Centro de Operación de la Red NOCUNAM

Octubre 2019

Manual para la implementación de un sistema de monitoreo de flujos de red con soporte para Netflow / IPFIX / Sflow

Versión 1.0

Índice

1. Introducción

El uso del protocolo NETFLOW de la marca CISCO para el análisis de tráfico es una tecnología que tiene poca o nula competencia, se desarrolló alrededor del concepto de flujos de red de datos para apoyar la inspección del comportamiento de las comunicaciones.

Este protocolo ha crecido de importancia junto con el consumo de ancho de banda debido a la importancia de la obtención de información relativa a la operación de los enlaces de comunicaciones y el comportamiento de las propias redes locales.

Por ello se propone este manual para que los que puedan utilizar esta tecnología ya sea porque cuentan con equipos de red de la marca CISCO, los que quieran transformar sus estadísticas provenientes de capturas a datos de flujos y quienes deseen realizar pruebas mediante el análisis por medio de esta tecnología lo realicen aprovechando las recomendaciones derivadas de la experiencia que el NOC UNAM tiene en la operación de la misma.

2. Objetivo

Proveer una alternativa al análisis de tráfico y obtención de información estadística por medio de la implementación del análisis de flujos con apoyo de la tecnología NETFLOW ya sea explotando esta característica dentro de los propios *routers* o implementado una solución que analice el tráfico y obtenga la información en el formato que este protocolo utiliza.

3. Alcance

Realizar recomendaciones sobre el empleo del protocolo NETFLOW en equipos CISCO con el objetivo de que la operación del mismo no afecte el envío de paquetes en los equipos de red donde se implementen.

Establecer las recomendaciones mínimas basadas en pruebas realizadas por el NOC RedUNAM para emplear la técnica de análisis de flujos en el análisis estadístico del comportamiento de las comunicaciones en las redes de datos.

Mostrar las principales características a considerar en la configuración de este tipo de análisis en las redes de datos.

4. Principales consideraciones para la implementación del sistema

En el Sistema Operativo:

Sistema operativo: 64 bits dedicados debido a que la implementación de un sistema de este tipo requiere recursos dedicados que podrían afectar a otros servicios ante una operación sobre exigida de las soluciones.

Disco Duro: 1 a Terabytes por cada 5 equipos monitoreados tomando en cuenta que estos tengan una retención de información estadística de 30 días y evaluando que sea para conexiones a 1 Gbps.
Este almacenamiento puede variar

Memoria RAM: Dependiendo la cantidad de dispositivos monitoreados de forma simultanea de 8ª 16 GBytes.

En la aplicación: Aislamiento del almacenamiento estadístico de la base de datos, reportes y estadísticas en particiones diferentes, preferentemente en discos duros aislados.

En el dispositivo a monitorear:

Los sistemas de monitoreo dedicados de software libre no requieren licenciamiento por lo que bien pueden ser instalados en un servidor y respaldados para que ante una falla pueda recuperarse el servicio sin problemas, este es el caso de sistemas como NtopNG, FlowScan, NFsen.

En sistemas licenciados se recomienda un aislamiento completo del sistema con las bases de datos que este escriba debido a que en Discos Duros mecánicos el sistema puede operar por meses a máximo 1 año si es que este escribe una gran cantidad de datos.

