4.14.5. GENERACION DE ESTADISTICAS SOBRE NAVEGACION EN INTERNET

Para tener un visión de lo que los usuarios hacen en internet, a través del proxy, se puede configurar el sarg, para que nos presente de forma gráfica los LOGs de acceso a internet.

Se instalara una nueva versión, para fedora core 6, ubicada en /opt/instaladores:

```
[root@proxyudi squid]# cd /opt/instaladores/
[root@proxyudi instaladores]# ls -l sar*
-rw-r--r-- 1 root root 316208 may  9 21:09 sarg-2.2.1-1.fc6.rf.i386.rpm
[root@proxyudi instaladores]#
[root@proxyudi instaladores]# rpm -ivh sarg-2.2.1-1.fc6.rf.i386.rpm
warning: sarg-2.2.1-1.fc6.rf.i386.rpm: Header V3 DSA signature: NOKEY, key ID
1aa78495
Preparing...                ########################################### [100%]
   1:sarg                   ########################################### [100%]
[root@proxyudi instaladores]#
```

Se edita el archivo de configuracion (/etc/sarg/sarg.conf):

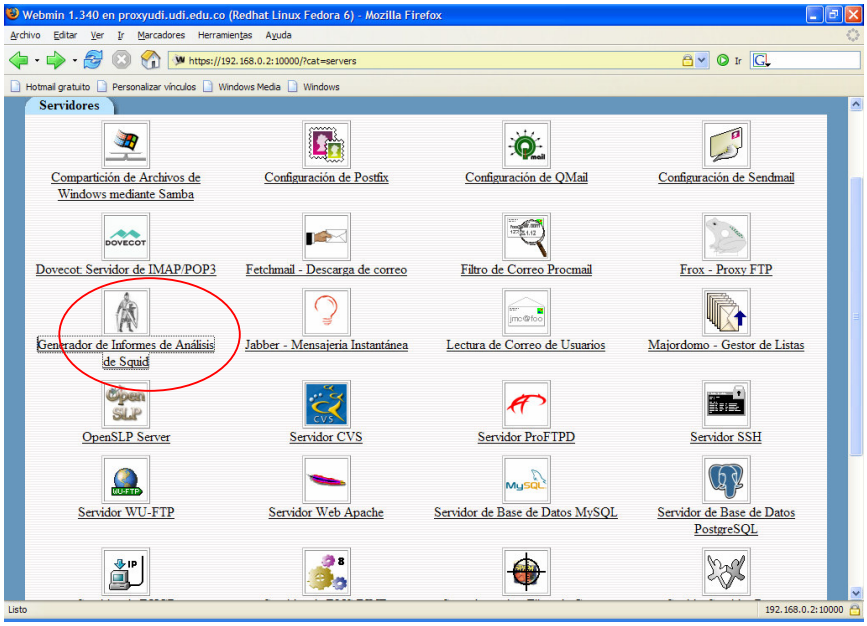
Descomentamos y se arreglan las siguientes lineas :

```
access_log /var/log/squid/access.log
output_dir /home/paginas/reportes
```

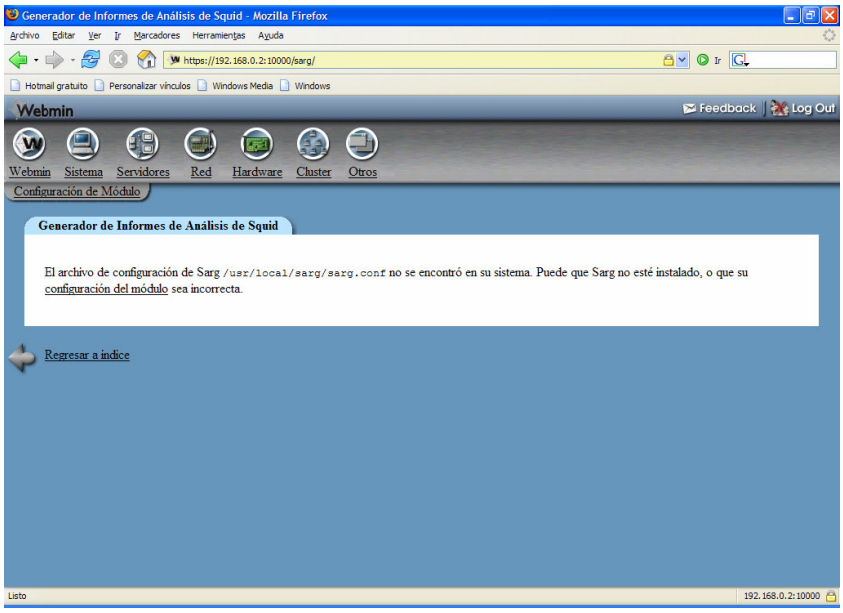
Se crea la carpeta donde residirán los reportes y se dan permisos:

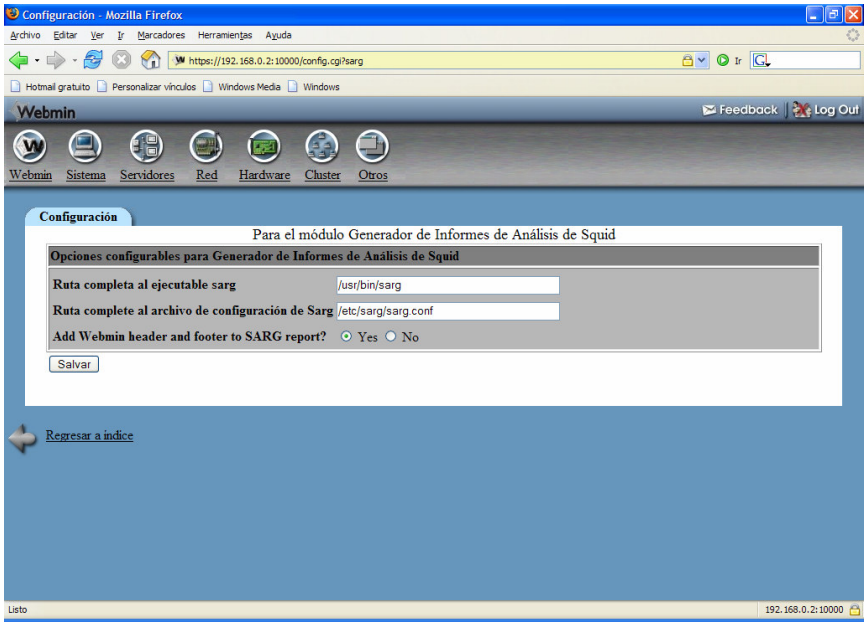
```
[root@www sarg]# mkdir /home/web/reportes
[root@www sarg]# chown apache:apache /home/web/reportes
```

En el webmin, por servidores, hay un icono para configuración del sarg:

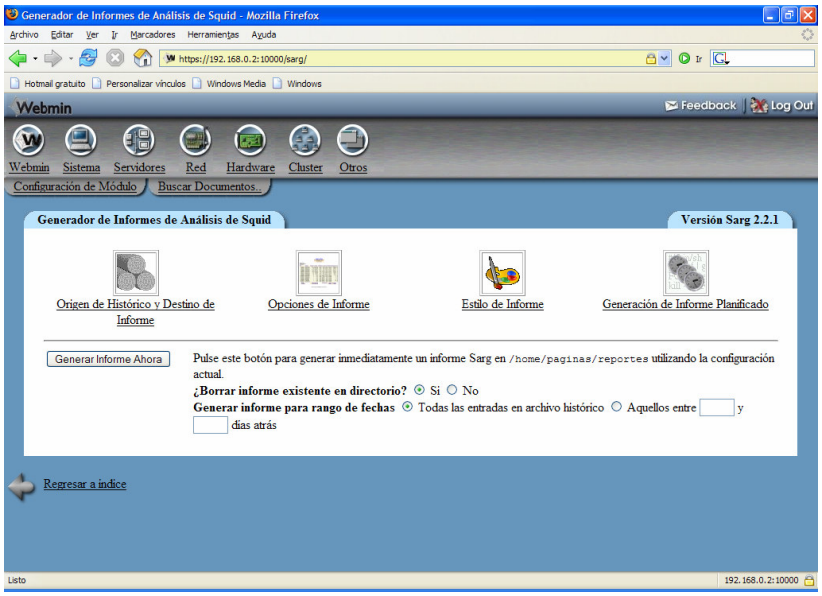


Se escoge, para configurarlo, pues el usa otro archivo de configuración:





Al salvar muestra:

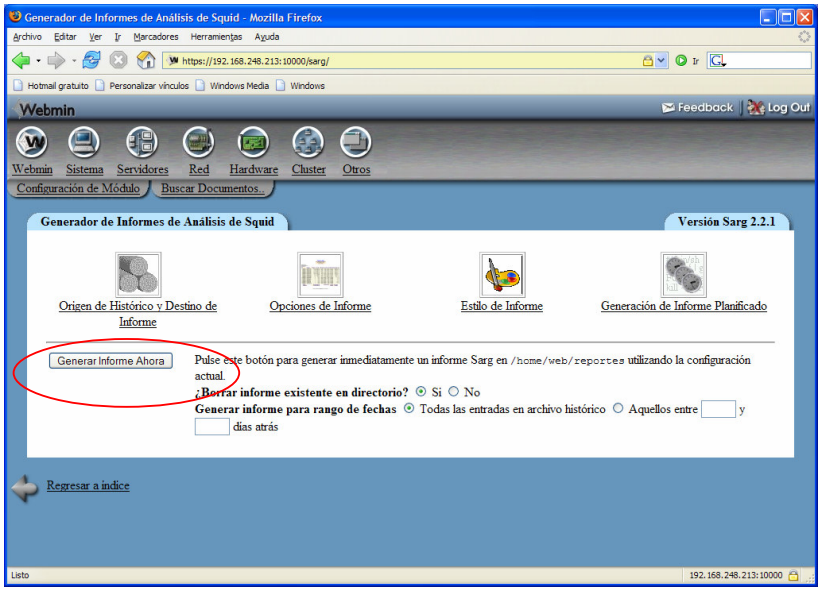


Se crea la carpeta de los reportes, debajo del directorio web:

Reiniciamos el servicio de apache:

```
[root@www reportes]# service httpd restart
Parando httpd:                                [  OK  ]
Iniciando httpd:                              [  OK  ]
```

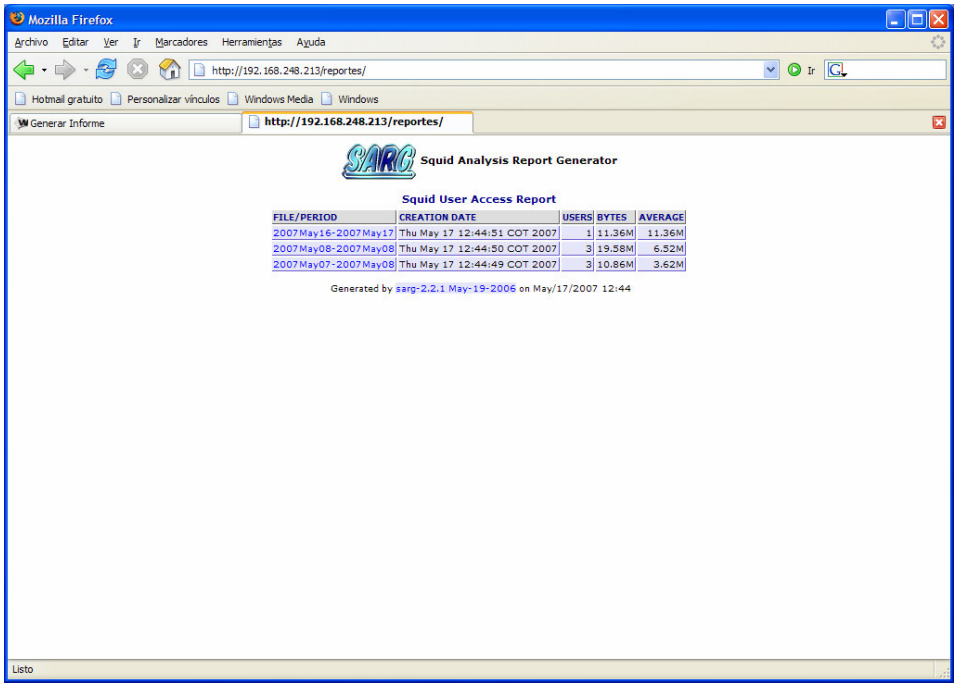
En la opción del webmin, dentro del sarg, se escoge generar informe:



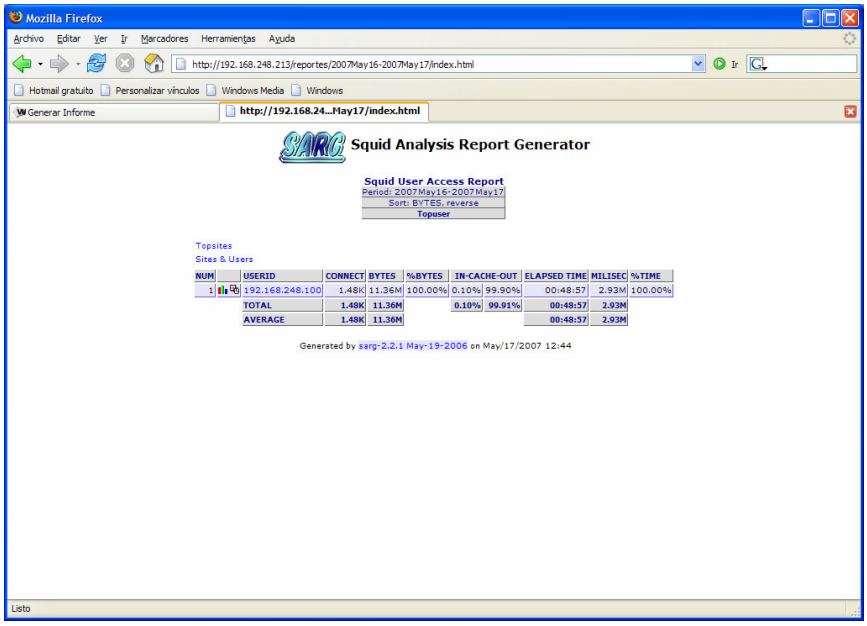
Ese informe debe ser ubicado en /home/web/reportes.

```
[root@www conf.d]# cd /home/web
[root@www web]# ls
exten.html  index.html  prohibit.html  reportes  urls.html
[root@www web]# cd reportes/
[root@www reportes]# pwd
/home/web/reportes
[root@www reportes]# ls
2007May07-2007May08  2007May08-2007May08  2007May16-2007May17  images
index.html
```

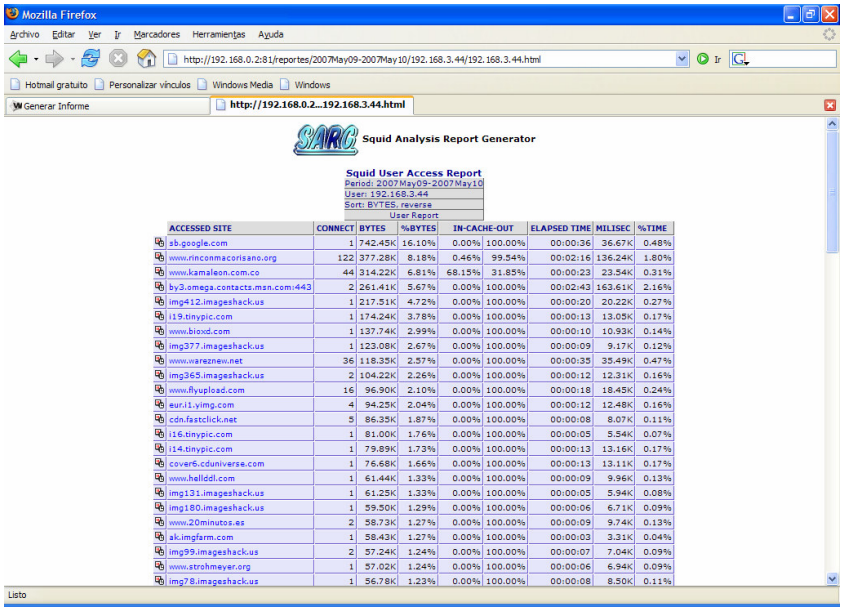
Vamos al navegador y verificamos si podemos ingresar a ver los reportes del sarg



Se escoge la fecha del informe:

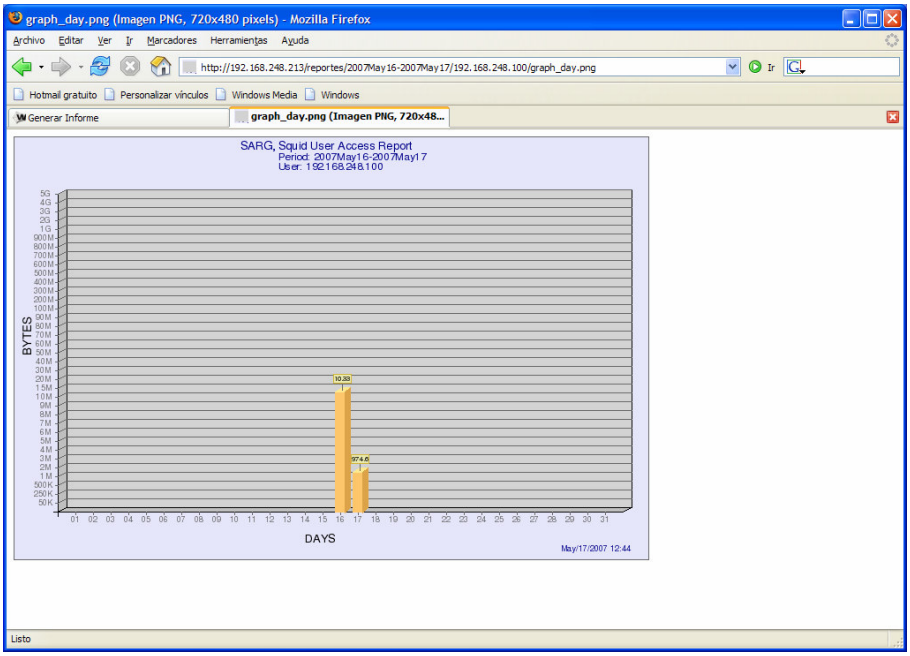


Se puede empezar a ver el detalle por usuario:



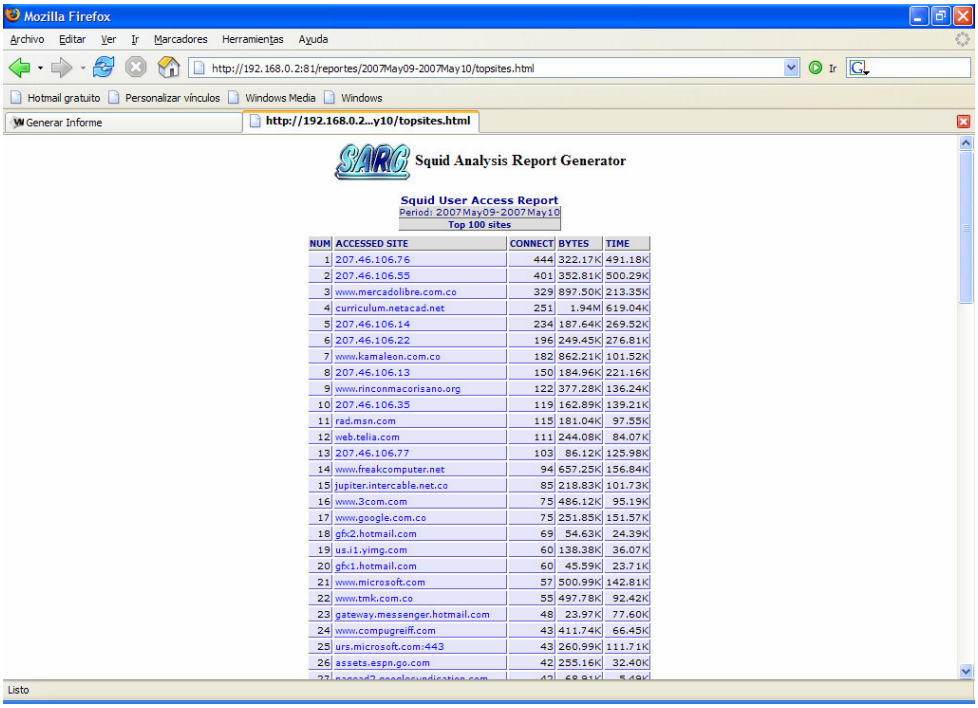
ACCESSED SITE	CONNECT	BYTES	%BYTES	IN-CACHE-OUT		ELAPSED TIME	MILISEC	%TIME
sb.google.com	1	742.45K	16.10%	0.00%	100.00%	00:00:36	36.67K	0.48%
www.rinconmacorisano.org	122	377.28K	8.18%	0.46%	99.54%	00:02:16	136.24K	1.80%
www.kamaleon.com.co	44	314.22K	6.81%	68.15%	31.85%	00:00:23	23.54K	0.31%
by3.omega.contacts.msn.com:443	2	261.41K	5.67%	0.00%	100.00%	00:02:43	163.61K	2.16%
img412.imageshack.us	1	217.51K	4.72%	0.00%	100.00%	00:00:20	20.22K	0.27%
i19.tinypic.com	1	174.24K	3.78%	0.00%	100.00%	00:00:13	13.05K	0.17%
www.bioxd.com	1	137.74K	2.99%	0.00%	100.00%	00:00:10	10.93K	0.14%
img377.imageshack.us	1	123.08K	2.67%	0.00%	100.00%	00:00:09	9.17K	0.12%
www.wareznew.net	36	118.35K	2.57%	0.00%	100.00%	00:00:35	35.49K	0.47%
img365.imageshack.us	2	104.22K	2.26%	0.00%	100.00%	00:00:12	12.31K	0.16%
www.flyupload.com	16	96.90K	2.10%	0.00%	100.00%	00:00:18	18.45K	0.24%
eur.i1.yimg.com	4	94.25K	2.04%	0.00%	100.00%	00:00:12	12.48K	0.16%
cdn.fastclick.net	5	86.35K	1.87%	0.00%	100.00%	00:00:08	8.07K	0.11%
i16.tinypic.com	1	81.00K	1.76%	0.00%	100.00%	00:00:05	5.54K	0.07%
i14.tinypic.com	1	79.89K	1.73%	0.00%	100.00%	00:00:13	13.16K	0.17%
cover6.cduniverse.com	1	76.68K	1.66%	0.00%	100.00%	00:00:13	13.11K	0.17%
www.helldl.com	1	61.44K	1.33%	0.00%	100.00%	00:00:09	9.96K	0.13%
img131.imageshack.us	1	61.25K	1.33%	0.00%	100.00%	00:00:05	5.94K	0.08%
img180.imageshack.us	1	59.50K	1.29%	0.00%	100.00%	00:00:06	6.71K	0.09%
www.20minutos.es	2	58.73K	1.27%	0.00%	100.00%	00:00:09	9.74K	0.13%
ak.imgfarm.com	1	58.43K	1.27%	0.00%	100.00%	00:00:03	3.31K	0.04%
img99.imageshack.us	2	57.24K	1.24%	0.00%	100.00%	00:00:07	7.04K	0.09%
www.strohmeyer.org	1	57.02K	1.24%	0.00%	100.00%	00:00:06	6.94K	0.09%
img78.imageshack.us	1	56.78K	1.23%	0.00%	100.00%	00:00:08	8.50K	0.11%

Se puede pedir graficar el consumo de un usuario, por ejemplo del equipo: 192.168.248.100:



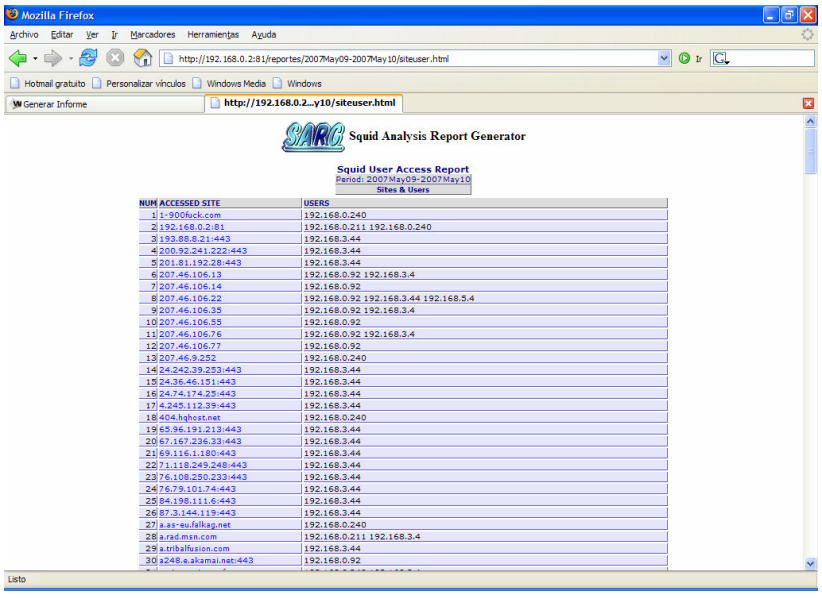
A continuación, veremos un breve vistazo al funcionamiento del sarg y los reportes que genera.

