Universidad Politécnica
de Madrid

Escuela Técnica Superior de
Ingenieros Informáticos

Grado en Ingeniería Informática

Trabajo Fin de Grado

PUESTA EN MARCHA DE UNA PLATAFORMA DE MONITORIZACIÓN RED

Autor: Diego Lamana Núñez

Tutor(a): Sonia De Frutos Cid

Madrid, enero 2022

Este Trabajo Fin de Grado se ha depositado en la ETSI Informáticos de la Universidad Politécnica de Madrid para su defensa.

Trabajo Fin de Grado
Grado en Ingeniería Informática
Título: PUESTA EN MARCHA DE UNA PLATAFORMA DE MONITORIZACION DE RED
enero 2022

Autor: Diego Lamana Núñez

Tutor: Sonia De Frutos Cid
Departamento de Lenguajes y Sistemas Informáticos e Ingeniería del Software
ETSI Informáticos
Universidad Politécnica de Madrid

Resumen

Este Trabajo de Fin de Grado tiene como misión aprender la importancia de la monitorización de una red en la actualidad.

Los objetivos que se llevarán a cabo en el proyecto serán aprender sobre las herramientas más usadas actualmente y aprender el proceso que necesita una de estas herramientas de monitorización para ser puesta en marcha en una red de gran tamaño.

El proyecto tratara primero de explicar de la manera más simple posible los aspectos básicos de la monitorización y de algunos protocolos indispensables en monitorización, también se tratarán los pasos que hay que seguir para desplegar una herramienta de monitorización, esto incluye el desligue físico que hay que realizar sobre el centro de procesamiento de datos, y de la prueba de las funciones que tiene esta herramienta cuando ya está desplegada sobre la red.

Estas pruebas de funciones incluyen la creación de alarmas, cuadros de mando y alta de dispositivos en la herramienta.

Por último, en este documento también se hará una breve introducción de la migración que se va a realizar de la antigua herramienta de monitorización a esta nueva herramienta que se va a desplegar.

Palabras clave: monitorización, despliegue físico en centro de procesamiento de datos, pruebas de funciones de la herramienta, migración

Abstract

The main aim of this end-of-degree dissertation is to learn about the importance of monitoring a network nowadays.

The objectives of the project will be to learn about the most used tools and to learn the process that one of these monitoring tools needs to be implemented in a large network.

The project will first try to explain in the simplest possible way the basics of monitoring and some essential monitoring protocols, also the steps to be followed to deploy a monitoring tool, including the physical detachment to be performed on the data center, and the testing of the functions that this tool has when it is already deployed on the network.

These function tests include the creation of alarms, dashboards, and device discovery in the tool.

Finally, this document will also provide a brief introduction of the migration from the old monitoring tool to this new tool to be deployed.

Keywords: *monitorization, physical detachment on the data center, testing the functions of the tool, dashboards, alarms, migration*

Tabla de contenidos

Índice de figuras

1 Introducción

La manera en la que controlamos el estado de nuestra red ha cambiado drásticamente a lo largo de los años. Al principio las redes se mantenían de manera local, teniendo aun operador comprobando el estado de cada equipo. Esto en redes pequeñas no suponía un gran problema, pero cuando hablamos de redes medianas y grandes este método es inviable, ya que no se puede estar monitorizando localmente miles de equipos.

Debido al incremento de redes de gran tamaño, se necesitó urgentemente una solución a esto, la primera de las soluciones fue el desarrollo de alguna herramienta de monitorización orientada a ICMP, pero que no daba ningún tipo de información del estado de los recursos de los equipos, únicamente indicaba si estos estaban caídos o no, o respondían muy lento. La solución final fue la creación de protocolos y herramientas de monitorización que fueran capaces de sacar información de los recursos como la CPU, memoria, disco, uso de interfaces y mucho más, incluso predecir fallas en los equipos antes de que se produjesen.

El primer protocolo de monitorización por excelencia a desarrollarse fue SNMP en 1990, un protocolo que era capaz de sacar información de los recursos de los equipos (CPU, memoria, estado, etc.), sacando su última versión en 2002 (v3). Junto a SNMP se desarrollaron otros protocolos de análisis de trafico de red como. A partir de estos protocolos se desarrollaron muchas herramientas de monitorización que solucionaron el problema de antaño.

Actualmente las empresas buscan tener la capacidad de controlar al milímetro sus redes, para que en caso de falla estas puedan solucionar casi de manera inmediata o incluso evitar que se produzca. Por eso todas las empresas actualmente usan herramientas de monitorización como medidor de salud de su red, que junto a los métodos de ciberseguridad es una de las aplicaciones más importante que realiza una empresa sobre su red.

1.1 Objetivos del trabajo

El objetivo principal del proyector es montar una herramienta de monitorización para un cliente en concreto que necesita urgentemente migrar de una herramienta obsoleta.

En este proyecto se realizará la instalación de la herramienta en dos CPDs del cliente, realizando pruebas de funcionamiento sobre esta herramienta y haciendo una breve introducción de la migración que se realizará de la herramienta de monitorización antigua a esta nueva.

La lista de tareas que van a llevarse a cabo en este proyecto es:

- Estudio de la aplicación
- Estudio del estado de las aplicaciones de monitorización que se usan actualmente en el mercado
- Requisitos de la aplicación
- Instalación de la aplicación
- Alta de dispositivos de prueba del cliente/filtros
- Configurar alarmas

- Crear cuadros de mandos
- Migración

2 Estado del arte

En este capítulo se va a recoger toda la información necesaria para comprender la monitorización de red, así como las aplicaciones que se usan en monitorización actualmente.

Este capítulo estará dividido en dos secciones, una primera sección que recogerá los conocimientos básicos de monitorización red, y una segunda sección que contendrá información sobre las herramientas de monitorización actuales en el mercado.

El objetivo de este capítulo es otorgar una pequeña introducción a la monitorización de red.

2.1 Fundamentos de la monitorización de red

En esta sección se explicarán los conocimientos básicos para poder comprender como funcionan las herramientas de monitorización.

Primero de todo se hará una breve introducción a las herramientas de monitorización, explicando su importancia, y también se hará una explicación de los protocolos más usados en estas herramientas como son los protocolos SNMP, ICMP y NetFlow.

2.1.1 Importancia de la monitorización de red

La monitorización se ha convertido en un elemento fundamental en cualquier empresa que tenga montada una red informática, sobre todo si se trata de una red de gran tamaño, en la que no puedes tener un operador en cada dispositivo para asegurar de que este funcione correctamente. La monitorización te permite tener únicamente un par de operadores, que con ayuda de una herramienta de monitorización sean capaces de mantener una gran red. De esta manera se puede tener una idea general del estado de la red, obteniendo avisos en los dispositivos críticos pudiendo así actuar con rapidez en caso de que se detecte algún tipo de problema en estos. Estos problemas se pueden arreglar incluso remotamente haciendo uso de SSH sin tener que ir presencialmente a cada dispositivo. En cuanto a seguridad, la monitorización también es de gran ayuda ya que se pueden detectar ataques de denegación de servicio antes de que se conviertan en algo incontrolable. Esto se podría detectar cuando una interfaz tiene un caudal de tráfico mayor al habitual, siempre que se esté en un habiente muy controlado, ya que no tiene por qué significar el aumento de tráfico en una interfaz un ataque DDOS.

Lo comentado anteriormente se consigue instalando una herramienta de monitorización, que nos permitirá dar de alta los dispositivos de nuestra red, configurar umbrales para que se generen alarmas si estos son pasados y crear cuadros de mando para poder visualizar los datos críticos que se obtienen de los dispositivos.

En general, la monitorización es un requisito fundamental actualmente en cualquier empresa que quiera tener controlada continuamente el estado de salud de su red.

2.1.2 SNMP

El protocolo SNMP (*Simple Network Management Protocol*), [1] es el protocolo principalmente más usado en la mayoría de las herramientas de monitorización. Este protocolo trabaja en la capa de aplicación y es un protocolo no orientado conexión, es decir que hace uso de UDP como protocolo de transporte.

El protocolo SNMP es compuesto principalmente de unos servidores SNMP que denominaremos gerentes que hacen uso del puerto 162, y de unos clientes que llamaremos agentes SNMP que hacen uso del puerto 161. El proceso básico que hace SNMP, es que el gerente se comunique con los agentes SNMP para pedir información sobre el dispositivo en el que este instalado el agente SNMP, o que los agentes SNMP envíen información al gerente sin que este se la pida directamente. Por lo que la aplicación que tiene esto en monitorización es clara, se tiene un servidor principal (gerente), que se encargara de recoger información de los dispositivos (agentes SNMP).

Ahora que se conece el funcionamiento básico del protocolo SNMP, voy a comentar los traps. Los traps son básicamente lo que permite a los agentes SNMP envirar información directamente al gerente sin que este tenga que intervenir. Estos *traps* se configuran en los dispositivos permitiendo su envió. De esta manera cuando por ejemplo cuando una partición el disco se llene por completo, el dispositivo generará un *trap* para informar de esto al gerente.

Otro elemento importante de SNMP es la MIB. La MIB es una base de datos que se encuentra en todos los agentes SNMP, que almacena con una estructura de árbol todas las variables que se monitorizan en los dispositivos. Esta base de datos se recorre con ayuda de lo OID, que es una secuencia de números que sirve como índice del árbol. Así haciendo uso de los OIDs se puede recorrer el árbol sencillamente y teniendo un valor único para identificar a cada variable de la MIB. Un ejemplo de un OID podría ser el siguiente 1.3.6.1.4.1.2021.11.11 que representa el uso de la CPU del dispositivo. [2]

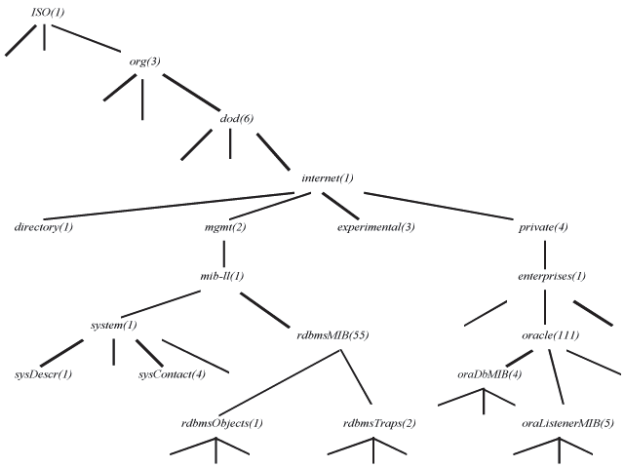

Figura 1 - Árbol MIB

Así que como un ejemplo final del funcionamiento de SNMP sería el siguiente: El usuario quiere consultar el *sysname* de un dispositivo, por lo que este hará una petición al agente SNMP que hay instalado en el dispositivo, esto internamente funcionaria de la siguiente manera, el servidor SNMP realizaría una petición GET al dispositivo sobre la OID que corresponde con el *sysname* en la MIB, y el agente SNMP le respondería con el *sysname*. Otro caso que puede pasar es que en un dispositivo que tiene un agente SNMP, se caiga una interfaz.

En este caso se enviará un *trap* al gestor indicando que sea caído una interfaz en el dispositivo.

Por último, se explicarán los mecanismos de seguridad que tiene SNMP y para ello hay que tener en cuenta las diferentes versiones que tiene SNMP. Actualmente SNMP tiene 3 versiones, aunque entre las 2 primeras no hay mucha diferencia, por lo que únicamente voy a cometer la versión 2 y 3. La versión 2 de SNMP usa como mecanismo de autentificación un *string* de texto plano llamado *community-string*, que básicamente se configura en los agentes SNMP y para que el gerente pueda comunicarse con este agente SNMP, tiene que usar la *community-string* correcta. En el caso de la versión 3, el funcionamiento es el mismo solo que la *community-string* es encriptada.

