

Netflow Analyzer de SolarWinds

Cris Taisigüe B97785 & Erick Vasquez B98334

Informática Empresarial, Universidad de Costa Rica

Curso de Redes en los Negocios IF-6000

Juan Jose Morales Hernández

21 de septiembre del 2021

Introducción

El propósito principal de este trabajo de investigación es la explicación teórica sobre Netflow Analyzer de SolarWinds. Abarcando por el uso de herramientas como SNMP, asimismo, se analizará las características de la herramienta el Analizador y Monitor Netspot.

Este tipo de herramientas son frecuentemente usadas por organizaciones que desean contar con un mayor control de los servicios de redes de sus empresas. La página oficial de SolarWinds define Netflow Analyzer como:

Un protocolo de red desarrollado por Cisco para recopilar información sobre el tráfico IP y supervisar el flujo de la red. Al analizar los datos de NetFlow, se puede obtener una imagen del flujo y el volumen de tráfico de la red¹.

(What Is Netflow? Analyze Network Flow and Data, n.d.)

El funcionamiento de NetFlow es por medio la creación de un registro de flujo, por el cual el servidor responde la solicitud del cliente y el cliente responde al servidor. Este tipo de funcionamiento se conoce por medio de la tecnología unidireccional. El objetivo de Netflow es el monitoreo de registros de un flujo de datos que brinda el tráfico de red, con el fin de analizar de forma más efectiva estos datos.

La importancia que se le atribuye a esta investigación en nuestro contexto consiste en poder erradicar el desconocimiento presente acerca del tema a tratar con la finalidad de que el público objetivo comprenda el concepto de este.

Para concretar lo anteriormente mencionado, en esta investigación se proporcionará una base teórica al explicar y difundir los aspectos más relevantes en lo que se refiere al tema tratado de SNMP, y los softwares asignados.

¹Traducción y adaptación al idioma español: NetFlow is a network protocol developed by Cisco for collecting IP traffic information and monitoring network flow. By analyzing NetFlow data, you can get a picture of network traffic flow and volume. [Fuente: propia]

Marco Teórico

En este capítulo se plantean brevemente algunos trabajos que sirven de antecedentes de la investigación, las bases teóricas referidas a aspectos sobre Netflow Analyzer de SolarWinds.

Antecedentes

Varios son los autores que se han dedicado a investigar sobre las implementaciones de herramientas de monitoreo del tráfico de redes para un mejor rendimiento en las organizaciones.

Resultado de investigaciones destacan el uso de herramientas como Netflow para la recolección de datos de tráfico de red el cual, facilita en la detección de actividad sospechosa, por ende, comúnmente se utiliza para detectar técnicas de ciberataques como el Watering Hole².

NetFlow se ha convertido en un protocolo de red con el fin de monitorear todos los aspectos con la red de banda ancha IP, creado por la compañía de red y seguridad, Cisco Systems, para recolectar información sobre tráfico IP. Se encuentran disponibles en varias distribuciones del sistema operativo Linux. Existen distintas compañías que realizan software a partir de este protocolo, una de ellas es en la que se desarrollará esta investigación, el cual es SolarWinds.

Recientes investigaciones realizadas por Zambrano Montenegro demuestran que Netflow es el mejor protocolo con respecto a similares en el mercado (2015). Dado que Netflow utiliza el flujos como tipo de información, asimismo recolecta desde pequeñas hasta grandes cantidades de datos gracias a que utilizan datos de la capa de enlace y de la capa de

² Watering Hole es una estrategia de ataque informático en la que un atacante adivina u observa qué sitios web utiliza a menudo una organización e infecta uno o varios de ellos con malware. [Fuente: https://en.wikipedia.org/wiki/Watering_hole_attack]

transporte, esto se debe a qué el desarrollo de tecnología está basada en software y no en hardware.