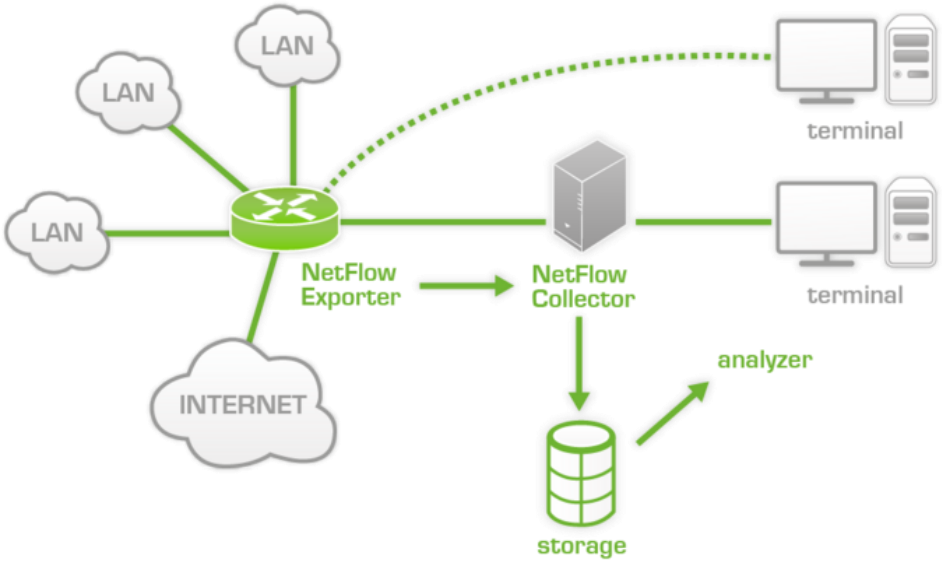
Los sistemas de monitoreo abren puertos de escucha que van del 2000 al 9000, es importante controlar que puertos se están abriendo pues representan una posible falla de seguridad.

Así mismo la convivencia con otras aplicaciones no se recomienda pues por lo regular la demanda de recursos varía dependiendo la cantidad de flujos que lleguen al servidor, los cuales tienen que ser desempaquetados y la información procesada para la elaboración de reportes.

5. Configuración del sistema de monitoreo

La configuración del monitoreo de flujos implica la configuración de:

A) Configuración de un servidor colector de flujos
B) Configuración de un servidor que procese los flujos recibidos en el formato que son enviados
C) El sistema que ofrece una interfaz gráfica para análisis de los flujos procesados
D) La base de datos donde se guardan los flujos recibidos y de ser necesario otra donde se guarda la información procesada de estos flujos recibidos.
E) Habilitar cada agente en los equipos de red para el envío de flujos en el formato que se espere recibir.
F) En el caso de que los dispositivos de red no cuenten con el soporte para el agente se vuelve necesario obtener el tráfico en mirror/espejo en la sección de la red que interesé y que esta información sea procesada para la elaboración de paquetes Netflow/IPFIX que serán enviados al servidor colector.



Imagen, *Configuración de Netflow con NtopNG*, jpg, recuperado del sitio Web: https://wiki.pandorafms.com/images/thumb/8/80/Netflow_architecture.png/700px-Netflow_architecture.png

Para el presente manual se muestra la forma de la implementación de 2 de los sistemas de monitoreo de flujos, NFSEN y NtopNG. La implementación del sistema de monitoreo implica los siguientes pasos:

Instalación de NFSEN:

Instalacion de Prerequisitos:
1. NFDUMP

Instalamos la última versión de nfdump: https://github.com/phaag/nfdump

Se requiere instalar modulos de perl:

```
perl -MCPAN -eshell
install Mail::Header
install Mail::Internet
install Socket6
```

2. Si no se tiene recompila pho con sockets habilitados:

```
se recompila si no se tiene la opcion --enable-sockets
./configure --prefix=/usr/local/php \
        --with-apxs2=/usr/local/http/bin/apxs \
        --enable-mbstring \
        --with-gettext \
        --with-png-dir=/usr/include/libpng \
        --with-zlib=/usr/local/zlib/ \
        --with-zlib-dir=/usr/local/zlib/ \
        --with-libxml-dir=/usr/lib \
        --with-jpeg-dir=/usr/lib \
        --with-xpm-dir=/usr/lib \
        --with-curl=/usr/include/curl \
        --with-freetype-dir=/usr/lib/ \
        --with-gd=/usr/ \
        --enable-gd-native-ttf \
        --enable-sockets
```

