



Usando NfSen

Qué vamos a hacer

1. Su enrutador ya debería estar enviando flujos a cada PC en su grupo
2. Asegúrese de que NfSen está activo mirando en la página web y confirmando que puede ver los gráficos sin ningún error
3. Ahora veremos qué tipo de tráfico está pasando a través del router de su grupo

Cree una estadística para graficar tráfico específico

- Abra la página de NfSen y oprima 'live' en la esquina superior derecha y seleccione "New Profile ..." – *Es posible que tenga que hacerlo un par de veces ya que NfSen es quisquilloso.*
 - Escriba el nombre 'HTTP_TRAFFIC' como nombre de perfil y también cree un grupo llamado "grupoX" donde X es su número de grupo
 - Seleccione *individual channels y shadow profile*.
 - Individual channel – puede crear canales con nuestros propios filtros
 - Shadow profile – Ahorrar espacio en disco al no crear nuevos datos, sino analizar los datos existentes
- ➔ **Ve la página siguiente para una imagen de ejemplo...**

Profile:	HTTP_TRAFFIC	?
Group:	New group ... group1	?
Description:	edit	
Start:	Format: yyyy-mm-dd-HH-MM	?
End:	Format: yyyy-mm-dd-HH-MM	?
Max. Size:	10G	?
Expire:	60 Days	?
Channels:	☐ 1:1 channels from profile live ☒ individual channels	?
Type:	☐ Real Profile ☒ Shadow Profile	?
Cancel Create Profile		

Oprima "Create Profile"
abajo

Profile: HTTP_TRAFFIC 

Group:	group1 
Description:	
Type:	Continuous / shadow 
Start:	2012-10-11-21-0
End:	2012-10-11-22-5
Last Update:	2012-10-11-22-5
Size:	0 B
Max. Size:	unlimited
Expire:	never
Status:	OK
Channel List: 	

Oprima (+) al lado de 'Channel List' al fondo de la página luego llene el formulario como se indica y oprima 'Add Channel' al final.

El filtro "any" significa TODO el tráfico. Elija sus fuentes en "Available Sources" y presione ">>" para agregarlos al "Selected Sources". Haga clic en "add channel"

Channel name

Colour:	Enter new value #abcdef or Select a colour from						
Sign:	+						
Order:	1						
Filter:	any edit						
Sources:	<table border="1"><thead><tr><th>Available Sources</th><th></th><th>Selected Sources</th></tr></thead><tbody><tr><td> </td><td> << >> </td><td> rtr1 rtr2 </td></tr></tbody></table>	Available Sources		Selected Sources		<< >>	rtr1 rtr2
Available Sources		Selected Sources					
	<< >>	rtr1 rtr2					

Channel name		pc2							
Colour:	Enter new value	#FF0033 or Select a colour from	↓						
Sign:	+	Order:	2						
Filter:	src port 80 and dst host 10.10.1.2 edit								
Sources:	<table border="1"><thead><tr><th>Available Sources</th><th></th><th>Selected Sources</th></tr></thead><tbody><tr><td> </td><td> << >> </td><td> rtr1 rtr2 </td></tr></tbody></table>			Available Sources		Selected Sources		<< >>	rtr1 rtr2
Available Sources		Selected Sources							
	<< >>	rtr1 rtr2							
Cancel Add Channel									

Agregue otro canal oprimiendo (+) al lado de 'Channel List'. Rellene los detalles como se muestra a la izquierda. Sustituya pc2 por una PC de tu grupo distinto del tuyo. También sustituya la IP en el campo Filter para que corresponda con la IP de la PC en cuestión.

Con esto estaremos monitorizando cuánto tráfico HTTP está yendo a esa PC, cuánto se está descargando. En HTTP, las descargas siempre tienen el puerto 80 como fuente.

Asegúrese de cambiar el color. Puede usar el selector de colores o escribir un valor como el del ejemplo.

Seleccione los enrutadores de su grupo como "Sources" y oprima "Add Channel"

Active el perfil

- Oprima la marca verde para activar su perfil.
- Oprima Live, luego seleccione el grupo que ha creado y “HTTP_TRAFFIC” para ver su perfil. Luego oprima “Home” en el menú de la esquina superior izquierda

Profile: HTTP_TRAFFIC	
Group:	group1
Description:	
Type:	Continuous / shadow
Start:	2012-10-11-21-
End:	2012-10-11-21-
Last Update:	2012-10-11-21-
Size:	0 B
Max. Size:	unlimited
Expire:	never
Status:	new
Channel List:	
pc2	
Colour:	#FF0033
Sign:	+
Order:	2
Filter:	src port 80 and dst host 10.10.1.2

Descargue datos de HTTP a pcY

Ingresa en pcY y use el comando `wget` para hacer una descarga HTTP

```
ssh sysadm@pcY.ws.nsrc.org
```

```
$ cd /tmp
```

```
$ wget http://noc.ws.nsrc.org/downloads/BigFile
```

