Universidad Católica Andrés Bello

Facultad De Ingeniería

Escuela De Ingeniería De Telecomunicaciones

IMPLEMENTACIÓN DE UN SISTEMA DE ANÁLISIS DE TRÁFICO DE RED, MEDIANTE EL PROTOCOLO SFLOW EN LA RED INTERNA DE LA TORRE MISTRAL PARA LA EMPRESA SANFAR

INFORME DE AVANCE DEL TRABAJO ESPECIAL DE GRADO
Presentado ante la
UNIVERSIDAD CATÓLICA ANDRÉS BELLO
Como parte de los requisitos para optar al título de
INGENIERO EN TELECOMUNICACIONES

REALIZADO POR: Br. Chacón Ramones, Luis Orlando
Br. Moreno Baute, Robert Alejandro
TUTOR: Lic. Salazar Cardozo, Dagny Rene

Caracas, octubre de 2021

Resumen

El presente proyecto tiene como finalidad, mostrar el producto final del Trabajo Especial de Grado, sobre la "Implementación de un Sistema de Análisis de Tráfico de Red", Mediante el Protocolo sFlow en la Red Interna de la Torre Mistral para la Empresa SANFAR". El Trabajo de Grado, busca diseñar una propuesta de implementación de un protocolo de análisis de flujo de tráfico. El protocolo que se implementó es sFlow, por su interoperabilidad con la infraestructura tecnológica existente; además, de ser un estándar de la industria que se encuentra publicado en el RFC (*Request For Comments*) 3176 de la IETF (*Internet Engineering Task Force*), cabe destacar su versatilidad a la hora de recopilar información que se encuentra desde la capa 2 a capa la 7 del modelo OSI (*Open Systems Interconnection*) del tráfico de la red. La información recolectada se envía a la plataforma Prometheus, esta base de datos a su vez, se encarga de publicar la información a Grafana para la visualización y posterior análisis del flujo de tráfico. Como premisa antes de implementar la plataforma de monitoreo, se realizó una prueba de concepto entre varias herramientas, para que a través de una matriz comparativa se seleccionara la que mejor se adaptara a las necesidades de la corporación; dichas pruebas se virtualizaron en un servidor corporativo, donde se determinó la plataforma idónea.

Como parte de este proyecto se ejecutó un levantamiento de información de la red LAN empresarial, con la finalidad de tener una visión general de los dispositivos, diseño lógico-físico y protocolos pertenecientes a dicha red.

Una vez recopilada la información necesaria, se reunieron los resultados de la prueba de concepto y se procedió a la implementación de la plataforma en la red.

Palabras Claves: Análisis de Tráfico de Red, sFlow, IETF, RFC, modelo OSI, Prometheus, Grafana, monitoreo, LAN.

Índice General

Índice de Tablas

Índice de Figuras

CAPÍTULO I

Introducción

Hoy en día es necesario monitorear el tráfico interno de la red para inspeccionar las actividades realizadas por los usuarios, realizando una auditoría de las operaciones efectuadas, examinando el tráfico que estas generan, tipos de protocolos en la comunicación, equipos a los cuales acceden dentro de la empresa, usuario que efectúa la conexión y cuáles son los servicios corporativos a los que acceden, analizando si lo utilizan apropiadamente.

El presente Trabajo de Grado se implementó en la empresa SANFAR, industria perteneciente a la rama farmacéutica, creada en el año 1951 con la cadena de Farmacias S.A. Nacional Farmacéutica (SANFAR). Absorbida en el 2004 por el Grupo Mistral, institución con amplia trayectoria en el mercado venezolano dedicado a ofrecer productos y servicios de alta calidad para el bienestar de sus clientes, desarrollándose en la distribución, compra y venta de productos farmacéuticos naturales, preparaciones galénicas, cosméticas, perfumería, misceláneos, material médico quirúrgico, productos veterinarios, productos biológicos y en general todo tipo lícito de comercio ajustado a la Ley del Ejercicio de la Farmacia y su reglamento. Teniendo como misión “ser un grupo apasionado y persistente que brinda bienestar a nuestros clientes, trabajadores, accionistas, proveedores y comunidad, con calidad impecable de nuestra gente, procesos, productos y servicios” y visión “posicionar nuestros negocios entre los tres primeros en su ramo, utilizando nuestras sinergias naturales para satisfacer a nuestro consumidor”.

Para llevar a cabo el desarrollo de este proyecto se definieron tres fases, la primera consistió en toda la recopilación de la información pertinente a la teoría y funcionamiento, además de comparar las características presentes en cada uno de los sistemas de monitoreo a implementar. En la segunda fase, se realizó la

implementación de pruebas de conceptos de los diferentes sistemas de monitoreo, en donde se obtuvieron las características de cada sistema, así como sus ventajas y desventajas, para poder determinar cuál es el sistema que mejor se adapta a las necesidades de la empresa Mistral. La tercera y última fase, consistió en el acoplamiento del sistema de análisis con el resto de la red, en donde con base a los resultados obtenidos en la segunda fase, se eligió y sistema de monitoreo a implementar.

I.1.- Planteamiento del Problema

Debido a la imposibilidad de identificar la procedencia del tráfico interno en la red LAN, las constantes consultas realizadas a los distintos servidores, la falta de registro del tráfico por parte de los usuarios finales y debido a los ataques sufridos a los servidores internos de la Torre Mistral, surge la necesidad de implementar un sistema de monitoreo capaz de identificar dicho tráfico interno. Por lo expuesto anteriormente, se propone a la empresa SANFAR que se implemente un sistema de análisis del flujo interno de la red basado en el protocolo sFlow, en la Torre Mistral, que permita constatar en tiempo real el tráfico interno de la red y crear registros históricos del mismo. Es importante mencionar que el flujo de tráfico de la red está conformado por paquetes, que se analizan muestreando cierta información contenida dentro del flujo, por el contrario a otros métodos de análisis que capturan el paquete completo. A través del protocolo sFlow se extrae información como la contenida en la cabecera de los paquetes, el origen y el destino de los paquetes, los puertos involucrados, dirección del próximo salto, a cuál VLAN pertenece el paquete y más información que permita tener mayor visibilidad del tráfico de la red. La información será recopilada, analizada y entregada a un servidor virtualizado que pasará a formar parte de la red y este contendrá una plataforma de visualización y base de datos que permita la auditoría de las conexiones internas de la red por parte de la gerencia IT.

I.2.- Objetivos

I.2.1.- Objetivo General:

Implementar un sistema de análisis de tráfico de red, mediante el protocolo sFlow en la intranet de la Torre Mistral, con el fin de monitorear y analizar el tráfico, obtener registros históricos de las actividades de los usuarios y equipos pertenecientes a la red.

I.2.2.- Objetivos Específicos:

- Investigar distintas plataformas de análisis de monitoreo compatibles con el protocolo sFlow.
- Identificar los dispositivos pertenecientes a la red interna a monitorear y su compatibilidad con el protocolo.
- Realizar una matriz comparativa entre las distintas plataformas de análisis compatibles con el protocolo sFlow.
- Desarrollar pruebas de conceptos de las plataformas de monitoreo propuestas previamente estudiadas.
- Aplicar la plataforma de monitoreo seleccionada para la red Interna en La Torre Mistral.

I.3.- Justificación

El desarrollo de este Trabajo de Grado pretende la implementación de un sistema de análisis de tráfico de red. La importancia de este sistema es conocer el origen y destino del tráfico interno en la red LAN, debido a la importancia de la información que se maneja internamente en la Torre Mistral, esto agregaría una medida de seguridad extra a la actual red, además de funcionar como un sistema de auditoría y una herramienta ideal para la detección y mitigación de las tormentas de broadcast.

I.4.- Alcances

El Trabajo de Grado se verá limitado a la implementación de un sistema de análisis para el tráfico interno en la red, exclusivamente de la Torre Mistral, tomando como término del Trabajo de Grado, cuando el sistema se encuentre operativo monitoreando el tráfico. Donde se estará analizando los protocolos TCP y UDP entre las conexiones que surjan entre los segmentos internos.

Con respecto a las acciones irregulares detectadas en el sistema por parte del personal, se tomarán correctivos y remediaciones, infundidos por la gerencia de IT.

I.5.- Limitaciones

Se busca la implementación de un proyecto por parte de la empresa SANFAR que tenga como fin la implementación de un sistema de análisis de tráfico de red, para conocer los protocolos de capa 2 a la capa 7 que se encuentran en la LAN de la Torre Mistral, invirtiendo el menor capital posible.

Es importante mencionar que en el desarrollo del Trabajo de Grado los estudiantes disponían con acceso directo al servidor virtualizado. Para efectuar cualquier cambio que afectara la red se debía consultar a la gerencia de IT para que ellos analizaran el nivel de afección y posteriormente ejecutaran las modificaciones en el switch Core de ser posible el cambio. Los estudiantes no tenían acceso al switch Core por motivos de seguridad y políticas internas de la empresa.

CAPÍTULO II

Marco Teórico

Este capítulo tiene como propósito definir los conceptos que permitan el entendimiento de los conocimientos que forman parte de este Trabajo de Grado. Se abordaron temas relacionados con los sistemas de monitoreo, análisis de tráfico y protocolos utilizados para identificar el rendimiento de red.

II.1.- Modelo de Referencia OSI

El modelo de Interconexión de Sistemas Abiertos, en inglés *Open Systems Interconnection* (OSI) fue desarrollado por la Organización Internacional de Normalización, en inglés International *Organization for Standardization* (ISO) y se formalizó en 1984. Proporcionó el primer marco que regula cómo debe enviarse la información a través de una red.

El modelo OSI, es un modelo de referencia de protocolos de red, diseñado para la interconexión de sistemas abiertos que consta de siete capas, cada una de las cuales corresponde a una función de la red:

Capa	Nombre	Función
7	Aplicación	Es la última capa del modelo OSI y proporciona la interfaz entre la aplicación del usuario y la red. Un navegador web y un cliente de correo electrónico son ejemplos de aplicaciones de usuario.
6	Presentación	La capa de presentación es la que controla el formato y la construcción de los datos del usuario para la capa de aplicación. Esto asegura que los datos de la aplicación emisora

		puedan ser entendidos por la aplicación receptora.
5	Sesión	Es la quinta capa del modelo OSI, cuya función es ser la responsable de establecer, mantener, y, en última instancia, finalizar las sesiones entre dispositivos. Si una sesión se pierde, esta capa puede intentar recuperar la sesión.
4	Transporte	La capa de transporte en realidad no envía datos, a pesar de su nombre. En cambio, es la responsable de la transferencia confiable de datos, asegurando que los datos lleguen a su destino sin errores y en orden.
3	Red	La capa de red es la encargada de controlar la comunicación en la red, y tiene dos funciones clave: • Direccionamiento lógico: proporciona una dirección única que identifica tanto el host y la red en la que se encuentra. • Enrutamiento: determina mejor camino a un destino particular red para que posteriormente sean enviados los datos desde el origen al destino.
2	Enlace de datos	Es la segunda capa del modelo OSI y se encarga de empaquetar los datos de las capas superiores en frames, con el fin de que los datos se puedan colocar en el medio físico de conexión. Este procedimiento de envasado es denominado proceso de encapsulado.

1	Física	Es la capa que controla la señalización y transferencia de bits en el medio físico. Y se encuentra estrechamente relacionada con la capa de enlace de datos, debido a que muchas tecnologías (como Ethernet) contienen funciones físicas y de enlace de datos.

