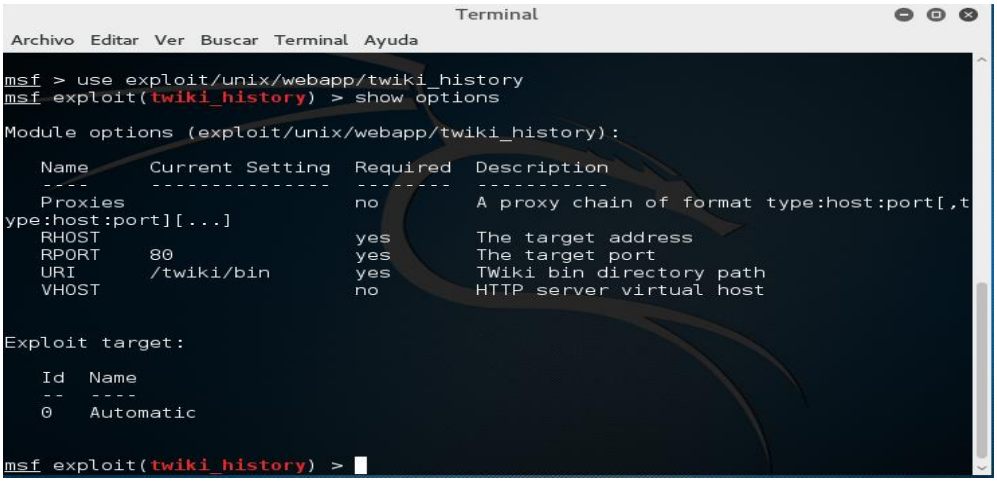
Figura 49. Intento fallido por servicio ftp



Fuente: Autor del trabajo

Para atacar el servicio apache del equipo se optó por usar un exploit y un payload con el fin de realizar un ataque más fuerte hacia el servicio como se puede ver en la siguiente imagen.

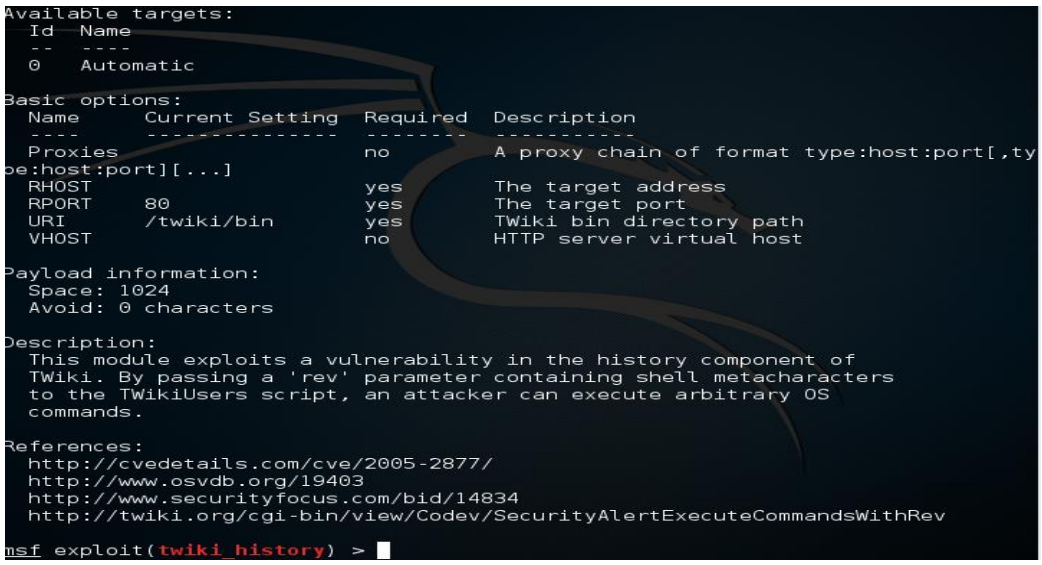
Figura 50. Exploit para servicio httpd



Fuente: Autor del trabajo

Dentro del exploit se agrega la dirección IP que se desea vulnerar y se selecciona el payload como se puede observar en la siguiente imagen

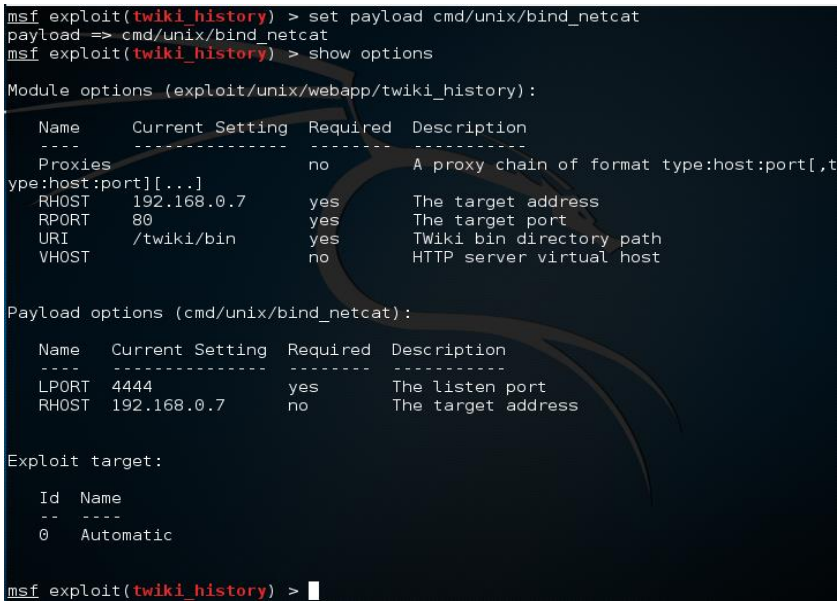
Figura 51. Información para servicio httpd



Fuente: Autor del trabajo

La siguiente imagen representa las opciones que posee el exploit para realizar el proceso de ataque, el cual solo se debe agregar la dirección del servidor y el puerto que usa para establecer una conexión con el servicio