Los siguientes paquetes puede que se encuentren instalados, verificalos:

```
libpng12-dev libfreetype6-dev libart-2.0-dev bison flex rrdtool
```

3. Instalando NFDUMP:

```
wget http://sourceforge.net/projects/nfdump/files/stable/nfdump-1.6.11/nfdump-1.6.11.tar.gz/download
mv download nfdump-1.6.11.tar.gz
tar -vxf nfdump-1.6.11.tar.gz
cd nfdump-1.6.11
./configure --prefix=/usr/local/nfdump --enable-nfprofile --enable-sflow --enable-nftrack
make
make install
```

Se instala NFSEN ahora que ya se cumplieon las dependencias:
1. Se elige la version nfsen-1.3.5 porque la 1.3.6 presenta bugs todabía al ejecutar el instalador:

```
wget http://sourceforge.net/projects/nfsen/files/stable/nfsen-1.3.5/
tar -vzxf nfsen-1.3.5.tar.gz
cd nfsen-1.3.5
```

2. Se hace una copia de la configuracion por default y modificamos las lineas siguientes:

```
cp etc/nfsen-dist.conf etc/nfsen.conf
$BASEDIR = "/usr/local/nfsen";
$HTMLDIR    = "/usr/local/http/htdocs/nfsen/";
# nfdump tools path
$PREFIX  = '/usr/local/src/nfdump_src/nfdump-1.6.11/bin';
$USER    = "www-data";
$WWWUSER  = "www-data";
```

3. Se ejecuta el script de instalacion dando como argumento el archivo antes modificado:

```
./install.pl etc/nfsen.conf
```

Esta ejecucion presenta también un error:
-Error getting nfdump version at ./install.pl line 204, <STDIN> line 1.
Se resuelve editando el archivo de instalación en la linea 204 para cambiar la condicional:

```
...
if ( scalar @out == 2 ) {
...
```

Se comentan las siguintes lineas en el archivo etc/nfsen.conf para evitar mensajes de error en la configuración de las fuentes de datos:

```
...
%sources = (
   'upstream1'    => { 'port' => '9995', 'col' => '#0000ff', 'type' => 'netflow' },
#    'peer1'       => { 'port' => '9996', 'IP' => '172.16.17.18' },
#    'peer2'       => { 'port' => '9996', 'IP' => '172.16.17.19' },
```

```
);
```

Esta configuración mantendra un canal de captura nfsen por el puerto 9995 para que cualquier equipo que soporte netflow versiones 1 o 5 pueda mandarle sus flujos para diseccionarlos por medio de nfdummp.
4. Se inicia NfSen:

Es posible que nfsen requiera reconfiguración de las interfaces:

```
/usr/local/nfsen/bin/nfsen reconfig
Ahora si iniciamos el servicio:
/usr/local/nfsen/bin/nfsen start
```

Se instala los plugins de NfSen:

PortTracker
Este plugin está incluido en los archivos fuente de nfsen. Provee graficas de utilización por puerto mostradas en formato RRD:
Se requiere rrdtool para utilizar el plugin pero puede que necesite compilarse: 0 Paquetes necesarios (necesarios para compilar rrdtool):

```
libart-2.0 libart-2.0-dev tcllib tcl-dev ruby-dev libruby-1.8-dbg librrd-ruby1.8 ruby
y poner las siguientes ligas si no reconoce las rutas tlc:
ln -s /usr/include/tcl/tcl.h /usr/include/tcl.h
ln -s /usr/include/tcl/tclDecls.h /usr/include/tclDecls.h
ln -s /usr/include/tcl/tclPlatDecls.h /usr/include/tclPlatDecls.h
ln -s /usr/include/tcl/tcl-private.h /usr/include/tcl-private.h
```

Ahora se instala RRDTOOL:

```
wget http://oss.oetiker.ch/rrdtool/pub/rrdtool.tar.gz
tar zxvf rrdtool.tar.gz
cd rrdtool-1.2.27
./configure --enable-perl-site-install --prefix=/usr/local/rrdtool-1.2.30
make && make install
```