2.1.3 ICMP

El protocolo ICMP (*Internet Control Message Protocol*) [3] es usado para el envío de mensajes de control de errores e información. Este protocolo es usado habitualmente con el comando *ping* y *traceroute*.

La función principal de este protocolo en monitorización es respaldar la información que se recibe del protocolo SNMP, por ejemplo, si el protocolo SNMP no alcanza al dispositivo en cuestión, usaremos el protocolo ICMP para comprobar si se ha caído el agente SNMP, se ha caído el dispositivo al completo o hay alguna lista de acceso que está bloqueando los paquetes SNMP.

En general, ICMP se usa para localizar los dispositivos que se quieren monitorizar desde el servidor donde se encuentre el gerente SNMP y comprobar si son alcanzables, en ese caso se conectarían por SNMP, y si no se pudiese se usaría para depurar que dispositivos están bloqueando al protocolo SNMP.

2.1.4 TELNET

Telnet [4] es un protocolo/servicio creado para poder realizar conexiones remotas con servidores y equipos a través de internet. Este protocolo tiene el problema de que al realizar la conexión no envía la información cifrada de extremo a extremo, por lo que este protocolo está muy limitado y se usa únicamente en a redes internas.

2.1.5 SSH

SSH [5] es un protocolo/servicio usado para establecer conexiones remotas seguras con servidores o equipos a través de internet usando cifrado de extremo a extremo. Este protocolo es usado principalmente para gestionar equipos o servidores de manera remota sin tener que ir a conectarse físicamente a ellos. Como se ha comentado Telnet es un protocolo similar, a diferencia de SSH que se creó para sustituir a este, ya que Telnet tiene problemas de seguridad ya que no ofrece por defecto cifrado de extremo a extremo cuando SSH sí.

2.1.6 Syslog

Syslog [6] es un protocolo muy sencillo que se activa en los dispositivos que se quieren monitorizar para que estos envíen un mensaje plano de no más de 1024 bytes al servidor de monitorización. Este protocolo tiene problemas de seguridad ya que como hemos comentado envía mensajes planos por UDP, por lo que cualquier intruso en la red con un analizador de tráfico podría ver su contenido. Actualmente existe una versión de syslog que encripta los mensajes que resuelve este problema comentado.

Generalmente este protocolo solo envía mensajes sencillos que no contienen mucha información crítica, como puede ser un fallo de inicio de sesión o que el SO del dispositivo tiene una actualización.

2.1.7 NetFlow

NetFlow [7] se trata de un protocolo de visualización de tráfico, usado para sacar información de los paquetes en una red controlada. Este protocolo es principalmente usado junto con DPI para poder detectar que tráfico está causando aglomeraciones en la red y de donde proviene, para así poder actuar al respecto y evitar ralentizaciones en la red, y para supervisar tráfico de entrada y de salida.

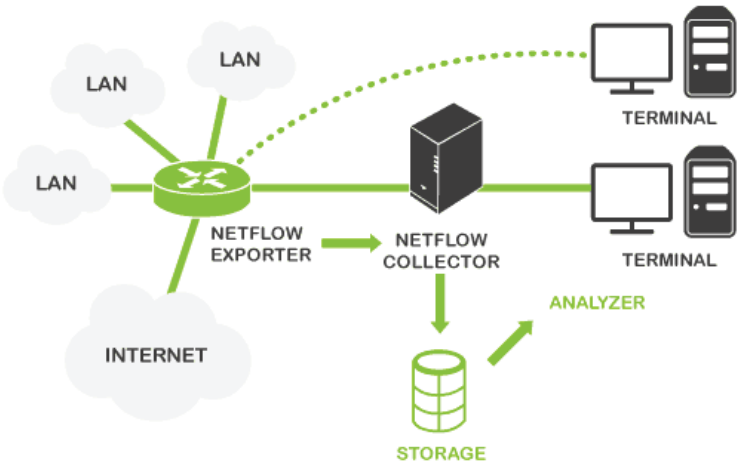

Figura 2 - Funcionamiento NETFLOW

Este protocolo es activado en las interfaces de los *routers* de las que se quiere analizar el tráfico, de esta manera cuando pase tráfico por estas interfaces donde tenemos configurado NetFlow, se almacenara la información del paquete en la cache del *router* reservada para NetFlow y esta se la enviara a nuestro colector de NetFlow para poder analizarlo.

2.1.8 SPAN

SPAN [8] es un protocolo de monitorización que se aplica en los *switches*. Este protocolo permite seleccionar unos puertos que estén conectados a la red, y duplicar su información hacia un puerto de salida que está conectado a un

dispositivo de monitorización, que usara esta información duplicada para analizar los paquetes que pasan por el *switch*. De esta manera este protocolo es de gran utilidad en monitorización, ya que permite analizar el tráfico red, así como también usarse como un IDS (*Intrusion Detection System*).

2.1.9 DPI

DPI (*Deep Packet Inspection*), se trata de la inspección sobre un paquete de las capas 2 - 7 del modelo OSI, es decir DPI es capaz de examinar el contenido de los mensajes e identificar la aplicación o servicio específico del que proviene. [9]

Principalmente DPI se usa como una herramienta de seguridad, ya que combina las funciones de un sistema de detección de intrusos, de un sistema prevención de intrusos y de un *firewall* de estado, y al tener todas estas funciones de seguridad juntas las empresas han optado por sustituir el tradicional *firewall* de estado por esta herramienta, ya que incluso permite a los administrados configurar ciertas reglas para que se cumplan en todos los niveles de red. [9]

Aparte del uso que tiene DPI protegiendo la red de la empresa, esta herramienta actualmente también se usa para gestionar la red para agilizar el fujo de las redes.

2.1.10 MTTR

MTTR es una media utilizada para medir el tiempo medio de coste que va a tener la reparación de una avería de un dispositivo en una red. Esta medida es utilizada en algunas herramientas de monitorización para sacar una aproximación del tiempo de reparación de los dispositivos averiados. [10]

2.1.11 Network Configuration Manager

NCM es una funcionalidad que ofrecen muchas herramientas de monitorización. La función de NCM es la de llevar un control de la configuración de los dispositivos monitorizados en una red, de manera que NCM ofrece una base de datos donde se almacenan todas las configuraciones y también un historial de los cambios que se han realizado en las configuraciones.

Capture Time	Line Changes	Is Refere...	Running vs. Startup	Last Verified Time	NCM Mode	NCM User	Device User	Source	Location
Oct 27, 2021 11:01:12 PM CE...	1 changes			Nov 2, 2021 11:01:55 P...	N/A	N/A	Unknown	Unknown	Unknown
Oct 25, 2021 11:01:37 PM CE...	2 changes			Oct 26, 2021 11:01:31 P...	N/A	N/A	Unknown	Unknown	Unknown
Oct 21, 2021 11:03:38 PM CE...	2 changes			Oct 24, 2021 11:01:38 P...	N/A	N/A	Unknown	Unknown	Unknown
Oct 20, 2021 11:02:06 PM CE...	1 changes				N/A	N/A	Unknown	Unknown	Unknown
Oct 11, 2021 11:00:41 PM CE...	13 changes			Oct 19, 2021 11:03:18 P...	N/A	N/A	Unknown	Unknown	Unknown
Sep 28, 2021 11:42:57 AM CE...	2 changes			Oct 10, 2021 11:00:53 P...	N/A	N/A	Unknown	Unknown	Unknown
Feb 16, 2021 11:02:40 PM CET	3 changes			Sep 27, 2021 11:00:49 P...	N/A	N/A	Unknown	Unknown	Unknown
Feb 15, 2021 11:01:49 PM CET	1 changes				N/A	N/A	Unknown	Unknown	Unknown
Dec 10, 2020 11:02:25 PM CET	1 changes			Feb 14, 2021 11:03:00 P...	N/A	N/A	Unknown	Unknown	Unknown

Figura 3 - Spectrum NCM

De esta manera si se perdiese alguna configuración se podría restaurar sin problemas, también si después de realizar algún cambio en una configuración esta no funcionase, se podría comprobar los cambios con la antigua para averiguar que es diferente y así poder depurar el problema.

2.2 Herramientas de monitorización de red actuales

En esta sección se va a hacer un estudio y análisis sobre las diferentes aplicaciones de monitorización que hay disponibles actualmente en el mercado, comentando de cada una sus ventajas y desventajas.

Las primeras aplicaciones de las que se va a hablar en este apartado van a ser las que actualmente se usan en mi cliente, que son Spectrum y UIM.

Habitualmente se pueden diferenciar muchos tipos de aplicaciones de monitorización: las que se centran en la configuración de alarmas y la creación de una vista topológica, las que se centran en la creación de cuadros de mando, las que se centran en el análisis del tráfico red o las que juntan varias de estas cualidades en una única herramienta.

2.2.1 Spectrum

Spectrum es una herramienta de monitorización de la empresa CA Broadcom, centrada principalmente en la creación de alarmas y de una topología.

La estructura de esta herramienta es la siguiente, tiene un servidor principal que se llama Spectrum y otro servidor que se llama oneclick, de estos servidores se pueden instalar más de uno, por ejemplo, se podrían instalar uno de cada para que haya redundancia por si se cae alguno. El servidor Spectrum se encarga de comunicarse con los dispositivos a monitorizar y el servidor oneclick se encarga de la visualización de las alarmas y los dispositivos. [11]

Figura 4 - Diagrama Spectrum

Una de las principales ventajas que tiene esta herramienta es que crea una topología muy bien llevada. Esta topología se crea automáticamente mientras se van creando contenedores (donde se guardan los dispositivos, esto se usa principalmente para organizar la herramienta), dando de alta los dispositivos en la herramienta y configurando las conexiones que existen entre los dispositivos pintando así estas líneas. Esto permite tener una alta visión de toda la arquitectura red.

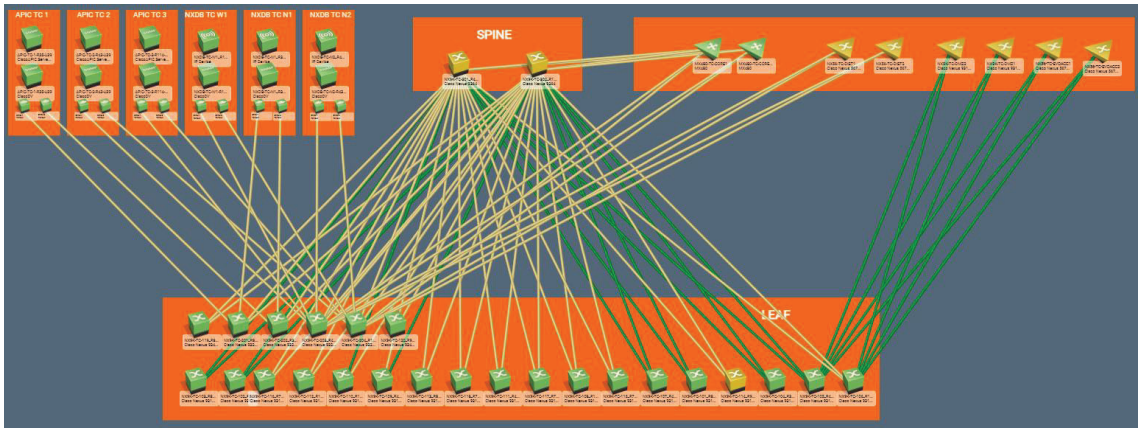

Figura 5 – Topología Spectrum

Otra de las ventajas principales de esta aplicación, es su sistema de alarmas. Este sistema de alarmas funciona a través de eventos. Estos eventos se generan a partir de los traps SNMP que envían los dispositivos al servidor de monitoreo generando eventos, y dependiendo de cómo estén configurados estos eventos se generara una alarma o no. Esta herramienta también permite la creación de eventos y alarmas personalizadas, aunque por defecto en Spectrum ya vienen una gran cantidad de ellas. También en cada alarma se puede configurar una serie de recomendaciones para solucionar lo que ha generado la alarma.

