Anexo C

Manual de usuario del software Listry-AIGC

Nfsen.

Verificación si los servicios están encendidos.

Antes de ejecutar el software Nfsen hay que verificar si el servidor apache esta encendido:

```
# service httpd status
```

En caso de que el servicio httpd se encuentre, encenderlo y añadirlo al nivel de arranque.

```
#       service httpd start
#       chkconfig –level 35 httpd on
```

Verificar el estado del servicio del software Nfsen:

```
#       cd /var/lib/netflow/nfsen-1.3.2/bin
#       ./nfsen status
```

De igual manera que con el servicio httpd, si nfsen se encuentra apagado encenderlo.

```
#       ./nfsen start
```

Añadir equipos a Nfsen.

Dirigirse a la carpeta de instalación del software Nfsen y abrir el archivo “nfsen.conf”:

```
#       cd/Listry-AIGC/nfsen-1.3.2/etc/
#       vi nfsen.conf
```

Buscar “Sources” y añadir los dispositivos activos, con el siguiente formato:

- 'ident' => { 'port' => '<portnum>', 'col' =>'<colour>', 'type' => '<type>' }
  - <Iden>: Nombre del equipo
  - <Portnum>: Número de puerto de escucha.
  - <Colour>: Formato del color (Escrito en hexadecimal).
  - <type>: Tipo de datos que recolectara (Netflow).

Ejemplo:

- 'NOMBRE' => { 'port' => '2001', 'col' => '#00aa00','type' => 'netflow' },

Añadir todos los equipos que generarán estadísticas en formato Netflow, separados por “,” :

- *%sources = (*
  'upstream1' => { 'port' => '9995', 'col' => '#0000ff', 'type' => 'netflow' },
  'peer1' =>{ 'port' => '9996', 'col' => '#ff0000' },
  'routin2' => { 'port' => '9997', 'col' => '#00aa00','type' => 'netflow' },
  );

Guardar el archivo de configuración y reiniciar el servicio de nfsen:

```
#       cd /var/lib/netflow/nfsen-1.3.2/bin
#       ./nfsen reconfig
```

El script preguntará si se desean borrar los datos antiguos de los equipos. Dependiendo de la opción que se seleccione, el script procede a configurar y añadir a los nuevos equipos. Al momento que el script termina de realizar los cambios, acceder a la interfaz web y observar los nuevos equipos añadidos en la página de inicio del software Nfsen.

Acceso a Nfsen

Página de inicio de Nfsen.

Para acceder a la interfaz web del software Nfsen, en un navegador web ejecutar la siguiente URL y autenticarse:

- https://ip_host/nfsen/nfsen.php
  - User: admin
  - Password: *****,

Aparece una ventana de inicio similar a la siguiente.

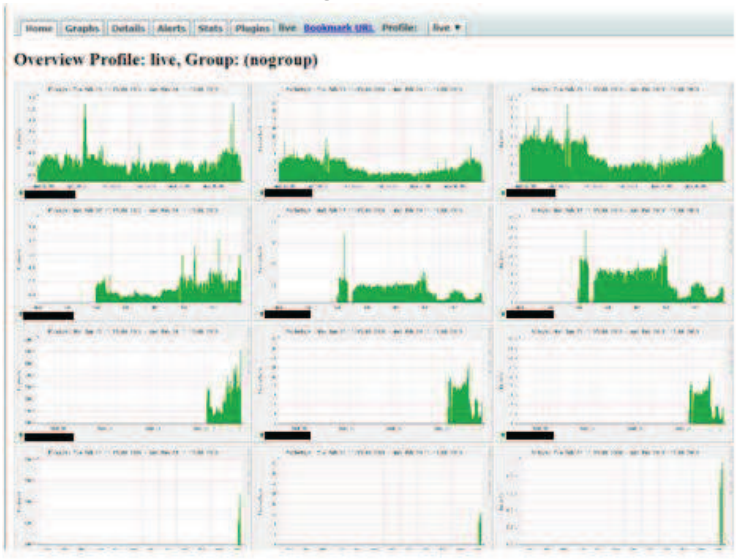


Figura C.1 Ventana de inicio del software Nfsen.

Nfsen por default captura información proveniente de los routers configurados cada 5 minutos y muestra esta información en el profile “live”, este profile captura todos los datos provenientes de los routers y gráfica estos datos.

Menú principal

La siguiente imagen muestra el menú de opciones del software Nfsen:

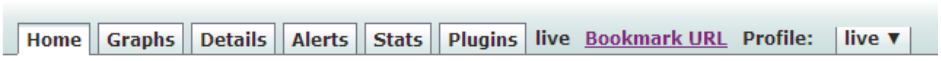


Figura C.2 Menu del software Nfsen.

Home

La opción **Home** se carga por default y muestra todas la gráficas generadas (hora, semana, día y mes).

Las gráficas están divididas en 4 grupos de 3 graficas cada grupo. De la siguiente forma.

- Gráfica los flujos, paquetes y el tráfico generado cada hora.
- Gráfica los flujos, paquetes y el tráfico generado cada día.
- Gráfica los flujos, paquetes y el tráfico que se generado cada semana.
- Gráfica los flujos, paquetes y el tráfico que se generado cada mes.

Graphs

La opción **Graphs** permite observar mejor las gráficas generadas.

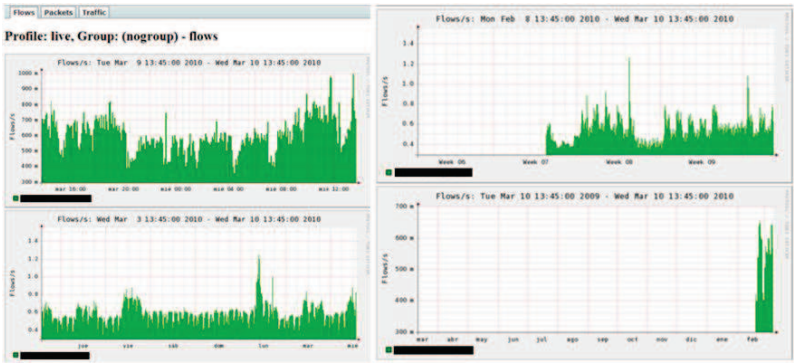


Figura C.3 Ventana correspondiente al menu “graphs” en el software Nfsen.

Tanto en la opción **Home**, como en la opción **Graphs**, es posible dar clic en cualquier gráfica y acceder a la opción **Details**, esta sección permite observar detalladamente el comportamiento de la gráfica seleccionada.

Details

Esta opción permite visualizar en la gráfica los datos capturados en tiempo real y, en base a estos datos, permite realizar análisis aplicando filtros con condiciones específicas.

Figura C.4 Ventana correspondiente al menu “details” en el software Nfsen.

En la imagen mostrada, se observa una gráfica principal, previamente seleccionada, dicha gráfica esta generada de manera general (sin tomar en cuenta ningún filtro) y muestra la cantidad de flujos capturados.

En la parte superior de la imagen, se observan cuatro gráficas, estas graficas desglosan la información de acuerdo a lo que se capturo en el protocolo TCP, UDP, ICMP y otros.

En la parte derecha de la gráfica principal se observan las gráficas obtenidas para los paquetes y el tráfico.