Para que NFDUMP opere correctamente se recompila indicando donde se encuentra ahora rrdtool:

```
./configure --prefix=/usr/local/nfdump \
        --enable-nfprofile
        --enable-sflow \
        --enable-nftrack \
        --with-rrdpath=/usr/local/rrd-1.2.30
```

make make install
Se agerga una liga suave de librrd.so.2 si es que no se encuentra una en /usr/lib:

```
ln -s /usr/local/rrdtool-1.2.30/lib/librrd.so.2 /usr/lib/librrd.so.2
(Este ultimo paso es requerido a veces para la instalacion del plugin PortTracker)lsls
```

1. Se compila el plugin:

```
cd /usr/local/src/nfsen_src/nfsen_1.3.5/contrib/PortTracker/
```

Se edita en el archivo "do_compile" las variables NFDUMP, RRDINCLUDE y RRDLIB en las siguientes lineas:

```
NFDUMP=/usr/local/src/nfdump
RRDINCLUDE=/usr/local/rrdtool-1.2.30/include
LIBRRD=/usr/local/rrdtool-1.2.30/lib
```

Ahora si se compila el plugin:

```
./do_compile
```

Puede mostrar varios errores porque hay errores con la version de GCC

2. Se crea un directorio para PortTracker para guardar los datos (requiere por lo menos 10 GB). El usuario de escritura debe ser el que ejecuta apache

```
mkdir /usr/local/nfsen/var/porttracker
chown www-data:www-data /usr/local/nfsen/var/porttracker
chmod 775 /usr/local/nfsen/var/porttracker
```

Editar PortTracker.pm

```
my $PORTSDBDIR = "/usr/local/nfsen/var/porttracker";
```

Se copian los archivos de backend y frontend:

```
cp PortTracker.pm /usr/local/nfsen/plugins/
cp PortTracker.php /usr/local/http/htdocs/nfsen/plugins/
```

Se agrega el plugin al archivo nfsen.conf con el formato adecuado:

```
vi /opt/nfsen/etc/nfsen.conf
@plugins = (
[ 'live',   'PortTracker'],
```

```
);
```

Se inicializa la base de PortTraker

```
cd /usr/local/nfdump/bin
# sudo -u www-data nftrack -I -d /usr/local/nfsen/var/porttracker
(This can take a LONG time! - 8 GB worth of files will be created)
```

Se cambian los permisos sobre el directorio donde se guardan los datos de PortTaker

```
# chown -R netflow:www-data /usr/local/nfsen/var/porttracker
# chmod -R 775 /usr/local/nfsen/var/porttracker
```

Se reinicia Nfsen

```
# /usr/local/nfsen/bin/nfsen reload
Ahora ya se deberia poder visualizarlo sin problemas en la pagina de NFSEN.
(recompilar nfdummp con soporte rrd para que nftrak pueda usarse
```

Instalación de NtopNG:

La implementación de NtopNG tiene una estructura similar, pero para el caso de NtopNG, se tiene la ventaja de que en sistemas operativos como Linux Debian y Centos, ya se cuenta con el paquete pre compilado y puesto que n omaneja base de datos externa, se puede instalar de la siguiente forma:

En el caso del SO Debian

```
#apt-get install ntop-ng
```

En el caso de Centos y sistemas derivados de RedHat con gestor de paquetes YUM:

```
-Se instala ntopng y redis forzando el repositorio epel
yum --enablerepo=epel install redis ntopng

-Se instala otra dependencia desde “epel”
yum --enablerepo=epel install hiredis-devel

-Activamos, ejecutamos y verificamos el servicio redis
systemctl enable redis
```

```
systemctl start redis
systemctl status redis

-Se prueba el servicio ntopng
systemctl enable ntopng
systemctl start ntopng
systemctl status ntopng
```

```
-Se modifica el archivo .conf de ntopng para que se ejecute en modo community y no pida licenciamiento
vi /etc/ntopng/ntopng.conf
-G=/var/run/ntopng.pid --community

-Se reinicia el servicio de ntopng y verificamos su ejecución
systemctl restart ntopng
systemctl status ntopng
-Se permite conexiones al puerto 3000 tcp de ntopng para poder conectarnos desde otro pc
firewall-cmd --permanent --add-port=3000/tcp
success

-Se reinicia el servicio de firewalld para que tome el cambio
systemctl restart firewalld

-Se abre un browser en otro equipo y navegamos a http://IP-Servidor-ntopng:3000. Los datos iniciales de conexión ntopng:
user: admin
password: admin (modificar inmediatamente después de la instalación)
```

La configuración del sistema de monitoreo por lo regular depende de la aplicación que se manejé, por ejemplo, en la mayoría de los sistemas propietarios, se debe configurar el agente y este escucha por un solo puerto.

6. Configuración del agente de monitoreo en los equipos de red

Si el dispositivo de red cuenta con la tecnología habilitada, estos son los pasos:

En el caso de la marca CISCO versión 5 del protocolo:

```
R1(config)# interface GigabitEthernet 0/1
R1(config-if)# ip flow ingress
R1(config-if)# ip flow egress
```

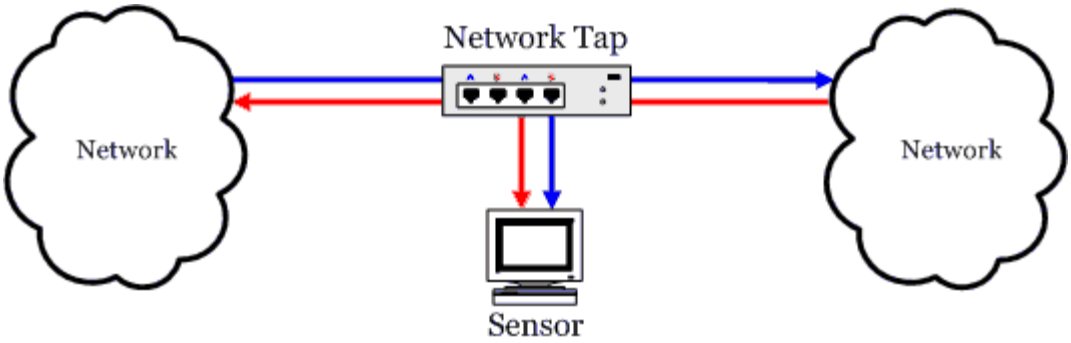
```
R1(config-if)# exit
R1(config)# ip flow-export destination 192.168.1.3 2055
R1(config)# ip flow-export version 5
R1(config)# ip flow-export source FastEthernet2/1 ( this is the interface used to export the Netflow data to the collector)
R1(config)# ip flow-export version 5
R1(config)# ip flow-export destination 1.1.1.1 2055
R1(config)# ip flow-cache timeout active 1
R1(config)# ip flow-cache timeout inactive 15
```

En el caso de la marca CISCO versión 9:

```
R1(config)# flow exporter EXPORTER-1
R1(config)#  destination 172.16.10.2
R1(config)#  export-protocol netflow-v9
R1(config)#  transport udp 90
R1(config)#  exit
R1(config)# flow record v4_r1
R1(config)# match ipv4 tos
R1(config)# match ipv4 protocol
R1(config)# match ipv4 source address
R1(config)# match ipv4 destination address
R1(config)# match transport source-port
R1(config)# match transport destination-port
R1(config)# collect counter bytes long
R1(config)# collect counter packets long
R1(config)# flow monitor FLOW-MONITOR-1
R1(config)#  record v4_r1
R1(config)#  exporter EXPORTER-1
R1(config)#ip cef
R1(config)# interface GigabitEthernet 0/0/0
R1(config)#  ip address 172.16.6.2 255.255.255.0
R1(config)#  ip flow monitor FLOW-MONITOR-1 input
```

En caso de no contar con la tecnología se puede implementar lo que se conoce como TAP (puerto espejo), además de integrar un equipo o software ya sea en el sensor o de forma independiente que permita obtener los paquetes de netflow necesarios para enviarlos al colector con toda la información necesaria para su análisis.