Tabla 1. Referencia del Modelo OSI

Fuente: Microsoft Word - osi.doc (routeralley.com)

II.2.- Protocolos de Red

Los protocolos de red son aquellas normativas comunes que tiene como fin el entendimiento a través de la comunicación y permite el intercambio de información entre dispositivos.

II.3.- UDP

El UDP es el Protocolo de Datagramas de Usuario, en inglés *User Datagram Protocol*, encargado de enviar datagramas sin que previamente se establezca una conexión.

Postel. J (1980) describe este protocolo:

> El protocolo de Datagramas de Usuario (UDP) se define para hacer disponible un modo de datagrama de comunicación entre los paquetes de las computadoras en el entorno de un conjunto interconectado de redes informáticas. Este protocolo asume que el Protocolo de Internet (IP), se utiliza como el protocolo subyacente.

Este es un protocolo utilizado para transmisiones en donde se necesita que la información llegue a su destino de forma rápida, siendo una comunicación no

orientada a la conexión, es decir no se necesita que la información llegue de manera íntegra.

II.4.- TCP

Las siglas TCP es el Protocolo de Control de Transmisión, en inglés *Transmisión Control Protocol*, el mismo permite que se puedan enviar y recibir datos de forma simultánea, una vez establecida la conexión.

Además, Postel. J (1980) explica que dicho protocolo se enfoca en las transmisiones "tanto la entrega como la protección ante duplicados no se garantizan. Las aplicaciones que requieran de una entrega fiable y ordenada de secuencias de datos deberían utilizar el Protocolo de Control de Transmisión" (p.1).

II.5.- LAN

Una red de área local, en inglés *Local Area Network* (LAN) es descrita por Cisco (s.f.) como "un conjunto de dispositivos conectados entre sí en una ubicación física, como un edificio, una oficina o un hogar". La misma puede tener distintos tamaños y cantidades de usuarios, son empleadas tanto en entornos profesionales como domésticos.

II.6.- Telemetría

Dentro de las áreas de la ingeniería se encuentra la telemetría, está orientada a la medición de datos y/o unidades, la cual necesita de interfaces electrónicas que, tal y como explica Herrera. L (2006), estén "conectadas a través de alguna línea de transmisión ya sea un medio guiado o no guiado permiten enviar la información a un centro de gestión" (p.120).

II.7.- Monitoreo de Red

El análisis de tráfico en redes LAN, permite conocer diversos parámetros que indican el comportamiento de la red, con la finalidad de detectar inconvenientes que puedan afectar el uso de esta. Existen diversas herramientas destinadas a realizar este tipo de análisis y monitoreo a la red, utilizando una variedad de protocolos cada uno destinado a recolectar información específica de dispositivos y del tráfico de la red.

Asimismo, Cisco (s.f.) plantea que:

> El monitoreo de red proporciona la información necesaria para determinar, en tiempo real, si una red está funcionando de manera óptima. Con herramientas como el software de monitoreo de redes, los administradores pueden identificar deficiencias y optimizar la eficiencia de manera proactiva.

De igual forma, la primera etapa en el proceso de monitoreo de tráfico de red, consiste en definir los parámetros que se desean monitorear de la red, en función de las necesidades que existen en la misma. Para esto es necesario tener en cuenta todos y cada uno de los dispositivos que conforman la red como lo son firewall, servidores, switches, routers, entre otros. Debido a que el tráfico generado en la red, se desplazará a través de estos dispositivos, esto permite a los administradores encontrar fallos a través del monitoreo, como lo son las pérdidas de paquetes, alto consumo de ancho de banda o detectar un problema en específico.

Luego, una vez identificados los dispositivos claves de la red a monitorear y los parámetros de relevancia, se procede a definir cuáles son aquellos protocolo y/o plataformas que sean compatibles, que permitan obtener la información y que ésta sea presentada a través de la interfaz gráfica de una manera comprensiva y que facilite su evaluación.

II.8.- Tipos de Análisis de Tráfico

Al momento de llevar a cabo un análisis de tráfico de red, existen dos (2) enfoques diferentes, los cuales son: análisis de paquetes y análisis del flujo de tráfico de red. Ambos cumplen con el propósito de recopilar, analizar y presentar la información del tráfico de red, teniendo como diferencia la forma de recolección y extracción de datos.

Figura 1. Comparación de Tipos de Análisis de Tráfico

Fuente: Realizado por Autores

II.8.1.- Análisis de Paquetes o Captura de Paquetes

Un analizador de paquetes normalmente es referido como un protocolo de análisis, que describe el proceso de captura e interpretación de los datos en vivo que están recorriendo la red, otorgando un orden a los paquetes para entender qué está sucediendo en la red.

Análogamente, el análisis de paquetes normalmente se realiza mediante un programa ejecutado en un dispositivo perteneciente a la red que tiene como función capturar paquetes, este dispositivo recibe pasivamente todas las tramas de la capa de enlace de datos que lleguen hasta el adaptador de red del dispositivo, sin importar que vayan dirigidos a otro dispositivo.

Asimismo, algunos dispositivos de red, poseen la capacidad de realizar la inspección del tráfico entrante en sus puertos, mediante la configuración de un puerto espejo, el mismo se encarga de replicar todo el tráfico proveniente de un puerto del cual se requiera inspeccionar su tráfico.

Un analizador de paquetes permite:

- Entender las características de la red
- Saber quién está en la red
- Determinar quién o qué está utilizando el ancho de banda disponible
- Identificar picos en la red en periodos de tiempo
- Distinguir las actividades maliciosas en la red
- Hallar aplicaciones inseguras que están siendo usadas

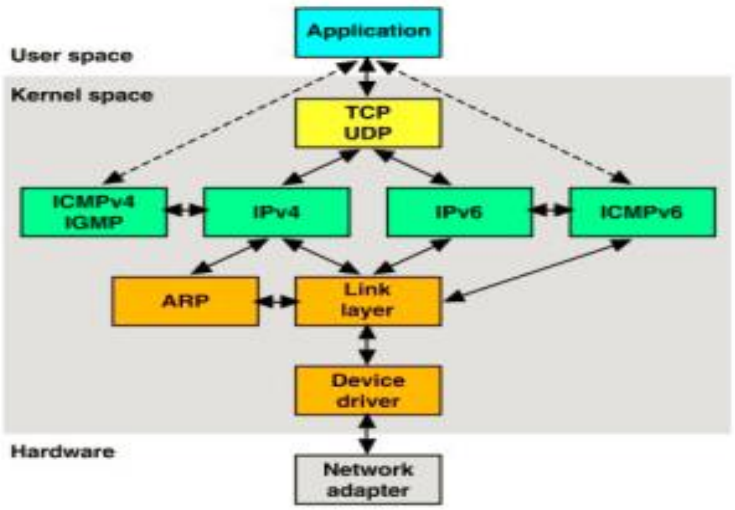

Figura 2. Flujo de paquetes

Fuente:

https://www.researchgate.net/publication/232625696_Network_Traffic_Analysis_and_Intrusion_Detection_Using_Packet_Sniffer

II.8.2.- Análisis de Flujo de Tráfico

En el análisis de flujo de tráfico se utilizan los dispositivos que pertenecen a la red para generar un flujo del tráfico, el mismo contiene información sobre los paquetes que pertenecen al tráfico. Al contrario del análisis de tráfico de paquetes, en el análisis de flujo no se observa la información completa del paquete, más bien se evalúan ciertas características en común que pudieran poseer los paquetes. Esta información será almacenada y posteriormente enviada a una plataforma que permita su análisis y visualización con base a las características definidas por el administrador de la red.

Un flujo es definido como la cantidad de paquetes que son recibidos en una interfaz.

A continuación se explica el esquema básico de cómo funciona un análisis de flujo de tráfico, el cual tiene 3 componentes que se pueden definir como:

- Exportador: componente encargado de recopilar la información y data del flujo de tráfico, para posteriormente ser enviada al colector
- Colector: es aquel que recibe la información del exportador y tiene como fin el almacenamiento y procesamiento de la data, dicha información luego es enviada al analizador.
- Analizador: es el último componente del esquema del análisis de flujo de tráfico, en el analizador se lleva a cabo el proceso de filtrado y análisis de los datos obtenidos del colector. Otra de las funciones, es encargarse de la visualización en forma gráfica de los datos recopilados.

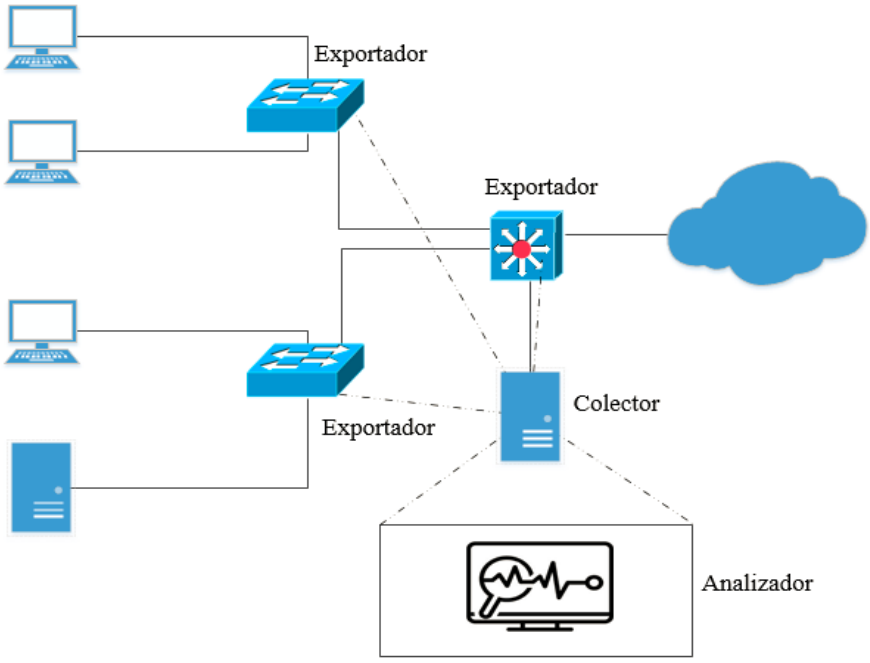

Figura 3. Esquema de Análisis de Flujo de Tráfico

Fuente: Realizado por Autores

En la actualidad, el análisis de flujo de tráfico se encuentra basado en una serie de protocolos, los cuales cumplen con las características necesarias para llevar a cabo los procesos que conlleva dicho análisis.

II.9.- NetFlow

NetFlow es un sistema de protocolo de red creado por Cisco, que recoge el tráfico de red a medida que éste entra o sale de la interfaz de un dispositivo de red. Los datos recopilados son enviados mediante UDP a un Colector. Netflow proporciona una visión más detallada de cómo se utiliza el ancho de banda y el tráfico de red.