Las letras:

Profileinfo:
Type: live
Max: unlimited
Exp: never
Start: Feb 17 2010 - 14:55 CST
End: Feb 24 2010 - 12:05 CST

t_{start} 2010-02-24-00-05
t_{end} 2010-02-24-00-05

Muestran información de la gráfica en un punto de observación específico, de la siguiente forma:

- ***Type:*** Indica el tipo de profile que se está observando, en este caso es el profile default "Live".
- ***Max:*** Indica el máximo tamaño que tendrá el colector para guardar sus datos (en este caso ilimitado).
- ***Exp.*** Indica el tiempo en el cual el colector dejará de recolectar datos (en este caso nunca).
- ***Start.*** Indica la fecha en la cual se empezaron a capturar los datos.
- ***End.*** Indica la fecha (Momentánea) en la cual se termina de capturar los datos, normalmente es el último archivo capturado en el momento que se observa la gráfica.
- t_{start}**:** Tiempo específico que se está observando (En este caso es el 24/02/2010 00:15hrs). Esto es utilizado para obtener información sobre la cantidad de flujos, paquetes y el tráfico que se generó en ese momento en las tablas.
- t_{end}**:** Tiempo en el cual terminara de observarse (Utilizado en la opción "Time Window").

Las siguientes opciones permiten navegar en la gráfica:

Figura C.5 Panel de navegación en las gráficas del software Nfsen.

En el campo **select** se puede seleccionar:

- ***Single Timeslot:*** Muestra información de un flujo capturado.
- ***Time Windows:*** Permite seleccionar el tiempo de inicio y el tiempo final de la captura, en base a esto se observa un promedio de los flujos capturados en ese rango de tiempo.

En el campo ***display*** permite observar la graficas en diferentes periodos de tiempo (cada 12 horas, diario, cada 2 días, semanalmente, cada mes, etc.

Es posible observar un dato específico moviendo el cursor ubicado en la gráfica o dar clic en el área de interés.

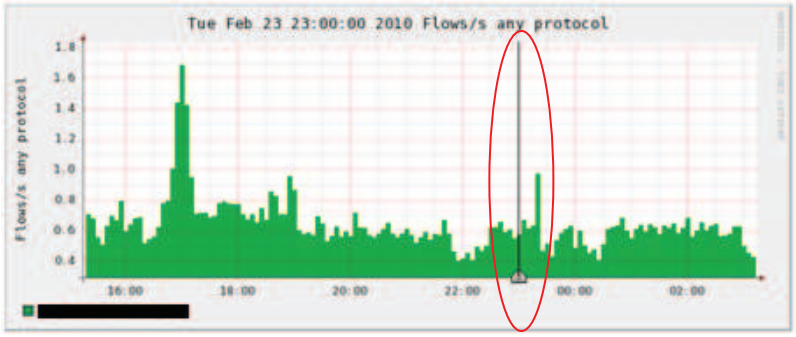
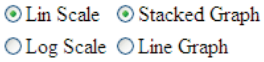


Figura C.6 Grafica creada en el software Nfsen.

- El botón "**<<**" permite regresar en la gráfica el tiempo seleccionado en "Display".
- El botón "**<**"permite regresar a la captura anterior.
- El botón "**|**"centra el cursor.
- El botón "**^**"permite centrar el cursor en el máximo pico encontrado.
- El botón "**>**"permite ir a la captura siguiente.

- El botón **">>"**permite adelantar la gráfica el tiempo seleccionado en "Display"
- El botón **">|"**redirige el cursor al último valor capturado.

Las opciones ***"Lin Scale"***, ***"Stacked Graph"***, ***"Log Scale"***, ***"Line Graph"*** son utilizadas para dar formato a la gráfica. De la siguiente forma:



- **Lin Scale:** Escala de la gráfica en formato lineal.
- **Log Scale:** Escala de la gráfica en modo logarítmico.
- **Stacked Graph:** Dibuja todo el contorno de la gráfica.
- **Line Graph:** Solo dibuja la línea superior de la gráfica.

La parte ***"Stadistic"*** se observa una tabla que contiene información del total de los flujos, paquetes y el tráfico capturados en ese instante de tiempo, esta información se divide en cuatro filas (All, tcp, udp, icmp).

La información se puede visualizar en dos formas.

- "***Rate":*** Se observa la información en base al tiempo [S].

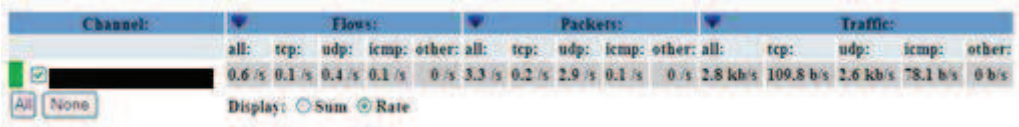


Figura C.7 Estadisticas correspondientes a la opción "Rate" en el software Nfsen.

- ***"Sum":*** Se observa la información en base al ancho de banda consumido.

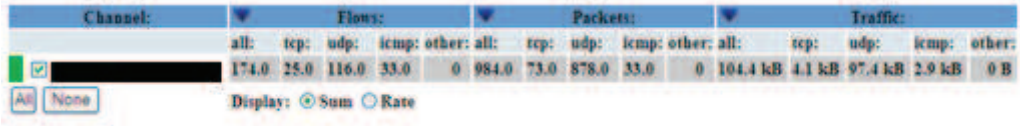


Figura C.8 Estadisticas correspondientes a la opción "Sum" en el software Nfsen.

La última parte de esta sección "**netflow processing**", permite aplicar filtros específicos para observar información de manera detallada.

Figura C.9 Filtros a aplicar sobre flujos.

En la opción ***"source"*** seleccionamos el colector sobre el cual deseamos realizar un análisis más detallado.

Filtros.

Los filtros son operaciones específicas que permiten acotar la información. Para la creación de filtros se utiliza la siguiente sintaxis:

expr and expr, expr or expr, not expr, (expr)

Se puede aplicar múltiples filtros mediante el uso de los operadores lógicos:

- ✓ and
- ✓ or
- ✓ not

Los campos 'expr' pueden ser sustituidos por las siguientes opciones.

- Protocolo: **proto TCP, UDP, ICMP, GRE, ESP, AH, RSVP**
  o**proto num**(donde *'num'* es el número del protocolo)
- Puerto: ***port num*** (Donde 'num' representa el número del puerto).
- IP: ***ip a.b.c.d*** (donde 'a.b.c.d' representa el número de la dirección IP).
- IP Origen: ***src ip a.b.c.d***
- IP Destino: ***dst ip a.b.d.c***
- Red: ***net a.b.c.d m.n.r.s*** (donde 'm.n.r.s' representa la máscara correspondiente en decimal.
  Ó ***net a.b.c.d/num*** (donde 'num' representa los números de unos encendidos en la máscara.
- Red origen: ***src net a.b.c.d/num***
- Red destino: ***dos net a.b.c.d/num.***

Nfdump soporta las opciones de comparación: "**<, >, =, ==**"

- Packetes ***packets comparador num*** (donde 'num' será el número a comparar).
- Bytes ***bytes comparador num***
- Flujos ***flow comparador num***
- Bandera activa: ***flags Y*** (donde 'Y' es la letra inicial de la bandera utilizada).

Banderas. Nfdump provee de una serie de banderas que pueden estar activas e indicar información del estado de la red. Las banderas usadas por el colector Nfdump son las siguientes:

A ACK
S SYN
F FIN
R Reset
P Push
U Urgent
X All flags on

Ejemplos de la creción de filtros:

1) Realizar un filtro para observar todo el flujo que pasa a través de la dirección IP 192.168.1.32
   ip 192.168.1.32

2) Realizar un filtro para observar todo el flujo que pasa a través de la IP origen 192.168.1.32 hacia la IP 192.168.233.33
   src ip 192.68.1.32 and dst ip 192.168.1.33

3) Realizar un filtro que observe todo el flujo que pasa a través de la red origen 192.168.0.0 con la bandera SYN activada, u observar lo que pasa a través de la red destino 192.168.2.0 donde todos los bytes sean mayores a 100.
   (src net 192.168.0/24 and flags S) or (dst net 192.168.1/24 and bytes >100)

Alertas.