Cuando termine la descarga, puede borrar el archivo:

```
$ rm /tmp/BigFile
```

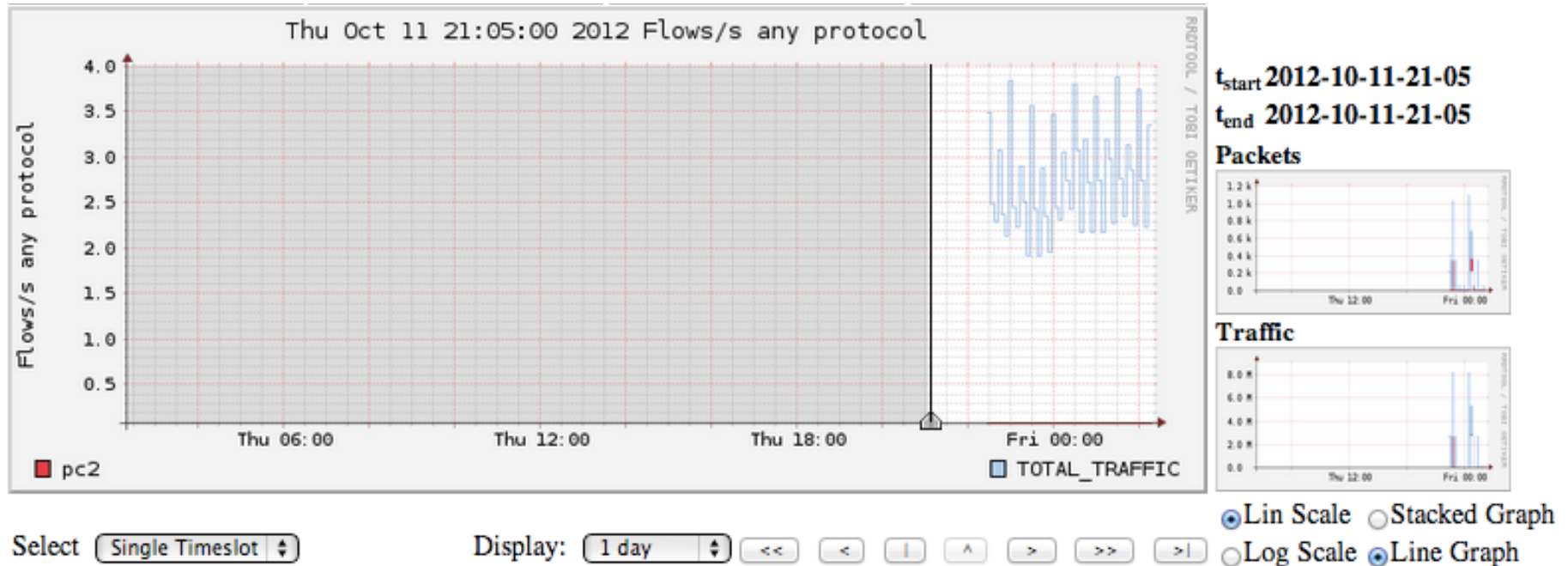
```
$ exit
```

(salir de pcY)

Ver el tráfico

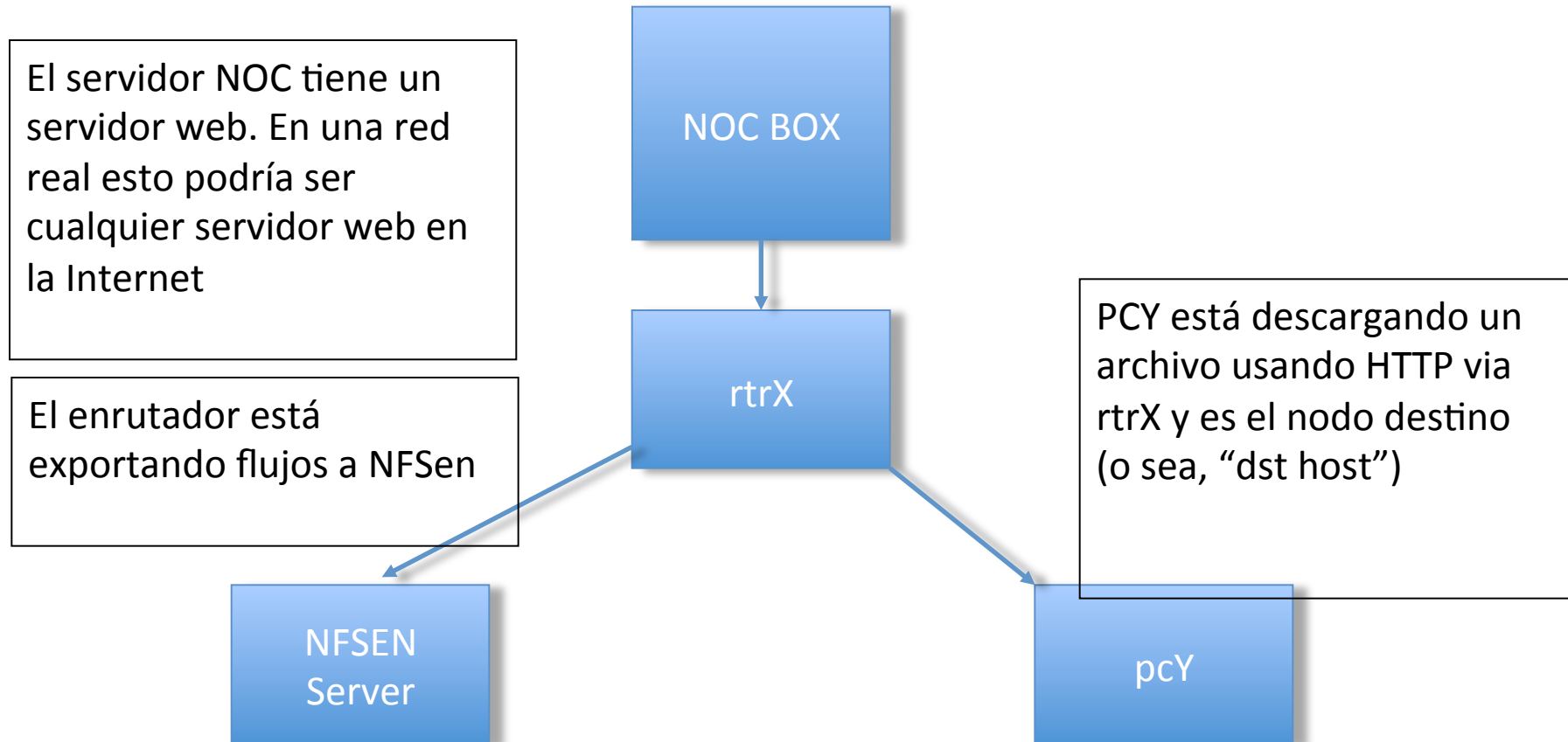
Su gráfico puede tardar hasta 15 minutos para actualizarse.