Existen protocolos como Sflow, aunque este se desarrolla por medio de un chip físico, el cual puede traer inconvenientes como por ejemplo solo obtiene parcialmente los paquetes de datos. El protocolo que es similar a Netflow es IPFIX, a diferencia de Netflow este recolecta los datos en forma de muestra aleatoria.

La mayoría de los estudios realizados citan que Netflow Analyzer permite obtener datos por medio de secuencias constantes de tráfico de red, asimismo tiene la habilidad de poder procesar en tiempo real cuadros. Con esto sabemos quienes la utilizan y su fin, facilitando la búsqueda de cuellos de botella y los excesos de banda ancha.

En este sentido vale la pena mencionar el trabajo de Gede Barkah Widagdo el cual nos indica que al utilizar herramientas como Netflow Analyzer puede solventar ataques de ciberseguridad en muy poco tiempo.

Por lo tanto, los principales componentes para detectar la amplificación NTP son la monitorización del ancho de banda; la monitorización del ancho de banda se utiliza para registrar el tráfico en bits por segundo, mientras que los otros componentes son el analizador de flujo de red, la salida de este analizador son los paquetes por segundo, la dirección IP de origen, la dirección IP de destino, los protocolos, el número de puerto y el tamaño del paquete.

(Barkah Widagdo, 2016, p. 81)³

Cabe destacar que Gede Barkah Widagdo (2016) encontró un ataque en tan solo dos minutos por medio el software, “Al final pudimos detectar la amplificación NTP incluyendo

³ Traducción de inglés a español: So the main components to detect NTP Amplification is a bandwidth monitoring; bandwidth monitoring used to record traffic in bits per second, whereas the other components is the network flow analyzer, the output of this analyzer are packet per second, source IP address, destination IP address, protocols, port number and size of packet. [Fuente: propia]

la dirección IP de origen, la dirección IP de destino del objetivo del ataque, y los protocolos de aplicación en menos de 2 minutos.”(Barkah Widagdo, 2016, p. 81)

Un aporte importante presenta S.N (2020) sostiene que el software puede cubrir cualquier tipo de redes, ya sea LAN, WLAN o WAN, a la vez puede con servicios en la nube “se instalan en Windows Server y están escritas en una plataforma común para que puedan interoperar. Esta comunicación permite utilizar una serie de módulos comunes, incluyendo PerfStack, que muestra los recursos básicos de cada aplicación y su estado actual.” (S.N, B, 2020)

De allí que el presente trabajo pretende exponer y contestar conceptos qué abarcan el software de Netflow Analyzer de SolarWind y herramientas como SNMP.

Desarrollo

I. Historia y versiones de SNMP

Simple Network Management Protocol (SNMP) es un estándar para el control de redes usado en redes TCP/IP. Utiliza routers y equipos de servidor como host de redes donde se implementa de tipo Netflow para su administración.

En el modelo OSI se encuentra en la capa de aplicación, el cual automatiza el intercambio de información del uso que se le da a todos los dispositivos de red, por ejemplo puentes, routers y nodos. Algunas de las bondades de este estándar es la posibilidad de administrar de forma remota el cual, en tiempos que el trabajo remoto es un hecho, facilita el control del rendimiento de la red de forma remota. A la vez, se puede encontrar y resolver problemas y planificar la banda ancha.

Algunas de las características con las que cuenta SNMP son:

1. Configurar dispositivos remotos.
2. Seguimiento de la velocidad de procesamiento.
3. Recopilación de datos.
4. Detectar errores en la red o accesos inadecuados.
5. Puede configurar las alarmas que se desencadenarán en los dispositivos de red cuando se produzcan ciertos sucesos
6. Puede supervisar el uso general de la red para identificar el acceso de un grupo o usuario, y los tipos de uso de servicios y dispositivos de la red.

Para clarificar lo anterior, es importante mencionar las versiones que ha contado SNMP a lo largo de su historia. En total cuenta con 3 versiones, las cuales se explicaran a continuación:

SNMP versión 1: se utiliza por medio texto sin formato. Solo admite contadores de arquitectura de 32 bits. Su seguridad es muy baja por lo que el riesgo de contar con incidentes es muy alto.

