Capítulo II

Investigación y elección del software libre a implementar

2.1 Introducción.

Uno de los objetivos del software libre, como se describió en el capítulo anterior, es desarrollar alternativas de uso libre sobre algún software propietario específico. En este caso el software propietario Netflow ofrece un desempeño eficiente y poderoso en la obtención de estadísticas, reportes, costo de ancho de banda, etc. Sin embargo se tiene el inconveniente de tener que pagar elevadas cantidades por su uso en ambientes de producción.

Esto ha motivado a que se realice una investigación con el objetivo de encontrar alguna alternativa de uso libre que soporte el protocolo Netflow. La alternativa encontrada deberá de cumplir con los siguientes requerimientos para su elección y puesta en marcha:

- ✓ Software libre.
- ✓ No se tenga restricciones en cuanto al número de exportadores instalados.
- ✓ Tenga un colector.
- ✓ Soportar el protocolo Netflow.
- ✓ Generar gráficas y poder observar los datos presentes en ellas.
- ✓ Que soporte por lo menos las versiones 5, 7 y 9 del protocolo Netflow.
- ✓ Que tenga interfaz cliente-servidor vía web.

En este capítulo se explicará todo el proceso realizado para la elección del software libre. El proceso de investigación y elección fue resultado de una búsqueda y análisis de la mejor alternativa que cumplió con las restricciones mencionadas. Además de mostrar una comparación entre el software libre elegido con el software propietario utilizado en la institución.

2.2 Investigación sobre las alternativas de software libre.

La investigación se realizó mediante una búsqueda en internet sobre alternativas de uso libre que cumplieran con los requerimientos descritos, descartando a alternativas que no cumplieran con algún requerimiento establecido.

Durante la investigación se presentaron los siguientes inconvenientes:

- ➢ La mayoría del software libre encontrado sólo soportaba un número limitado de exportadores (no permitían tener más de cinco dispositivos activos enfocados a recolectar información).
- ➢ La mayoría de las alternativas encontradas eran soportadas por S.O. Linux, y muy pocas soportaban S.O. Windows. Esto representa un problema para usuarios que no cuenten con conocimientos básicos del uso de S.O. Linux, debido a que no lograran utilizar el nuevo software al 100%.
- ➢ La versión comercial de Netflow utilizada (no se mencionará el nombre real de este software propietario utilizado, por cuestiones de integridad y confidencialidad de la información presente en la institución), trabaja en S.O. Windows ofreciendo estadísticas muy detalladas del tráfico presente en la red, además de diversas funcionalidades, como lo son:

- Cálculo de costo por tráfico consumido.
- Generación de reportes.
- Clasificación de redes en forma automática.
- Poderosa interfaz web.
- Entre otras.

Debido a las características mencionadas de la versión comercial de Netflow utilizada, fue muy complicado encontrar alguna alternativa software libre que logre sustituir completamente todas las funcionalidades ofrecidas por este software. Al final de este capítulo se muestra una comparación entre la alternativa software libre elegida y la versión comercial utilizada en la institución.

La tabla 2.1 muestra el resultado obtenido de la primera investigación realizada. Mostrando los posibles candidatos que podrían sustituir al software comercialNetflow utilizado en la institución.

Tabla 2.1 Alternativas Open Source a sustituir a la versión comercial de Netflow utilizada