La información recuperada por los paquetes IP utilizados por NetFlow de detallan seguidamente:

- IP Origen
- IP Destino

- Puerto Origen
- Puerto Destino
- Tipo de protocolo de capa 3
- Tipo de servicio
- Interfaz física de origen del tráfico

Adicionalmente NetFlow añade la siguiente información al flujo:

- Marcas de tiempo para entender la vida de un flujo, las cuales son útiles para calcular los paquetes y bytes por segundo
- Direcciones IP del siguiente salto, incluidos los sistemas autónomos de enrutamiento BGP (AS)
- Máscara de subred para las direcciones de origen y destino para calcular los prefijos
- Banderas TCP para examinar los handshakes TCP

Para la implementación de informes de datos del protocolo Netflow, es necesario realizar los siguientes procedimientos:

- El protocolo se configura para capturar flujos dentro de la memoria caché del dispositivo, conocida como memoria caché de NetFlow
- Configurar la exportación de NetFlow para enviar los flujos al colector
- Buscar en la memoria caché de NetFlow los flujos que han terminado y éstos se exportan al servidor del colector de NetFlow
- Agrupar entre 30 a 50 flujos para ser transportados, normalmente en formato UDP, al servidor del colector de NetFlow
- El software del colector NetFlow crea informes en tiempo real o históricos a partir de los datos obtenidos

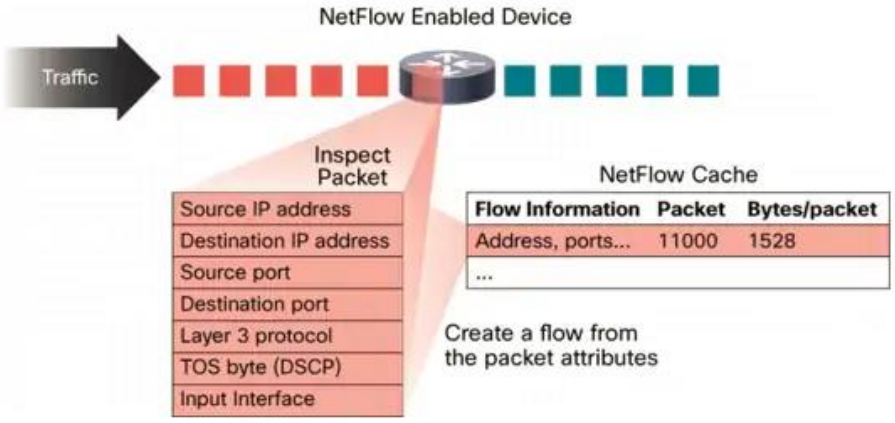

Figura 4. Análisis del Flujo con NetFlow

Fuente: https://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/ios-netflow/prod_white_paper0900aecd80406232.html

II.10.- IPFIX

El Protocolo de Internet para la Exportación de Información de Flujo, en inglés *Internet Protocol Flow Information Export* (IPFIX) es un protocolo creado por el Grupo de Trabajo de Ingeniería de Internet, en inglés *Internet Engineering Task Force* (IETF), como un estándar universal para la información de flujo, desarrollado usando la versión 9 del protocolo NetFlow. El estándar IPFIX determina cómo se exporta la información de flujo de IP y se envía a un recopilador o analizador IPFIX. El protocolo hace referencia a un flujo como una cantidad de paquetes observados en un período específico de tiempo y un número de porciones de propiedades.

Este protocolo envía constantemente datos a una herramienta de monitoreo. Estos datos incluyen información sobre tipos de tráfico como chats, transferencias de archivos, tráfico de correo electrónico, tráfico web y otro tráfico UDP y TCP. Extrayendo esta información de:

- Dirección IP

- Puerto Destino
- IP Destino
- IP Origen
- Protocolos (ICMP, OSPF, UDP, TCP, entre otros)
- Tipo de servicio (ToS)
- Punto de Código de Servicios Diferenciados (DSCP)

La data e información es enviada desde los routers y switches, a un colector del protocolo IPFIX y su analizador permite visualizar estos datos, lo que permite monitorear el tráfico de la red.

II.11.- sFlow

El protocolo sFlow está conformado de un Agente sFlow (embebido en un switch o router o en una sonda independiente) y un Colector sFlow. El uso de este sistema es explicado por Phaal. P & Lavine. M (2004) como "la arquitectura y técnicas de muestreo usadas en el sistema de monitoreo sFlow, que fueron diseñados para proporcionar monitoreo continuo del tráfico en todo el sitio" (p.2).

La implementación de sFlow es ideal debido a que cumple con una serie de requisitos claves para monitorear el tráfico interno de la red:

- Proporciona visibilidad del tráfico de la red, pudiendo visualizar las rutas que se encuentren activas y obtener información del flujo de paquetes desde la capa 2 hasta la capa 7 del modelo OSI

- Es un protocolo escalable y de bajo consumo de recursos, el cual permite analizar el tráfico de enlaces de hasta 10Gb/s sin afectar el rendimiento de los dispositivos pertenecientes a la red

- Es un estándar con más de 15 años en la industria publicada bajo el RFC 3176, encontrándose en una gran variedad de dispositivos de diferentes proveedores

- La configuración en los dispositivos en los cuales se requiere monitorear el tráfico, es de fácil implementación

Un sistema de monitoreo a través de sFlow según Peter Phaal, Sonia Pachen y Neil McKee (2001) consiste en un Agente sFlow (integrado en el dispositivo a monitorear) y un colector central de datos o analizador de sFlow. El Agente sFlow se basa en tecnología de muestreo para recopilar estadísticas de tráfico del dispositivo que está monitoreando. El Agente sFlow es un proceso que se ejecuta como parte del software de gestión de red dentro de un dispositivo, este se encuentra constantemente enviando información a la base de datos de sFlow para su posterior análisis y visualización en tiempo real del flujo de tráfico de la red.

El Agente sFlow usa la tecnología de muestreo para capturar la estadística de tráfico desde el dispositivo que monitorea. Los datagramas sFlow son usados para enviar las estadísticas de tráfico probadas a un Analizador sFlow para el análisis.

II.11.1.- Mecanismos de Muestreo

El Agente sFlow realiza el proceso de muestreo a través de dos procedimientos distintos: muestreo basado en flujos de paquetes conmutados o enrutados, y el muestreo basado en el tiempo de contadores.

II.11.1.1.- Flujos de Paquetes Conmutados o Enrutados

Cuando un paquete llega a una interfaz, el dispositivo debe tomar la decisión de descartar o no el paquete. El mecanismo de flujo de paquetes conmutados, actúa con un contador que va a ir en decremento a medida que pase un paquete, al llegar a cero el contador, toma una muestra. Con cada muestra que se realiza, aumenta en uno (1) la variable Total_Samples y con cada paquete que pasa a través de la interfaz del equipo, aumenta en uno (1) la variable de Total_Packet.

Al ser tomada una muestra se toma la cabecera del paquete o se extrae características del paquete, cada una de las muestras son enviadas al Agente sFlow para ser procesadas. Además de las características del paquete, también se toma el valor de las variables Total_Packets y Total_Samples al momento de realizar un muestreo.

II.11.1.2.- Muestreo de contadores

El mecanismo de muestreo de contadores funciona contabilizando la cantidad de contadores que se generan por cada paquete que ingresa y sale en una interfaz de red del dispositivo. Con esto, se medirá el volumen total del tráfico asociado a los dispositivos conectados a dicha interfaz, pero sin la posibilidad de distinguir los protocolos, puertos o servicios contenidos en dicho flujo.

II.11.2.- Transporte

El tráfico de información circula por toda la red sin encriptación desde el Agente sFlow hasta el Analizador sFlow, siendo poco seguro al estar la data en texto plano y teniendo gran vulnerabilidad ante los softwares analizadores de paquetes.

II.11.3.- Confidencialidad

El manejo del tráfico de información puede contener información confidencial, por lo que es recomendable limitar el grado de visualización, controlando la cantidad de bytes que van a ser tomados en el encabezado de los paquetes.

Los patrones de tráfico pueden ser conocidos por el decodificador de datagramas en el Colector sFlow, mostrando información de un individuo de la red, por lo que se debe tener asegurada la información que accede al colector.

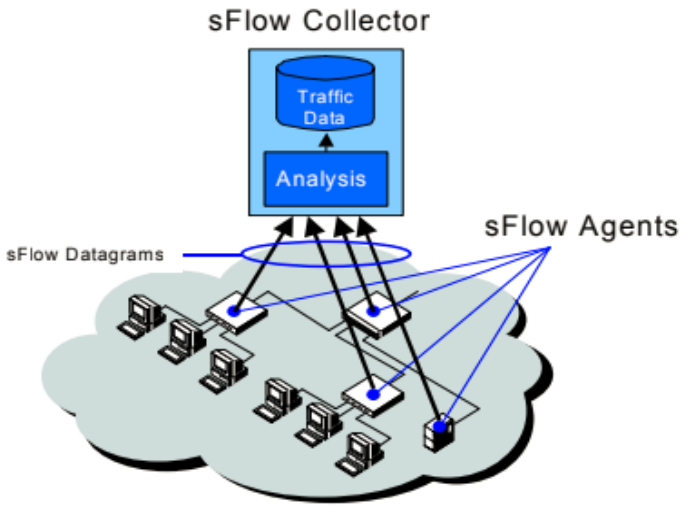

Figura 5. Análisis del Flujo con sFlow

Fuente: https://sflow.org/sFlowOverview.pdf

II.12.- sFlowTrend

La primera aplicación que se utilizó, para optar por la implementación de un sistema de monitoreo en la Torre Mistral fue sFlowTrend, que es un software libre de visualización y analítica que utiliza el protocolo sFlow, en el cual se plasma en forma de gráficos los datos de la red supervisada. Entre los gráficos más relevantes se encuentran las aplicaciones que utilizan más ancho de banda, el destino de los usuarios de la red, entre otros datos.

Dentro de sus características tiene como puerto escucha el 8087, una interfaz intuitiva para el usuario y un menú con amplias opciones que da resultados detallados de la red y los dispositivos que la componen.

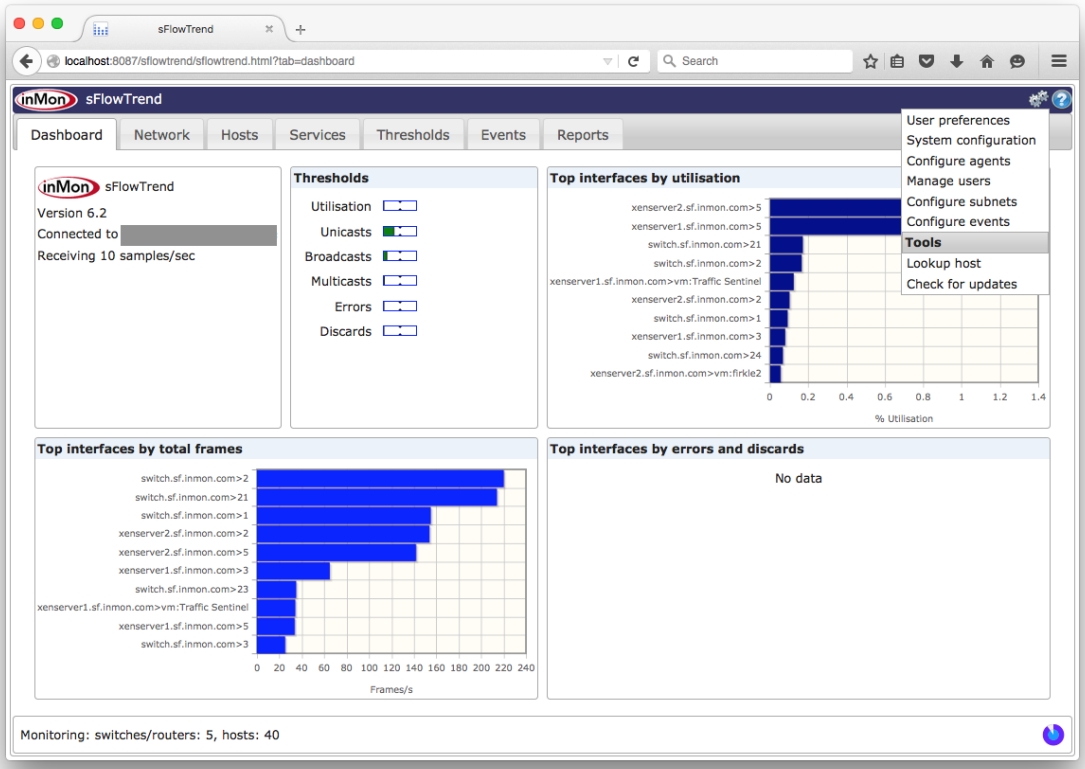

Figura 6. Interfaz de sFlowTrend

Fuente: https://inmon.com/products/sFlowTrendIntro-v6.0.php

II.13.- Query

Una vez explicadas las diversas herramientas que se usaron para realizar la monitorización de red interna de la Torre Mistral, se procede a explicar un término que se utiliza para realizar filtros en la información. Se necesitan palabras claves denominadas query, terminación que permite filtrar la información de los datos, para su posterior expresión en forma gráfica con alguna herramienta de visualización de la información específica que se requiere. En una misma gráfica se puede implementar más de un query a la vez si es requerido, con el fin de combinar más de un filtro en la gráfica.