SNMP versión 2c: en esta versión, se habilita la compatibilidad con contadores de arquitectura de 64 bits. Actualmente la mayoría de los dispositivos solo admiten esta versión de SNMP, dado que los dispositivos de 32 bits se consideran obsoletos e inseguros.

SNMP versión 3: se agrega niveles de seguridad mucho más robustos ya que se añade el cifrado de datos y autenticación de usuarios.

A. MIB's

MIB (Management Information Base) es una base de datos que incluye todas las informaciones de los dispositivos. Existen dos tipos de MIB, los cuales son los públicos y los privados. Las públicas son datos compatibles entre los diferentes productores de dispositivos, para permitir una supervisión independiente y estandarizada.

Los privados, los cuales así han sido creados todos los dispositivos, revelan los datos únicamente por el estándar SNMP. Los MIBs privados no son expuestos por los fabricantes como sí lo hacen con los MIBs públicos.

Una aplicación de consola de administración SNMP puede manipular los objetos en una computadora específica.

II. Comunidad SNMP, credenciales e interfaces por defecto

A. Credenciales de usuario

Los usuarios en el protocolo SNMP posee ciertos atributos heredados del grupo al cual pertenece, la gestión de inicio de sesión de los usuarios se maneja de forma tradicional, mediante un nombre de usuario, contraseña y método de validación, a continuación, Cisco nos ofrece una perspectiva acerca de los usuarios en SNMP:

An SNMP user is defined by its login credentials (username, passwords and authentication method), and also by the context/scope in which it operates by association with a group and an Engine ID.

After a user is authenticated, it takes on the attributes of its group and can then see/not see the views associated with this group.

[Un usuario SNMP se define por sus credenciales de inicio de sesión (nombre de usuario, contraseñas y método de autenticación), y también por el contexto / alcance en el que opera por asociación con un grupo y una ID de motor.

Una vez que un usuario está autenticado, adquiere los atributos de su grupo y luego puede ver / no ver las vistas asociadas con este grupo.] (Cisco, s.f.-b)

También Cisco menciona lo siguiente acerca de los grupos de usuarios: “Groups enable network managers to assign access rights to specific device features, or feature aspects to an entire group of users instead of to a single user.” [Los grupos permiten a los administradores de red asignar derechos de acceso a funciones específicas del dispositivo o aspectos de las funciones a todo un grupo de usuarios en lugar de a un solo usuario.] (Cisco, s.f.-b)

B. Interfaces por defecto

El protocolo SNMP emplea para su funcionamiento dos puertos por defecto:

1. Puerto 161: dedicado al agente.
2. Puerto 162: dedicado al gestor.

Además de estos, el software Netflow Analyzer emplea los siguientes puertos por defecto para realizar sus funciones:

1. Puerto 80: Puerto usado para acceder a la consola web.
2. Puerto 137: Es utilizado para el tráfico saliente cuando la resolución NetBIOS es activa.
3. Puerto 1433: Este puerto se utiliza para comunicar un servicio de NTA con un servidor SQL.
4. Puerto 1434: Es usado para comunicar el servicio de NTA con una base de datos ORION.
5. Puerto 5671: puerto utilizado para negociaciones mediante el software RabbitMQ.
6. Puerto 17777: Dedicado al intercambio de información entre los módulos de Solarwinds. como por ejemplo Network Performance Monitor (NPM).
7. Puerto 17778: Acceso al api de información de Solarwinds.
8. Puerto 17791: Acceso a servidor Orion Solarwinds en Windows Server.

C. Comunidad SNMP

Las comunidades SNMP representan un medio de administración con el cual ciertos dispositivos que pertenecen a una comunidad en específico poseen accesos asignados por la administración, según Cisco las comunidades SNMP:

The community is a type of shared password between the SNMP management station and the device, which is used to authenticate the SNMP management station.