Por último, otra ventaja que tiene esta herramienta es tiene un gran sistema de autodescubrimiento de dispositivos y conexiones, simplificando de manera considerable la creación de la topología.

Después de haber comentado las principales ventajas de la aplicación, ahora voy a comentar los contras de esta aplicación.

La primera desventaja que comentar, es la dependencia de tener que instalar otra aplicación que se encarga de las creaciones de cuadros de mando para la visualización de los datos, ya que Spectrum no tiene esta función.

Otra desventaja, son los servidores oneclick, ya que estos clientes fallan habitualmente al intentar mostrar información o topología y hay que reiniciarlos con frecuencia.

Como ultima desventaja esta aplicación no hace un análisis del tráfico red.

En general Spectrum es una gran herramienta de monitorización, y estas desventajas que he comentado se solucionan haciendo una integración con otra herramienta de CA Broadcom que es UIM, que es la que comentare a continuación.

2.2.2 UIM

UIM es una herramienta de monitorización de la empresa CA Broadcom, y al contrario de Spectrum, esta herramienta fue creada para realizar las tareas que no tenía Spectrum implementadas, la visualización de datos a partir de cuadros de mando.

La estructura de esta herramienta es compuesta por tres conceptos: *hub*, robot y sonda. Los *hub* son los contenedores donde se almacenan los robots, estos robots son un software que se instala en los dispositivos a monitorizar, y en los robots se instalan sondas que son las herramientas que se encargaran de

monitorizar los dispositivos donde están instalados los robots. Como ejemplo, tenemos un hub que está instalado en nuestro servidor de gestión (UIM server), y queremos monitorizar unos servidores. Para hacer esto, instalaríamos un robot en cada servidor a monitorizar y dentro de estos robots instalaríamos unas sondas para que monitoricen este servidor, como podría ser la sonda CDM (CPU, DISK, MEMORY), que se trata de una sonda que monitoriza el disco, la CPU y la memoria del dispositivo. Por último, la información recogida por la sonda es enviada por el robot al *hub*, y el *hub* mostraría esta información en la consola del operador. [12]

Ahora que se ha comentado como funciona UIM, se van a presentar las ventajas y contras de esta aplicación.

Una de las principales ventajas es que, UIM al centrarse en la visualización de los datos, solo necesitara descubrir los dispositivos más críticos de la empresa, que son de los que se querrá crear unos cuadros de mando personalizados y activar unas alarmas más complejas que las que ofrece Spectrum.

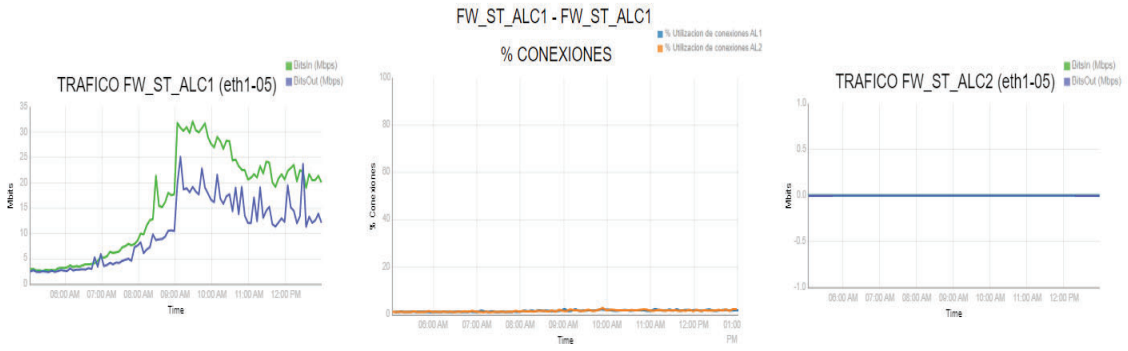

Figura 6 – Cuadros de mando UIM

Otra ventaja es que al pertenecer Spectrum y UIM a la misma empresa, estas dos herramientas son capaces de sincronizarse entre sí. De manera que las alarmas configuradas en UIM también saltarían en la consola de alarmas de Spectrum.

También cabe destacar que UIM es una herramienta que permite personalizar los cuadros de mando al gusto del operador y elegir una franja de tiempo para la visualización de los datos, y esto es otro gran punto a su favor.

Por el contrario, al usar esta solución se están instalando muchos servidores por separado, los servidores de Spectrum y UIM, y esto tiene un gran coste, cuando hay otras herramientas que hacen las funciones de estas dos herramientas con únicamente un servidor.

También estas herramientas necesitan un gran conocimiento sobre ellas para realizar sus configuraciones.

Como último punto en contra, esta herramienta al igual que Spectrum no realiza un análisis del tráfico red.

En general, usar estas dos herramientas es una gran solución para la monitorización de una red, ya que al tener montadas las dos herramientas y configuradas correctamente, se consigue un control elevado sobre el estado de la red, con la desventaja de que esta configuración y levantamiento de estas herramientas es muy tediosa, y el coste de mantenimiento es elevado.

2.2.3 Viewtinet

Viewtinet se trata de una herramienta de monitorización orientada principalmente en la creación y personalización de cuadros de mando.

Está formado por dos servidores uno que se encarga de la configuración de la herramienta y otro que se encarga de la visualización de los datos al usuario y de la creación de cuadros de mando. [13]

Esta herramienta a diferencia de otras permite a cualquier usuario crear cuadros de mandos de manera muy sencilla y sacar informes de estos de manera muy rápida. Esta herramienta ofrece diferentes tipos de cuadros de mando, como pueden ser cuadros de mando de tópicos, por ejemplo, un cuadro de mando que muestre el top 10 dispositivos más alarmados, y cuadros de mando con mapas de calor sobre un mapa geográfico. También esta herramienta añade muchas features a los cuadros de mando, como pueden ser el cambio de granularidad de los datos y que al pasar a un dispositivo móvil los cuadros de mando se adaptan a este. [13]

Aparte de los cuadros de mando, esta herramienta también ofrece una configuración de alarmas sobre los dispositivos que se monitorizar, polling SNMP, creación de una topología sencilla y análisis de tráfico usando NetFlow.

Como podemos ver esta herramienta es muy completa, y el único punto en contra que podríamos sacar es que se centre demasiado en la creación de cuadros de mando, y que divide la aplicación en diferentes herramientas en vez de tenerlo todo en una.

En conclusión, Viewtinet es una buena opción para una empresa que quiera tener acceso a cuadros de mando al instante y reportes sobre el estado de su red en todo momento.

2.2.4 NGeniusONE

NGeniusONE es una herramienta de monitorización desarrollada por la empresa NETSCOUT. Esta herramienta está centrada principalmente en la visualización del tráfico red, de manera que se obtienen cuadros de mando que nos permiten hacer un análisis de rendimiento de la red, un análisis de las aplicaciones y un análisis de las sesiones de los usuarios. Con todo esto la herramienta también ofrece una configuración de alarmas y un *mapping* de la topología. Todo esto se consigue principalmente haciendo uso de los protocolos SPAN en los switches y NetFlow en los routers [14]

Para la instalación de esta herramienta, la empresa ofrece una instalación "*out-of-the-box*" es decir que un *rack* listo únicamente para ser conectado al armario, obteniendo así una instalación rápida y sencilla. Aunque es recomendable como en toda red informática si se puede, tener un servidor de *backup* con las mismas características para que así la red de monitorización tenga redundancia en caso de cualquier tipo de fallo. [14]

Figura 7 – Cuadros de mando Viewtinet

Ahora que se conocen el funcionamiento y arquitectura de la herramienta, presentaremos sus pros y contras.

Una de las primeras ventajas de esta aplicación es que solo es necesario instalar un servidor para que esta funcione correctamente, a diferencia de Sepctrum y UIM.

Otra de las ventajas de esta aplicación es que nos ofrece una función, que es el análisis de tráfico red que no se incluye en muchas herramientas de monitorización.

En cambio, una de las principales desventajas que tiene esta aplicación, es que no ofrece una monitorización por SNMP de los dispositivos, por lo que la empresa necesitaría contratar otra solución para poder hacer esa función.

En general esta herramienta es bastante completa, y es una muy buena opción para usarla para monitorizar el tráfico de una gran red informática. De hecho, esta es la herramienta que desplegaremos como solución a Spectrum y UIM, y en la que nos centraremos en este proyecto. Teniendo en cuenta que esta empresa ya tiene lista una solución para la monitorización por SNMP y que solo le es necesario monitorizar el tráfico red, función que no ofrece ni Spectrum ni UIM.

2.2.5 Entuity

Entuity es una herramienta de monitorización muy competa que ofrece monitorización de los dispositivos mediante SNMP, monitoreo de flujos mediante NetFlow/SPAN, un análisis de los dispositivos y trafico red mediante cuadros de mando personalizados y alarmas. También esta aplicación permite la creación una topología interactiva con las mismas características que la topología de Spectrum.

Esta herramienta usa únicamente un servidor para funcionar con normalidad, ya que únicamente este servidor funcionara como agente SNMP y recolector de los flujos NetFlow/SPAN. Esto pasa igual en NGeniusONE, a diferencia de que este no tiene la función de gerente SNMP. [15]

Herramienta de monitorización con acceso a creación de cuadros de mandos, configuración de alarmas y topología.

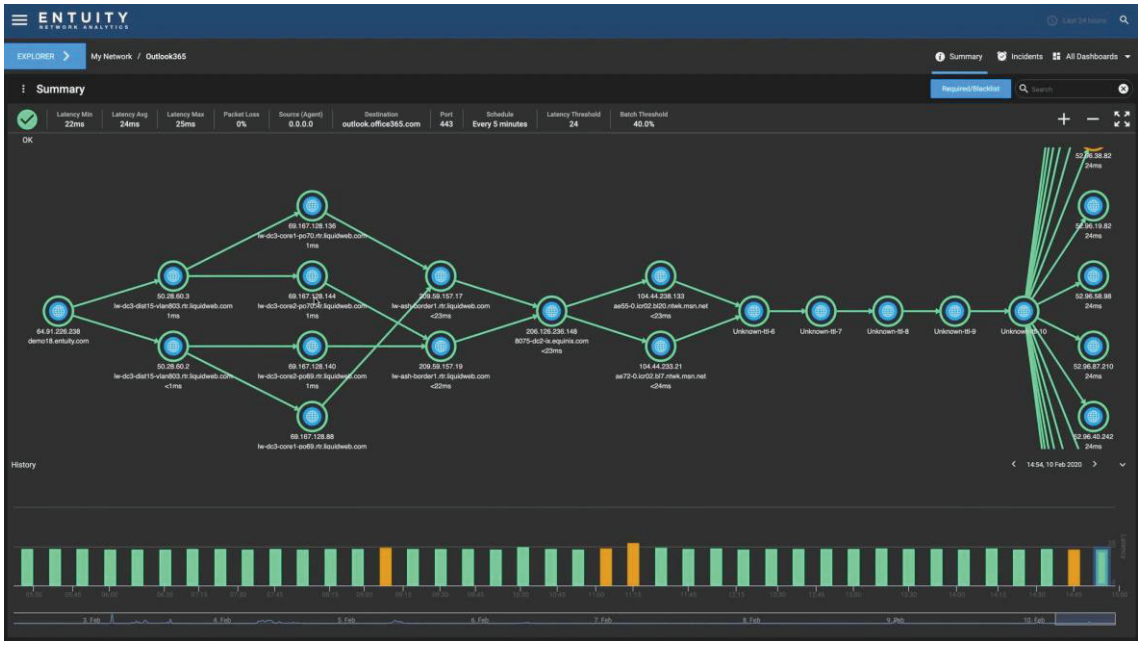

Figura 8 – Camino tráfico Entuity

Como se puede ver esta aplicación ofrece todas las características que necesita una empresa para poder monitorizar su red al completo sin problemas. Esta herramienta es muy parecida a Viewtinet, con la diferencia de que Entuity tiene todo en una única aplicación donde se configura todo.