Para el desarrollo del Trabajo de Grado el lenguaje en el que está basada la función query es en PromQl (*Prometheus Query Languaje*), permitiendo al usuario establecer las condiciones de los datos que necesite en tiempo real.

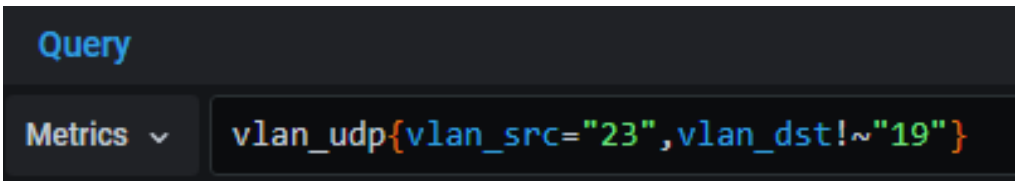

Figura 7. Query en Grafana

Fuente: Realizado por Autores

II.14.- Grafana

Es un software libre cuyo puerto de escucha por defecto es el 3000, este aplicativo se encarga de la visualización de los datos, plasmando la información requerida "traduciendo y transformando cualquiera de sus datos en paneles de control flexibles y versátiles" como lo muestra en su web Grafana Labs (s.f.). Para realizar los cambios de datos en los paneles, se deben realizar órdenes específicas llamadas query.

Esto permite la monitorización de la red, supervisando el tráfico originado, lo que genera que se disponga de la información de vital importancia como origen, destino, los bytes transmitidos, entre otros.

II.15.- Prometheus

Otra de las herramientas que se utiliza en conjunto con Grafana es Prometheus, teniendo como puerto por defecto el 9090, esta herramienta viene siendo explicada en su web Prometheus Authors (s.f.) como "un sistema de monitoreo de código abierto con un modelo de datos dimensional, un lenguaje de consulta flexible, una base de datos de series de tiempo eficiente y un enfoque de alerta moderno". El aplicativo Prometheus permite encargarse del registro de métricas en tiempo real con su propia base de datos, además de ser una aplicación de monitorización que se utiliza para

saber el estado y rendimiento en tiempo real de la red, a través de gráficos, permitiendo la consulta al usuario para que analice el estado de la red.

II.16.- Base de Datos

Una vez obtenida la información debe ser guardada en el apartado de base de datos que es descrita en la web de Microsoft (s.f.) como "una herramienta para recopilar y organizar información". Con el fin de obtener un conjunto de documentación estructurada, que posea hora, usuario, comando aplicados, entre otros, este tipo de documentación organizada en forma de registros son llamados logs. Esto sirve para tener un historial, y así guardar y buscar la información de manera cronológica de los eventos ocurridos en la red.

II.17.- Métrica

Una vez hablado del término query, también se debe mencionar al término métrica, estos dos conceptos van agrupados, ya que es el conjunto de parámetros que conforman el query, permitiendo al usuario filtrar funciones específicas en base al flujo de información que se encuentra en la red. Las funciones más destacadas serían:

- IP Origen
- IP Destino
- Puerto origen TCP
- Puerto destino TCP
- Puerto origen UDP
- Puerto destino UDP
- VLAN origen
- VLAN destino

II.18.- Elastic Stack

Este último apartado de herramientas es un grupo de aplicaciones de código abierto trabajando en conjunto con el fin de que los usuarios puedan buscar, analizar y visualizar datos de la red monitoreada. Esta agrupación de servicios anteriormente era llamado ELK Stack, explicado en su web Elasticsearch B.V. (s.f.) como "la sigla para tres proyectos open source: Elasticsearch, Logstash y Kibana". Posteriormente, se agregaría el aplicativo Beats que será explicado en este apartado.

La aplicación principal y más importante del conglomerado Elastic Stack es Elasticsearch, teniendo como puerto por defecto el 9200 y siendo definido en su página web Elasticsearch B.V. (s.f.) como "El motor de búsqueda open source, distribuido, RESTful basado en JSON. Fácil de usar, escalable y flexible, ganó notoriedad entre los usuarios y una empresa se formó a su alrededor". Elasticsearch fue desarrollado para el almacenamiento de diversos tipos de datos, como lo son los numéricos y textuales.

Para el apartado del proceso se utiliza la aplicación Logstash, definida en la página de Elasticsearch B.V. (s.f.) como "una pipeline de procesamiento de datos open source y del lado del servidor que te permite gestar datos de múltiples fuentes simultáneamente y enriquecerlos y transformarlos antes de que se indexen en Elasticsearch". Siendo Logstash el software encargado de la adición y análisis de datos para su posterior envío a Elasticsearch.

Con el paso del tiempo los usuarios de la comunidad ELK Stack, incidieron en la necesidad de realizar seguimientos en específico de un solo archivo, por lo cual en el 2015 la empresa Elastic NV introdujo Beats, explicado en su página oficial Elasticsearch B.V. (s.f.) como "familia de agentes de datos de propósito único y livianos en la ecuación del ELK Stack".

Luego de haber recolectado y procesado la información, se procedió a la recepción de la información para el usuario de forma gráfica, con el fin de facilitar la

interpretación de la información recabada. A partir de este instante se encarga del proceso Kibana, teniendo como puerto por defecto el 5601 y siendo definido en la página oficial Elasticsearch B.V. (s.f.) como "la herramienta de visualización flexible", encargada de administrar la interfaz gráfica a través de la creación de tableros dinámicos, informes, gráficos, entre otros para el mejor entendimiento de los datos por medio de la visualización.

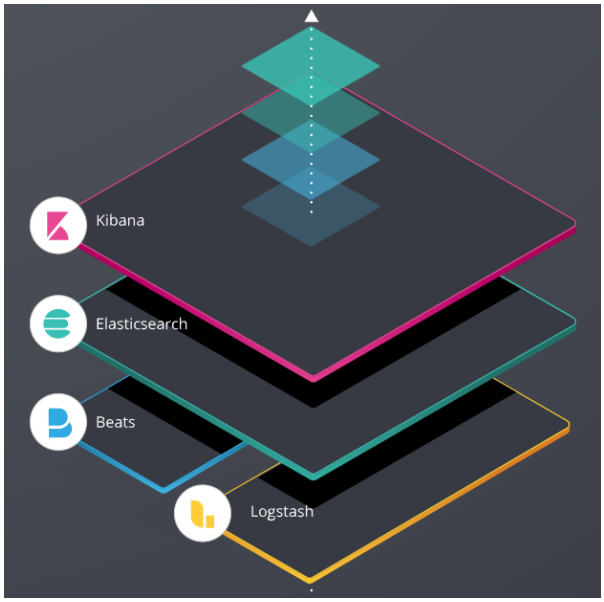

Figura 8. Estructura de Elastic Stack

Fuente: https://www.elastic.co/es/what-is/elk-stack

CAPÍTULO III

Marco Metodológico

En el capítulo se describe la metodología aplicada para el desarrollo del trabajo especial de grado, en conjunto con los distintos procedimientos a realizar teniendo como fin el análisis de tráfico de red.

III.1.- Tipo de Investigación y Metodología Empleada

El trabajo especial de grado para optar al grado académico de Ingeniería en Telecomunicaciones ante la Universidad Católica Andrés Bello se enmarca, de acuerdo con la Universidad Pedagógica Libertador UPEL (2006), en un Proyecto Descriptivo. Sabiendo que, en este sentido, la UPEL define el proyecto descriptivo como un estudio "que consiste en la caracterización de un hecho, fenómeno, individuo o grupo con el fin de establecer su estructura o comportamiento".

III.2.- Investigación Oficial

Se llevó a cabo el estudio detallado del funcionamiento de los protocolos de análisis de flujo, sus diferencias y aplicaciones, enfocado al desarrollo del funcionamiento del protocolo sFlow.

Además, se realizó la investigación de distintas plataformas de análisis compatible con el protocolo, de dicha investigación se tomó en cuenta las plataformas que requieren licenciamiento pago y alternativas open source.

III.3.- Identificación de los Dispositivos Pertenecientes a la Red Interna a Monitorear

Durante el proceso de levantamiento de información se recopiló la data del funcionamiento de la red interna de la empresa SANFAR, dicho levantamiento incluye una lista de equipos pertenecientes a la red, modelos de los dispositivos, nombre del equipo, direccionamiento lógico y las VLAN a monitorear de la red.

VLAN ID	Nombre
1	DEFAULT_VLAN
2	Vlan-VoIP
14	DMZ4
15	DMZ3
23	Vlan-Administracion
24	VLAN Servidores
26	red_privada_virtuales
28	Vlan-Impresion
30	Vlan-Vigilancia
31	FrontEnd_Produccion
32	FrontEnd_Desarrollo_QA
33	BackEnd
34	Vlan-VoIP-Xorcom
36	Vlan-VDC
40	ADM_EQUIPOS_ORACLE

41	SERVICIOS_ORACLE
42	ADM_VIRTUAL_ORACLE
43	Oracle_QA
44	Oracle_DES
45	Oracle_PRD
100	Vlan-PBMZTZ
172	Vlan-VoIP-Vonage
176	VLAN_Wifi_Mistral-DG
177	Vlan-Wifi-Guest
178	Vlan-Wifi-VIP
179	Vlan-Wifi-Tecnologia
180	Vlan_Wifi_Mistral-Corpo
181	Vlan-TM-Wifi-PDA
182	Vlan_Wifi-Mercadeo
183	Vlan_Wifi-Avanzada
200	Vlan-P1P2P3
210	VLAN-Clientes-P3
500	Vlan-P4P5P6
700	Vlan-P7P8
710	VLAN-SAP-Trainning
737	VLAN-Empresas-Terceros
1000	VLAN-InterWAN

4000	765zl_inter
4001	765zl_lan
4002	Vlan-Contingencia-SSLVPN

Tabla 2. VLANs de Torre Mistral

Fuente: Realizado por los Autores

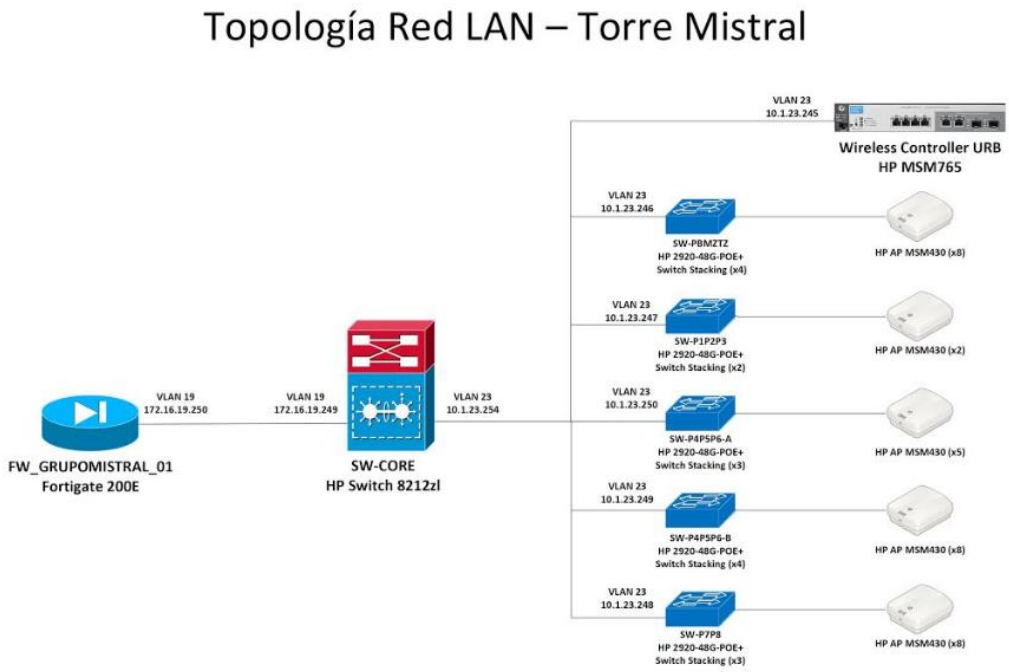

Figura 9. Topología de la Red Interna de la Torre Mistral

Fuente: Realizado por Autores

Luego de obtener la lista de los dispositivos de red, pertenecientes a la red de la Torre Mistral, se realizó una búsqueda en las hojas de datos de cada dispositivo, para determinar su compatibilidad con protocolo sFlow.