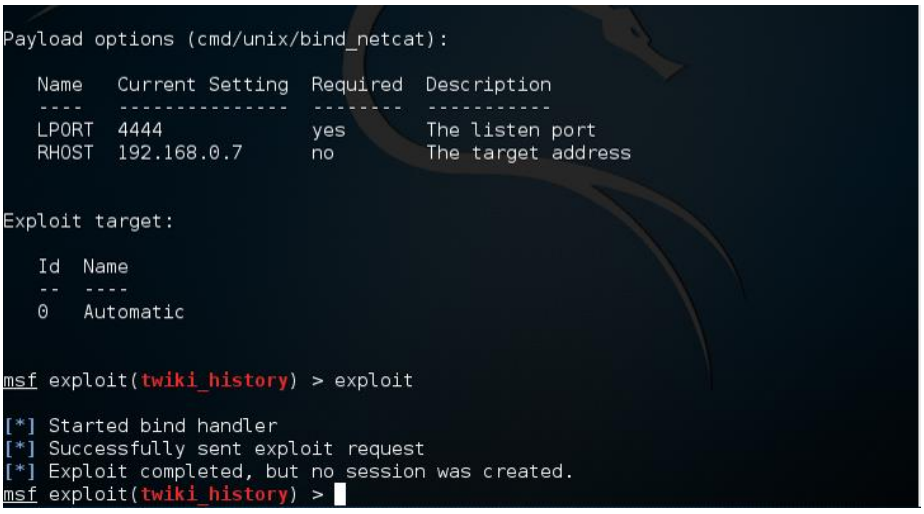
Figura 52. Opciones del Exploit para servicio httpd



Fuente: Autor del trabajo

La siguiente imagen pauta el proceso de ejecución del exploit con todas las opciones configuradas, pero el acceso no fue satisfactorio ya que no se logró crear la sesión en el servidor.

Figura 53. Ejecución del Exploit par servicio httpd



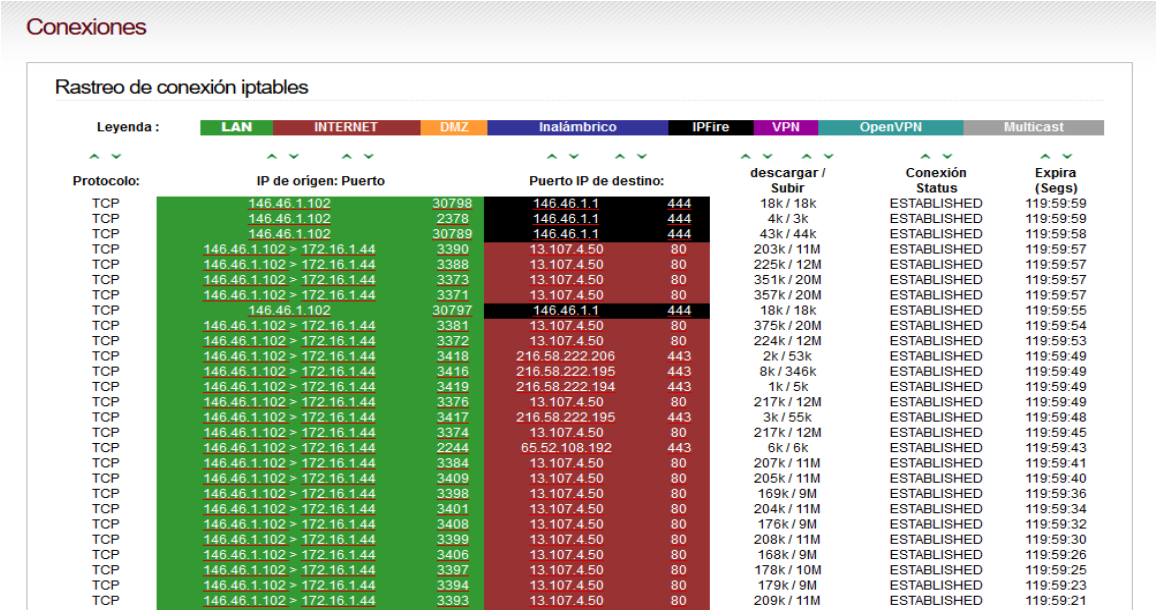
Fuente: Autor del trabajo

6.4 INFORME DE EJECUCIÓN

Al implementar el *appliance* dentro de la infraestructura de la empresa es posible evidenciar la capacidad de procesamiento del dispositivo al conectar diez equipos simultáneamente al interfaz de red verde del *firewall*.

Estos equipos generaron tráfico de datos normal de la empresa hacia internet, en el cual los equipos y los usuarios realizaron diferentes actividades como actualizaciones, descarga de archivos, visita a sitios web, entre otras actividades. El *firewall* logro capturar y analizar todo el tráfico permitido o denegado configurado en el filtro web obteniendo los siguientes resultados:

Figura 54. Registro de conexiones

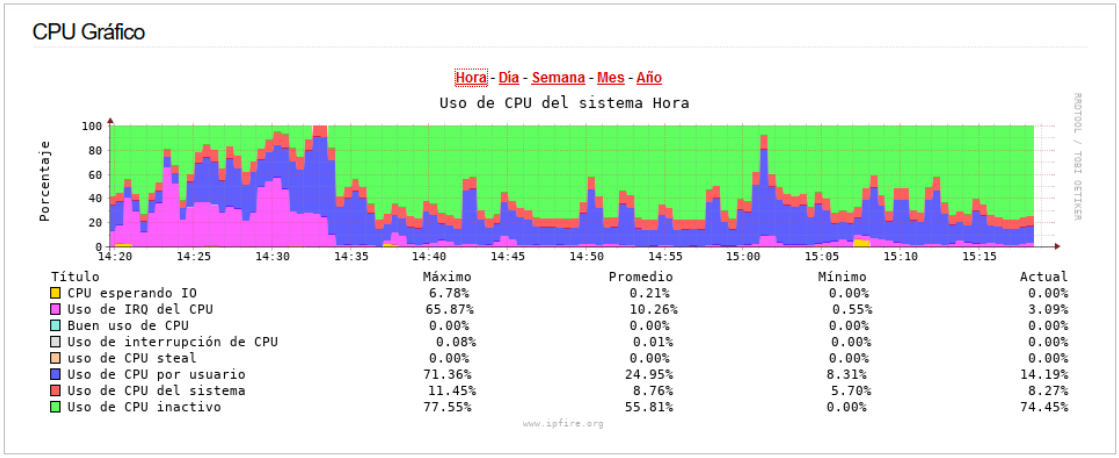


Protocolo:	IP de origen: Puerto		Puerto IP de destino:		descargar / Subir	Conexión Status	Expira (Segs)
TCP	146.46.1.102	30798	146.46.1.1	444	18k / 18k	ESTABLISHED	119:59:59
TCP	146.46.1.102	2378	146.46.1.1	444	4k / 3k	ESTABLISHED	119:59:59
TCP	146.46.1.102	30789	146.46.1.1	444	43k / 44k	ESTABLISHED	119:59:58
TCP	146.46.1.102 > 172.16.1.44	3390	13.107.4.50	80	203k / 11M	ESTABLISHED	119:59:57
TCP	146.46.1.102 > 172.16.1.44	3388	13.107.4.50	80	225k / 12M	ESTABLISHED	119:59:57
TCP	146.46.1.102 > 172.16.1.44	3373	13.107.4.50	80	351k / 20M	ESTABLISHED	119:59:57
TCP	146.46.1.102 > 172.16.1.44	3371	13.107.4.50	80	357k / 20M	ESTABLISHED	119:59:57
TCP	146.46.1.102	30797	146.46.1.1	444	18k / 18k	ESTABLISHED	119:59:55
TCP	146.46.1.102 > 172.16.1.44	3381	13.107.4.50	80	375k / 20M	ESTABLISHED	119:59:54
TCP	146.46.1.102 > 172.16.1.44	3372	13.107.4.50	80	224k / 12M	ESTABLISHED	119:59:53
TCP	146.46.1.102 > 172.16.1.44	3418	216.58.222.206	443	2k / 53k	ESTABLISHED	119:59:49
TCP	146.46.1.102 > 172.16.1.44	3416	216.58.222.195	443	8k / 346k	ESTABLISHED	119:59:49
TCP	146.46.1.102 > 172.16.1.44	3419	216.58.222.194	443	1k / 5k	ESTABLISHED	119:59:49
TCP	146.46.1.102 > 172.16.1.44	3376	13.107.4.50	80	217k / 12M	ESTABLISHED	119:59:49
TCP	146.46.1.102 > 172.16.1.44	3417	216.58.222.195	443	3k / 55k	ESTABLISHED	119:59:48
TCP	146.46.1.102 > 172.16.1.44	3374	13.107.4.50	80	217k / 12M	ESTABLISHED	119:59:45
TCP	146.46.1.102 > 172.16.1.44	2244	65.52.108.192	443	6k / 6k	ESTABLISHED	119:59:43
TCP	146.46.1.102 > 172.16.1.44	3384	13.107.4.50	80	207k / 11M	ESTABLISHED	119:59:41
TCP	146.46.1.102 > 172.16.1.44	3409	13.107.4.50	80	205k / 11M	ESTABLISHED	119:59:40
TCP	146.46.1.102 > 172.16.1.44	3398	13.107.4.50	80	169k / 9M	ESTABLISHED	119:59:36
TCP	146.46.1.102 > 172.16.1.44	3401	13.107.4.50	80	204k / 11M	ESTABLISHED	119:59:34
TCP	146.46.1.102 > 172.16.1.44	3408	13.107.4.50	80	176k / 9M	ESTABLISHED	119:59:32
TCP	146.46.1.102 > 172.16.1.44	3399	13.107.4.50	80	208k / 11M	ESTABLISHED	119:59:30
TCP	146.46.1.102 > 172.16.1.44	3406	13.107.4.50	80	168k / 9M	ESTABLISHED	119:59:26
TCP	146.46.1.102 > 172.16.1.44	3397	13.107.4.50	80	178k / 10M	ESTABLISHED	119:59:25
TCP	146.46.1.102 > 172.16.1.44	3394	13.107.4.50	80	179k / 9M	ESTABLISHED	119:59:23
TCP	146.46.1.102 > 172.16.1.44	3393	13.107.4.50	80	209k / 11M	ESTABLISHED	119:59:21

Fuente: Autor del trabajo

La anterior imagen describe algo del trafico que fue analisado a travez de los distintos equipos en la interfaz verde o LAN, estos registros son guardados en el sistema y pueden ayudar a generar informes para la toma de desiciones y ayudar a mantener un adecuado uso del canal de internet de la empresa.

Figura 55. Uso del CPU

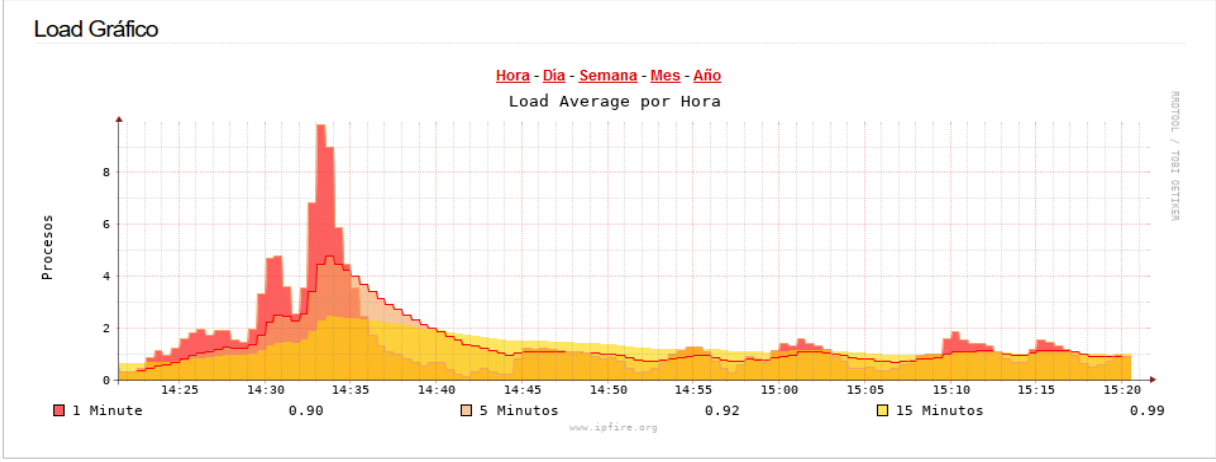


Fuente: Autor del trabajo

En la anterior imagen se respeta la discriminación del uso de la capacidad del procesador de la placa de circuitos durante una hora en constante funcionamiento, en el periodo de tiempo se realizaron actualizaciones de los sistemas operativos y actividades generales del personal por esta razón el equipo se ve en la necesidad de usar gran parte en el “Uso del CPU por usuario”.

En el siguiente periodo de tiempo el CPU, no uso tantos recursos, pero a pesar de que antes se usó el canal en distintas actividades, la capacidad de respuesta no se vio opacada por la exigencia en cuanto al procesamiento de datos.