Una alerta es una acción específica que se ejecuta en el profile “live”. Si se cumplen la(s) condicione(s) programadas en la alerta, se ejecutan ciertas acciones, como el enviar un correo electrónico al administrador o el ejecutar algún trigger o plugin que realizará alguna acción en específico.

Toda alerta debe de ser creada en el profile live y debe de cumplir con el siguiente esquema:

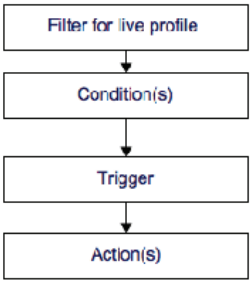


Figura C.10 Esquema de ejecución de una alerta.

En la opción ***“Alerts”*** del menú principal del software Nfsen es un donde se crean y administraran las alertas de la siguiente forma.

En el menú alertas, seleccionar el botón “+” (add new alert), aparece la siguiente ventana:

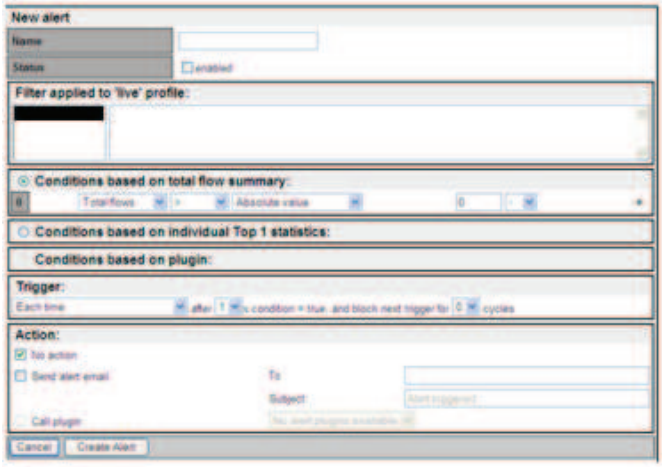


Figura C.11 Ventana de creación de una alerta

- ✓ La sección “Filter applied to 'live' profile:” es utilizada para aplicar filtros a esta alerta
- ✓ Seleccionar la opción “Enabled”.
- ✓ Seleccionar alguna de las 3 opciones de acuerdo a la acción que se desee realizar en la alerta:
  - **Conditions based on total flow summary.** Esta opción permite habilitar varias condiciones que se deberán de cumplir para que la alerta sea ejecutada.

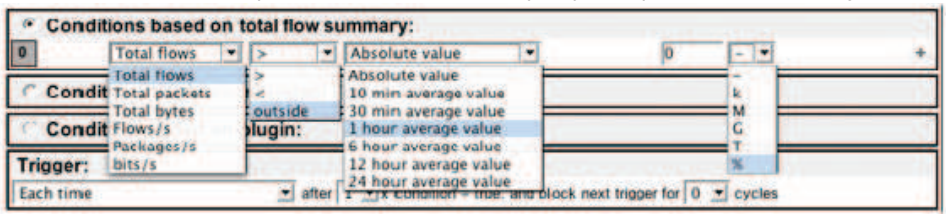


Figura C.12 Posibles condiciones a aplicar en una alerta

- **Conditions based on individual Top 1 statistics.** En esta opción, se deberá de cumplir la condición o condiciones deseadas, con la característica que se basara en estadísticas topN (primer lugar de la lista).

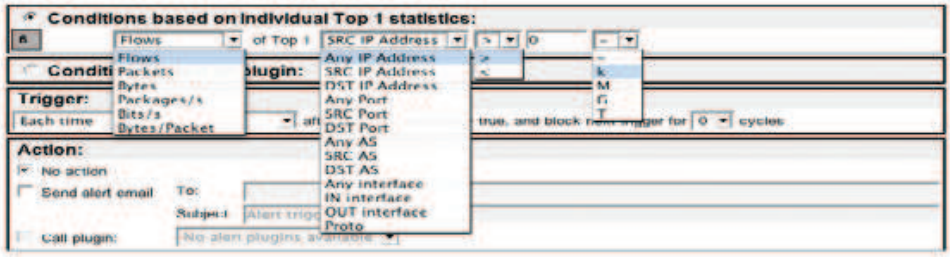


Figura C.13 Posibles condiciones a aplicar en una alerta basándose en estadísticas TOPN

- **Conditions based on plugin.**Un plugin es unaacción programada por el usuario, la cual se deberá de cumplir para que se ejecute la alerta.

Trigger.
Al momento en que las condiciones se cumplen, se ejecuta un trigger. Este trigger puede ser programado para que se ejecute una sola vez o se ejecute cada que la condición sea verdadera.

Al activarse un trigger realiza una acción específica, como puede ser: mandar un email al administrador o ejecutar algún plugin específico.

Estados de alerta.

inactive	Indica que la alerta no se está ejecutando.
armed	La alerta esta activa y es evaluada cada ciclo hasta que se cumpla la condición.
armed 1/3	La alerta esta activa y es evaluada cada ciclo. Al momento que una condición sea verdadera, se necesitará que las siguientes dos condiciones (los siguientes dos ciclos) sean verdaderos para que se ejecute esta alerta.
fired	La alerta esta activa y es evaluada cada ciclo. El trigger se ejecuta en el último ciclo y realiza la acción indicada.
fired --	Esta alerta solo se dispara una sola vez y volverá a estar activa, a menos que se reactive manualmente.
blocked 1:2	La alerta esta activa pero se bloquea cada dos ciclos. En el siguiente ciclo se continúa ejecutando normalmente.

Ejemplo de creación de alertas.
Crear una alerta que observe todo tráfico a través del protocolo tcp y que cumpla con las siguientes condiciones para que se ejecute:

- La cantidad de flujos/segundo sea mayor en un diez por ciento al valor promedio que fluye cada 30 minutos.
- La cantidad de paquetes/segundo sea mayor en un veinte por ciento al valor promedio que fluye cada 30 minutos.
- La cantidad de bit/segundo sea mayor en un diez por ciento al valor promedio que fluye cada 30 minutos.

- La alerta se active cada que se detecte un valor anormal en tres ciclos seguidos y se envié un email para notificar.

Filtro aplicado: proto tcp
Condiciones:

- Flows/s > 30 min average value + 20%
- && Packages/s > 30 min average value + 20%
- && Bit/s > 30 min average value + 10%

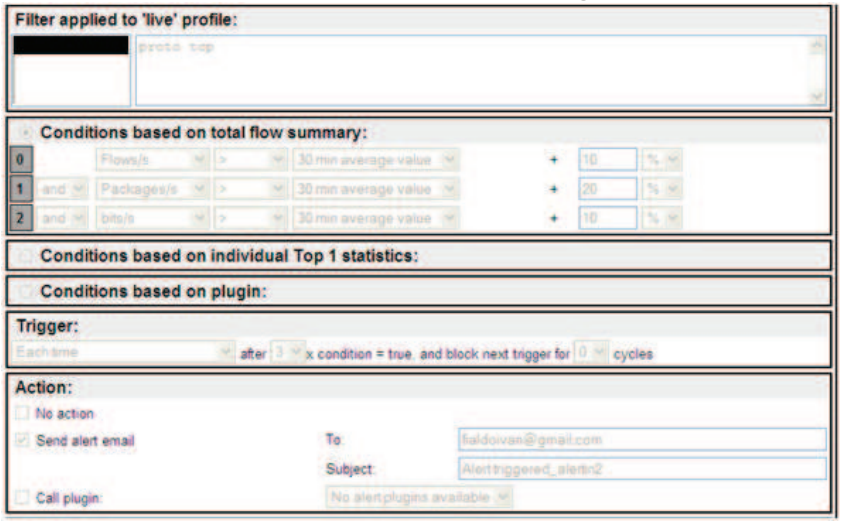


Figura C.14 Ejemplo de creación de una alerta

Después de ejecutar la alerta 8 horas, se observa la siguiente grafica generada:

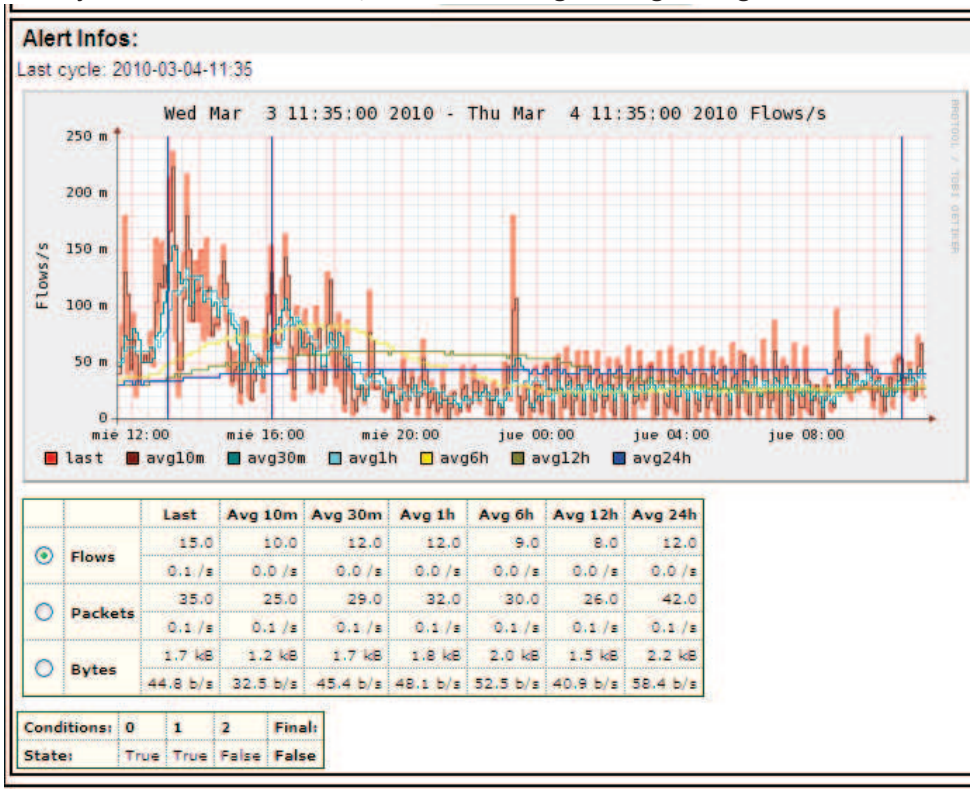


Figura C.15 Ejemplo de una alerta en ejecución

La gráfica mostrada es una comparación del valor obtenido en el ciclo pasado (cada cinco minutos) en comparación con los valores calculados cada diez minutos, treinta minutos, una hora, seis horas doce horas, veinticuatro horas.

En la tabla se muestran los valores obtenidos y las condiciones evaluadas. Toda condición se evalúa con lo calculado el ciclo pasado en comparación con las condiciones deseadas. Se aplica una operación and, en la cual todos los valores deben de cumplirse para activar el primer ciclo de la alerta.

Profile.

Un profile es un punto de vista específico de los routers. Se pueden crear diferentes profiles que realicen diferentes acciones, como observar el tráfico que pasa a través de puertos conocidos, u observar el comportamiento de ciertas direcciones IP o redes, etc.

Los profiles pueden pertenecer a estos grupos:

- **Históricos.** Se define el tiempo inicial y el tiempo final de observación de datos que se han obtenido en el pasado (datos ya capturados).
- **Continuos.** Este tipo de profile empieza a capturar datos en una fecha específica y se continuara ejecutando en cada actualización del software Nfsen.
- **Shadow.** Estos profiles no recolectan datos de con formato Netflow.

Canales.

Al momento de definir un profile, es posible anexar uno o varios canales. Un canal es un punto de observación específico, el cual genera datos que se observarán tanto en la gráfica como en la tabla correspondiente al instante de tiempo observado.

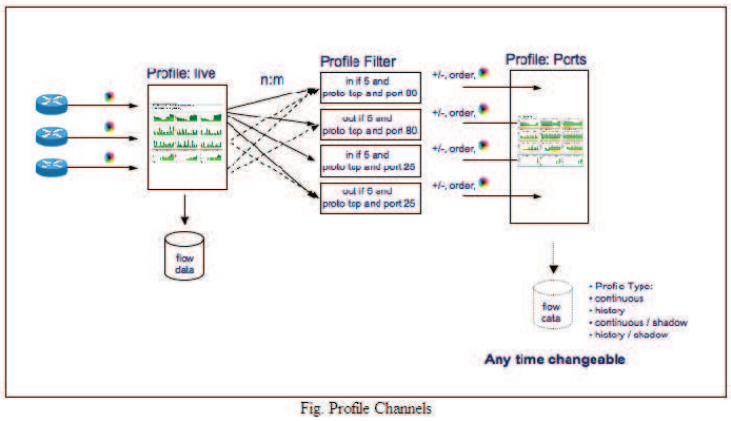


Fig. Profile Channels

Figura C.16 Esquema de creación de un profile

Al momento de definir un canal, es necesario aplicar un filtro específico.

Los canales pueden estar definidos en una o más fuentes de información (colectores) y son independientes del número de fuentes de información.

Creación de un profile.

En la pestaña live. Seleccionar new profile.

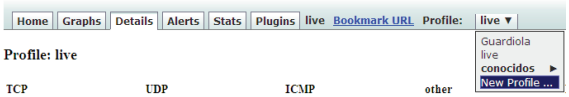


Figura C.17 Creación de un nuevo profile

Aparecerá la siguiente ventana:

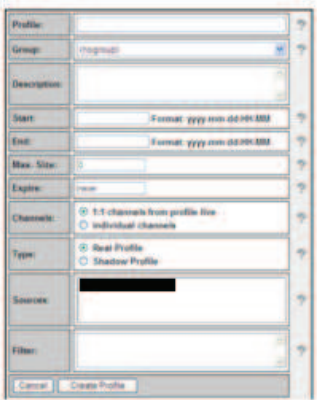


Figura C.18 Datos requeridos en la creación de un profile

Si se desea, agrupar el nuevo profile a un grupo. En la opción ***'start'*** seleccionar el día en el cual empezará a operar el profile (formato aaaa-mm-dd-hh-minmin), debe de existir alguna captura realizada por nfcapd que corresponda al día seleccionado.

Las opciones '**Max Size'** y '**Expire'** dependen del número de canales que se desean seleccionar y del tipo de profile.

En la opción '**channels'** se puede seleccionar alguna de estas dos opciones:

- **1:1 channels from profile live:** Al seleccionar esta opción solo se tiene 1 canal, en la opción '***filter'***, escribir el filtro.
- **Individual channels:** Al seleccionar esta opción el profile se compondrá de múltiples channels, cada canal creado deberá de tener su propio filtro.

En la opción '**type'** seleccionar el tipo de profile que se desea crear:

- **Real profile:** Profile que se basa en datos en formato Netflow y pude ser histórico o continuo.
- **Shadow profile:** Profile que no se basa en datos en formato Netflow.

En la opción '**sources'** seleccionar el colector (router) que se desea analizar.