III.3.1.- Core

El switch core es el núcleo de las redes empresariales siendo la capa superior en la jerarquía de los switches cuya función principal es ser el troncal para el acceso a la LAN y entre sus características destacadas están, el enrutamiento y conmutación, funcionamiento de las VLANs de capa 2 y 3, ACL para la seguridad de la red interna, default Gateway de la red, reenvió de paquetes a altas velocidad, entre otros. El switch core HP 8200 zl es definido según Hewlett Packard Enterprise Development LP (s.f.) como:

> Alto rendimiento, escalabilidad y una amplia gama de funciones en una plataforma de alta disponibilidad que reduce drásticamente la complejidad. Esta serie proporciona tecnología de plataforma, software de sistema, gestión de sistemas, integración de aplicaciones, integración cableada e inalámbrica, seguridad de red y soporte que son comunes a los conmutadores modulares y de puerto fijo de HP.

Según las hojas de datos del switch core HP 8212 zl es compatible con el protocolo sFlow.

III.3.2.- Switch

El switch es un dispositivo que tiene como función la interconexión de varios equipos pertenecientes a la misma red local (LAN), teniendo entre sus características más relevantes, la segmentación de la red a través de las VLANs, conexión entre varios switches sin crear bucles debido al STP, poseer numerosos puertos de conexión, entre otros. Siendo definido el modelo HP 2920 en la página web de Intercompras Comercio Electrónico SA de CV (s.f.), como:

> La serie de switches HP 2920 consta de cinco switches: Los switches HP 2920-24G y 2920-24G-PoE+ con 24 puertos 10/100/1000 y los HP 2920-48G y 2920-48G-PoE+ y 2920-48G 740W PoE+ con 48 puertos 10/100/1000. Cada switch dispone de cuatro puertos de doble función para conectividad 10/100/1000 o SFP. Además, la serie de switches 2920 admite hasta cuatro enlaces opcionales de 10 puertos Gigabit Ethernet (SFP+ y/o 10GBASE-T), así como un módulo dos puertos stack. Estas opciones le proporcionan apilamiento y enlaces ascendentes flexibles y fáciles de implementar. Junto con el enrutamiento estático RIP, unas sólidas prestaciones de seguridad y gestión profesionales, garantía de por vida gratuita y actualizaciones de software gratuitas, la serie de switches HP 2920 es una solución económica y ampliable para clientes que están creando redes de alto rendimiento.

Según las hojas de datos de los switches HP 2920, son compatibles con el protocolo sFlow.

III.3.3.- AP

El punto de acceso, en inglés *access point* (AP), es un dispositivo de red que permite que los equipos con calidad de conexión inalámbrica se vinculen a una red. Teniendo como principal característica la movilidad de los equipos al poder prescindir del cableado para la conexión a la red. En Intercompras Comercio Electrónico SA de CV (s.f.) se define a la serie 802.11n de doble radio como:

> Soluciones de red de alto rendimiento. La arquitectura de controlador mejorada se adapta a IEEE 802.11n, sin necesidad de sustituir el controlador. El controlador

> proporciona una gestión avanzada de los recursos de radio (RRM), incluyendo el equilibrio de la carga del cliente y la mitigación de las interferencias. Los controladores inalámbricos de HP admiten una capacidad de itinerancia rápida - Una característica importante, especialmente para las comunicaciones VoIP.

Según las hojas de datos de los 802.11n no son compatibles con el protocolo sFlow.

III.3.4.- WLC

El controlador de LAN inalámbrica, en inglés *wireless LAN controller* (WLC) es el dispositivo de red que gestiona los puntos de acceso (AP) a la red inalámbrica y permite que los dispositivos inalámbricos se conecten a la red. El WLC simplifica el monitoreo de los puntos de acceso. La compañía Hewlett-Packard Development Company (2004) explica que WLC trabajan:

> Al unísono con los puntos de acceso HP MSM y Unified, la serie de controladores HP MSM preparados para IEEE 802.11ac ofrece una solución de red de alto rendimiento. La arquitectura de controlador mejorada se adapta a los nuevos estándares WLAN sin necesidad de sustituir el controlador. Los controladores MSM proporcionan una gestión avanzada de recursos de radio (RRM), que incluye el equilibrio de la carga de clientes y la mitigación de interferencias. Los controladores inalámbricos MSM también admiten una capacidad de itinerancia rápida. La seguridad inalámbrica es completa, con IDS inalámbrico integrado y compatibilidad con servidores de autenticación, autorización y contabilidad (AAA) internos

y externos; un cortafuegos con estado integrado; asignación de VLAN por usuario; y autenticación.

Según las hojas de datos del WLC, no es compatible con el protocolo sFlow.

III.4.- Pruebas de Conceptos

Para esta fase se realizó un análisis de la red en la cual se hizo el Trabajo de grado, se extrajo información de la clasificación de los equipos que conforman la red, las VLANs pertenecientes a la empresa, plataformas de monitoreo compatibles, entre otros. Una vez adquirida la información se procedió con las pruebas de concepto, comparando en un entorno controlado las plataformas que se estudiaron, sFlowTrend, Elastic Stack y Grafana en conjunto a Prometheus.

Se evaluó la recolección de los datos de las distintas plataformas, considerando los problemas que se tuvieron con la implementación de sFlowTrend y los aplicativos de Elastic Stack. Dando como resultado la selección de Grafana junto a Prometheus para que se implementen como plataforma de monitoreo.

Una vez escogida la plataforma, se adecuó a la red interna, estudiando el lenguaje de los query con el fin de que extraiga la información de IP origen, IP destino, VLAN origen, VLAN destino, entre otros datos del switch core. Posteriormente, se establecieron las tablas y gráficos que generarían los dashboards ideales para el monitorear, propiciando como resultado información útil para el equipo de IT.

Finalizando esta etapa se realiza el pase a producción, ya teniendo la plataforma seleccionada, implementada y ajustada a las necesidades del equipo de IT, se procede transferir el producto a los administradores de red, con el objetivo de que utilicen el sistema para el fin con el que fue creado, monitorear la red.

III.5.- Documentación Final

Una vez se concluyó y realizó el análisis de las pruebas de conceptos, se procedió a la documentación del capítulo de Desarrollo del Trabajo de Grado, el cual contiene la explicación en detalle del proceso que se siguió para realizar todas las actividades ejecutadas con el fin de obtener la implementación del proyecto.

CAPÍTULO IV

Desarrollo

El presente capítulo comprende cada una de las actividades realizadas en las distintas fases del Trabajo de Grado mencionadas en el Marco Metodológico para el desarrollo del proyecto.

IV.1.- Fase Investigativa

En esta fase se procedió a examinar las plataformas gratuitas compatibles con el protocolo sFlow. Se escogieron tres (3) plataformas para desarrollar en un servidor virtualizado y posteriormente comparar los pros y contras de cada una de estas plataformas, con el fin de implementar el sistema de monitoreo para el equipo de IT. Dichas plataformas que se investigaron fueron:

- Grafana, integrado con Prometheus
- sFlowTrend
- Elastic Stack (Elasticsearch, Logstash, Kibana y Beats)

Además se realizó un cuadro comparativo, representando en una tabla los datos representativos de las tres (3) plataformas de monitoreo seleccionadas. A continuación se observa la tabla con las características más relevantes:

Plataforma	Características
Grafana y Prometheus	• Visualización interactiva con paneles dinámicos • Creación de alertas y notificaciones • Creación de métricas personalizadas • Recolección centralizada de la base de datos • Visualización centralizada de todos los gráficos y tablas creados

sFlowTrend	• Comprensión rápida e intuitiva por parte del administrador que está usando la red y qué están realizando los host • Cumplimiento de las políticas empresariales con el fin de cumplir el correcto funcionamiento del uso de la red • Se identifica pronta y precisamente cualquier problema con el fin de obtener la causa del tráfico irregular • Supervisión de los parámetros de rendimiento con mayor importancia del host. Por ejemplo: utilización de la CPU y la memoria • Se generan informes con respecto al desempeño actual e histórico
Elastic Stack	• Escalabilidad • Fácil administración de gráficos y tablas • Seguridad • Monitorización orientado al comportamiento de redes • Integración entre plataformas del mismo conglomerado • Integración de diversos lenguajes de programación para la creación de los query • Introducción automática e intuitiva a todas las aplicaciones del conjunto

Tabla 3. Comparativa de Plataformas de Monitoreo

Fuente: Realizado por los Autores

IV.2.- Fase de Implementación

En la fase anterior al haberse investigado las plataformas de monitoreo, se procedió a desarrollar las pruebas de conceptos, utilizando un servidor virtualizado

para posteriormente observar el funcionamiento del sistema de análisis mediante el protocolo sFlow.

Para este apartado se contó con la colaboración del equipo de IT, el cual entregó el servidor virtualizado corporativo con las siguientes características presentes, para realizar las pruebas de conceptos:

- Sistema Operativo: Debian
- RAM: 8Gb
- Disco: 320Gb

Lo primero que se realizó fue instalar Java 1.8+, debido a que es un requisito para la aplicación sFlow-RT que será explicada más adelante en este mismo capítulo.

Descarga del OpenJDF 8:

```
#apt install openjdk-8-jdk
```

Certificación de la versión de Java:

```
#java -version
```

Luego se procedió a la instalación de sFlow-rt, software que permite recibir el flujo continuo de los agentes sFlow integrados en el switch core. Para ello implementamos en el modo súper usuario (#sudo su), los siguientes comandos:

Descarga desde la página web de Inmon:

```
#wget https://inmon.com/products/sFlow-RT/sflow-rt.tar.gz
```

Desempaquetado y descomprensión del archivo:

```
#tar -xvzf sflow-rt.tar.gz
```

Ejecución del archivo:

```
#./sflow-rt/start.sh
```

Permitir que el servicio inicie en el arranque del servidor:

```
#systemctl enable sflow-rt
```

Una vez implementado sFlow-rt, se configuró en el puerto 8080 y se procedió a realizar la primera prueba de concepto, la cual fue con el aplicativo de Grafana, junto al software Prometheus.