Figura 56. Procesos atendidos



Fuente: Autor del trabajo

Como se mencionó anteriormente el dispositivo proceso diferentes peticiones de los equipos de los usuarios y el consumo de memoria RAM tampoco presento alteraciones por la demanda de peticiones, como se puede observar en la siguiente imagen

Figura 57. Uso de memoria RAM

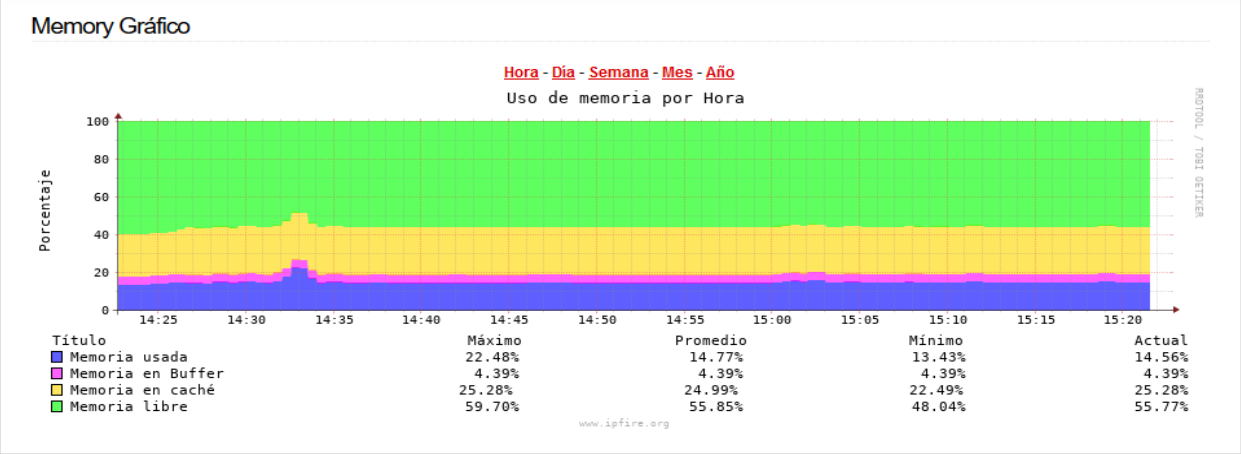
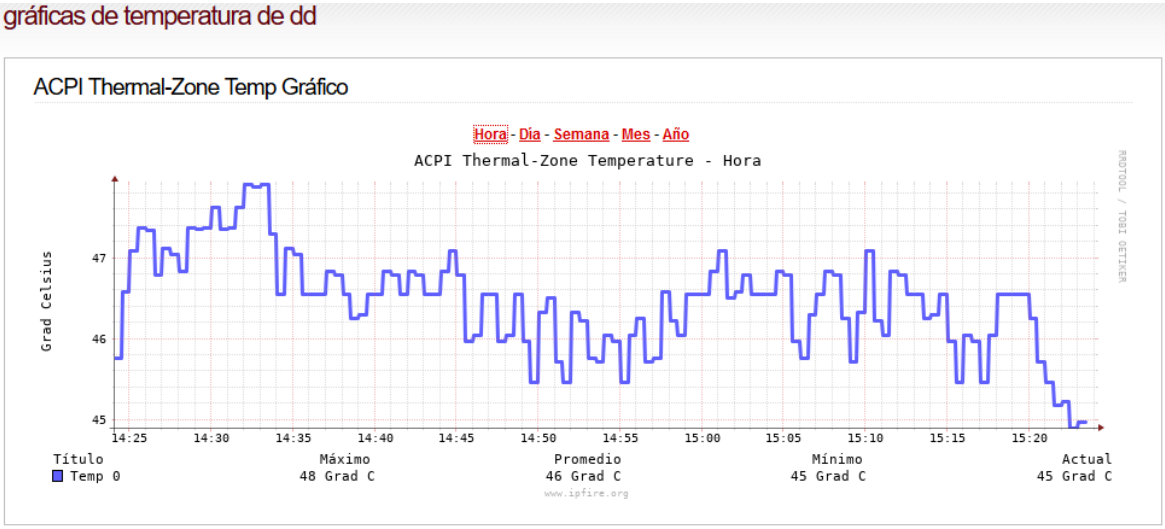


Figura 57. (Continuación)

Fuente: Autor del trabajo

Otra de las herramientas del sistema es la de monitorear el estado de la temperatura del hardware y tomar daciones frente al tema, como añadir disipadores de calor o ventiladores.

Figura 58. Temperatura



Fuente: Autor del trabajo

En la imagen anterior se evidencia el registro de temperatura generado por el uso continuo del equipo puede ser fácilmente controlado por pequeños disipadores que aportan a la expulsión del calor generado por la energía en los microprocesadores con el fin de no interferir con el correcto funcionamiento del *appliance*.

En cuanto al funcionamiento del *firewall* como dispositivo de seguridad perimetral, logro bloquear los intentos de intrusión mediante las políticas y herramientas de

sistema de detección de intrusos, probando que es un dispositivo que puede ser fácilmente implementado en una red de datos de una empresa pequeña.

Figura 59. Registro de conexiones permitidas y denegadas

Hora	Cadena	Iface	Proto	Orígen Destino	Puerto orígen Puerto Dst	País	Dirección MAC
16:58:35	DNAT	red0	TCP	192.168.0.100 192.168.0.7	52549 80(HTTP)		08:00:27:43:82:bb
16:58:35	DNAT	red0	TCP	192.168.0.100 192.168.0.7	52549 22(SSH)		08:00:27:43:82:bb
16:58:35	DNAT	red0	TCP	192.168.0.100 192.168.0.7	52549 21(FTP)		08:00:27:43:82:bb
16:58:37	DNAT	red0	TCP	192.168.0.100 192.168.0.7	52560 80(HTTP)		08:00:27:43:82:bb
16:58:38	DNAT	red0	TCP	192.168.0.100 192.168.0.7	52561 80(HTTP)		08:00:27:43:82:bb
20:47:44	DROP_NEWNOTSYN	green0	TCP	146.46.1.10 192.168.0.100	21(FTP) 39251		08:00:27:f9:e3:fc
23:37:25	DNAT	red0	TCP	192.168.0.100 192.168.0.7	35875 80(HTTP)		08:00:27:43:82:bb
23:37:26	DROP_INPUT	red0	TCP	192.168.0.100 192.168.0.7	44667 4444		08:00:27:43:82:bb
23:37:28	DROP_INPUT	red0	TCP	192.168.0.100 192.168.0.7	44667 4444		08:00:27:43:82:bb
23:37:32	DROP_INPUT	red0	TCP	192.168.0.100 192.168.0.7	44667 4444		08:00:27:43:82:bb