En este punto se recomienda la utilización de lo que ya es un estándar IPFIX en lugar de alguna de las versiones de Netflow



Imagen, Derivación de red con Tap, JPG, recuperado de https://www.dgonzalez.net/papers/roc_es/tap_inline.png

7. Recomendaciones sobre la operación del monitoreo de flujos de red

Los agentes de monitoreo de red en los equipo de red no se dimensionan por los fabricantes para su uso al 100% de capacidad en todas las interfaces que tienen los equipos, más aún porque estos son modulares, es decir, no se sabe la cantidad de puertos con las que va a trabajar el equipo y si estos estarán saturados.

Por tal condición y debido a que a pesar de que los proveedores lo saben, el habilitar al máximo el uso de la aplicación de análisis de flujos sobre un equipo, es algo que no debe hacerse en equipos de producción.

De cualquier manera si existen formas para que el análisis de flujos se dé en todas las interfaces de los equipos con una configuración adecuada, para ello se muestra aca recomendaciones al respecto:

En el caso de la versión 5 de Netflow o Sflow para equipos que soportan esta tecnología, basta con poner el muestreo de 1 paquete cada 2048 paquetes, esto mantiene la operación de los equipos por

debajo del 50% a pesar de estar saturados, esta versión del protocolo es menos agresiva pero también proporciona menos información.

Para Netflow Flexible o configuraciones posteriores a la versión 5 de Netflow, IPFIX o si los flujos se generan a través de un TAP, es necesario ajustar los parámetros, para estos casos se muestra una configuración con descripción de puntos importantes.

En la versión de Flexible Netflow pueden agregarse datos a la información recolectada, es el caso de esta sección:

```
flow record AVC_FLOW
        match ipv4 protocol
        match ipv4 source address
        match ipv4 destination address
        match transport tcp source-port
        match transport tcp destination-port
        match interface input (este dato es un dato que se agrega)
        match flow direction
        match application name
        collect transport tcp flags
        collect interface output
        collect counter bytes
        collect counter packets
        collect timestamp sys-uptime first
        collect timestamp sys-uptime last
        collect ipv4 id
        collect network delay sum
        collect connection server counter bytes network long
        collect connection client counter bytes network long
        collect connection new-connections
        collect connection sum-duration
!
flow record LIVEACTION-FLOWRECORD
        description DO NOT MODIFY. USED BY LIVEACTION.
        match flow direction
        match interface input
        match ipv4 destination address
        match ipv4 protocol
        match ipv4 source address
        match ipv4 tos
        match transport destination-port
        match transport source-port
        collect application http host
        collect application name
```

```
        collect application ssl common-name
        collect counter bytes
        collect counter packets
        collect flow sampler
        collect interface output
        collect ipv4 destination mask
        collect ipv4 dscp
        collect ipv4 id
        collect ipv4 source mask
        collect ipv4 source prefix
        collect routing destination as
        collect routing next-hop address ipv4
        collect routing source as
        collect timestamp sys-uptime first
        collect timestamp sys-uptime last
        collect transport tcp flags
       !
```

Existen secciones específicas para el protocolo IPv6 ahora:

```
flow record v6_r1
        match ipv6 traffic-class
        match ipv6 protocol
        match ipv6 source address
        match ipv6 destination address
        match transport source-port
        match transport destination-port
        match flow direction
        match interface input
        match ipv6 extension map
        collect counter bytes long
        collect counter packets long
        collect ipv6 source prefix
        collect ipv6 destination prefix
!
```