En conclusión, esta herramienta será la opción más correcta para una empresa que únicamente quiera tener toda la gestión de la red en una única aplicación sin tener que usar muchos recursos.

2.2.6 Pandora FMS

Pandora FMS es una herramienta de monitorización que ofrece todas las características que necesita una gran empresa para monitorizar su red sin preocuparse por la escalabilidad de esta.

Esta herramienta tiene control de flujo de la red haciendo uso de protocolos como NetFlow, permite el uso de todas las versiones de SNMP, es capaz de mapear toda la red de la empresa a nivel 2 y 3 usando ICMP y SNMP y ofrece como en casi todas las herramientas de monitorización, la creación y configuración de cuadros de mandos y alarmas. También cabe destacar de que ofrece la conexión a los dispositivos mediante SSH o Telnet, igual que Spectrum. [16]

En cuanto a la arquitectura de la aplicación, está compuesta por unos servidores llamados Pandora FMS Server, cada uno tiene su propia base de datos en la que se almacena la información que recoge el servidor de los agentes SNMP y flujos NetFlow, y toda esta información se muestra en una consola (*MetaConsole*) de usuario que recoge la información de todos los servidores que tenga la empresa. Esto permite escalabilidad en la empresa ya que únicamente sería necesario instalar otro servidor pandora y automáticamente se integraría con los demás. [16]

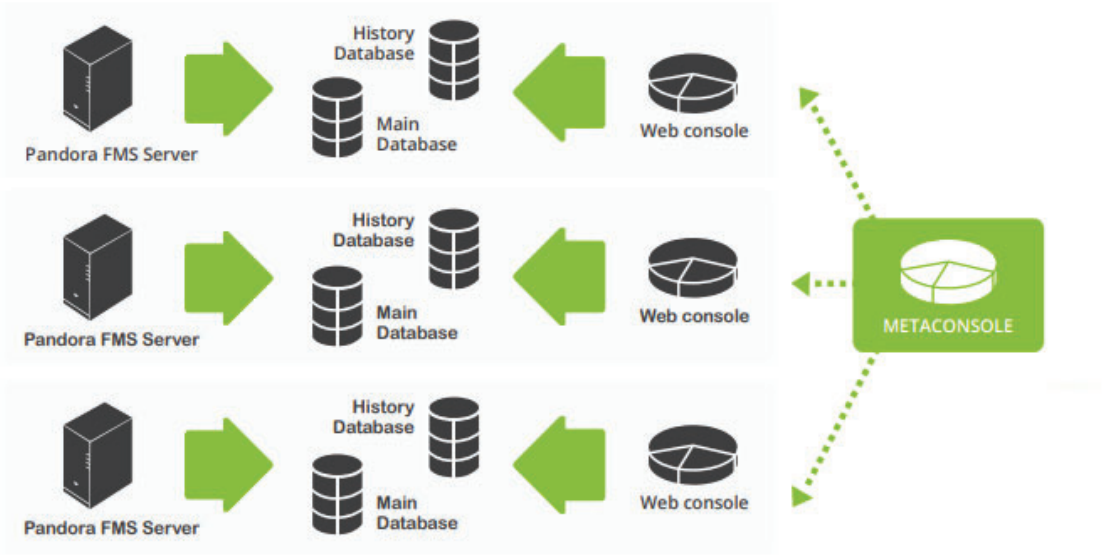

Figura 9 – Diagrama Pandora FMS

En conclusión, esta aplicación, sería una de las mejores opciones para empresas de gran tamaño, ya que ofrece escalabilidad y todas las funciones necesarias para tener monitorizada correctamente una red de gran tamaño.

3 Desarrollo

En este capítulo se explicará el proceso de instalación y configuración de la herramienta y equipos de monitorización *NGeniusOne*. Por lo que este capítulo está dividido en 4 apartados, un primer apartado en el que se nombran los requisitos previos a la instalación y configuración de los equipos, un segundo apartado en el que se explicará todo el proceso de instalación de los equipos en el CPD, un tercer apartado en el proceso de configuración de los equipos, y un último apartado en el proceso de la configuración de la herramienta de monitorización para dar de alta los dispositivos, el análisis de paquetes, creación de cuadros de mando y alarmas.

En este apartado se mostrará el proceso de instalación de manera física en los CPDs del cliente, así como los equipos a instalar y la arquitectura.

La instalación se realizará por duplicado, una para cada CPD del cliente. En cada CPD se instalará un *switch* (*Packet Flow Switch*), una sonda (*InfinitiStreamNG*) y dos taps, por último, se instalará en una máquina virtual una consola. Lo más probable es que en una cuarta fase se duplique esta configuración en cada CPD para tener redundancia, en el caso de fallo de algún dispositivo de la red de gestión o de mantenimiento en la red de gestión.

Primero de todo se mostrarán las especificaciones de cada equipo a instalar en los CPDs, más tarde la arquitectura y por último el proceso de instalación.

3.1 Requisitos

En este apartado se comentarán los requisitos que se han establecido previos a la instalación física y configuración de los equipos.

Lo primero de todo se necesitará tener acceso al CPD y saber la ubicación de los equipos en el CPD junto al cableado a usar para poder realizar la instalación física.

En segundo lugar, se necesitará tener acceso a una VPN para poder acceder por acceso remoto a los dispositivos para realizar su configuración.

En tercer lugar, se necesitará saber el direccionamiento de los equipos más el diseño actual de la red.

Por último, se necesitará asegurarse de que los nuevos equipos tienen acceso a toda la red, es decir los FW/ACL tienen los permisos adecuados.

Por lo que se obtendrán los siguientes requisitos finales:

1. Altas y permisos de acceso a CPD
2. Ubicación de los equipos en CPD, distribución de cableado e identificación de puertos
3. Generación de VPN para acceso remoto a los dispositivos
4. Direccionamiento de los equipos
5. Diseño de red actual
6. Aseguramiento de permisos FW-red de los nuevos equipos

3.2 Equipos

En este apartado se muestran las especificaciones de los equipos que se instalarán en cada CPD y las funciones que tendrán cada uno en la red.

3.2.1 NGenius 5110 Packet Flow Switch

Este equipo de tipo *switch* se encarga de dos funciones principales:

- Recoger el tráfico red que el otorga los puertos espejo (SPAN).
- Enviar la información que recoge de SPAN a diferentes sondas (DPI, IPS, *InfinitiStreamNG*) para analizar el tráfico, crear cuadros de mando, alarmas, etc.

Por lo que, en resumen, este *switch* hará la función de receptor de tráfico del CPD que se quiera analizar y enviara este tráfico a diferentes sondas que usaran estos datos para diferentes funciones.

Figura 10 - NGenius 5110 Packet Flow Switch

Por último, se mostrarán en la siguiente tabla las especificaciones del equipo en cuestión, que sea pedido para realizar la instalación:

Puertos	48 x 1GbE/10GbE/25GbE 6 x 40GbE/100GbE
RU (Rack Unit)	1 RU
Dimensiones	Altura: 44 mm Anchura: 438 mm Profundidad: 473 m
Peso	9.43 kg
Power (AC)	583W (1989 BTU/hr) max
Operating Temperature	0° - 45°C
Storage Temperature	-40° - 70°C

Figura 11 – Especificaciones NGenius 5110 Packet Flow Switch *[17]*

3.2.2 InfinitiStreamNG 6600 Series

A este equipo se le denomina sonda, ya que es uno de los equipos que están conectados al *Packet Flow Switch* (encargado de recoger y enviar los datos recogidos vía SPAN) para recibir datos que este le emite. Esta sonda realiza diferentes funciones que se enumerarán a continuación:

- Alimentar datos a vistas para la creación de cuadros de mando y alarmas
- Crear análisis de los errores de red y aplicación
- Registros de sesión
- Decodificación de paquetes, como pueden ser la eliminación de las etiquetas VLAN
- Conexión directa con la consola web

Figura 12 - InfinitiStreamNG 6600 Series

Por último, se mostrarán en la siguiente tabla las especificaciones del equipo en cuestión, que sea pedido para realizar la instalación:

Puertos	4 x 10GeB
RAM	192GeB
Capacidad	48TB SSD
RU (Rack Unit)	3 RU
Dimensiones	Altura: 132 mm Anchura: 437 mm Profundidad: 648 mm
Peso	37.19 kg
Power (AC)	1000W (3412 BTU/Hr) max
Power (DC)	1042W (3554 BTU/Hr) max
Operating Temperature	10° - 35°C
Storage Temperature	10° - 35°C

Figura 13 – Especificaciones InfinitiStreamNG 6600 Series *[18]*

3.2.3 Tap

Los *taps* son equipos encargados de recoger tráfico de la red y de redirigirlo a un receptor de datos (*Packet Flow Switch*). Estos equipos son una alternativa al uso de puertos espejos (SPAN) en los *switches*. Los beneficios de instalar un *Tap* en vez de activar SPAN en los *switches*, es que, al tener una red de gran tamaño, si se tienen activados en cada *switch* un puerto dedicado a SPAN, se está perdiendo dicho puerto y mucho proceso de CPU, por lo que, si únicamente instalamos un *Tap*, este duplicara el tráfico y lo renviara para su análisis, obteniendo así mayor rendimiento en los *switches* y ahorro de recursos.

Figura 14 – Tap

Por último, se mostrarán en la siguiente tabla las especificaciones del equipo en cuestión, que sea pedido para realizar la instalación:

Puertos	2 x 1GbE/10GbE
Rack Unit	1 U. Esta unidad puede almacenar hasta 20 de estos equipos
Dimensiones	Altura: 44.5mm Anchura: 440mm Profundidad: 256mm
Peso	3.39kg
Power (AC)	2.5W

Figura 15 – Especificaciones Tap

3.2.4 Consola virtual de EngeniusOne

El ultimo equipo del que se hablará, es de la consola, que es la que proporcionará una interfaz para los usuarios y los administradores. Esta consola se instalará de manera virtual con un OVA en VMWARE, y recibirá el tráfico de las dos sondas, usando lo para pintar gráficas, generar análisis, alarmas etc.

Figura 16 - Consola Virtual de EngeniusOne

Por último, se mostrarán en la siguiente tabla las especificaciones del equipo en cuestión, que sea pedido para realizar la instalación:

Puertos	5 Port Gigabit Ethernet (RJ45)
RAM	64GB
Capacidad	8TB
CPU	24 vCPU
RU (Rack Unit)	2 RU
Dimensiones	Altura: 87mm Anchura: 482mm Profundidad: 760mm
Peso	28.6kg
Power (AC)	750W

Figura 17 – Especificaciones Consola Virtual de EngeniusOne *[19]*

3.3 Arquitectura y diseño de la red de monitorización a implementar

Antes de empezar con la explicación de la arquitectura y el diseño de la red se va a comentar el nombre que se usará para cada CPD, que como se he comentado con anterioridad la instalación se realizaría en 2 del cliente. Al primer CPD se le denominará sede 1 y al segundo CPD sede 2.