Fuente: Autor del trabajo

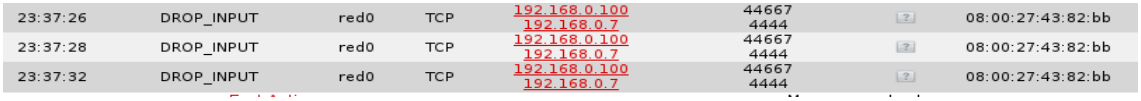
La cadena “DNAT” representa las conexiones entrantes re direccionadas y la cadena “DROP_INPUT” representa las conexiones bloqueadas por el sistema

7. RESULTADOS

La ejecución de una buena configuración en un *firewall*, puede ayudar a mitigar los riesgos que posee la infraestructura tecnológica ya que a pesar de tener instalado servicios que no se encuentran parchados o actualizados poseen amenazas a las cuales, distintos tipos de delincuentes informáticos tienen acceso.

Dentro del laboratorio desarrollado se evidenciaron que las aplicaciones del *firewall* responden correctamente y que los accesos denegados son registrados y bloqueados para ayudar a los administradores y responsables de respaldar y proteger la información en la entidad.

Figura 60. Registro de bloqueo



23:37:26	DROP_INPUT	red0	TCP	192.168.0.100 192.168.0.7	44667 4444		08:00:27:43:82:bb
23:37:28	DROP_INPUT	red0	TCP	192.168.0.100 192.168.0.7	44667 4444		08:00:27:43:82:bb
23:37:32	DROP_INPUT	red0	TCP	192.168.0.100 192.168.0.7	44667 4444		08:00:27:43:82:bb

Fuente: Autor del trabajo

La anterior imagen evidencia el registro y bloqueo del intento de vulnerar los servicios implementados, a los cuales los distintos tipos de personas tienen acceso.

Tabla 3. Descripción de resultados de ataques a los servicios

Nombre del Servicio	Puerto	Versión	Descripción del Ataque ejecutado	Resultado del Ataque a los servicio
FTP	21	vsftp 2.3.4	Para este servicio se usó el exploit vsftpd_234_backdoor que ejecuta una serie de instrucciones ante la versión de este servicio vulnerable, pero no se logró establecer una sesión ya que el firewall bloquea ese tipo de conexiones	Fallido
SSH	22	OpenSSH 4.7	En este servicio se efecto un ataque de fuerza bruta pero difícilmente se lograra tener éxito si no se conoce un usuario y contraseña para la conexión ya que existen un amplio campo de posibilidades y una maquina normal tardaría demasiado tiempo en probar todas las combinaciones	Fallido
HTTPD Apache	80	Apache httpd 2.2.8	El ataque a este servicio no logro efectuarse ya que el firewall bloqueo la conexión entre la maquina atacante, se usó el exploit twiki_hisory de la categoría de los equipos Unix – webapp y se usó el payload bind_netcat	Fallido

Fuente: Autor del trabajo

De acuerdo a la anterior tabla se puede evidenciar que todos los ataques realizados a los diferentes servicios no pudieron ser efectuados ya que el *firewall* logro bloquear y registrar las conexiones que pueden interferir con el correcto funcionamiento del servicio atacado.

A pesar de que el *appliance* cumplió con las expectativas propuestas, es necesario describir algunos aspectos importantes y recomendaciones que se generaron a través de la construcción e implementación del dispositivo.

La placa de circuitos reducida es muy sencilla de encontrar dentro de muchas tiendas especializas en robótica o tiendas en internet, en un costo muy bajo y el *firewall*, al ser código abierto está disponible para cualquier persona que desee usar este *software*, pero el medio de almacenamiento usado en este proyecto fue una memoria micro SD de 8 GB clase 4, esta memoria presenta demora en la lectura y escritura de datos, aunque son tiempos cortos pueden llegar a mejorarse mediante el uso de dispositivos de almacenamiento mejores como memorias micro SD de 8 GB o más, clase 10, las cuales ayudaría a mejorar la velocidad de trasferencia en cuanto a lectura y escritura de los datos del sistema.

Dentro de las debilidades evidenciadas en la implementación del *appliance* se destaca que, al ser un *hardware* limitado por sus componentes la cantidad de equipos conectados puede ser limitada, por esta razón se recomienda realizar un monitoreo más exhaustivo si los equipos conectados sobrepasan los diez (10)

dispositivos ya que en la evaluación realizada del uso del procesador, su máximo funcionamiento se evidencio en el momento que el sistema operativo de la gran mayoría de los equipos descargaba actualizaciones del sistema y otros usuarios navegaban normalmente. Aunque no se evidencio retraso en sobre la transferencia de datos a través de un navegador web, estos procesos ejecutados simultáneamente durante un largo periodo de tiempo, pueden interferir con el normal funcionamiento del dispositivo. Para solucionar este tipo de inconvenientes es posible bloquear el tráfico o descarga de actualizaciones mediante reglas de salida del *firewall*.

Los aspectos positivos logrados recolectar a través de la constricción, configuración e implementación del dispositivo se encuentra la administración del equipo ya que presenta un entorno intuitivo, facilitando a los usuarios mecanismo para optimizar el canal de internet.

El *software* presenta mucha fluidez en el *hardware* y constantemente se pueden encontrar actualizaciones del sistema que ayudan a mitigar cualquier tipo de vulnerabilidad del sistema, mejorando las funciones del sistema. Por otra parte, existen múltiples complementos que ayudarían al fortalecimiento del dispositivo.
Dada la versatilidad del *hardware* usado en este proyecto no requiere de unas condiciones específicas para su funcionamiento, no obstante, es necesario disponer de un lugar en el cual la placa de circuitos no este expuesta a condiciones que puedan afectar su funcionamiento, como exceso de calor, luz solar directa, entre otras. Por esta razón se recomienda buscar un espacio adecuado para su implementación.

Cabe resaltar que, a pesar de ser una solución para mejorar la seguridad perimetral de la empresa, ayuda considerablemente a mejorar la administración y restricción de permisos de acceso a la red interna y externa, ya que el tráfico es analizado en tiempo real y mediante las reglas configuradas es posible restringir o permitir el acceso.