Software	Licencia	S.O. Soportados	Comentario	Sitio Oficial.
Argus	GNU GPL	Linux, MAC, Windows NT	Soporta las versiones Netflow 1-8, actualmente se está trabajando en la lectura de datos de la versión 9. Sin embargo hay muchas diferencias entre los datos de argus y datos de Netflow, como son: ➢ Protocolo de soporte, ➢ Reportes, ➢ Precisión del tiempo, ➢ Tamaño de los registros, ➢ El estilo y el tipo de la métrica.	http://www.qosient.com/argus/argusnetflow.htm
Cflowd	Freeware	Linux	➢ Creado para recopilar y analizar la información obtenida disponible de los flujos en Netflow. Le permite al usuario almacenar la información. ➢ Solamente es utilizado como colector.	http://www.caida.org/tools/measurement/cflowd/
Nfdump y Nfsen	BSD	Linux	➢ Poderosa lectura, interpretación y análisis de datos por línea de comandos con Nfdump. ➢ Soporta las versiones 5, 7 y 9 de Netflow ➢ Ambiente web con la herramienta Nfsen, adaptada completamente para el soporte de Nfdump. ➢ El software Nfsen es capaz de crear alertas, acepta programación exterior además de la creación de filtros con el objetivo acotar la información.	http://nfdump.sourceforge.net/ http://nfsen.sourceforge.net/
EHNT	Freeware	Linux	➢ Solamente soporta la versión 5 de Netflow. ➢ Genera estadísticas de puertos tcp/udp. ➢ Solo disponible en modo texto.	http://www.networkuptime.com/tools/netflow/ehnt.html
F.L.A.V.I.O	GNU GPL	Linux	➢ Usado únicamente para graficar datos en formato Netflow.	http://www.networkuptime.com/tools/netflow/flavio.html
Flowd	BSD	Linux	➢ Recolecta rápidamente y de forma segura datos en formato Netflow. ➢ No puede almacenar flujos en múltiples formatos para realizar	http://www.mindrot.org/flowd.html

			análisis de datos. ➢ Solamente soporta versión 5.	
FlowScan	GNU GPL	Linux	➢ Analiza y reporta datos en formato Netflow mediante Cflow. ➢ Examina el flujo de datos y mantiene contadores reflejando lo que fue encontrado. ➢ Los valores del contador se almacenan con ayuda de RRDtool (BD utilizada sistemas cronológicos). ➢ Soporta la versión 5.	http://www.caida.org/tools/utilities/flowscan/
JNCA	Free	Linux, Windows	➢ JNCA (Java Netflow Collector and Analizer) es una solución a la administración de flujos de red basados en Netflow creada por java ➢ Diseñada para recolectar y analizar datos en formato Netflow.	http://www.networkuptime.com/tools/netflow/jnca.html
Ntop	GNU GPL	Windows, Linux	➢ Recolecta datos en formato Netflow. ➢ Genera tablas y gráficas. ➢ Utiliza el software Nscape como una interfaz web, sin embargo cuenta con una administración y configuración limitada.	http://www.ntop.org/
Silk	GNU GPL	Linux	➢ Creada por CERT. Encargada de coleccionar y analizar flujos de datos. ➢ Puede recolectar datos de Netflow v9 o v5.	http://tools.netsa.cert.org/silk/
Stager	GNU GPL	Linux	➢ Recolecta datos en formato Netflow basándose en el colector Nfdump. ➢ Utiliza Posgret SQL. ➢ Crea reportes, genera tablas y gráficas, ambiente web.	http://software.uninett.no/stager/

La información mostrada en la tabla 2.1 fue de vital importancia para elegir a los posibles candidatos capaces de sustituir al software comercial Netflow utilizado. La elección de las posibles alternativas, fue resultado de un análisis entre cada una de las alternativas presentadas, descartando aquel software que ofrecía un funcionamiento menor en comparación a los demás. Como resultado de la investigación y análisis realizado, los tres candidatos elegidos fueron:

1. Nfdump y Nfsen.
2. Flow Scan.
3. Stager.

El siguiente paso fue realizar una investigación acerca del funcionamiento, requerimientos, colector utilizado, última versión, etc., de las tres alternativas elegidas. Como resultado de la investigación realizada se obtuvo la tabla 1.2, esta tabla fue de vital importancia para efectuar un análisis entre cada software: observar cuál o cuáles mostraban un mejor comportamiento y descartar a aquel(los) que mostrara(n) un funcionamiento menor.