Top sities: en este caso por defecto muestra 100 sitios mas visitados



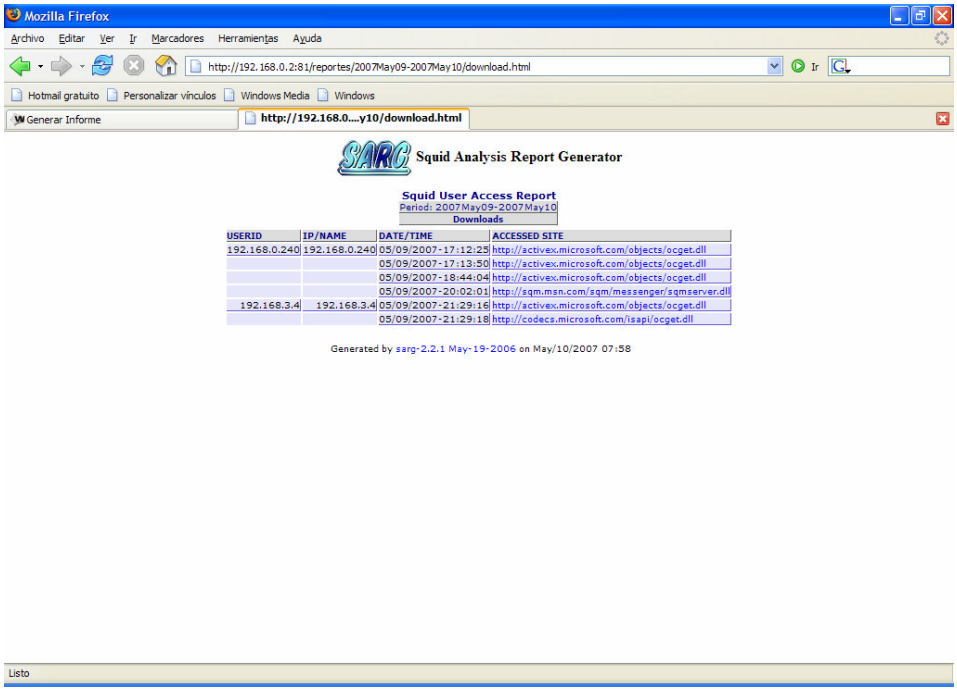
NUM	ACCESSED SITE	CONNECT	BYTES	TIME
1	207.46.106.76	444	322.17K	491.18K
2	207.46.106.55	401	352.81K	500.29K
3	www.mercadolibre.com.co	329	897.50K	213.35K
4	curriculum.netacad.net	251	1.94M	619.04K
5	207.46.106.14	234	187.64K	269.52K
6	207.46.106.22	196	249.45K	276.81K
7	www.kamaleon.com.co	182	862.21K	101.52K
8	207.46.106.13	150	184.96K	221.16K
9	www.rinconmacorisano.org	122	377.28K	136.24K
10	207.46.106.35	119	162.89K	139.21K
11	rad.msn.com	115	181.04K	97.55K
12	web.telia.com	111	244.08K	84.07K
13	207.46.106.77	103	86.12K	125.98K
14	www.freakcomputer.net	94	657.25K	156.84K
15	jupiter.intercable.net.co	85	218.83K	101.73K
16	www.3com.com	75	486.12K	95.19K
17	www.google.com.co	75	251.85K	151.57K
18	gfx2.hotmail.com	69	54.63K	24.39K
19	us.i1.yimg.com	60	138.38K	36.07K
20	gfx1.hotmail.com	60	45.59K	23.71K
21	www.microsoft.com	57	500.99K	142.81K
22	www.tmk.com.co	55	497.78K	92.42K
23	gateway.messenger.hotmail.com	48	23.97K	77.60K
24	www.compugreiff.com	43	411.74K	66.45K
25	urs.microsoft.com:443	43	260.99K	111.71K
26	assets.espn.go.com	42	255.16K	32.40K

Sitios y usuarios:

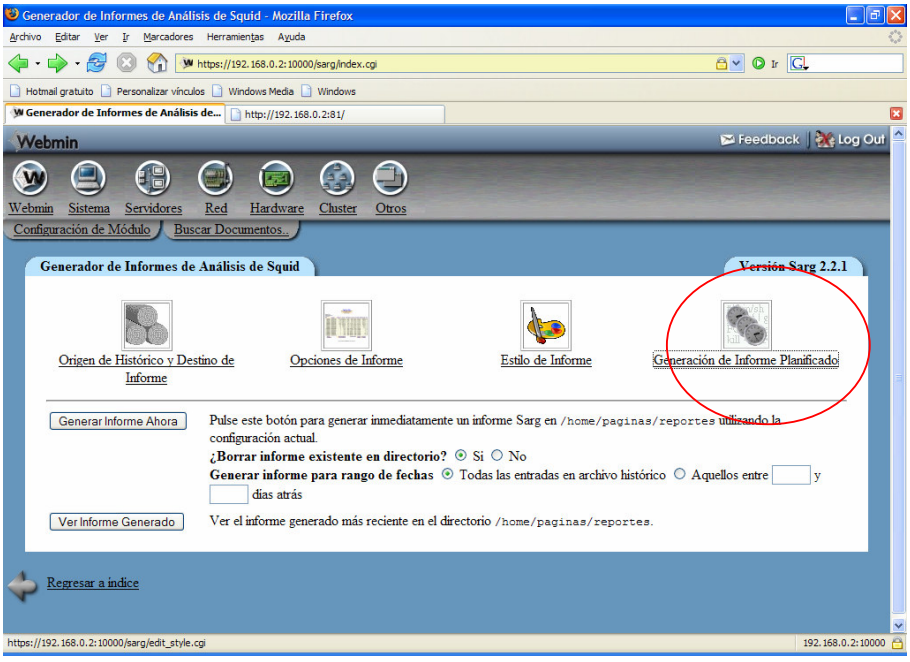


NUM	ACCESSED SITE	USERS
1	1-900fuck.com	192.168.0.240
2	192.168.0.2:81	192.168.0.211 192.168.0.240
3	193.88.8.21:443	192.168.3.44
4	200.92.241.222:443	192.168.3.44
5	201.81.192.28:443	192.168.3.44
6	207.46.106.13	192.168.0.92 192.168.3.4
7	207.46.106.14	192.168.0.92
8	207.46.106.22	192.168.0.92 192.168.3.44 192.168.5.4
9	207.46.106.35	192.168.0.92 192.168.3.4
10	207.46.106.55	192.168.0.92
11	207.46.106.76	192.168.0.92 192.168.3.4
12	207.46.106.77	192.168.0.92
13	207.46.9.252	192.168.0.240
14	24.242.39.253:443	192.168.3.44
15	24.36.46.151:443	192.168.3.44
16	24.74.174.25:443	192.168.3.44
17	4.245.112.39:443	192.168.3.44
18	404.hqhost.net	192.168.0.240
19	65.96.191.213:443	192.168.3.44
20	67.167.236.33:443	192.168.3.44
21	69.116.1.180:443	192.168.3.44
22	71.118.249.248:443	192.168.3.44
23	76.108.250.233:443	192.168.3.44
24	76.79.101.74:443	192.168.3.44
25	84.198.111.6:443	192.168.3.44
26	87.3.144.119:443	192.168.3.44
27	a.as-eu.falkag.net	192.168.0.240
28	a.rad.msn.com	192.168.0.211 192.168.3.4
29	a.tribalfusion.com	192.168.3.44
30	a248.e.akamai.net:443	192.168.0.92

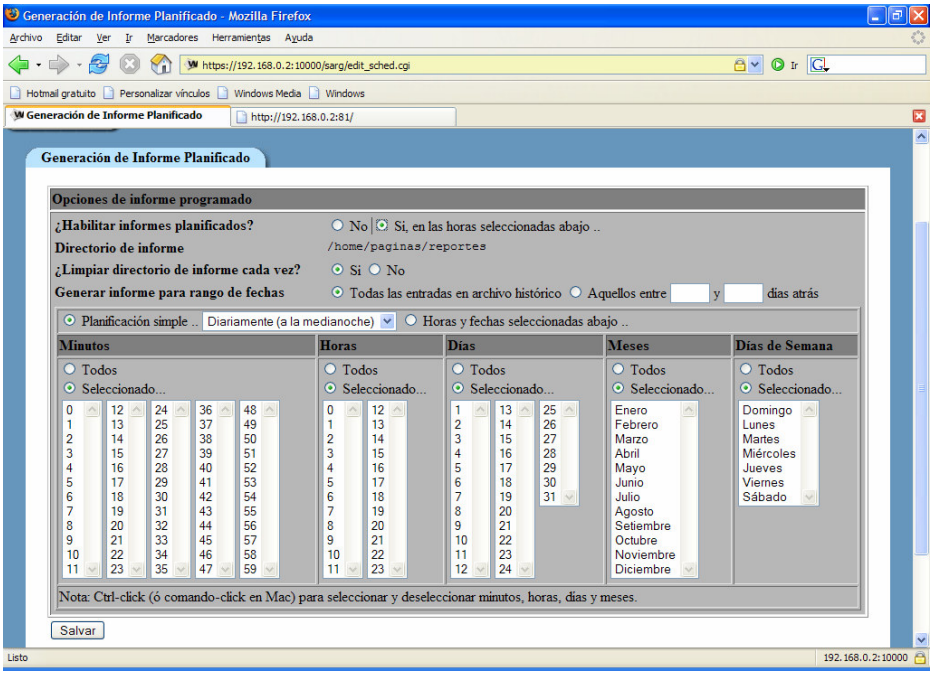
Bajados:



Por la opción del webmin de planificar reportes se puede pedir la generación de estos a determinadas horas y de los dias escogidos:



Por defecto se activo para que genere diario a la medianoche.