8. CONCLUSIONES

Al finalizar la ejecución del proyecto se cumplió con todos los objetivos planteados, ayudando a mejorar la seguridad perimetral de la empresa, implementando así un mecanismo más, para el apoyo de la protección de todo el parque tecnológico y de la información de la empresa.

Gracias al levantamiento de requisitos de la infraestructura tecnológica de la empresa se realizó un diseño acertado a las necesidades de la empresa TAIO SYSTEMS permitiendo generar una propuesta eficaz para la implementación del dispositivo de seguridad perimetral.

Teniendo en cuanta el estudio realizado en la etapa previa al diseño del dispositivo se identificaron los componentes necesarios para la construcción del equipo, creando una propuesta adecuada para la protección de datos según el esquema planteado.

Al generar el dispositivo como propuesta para apoyar la seguridad perimetral de la red de datos de TAIO SYSTEMS se implementó un control adecuado para el tráfico de datos que mantiene la empresa. Gracias a la creación de un conjunto de reglas dentro del *firewall* se logró establecer un adecuado uso del canal de internet mejorando considerablemente el tiempo de respuesta de los exploradores de internet

La adecuada configuración de la propuesta planteada, para mejorar la seguridad perimetral de TAIO SYSTEMS sirvió para demostrar la eficiencia del dispositivo al denegar conexiones que no se encuentren dentro del conjunto de reglas evitando así ataques o conexiones no deseadas hacia la empresa como desde dentro de ella, ya que el laboratorio realizado genero resultados satisfactorios al usar ataques ya probados en servicios vulnerables que no poseen ninguna actualización para mejorar su rendimiento.

9. RECOMENDACIONES

Se recomienda usar un medio de almacenamiento como una memoria micro USB mayor de 8 GB clase 10.

La placa al no contar con ninguna protección física es necesario disponer un sitio donde el sol no se proyecte directamente

10. BIBLIOGRAFÍA

Anon. Las pymes son más propensas a los ataques en la red En Colombia.com Internet: (<http://www.colombia.com/tecnologia/actualidad/sdi/111715/las-pymes-son-mas-propensas-a-los-ataques-en-la-red>).

Anon. Seguridad informática en Colombia por buen camino En Latin Pyme Internet: (<http://www.latinpymes.com/articulo/3263>).

ASTUDILLO, Karina. Hacking Ético 101. Cómo hackear profesionalmente en 21 días o menos!. July, 2016. Create Space.

ECHEVERRY MATIAS, Daniel. Propuesta E Implementación De Un Appliance De Seguridad A Partir Del Re-Uso Tecnológico. Pereira, 2011.Tesis. Universidad Católica De Pereira.

Du R., Safavi R., Susilo W. Design and Implementation of A Content Filtering Firewall (Diseño e implementación de un firewall de filtrado web). Australia. Tesis. University of Wollongong.

JARA, Héctor y PACHECO, Federico. Ethical hacking 2.0. 1ª ed. Buenos Aires, 2012. Fox Andina.

PEÑREDONDA, José, “Cifras del mintic revelan que las pymes se montaron en internet”.Internet: (http://www.enter.co/especiales/enterprise/cifras-del-mintic-revelan-que-las-pymes-se-montaron-en-internet/).

PERAFÁN RUIZ, John Jairo y CAICEDO CUCHIMBA, Mildred. Análisis de Riesgos de la Seguridad de la Información para la Institución Universitaria Colegio Mayor Del Cauca. Popayán, 2014. Tesis posgrado, Universidad Nacional Abierta y a Distancia.

PÉREZ LLOPIS, Israel. Arquitectura de un sistema C4ISR para pequeñas unidades. Tesis doctoral.

MARTÍNEZ K, Pacheco y ZÚÑIGA, J. FIREWALL-LINUX: una solución de seguridad informática para pymes (pequeñas y medianas empresas). Tesis. Universidad Industrial de Santander.

MARTINSEN, P. Titulado Configuration And Implementation Issues For A Firewall System Running On A Mobile Handset. Tesis (master of information). Queensland University of Technology.

MORALES TEJEDA, Carlos Gustavo. Estudio, diseño e implementación de un Firewall. 2002. Tesis.

SANTOS, Mateo, "Las Pymes son el eslabón más débil de la cadena de seguridad". Internet:(<http://www.enter.co/chips-bits/enterprise/las-pymes-son-el-eslabon-mas-debil-de-la-cadena-de-seguridad/>).

_____, "Los retos de seguridad para las Pymes". Internet: (<http://www.enter.co/especiales/enterprise/los-retos-de-seguridad-para-las-pymes/>).

_____, "Las Pymes son el eslabón más débil de la cadena de seguridad". Internet: (http://www.enter.co/chips-bits/enterprise/las-pymes-son-el-eslabon-mas-debil-de-la-cadena-de-seguridad/).

SIERRA JARAMILLO, Oscar Andrés. Estudio De Los Procesos De Seguridad De La Información Digital En Las Empresas Del Departamento De Risaralda. Pereira, 2011. Tesis. Universidad Tecnológica De Pereira.

ABC
www.abc.es <http://www.abc.es/economia/abci cibercrimen-empresas-arman-contra-guerra-virtual-201601112310_noticia.html>

ARROW
www.arrowecs.es <http://www.arrowecs.es/ficheros/partners/20_FortiGate.pdf>

FORTINET
www.fortinet.com <https://www.fortinet.com/>

IPCOP
www.ipcop.org <http://www.ipcop.org/>

IPFIRE
www.ipfire.org < http://www.ipfire.org/>

ITPROPORTAL
www.itproportal.com <http://www.itproportal.com/2015/08/21/the-top-enterprise-firewalls-of-2015>