La investigación realizada hacia las tres posibles alternativas consistió en una búsqueda efectuada sobre las páginas WEB y foros de cada software, arrojando los siguientes resultados:

Tabla 2.2 Comparación general entre posibles alternativas

Software	NFSEN	FlowScan	Stager
Licencia	BSD	GNU GPL	GNU GPL
S.O.	Linux	Linux	Linux
Última Versión	1.3.4 04/07/2010	1.0.1 28/02/2001	4.0.1 12/01/2010
Versiones de Netflow soportadas.	V5, V7, V9	V5	V5,V7,V9
Colector	Nfdump	Cflow	NFdump
Ambiente WEB	Sí	Sí	Sí
B.D.	Archivos o RRDTool	RRDTool	Posgret SQL
Reportes	Sí	No	Sí
Graficas	Sí	Sí	Sí
Foros	Sí	No	Sí

Por medio del análisis realizado a la tabla seis, se observó que el software FlowScan tiene un desempeño menor en comparación con las otras dos alternativas. Esteproblema fue de vital importancia para la eliminación del software mencionado, además de encontrar los siguientes inconvenientes:

- Al momento de observar que la última versión del software Flow Scan fue creada en el año 2001, se adquirió demasiada desconfianza en la investigación efectuada hacia este software. Esto ocasionó dudas acerca del correcto funcionamiento del software. Por ejemplo: si contaba con un mantenimiento adecuado, funcionamiento óptimo, foros actualizados, etc. Las sospechas fueron comprobadas al encontrar escasa información del software y su funcionamiento (prácticamente solo se contaba con la información proporcionada por la página web del software).
- La interfaz web del software es muy limitada; su mejor funcionamiento es mediante línea de comandos.
- El encontrar escasa información del colector utilizado por el software Flow Scan, Cflow, representaría dificultades al tener un problema en el funcionamiento del software Flow Scan y tratar de resolverlo.

Como siguiente paso en la investigación se realizó una búsqueda, análisis y comparación detallada entre el software Nfsen y el software Stager.

2.3 Nfsen vs Stager.

El objetivo de realizar un análisis detallado entre las dos alternativas es observar cual mostraba un mejor funcionamiento, las ventajas y desventajas que presenta cada uno de ellos, su comportamiento una vez instalado, etc. Los puntos principales que debía contener la investigación fueron los siguientes:

- Requerimientos necesarios para su instalación
- Funcionamiento
- Colector Utilizado
- Documentación
- Versiones
- Foros
- Interfaz web

Todos estos factores se obtuvieron de la página web oficial de cada software, así como de investigaciones realizadas fuera de su página web. Cabe mencionar que las dos alternativas finales satisfacían los requerimientos planteados. Por este motivo se decidió observar el funcionamiento de cada software de manera detallada y así poder concluir cuál de ellos se adaptaba mejor a las necesidades requeridas.

Las dos alterativas fueron instaladas en un S.O. Centos 5.5 virtualizado en "VmWare Server 2.0". El servidor de pruebas utilizado tiene instalado un S.O Windows Server 2003; Dicho servidor está configurado con una IP clase C estática pertenece a una red de usuarios. La máquina virtual creada fue puenteada (modo bridge) hacia la misma red de usuarios asociándole una IP estática clase C.

La figura 2.1 muestra el esquema utilizado en el proceso de pruebas.