4.15. CONFIGURACION DE MRTG

MRTG usa SNMP (Simple Networque Management Protocol) para recolectar los datos de tráfico de un determinado dispositivo (routers o servidores).

Software requerido para el funcionamiento de MRTG:

- net-snmp-5.1 o superior
- net-snmp-utils-5.1 o superior
- mrtg-2.14.5-2

Verificamos que el snmp este instalado y revisamos su versión:

Se verifica que el snmp esta instalado y activo:

```
[root@www mrtg]# rpm -a -q | grep snmp
net-snmp-libs-5.3.1-11.fc6
```

Faltan algunos módulos que se descargan de internet y se ubican en instaladores:

```
[root@www instaladores]# ls *snmp*
net-snmp-5.3.1-11.fc6.i386.rpm       net-snmp-perl-5.3.1-11.fc6.i386.rpm
net-snmp-devel-5.3.1-11.fc6.i386.rpm  net-snmp-utils-5.3.1-11.fc6.i386.rpm
[root@www instaladores]#
[root@www instaladores]# rpm -ivh net-snmp-5.3.1-11.fc6.i386.rpm
Preparing...                ########################################### [100%]
   1:net-snmp               ########################################### [100%]
```

```
[root@www instaladores]# rpm -ivh net-snmp-devel-5.3.1-11.fc6.i386.rpm
error: Failed dependencies:
        beecrypt-devel is needed by net-snmp-devel-5.3.1-11.fc6.i386
        elfutils-devel is needed by net-snmp-devel-5.3.1-11.fc6.i386
[root@www instaladores]# rpm -ivh net-snmp-utils-5.3.1-11.fc6.i386.rpm
Preparing...                ########################################### [100%]
   1:net-snmp-utils         ########################################### [100%]
[root@www instaladores]# rpm -ivh net-snmp-perl-5.3.1-11.fc6.i386.rpm
Preparing...                ########################################### [100%]
   1:net-snmp-perl          ########################################### [100%]
```

```
[root@www /]# rpm -aq | grep snmp
net-snmp-libs-5.3.1-11.fc6
net-snmp-utils-5.3.1-11.fc6
net-snmp-5.3.1-11.fc6
net-snmp-perl-5.3.1-11.fc6
[root@www /]#
```

Se deben crear las entradas correspondientes en el fichero **/etc/snmp/snmpd.conf** que servirán para definir quien tendrá acceso hacia el servicio *snmpd*. Sin embargo no olvidar hacer una copia del archivo de configuración del snmpd.conf:

```
[root@www instaladores]# cd /etc/snmp
[root@www snmp]#cp snmpd.conf snmpd.conf.ori
[root@www snmp]#ls
snmpd.conf  snmpd.conf.ori
```

```
[root@www snmp]# cat snmpd.conf

# Listas de control de acceso (ACL)
## sec.name source community (alias clave de acceso)
com2sec  local   192.168.1.1      public

#Se asigna ACL al grupo de lectura escritura, en este caso no lo asignamos a ningun
grupo.
group   notConfigGroup v1          local
group   notConfigGroup v2c         local

# Ramas MIB que se permiten ver
## name   incl/excl subtree   mask(optional)
 view     all          included         .1               80

# Establece permisos de lectura y escritura en este caso solo de lectura.
## group        context        sec.model     sec.level prefix  read   write   notif
access      notConfigGroup ""      any       noauth    exact    all     none   none
```

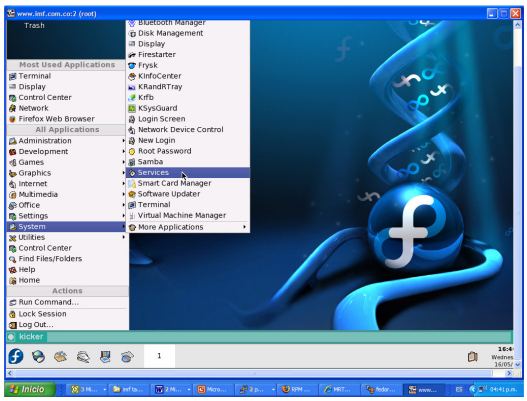
```
# Información de Contacto del Sistema
syslocation Servidor Linux en imf.com.co
syscontact Administrador
```

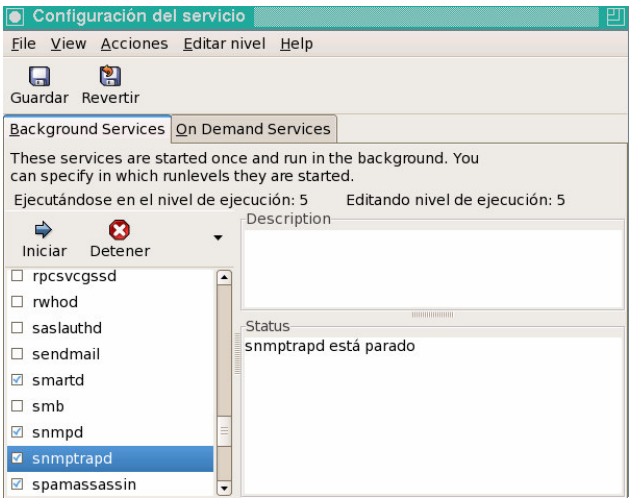
Iniciar el servicio y añadirlo a los servicios de arranque del sistema:

Inicie el servicio de SNMP y añada éste al resto de los servicios que arrancan junto con el sistema:

```
[root@www snmp]# service snmpd restart
Parando snmpd:                                [  OK  ]
Iniciando snmpd:                              [  OK  ]
[root@www ~]# chkconfig snmpd on
```

Se configura para que el servicio siempre inicie con la máquina:





Comprobamos el correcto funcionamiento del snmp: Como se asigno clave de acceso public en el sistema con dirección IP es **192.168.1.1**, para probar si la configuración funciona, solo hay que ejecutar los dos siguiente mandatos a fin verificar que devuelvan información acerca del sistema consultado.

```
[root@www ~]# snmpwalk -v 1 -c public 192.168.1.1 system
SNMPv2-MIB::sysDescr.0 = STRING: Linux www.imf.com.co 2.6.18-1.2798.fc6 #1
SMP Mon Oct 16 14:37:32 EDT 2006 i686
SNMPv2-MIB::sysObjectID.0 = OID: NET-SNMP-MIB::netSnmpAgentOIDs.10
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (4361) 0:00:43.61
SNMPv2-MIB::sysContact.0 = STRING: Root <root@localhost> (configure
/etc/snmp/snmp.local.conf)
SNMPv2-MIB::sysName.0 = STRING: www.imf.com.co
SNMPv2-MIB::sysLocation.0 = STRING: Unknown (edit /etc/snmp/snmpd.conf)
SNMPv2-MIB::sysORLastChange.0 = Timeticks: (1) 0:00:00.01
SNMPv2-MIB::sysORID.1 = OID: SNMPv2-MIB::snmpMIB
SNMPv2-MIB::sysORID.2 = OID: TCP-MIB::tcpMIB
SNMPv2-MIB::sysORID.3 = OID: IP-MIB::ip
SNMPv2-MIB::sysORID.4 = OID: UDP-MIB::udpMIB
SNMPv2-MIB::sysORID.5 = OID: SNMP-VIEW-BASED-ACM-MIB::vacmBasicGroup
SNMPv2-MIB::sysORID.6 = OID: SNMP-FRAMEWORK-
MIB::snmpFrameworkMIBCompliance
SNMPv2-MIB::sysORID.7 = OID: SNMP-MPD-MIB::snmpMPDCompliance
SNMPv2-MIB::sysORID.8 = OID: SNMP-USER-BASED-SM-MIB::usmMIBCompliance
SNMPv2-MIB::sysORDescr.1 = STRING: The MIB module for SNMPv2 entities
SNMPv2-MIB::sysORDescr.2 = STRING: The MIB module for managing TCP
implementations
SNMPv2-MIB::sysORDescr.3 = STRING: The MIB module for managing IP and ICMP
implementations
SNMPv2-MIB::sysORDescr.4 = STRING: The MIB module for managing UDP
implementations
SNMPv2-MIB::sysORDescr.5 = STRING: View-based Access Control Model for SNMP.
SNMPv2-MIB::sysORDescr.6 = STRING: The SNMP Management Architecture MIB.
SNMPv2-MIB::sysORDescr.7 = STRING: The MIB for Message Processing and
Dispatching.
SNMPv2-MIB::sysORDescr.8 = STRING: The management information definitions for
the SNMP User-based Security Model.
SNMPv2-MIB::sysORUpTime.1 = Timeticks: (1) 0:00:00.01
SNMPv2-MIB::sysORUpTime.2 = Timeticks: (1) 0:00:00.01
SNMPv2-MIB::sysORUpTime.3 = Timeticks: (1) 0:00:00.01
SNMPv2-MIB::sysORUpTime.4 = Timeticks: (1) 0:00:00.01
SNMPv2-MIB::sysORUpTime.5 = Timeticks: (1) 0:00:00.01
SNMPv2-MIB::sysORUpTime.6 = Timeticks: (1) 0:00:00.01
SNMPv2-MIB::sysORUpTime.7 = Timeticks: (1) 0:00:00.01
SNMPv2-MIB::sysORUpTime.8 = Timeticks: (1) 0:00:00.01
[root@www ~]#
```

```
[root@www ~]# snmpwalk -v 1 -c public 192.168.1.1 interface
IF-MIB::ifNumber.0 = INTEGER: 4
IF-MIB::ifIndex.1 = INTEGER: 1
```

```
IF-MIB::ifIndex.2 = INTEGER: 2
IF-MIB::ifIndex.3 = INTEGER: 3
IF-MIB::ifIndex.4 = INTEGER: 4
IF-MIB::ifDescr.1 = STRING: lo
IF-MIB::ifDescr.2 = STRING: eth1
IF-MIB::ifDescr.3 = STRING: eth0
IF-MIB::ifDescr.4 = STRING: sit0
IF-MIB::ifType.1 = INTEGER: softwareLoopback(24)
IF-MIB::ifType.2 = INTEGER: ethernetCsmacd(6)
IF-MIB::ifType.3 = INTEGER: ethernetCsmacd(6)
IF-MIB::ifType.4 = INTEGER: tunnel(131)
IF-MIB::ifMtu.1 = INTEGER: 16436
IF-MIB::ifMtu.2 = INTEGER: 1500
IF-MIB::ifMtu.3 = INTEGER: 1500
IF-MIB::ifMtu.4 = INTEGER: 1480
IF-MIB::ifSpeed.1 = Gauge32: 10000000
IF-MIB::ifSpeed.2 = Gauge32: 0
IF-MIB::ifSpeed.3 = Gauge32: 100000000
IF-MIB::ifSpeed.4 = Gauge32: 0
IF-MIB::ifPhysAddress.1 = STRING:
IF-MIB::ifPhysAddress.2 = STRING: 0:18:fe:77:42:f9
IF-MIB::ifPhysAddress.3 = STRING: 0:c:46:cd:e0:3
IF-MIB::ifPhysAddress.4 = STRING:
IF-MIB::ifAdminStatus.1 = INTEGER: up(1)
IF-MIB::ifAdminStatus.2 = INTEGER: up(1)
IF-MIB::ifAdminStatus.3 = INTEGER: up(1)
IF-MIB::ifAdminStatus.4 = INTEGER: down(2)
IF-MIB::ifOperStatus.1 = INTEGER: up(1)
IF-MIB::ifOperStatus.2 = INTEGER: down(2)
IF-MIB::ifOperStatus.3 = INTEGER: up(1)
IF-MIB::ifOperStatus.4 = INTEGER: down(2)
IF-MIB::ifLastChange.1 = Timeticks: (0) 0:00:00.00
IF-MIB::ifLastChange.2 = Timeticks: (0) 0:00:00.00
IF-MIB::ifLastChange.3 = Timeticks: (0) 0:00:00.00
IF-MIB::ifLastChange.4 = Timeticks: (0) 0:00:00.00
IF-MIB::ifInOctets.1 = Counter32: 23983
IF-MIB::ifInOctets.2 = Counter32: 0
IF-MIB::ifInOctets.3 = Counter32: 34634
IF-MIB::ifInOctets.4 = Counter32: 0
IF-MIB::ifInUcastPkts.1 = Counter32: 276
IF-MIB::ifInUcastPkts.2 = Counter32: 0
IF-MIB::ifInUcastPkts.3 = Counter32: 124
IF-MIB::ifInUcastPkts.4 = Counter32: 0
IF-MIB::ifInNUcastPkts.1 = Counter32: 0
IF-MIB::ifInNUcastPkts.2 = Counter32: 0
IF-MIB::ifInNUcastPkts.3 = Counter32: 0
IF-MIB::ifInNUcastPkts.4 = Counter32: 0
IF-MIB::ifInDiscards.1 = Counter32: 0
IF-MIB::ifInDiscards.2 = Counter32: 0
IF-MIB::ifInDiscards.3 = Counter32: 0
IF-MIB::ifInDiscards.4 = Counter32: 0
IF-MIB::ifInErrors.1 = Counter32: 0
IF-MIB::ifInErrors.2 = Counter32: 0
IF-MIB::ifInErrors.3 = Counter32: 0
IF-MIB::ifInErrors.4 = Counter32: 0
```

```
IF-MIB::ifInUnknownProtos.1 = Counter32: 0
IF-MIB::ifInUnknownProtos.2 = Counter32: 0
IF-MIB::ifInUnknownProtos.3 = Counter32: 0
IF-MIB::ifInUnknownProtos.4 = Counter32: 0
IF-MIB::ifOutOctets.1 = Counter32: 23983
IF-MIB::ifOutOctets.2 = Counter32: 0
IF-MIB::ifOutOctets.3 = Counter32: 21116
IF-MIB::ifOutOctets.4 = Counter32: 0
IF-MIB::ifOutUcastPkts.1 = Counter32: 276
IF-MIB::ifOutUcastPkts.2 = Counter32: 0
IF-MIB::ifOutUcastPkts.3 = Counter32: 139
IF-MIB::ifOutUcastPkts.4 = Counter32: 0
IF-MIB::ifOutNUcastPkts.1 = Counter32: 0
IF-MIB::ifOutNUcastPkts.2 = Counter32: 0
IF-MIB::ifOutNUcastPkts.3 = Counter32: 0
IF-MIB::ifOutNUcastPkts.4 = Counter32: 0
IF-MIB::ifOutDiscards.1 = Counter32: 0
IF-MIB::ifOutDiscards.2 = Counter32: 0
IF-MIB::ifOutDiscards.3 = Counter32: 0
IF-MIB::ifOutDiscards.4 = Counter32: 0
IF-MIB::ifOutErrors.1 = Counter32: 0
IF-MIB::ifOutErrors.2 = Counter32: 0
IF-MIB::ifOutErrors.3 = Counter32: 0
IF-MIB::ifOutErrors.4 = Counter32: 0
IF-MIB::ifOutQLen.1 = Gauge32: 0
IF-MIB::ifOutQLen.2 = Gauge32: 0
IF-MIB::ifOutQLen.3 = Gauge32: 0
IF-MIB::ifOutQLen.4 = Gauge32: 0
IF-MIB::ifSpecific.1 = OID: SNMPv2-SMI::zeroDotZero
IF-MIB::ifSpecific.2 = OID: SNMPv2-SMI::zeroDotZero
IF-MIB::ifSpecific.3 = OID: SNMPv2-SMI::zeroDotZero
IF-MIB::ifSpecific.4 = OID: SNMPv2-SMI::zeroDotZero
[root@www ~]#
```

Ahora se descarga de Internet las fuentes de MRTG, y lo ubicamos en /opt/instaladores que es en donde estan todos los paquetes instalados en nuestro sistema:

```
 [root@www instaladores]# rpm -ivh mrtg-2.14.5-2.i386.rpm
Preparing...                ########################################### [100%]
   1:mrtg                   ########################################### [100%]
[root@www instaladores]#
```

Vamos al archivo de configuracion de mrtg:

```
[root@practica ~]# cd /etc/mrtg
[root@practica mrtg]# cp mrtg.conf mrtg.conf.ori
mrtg.cfg mrtg.conf.ori
```

Creamos un nuevo archivo mrtg con unas especificaciones propias para que direccione las estadisticas graficas a /home/web/mrtg y salida del archivo en /etc/mrtg/mrtg.cfg del router con ip 192,168,248,213

[root@practica mrtg]# **cfgmaker --global "WorkDir: /home/web/mrtg" --global "Options[_]: bits,growright" --output /etc/mrtg/mrtg.cfg public@192.168.1.1**