Vaya a Graphs -> Traffic -> Details y seleccione 'Line Graph' al fondo



Este gráfico muestra el total de tráfico que pasa por rtrX
vs las descargas HTTP de pcY

Un momento! ¿Qué está pasando?



Hemos configurado NFSen para graficar tráfico cuyo puerto fuente es 80 y la IP destino es 10.10.X.Y. Puede hacer algo similar en su red para graficar tráfico desde un servidor web específico con ‘src host a.b.c.d’ por ejemplo usando la IP de Facebook

Ver una descarga FTP desde el NOC

- Siga exactamente los mismos pasos desde la diapositiva 5, pero esta vez, cambie 'HTTP_TRAFFIC' a 'FTP_TRAFFIC'
- El protocolo FTP puede usar puertos al azar, así que puede que no sea el puerto 20. Sí sabemos que será un puerto mayor que 1024, por lo que podemos crear un filtro así:

```
src port > 1024 and dst host 10.10.X.Y
```
- Asegúrese de seleccionar la fuente correcta en "Available Sources"
- Ahora baje el mismo archivo grande desde el NOC usando FTP a pcy.ws.nsrc.org
- ➔ **Instrucciones en la siguiente pantalla**

Descargar datos con FTP a pcY

Ingresa en pcY y use el comando ftp para generar tráfico FTP desde NOC hasta pcY

```
ssh sysadm@pcY.ws.nsrc.org
```

```
$ sudo apt-get install ftp
```

```
$ ftp noc.ws.nsrc.org
```

```
Name (noc.ws.nsrc.org:sysadm): anonymous
```

```
Password: <YourEmailAddress>
```

```
ftp> lcd /tmp
```

```
ftp> get BigFile (tarda mucho tiempo)
```

```
ftp> quit
```

```
$ rm /tmp/BigFile
```

Su gráfico tardará hasta 15 minutos para actualizarse. Vaya a Graphs -> Traffic -> Details y seleccione “Line Graph” al fondo para ver los resultados

Parte 2

Graficar una interfaz específica en el router

- Use el comando `snmpwalk` en su PC para determinar el número de índice de una interfaz que quiera graficar

```
$ snmpwalk -v2c -c NetManage rtrX.ws.nsrc.org ifDescr
```

```
IF-MIB::ifDescr.1 = STRING: FastEthernet0/0  
IF-MIB::ifDescr.2 = STRING: FastEthernet0/1  
IF-MIB::ifDescr.3 = STRING: VoIP-Null0  
IF-MIB::ifDescr.4 = STRING: Null0  
IF-MIB::ifDescr.5 = STRING: Loopback0
```

- Esto significa que a F0/0 se le asignó el número 1. Podemos usar NFSen para graficar el tráfico de esta interfaz en particular
 - Esta interfaz debe tener ‘ip flow egress’ o ingress activado
 - Con ‘snmp ifindex persist’ el índice se mantiene

Agregue la interfaz en NFSen

Profile:	Interface_FastEthernet_0	?
Group:	group1	?
Description:	edit	
Start:	Format: yyyy-mm-dd-HH-MM	?
End:	Format: yyyy-mm-dd-HH-MM	?
Max. Size:	10G	?
Expire:	60 Days	?
Channels:	☐ 1:1 channels from profile live ☒ individual channels	?
Type:	☐ Real Profile ☒ Shadow Profile	?
Cancel Create Profile		