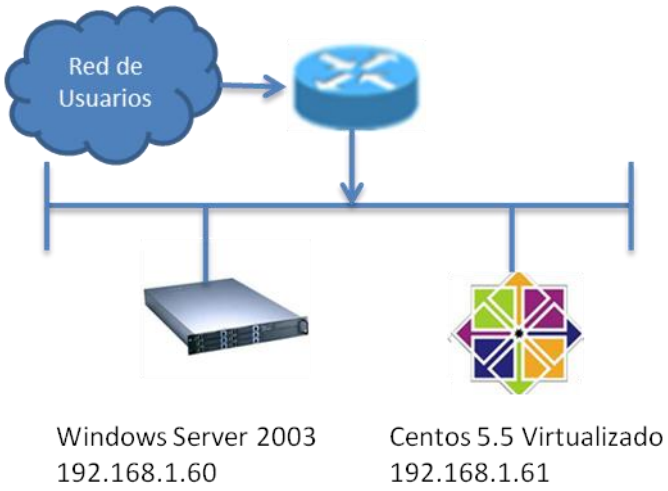

Figura 2.1 Esquema de Pruebas utilizado

La tabla 2.3 muestra una comparación realizada entre el software Nfsen y Stager. Resultado de la investigación realizada.

Tabla 2.3 Comparación entre Nfsen y Stager

Software	Nfsen	Stager
Requisitos para su instalación	➢ S.O. Linux ➢ Servidor Web ➢ Perl y PHP o Perl > 5.6.0 o PHP > 4.1 ➢ Módulos de perl. o Mail:: Header, Mail:: Internet ➢ Herramientas RRD o Todos los gráficos Netflow en NfSen requieren RRD. Por lo menos se requiere el módulo de Perl RRDs ➢ Herramientas Nfdump o Necesarias para recoger y procesar datos de Netflow o Instalar la versión 1.5.8	➢ S.O Linux o BSD ➢ Nfdump ➢ Perl o DBI (Modulo de interfaz de BD) ➢ PostgreSQL ➢ Servidor Http ➢ Php o Smarty: template engine o JpGraph: graph creating library
Colector Utilizado	Nfdump	Nfdump
Descripción General	El software Nfsen surgió como una aplicación creada con el objetivo de proporcionar una interfaz web al colector Nfdump. Por este motivo presenta una excelente compatibilidad con el software Nfdump. Además de lo mencionado también añadieron nuevas funcionalidades en el software Nfsen: como la creación de alertas, profiles y plugins (logrando realizar acciones específicas enfocadas hacia el monitoreo de red y análisis de datos)	Stager utiliza el colector Nfdump. Los autores del software decidieron enfocarlo más hacia las bases de datos, a tal modo que lograron implementar una base de datos en donde se guarda toda la información capturada por Nfdump. Sin embargo no implementaron todas las funcionalidades disponibles en el softwareNfdump.
Comparación entre graficas realizadas	Nfsen utiliza un software dedicado especialmente a graficar (RRDtool). Los desarrolladores enfocaron el software a la actualización de las gráficas en forma continua. Sin embargo, se tiene el inconveniente de solo tener un único formato de gráfica.	Stager utiliza jpGraph para la creación de sus gráficas. Esta herramienta permite crear gráficas en tercera dimensión y la elección de múltiples formatos para su creación. Sin embargo, las gráficas creadas solo muestran información general y no son actualizadas periódicamente.
Interfaz Web.	Nfsen presenta en su página de inicio gráficas basadas en el profile live (profile creado por default que contiene toda la información de los colectores instalados), divide la información en 12 gráficas; cada una de ellas grafica la cantidad de flujos, paquetes y bits que circulan en la red diario, semanalmente, al mes y al año. La interfaz web cuenta con un menú sencillo y potente que permite	Stager presenta en su página de inicio un conjunto de opciones relacionadas a seleccionar alguna interfaz y crear un reporte. Al realizar esta opción es posible observar las tablas creadas y graficarlas en caso que lo requeríamos. La interfaz web es de fácil utilización para el usuario.