Vamos al archivo de configuracion de mrtg para observer cuantas Interfaces posee el dispositivo:

```
[root@www ]#cd /etc/mrtg
[root@www mrtg]# cat mrtg.cfg
# Created by
#  /usr/bin/cfgmaker --global 'WorkDir: /home/web/mrtg' --global 'Options[_]: bits,growright' --output /etc/mrtg/mrtg.cfg public@192.168.1.1


### Global Config Options

#  for UNIX
# WorkDir: /home/http/mrtg

#  or for NT
# WorkDir: c:\mrtgdata

### Global Defaults

#  to get bits instead of bytes and graphs growing to the right
# Options[_]: growright, bits

EnableIPv6: no
WorkDir: /home/web/mrtg
Options[_]: bits,growright

######################################################################
#
# System: www.imf.com.co
# Description: Linux www.imf.com.co 2.6.18-1.2798.fc6 #1 SMP Mon Oct 16 14:37:32 EDT 2006 i686
# Contact: Root <root@localhost> (configure /etc/snmp/snmp.local.conf)
# Location: Unknown (edit /etc/snmp/snmpd.conf)
######################################################################
#


### Interface 1 >> Descr: 'lo' | Name: 'lo' | Ip: '127.0.0.1' | Eth: '' ###
### The following interface is commented out because:
### * it is a Software Loopback interface
#
# Target[192.168.1.1_1]: 1:public@192.168.1.1:
# SetEnv[192.168.1.1_1]: MRTG_INT_IP="127.0.0.1" MRTG_INT_DESCR="lo"
# MaxBytes[192.168.1.1_1]: 1250000
# Title[192.168.1.1_1]: Traffic Analysis for 1 -- www.imf.com.co
# PageTop[192.168.1.1_1]: <h1>Traffic Analysis for 1 -- www.imf.com.co</h1>
#             <div id="sysdetails">
#                     <table>
#                             <tr>
```

```
#                               <td>System:</td>
#                                                       <td>www.imf.com.co in Unknown (edit
/etc/snmp/snmpd.conf)</td>
#                           </tr>
#                           <tr>
#                               <td>Maintainer:</td>
#                                                   <td>Root &lt;root@localhost&gt; (configure
/etc/snmp/snmp.local.conf)</td>
#                           </tr>
#                           <tr>
#                               <td>Description:</td>
#                               <td>lo  </td>
#                           </tr>
#                           <tr>
#                               <td>ifType:</td>
#                               <td>softwareLoopback (24)</td>
#                           </tr>
#                           <tr>
#                               <td>ifName:</td>
#                               <td>lo</td>
#                           </tr>
#                           <tr>
#                               <td>Max Speed:</td>
#                               <td>10.0 Mbits/s</td>
#                           </tr>
#                           <tr>
#                               <td>Ip:</td>
#                               <td>127.0.0.1 (localhost.localdomain)</td>
#                           </tr>
#                   </table>
#           </div>


### Interface 2 >> Descr: 'eth0' | Name: 'eth0' | Ip: '10.21.28.2' | Eth: '00-0c-46-cd-e0-
03' ###

Target[192.168.1.1_2]: 2:public@192.168.1.1:
SetEnv[192.168.1.1_2]:      MRTG_INT_IP="10.21.28.2"      MRTG_INT_DESCR="eth0-
externa"
MaxBytes[192.168.1.1_2]: 1250000
Title[192.168.1.1_2]:  Analisis Trafica canal WAN  -- www.imf.com.co
PageTop[192.168.1.1_2]: <h1>Analisis canal wan  -- www.imf.com.co</h1>
            <div id="sysdetails">
                <table>
                    <tr>
                        <td>System:</td>
                        <td>www.imf.com.co            in            Unknown            (edit
/etc/snmp/snmpd.conf)</td>
                    </tr>
                    <tr>
                        <td>Maintainer:</td>
                        <td>Root              &lt;root@localhost&gt;              (configure
/etc/snmp/snmp.local.conf)</td>
                    </tr>
                    <tr>
```

```
                        <td>Description:</td>
                        <td>eth0  </td>
                    </tr>
                    <tr>
                        <td>ifType:</td>
                        <td>ethernetCsmacd (6)</td>
                    </tr>
                    <tr>
                        <td>ifName:</td>
                        <td>eth0</td>
                    </tr>
                    <tr>
                        <td>Max Speed:</td>
                        <td>10.0 Mbits/s</td>
                    </tr>
                    <tr>
                        <td>Ip:</td>
                        <td>10.21.28.2 ()</td>
                    </tr>
                </table>
            </div>


### Interface 3 >> Descr: 'eth1' | Name: 'eth1' | Ip: '192.168.1.1' | Eth: '00-18-fe-77-42-
f9' ###

#Target[192.168.1.1_3]: 3:public@192.168.1.1:
#SetEnv[192.168.1.1_3]: MRTG_INT_IP="192.168.1.1" MRTG_INT_DESCR="eth1"
#MaxBytes[192.168.1.1_3]: 12500000
#Title[192.168.1.1_3]: Traffic Analysis for 3 -- www.imf.com.co
#PageTop[192.168.1.1_3]: <h1>Traffic Analysis for 3 -- www.imf.com.co</h1>
            <div id="sysdetails">
                <table>
                    <tr>
                        <td>System:</td>
                        <td>www.imf.com.co            in            Unknown            (edit
/etc/snmp/snmpd.conf)</td>
                    </tr>
                    <tr>
                        <td>Maintainer:</td>
                        <td>Root            &lt;root@localhost&gt;            (configure
/etc/snmp/snmp.local.conf)</td>
                    </tr>
                    <tr>
                        <td>Description:</td>
                        <td>eth1  </td>
                    </tr>
                    <tr>
                        <td>ifType:</td>
                        <td>ethernetCsmacd (6)</td>
                    </tr>
                    <tr>
                        <td>ifName:</td>
                        <td>eth1</td>
                    </tr>
```

```
                        <tr>
                                <td>Max Speed:</td>
                                <td>100.0 Mbits/s</td>
                        </tr>
                        <tr>
                                <td>Ip:</td>
                                <td>192.168.1.1 (www.imf.com.co)</td>
                        </tr>
                </table>
        </div>


### Interface 4 >> Descr: 'sit0' | Name: 'sit0' | Ip: '' | Eth: '' ###
### The following interface is commented out because:
### * it is administratively DOWN
### * it is operationally DOWN
### * has a speed of 0 which makes no sense
#
# Target[192.168.1.1_4]: 4:public@192.168.1.1:
# SetEnv[192.168.1.1_4]: MRTG_INT_IP="" MRTG_INT_DESCR="sit0"
# MaxBytes[192.168.1.1_4]: 0
# Title[192.168.1.1_4]: Traffic Analysis for 4 -- www.imf.com.co
# PageTop[192.168.1.1_4]: <h1>Traffic Analysis for 4 -- www.imf.com.co</h1>
#         <div id="sysdetails">
#                 <table>
#                         <tr>
#                                 <td>System:</td>
#                                                         <td>www.imf.com.co in Unknown (edit
/etc/snmp/snmpd.conf)</td>
#                         </tr>
#                         <tr>
#                                 <td>Maintainer:</td>
#                                                 <td>Root &lt;root@localhost&gt; (configure
/etc/snmp/snmp.local.conf)</td>
#                         </tr>
#                         <tr>
#                                 <td>Description:</td>
#                                 <td>sit0  </td>
#                         </tr>
#                         <tr>
#                                 <td>ifType:</td>
#                                 <td>Encapsulation Interface (131)</td>
#                         </tr>
#                         <tr>
#                                 <td>ifName:</td>
#                                 <td>sit0</td>
#                         </tr>
#                         <tr>
#                                 <td>Max Speed:</td>
#                                 <td>0.0 bits/s</td>
#                         </tr>
#                 </table>
#         </div>
```

El paquete de **MRTG** incluye un guión para **crond**, el cual se instala en la ruta **/etc/cron.d/mrtg**, de modo que éste ejecute **MRTG**, de forma **automática**, cada 5 minutos. Si se quiere comprobar la configuración solo es necesario esperar algunos minutos y consultar los resultados.

```
[root@www /]# cd /etc/cron.d/
[root@www cron.d]# ls
mailman  mrtg
[root@www cron.d]# cat mrtg
*/5 * * * * root LANG=C LC_ALL=C /usr/bin/mrtg /etc/mrtg/mrtg.cfg --lock-file
/var/lock/mrtg/mrtg_l --confcache-file /var/lib/mrtg/mrtg.ok
[root@www cron.d]#
```

Para poder visualizar en una sola pagina todas las interfaces asociadas al dispositivo a monitorear, ingresamos:

```
[root@www /]#indexmaker --output /home/web/mrtg/index.html  /etc/mrtg/mrtg.cfg
```