Una vez seleccionados todos los datos, crear el profile seleccionando el botón "***create profile***". Si el profile se compone de un solo canal inmediatamente se creará y se podrá observar su funcionamiento, en caso de que se componga de múltiples canales el profile se crea, pero se tendrán que agregar los canales correspondientes.

Cuando el profile es creado, aparece la siguiente frase.

Esta frase Indica que se ha creado correctamente el profile. En el menú principal de Nfsen, seleccionar la opción "Stats" para observar la información creada del profile.

Para este ejemplo se ha creado un profile llamado 'protocolos', este profile pertenece al grupo 'conocidos' y contiene múltiples canales.

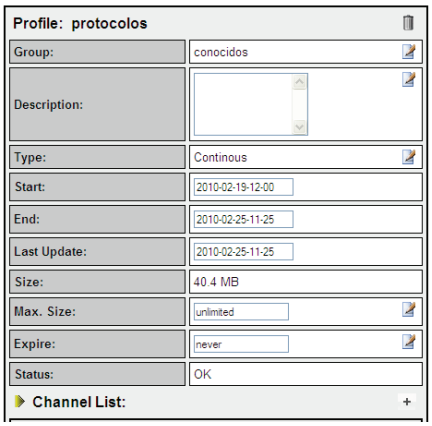


Figura C.19 Ejemplo de creación de un profile

Agregar un canal.

Ahora se procederá a crear los canales correspondientes para este profile.

Para cada canal que se desea agregar, dar clic en el botón "Add new channel" (+):

Figura C.20 Ventana de creación de un canal

Escribir el nombre del canal. En la opción "**Colour"** seleccionar el color que distingue a este canal (este color será para observar su comportamiento tanto en la gráfica como en la tabla), es posible seleccionar un amplio abanico de colores en la opción color ***'picker'***

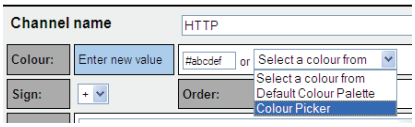


Figura C.21 Diversos métodos de seleccionar colores en el canal a crear

Una vez seleccionado el color. En la opción "**filter**", crear el filtro de acuerdo a las necesidades requeridas, en este ejemplo se aplicó el siguiente filtro:

- Port 80

En la opción **"sources",** seleccionar el colector a observar, se pueden seleccionar múltiples colectores. Para añadir estos colectores al nuevo canal, dar clic en el botón ***">> ".*** La fuente seleccionada se mueve de ***Avaliable Sources*** a **Selected Sources**.

Finalmente, dar clic en el botón ***'Add Channel'*** para agregar el nuevo canal en el profile protocolos.

Figura C.22 Ejemplo de creación de un canal

Quedando el profile de la siguiente forma:

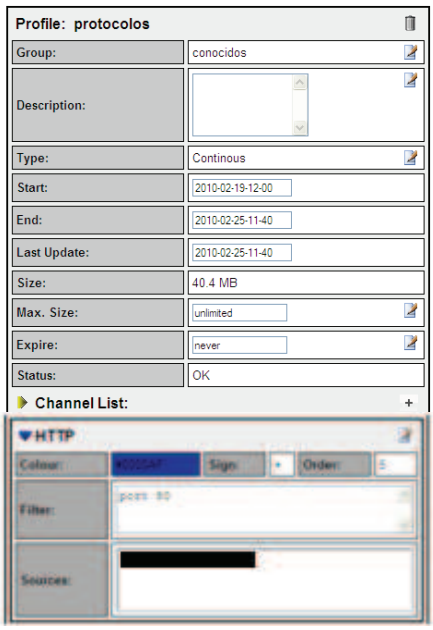


Figura C.23 Ejemplo de creación de un profile con sus canales

Para este profile además del puerto http se agregaron los puertos ftp, ssh, telnet, smtp, snmp con el mismo procedimiento. Una vez creados todos los canales, en la opción "***Status***" se observa la leyenda "new", dar click en ***"Commit new profile"*** (√).

En la siguiente figura, se observa el proceso de construcción del profile (en la parte status aparece build % - locked)

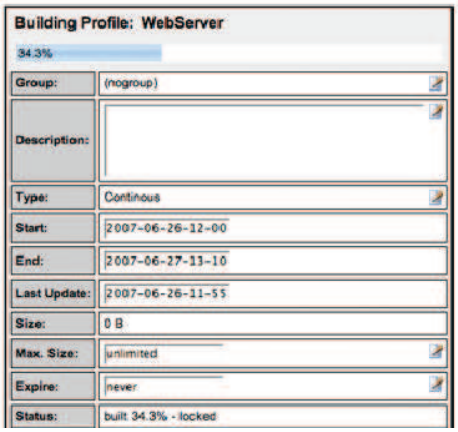


Figura C.24 Proceso de construcción de un profile

Al terminar de construirse el profile correctamente, se observa en la opción ***'status'*** la leyenda OK, quedando el profile de la siguiente forma:

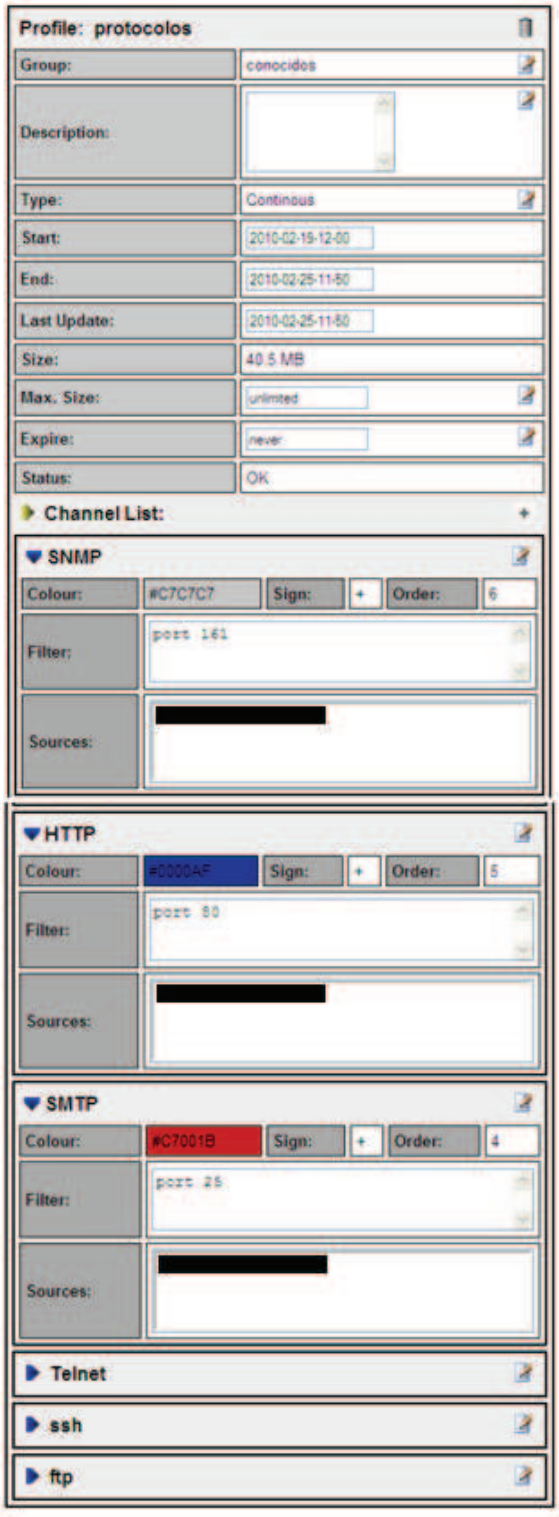


Figura C.25 Ejemplo completo de creación de un profile con sus canales

Es posible observar en la opción del menú home, las gráficas creadas correspondientes a este perfil.