Al término de la configuración sobre la información que se desea recolectar solo se especifíca el puerto y la IP con la que se enviarán los paquetes al colector:

```
flow exporter AVC_EXPORT
        destination 132.248.64.101
        source TenGigabitEthernet0/0/1
        transport udp 2055
        template data timeout 60
```

```
option interface-table
option exporter-stats
option application-table timeout 60
```

En el colector:

Así como en el dispositivo es importante saber la cantidad de paquetes a enviar, también en el colector es necesario conocer las características de recepción, ya que están directamente ligadas al consumo de ancho de banda. Es importante recordar que el monitoreo se hace mediante muestreo y la cantidad de procesamiento necesario para crear las estadísticas es directamente proporcional a la cantidad de información de flujos que se envía cada periodo de tiempo desde los dispositivos.

Entonces se ofrecen las siguientes recomendaciones dependiendo el escenario con que se cuente:

Para un dispositivo que cuente con interfaces en 1Gbps y que estén comúnmente saturadas:

- Muestro inicial entre 2048 a 4096 dependiendo de la utilización de los puertos donde se habilite el muestreo.

Para dispositivos con interfaces mayores a 1 Gbps

- Muestreo inicial de 2096 dependiendo de la utilización de los puertos donde se habilite el muestreo.

Cabe mencionar que estas recomendaciones no son garantía de operación debido a que cada red y aplicaciones que funcionen en ellas tiene un comportamiento que no se puede deducir, por lo que siempre hay que estar atentos al comportamiento de los recursos de los dispositivos de red:

Procesamiento:
- Inferior al 80%
- En caso de ser un equipo central de la red menor al 60%

Memoria:
- Consumo menor al 80% en todos los casos

Para ellos se pueden emplear los siguientes comandos:

- Show proc cpu hist
- Show mem
- show platform hardware qfp datapath
- show platform software process memory

En el colector con apoyo de estos comandos los recursos del servidor:

- Iotop
- Top
- Htop
- Iftop

Esto permitirá tener un mejor control sobre la operación de la solución de análisis de flujos de red.

8. Ligas de descarga y soporte para la implementación

Sitio web principal del proyecto de NTOP, recuperado de su proyecto libre

https://www.ntop.org/

Sección del sitio web del proyecto NTOP para el modulo NPROBE, recuperado de su proyecto libre

https://www.ntop.org/products/netflow/nprobe/

Sitio web del proyecto de NFSEN, recuperado de su página de incio

http://nfsen.sourceforge.net/

Sitio web del proyecto nfdump, soporte para que el Sistema NFsen pueda operar

http://nfdump.sourceforge.net/

Proyecto migrado de Nfdump, soportado por Github para su descarga:

https://github.com/phaag/nfdump

Manual de Implementación de Nfsen que puede servir de guía alterna, recuperado de NRSC.ORG

https://nsrc.org/workshops/2016/walc/gestion/exercises/ejercicio2-instalar-nfdump-nfsen.htm

Control de Versiones al Documento

Versión	Descripción	Autor	Fecha
1.0	Creación del documento	Esteban Roberto Ramírez Fernández	21/10/2019

Revisión del Documento

Puesto/Rol	Nombre	Revisó
Jefe del Centro de Monitoreo del NOC UNAM	Hugo Rivera Martínez	Contenido
Staff NOC UNAM	Erika Hernández Valverde	Estructura del documento

Aprobación del documento

Puesto/Rol	Nombre y Firma	Fecha de aprobación
Jefe del Centro de Operación de RedUNAM (NOC-RedUNAM	Hugo Rivera Martínez	23/10/2019

Repositorio y publicación

Medio	Ubicación
Sitio Web del NOC www.noc.unam.mx	http://www.noc.unam.mx/conocimiento/
Repositorio Nube NOC	www.nocloud.noc.unam.mx/NOC/ProductosyPublicaciones

Control de Cambios

Revisión	Fecha	Motivo del Cambio
Esteban Ramírez	Septiembre 09, 2019	Se revisó los y actualización de ligas de descarga de sistema. Recuperado de la Base de conocimientos www.wiki.noc.unam.mx