Ahora es necesario revisar estos reportes a traves del navegador, para ello es necesario ir al directorio conf.d del apache y en el archivo mrtg moverlo para que en el httpd.conf se pueda especificar al Alias donde esta ubicada la pagina index.html generada por el mrtg y no cree conflicto:

```
[root@practica mrtg]# cd /etc/httpd/conf.d
[root@practica conf.d]# ls
auth_kerb.conf        htdig.conf      perl.conf       squirrelmail.conf       welcome.conf
auth_mysql.conf       mailman.conf  php.conf        ssl.conf
        wordtrans.conf
auth_pgsql.conf       manual.conf   python.conf     subversion.conf
        authz_ldap.conf  mrtg.conf            README      webalizer.conf
[root@www conf.d]# cat mrtg.conf
#
# This configuration file maps the mrtg output (generated daily)
# into the URL space.  By default these results are only accessible
# from the local host.
#
Alias /mrtg/ " /home/web/mrtg"

<Location /mrtg>
 Allow from
 Allow from ::1
 Allow from
</Location>
[root@www conf.d]# mv mrtg.conf mrtg.conf.ori
```

```
[root@practica conf.d]# cd ..
[root@www conf]# vi httpd.conf
Alias /mrtg/ "/home/web/mrtg/"
```

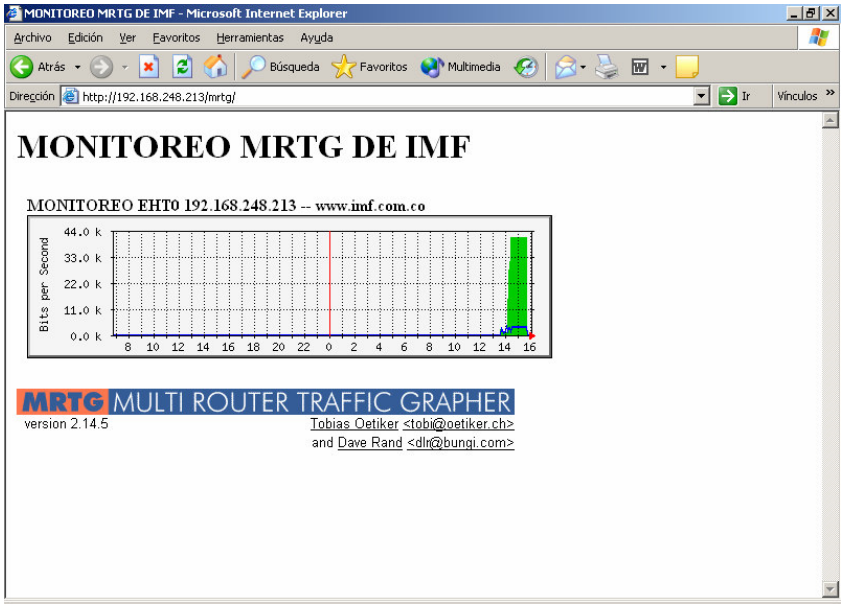
reiniciamos el apache para que tome los cambios;

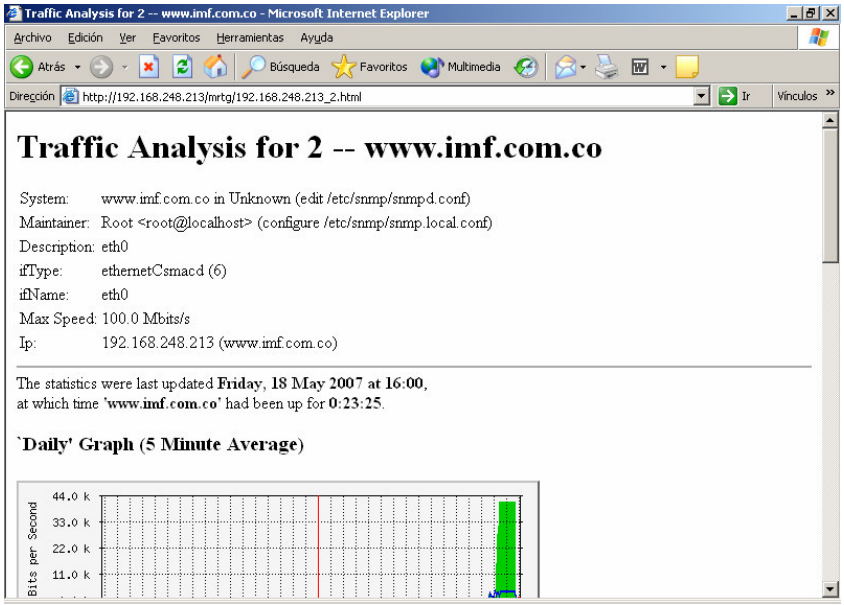
```
[root@www /]# service httpd restart
Parando httpd:                                [  OK  ]
Iniciando httpd:                              [  OK  ]
```

Revisamos los permisos que contiene el directorio mrtg para que sea visualizado a traves del navegador

```
[root@www conf]# cd /home/web
[root@www web]# ls -l
total 24
-rw-r--r-- 1 root   root    742 may  8 22:38 exten.html
-rw-r--r-- 1 root   root     68 may  3 17:58 index.html
drwxr-xr-x 2 root   root   4096 may 18 16:30 mrtg
-rw-r--r-- 1 root   root     85 may  8 16:07 prohibit.html
drwxr-xr-x 6 apache apache 4096 may 17 12:44 reportes
-rw-r--r-- 1 root   root    734 may  8 22:36 urls.html
[root@www web]# cd mrtg
[root@www mrtg]# ls -l
total 256
-rwxr-xr-x 1 apache root  1787 may 18 16:05 10.21.28.1_2-day.png
-rwxr-xr-x 1 apache root  6709 may 18 16:05 10.21.28.1_2.html
-rw-r--r-- 1 root   root 48440 may 18 16:05 10.21.28.1_2.log
-rwxr-xr-x 1 apache root  1460 may 18 15:35 10.21.28.1_2-month.png
-rw-r--r-- 1 root   root 48421 may 18 16:00 10.21.28.1_2.old
-rwxr-xr-x 1 apache root  1572 may 18 15:50 10.21.28.1_2-week.png
-rwxr-xr-x 1 apache root  1752 may 18 13:35 10.21.28.1_2-year.png
-rw-r--r-- 1 root   root  1397 may 18 16:30 10.21.28.1_3-day.png
-rw-r--r-- 1 root   root  6491 may 18 16:30 10.21.28.1_3.html
-rw-r--r-- 1 root   root 48180 may 18 16:30 10.21.28.1_3.log
-rw-r--r-- 1 root   root  1368 may 18 16:10 10.21.28.1_3-month.png
-rw-r--r-- 1 root   root 48199 may 18 16:25 10.21.28.1_3.old
-rw-r--r-- 1 root   root  1416 may 18 16:10 10.21.28.1_3-week.png
-rw-r--r-- 1 root   root  1752 may 18 16:10 10.21.28.1_3-year.png
-rwxr-xr-x 1 apache root  2465 may 18 14:17 index.html
-rwxr-xr-x 1 apache root   538 may 18 13:35 mrtg-l.png
-rwxr-xr-x 1 apache root   414 may 18 13:35 mrtg-m.png
-rwxr-xr-x 1 apache root  1759 may 18 13:35 mrtg-r.png
[root@www mrtg]#
```

En el navegador se digita: http://192.168.1.1/mrtg , y lo que muestra es el analisis de trafico de la eth0 en bits por segundos vs. tiempo


MONITOREO MRTG DE IMF - Microsoft Internet Explorer
Archivo Edición Ver Favoritos Herramientas Ayuda
Atrás Búsqueda Favoritos Multimedia
Dirección http://192.168.248.213/mrtg/
Ir Vínculos
MONITOREO MRTG DE IMF
MONITOREO EHT0 192.168.248.213 -- www.imf.com.co
Bits per Second
44.0 k
33.0 k
22.0 k
11.0 k
0.0 k
8 10 12 14 16 18 20 22 0 2 4 6 8 10 12 14 16
MRTG MULTI ROUTER TRAFFIC GRAPHER
version 2.14.5
Tobias Oetiker <tobi@oetiker.ch>
and Dave Rand <dlr@bungi.com>


Traffic Analysis for 2 -- www.imf.com.co - Microsoft Internet Explorer
Archivo Edición Ver Favoritos Herramientas Ayuda
Atrás Búsqueda Favoritos Multimedia
Dirección http://192.168.248.213/mrtg/192.168.248.213_2.html
Ir Vínculos
Traffic Analysis for 2 -- www.imf.com.co
System: www.imf.com.co in Unknown (edit /etc/snmp/snmpd.conf)
Maintainer: Root <root@localhost> (configure /etc/snmp/snmp.local.conf)
Description: eth0
ifType: ethernetCsmacd (6)
ifName: eth0
Max Speed: 100.0 Mbits/s
Ip: 192.168.248.213 (www.imf.com.co)
The statistics were last updated Friday, 18 May 2007 at 16:00,
at which time 'www.imf.com.co' had been up for 0:23:25.
`Daily' Graph (5 Minute Average)
Bits per Second
44.0 k
33.0 k
22.0 k
11.0 k