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

Luis Chacón, Robert Moreno

Escuela de Ingeniería en Telecomunicaciones, Universidad Católica Andrés Bello

Caracas, Venezuela

luisorlandochacon1@gmail.com

robertmoreno504@gmail.com

I. RESUMEN

El presente proyecto tiene como finalidad 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". Diseñando una propuesta a través del protocolo de sFlow, por su interoperabilidad con la infraestructura tecnológica existente; además, de ser un estándar abierto de la industria.

Cabe destacar la versatilidad del protocolo sFlow 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.

II. INTRODUCCIÓN

A través de este artículo se realiza una breve descripción acerca del trabajo de grado, el cual consistió en la implementación de un sistema de monitoreo a través del protocolo sFlow. En el artículo se explica de manera concreta los aspectos más destacados del Trabajo de Grado.

III. 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 y la falta de registro del tráfico por parte de los usuarios finales de la Torre Mistral, surge la necesidad de implementar un sistema de monitoreo capaz de identificar dicho tráfico interno.

Es por ello que se implementa el protocolo sFlow, con el fin de extraer 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.

.

IV. OBJETIVOS

IV.1. Objetivo General

Diseñar e 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.

IV.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.

- Implementar la plataforma de monitoreo seleccionada para la red Interna en La Torre Mistral.

V. MARCO TEÓRICO

V.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.

V.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.

V.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.

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

V.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.

V.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".

V.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.

V.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.

V.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.

V.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.

V.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.

V.9. 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.

V.10. IPFIX

El Protocolo de Internet para la Exportación de Información de Flujo, en inglés *Internet Protocol Flow Information Export* (IPFIX) determina cómo se exporta la información de flujo de IP y se envía a un recopilador o analizador.

V.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).

V.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.

V.11.1.1. Flujo 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

V.11.1.2. Flujo de paquetes Conmutados o Enrutados

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.

V.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.

V.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.

V.12. sFlowTrend

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.

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.

V.13. 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.

V.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.).

V.15. Prometheus

Prometheus es un software que tiene 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".

V.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.

V.17. Métrica

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.

V.17. Elastic Stack

Agrupación de servicios conformados por Elasticsearch, Logstash, Kibana y Beats.

El primero de ellos tiene, Elasticsearch 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".

La aplicación Logstash es el software encargado de la adición y análisis de datos para su posterior envío a Elasticsearch

Beats, explicado en su página oficial Elasticsearch B.V. (s.f.) como "familia de agentes de datos de propósito único y livianos".

Por último Kibana es la 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.

VI. MARCO METODOLÓGICO

VI.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".

VI.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.

VI.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.

VI.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.

VI.3.2. 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.

VI.3.3. Switch

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.

VI.3.3. 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.

VI.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.

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.

VI.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.

VII. DESARROLLO

VII.1. Fase de Levantamiento de Información

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.

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 2. Comparativa de Plataformas de Monitoreo

VII.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 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.

VII.2.1 Prometheus y Grafana

VII.2.1.1 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.

VII.2.1.1 Prometheus

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 start
```

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.

VII.2.2. Elastic Stack

VII.2.2.1 Elasticsearch

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.

VII.2.2.2 Kibana

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
```

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.

VII.2.2. Elastic Stack

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.

VII.3. Fase de Diseño

Una vez se implementó 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.

VII.4. Fase de Pase a Producción

Después de mantener durante 1 semana la herramienta según los acuerdos obtenidos en las mesas técnicas y las necesidades del cliente, se realizó el pasé formal a producción. Cumpliendo con los requisitos del equipo de IT y los objetivos del proyecto.

VIII. RESULTADOS

VIII.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 este 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.

VIII.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 fueron debido a que 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

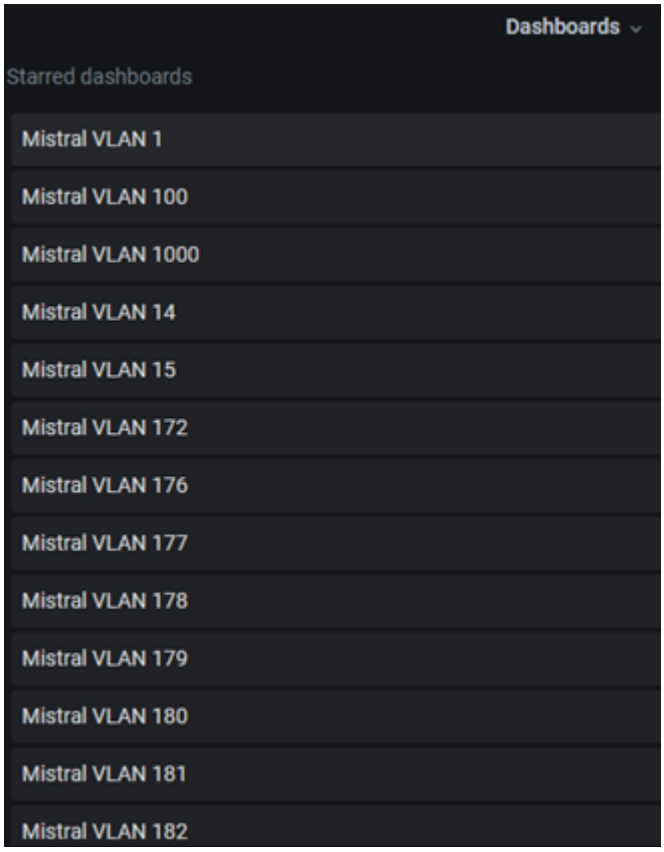

Fig. 1 Interfaz de Grafana

VIII.3. Plataforma Implementada

La herramienta utilizada para el sistema de monitoreo de la red interna de la Torre Mistral fue Grafana junto a Prometheus, el cual se dimensionó 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 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 3. Conformación de los Dashboards

IX. CONCLUSIONES Y RECOMENDACIONES

IX.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.

IX.2. Recomendaciones

Evaluación periódica de las capacidades de los servidores virtuales empresariales, con el fin de expandir los recursos en caso de ser necesario.

Se aconseja disponer con el 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.

Trabajar 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.

Monitorear las demás localidades de todo el grupo Mistral, como parte del plan estratégico de la dirección de tecnología. Está la pudiese enfocar como futura expansión de este Trabajo de grado

REFERENCIAS

Cisco, (s.f.), Introduction to Cisco IOS NetFlow. Available: 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? Available: 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?. Available: https://www.cisco.com/c/es_mx/solutions/automation/what-is-network-monitoring.html

Elasticsearch B.V., (s.f.), ¿Qué es el ELK Stack? Available: https://www.elastic.co/es/what-is/elk-stack

Grafana Labs, (s.f.), Dashboard anything. Observe everything. Available: 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. Available: 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. Available: 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. Available: 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. Available: https://intercompras.com/p/punto-acceso-hp-msm460-dual-radio-80211n-71977

Microsoft, (s.f.), Conceptos básicos sobre bases de datos. Available: 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. Available: https://sflow.org/sflow_version_5.txt

Postel. J, (1980), User Datagram Protocol. Available: https://tools.ietf.org/html/rfc768#ref-2

Prometheus Authors, (s.f.), ¿Qué es Prometheus?. Available: https://prometheus.io/docs/introduction/overview/