Ahora que ya se conocen los lugares donde se van a encontrar los equipos, se va a comentar que equipos son estos. La red está formada por un switch un servidor, dos dispositivos para capturar el tráfico y una consola, todos estos equipos están por duplicado en cada CPD a excepción de la consola que estará instalada en un VMWARE en uno de los CPDs, por lo que en total la red tiene 2 servidores, 2 switches. 2 taps y una consola.

Ahora que ya se conocen los equipos que componen la red y los lugares donde se van a encontrar, faltaría saber el direccionamiento que van a tener, sus conexiones entre ellos.

3.3.1 Direccionamiento

La red que se ha asignado para los equipos es la 172.16.216.0/21 con *Gateway* 172.16.216.1, por lo que los equipos estarán en el rango que hay entre la IP 172.16.216.2 – 172.16.223.254. Del rango mostrado, se han asignado las siguientes IPs a los equipos:

	IP/Mascara	Gateway
Packet Switch Flow SEDE1	172.16.217.18/21	172.16.216.1
Sonda SEDE1	172.16.217.19/21	172.16.216.1
Packet Switch Flow SEDE2	172.16.221.18/21	172.16.216.1
Sonda SEDE2	172.16.221.19/21	172.16.216.1
Consola	172.16.221.20/21	172.16.216.1

Figura 18 – Tabla de direccionamiento

Con el direccionamiento ya asignado, también es necesario tener unos servidores DNS y NTP, para poder realizar la configuración de los dispositivos. Los servidores de dominio y NTP que se nos han asignado son los siguientes:

	IP
DNS	10.128.4.45/10.128.66.28
NTP	10.128.4.45/10.128.66.28

Figura 19 – Tabla servicios

Por último, para finalizar con este apartado faltarían por asignar el nombrado de los equipos. Los nombres que se han asignado para cada equipo son los siguientes:

	Nombrado
Packet Flow Switch SEDE1	S1-NS-PFS01
Sonda SEDE1	S1-NS-SON01
Packet Flow Switch SEDE2	S2-NS-PFS01
Sonda SEDE2	S2-NS-SON01
Consola	S2-NS-CON01

Figura 20 – Tabla nombrado

3.3.2 Conexiones

Con el direccionamiento ya planificado, se podrá empezar con la planificación del conexionado.

Lo primero será comentar los puertos que usaremos para el conexionado en cada uno de los equipos; para los PFS usaremos 9 puertos de fibra (10G), para las sondas usaremos 3 puerto de fibra y para los taps 2 puertos de fibra en cada uno.

Una vez conocidos los puertos que se van a usar, comentaremos las conexiones que se realizarán en estos. Los taps se conectarán a cuatro de los puertos de fibra de los PFS, dos para cada *Tap*, la sonda se conectará a dos de los puertos de fibra del PFS y por último al PFS se conectarán a dos puertos de fibra recepción de tráfico SPAN y un puerto de fibra para la recepción de tráfico proveniente de ERSPAN.

Las conexiones comentadas con anterioridad pertenecen únicamente a un CPD, pero como el conexionado va a ser idéntico en los ambos CPD no hay nada más que añadir.

Por último, se van a mostrar unas tablas con las conexiones realizadas:

- CPD SEDE1

S1-NS-PFS01	Tap1	Tap2	S1-NS-SON01	SPAN	ERSPAN
Port1	Port1				
Port2	Port2				
Port3		Port1			
Port4		Port2			
Port5			Port4		
Port6			Port6		
Port7				X	
Port8				X	
Port9					X

Figura 21 – Tabla conexionado de interfaces sede 1

- CPD SEDE2

S2-NS-PFS01	Tap1	Tap2	S2-NS-SON01	SPAN	ERSPAN
Port1	Port1				
Port2	Port2				
Port3		Port1			
Port4		Port2			
Port5			Port3		
Port6			Port5		
Port7				X	
Port8				X	
Port9					X

Figura 22 – Tabla conexionado de interfaces sede 2

3.3.3 Topología final

Para terminar con la arquitectura y el diseño de la red, mostrare la topología final de manera gráfica.

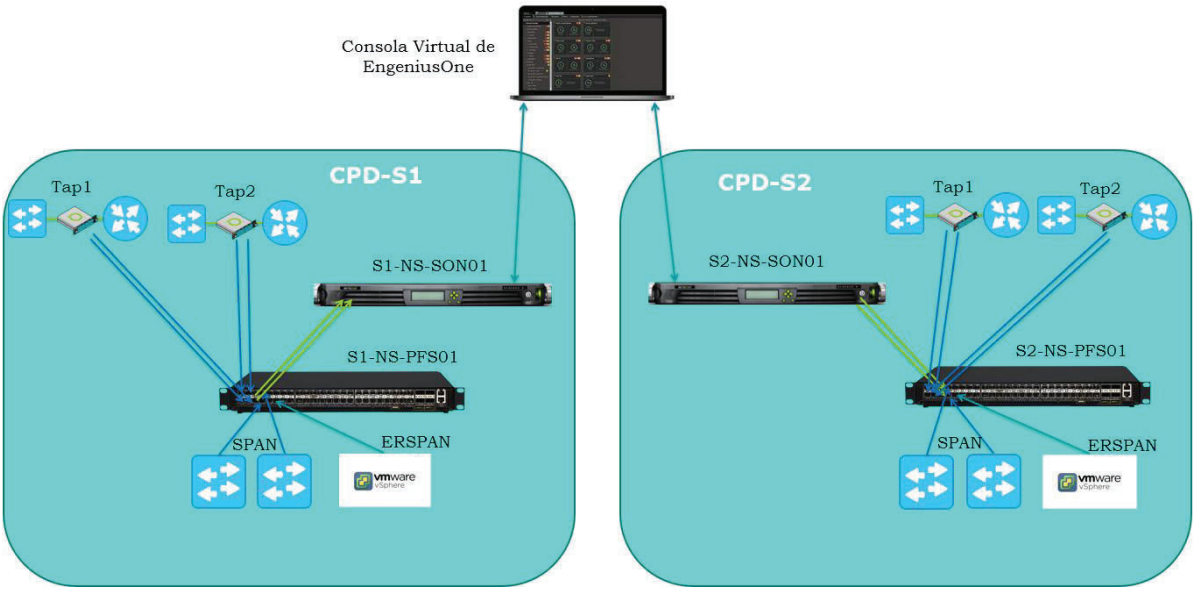

Figura 23 - Topología final

3.4 Instalación física en CPD

En este apartado se comentará el procedimiento que se llevó a cabo para realizar la instalación física de los equipos, que son el PFS (*Packet Flow Switch*), la Sonda y los dos *taps*. Cabe destacar que en este apartado solo comentare la instalación en uno de los CPD (sede 1) ya que es la misma en los dos.

Antes de realizar la instalación es necesario la obtención de los permisos adecuados para acceder al centro de datos. Ya con los permisos obtenidos, se recogerán los equipos y se llevarán al CPD. Para poder realizar la instalación de los equipos se necesitarán 5 U *racks* libres. Con todos estos puntos cumplimentados, se realizarán los siguientes pasos para su instalación en el CPD:

1. Instalación de los equipos: colocar los raíles en los racks correspondientes para poder insertar los equipos, se colocarán en el siguiente orden, sonda (3U), PFS (1U) y *Taps* (1U).
2. Instalación *hardware*: colocar en la sonda la tarjeta de red especializada en las funciones que realiza la sonda, esta tarjeta se conecta a un puerto PCI, y para conectarla de manera segura es necesario ponerse una pulsera estática.
3. Configuración de los equipos: la configuración básica, que es la IP, mascara, Gateway, servidor DNS y NTP.

Para configurar el PFS primero es necesario darle alimentación. Con la alimentación ya suministrada al PFS, habrá que conectarse con un ordenador externo al puerto de mantenimiento del PFS, en el caso de este equipo es el ETH0. Como la IP por defecto del PFS es la 192.168.1.1/24 habrá que

configurar una IP en el puerto del ordenador externo que esté en ese rango (192.168.1.1 - 254) para poder acceder a dicho equipo, en nuestro caso configuramos la IP 192.168.1.2. Realizados estos pasos se accederá al equipo sin problemas y se configurará.

La configuración de la sonda lleva un proceso completamente diferente al del PFS. Primero de todo se deberá alimentarlo y ya con el equipo alimentado tenemos que instalar el sistema operativo Linux insertando un disco DVD en la sonda. Con el sistema operativo ya instalado se expulsará el disco del SO y se insertará uno que instala el software de la sonda, cuando el software ya está instalado, ya se podrá configurar la sonda.

Por último, los *taps* no necesitan configuración ya que son equipos pasivos sin inteligencia en la red, que solo se encargaran de copiar el tráfico y pasárselo al PFS.

A continuación, se mostrará la configuración realizada en cada equipo, incluyendo la configuración en ambos CPDs:

- Sede 1

Equipo	Packet Switch Flow	Sonda (InfinityStream)
Puerto	MNGT	ETH0
IP/Mascara	172.16.217.18/21	172.16.217.19/21
Gateway	172.16.216.1	172.16.216.1
DNS	10.128.4.45/10.128.66.28	10.128.4.45/10.128.66.28
NTP	10.128.4.45/10.128.66.28	10.128.4.45/10.128.66.28

Figura 24 - Tabla direccionamiento sede 1

- CPD Sede 2

Equipo	Packet Switch Flow	Sonda (InfinityStream)
Puerto	MNGT	ETH0
IP/Mascara	172.16.221.18/21	172.16.221.19/21
Gateway	172.16.216.1	172.16.216.1
DNS	10.128.4.45/10.128.66.28	10.128.4.45/10.128.66.28
NTP	10.128.4.45/10.128.66.28	10.128.4.45/10.128.66.28

Figura 25 – Tabla direccionamiento sede 2

En cuarto lugar, se instalará los SFPs de fibra (10G) en los cuatro puertos de la tarjeta red de la sonda y 8 en el PFS, y también 8 SFPs de cobre (1G) en el PFS. Igualmente se tendrán que poner tapones en los puertos sin utilizar para evitar la entrada de polvo en ellos.

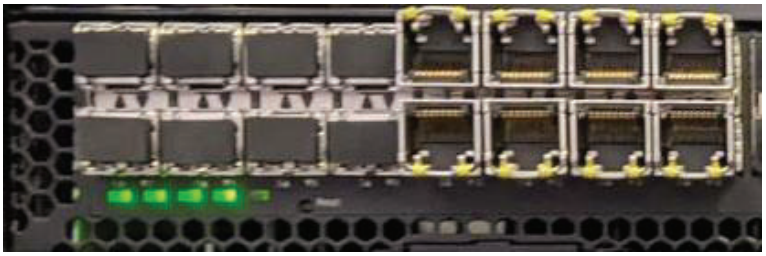

Figura 26 – SFPs PFS sede 1

En la imagen se muestran los SFPs instalados en el PFS, los 8 de la izquierda son los de fibra y los de la derecha son los de cobre.

Figura 27 – SFPs Sonda sede 1

En esta última imagen se muestran los SFPs colocados en los puertos de la tarjeta red de la sonda con sus correspondientes tapones.