Communities are only defined in SNMPv1 and v2 because SNMP v3 works with users instead of communities. The users belong to groups, which have access rights assigned to them.

The *SNMP Communities Page* associates' communities with access rights, either directly (Basic Table) or through groups (Advanced Table).

[La comunidad es un tipo de contraseña compartida entre la estación de administración SNMP y el dispositivo, que se utiliza para autenticar la estación de administración SNMP.

Las comunidades solo se definen en SNMPv1 y v2 porque SNMP v3 funciona con usuarios en lugar de comunidades. Los usuarios pertenecen a grupos a los que se les asignan derechos de acceso.

La página de comunidades SNMP asocia comunidades con derechos de acceso, ya sea directamente (tabla básica) o mediante grupos (tabla avanzada).] (Cisco, s.f.-a)

III. Características de Analizador y Monitor

A. Netspot

NetSpot es una herramienta ideal para realizar auditorías de red en entornos relativamente medianos, este software añade múltiples características como son las siguientes:

1. Búsqueda de canales wifi: NetSpot nos permite analizar la cobertura wifi, para poder elegir el punto de acceso más adecuado.
2. Mapa de señal wifi: NetSpot nos ofrece esta herramienta para poder detectar y determinar qué espacios físicos en el entorno son factibles o no para procesos inalámbricos.
3. Análisis wifi: NetSpot es una herramienta muy útil, esta característica nos permite planificar mejor las redes inalámbricas en nuestro entorno, podemos obtener información detallada de las redes en nuestro entorno inclusive mapas de calor.

Y dispone de más beneficios como lo son:

1. Posee una versión gratuita
2. Fácil de implementar y recomendado para principiantes
3. Sus herramientas se utilizan mediante una interfaz gráfica amigable con el usuario
4. Su versión de paga es más cómoda en comparación con otros productos similares

NetSpot es ideal para planificar mejor las redes mediante sus herramientas de auditoría de red, es recomendado para redes en un contexto mediano, es decir es perfecta su utilización en redes de tipo LAN.

B. Netflow Traffic Analyzer

Netflow Traffic Analyzer en sus siglas N.T.A perteneciente a la compañía SolarWinds es muy ideal para las empresas y demás entidades quienes quieran poseer un control, monitoreo y gestión sobre sus redes con la finalidad de identificar anomalías y poder optimizarla, sus principales características son las siguientes:

1. Monitorear el ancho de banda: ver historial de flujos IPv4 e IPv6
2. Alertas sobre la red: este software permite desplegar alertas cuando ocurran anomalías como lo es la suspensión del tráfico en la red.
3. Análisis del tráfico de red: análisis de patrones con los datos recolectados mediante herramientas interactivas que despliegan informes de la red.
4. Análisis de desempeño: esta característica es bastante importante, porque nos permite identificar las posibles precursores de distintas situaciones de la red de forma interactiva y dinámica.