Oprima *Live* y luego *New Profile*

Asigne al perfil un nombre apropiado y agréguelo al mismo grupo que creó anteriormente

Seleccione *individual channels* y *shadow profile* como antes, luego oprima *Create Profile*

Luego, en la ventana siguiente oprima (+) al lado de *Channel List*

Status:	new
Channel List:	+

in_interface_1

Colour: Enter new value #66FF33 or Select a colour from

Sign: + Order: 1

Filter: in if 1

Sources:

Available Sources		Selected Sources
		rtr1 rtr2

<< >>

Cancel Commit Changes

out_interface_1

Colour: Enter new value #FF0000 or Select a colour from

Sign: + Order: 2

Filter: out if 1

Sources:

Available Sources		Selected Sources
		rtr1 rtr2

<< >>

Cancel Commit Changes

Esto significa “grafica todo el tráfico que pasa ENTRANDO por la interfaz 1”. Oprima Add Channel y oprima (+) para agregar un segundo canal

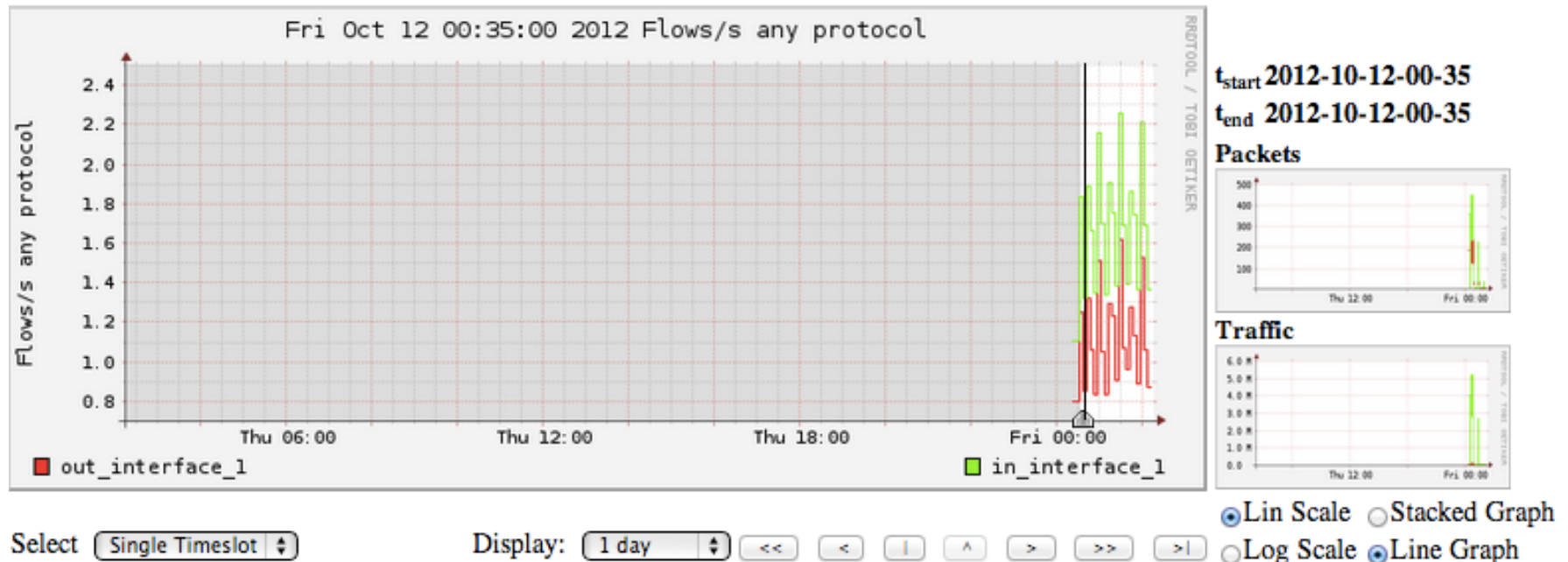
Nota: La interfaz “1” se refiere al número de índice de FastEthernet 0/0 en rtrX

Esto significa “grafica todo el tráfico SALIENDO por la interfaz 1”. Oprima “Add Channel” y luego active el filtro en la pantalla siguiente oprimiendo la marca verde