En último lugar se realizarán las conexiones con los puertos en los que se configurarán las IPs y donde se realizarán pruebas sobre ellos para comprobar que la configuración realizada funciona correctamente.

Figura 28 – Parte delantera Sonda sede 1

En esta imagen se muestra la parte frontal del armario, donde se puede ver de abajo a arriba la sonda, el PFS y los taps (arriba a la izquierda). También se puede ver la conexión con el puerto de MGNT del PFS, que es el puerto en el que está configurada la IP (En esta imagen no se visualizan las conexiones que hay entre los taps y el PFS, y las conexiones que hay entre el PFS y la sonda,

esto es porque estas conexiones las realizara el cliente, ya que solo se configuró la instalación inicial de los equipos en los racks).

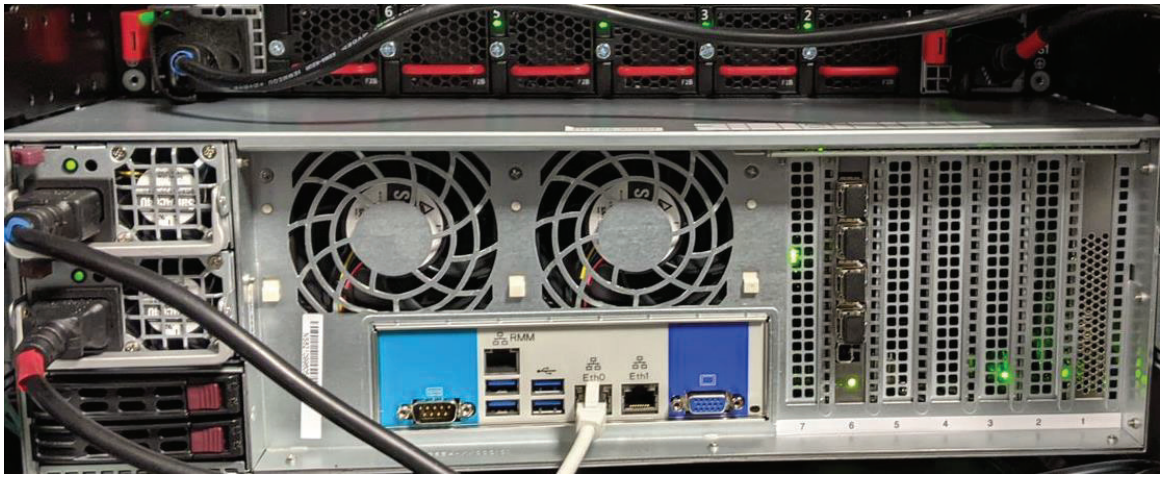

Figura 29 – Parte trasera Sonda sede 1

En esta última figura, se muestra la parte trasera del armario, donde se ven las conexiones de alimentación con la sonda y el PFS, y también la conexión con el puerto ETH0 de la sonda, que es en la que se configuró la IP.

Por último, se mostrará como quedó la instalación en el otro CPD (sede 2).

Figura 30 – Taps, PFS y Sonda de sede 1

En esta imagen se pueden visualizar la sonda, el PFS y los taps instalados en el CPD de sede 2.

3.5 Prueba de funcionamiento inicial

En esta prueba de funcionamiento inicial, se harán pruebas sobre la sonda y consola para asegurarnos de que las funciones de estás operan correctamente, como son las alarmas, cuadros de mando, análisis de paquetes, detección de protocolos, etc. Cabe destacar que esta prueba se realizara en remoto.

Para la realización de esta prueba, el cliente conectará el tráfico de salida de uno de los puertos del antiguo captador de tráfico con un puerto de la sonda (ambos puertos de 10G por lo tanto esta conexión es de fibra), para que así pueda llegar el tráfico actual de la red a nuestra sonda aplicando los filtrados ya existentes en el antiguo captador. De esta manera nuestra sonda captará este tráfico de la red y se podrá hacer pruebas configurando cuadros de mando, alarmas en la consola, etc.

3.5.1 Configuración de filtros de trafico

Antes de comprobar si el tráfico llega o no correctamente a la sonda para que este sea procesado, se configurará un filtro de tráfico, encargado de seleccionar el tráfico que se enviará a la sonda.

Para poder configurar un filtro de tráfico es necesario conocer las IP de los equipos destino y origen que generan el tráfico, el protocolo de aplicación (HTTPS, HTTP, DNS) del tráfico a capturar y por último el protocolo de transporte (TCP o UDP).

En nuestro caso se decidirá únicamente tomar el tráfico de un balanceador que se encuentra en la misma red que la sonda. Para ello se configurará el siguiente filtro de tráfico:

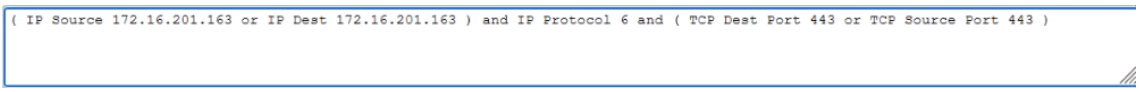

Figura 31 – Filtro del tráfico a analizar

En este filtro de tráfico se verá que se han tomado como IP de origen y destino la 172.16.201.163, como protocolo de transporte TCP y como protocolo de aplicación 443 que se refiere a HTTPS.

Por lo tanto, cuando un paquete en su cabecera IP tenga en los campos destino u origen la IP 172.16.201.163 junto con el campo de protocolo relleno con el código que identifica TCP y por último que en el segmento TCP en los campos de puerto destino u origen estén rellenos con 443 que identifica el protocolo HTTPS, se reenviarán estos paquetes a nuestra sonda para procesarlos, y los paquetes que no cumplan con el filtro no se reenviaran.

A continuación, se mostrarán como deberán de ser la cabecera IP y el segmento TCP para que el filtro acepte los paquetes.

- Cabecera IP:

Versión	Longitud	Campo DS	Longitud del Paquete	
Identificación			Bandera	Desplazamiento del Fragmento (Offset)
Time to Live (TTL)		Protocolo -> 0x06 (TCP)	Suma de Comprobación (Checksum)	
Dirección IP de Origen -> 172.16.201.163				
Dirección IP de Destino ->172.16.201.163				

Figura 32 - Cabecera IP

- Segmento TCP:

Puerto de Origen -> 443 (HTTPs)			Puerto de Destino -> 443 (HTTPs)
Número de secuencia			
Número de reconocimiento			
Offset	Reservado	Bits de Bandera (Flag)	Ventana
Suma de Control (Checksum)			Urgente

Figura 33 - Segmento TCP

Es importante destacar que para el caso de la dirección origen y destino, y el puerto origen y destino, no tienen por qué estar rellenos ambos con lo mismo respectivamente, ya que en el filtro se especifica un "*or*".

3.5.2 Prueba de captura de trafico

Con los filtros ya configurados el siguiente paso será comprobar si está llegando tráfico a la sonda por el puerto indicado por el cliente. Para comprobar esto se realizará una conexión por SSH a la sonda de la sede 2 que es en la que se hará la prueba. Usando las credenciales correspondientes nos conectaríamos a la sonda. Ya dentro de la maquina Linux, se insertará el siguiente comando "*./localconsole*" para ejecutar el programa administrador de la sonda. Al ejecutar el programa se nos muestra lo siguiente:

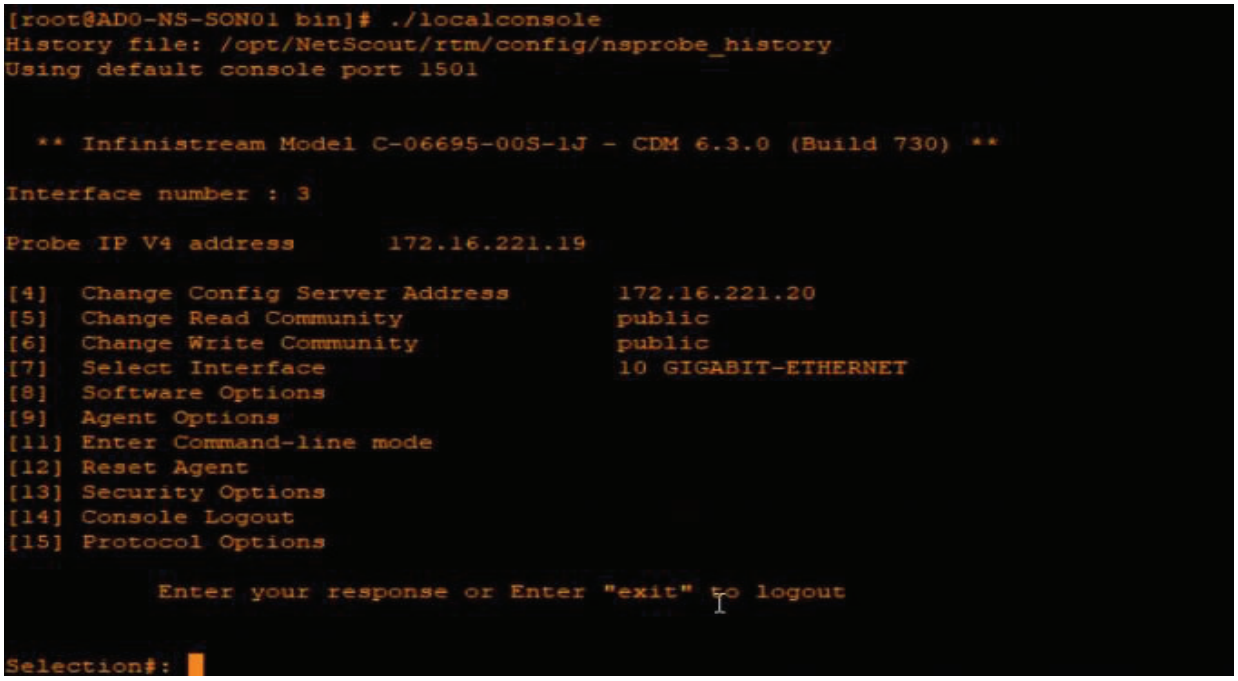

Figura 34 – Resultado ejecución comando ./localconsole

Seleccionando la opción 11, y escribiendo en la línea de comandos "11 se nos activará el modo de línea de comandos. En este modo se insertará el comando "*get dump perf 0*" que nos mostrará el tráfico en todas las interfaces de la sonda, en este caso solo la interfaz 3 tiene tráfico ya que la prueba solo se realizará sobre una interfaz de la sonda.

Estos datos que recibe esta interfaz no están todavía pintando datos en la consola web ya que la interfaz no está activada en la consola. Pero antes de pasar a la consola se terminará con una configuración más en la sonda, que consiste en configurar los recursos que se otorgarán a cada interfaz de la sonda.