Lo primero que se realizó fue ingresar en la página oficial de Prometheus y en el apartado de descargas, buscamos el archivo compatible con el sistema operativo del servidor y se procede con la instalación. Es menester destacar, que siempre se debe estar en el modo súper usuario para efectuar todos los comandos a continuación:

Descarga de Prometheus:

```
#wget
https://github.com/prometheus/prometheus/releases/download/v2.28.1/prometheus
-2.28.1.linux-amd64.tar.gz
```

Descomprimir el archivo:

```
#tar –xvf prometheus-2.28.1.linux-amd64.tar.gz
```

Iniciar Prometheus como servicio:

```
#service prometheus start
```

Permitir que el servicio inicie en el arranque del servidor:

```
#systemctl enable prometheus
```

Finalizando la instalación del aplicativo Prometheus, se configuró en el puerto 9090 en el servidor virtual.

Luego se instaló el aplicativo Grafana directamente desde su página web oficial, teniendo en cuenta que la versión debe ser compatible con el sistema operativo Debian. Para los siguientes comandos es necesario estar en el modo de súper usuario:

Descarga de Grafana:

```
#wget https://s3-us-west-2.amazonaws.com/grafana-releases/release/grafana_5.2.3_amd64.deb
```

Instalación de paqueterías en Debian:

```
#dpkg -i grafana_5.2.3_amd64.deb
```

Actualización de la paquetería:

```
#apt update
```

Instalación de Grafana:

```
#apt install grafana
```

Iniciar Grafana como servicio:

```
# systemctl start grafana
```

Permitir que el servicio inicie con arranque del servidor:

```
#systemctl enable grafana
```

Culminando la primera plataforma de monitoreo con la configuración de Grafana en el puerto 3000 en el servidor que se asignó por parte del equipo de IT.

Para la segunda opción de pruebas de conceptos se implementó el Elastic Stack, el primer componente que se instaló y se configuró fue Elasticsearch, implementando todos los comandos en modo súper usuario:

Descarga de Elasticsearch:

```
#wget https://artifacts.elastic.co/downloads/elasticsearch/elasticsearch-7.13.3-amd64.deb
```

Identificación de integridad del fichero:

```
# shasum -a 512 -c elasticsearch-7.13.3-amd64.deb.sha512
```

Instalación de paqueterías en Debian:

```
#dpkg -i elasticsearch-7.13.3-amd64.deb
```

Instalar Elasticsearch:

```
#apt install elasticsearch
```

Iniciar Elasticsearch como servicio:

```
#systemctl start elasticsearch
```

Permitir que el servicio inicie con arranque del servidor:

```
#systemctl enable elasticsearch
```

Para finalizar con la implementación del software de Elasticsearch se configuró en el puerto 9200 del servidor virtual.

Luego se procedió con el aplicativo de visualización Kibana, implementando en modo súper usuario los siguientes comandos:

Descarga de Kibana:

```
#wget https://artifacts.elastic.co/downloads/kibana/kibana-7.13.3-amd64.deb
```

Identificación de integridad del fichero:

```
# shasum -a 512 -c kibana-7.13.3-amd64.deb.sha512
```

Instalación de paqueterías en Debian:

```
#dpkg -i kibana-7.13.3-amd64.deb
```

Instalar Kibana:

```
#apt install kibana
```

Iniciar Kibana como servicio:

```
#systemctl start kibana
```

Permitir que el servicio inicie con arranque del servidor:

```
#systemctl enable kibana
```

Kibana se le asignó el puerto 5601 en el servidor virtual, con este procedimiento se finalizó la instalación del software.

Una vez instalado el Elasticsearch y el Kibana, se observó que la memoria RAM del servidor se encontraba al 100%, por lo que no se pudo continuar con la instalación de los otros dos (2) aplicativos del Elastic Stack, Logstash y Beats. A continuación se observa el estado de la memoria RAM:

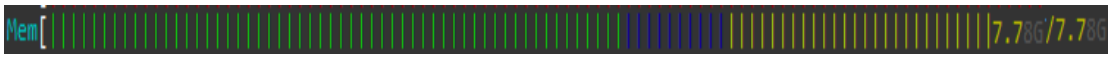

Figura 10. Memoria RAM al 100%

Fuente: Realizado por Autores

Por último se implementó el aplicativo sFlowTrend, para ello fue necesario implementar los comandos en modo súper usuario:

Descarga de sFlowTrend:

```
#wget https://github.com/sflow/host-sflow/releases/download/v2.0.25-3/hsflowd_amd64.deb
```

Instalación de paqueterías en Debian:

```
#dpkg -i hsflowd-ubuntu18_2.0.25-3_amd64.deb
```

Instalar sFlowTrend:

```
#apt install sFlowTrend
```

Iniciar sFlowTrend como servicio:

```
#systemctl start sFlowTrend
```

Permitir que el servicio inicie con arranque del servidor:

```
#systemctl enable sFlowTrend
```

Una vez implementado el aplicativo sFlowTrend en el puerto 8087, se observó que el mismo tiene capacidad de almacenamiento por 24 horas, por lo que se descartó para el desarrollo como plataforma de monitoreo de la red interna de la Torre Mistral, al poseer un período de almacenamiento en tiempo muy limitado.

Esto causaría un impedimento en la verificación de los sucesos en la red en un espacio de tiempo amplio como días o meses.

IV.3.- Fase de Acoplamiento

Luego de sucesivas mesas técnicas con los especialistas IT de Mistral, se dilucidaron los puntos y las necesidades en cuanto a el monitoreo específico de cada protocolo, tipo de gráfico y demás necesidades requeridas de la herramienta de monitoreo. Una vez se instalaron las tres (3) opciones seleccionadas con antelación, se procedió al diseño del aplicativo de Grafana con Prometheus, debido a que el Elastic Stack (Elasticsearch, Kibana, Logstash y Beats) requería más recursos de memoria RAM, con los cuales no se disponía. Y sFlowTrend poseía una base de datos limitada en tiempo, lo cual hacía inviable a la aplicación al momento de revisar las conexiones realizadas en la red interna de la Torre Mistral.

Lo primero que se realizó fue implementar a Prometheus, como una base de datos cuya duración es de 180 días, el cual siempre transmite tráfico a Grafana. Este último aplicativo se utilizó para la visualización a través de gráficos y tablas que permitiese entender al usuario lo que está sucediendo en la red.

Para tener un control más detallado de lo ocurrido en la red interna de la Torre Mistral, se realizaron un total de 40 dashboards, cuyos nombres son “Mistral VLAN 'número de la VLAN '”.

Al ser Grafana el aplicativo de visualización, se le asignó a los especialistas de IT usuario y contraseña con privilegios de administrador.

CAPÍTULO V

Resultados

Para el presente capítulo se procede a exponer los resultados del proyecto conseguidos que se utilizaron en el capítulo anterior del Trabajo de Grado, siendo empleado el procedimiento por etapas como es señalado en el capítulo III.

V.1.- Recopilación de Información Propia del Trabajo De Grado

Como consecuencia de la etapa investigativa se efectuó el capítulo II del presente Trabajo de Grado, Marco Teórico, en el cual se organizan y explican los fundamentos de las bases teóricas trabajados para lograr obtener la plataforma que desempeñará la función de sistema de análisis de monitoreo, concediendo poner en manifiesto los siguientes puntos:

- La seguridad cibernética de las empresas es de alta prioridad debido a la valiosa información que posee tanto de la misma empresa como de sus trabajadores, esta situación encamina a tener un método de seguridad de resguardo a través de un sistema que esté en constante revisión del uso interno de la red, permitiendo tener conocimiento en todo momento de lo sucedido entre los equipos residentes en la empresa
- El protocolo sFlow es una herramienta de gran utilidad para realizar monitoreo en la red a través del análisis de paquetes, permitiendo que su versatilidad realice captura del flujo de tráfico en la red de manera perpetua, analizando los parámetros y consumiendo la mínima cantidad de consumos, convirtiendo en un software óptimo

La plataforma de monitoreo Grafana y Prometheus se consolidaron para la generación del producto final del proyecto, debido a la compaginación entre los dos

sistemas, presentación de datos, interfaz intuitiva y administración eficientes de recursos.

Para alcanzar la culminación del Trabajo de Grado se realizó una investigación en páginas webs, foros, libros, entre otros relacionados al ámbito de las redes de telecomunicaciones, protocolos de monitoreo, sistemas de monitoreo y programación en Debian.

V.2.- Pruebas de Conceptos

Una vez obtenidos los resultados de las implementaciones de las distintas herramientas se excluyeron las plataformas de sFlowTrend y Elastic Stack, implementándose Grafana en conjunto con Prometheus.

Las plataformas que se excluyeron presentaron un inconveniente, con el apartado de sFlowTrend, una vez implementado el aplicativo correctamente, se observó que sólo contaba con 24 horas de almacenamiento de la información de los registros. Esta situación impedía al equipo de IT conseguir un registro detallado en un período prolongado de tiempo.

Con respecto al conjunto de aplicativos de Elastic Stack, se realizó la instalación de Elasticsearch y Kibana con los comandos aplicados en el capítulo anterior, luego de la implementación se contempló que la memoria RAM del servidor virtual estaba en 100%, consumiéndose todos los recursos del mismo y faltando la instalación de Logstash y Beats. Esta situación impactó en la continuidad de la instalación al no permitir progresar debido al excesivo consumo de recursos exigidos por el conjunto de aplicaciones Elastic Stack.

Por otro lado, al implementar Grafana junto a Prometheus, se contempló que los aplicativos podían correr con normalidad sin consumir excesivamente alguno de los recursos del servidor. Además, que las aplicaciones se asociaban de manera adecuada, en Grafana la interfaz es intuitiva y se visualizan las gráficas junto a las

tablas de manera que el usuario evidencia en el menú cada una de las VLAN de la red que se encuentran monitoreadas.

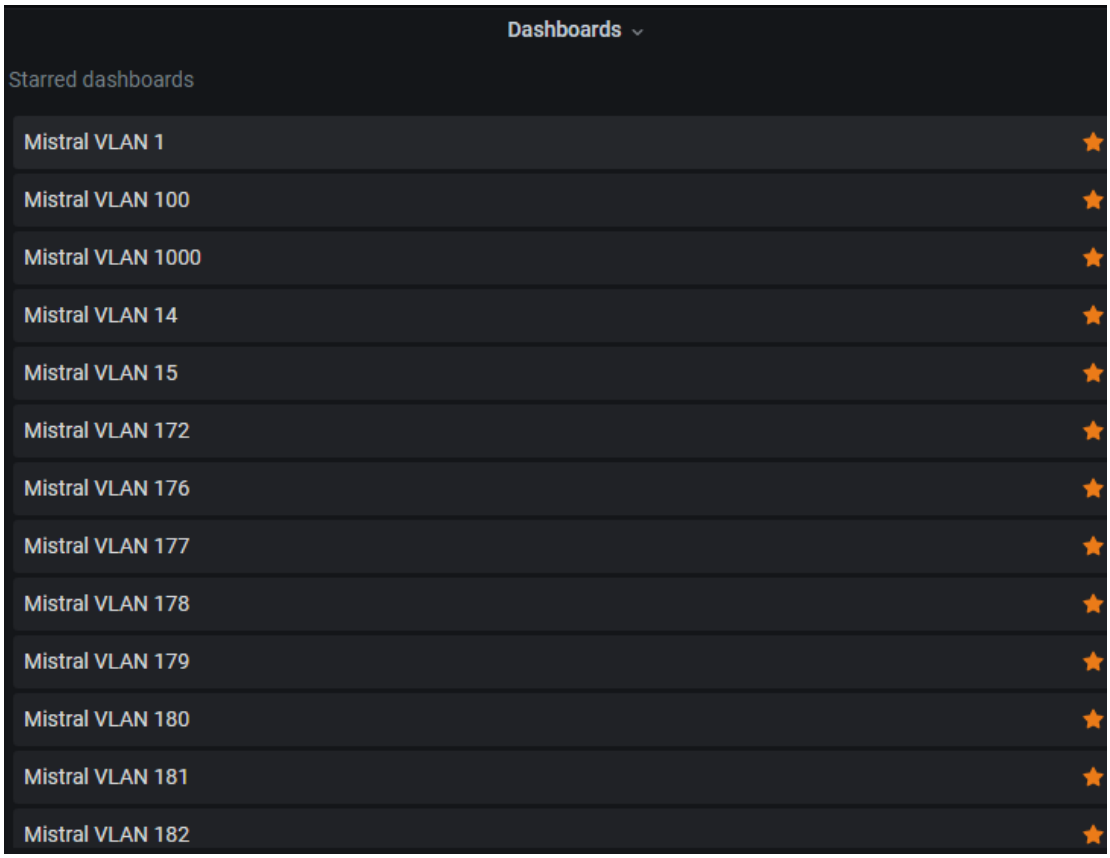

Figura 11. Interfaz de Grafana

Fuente: Realizado por Autores.