Dele tiempo para que genere el gráfico. Compare los datos con Cacti

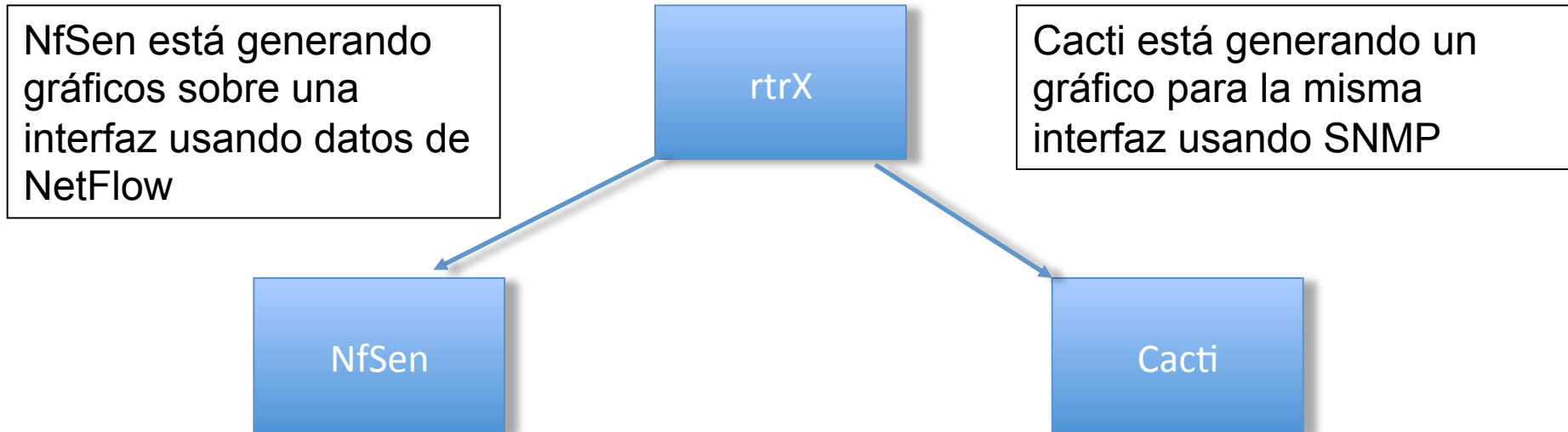
Vea el tráfico

Su gráfico tardará hasta 15 minutos para actualizarse. Vaya a Graphs -> Traffic -> Details y seleccione “Line Graph”.



Este es un gráfico del tráfico total que pasa por el enrutador rtrX, interfaz FastEthernet0/0

Un momento! ¿Qué está pasando?

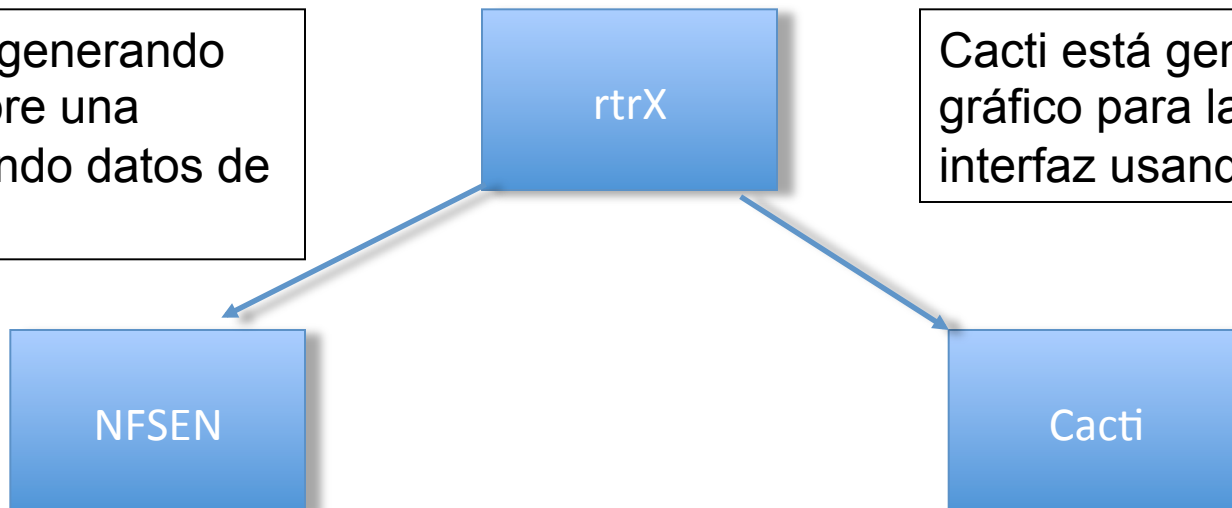


Con NfSen puede extraer información más detallada, tal como cuáles direcciones IP están comunicando, cuáles son los puertos más utilizados según número de octetos, cuáles son los números de sistemas autónomos que son origen o destino del tráfico y mucho más