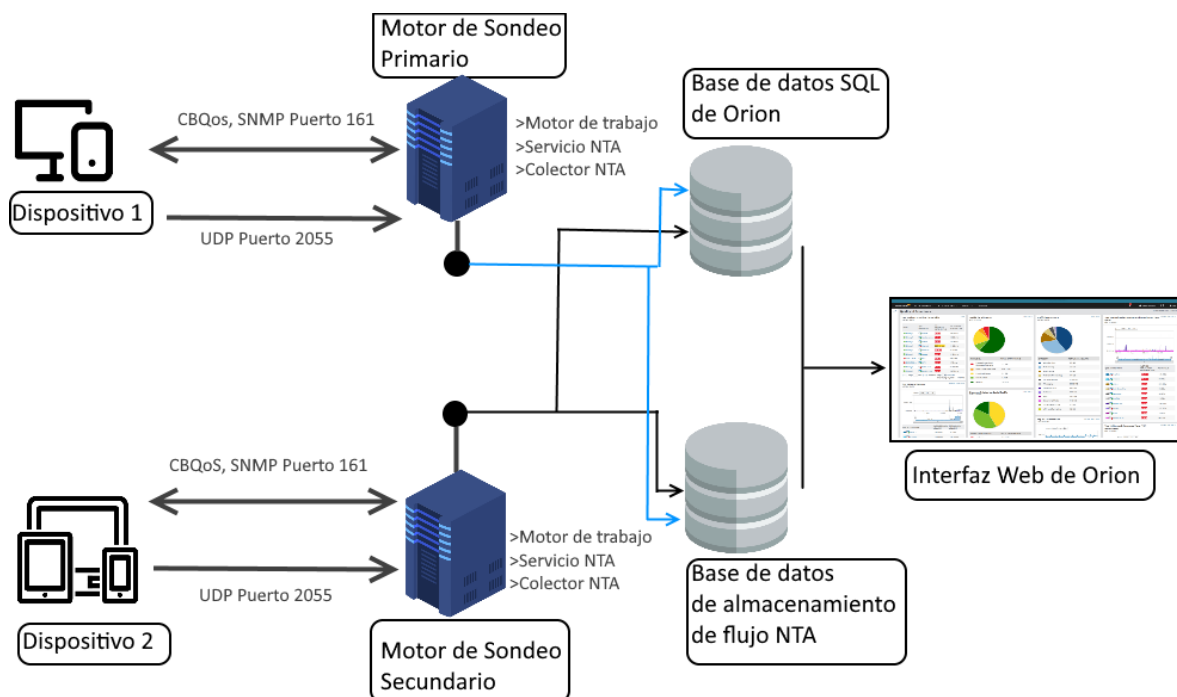
El software de Netflow Traffic Analyzer (NTA) de SolarWinds, por su estructuración e implementación en una red y por el hecho de que sus interfaces interactúan con múltiples dispositivos en varios niveles es factible para redes LAN Y WAN, por el hecho de que el software fue pensado para adaptarse ante posibles redes crecientes.

C. Diseño que se realiza para monitorear un servidor

En el contexto de esta investigación es muy importante abarcar el funcionamiento del software asignado el cual es Netflow Analyzer, cómo se lleva a cabo el monitoreo de una red mediante las distintas interfaces presentes en dicha, este software emplea una serie de componentes que mediante protocolos le es posible coleccionar, almacenar y desplegar la información de los dispositivos en la red, a continuación, se propone una ilustración del diseño estructural y funcional en el cual Netflow Analyzer se ejecuta.

Figura 1

Imagen de Diseño estructural del funcionamiento de Netflow Traffic Analyzer



Como bien se puede apreciar en el anterior diseño estructural del funcionamiento del software Netflow Traffic Analyzer, se emplean múltiples dispositivos para llevar a cabo la gestión y monitoreo de la red. En los dispositivos podemos observar dos flechas, la inferior representa a los dispositivos enviando datos de flujo al colector o Motor de Sondeo mediante el puerto 2055, y la flecha superior representa un sondeo por parte del colector o Motor de sondeo mediante el puerto 161 a dispositivos que están habilitados en CBQoS, según solarwinds CBQoS es:

Class-Based Quality of Service (CBQoS) is an SNMP-based, proprietary Cisco technology available on selected Cisco devices that gives you the ability to prioritize and manage traffic on your network. Using policy maps, also known as policies, the different types of traffic on your network are categorized, and then given a priority. Based on assigned priorities, only specified amounts of selected traffic types are allowed through designated, CBQoS-enabled devices.