V.3.- Plataforma Implementada

La herramienta utilizada para el sistema de monitoreo de la red interna de la Torre Mistral fue Grafana junto a Prometheus, en el cual se dimensionaron las VLANs 1, 2, 14, 15, 23, 24, 26, 28, 30, 31, 32, 33, 34, 36, 40, 41, 42, 43, 44, 45, 100, 172, 176, 177, 178, 179, 180, 181, 182, 183, 200, 210, 500, 700, 710, 737, 1000, 4000, 4001, 4002 que poseen las características de dashboards, tablas, gráficos y parámetros los cuales son:

Dashboard	Tablas y Gráficos	Parámetros
Mistral VLAN 'número de la VLAN '	Tráfico TCP (Origen | Destino)	○ IP Origen ○ Puerto TCP de Origen ○ VLAN de Origen ○ IP de Destino ○ Puerto TCP de Destino ○ VLAN de destino
	Tráfico UDP (Origen | Destino)	○ IP Origen ○ Puerto UDP de Origen ○ VLAN de Origen ○ IP Destino ○ Puerto UDP de Destino ○ VLAN de destino
	Puerto Destino TCP	○ Puerto Destino TCP
	Puerto Destino UDP	○ Puerto Destino UDP
	Tabla TCP	○ Fecha ○ IP de Origen ○ IP Destino ○ Puerto TCP Origen ○ VLAN Origen ○ Puerto TCP Destino ○ VLAN Destino ○ Tráfico (en bytes)
	Tabla UDP	○ Fecha ○ IP de Origen ○ IP Destino

		○ Puerto UDP Origen ○ VLAN Origen ○ Puerto UDP Destino ○ VLAN Destino ○ Tráfico (en bytes)

Tabla 4. Conformación de los Dashboards

Fuente: Realizado por Autores

V.4.- Gráfico

- Tráfico TCP (Origen | Destino): este esquema entrega la información del tráfico TCP de la VLAN del dashboard seleccionado. Permitiendo tener una perspectiva visual de los datos, de esta forma, el equipo de IT monitorea el tráfico de la red interna de la Torre Mistral, pudiendo detectar cualquier anomalía y reportarla de manera pronta y efectiva. Los parámetros que componen esta gráfica son:
    - IP Origen
    - Puerto TCP de Origen
    - VLAN de Origen
    - IP Destino
    - Puerto TCP de Destino
    - VLAN de destino

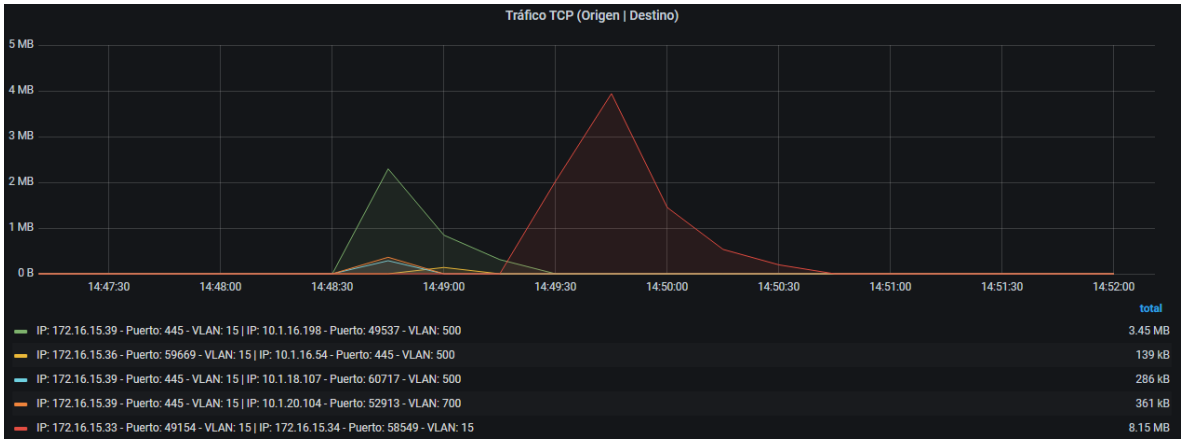

Figura 12. Gráfico de Tráfico TCP (Origen | Destino)

Fuente: Fuente: Realizado por los Autores

- Tráfico UDP (Origen | Destino): este esquema entrega la información del tráfico UDP de la VLAN del dashboard seleccionado. Permitiendo tener una perspectiva visual de los datos, de esta forma, el equipo de IT monitorea el tráfico de la red interna de la Torre Mistral, pudiendo detectar cualquier anomalía y reportarla de manera pronta y efectiva. Los parámetros que componen esta gráfica son:
    - IP Origen
    - Puerto UDP de Origen
    - VLAN de Origen
    - IP Destino
    - Puerto UDP de Destino
    - VLAN de destino

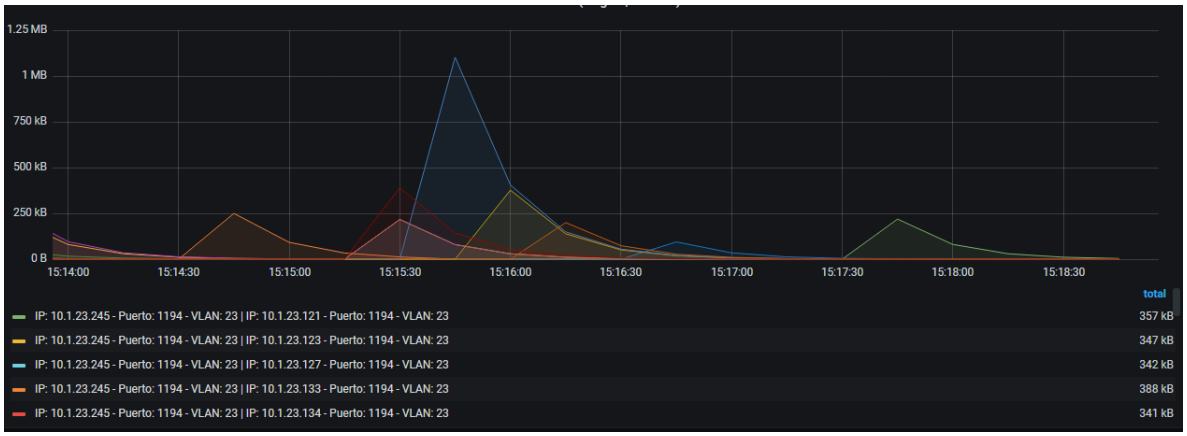

Figura 13. Gráfico de Tráfico UDP (Origen | Destino)

Fuente: Fuente: Realizado por los Autores

- Puerto Destino TCP: este esquema entrega la información del puerto destino TCP de la VLAN del dashboard seleccionado. Permitiendo tener una visual de gráfica pastel, de esta forma, el equipo de IT monitorea los puertos destino TCP del tráfico de la red interna de la Torre Mistral. El parámetro que componen esta gráfica es:
    - Puerto Destino TCP

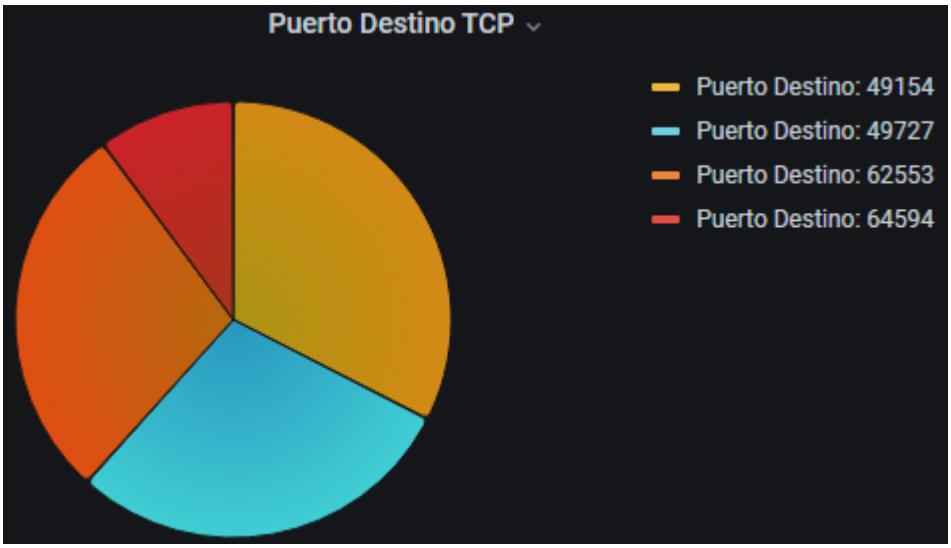

Figura 14. Gráfico de Puerto Destino TCP

Fuente: Fuente: Realizado por los Autores

- Puerto Destino UDP: este esquema entrega la información del puerto destino UDP de la VLAN del dashboard seleccionado. Permitiendo tener una visual de gráfica pastel, de esta forma, el equipo de IT monitorea los puertos destino TCP del tráfico de la red interna de la Torre Mistral. El parámetro que componen esta gráfica es:
    - Puerto Destino UDP