	moverte fácilmente hacia cualquier opción del software, haciendo muy fácil el navegar sobre él.	
Procesamiento de datos	Nfsen tanto en sus gráficas como en tablas muestra la cantidad de flujos, paquetes y bits que circulan enla red. Se puede realizar un análisis más detallado mediante la aplicación de filtros, acotando la información a estadísticas muy específicas. Nfsen actualiza la información cada cinco minutos, logrando un monitoreo constante y la posibilidad de detectar en tiempo real alguna anomalía presentada.	Al igual que en Nfsen, Stager muestra la información de acuerdo a los flujos, bits y paquetes que circulan en la red. Sin embargo, como valor mínimo muestra lo que paso por la red cada hora y no permite realizar un análisis sobre los datos presentes.
Comentarios acerca de su funcionamiento	Nfsen al momento de ser implementado ha demostrado tener un buen funcionamiento, por los siguientes motivos: ➢ Las gráficas creadas se actualizan constantemente. ➢ Se observa información en sus tablas creadas referente a las gráficas ➢ Recolección de datos cada cinco minutos ➢ Creación de alertas y notificación inmediata sobre anomalías encontradas ➢ Capacidad de crear filtros específicos con el objetivo de acotar la información ➢ Capacidad de crear puntos de observación específicos sobre lo que está pasando a través de la red (profiles) ➢ Permitir ejecutar programación exterior al software mediante plugins.	Al momento de la instalación del software Stager se encontraron algunos errores de programación, esto causo dudas acerca de su funcionamiento. Una vez realizada la investigación acerca de los errores presentados y su resolución, se observó que solo está limitado a la representación de la información obtenida en tablas y gráficas. A comparación del software Nfsen, en Stager no es posible realizar un análisis de los datos obtenidos, ni el separar los datos o crear vistas específicas de ellos.
Conclusión	El software Nfsen mostró un mejor comportamiento en la fase de pruebas, debido a que además de su función principal la interpretación en ambiente web de los datos en formato Netflow proporcionados por el colector Nfdump, permite lo siguiente: ➢ Crear vistas específicas sobre los datos. ➢ La generación de alertas y notificación al detectar algo anormal ➢ El uso de filtros para observar información detallada. ➢ Gráficas de comparación por horas, día, semana, mes tanto de flujos, paquetes y bits. ➢ Posibilidad de implementar programación exterior sobre él.	El software Stager cumple con la función de recolectar, almacenar e interpretar los datos provenientes de exportadores de Netflow. Utiliza el colector Nfdump únicamente para la interpretación de los datos en formato Netflow. No aprovecha todo el potencial del colector mencionado y no proporciona mayores funcionalidades.

2.4 Elección de la alternativa Open Source

Como se observa en la tabla siete el software Nfsen mostró un mejor comportamiento que el software Stager. En la última prueba realizada antes de la elección, se decidió agregar un equipo exportador a Nfsen para observar su funcionamiento en tiempo real. Obteniendo lo siguiente:

- Al momento de agregar el dispositivo exportador al software Nfsen, se observó la actualización de las gráficas cada cinco minutos; en las tablas creadas se muestran las estadísticas obtenidas correspondientes al valor específico observado en la gráfica.
- Al probar la opción de filtros se observó el gran potencial que tiene para realizar análisis detallados y obtener información muy específica.
- Se comprobó que Nfsen fue desarrollado para mostrar en ambiente web todos los datos y opciones presentadas en línea de comandos por el software Nfdump. Cabe mencionar la gran facilidad proporcionada por Nfsen para generar comandos Nfdump y el gran potencial que tiene al aplicar filtros.
- La capacidad de crear puntos de vista específicos (profiles), y la creación de gráficas y tablas relacionadas con los datos aplicados sobre el/los filtros específicos, como puede ser:
    - Monitorear la utilización de puertos bien conocidos.
    - Monitorear la utilización de redes específicas.
    - Monitorear el tráfico sobre los protocolos TCP, UDP, ICMP, entre otras.
- La utilización de alertas para monitorear posibles anomalías que se presenten en nuestra red.
- La utilización de programación exterior (plugins) en el software Nfsen.

Por los motivos mencionados y como resultado de la investigación se decidió implementar el software Nfsen en la institución.

En el anexo B se muestra la guía de instalación del software mencionado.A continuación se muestran las características generales de la implementación realizada.