[La calidad de servicio basada en clases (CBQoS) es una tecnología patentada de Cisco basada en SNMP disponible en dispositivos Cisco seleccionados que le brinda la capacidad de priorizar y administrar el tráfico en su red. Usando mapas de políticas, también conocidos como políticas, los diferentes tipos de tráfico en su red se categorizan y luego se les da una prioridad. Según las prioridades asignadas, solo se permiten cantidades específicas de tipos de tráfico seleccionados a través de dispositivos habilitados para CBQoS designados.](solarwinds, s.f.-d)

Los datos e información recopilada mediante los distintos puertos y protocolos, son enviados preferiblemente a dos bases de datos, la primera es la base de datos SQL de Orion y

la segunda es una base de datos que almacena la actividad del flujo, una vez con estos datos almacenados se pueden realizar distintas operaciones mediante la interfaz web de Orion.

IV. Preferencia a realizar un análisis en su empresa

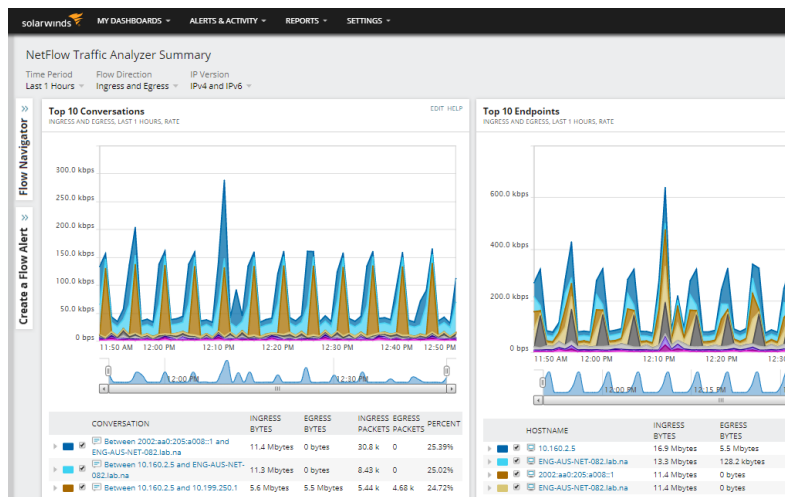
Como vimos en un inicio en el documento, los beneficios al usar el software Netflow Analyzer contraen grandes beneficios para el uso en las organizaciones. Si somos específicos escogemos de la empresa SolarWinds, dado que esta compañía de software es reconocida por su confiabilidad y eficiencia en sus productos de software y en el caso de Netflow Analyzer es una de las herramientas más usadas de su tipo. Algunos de los motivos por el cual elegimos esta herramientas son:

1. *Visibilidad clara:* Posibilidad de monitorear la red, análisis de patrones de tráfico y evitar cuello de botella.
2. *Rapidez:* Solución de problemas con mayor eficiencia en el prevenir ciberataques por medio de flujos de tráfico maliciosos
3. *Integración completa:* Se integra con herramientas como el monitor de rendimiento y el administrador de red.

Ser capaz de actuar rápidamente si hay un cambio inusual en el tráfico de aplicaciones es de suma importante para cualquier organización, es por esta la razón que decidimos escoger esta herramienta. Asimismo por las alertas al notificar si un dispositivo deja de enviar datos de flujo, por lo que puede solucionarse de manera automatizada.

Figura 2

Imagen de Monitor de banda ancha de SolarWinds.



Nota. Imagen obtenida de la pagina oficial de SolarWinds

(<https://www.solarwinds.com/netflow-traffic-analyzer>)

V. Costo

A. Software

En este apartado veremos los precios estimados de las licencias de los softwares

NetSpot y Netflow Traffic Analyzer de Solarwinds.

1. Solarwinds NTA: en el caso de este software Solarwinds nos ofrece dos opciones de licencia: la perpetua que cuesta \$1,945 que permite usar el software de forma temporal y con el primer año de soporte incluido y la capacidad de renovarlo. El tipo de licencia por suscripción cuesta \$1,072 y permite usar el software por el tiempo estipulado en un acuerdo y durante este tiempo el soporte es incluido.
2. NetSpot: respecto a este software, posee una versión gratuita con características limitadas. Su versión NetSpot Home cuesta \$49.00 y la versión NetSpot PRO & Enterprise cuesta \$149.00.