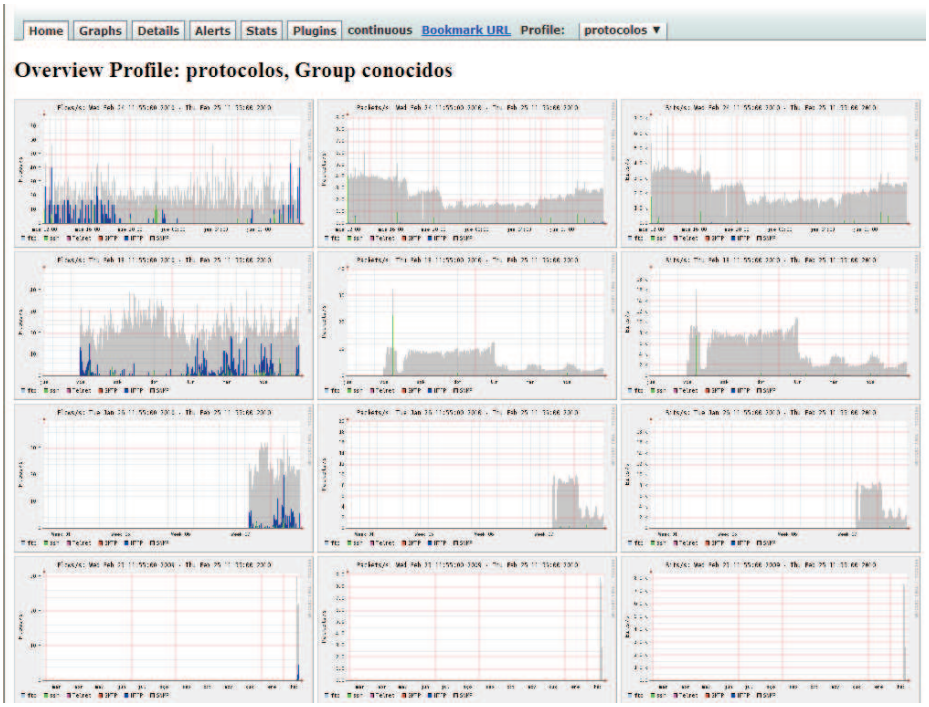


Figura C.26 Gráficas creadas por un profile

Al seleccionar cualquier gráfica al igual que en el profile live, se pueden obtener datos de una manera más detallada.

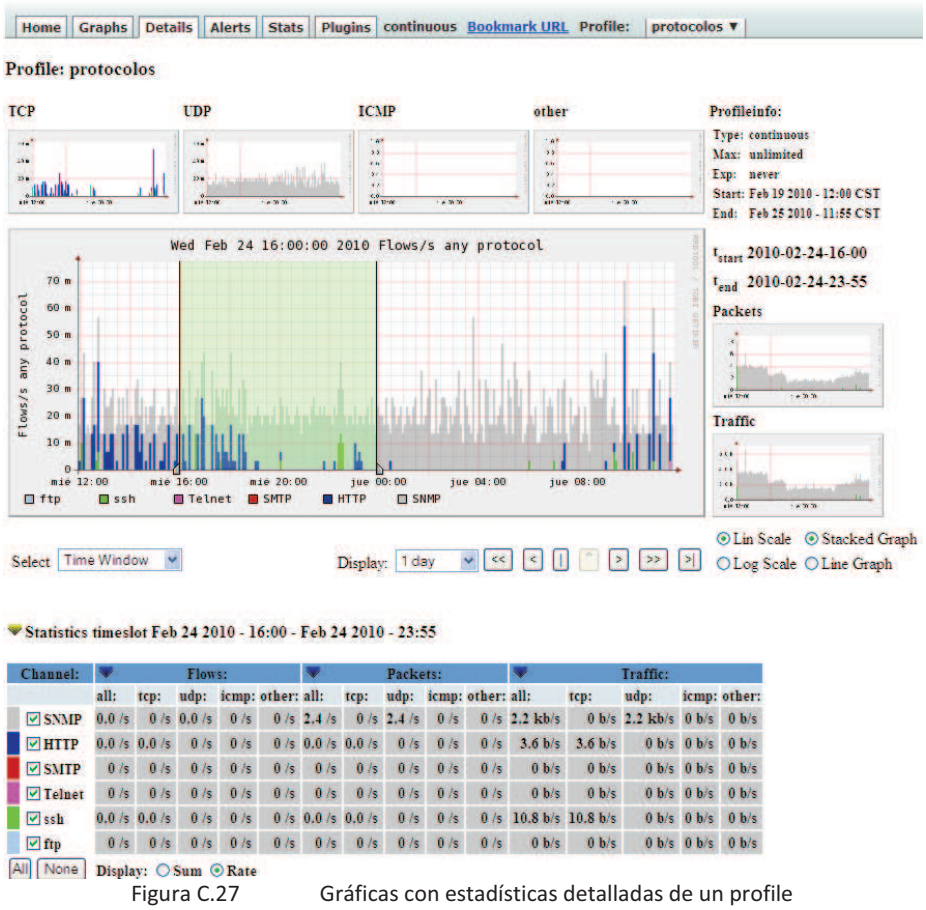


Figura C.27 Gráficas con estadísticas detalladas de un profile

Y aplicar filtros específicos para realizar análisis específicos sobre los profile creados.

Plugin.

Los plugins son una potente herramienta utilizada por el software Nfsen, que permiten añadir programación exterior de acuerdo a las necesidades requeridas. Por medio de plugins creados en Nfsen se logra hacer a este software tan potente como se desee; además de enfocarlo hacia análisis de seguridad, poner precio al tráfico consumido, generar gráficas muy detalladas, entre otras cosas.

En el capítulo 3, sección 3.3.2.4 se describieron los tipos de plugins que soporta el software Nfsen, en esta parte se describirán las subrutinas y configuración necesarias para la creación de un plugin.

Creación de un plugin Backend.

Un plugin backend es escrito como un módulo en perl. Cualquier plugin backend escrito debe de contener el siguiente código:

```
# Name of the plugin
package PluginName;
use strict;

# This string identifies the plugin as a version 1.3.0 plugin.
our $VERSION = 130;

sub Init {
return 1;
}
1;
```

La subrutina 'init' es inicializada cuando el plugin es cargado, con el propósito de dar la posibilidad de que el plugin se ejecute por sí mismo. La función init regresa '1' si se cargó correctamente o '0' se existió algún error.

Dependiendo de la función del plugin, se pueden añadir otras subrutinas, estas subrutinas son:

Cleanup.

Subrutina creada para limpiar el plugin, cuando el software Nfsen termina se ejecución. El propósito de esta subrutina es dar la posibilidad al plugin de terminar por sí mismo, sin necesidad de tener que terminar el proceso forzosamente. El código de esta subrutina es el siguiente:

```
sub Cleanup {
syslog("info", "demoplugin Cleanup");
# not used here
}
```

run

Subrutina necesaria cuando el plugin es recargado en cada actualización del software Nfsen. El código necesario en esta subrutina es el siguiente:

```
sub run {
my $profile = shift;
my $timeslot = shift;
syslog('debug',"Plugin escaneo run: Profile: $profile, Time: $timeslot");
## Añadir codigo aqui
}
```

alert_condition

Subrutina necesaria cuando un plugin es utilizado como un módulo requerido para la ejecución de una alerta, como se observa en la figura.