Sistema Operativo	Centos 5.5 (arquitectura de 32 bits)
Versión Nfdump Instalada	1.6.1
Versión Nfsen Instalada	1.3.2
Virtualización	Vmware Server 2.0
Dependencias Instaladas	➢ Servidor apache 2.0, habilitado con autenticación de usuarios ➢ Perl 5.6.0 ➢ Php 5.0 ➢ Modulos de perl: ▪ Mail:: Header ▪ Mail:: Internet ➢ RRD tool 1.4 ➢ Nfdump 1.5.8

La última sección en este capítulo pretende realizar una comparación entre el software libre implementado, Nfsen, y el software comercial Netflow utilizado por la institución.

2.5 Comparación entre versión comercial de Netlfow utilizada y Nfsen

En la tabla 2.4 se muestra una comparación realizada entre el software comercial Netlfow y el software libre Nfsen.

Tabla 2.4 Comparación entre la versión comercial de NetFlow utilizad y el software Nfsen

Software	Versión comercial de Netflow	Nfsen
S.O. Soportado	Windows XP, Vista, 7, Server 2003 o 2008	Linux
Tipo de Licenciamiento	Requiere licencia de uso de software.	BSD
Costo	Miles de dólares: depende de exportadores instalados e interfaces a monitorear.	Costo de Licencia **$0.00**: costos mínimos de capacitación a usuarios no familiarizados con el sistema operativo Centos.
Recursos Utilizados	La versión comercial de Netflow utilizada, por ser un software tan complejo consume demasiados recursos en el servidor instalado, en ocasiones llega a funcionar lento debido a las potentes funcionalidades desarrolladas sobre él.	Nfsen consume una mínima cantidad de recursos en el servidor instalado. Es óptimo para instalarse en computadoras con bajos recursos. Su funcionamiento es rápido en comparación del software comercial utilizado.
Descripción General	La versión comercial de Netlfow utilizada es un software enfocado hacia el monitoreo de red, presenta una excelente solución al analizar lo que está presente en la red, así como diversas funcionalidades.	El software Nfsen surgió como una aplicación creada con el objetivo de proporcionar una interfaz web al colector Nfdump. Por este motivo presenta una excelente compatibilidad con el software Nfdump.
Interfaz Web	La interfaz web del software comercial utilizado, es muy potente y de fácil utilización para el usuario. Además trae incorporado un manual de usuario y las gráficas creadas son en 2D o 3D.	La interfaz web del software Nfsen es más limitada en comparación con la versión comercial. Sin embargo es de fácil utilización. Además trae una pequeña explicación sobre las diferentes funcionalidades del software
Procesamiento de datos	El software comercial Netlfow utilizado, permite separar la información automáticamente en las redes presentes en el exportador. Además permite realizar análisis muy detallados (background) de lo que está presente en la red. Las gráficas creadas son actualizadas cada que el usuario lo desee (previa configuración), además se pueden observar datos en un lapso de tiempo específico. Los exportadores son agregados directamente sobre la interfaz web de una manera fácil y ágil. Además es posible mediante archivos el agregar redes de datos de forma automática.	Nfsen no separa la información automáticamente. Sin embargo con la ejecución de profiles es posible agrupar la información de igual forma que el software Netlfow comercial lo realiza. También es posible la realización de un background por medio de filtros e ir obteniendo cada vez información más específica. Las gráficas creadas se actualizan cada cinco minutos y es posible observar datos en un lapso de tiempo específico. Los exportadores y plugins creados en Nfsen tienen que ser agregados de forma manual en su archivo de configuración. Sin embargo una vez agregados presentan un comportamiento bastante eficaz sobre el software.
Soporte	Por ser software propietario, la versión comercial de Netflow	Nfsen no cuenta con soporte proporcionado directamente a sus