PFSENSE
www.pfsense.org <https://www.pfsense.org/>

RASPBERRY PI
www.raspberrypi.org <https://www.raspberrypi.org/>

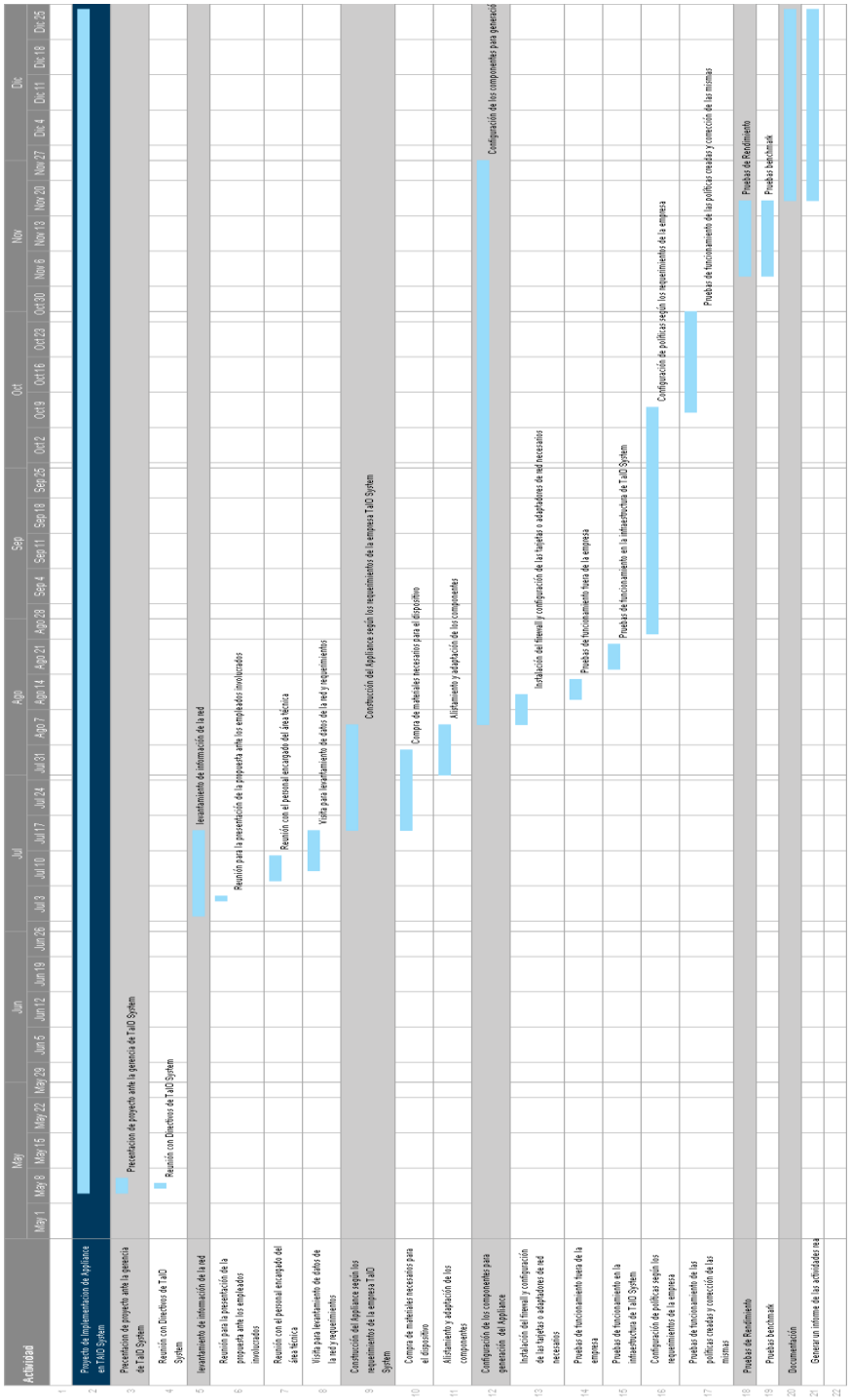
SYMANTEC
www.symantec.com/es/es <https://www.symantec.com/es/es/>

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
unad.edu.co <http://unad.edu.co>

WELIVESECURITY
www.welivesecurity.com <http://www.welivesecurity.com/la-es/2014/07/29/por-que-necesario-firewall-entornos-corporativos/>

11.ANEXOS

Diagrama de Gantt



CARTA DE APROBACIÓN DE LA EMPRESA:

Popayán, 17 de Mayo de 2016

Señores
Universidad Nacional Abierta y a Distancia UNAD

Asunto: Aceptación de propuesta sobre el análisis de funcionamiento de proyecto planteado por el estudiante Juan Sebastián Chcaiza Pareja

Cordial saludo.

El motivo de esta carta es informarle de la aceptación del alumno de la especialización en seguridad informática Juan Sebastián Chicaiza de cedula de ciudadanía 1061746279 para realizar las pruebas necesarias para lograr culminar su análisis en la implantación de un appliance de seguridad dentro de nuestro empresa TalO Systems, realizando la labor de registro de datos en cuanto a rendimiento y otros estudios.

Atentamente,

FRANCISCO MARTÍNEZ
Gerente TalO Systems

Formato RAE

Fecha de Realización: 6/12/2016
Título: IMPLEMENTACIÓN DE UN FIREWALL CONSTRUIDO A PARTIR DE SOFTWARE Y UNA PLACA DE CIRCUITOS COMPACTA O SBC (SINGLE BOARD COMPUTER) EN LA EMPRESA TAIO SYSTEMS DE LA CIUDAD DE POPAYÁN
Autor: CHICAIZA PAREJA, Juan Sebastian
Palabras Claves: Placa de Circuitos compacta, firewall, seguridad perimetral, Appliance, pymes, red de datos, pentest.
Descripción: El proyecto consiste en la implementación de un firewall construido con tecnología de bajo costo y software libre, para la empresa TaIO Systems de la ciudad de Popayán la cual no cuenta con medidas ni herramientas que apoyen la seguridad de la información de la red de la empresa
Fuentes: JARA, Héctor y PACHECO, Federico. Ethical hacking 2.0. 1ª ed. Buenos Aires, 2012. Fox Andina. SANTOS, Mateo, “Las Pymes son el eslabón más débil de la cadena de seguridad”. Internet:(<http://www.enter.co/chips-bits/enterprise/las-pymes-son-el-eslabon-mas-debil-de-la-cadena-de-seguridad/>). SANTOS, Mateo, “Los retos de seguridad para las Pymes”. Internet: (<http://www.enter.co/especiales/enterprise/los-retos-de-seguridad-para-las-pymes/>). Las pymes son más propensas a los ataques en la red En Colombia.com Internet: (<http://www.colombia.com/tecnologia/actualidad/sdi/111715/las-pymes-son-mas-propensas-a-los-ataques-en-la-red>). WELIVESECURITY www.welivesecurity.com, “Por qué necesario firewall entornos corporativos”. Internet: <http://www.welivesecurity.com/la-es/2014/07/29/por-que-necesario-firewall-entornos-corporativos/> Las pymes son más propensas a los ataques en la red En Colombia.com Internet: (<http://www.colombia.com/tecnologia/actualidad/sdi/111715/las-pymes-son-mas-

propensas-a-los-ataques-en-la-red>).