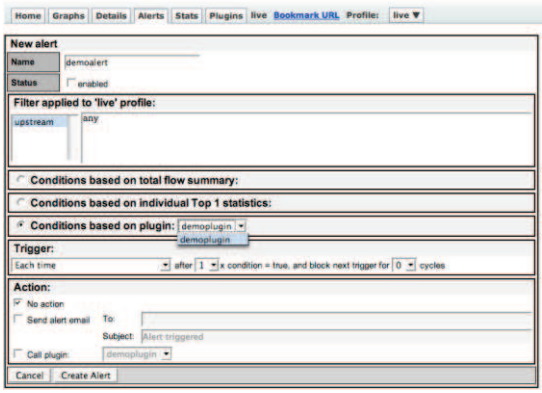


Figura C.28 Ventana de creación de un plugin

La subrutina 'alert_condition' es llamada después de que es aplicado el filtro. El archivo resultado es guardado en el directorio de la alerta. Y este archivo es pasado como parámetro a la subrutina. La subrutina devuelve 1 si las acciones programadas en ellas se cumplen, en caso contrario devuelve 0. El código necesario en esta subrutina es el siguiente:

```
sub alert_condition {
my $argref = shift;
my $alert     = $$argref{'alert'};
my $alertflows = $$argref{'alertfile'};
my $timeslot   = $$argref{'timeslot'};

syslog('info', "Alert condition called: alert: $alert, alertfile: $alertflows, timeslot: $timeslot");
      # Add your code here

return 1;
}
```

alert_action

Esta función es necesaria cuando se crea un plugin con el objetivo de observar por qué se ejecutó la alerta. El código de esta subrutina es el siguiente:

```
sub alert_action {
my $argref = shift;

my $alert    = $$argref{'alert'};
my $timeslot = $$argref{'timeslot'};

syslog('info', "Alert action function called: alert: $alert, timeslot: $timeslot");
      # Add your code here

return 1;
}
```

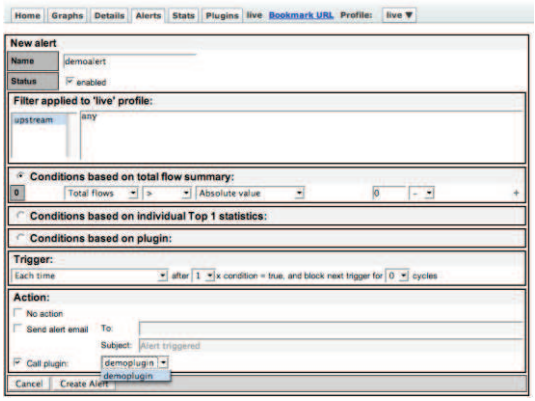


Figura C.29 Ventana de creación de un plugin seleccionando la opción "alert_action"

Creación de plugins Frontend.

Un plugin frontend es escrito como un módulo en php. Permite visualizar, en la interfaz web del software Nfsen, el resultado del módulo backend ejecutado. Cualquier plugin frontend escrito debe de contener el siguiente código:

```
<?php
/*
 * nameplugin_ParseInput is called prior to any output to the web browser and is intended for the plugin to parse possible form data. This function is called only, if this plugin is selected in the plugins tab. If required, this function may set any number of messages as a result of the argument parsing.The return value is ignored.
 */
functionnameplugin_ParseInput( $plugin_id ) {
        //your code here
} // End of nameplugin_ParseInput
/*
 * This function is called after the header and the navigation bar have  been sent to the browser. It's now up to this function what to display.
 * This function is called only, if this plugin is selected in the plugins tabIts return value is ignored.
 */
functionnameplugin_Run( $plugin_id ) {
        // your code here
} // End of nameplugin_Run
?>
```

La función utilizada en la creación de un plugin frontend, es 'nameplugin_Run', esta función recibe como parámetro el ID correspondiente del plugin. Y en base a este parámetro se asocia al plugin backend.

Configuración de plugin en Nfsen.

Para que un plugin pueda ser ejecutado por Nfsen, es necesario añadir al plugin en el archivo "nfsen.conf", buscar la siguiente línea:

```
#Example
@plugins = (
    # profile # module
[ '*', 'demoplugin' ],
);
```

En el arreglo "plugins" se guarda la información de cada plugin añadido al software Nfsen, con el siguiente formato:

- En el primer campo se observa al símbolo '*', este símbolo indica que el plugin es aplicable a cualquier profile y se actualiza periódicamente. Si se desea que el plugin sea ejecutado como una condición de alerta, se añade el símbolo '!'.
- En el segundo campo, se escribe el nombre del plugin a agregar en el Software Nfsen.

En este caso se añadió el plugin escaneo como un módulo que se actualiza periódicamente:

```
@plugins = (
   # profile    # module
[ '*', 'demoplugin' ],
[ '*',    'escaneo'],
);
```

Reiniciar el servicio de nfsen para que surjan efecto los cambios realizados.

```
#          /Listry-AIGC/nfsen-1.3.2/bin/nfsen reload
```

En el archivo "/var/log/messages", se observa que se han cargado los dos plugin exitosamente.

```
# tail -100 /var/log/messages | grep nfsen
Jan  9 23:01:54 localhost nfsen[6660]: Startup. Version: 1.3.2 $Id: nfsend 14 2009-06-10 08:07:06Z haag $
Jan  9 23:01:54 localhost nfsen[6662]: Comm server started: [6662]
Jan  9 23:01:54 localhost nfsen[6661]: nfsend: [6661]
Jan  9 23:01:54 localhost nfsen[6662]: Frontend module 'demoplugin.php' found
Jan  9 23:01:54 localhost nfsen[6662]: Loading plugin 'demoplugin': Success
Jan  9 23:01:54 localhost nfsen[6662]: demoplugin: Init
Jan  9 23:01:54 localhost nfsen[6662]: Initializing plugin 'demoplugin': Success
```

```
Jan  9 23:01:54 localhost nfsen[6662]: plugin 'demoplugin': Profile plugin: 1, Alert condition plugin: 1, Alert action plugin: 1
Jan  9 23:01:54 localhost nfsen[6662]: Frontend module 'escaneo.php' found
Jan  9 23:01:55 localhost nfsen[6662]: Loading plugin 'escaneo': Success
Jan  9 23:01:55 localhost nfsen[6662]: ** Important **: Plugin 'escaneo' is a legacy plugin.
Jan  9 23:01:55 localhost nfsen[6662]: Escaneo: Init
Jan  9 23:01:55 localhost nfsen[6662]: Initializing plugin 'escaneo': Success
```

Visualizar en la Ventana Plugin que se han cargado exitosamente ambos plugin.

Figura C.30 Ejemplo de ejecución de los dos plugins creados

OpenWebmail

El software OpenWebmail es una potente herramienta que permite la visualización y administración de correos electronicos. En el anexo B se describió como acceder a este software. En esta sección se describiran aspectos escenciales en el uso de este software.

Enviar correos con OpenWebmail.

- En el menu principal del software OpenWebmail, dar click en new.

Figura C.31 Menu del software OpenWebmail

- Seleccionar el destinatario y archivo a adjuntar, en caso de requerirse
- Al terminar de escribir el correo, dar click en enviar.