B. Hardware

En lo que respecta hardware como tal, en este apartado no se establece un precio, más, sin embargo, NTA de Solarwinds nos da unas recomendaciones y especificaciones para implementar su un servidor SQL adecuado a sus servicios con las cuales se puede realizar una estimación del coste:

1. Versión de Servidor SQL: SQL Server 2016 SP1, Versión Estándar o Empresarial.
2. procesador: procesador 12 Núcleos Intel Xeon E5 4640V4, 2.1 Ghz o equivalente.
3. Memoria: 64GB RAM.
4. Discos duros: 500GB SSD.

VI. Esquema COBIT sobre un Analizador de Protocolos

COBIT es un esquema que facilita a las organizaciones a conseguir objetivos de control de TI manteniendo un equilibrio entre los ámbitos de la empresa .Existen diferentes versiones de COBIT y la más actual es la versión 5, la cual se puede aplicar a organizaciones de todos los tamaños, tanto en el sector privado.

El esquema COBIT cuenta con 5 componentes principales, pero él para justificar la adquisición sería el principio de Satisfacer:

1. Satisfacer las necesidades: se alinean las necesidades de los objetivos empresariales específicos. En nuestro caso al adquirir el software de SolarWinds optimizamos las tareas de redes.

Conclusión

Al llegar al final de esta investigación sobre los temas abarcados de SNMP y los softwares asignados Netflow Traffic Analyzer de Solarwinds y NetSpot, pudimos comprender de forma más específica lo que involucra la gestión y monitoreo de las diversas redes. Para nosotros los realizadores de esta investigación es muy valioso que los conceptos englobados en el tema SNMP queden establecidos de forma clara, por la razón de que el público objetivo de esta investigación obtenga diversos conocimientos que al momento de verse involucrado en un contexto práctico, técnico y teórico posea sustento contextual ante estas situaciones.

De forma general, es beneficio conocer acerca del tema abarcado a lo largo de esta investigación de muchas maneras, las tecnologías de telecomunicación e informática en nuestra era actual se encuentran en un gran auge, lo que a consecuencia de esto hace que exista y crezca una gran demanda de productos y servicios en el campo de la informática y afines, la gestión de redes es un tema que cobra gran relevancia.

Es por eso que identificar los beneficios, necesidades, características y otros criterios acerca de la implementación y uso de sistemas analizadores y monitores de red nos ayudará a encontrar soluciones que se adecuen a las situaciones propuestas y que ofrecen gran rendimiento y fiabilidad.

Recomendaciones

En el mercado de software existen múltiples opciones de implementación de sistemas analizadores y monitores de red, para realizar una correcta inversión primero se deberá analizar el contexto en el cual se quiere implementar la infraestructura de monitoreo, para con esto definir las necesidades de gestión de red a satisfacer, se recomienda que al momento de inclinarse por el uso de un analizador de red tenga las siguientes características o funciones:

- Comunicación de las alertas.
- Integraciones con servidores externos
- API de acceso desde sistemas externos.
- Integraciones con Bases de Datos.
- Integración con máquinas virtuales
- Integraciones hardware
- Seguridad.
- Control remoto.
- Inventario de Hardware y Software.
- Monitorización de la nube.