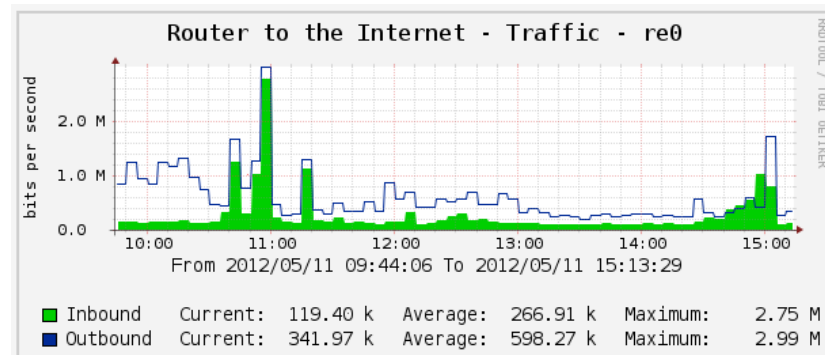
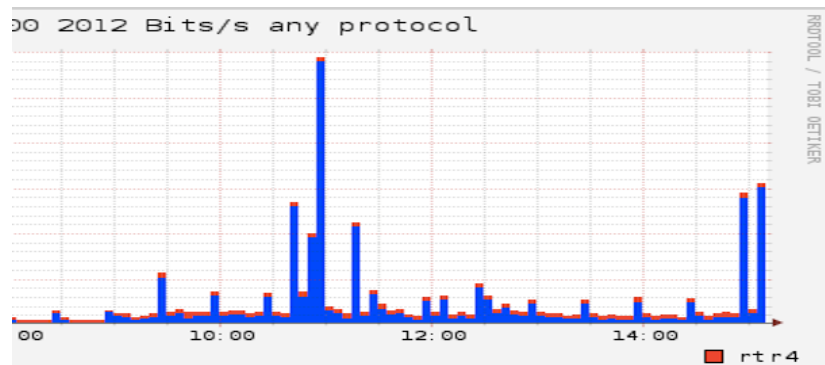
Un momento! ¿Qué está pasando?

NfSen está generando gráficos sobre una interfaz usando datos de NetFlow

Cacti está generando un gráfico para la misma interfaz usando SNMP

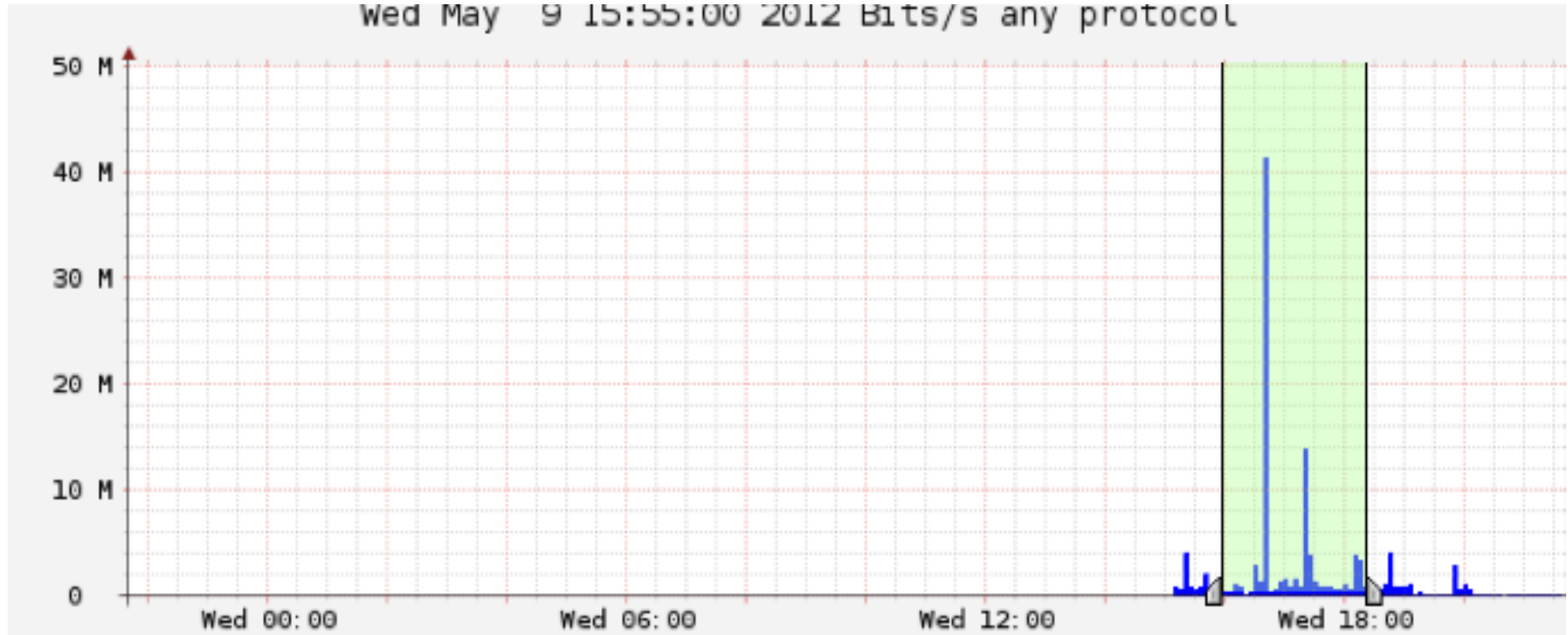


Si está midiendo la misma interfaz con Cacti y NfSen, debería obtener datos similares al copiar los bits/s



Parte 3

Procesamiento de NetFlow extendido



Vaya a Profile, seleccione el grupo que haya creado y luego seleccione "HTTP_TRAFFIC". Luego vaya a la pestaña "Details" y seleccione "Time Window" en lugar de "Time Slot" debajo del gráfico. Elija una parte del gráfico con actividad, como se muestra arriba