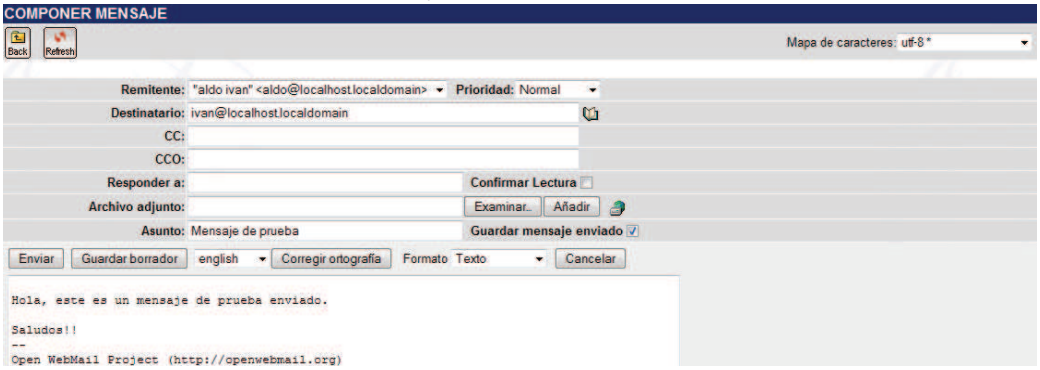


Figura C.32 Ventana de envió de un nuevo correo en OpenWebmail

Acceder con la cuenta “ivan” y visualizar el correo.

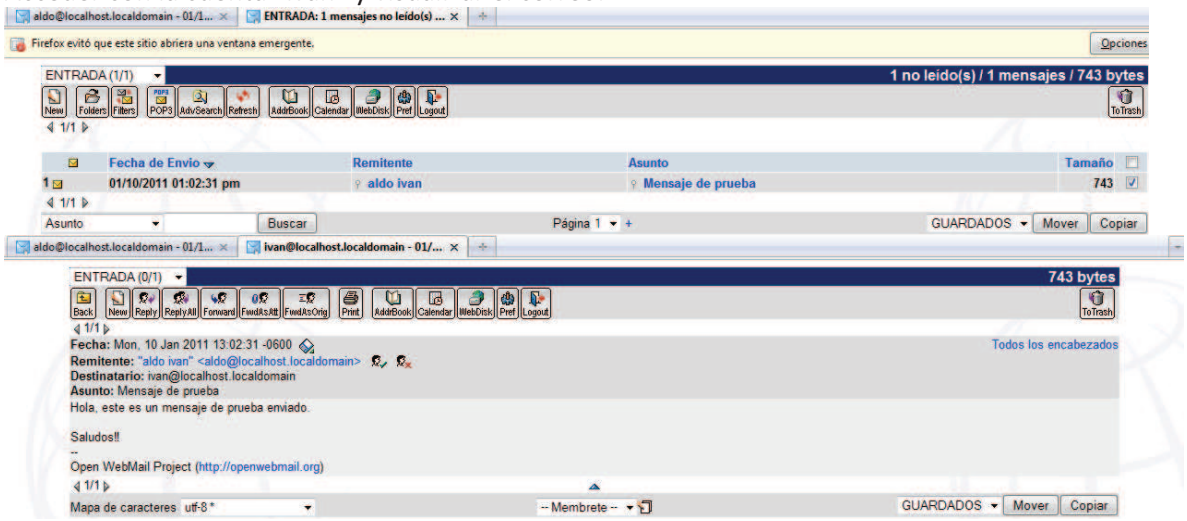


Figura C.33 Visualización de correos recibidos en OpenWebmail

El correo recibido puede ser agrupado en las carpetas: entrada, guardado, enviados, borrador, reenviar, papelera, spam, virus.

Búsqueda de correos

Otra característica importante del software OpenWebmail, es que permite realizar búsquedas muy detalladas de correos.

Al dar clic en “AdvSearch”, aparece una ventana que permite:

- Realizar búsquedas en correos enviados, recibidos, guardados, borradores o correos de detectados como SPAM o virus.
- Escribir el rango de fechas en la búsqueda.
- Seleccionar alguna parte específica del correo a realizar la búsqueda (remitente, destinatario, fecha, asunto, archivos adjuntados, contenido o todo).
- Acepta expresiones regulares para realizar búsqueda.

En este caso se creó un sencillo ejemplo que busca en los correos enviados por aldo@localhost.localdomain, todo correo que contenga la palabra "hola". El resultado se muestra en la figura.

Figura C.34 Busqueda avanzada de correos en OpenWebmail

Como resultado de la búsqueda se observa el correo enviado a ivan@localhost.localdomain. Este correo contiene la palabra "hola" en el cuerpo del mensaje.

Navicat.

Navicat es un software que permite la administración de bases de datos de forma muy simple. En el anexo B se explicó cómo acceder a este software y, crear bases de datos y tablas.

Acceder al contenido de tablas.

- Seleccionar la base de datos a usar y dar doble clic en cualquier tabla creada. En este caso se accedió al contenido de la tabla 'epuertos'

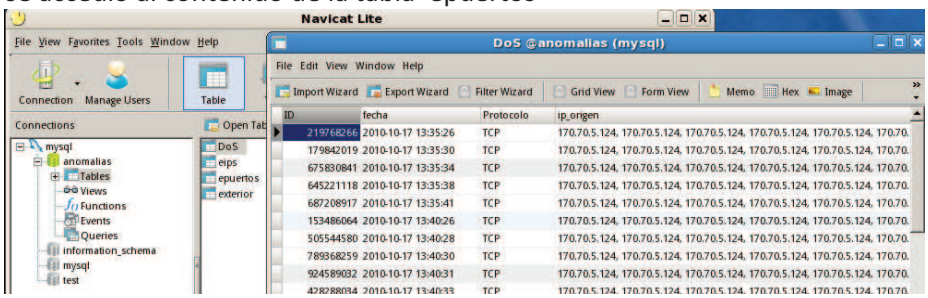


Figura C.35 Ejemplo de datos contenidos en la tabla "DoS"

- Es posible modificar los registros de la tabla al dar click en el registro y escribir el nuevo valor.

Realizar consultas a tablas.

Navicat permite de manera muy eficaz el realizar consultas en tablas de la siguiente forma:

- En el menú principal del software, seleccionar la opción query->new query
- Aparece una ventana en donde se realizan consultas con la sintaxis utilizada en MySQL.
- En este caso se realizó un query que muestre los registros en la tabla 'DoS' con fecha 2010-10-17 entre las 13:35 y 13:40.
- El resultado de este query se muestra en la figura.

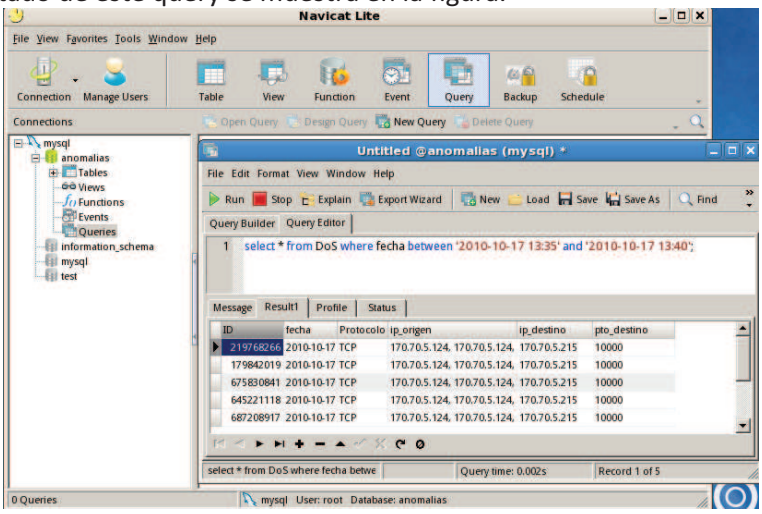


Figura C.36 Consulta realizada a la tabla "DoS" en Navicat

Además, el software Navicat permite:

- Crear funciones
- Realizar vistas en tablas
- Crear respaldos de bases de datos
- Programar tareas que se ejecutan a cierta hora
- Entre otras acciones.