Referencias

- What is netflow? Analyze network flow and data.* (n.d.). SolarWinds. Retrieved September 18, 2021, de <https://www.solarwinds.com/netflow-traffic-analyzer/use-cases/what-is-netflow>
- Zambrano Montenegro, D. F. (2015). “propuesta de utilización de herramientas de telemetría, para identificar técnicas de ciberdelitos como watering hole, en redes de infraestructura (caso de estudio netflow de cisco). *Pontificia Universidad Católica de Ecuador*. de <http://repositorio.puce.edu.ec/bitstream/handle/22000/8437/Tesis%20-%20Watering%20Hole.pdf?sequence=1&isAllowed=y>
- Barkah Widagdo, G. (2016). *View of real-time early detection NTP amplification attack*. WidagdoSwiss German University.
<https://proceedings.sgu.ac.id/acmit/index.php/acmit/article/view/29/26>
- S.N, B. (2020). *Я банан*. Cyberleninka. de <https://cyberleninka.ru/article/n/network-traffic-analysis-tools/viewer>
- Cisco. (n.d.). *SNMP communities*. Cisco. Visitado Septiembre 20, 2021, en https://www.cisco.com/assets/sol/sb/Switches_Emulators_v2_2_015/help/nk_configuring_snmp09.html
- Pandora FMS team. (2017, septiembre 25). *Monitoreo de red en 2021: Qué debemos saber sobre el tema*. Pandora FMS. <https://pandorafms.com/blog/es/monitoreo-de-red-que-debemos-saber/#avanzado>
- Battersby, J. (2019, February 28). NetSpot Wi-Fi Scanner Review: Get to know your wi-fi network. *IMore*. <https://www.imore.com/netspot>
- Cisco. (n.d.-b). *SNMP users*. Cisco. Visitado Septiembre 20, 2021, en https://www.cisco.com/assets/sol/sb/Switches_Emulators_v2_2_015/help/nk_configuring_snmp07.html

NetSpot. (2014, January 14). *What is the difference between NetSpot versions?* NetSpot.

<https://www.netspotapp.com/help/what-is-the-difference-between-netspot-free-scanner-reporter-and-pro/>

solarwinds. (n.d.-a). *Generate an Online Quote in 2 minutes*. Solarwinds. Visitado

Septiembre 21, 2021, en <https://www.solarwinds.com/onlinequotes/#/addLicense>

solarwinds. (n.d.-b). *Success Center*. Solarwinds. Visitado Septiembre 21, 2021, en

https://support.solarwinds.com/SuccessCenter/s/article/User-scenario-Recommended-SQL-server-disk-configuration?language=en_US

solarwinds. (n.d.-b). *How SolarWinds NTA works*. Solarwinds. Visitado Septiembre 21, 2021,

en https://documentation.solarwinds.com/en/success_center/nta/content/nta-how-nta-works.htm

solarwinds. (n.d.-d). *View CBQoS data in SolarWinds NTA*. Solarwinds. Visitado Septiembre 21, 2021, en

<https://www.solarwinds.com/documentation/en/flarehelp/netflow/content/nta-viewing-cbqos-data-sw1241.htm?cshid=OrionNetFlowAGViewingCBQoSData>

Smith, C. (2018, January 2). *NetSpot: This app tells you how bad your WiFi really is*.

KnowTechie. <https://knowtechie.com/netspot-this-app-tells-you-how-bad-your-wifi-really-is/>

Rusen, C. A. (2018, July 30). *NetSpot review: A great app for WiFi analysis and*

troubleshooting! Digital Citizen Romania. <https://www.digitalcitizen.life/netspot-review-free-pro/>

Luz, S. D. (2018, March 20). *NetSpot: Analizar redes inalámbricas Wi-Fi y crea mapas de*

calor. *RedesZone*. <https://www.redeszone.net/tutoriales/redes-wifi/netspot-monitor-analizar-redes-inalambricas-wi-fi/>

Setapp. (s.f.). *NetSpot en Setapp*. Setapp. Visitado Septiembre 21, 2021, en

<https://setapp.com/es/apps/netspot>

TrustRadius. (s.f.). *SolarWinds netflow traffic analyzer (NTA) reviews & ratings 2021*.

TrustRadius. Visitado Septiembre 21, 2021, en

<https://www.trustradius.com/products/solarwinds-netflow-traffic-analyzer/reviews?qs=pros-and-cons>

solarwinds. (2020, November 30). *NetFlow Analyzer - Análisis del tráfico del ancho de banda de la red remoto*. SolarWinds. <https://www.solarwinds.com/es/netflow-traffic-analyzer>