Options:

☐ List Flows ☒ Stat TopN

Top:

Stat: order by

Aggregate

☐ bi-directional

☒ proto

☒ srcPort

☒ dstPort

Limit: ☐

Output: ☐ / IPv6 long

Seleccione las opciones como se indica. Esto significa: *selecciona los 10 flujos mayor cantidad de bytes, ordenados de mayor a menor, y muestra los puertos e IPs de origen y destino*. Luego oprima process. Analice el resultado, que será algo parecido como se muestra abajo

aggregated flows 53/123

Top 10 flows ordered by bytes:

Date flow start	Duration	Proto	Src IP Addr	Src Pt	Dst IP Addr	Dst Pt	Packets	Bytes	bps	Bpp	Flows
2012-05-09 16:31:43.481	664.018	TCP	10.10.0.60	53731	10.10.0.250	22	1.0 M	1.5 G	18.1 M	1482	1
2012-05-09 17:10:21.896	722.117	TCP	10.10.0.254	42499	10.10.8.29	22	310886	466.2 M	5.2 M	1499	47
2012-05-09 16:22:44.095	4108.913	TCP	208.117.226.27	80	10.10.0.77	49757	69250	103.7 M	201865	1497	2
2012-05-09 18:13:16.475	45.837	TCP	10.10.0.60	54946	10.10.0.250	22	66924	99.5 M	17.4 M	1487	1
2012-05-09 18:18:45.625	30.212	TCP	10.10.0.250	16647	10.10.0.60	51007	66230	99.2 M	20.2 M	1480	1

Netflow Processing

Source:

pc2ftp
FTP_TRAFFIC
pc2
TOTAL_TRAFFIC

All Sources

Filter:

src port > 1024 and dst host 10.10.1.2

and <none>

Options:

☐ List Flows ☒ Stat TopN

Top: 10

Stat: Flow Records order by bytes

☒ bi-directional

☐ proto

☐ srcPort srcIP

☐ dstPort dstIP

☐ Packets > 0 -

Output: auto / IPv6 long

Clear Form

process

Pruebe lo mismo con la opción bidireccional. Qué observa? Pruebe jugando con las diferentes opciones. También puede agregar los mismos filtros en la ventana de filtros, al lado de Options

Pruebe los siguientes filtros:

src host 10.10.X.Y – flujos de este nodo

src port 22 – flujos donde el puerto origen es 22

src port 22 or src port 80 – flujos donde el puerto origen es 22 ó 80

src port 80 and in if 1 – puerto fuente 80 entrando por interfaz 1

dst net 10.10.0.0/16 – flujos con destino a la red dada

src port > 5000 – flujos cuyo puerto origen está por encima de 5000

Se pueden usar muchos más filtros

- Tráfico del sistema autónomo de Google (AS 15169)
 - `src as 15169`
- Puede hacer lo mismo con cualquier otro AS, pero su enrutador tiene que tener una tabla de rutas BGP y configurado con 'ip flow-export version 9 origin-as'
- Así se pueden generar gráficas para cada una de ellas usando Stadisticas como en el ejercicio anterior
- Más filtros aquí: <http://nfsen.sourceforge.net/#mozTocId652064>

Adicional/Opcional

Monitorizar un nodo en
específico

Profile:	Troublesome_User	?
Group:	New group ... Hosts	?
Description:	edit	
Start:	Format: yyyy-mm-dd-HH-MM	?
End:	Format: yyyy-mm-dd-HH-MM	?
Max. Size:	0	?
Expire:	Never	?
Channels:	☐ 1:1 channels from profile live ☒ individual channels	?
Type:	☐ Real Profile ☒ Shadow Profile	?
Cancel Create Profile		

- En el menú “Profile” de NfSen seleccione “New Profile...”
- Rellene y oprima “Create Profile”
- Verá el mensaje “new profile created”
- Luego oprima el (+) abajo para empezar a agregar canales

Monitorizar una IP en específico

The image shows a configuration window for monitoring a specific IP. It contains several sections: 'Channel name' with a text field 'User1'; 'Colour' with a button 'Enter new value', a color code '#abcdef', and a dropdown 'Select a colour from'; 'Sign' with a '+' button and 'Order' with a '1' button; 'Filter' with a text area containing 'host 10.10.1.2' and an 'edit' button; and 'Sources' with two lists: 'Available Sources' (empty) and 'Selected Sources' (containing 'rtr1' and 'rtr2'), with '<<' and '>>' buttons between them. At the bottom are 'Cancel' and 'Add Channel' buttons.

Channel name	User1			
Colour:	Enter new value	#abcdef	or	Select a colour from
Sign:	+	Order:	1	
Filter:	host 10.10.1.2 edit			
Sources:	Available Sources		Selected Sources	
			rtr1 rtr2	
Cancel Add Channel				

Sustituya
10.10.1.2 con
la IP de su
máquina
virtual.