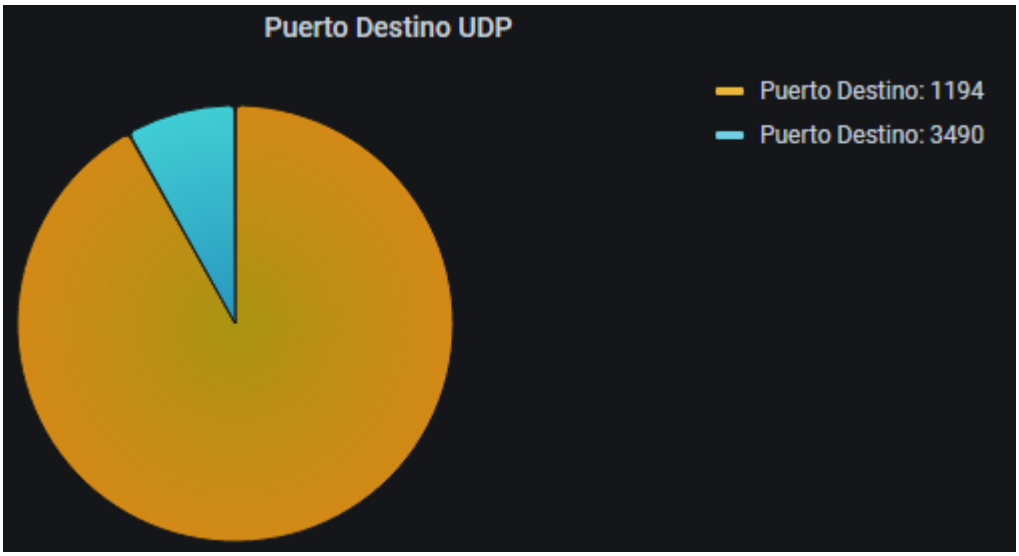

Figura 15. Gráfico de Puerto Destino UDP

Fuente: Fuente: Realizado por los Autores

V.5.- Tablas

- Tabla TCP: este esquema presenta la misma información que la gráfica "Tráfico TCP (Origen | Destino)", teniendo la data con mayor detalle del flujo de tráfico interno en la red de la Torre Mistral. Además, de poder aplicar filtros en los siguientes parámetros:
    - Fecha
    - IP Origen

- IP Destino
- Puerto TCP Origen
- VLAN Origen
- Puerto TCP Destino
- VLAN Destino
- Tráfico (en bytes)

Tabla TCP

Fecha	IP Origen	IP Destino	Puerto TCP Origen	VLAN Origen	Puerto TCP Destino	VLAN Destino	Tráfico
2021-09-29 10:59:47	172.16.15.39	10.1.16.183	445	15	49722	500	148 kB
2021-09-29 10:59:48	172.16.15.39	10.1.16.183	445	15	49722	500	138 kB
2021-09-29 10:59:49	172.16.15.39	10.1.16.183	445	15	49722	500	129 kB
2021-09-29 10:59:50	172.16.15.39	10.1.16.183	445	15	49722	500	121 kB
2021-09-29 10:59:51	172.16.15.39	10.1.16.183	445	15	49722	500	113 kB
2021-09-29 10:59:52	172.16.15.39	10.1.16.183	445	15	49722	500	106 kB
2021-09-29 10:59:53	172.16.15.39	10.1.16.183	445	15	49722	500	99.0 kB
2021-09-29 10:59:54	172.16.15.39	10.1.16.183	445	15	49722	500	92.6 kB
2021-09-29 10:59:55	172.16.15.39	10.1.16.183	445	15	49722	500	86.6 kB
2021-09-29 10:59:56	172.16.15.39	10.1.16.183	445	15	49722	500	81.0 kB
2021-09-29 10:59:57	172.16.15.39	10.1.16.183	445	15	49722	500	75.8 kB

Figura 16. Tabla TCP

Fuente: Fuente: Realizado por los Autores

- Tabla UDP: este esquema presenta la misma información que la gráfica "Tráfico UDP (Origen | Destino)", teniendo la data con mayor detalle del flujo de tráfico interno en la red de la Torre Mistral. Además, de poder aplicar filtros en los siguientes parámetros:
  - Fecha
  - IP Origen
  - IP Destino
  - Puerto UDP Origen
  - VLAN Origen
  - Puerto UDP Destino
  - VLAN Destino
  - Tráfico (en bytes)

Tabla UDP

Fecha	IP Origen	Puerto Origen UDP	VLAN Origen	IP Destino	Puerto Destino UDP	VLAN Destino	Tráfico
2021-09-29 15:14:22	10.1.23.245	1194	23	10.1.23.121	1194	23	709 B
2021-09-29 15:14:23	10.1.23.245	1194	23	10.1.23.121	1194	23	663 B
2021-09-29 15:14:24	10.1.23.245	1194	23	10.1.23.121	1194	23	620 B
2021-09-29 15:14:25	10.1.23.245	1194	23	10.1.23.121	1194	23	580 B
2021-09-29 15:14:26	10.1.23.245	1194	23	10.1.23.121	1194	23	543 B
2021-09-29 15:14:27	10.1.23.245	1194	23	10.1.23.121	1194	23	508 B
2021-09-29 15:14:28	10.1.23.245	1194	23	10.1.23.121	1194	23	475 B
2021-09-29 15:14:29	10.1.23.245	1194	23	10.1.23.121	1194	23	444 B
2021-09-29 15:14:30	10.1.23.245	1194	23	10.1.23.121	1194	23	416 B
2021-09-29 15:14:31	10.1.23.245	1194	23	10.1.23.121	1194	23	389 B
2021-09-29 15:14:32	10.1.23.245	1194	23	10.1.23.121	1194	23	364 B

Figura 17. Tabla UDP

Fuente: Fuente: Realizado por los Autores

CAPÍTULO VI

Conclusiones y Recomendaciones

Luego de haber conseguido los resultados, se realizan las conclusiones y recomendaciones en donde, se explica la resultante del producto final del Trabajo de Grado.

VI.1.- Conclusiones

En el transcurso del documento se ha demostrado la importancia de la seguridad informática a nivel empresarial, empezando por un sistema que brinde información sobre el tráfico interno de la red, pudiendo rastrear en todo momento la actividad de los usuarios, sabiendo el origen y destino de los equipos a los que intentan acceder. A su vez, el monitoreo ayuda a la administración de la red, permitiendo determinar los cuello de botella, debido a la auditoría que se efectúa.

Una vez se consiguieron los resultados aplicando la metodología del capítulo III, se observó que la información sobre el protocolo sFlow es escasa, este apartado es una desventaja con respectos a otros protocolos como IPFIX y Netflow. Lo que conllevó que se hiciera una investigación ardua y exhaustiva con el fin de alcanzar el objetivo planteado inicialmente en el Trabajo de Grado implementando el protocolo sFlow.

A medida que se aplicó el capítulo IV, referente al desarrollo, se realizaron comparaciones entre las distintas plataformas de monitoreo, Grafana junto a Prometheus, sFlowTrend y Elastic Stack. Las comparaciones entre las tres (3) herramientas dieron como resultado, seguir trabajando con la plataforma de Grafana junto a Prometheus debido a la plataforma que por las necesidades de Mistral, bajo consumo de recursos y mejor relación de capacidad.

El motivo por el cual se utilizó el protocolo sFlow es debido a su ventaja con respecto a otros protocolos como IPFIX y Netflow. Ya que posee virtudes como el ser un protocolo de estándar abierto, optimización de los recursos de la red, la fácil configuración, la escalabilidad y precisión de monitoreo en la red.

Resulta satisfactoria la implementación de sistema de análisis de monitoreo al cumplir con los objetivos planteados. Además, de cumplir con los requisitos planteados por el equipo de IT.

Se realizó la investigación de distintas plataformas de análisis de monitoreo compatibles con el protocolo sFlow, como serían: sFlowTrend, Elastic Stack y la combinación de Grafana y Prometheus. Dando como resultado una comparativa de las características obtenidas a nivel teórico y de implementación de cada una de las herramientas.

Una vez implementada las plataformas de análisis, se decidió por la implementación de la combinación de Grafana y Prometheus, debido a limitaciones que presentaba sFlowTrend, con respecto al almacenamiento de la información y el alto consumo de recursos que necesita la plataforma de Elastic Stack.

Se identificaron los dispositivos pertenecientes a la red interna de la Torre Mistral y se recopiló la información de cómo se encontraban interconectados. Dicha información incluyó la lista de equipos pertenecientes a la red, modelos de los dispositivos, nombre del equipo, direccionamiento lógico y las VLAN que pertenecen a la red. También se investigaron las hojas de datos de los dispositivos de red, para obtener cuáles son compatibles y candidatos a aplicar el protocolo sFlow, resultando compatibles los switches HP 2920 y el switch Core HP 8212 zl, siendo este último donde se decidió aplicar el protocolo.

VI.2.- Recomendaciones

Evaluación periódica de las capacidades de los servidores virtuales por parte de la empresa, con el fin de expandir los recursos en caso de ser necesario.

Se aconseja disponer del suficiente recurso de personal en IT, administradores de red, con el fin de tener en todo momento monitoreado cada uno de los dashboard, esto evitaría una posible equivocación por parte de los trabajadores.

Se recomienda a toda aquella persona que desee realizar una emulación sobre este Trabajo de Grado, tener conocimiento básico de programación en SQL, ya que es el lenguaje que se utiliza para la construcción de los de los query. Permitiendo diseñar consultas con la información de la base de datos acorde a la información requerida. Además, de dominio del sistema operativo Linux, con el fin de poder moverse a través de la línea de comandos en el servidor virtualizado empresarial.

Monitorear las demás localidades de todo el grupo Mistral, como parte del plan estratégico de la dirección de tecnología. Además, se recomienda al personal, hacer uso del sistema de alertas y alarmas que disponen las herramientas de Grafana y Prometheus, en los servidores críticos de la red, para estar al tanto de cuando surjan conexiones por parte de usuarios no permitidos. La recomendación se enfocaría como futura expansión de este Trabajo de grado.

Es aconsejable que toda persona que trabaje en el proyecto, lo realice a través de una VPN con el fin de tener acceso a la red en todo momento, además, de permitir la continuación del proyecto de manera remota, con el simple hecho de tener acceso a internet.

Bibliografía

Cisco, (s.f.), Introduction to Cisco IOS NetFlow

https://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/ios-netflow/prod_white_paper0900aecd80406232.html

Cisco, (s.f.), What Is a LAN?

https://www.cisco.com/c/en/us/products/switches/what-is-a-lan-local-area-network.html#~types

Cisco, (s.f.), ¿Qué es el monitoreo de red?

https://www.cisco.com/c/es_mx/solutions/automation/what-is-network-monitoring.html

Elasticsearch B.V., (s.f.), ¿Qué es el ELK Stack?

https://www.elastic.co/es/what-is/elk-stack

Grafana Labs, (s.f.), Dashboard anything. Observe everything.

https://grafana.com/grafana/

Herrera. L, (2006), Telemetría y telegestión en procesos industriales mediante canales inalámbricos Wi Fi utilizando instrumentación virtual y dispositivos PDA (Personal Digital Assitant) , p,120

https://www.dtic.ua.es/grupoM/recursos/articulos/JDARE-06-J.pdf

Hewlett Packard Enterprise Development LP, (s.f.), HP 8200 zl Switch Series - Overview

https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=c01818786

Intercompras Comercio Electrónico SA de CV, (s.f.), Paquete Switch HP 2920-48G-PoE+- 48 Puertos - Gigabit + Transceiver HP J4858C - X121/1g/SFP/ Lc Sx

https://intercompras.com/p/paquete-switch-hp-48g-poe-puertos-gigabit-transceiver-hp-j4858c-x1211gsfp-94060

Intercompras Comercio Electrónico SA de CV, (s.f.), Punto de Acceso HP MSM460 - Dual Radio - 802.11n

https://intercompras.com/p/punto-acceso-hp-msm460-dual-radio-80211n-71977

Microsoft, (s.f.), Conceptos básicos sobre bases de datos

https://support.microsoft.com/es-es/office/conceptos-b%C3%A1sicos-sobre-bases-de-datos-a849ac16-07c7-4a31-9948-3c8c94a7c204

Phaal. P & Lavine. M, (2004), sFlow Version 5 p. 2

https://sflow.org/sflow_version_5.txt

Postel. J, (1980), User Datagram Protocol

https://tools.ietf.org/html/rfc768#ref-2

Prometheus Authors, (s.f.), ¿Qué es Prometheus?

https://prometheus.io/docs/introduction/overview/