IPFIRE
www.ipfire.org < http://www.ipfire.org/>

RASPBERRY PI
www.raspberrypi.org <https://www.raspberrypi.org/>

MARTÍNEZ K, Pacheco y ZÚÑIGA, J. FIREWALL-LINUX: una solución de seguridad informática para pymes (pequeñas y medianas empresas). Tesis. Universidad Industrial de Santander.

PEÑREDONDA, José, “Cifras del mintic revelan que las pymes se montaron en internet”.Internet: (http://www.enter.co/especiales/enterprise/cifras-del-mintic-revelan-que-las-pymes-se-montaron-en-internet/).

Contenido del documento:

Con el desarrollo de la presenta propuesta,se busca diseñar una solución que apoye la protección de datos en una red mediante la implementación de un appliance de seguridad perimetral, haciendo uso de placas de circuitos llamada Raspberry PI modelo 1 B y un firewall libre, IpFire.

El trabajo realizado presenta un caso de éxito en la implementación del dispositivo en la empresa TaIO Systems de la ciudad de Popayán el cual fue concebido en un corto periodo de tiempo permitiendo apoyar en gran medida la protección de datos de la red de la empresa de una forma eficiente.

Como propuesta adicional al proyecto se planteó evaluar el funcionamiento del firewall, para ello se conformó un ambiente de pruebas en el cual se usaron máquinas virtuales con servicios que pueden ser vulnerados mediante porciones de código malicioso o exploits, que afectan el correcto funcionamiento de los equipos, gracias al uso de las herramientas especializadas para el reconocimiento de vulnerabilidades en dispositivos o equipo se evaluó los servicios implementados para ejecutar algunas pruebas y comprobar el funcionamiento del dispositivo, con el fin de mejorar la configuración implementada para la empresa donde se ejecutó el proyecto.

Por otra parte, se realizó un estudio del funcionamiento del firewall en el hardware

usado, presentando buenos resultados logrando procesar todas las peticiones en tiempo real sin afectar el correcto funcionamiento de la red de la empresa TaIO Systems mediante las herramientas de monitoreo del firewall.

Metodología:

TIPO DE INVESTIGACIÓN

El presente estudio es de carácter descriptivo, con enfoque cuantitativo y cualitativo. Se realizará un análisis cualitativo de la red de datos del edificio donde se encuentra ubicada la empresa TAIO SYSTEMS, con el fin de definir las posibles falencias que conllevaron a la problemática actual. La investigación explicativa permitirá analiza, las causas y las consecuencias derivadas de la falta de control de tráfico de datos.

La investigación tomará un enfoque cualitativo ya que el proyecto estará basado en el estudio de las características de un Firewall construido a partir de un software libre y una placa de circuitos compacta y un enfoque cuantitativo realizado por medio de pruebas de funcionamiento al dispositivo implementado.

MÉTODOS DE OBSERVACIÓN.

La técnica a utilizar es el método de análisis, que se realizará con la recolección de información del nivel de seguridad informática de acuerdo a los controles implementados en la empresa, encontrando de esta manera, las principales falencias en el marco de seguridad de la entidad que impide o pone en riesgo la protección de los datos y dispositivos a nivel perimetral, para lograr entender los efectos positivos que se tienen en la red con el uso de un dispositivo de seguridad perimetral, se desarrollara el estudio y análisis de las propuestas que han realizado diferentes personas, buscando así mejorar o controlar el tráfico de una red en una empresa por medio de soluciones de seguridad como un firewall open source.

Se realizarán visitas a la empresa TAIO SYSTEMS en la ciudad de Popayán y se hará un registro fotográfico, análisis y diagnóstico de los controles de red implementados con el fin de evidenciar las condiciones actuales en las que se encuentra la empresa en cuanto a seguridad informática.

Se registrarán datos observados, se interpretarán y se elaborarán conclusiones de acuerdo al análisis de dicha información.

Partiendo de las problemáticas identificadas, que no permiten un adecuado nivel de seguridad se propondrá la implementación de un appliance que apoye y aporte al mejoramiento de la seguridad perimetral de la empresa.

La investigación se llevará a cabo en 4 etapas:

Etapa 1. Interpretativa

Para la recolección de la información se parte del análisis de:

- Contextualización de la problemática actual de la seguridad informática.
- estudio de un firewall (funcionamiento y análisis)
- investigación de la placa de circuitos compacta RASPBERRY PI1.
- Networking (Trabajo de red)

Etapa 2. Trabajo de campo.

- Levantamiento de la información y análisis de la topología de red de la empresa para identificar sus principales falencias.
- Análisis visual y registro fotográfico del estado de la red de la empresa.
- Estudio de los factores positivos de la red de la empresa TAIO SYSTEMS
- Diagnóstico del estado de la red de datos de la empresa

Etapa 3. Propositiva:

Proponer una appliance que aporte al mejoramiento de la seguridad perimetral de la red de datos de la empresa, definiendo reglas ayuden al control de acceso o restricción a la red.

Etapa 4: pruebas.

Realizar pruebas del funcionamiento del appliance.

Conceptos nuevos: seguridad perimetral
Conclusiones: Al ejecutar el proyecto se cumplió con todos los objetivos planteados, ayudando a mejorar la seguridad perimetral de la empresa, implementando así un mecanismo más, para el apoyo de la protección de todo el parque tecnológico y de la información de la empresa Las reglas creadas dentro del firewall permitirán tener un mayor control sobre todo el tráfico de datos a través del canal de internet de TAIO SYSTEMS. El desarrollo e implementación de la propuesta planteada para mejorar la seguridad perimetral de TAIO SYSTEMS fue desarrollada con materiales de bajo costo generando un punto de partida para otras empresas que deseen implementar soluciones como estas. La configuración usada sirvió para demostrar que el appliance funciona correctamente bloqueado los accesos no autorizados a la red interna. El appliance puede ser fácilmente implementado en otra empresa que posea características similares en cuanto a infraestructura tecnología, topología de red y cantidad de equipos Se recomienda usar un medio de almacenamiento como una memoria micro USB mayor de 8 GB clase 10. La placa de circuitos, al no tener ninguna protección física es necesario disponer un sitio donde el sol no se proyecte directamente o adquirir un protector para la placa de circuitos
AUTOR: JUAN SEBASTIAN CHICAIZA PAREJA