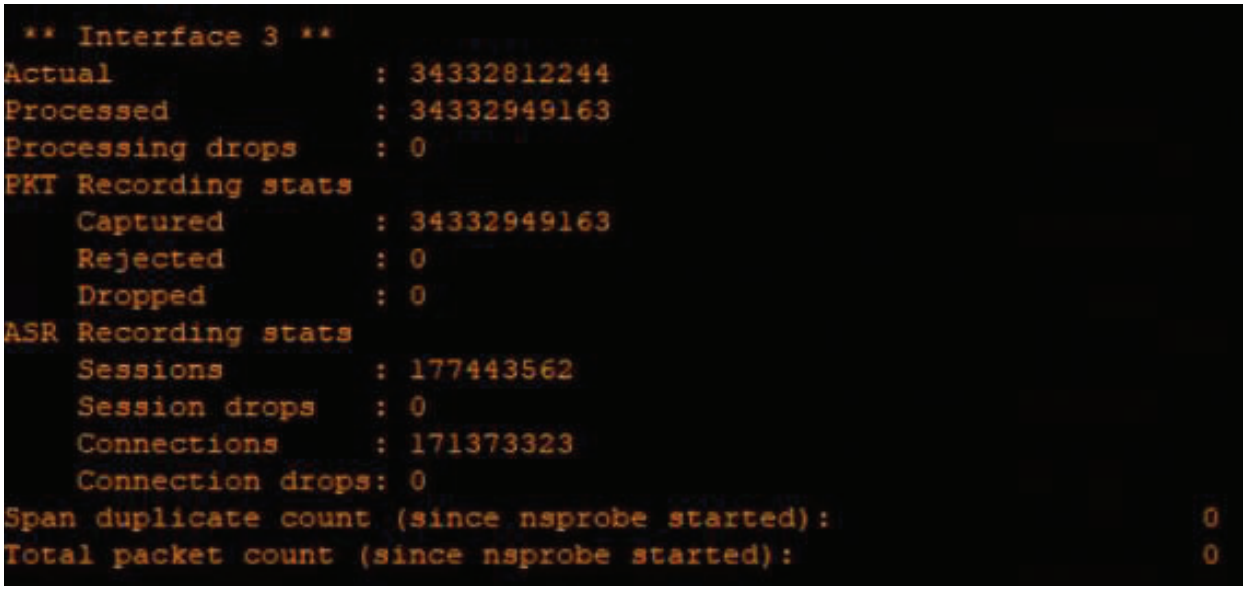

Figura 35 – Estado de tráfico interfaz 3 de la sonda

Se ejecutará el comando "*set tsa all*" para poder configurar el porcentaje de recursos que se usará en cada puerto de la sonda, en nuestro caso se

configurarán dos por el momento; la interfaz 3 que tiene tráfico y la 5 que no tiene. Para ello se dividirá el porcentaje entre las 4 interfaces de la sonda, a las interfaces 3 y 5 se les dará un 49% y a las restantes un 1%.

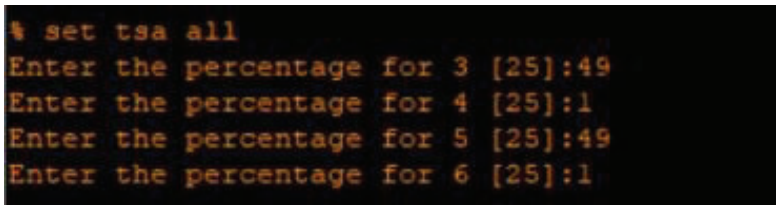

Figura 36 – Porcentaje de uso de las interfaces de la sonda

Para finalizar con la línea de comandos se insertará el siguiente comando "*set tsa commit*" que aplicará los cambios que se han realizado en la sonda.

3.5.3 Configuración de puertos receptores de trafico

Ahora que ya se han realizado las comprobaciones y configuraciones propias sobre las interfaces de la sonda, habrá que conectarse a la consola para configurar los puertos que serán los encargados de receptar el tráfico a analizar. La conexión a la consola se realizará por HTTPS. Ya en la consola se verá que están conectadas dos máquinas, que son las dos sondas, la de sede 1 y la de la sede 2.

Status	Health Status	Device	Name	Address	Alias	Type	Interfaces (Act)	Interfaces (Inact)	Model	Version	Upgrade	Provisioning Profile	Notes
		IS	AD0-NS-SON01	172.16.221.19		InfiniStream	2	2	C-06695-00S-1 J	6.3.0 Build 730	Up to date	O	
		IS	H12-NS-SON01	172.16.217.19		InfiniStream	3	1	C-06695-00S-1 J	6.3.0 Build 730	Up to date	O	

Figura 37 – Visualización de las sondas desde la interfaz

Centrándonos en la sonda de sede 2 que es con la que se realizará la prueba: activaremos las interfaces que queremos que sean las que generen datos, para ello se *clicará* en la máquina de sede 2 y se seleccionarán las interfaces 3 y 5, activándolas. En este caso de momento como se ha visto solo llega tráfico por la interfaz 3.

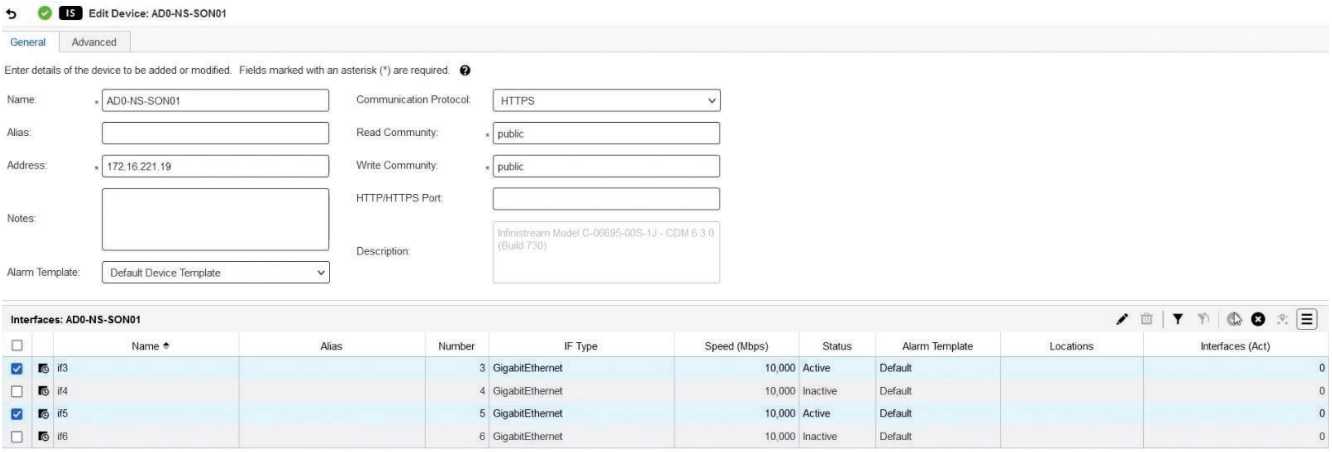

Figura 38 – Configuración de la sonda desde la interfaz

Ya con las interfaces activadas, la consola creará cuadros de mando y alarmas por defecto, por lo que para comprobar el funcionamiento de esto habrá que ver si se han creado y si tienen sentido.

3.5.4 Configuración de cuadros de mando y alarmas

En este apartado se comprobará el funcionamiento de los cuadros de mando y las alarmas sobre el tráfico de la interfaz configurada en el apartado anterior.

Se harán dos comprobaciones: una primera con el tráfico sin el filtro configurado en el apartado 3.5.1 y otra con el filtro.

Una vez comprobado el cuadro de mando que se ha generado sin el filtro, se apreciará que este está recibiendo todo tipo de tráfico. Como se puede ver en la figura 39 hay tráfico MYSQL, HTTPS, HTTP, LDAP, etc.

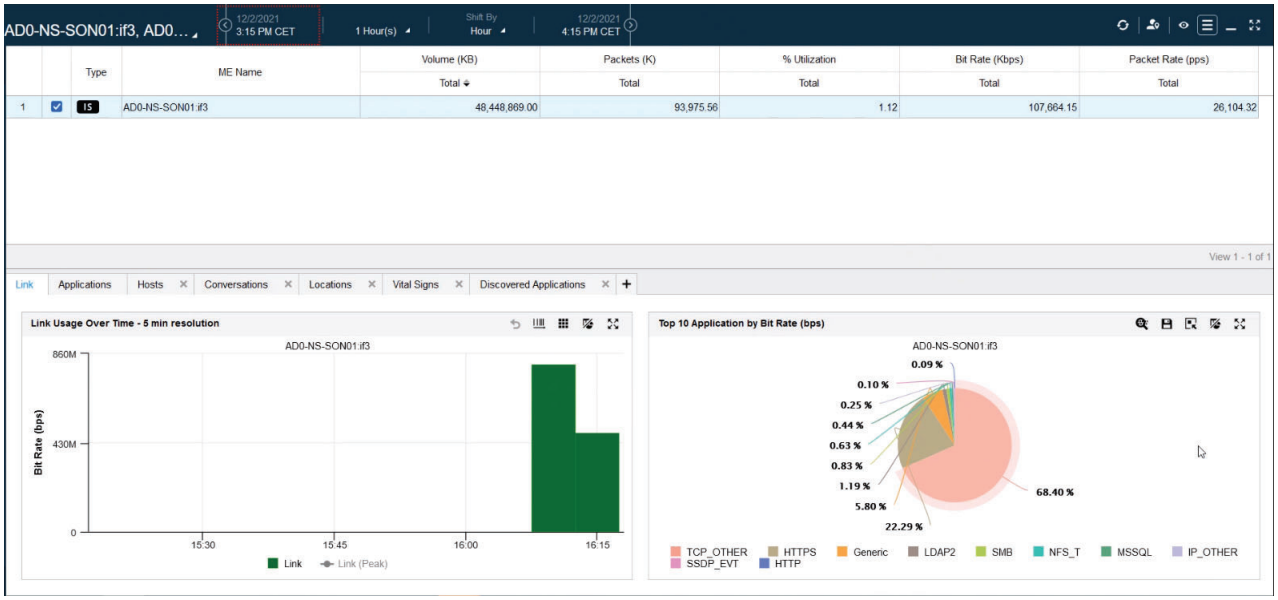

Figura 39 – Dashboards de tráfico 1

Las alarmas aparecerían en esta misma pantalla, pero en este caso no se ha generado ninguna.

Por último, se hará la prueba activando el filtro. Al activar el filtro configurado en el apartado 3.5.1, se genera el siguiente cuadro de mando:

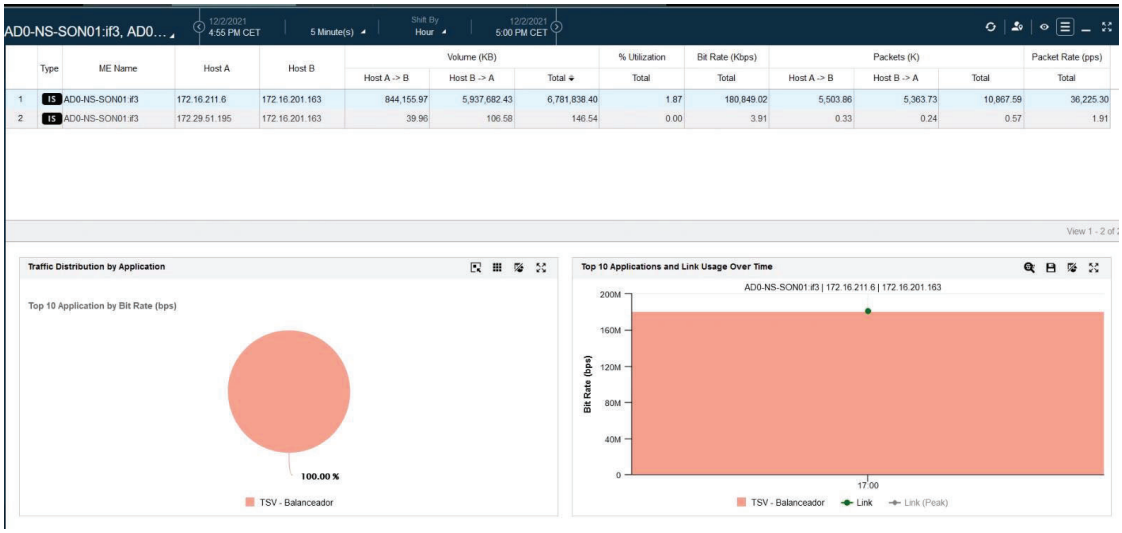

Figura 40 - Dashboards de tráfico 2

En efecto observando la imagen anterior se puede ver que solo se recibe un tipo de tráfico en la sonda, que es el tráfico HTTPS de los balanceadores, que es justo lo que se configuró en el filtro. Por lo tanto, todas las comprobaciones y configuraciones sobre la sonda han sido un éxito.