	utilizada cuenta con soporte técnico y de implementación proporcionado directamente por el fabricante. Sin embargo, solo está limitado al plazo de la licencia adquirida.	clientes. Sin embargo, es posible resolver problemas presentados preguntando en foros.
Funcionamiento	El software comercial NetFlow presenta un buen funcionamiento en términos generales. Se incorporaron a él diversas herramientas como son: generación de líneas bases, costo del ancho de banda consumido, generación de reportes muy precisos, notificación sobre anomalías encontradas entre otros. Sin embargo, en algunos casos no logra clasificar al 100% las redes de algún exportador específico y su uso se vuelve lento.	El software Nfsen no presenta funcionalidades tan complejas como la versión comercial de NetFlow. Sin embargo, es posible implementar en él, mediante la opción de plugins las funcionalidades realizadas por la versión comercial de Netlfow u otras que sean requeridas. Además tiene incorporada una opción de alertas basadas en filtros: mediante un análisis basado en filtros o plugins se logra encontrar tráfico anormal, haciendo muy potente el software.
Beneficios	La versión comercial de NetFlow utilizada, presenta los siguientes beneficios: ✓ Soporte prestado por profesionales las 24 horas del día. ✓ Costo de la licencia de acuerdo a las necesidades requeridas ✓ Compromiso de correcto funcionamiento. ✓ Fácil Instalación. ✓ Interfaz web muy potente y de fácil uso. ✓ Monitoreo de red potente, además de diversas funcionalidades complementarias. ✓ Creación de reportes muy potentes. ✓ Muy poca intervención del usuario.	Nfsen presenta los siguientes beneficios: ✓ Foro creado para la resolución de problemas presentes sobre el software. ✓ Software Libre. ✓ Observar el código fuente y hacer mejoras sobre él. ✓ Interfaz web limitada, pero de fácil utilización para el usuario. ✓ El monitoreo de red puede llegar a ser tan potente como el usuario lo requiera. ✓ Capacidad de agregar programación exterior (plugins) que satisfagan las necesidades del usuario. ✓ Una vez configurado de acuerdo a las necesidades requeridas, realiza los procesos de forma automática.
Conclusión	Por las características descritas, el software NetFlow comercial muestra ser muy robusto y potente. Sin embargo, se tiene el inconveniente que su licencia es de un alto costo, tomando en cuenta número de colectores instalados e interfaces monitoreadas.	A comparación con la versión comercial de NetFlow utilizada, Nfsen no es tan robusto. Sin embargo está diseñado para aprovechar al máximo sus funcionalidades. Puede llegar a ser tan robusto e inclusive superar al software comercial Netflow por medio de plugins, profiles y filtros enfocados a las necesidades requeridas.

Como se observa en la tabla ocho, la versión comercial de NetFlow utilizada proporciona un mejor desempeño que el software libre Nfsen. Sin embargo, una de las principales ventajas de Nfsen, además de ser libre y observar su código fuente, es el poder crear plugins enfocados hacia las necesidades requeridas. Esto ofrece un gran potencial al software Nfsen, a tal grado de igualar las funcionalidades desempeñadas por la versión comercial de NetFlow utilizada o incluso superarlas.

Cabe mencionar que el software Nfsen superó exitosamente la fase de pruebas y hasta el momento de publicación de este proyecto de tesis, no ha presentado errores en su funcionamiento. Logrando con esto el objetivo de encontrar una alternativa de uso libre capaz de poder sustituir al software Netflow comercial utilizado en la institución.

En conclusión, de todas las funcionalidades mostradas por el software Nfdump. Recomiendo el uso de este software frente a otros colectores por los siguientes motivos:

- Software Libre.
- Soporta las versiones 5, 7 y 9 de Netflow.
- Colector potente y configurable de acuerdo a las necesidades requeridas.
- Contabiliza el ancho de banda consumido.
- La herramienta nfdump es capaz de realizar análisis muy detallados.
- Pude ser enfocado hacia la seguridad informática.
- Muestra picos presentes sobre las redes o host que consumen un mayor BW (análisis mediante top n)
- Posibilidad de esconder la información.
- Filtros muy poderosos y de una sintaxis fácil.