Agregue un segundo canal

Profile: Troublesome_User	
Group:	Hosts
Description:	
Type:	Continuous / shadow
Start:	2012-10-12-01-4
End:	2012-10-12-01-4
Last Update:	2012-10-12-01-4
Size:	0 B
Max. Size:	unlimited
Expire:	never
Status:	new
Channel List:	
User1	
Colour:	#abcdef
Sign:	+
Order:	1
Filter:	host 10.10.1.2
Sources:	rtr1 rtr2

Channel name	User2							
Colour:	Enter new value	#FF0000 or Select a colour from						
Sign:	+	Order: 2						
Filter:	dst host 10.10.1.1							
Sources:	<table><thead><tr><th>Available Sources</th><th></th><th>Selected Sources</th></tr></thead><tbody><tr><td></td><td></td><td>rtr1 rtr2</td></tr></tbody></table>		Available Sources		Selected Sources			rtr1 rtr2
Available Sources		Selected Sources						
		rtr1 rtr2						
Cancel Add Channel								

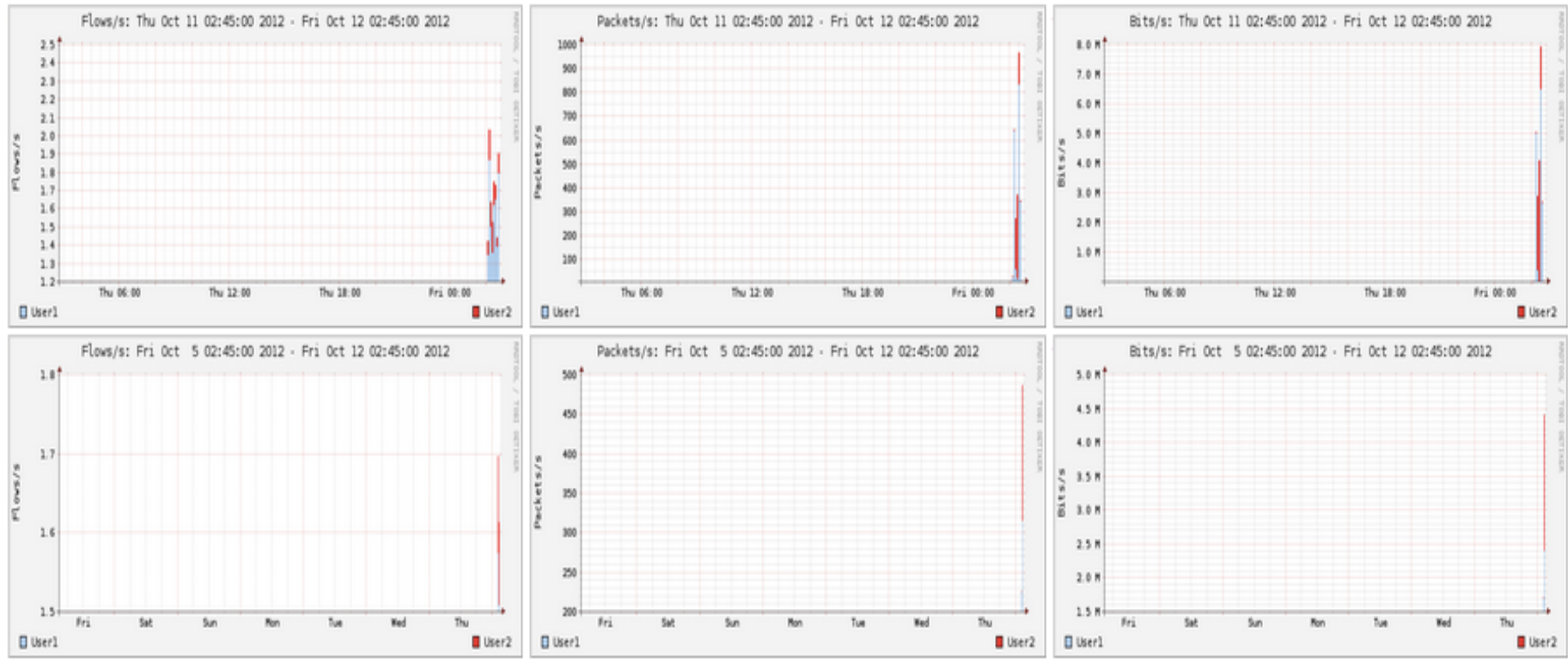
Oprima “Add Channel” y luego oprima la marca verde para activarlo. Llámelo “Usuario molesto”

Filtros

- Seleccione un color diferente para el segundo canal de manera que los gráficos puedan distinguirse
- Fíjese que los dos filtros son diferentes
 - El primer filtro capturará cualquier flujo relacionado con el primer PC
 - El segundo filtro sólo capturará flujos donde el segundo PC es el destino
 - Para ver un gráfico de este perfil, genera tráfico transfiriendo archivos desde el primer nodo hacia el segundo nodo
- Se pueden agregar más atributos como AS origen, AS destino, puertos origen, etc. utilizando la sintaxis de filtros de NfSen

Ver las tendencias

Overview Profile: Troublesome_User, Group Hosts



SIGA CON EJERCICIO 5

PortTracker Plugin