Gracias a esta prueba podemos comunicarle al cliente que la sonda y la consola tienen un comportamiento normal y que están listos para empezar la intervención y posteriormente la migración.

3.6 Intervención

En este apartado se explicará la intervención que se tuvo que realizar sobre los equipos desplegados en los CPDs.

Como nuestro cliente es una entidad pública, el presupuesto aportado al proyecto es público, por lo que para comprobar que este dinero público se ha usado de manera no fraudulenta es necesario la realización de una intervención, en la que el interventor o interventora debe de comprobar que los equipos instalados son los que figuran en los gastos del presupuesto.

Para la realización de la intervención el interventor o interventora primero debía de comprobar los equipos físicamente en ambos CPDs y más tarde hacer alguna comprobación de las características de los equipos que solo es posible obtenerlas por consola.

Como ya he comentado primero se hizo la comprobación física de los equipos y luego yo me encargue de darle los datos por consola que el interventor o interventora me solicitaban. El primer dato que me pidieron fue la comprobación de que la sonda tenía una memoria RAM de 196 GB y 12 discos de 4 TB cada uno. Para obtener esta información nos conectamos por SSH a la consola y usando el comando top podemos ver la RAM que consume cada proceso, así como el total disponible en la máquina.

Para sacar el dato de los discos primero debemos ejecutar un programa que nos permite sacar información sobre el equipo *"./localconsole"* y ya usando el comando "*raidconfig disk info*" obtenemos los 12 discos junto con su número de serie y el tipo de disco.

Por último, la interventora nos pidió los números de serie de los PFS. Para sacar los números de serie de estos equipos únicamente es necesario conectarse por HTTPS a la interfaz de los PFS.

Con esto último la interventora quedó satisfecha y la intervención fue un éxito.

3.7 Migración

El objetivo final del cliente es realizar una migración de la herramienta antigua que usan actualmente a esta nueva que se ha instalado. Este proceso de migración es muy largo, ya que hay que clonar lo que hay en la antigua herramienta a la nueva antes de desactivar por completo la antigua.

Para realizar esta migración la herramienta antigua tiene una opción de clonación de algunas de las configuraciones de la herramienta, por lo que usando esa función gran parte de la configuración de la herramienta la

tendríamos en la nueva. Pero otra gran parte de la configuración de la herramienta antigua habría que hacerla desde cero en la nueva.

Actualmente este proceso está inconcluso ya que para realizar esta migración es necesario tener acceso a la herramienta vía remoto haciendo uso de una VPN, y esta última todavía no nos la han otorgado.

Por lo que de momento estamos esperando a tener acceso para comenzar con la migración.

4 Conclusiones y líneas futuras

En este capítulo se presentan los resultados y conclusiones junto con algunas líneas futuras de desarrollo para poder mejorar el proyecto.

4.1 Resultados y conclusiones

Con este proyecto nos hemos familiarizado con los conceptos básicos necesarios para comprender la importancia de la monitorización de una red y los pasos que hay que seguir para desplegar una herramienta de monitorización en una red de gran escala.

En el documento hemos presenciado el despliegue de la herramienta siguiendo todos los pasos requeridos para realizarlo: solicitar los equipos que contendrán la herramienta y funciones de esta, localizar la red donde se instalarán estos equipos, asignarles una IP, instalarlos físicamente en el centro de procesamiento de datos (CPD), y realizar las pruebas iniciales de funcionamiento.

El resultado obtenido es una herramienta de monitorización de última generación, instalada en CPD funcionando 24/7 y capaz de analizar el tráfico en una red de gran tamaño, mediante la creación de cuadros de mando, y mediante la generación de alarmas y avisos.

Gracias a esta herramienta nuestro cliente ahora será capaz de localizar los puntos de saturación de la red, saber porque la red está saturada en ese punto y solucionarlo, junto con otras funciones que incluye la herramienta.

Se han cumplido todos los objetivos del proyecto, aunque la parte de migración del proyecto se ha dejado simplemente esbozada a nivel teórico debido a la gran cantidad de trabajo y tiempo que supondría.

El proyecto aún tiene mucho margen de mejora. A continuación, se expondrán algunas ideas en la siguiente sección.

4.2 Futuras líneas de desarrollo

En esta sección se muestran algunas ideas acerca de cómo mejorar el proyecto.

Para empezar, sería conveniente añadir más equipos "*tap*", de esta manera se podrían recoger desde más puntos más tráfico red ya que actualmente teniendo solo dos es escaso.

Otro aspecto que se podría mejorar es la instalación de un equipo que se encargase de analizar tráfico vía NetFlow, ya que actualmente este proceso está sin uso dentro de la herramienta.

Un buen añadido a este proyecto sería realizar parte de la monitorización con herramientas cloud, de esta manera se obtendrá un gran ahorro de recursos en los CPDs del cliente.

También un buen añadido a este proyecto sería cambiar el modo en el que se renvía el tráfico a la herramienta de monitorización. Como ya he comentado con

anterioridad, una buena mejora seria añadir más taps para que recojan tráfico de diferentes puntos, pero todo esto se podría sustituir por SDN, ya que facilitaría todo este proceso y a cambio se obtendrían un ahorro en costes y no se tendría tanta complejidad en la red.

Por último, quedaría pendiente terminar la migración de la herramienta, ya que es el objetivo de esta actuación.

5 Análisis de impacto

En este capítulo se realizará un análisis del impacto potencial de los resultados obtenidos durante el desarrollo del proyecto.

A nivel personal este proyecto me ha servido para desarrollar mis conocimientos sobre diferentes áreas. He adquirido importantes nociones de diferentes herramientas de monitorización, también he podido adquirir conocimientos en el área de montaje de equipos en CPDs y por último también conocimientos en toda el área de configuración de equipos de red, así como nociones del funcionamiento de una red. Además, gracias a esta instrucción adquirida he sido capaz de realizar montajes en CPDs y ayudar a administrar otras herramientas de monitorización.

A nivel económico y empresarial, se ha conseguido para la empresa un nuevo proyecto que le genera ingresos y le abre las puertas a un nuevo cliente.

Por otra parte, sería conveniente analizar el potencial impacto del proyecto haciendo referencia a los objetivos de Desarrollo Sostenible ODS de la agenda 2030.

El primer objetivo a tener en cuenta es el objetivo 12: Producción y Consumo Responsables. Gracias al uso de esta nueva herramienta, nuestra empresa ahorrara recursos y gastos, ya que esta nueva herramienta hace uso de menos equipos que la anterior. Por lo que se cumpliría este objetico ya que la empresa haría un consumo responsable cambiando de una herramienta que usaba recursos innecesarios a una que usa los justos. El objetivo 12 busca que el consumo y la producción mundial que dependen del uso del medioambiente natural y de los recursos no tengan un efecto tan destructivo sobre el planeta, por lo que esta solución ayuda a lograr este objetivo ya que al usar menos recursos sobre la nueva herramienta se está consiguiendo ayudar al medioambiente.

El segundo objetivo sería el 13: Acción por el clima. Como se ha explicado en el párrafo anterior, la informática produce bastantes desechos perjudiciales para el medioambiente. El objetivo 13 busca adoptar medidas para reducir el impacto del cambio climático y nuestro proyecto ha permitido reducir el número de equipos en un CPD, por lo que de esta manera conseguimos ahorrar recursos que son nocivos para el medioambiente.

El tercer objetivo sería el 8: Trabajo decente y crecimiento económico. Gracias a este nuevo proyecto ha surgido la necesidad de contratar más personal para su realización, por lo que gracias a este proyecto se han generado nuevos puestos de trabajo en el mercado laboral.

El cuarto objetivo sería el 9: Industria, innovación e infraestructura. Con este proyecto el cliente ha conseguido innovar su antiguo sistema de monitorización, consiguiendo así un progreso tecnológico en esta área y obtenido nuevas soluciones con las que antes no contaba.

Por último, hay que mencionar también el objetivo 3: Garantizar una vida sana y promover el bienestar para todos en todas las edades. Este proyecto tiene como cliente un servicio de salud que incide directamente en la población, y su objetivo es conseguir que todo el sistema funcione correctamente. Por lo que nuestro proyecto es esencial para monitorizar todos los sistemas informáticos de los hospitales de dicho cliente.

6 Bibliografía

[1] R. 1157 . Available: https://datatracker.ietf.org/doc/html/rfc1157.

[2] M. Wittmann, 23 March 2017 . Available: https://blog.paessler.com/snmp-monitoring-via-oids-mibs.

[3] R. 792. Available: https://datatracker.ietf.org/doc/html/rfc792.

[4] R. 854. Available: https://datatracker.ietf.org/doc/html/rfc854.

[5] R. 4253. Available: https://datatracker.ietf.org/doc/html/rfc4253.

[6] R. 5424. Available: https://datatracker.ietf.org/doc/rfc5424/.

[7] 17 September 2004. Available: https://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/ios-netflow/product_data_sheet0900aecd80173f71.html.

[8] S. Singh, 22 January 2019. Available: https://www.cisco.com/c/en/us/support/docs/switches/catalyst-6500-series-switches/10570-41.html.

[9] E. Martínez. Available: https://soporte.syscom.mx/es/articles/1506878-ubiquiti-unifi-dpi-que-es-como-funciona-para-que.

[10] 2005. Available: https://www.splunk.com/en_us/data-insider/what-is-mean-time-to-repair.html.

[11] 6 October 2021. Available: https://techdocs.broadcom.com/us/en/ca-enterprise-software/it-operations-management/spectrum/10-4/integrating/ca-performance-management-and-ca-spectrum.html.

[12] 4 October 2019. Available: https://techdocs.broadcom.com/es/es/ca-enterprise-software/it-operations-management/unified-infrastructure-management/8-1/procedimientos-iniciales/descripci_n-general-de-la-arquitectura-de-ca-uim.html.

[13] Viewtinet. Available: https://viewtinet.com/products/.

[14] Available: https://www.netscout.com/sites/default/files/2021-06/EPDS_025_EN-2101%20-%20nGeniusONE.pdf.

[15] entuity. Available: https://www.parkplacetechnologies.com/es/entuity/.

[16] Pandora. Available: https://pandorafms.com/es/.

[17] Available: https://www.netscout.com/sites/default/files/2019-10/PFSPDS_017_EN-1902%20-%20nGenius%205110%20Packet%20Flow%20Switch.pdf.

[18] Available: https://resources.netscout.com/data-sheets/infinistreamng-hardware-appliance-data-sheet.

[19] [Available: https://www.netscout.com/sites/default/files/2021-08/EPDS_026_EN-2102%20-%20nGeniusONE%20Server%20Data%20Sheet.pdf.

Este documento esta firmado por

Firmante	CN=tfgm.fi.upm.es, OU=CCFI, O=ETS Ingenieros Informaticos - UPM, C=ES
Fecha/Hora	Thu Jan 20 17:08:55 CET 2022
Emisor del Certificado	EMAILADDRESS=camanager@etsiinf.upm.es, CN=CA ETS Ingenieros Informaticos, O=ETS Ingenieros Informaticos - UPM, C=ES
Numero de Serie	561
Metodo	urn:adobe.com:Adobe.PPKLite:adbe.pkcs7.sha1 (Adobe Signature)