Universitat d'Alacant
Universidad de Alicante

APLICACIONES DE MONITORIZACIÓN

Universitat d'Alacant
Universidad de Alicante

- HERRAMIENTAS DE CONTROL
  - SERVICIOS DE RED, RECURSOS HW, SW
    - NAGIOS
  - DETECCIÓN DE INTRUSOS
    - SNORT - ACID

Universitat d'Alacant
Universidad de Alicante

- NAGIOS. Características
  - Sistema de monitorización de las aplicaciones y servicios proporcionados por el SI, que informa automática e instantáneamente 24 horas al día, 365 días al año, en caso de que se produzca un fallo en los mismos.
  - Software Libre. S.O. Linux.
  - Altamente configurable mediante plugins
  - Disponible interfaz web para consulta del estado de los recursos y servidores
  - Sistema de notificaciones muy flexible.

Universitat d'Alacant
Universidad de Alicante

- NAGIOS. Monitorización de servicios de red (I)
  - Correo (SMTP, POP3, IMAP)
  - Resolución de nombres (DNS)
  - Servidores WWW (HTTP), FTP, Proxies

- NAGIOS. Monitorización de servicios de red (II)
  - Carga de CPU
  - Chequeo de puertos (TCP, UDP)
  - Tráfico de red (carga de las interfaces)

- NAGIOS. Monitorización de recursos locales
  - Espacio en disco
  - Carga de CPU
  - Uso de memoria
  - Chequeo de logs
  - Hora del sistema
  - Procesos (Existencia o no, número, etc)
  - Ficheros (Existencia o no, fecha/hora, tamaño, etc)

Universitat d'Alacant
Universidad de Alicante

- NAGIOS. Monitorización de otros recursos.
  - Bases de datos.
  - Clusters de máquinas/servicios.
  - Servidores RAID.
  - Parámetros físicos
    - Temperatura, humedad, carga eléctrica.

- NAGIOS. Notificaciones (I).
  - Un servicio o recurso puede tener 4 estados
    - OK, CRITICAL, WARNING, UNKNOWN
  - Cuando se produce un cambio de estado se dispara una alerta que puede producir una notificación al responsable de la máquina/servicio.
  - Tipos de notificación.
    - Interfaz web (sonora, visual)
    - Mensaje Correo electrónico.
    - Mensaje SMS.

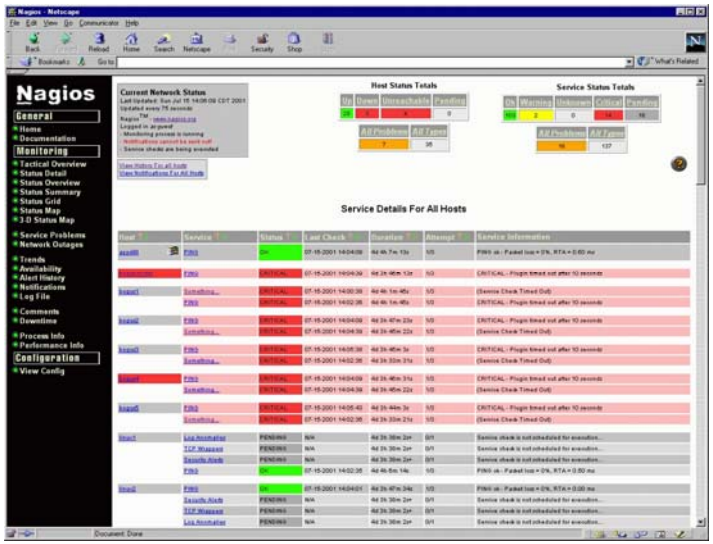
- NAGIOS. Notificaciones (II).
  - Permiten resolver el problema más rápidamente y en ocasiones de forma automática mediante "handlers" o pequeños programas que se ejecutan cuando ocurre un fallo en el sistema (ej. levantar servidor web si se detecta estado critical).
  - Tiene en cuenta las dependencias entre servicios (ej. Base de datos - aplicación web – servidor web)

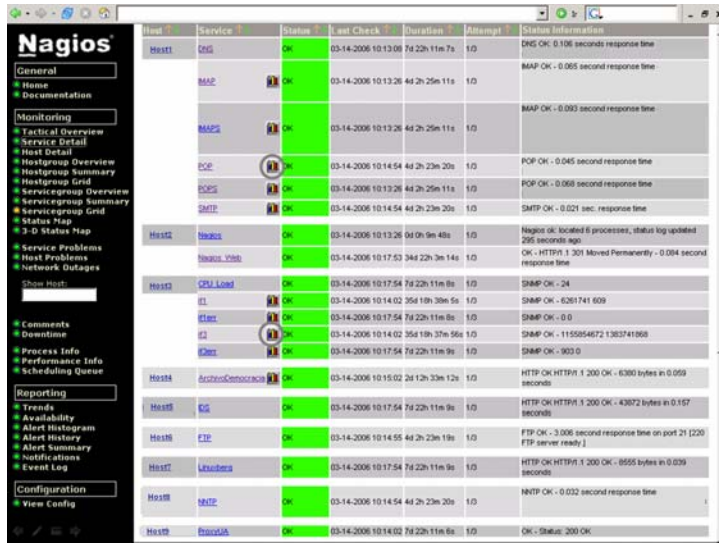
Universitat d'Alacant
Universidad de Alicante

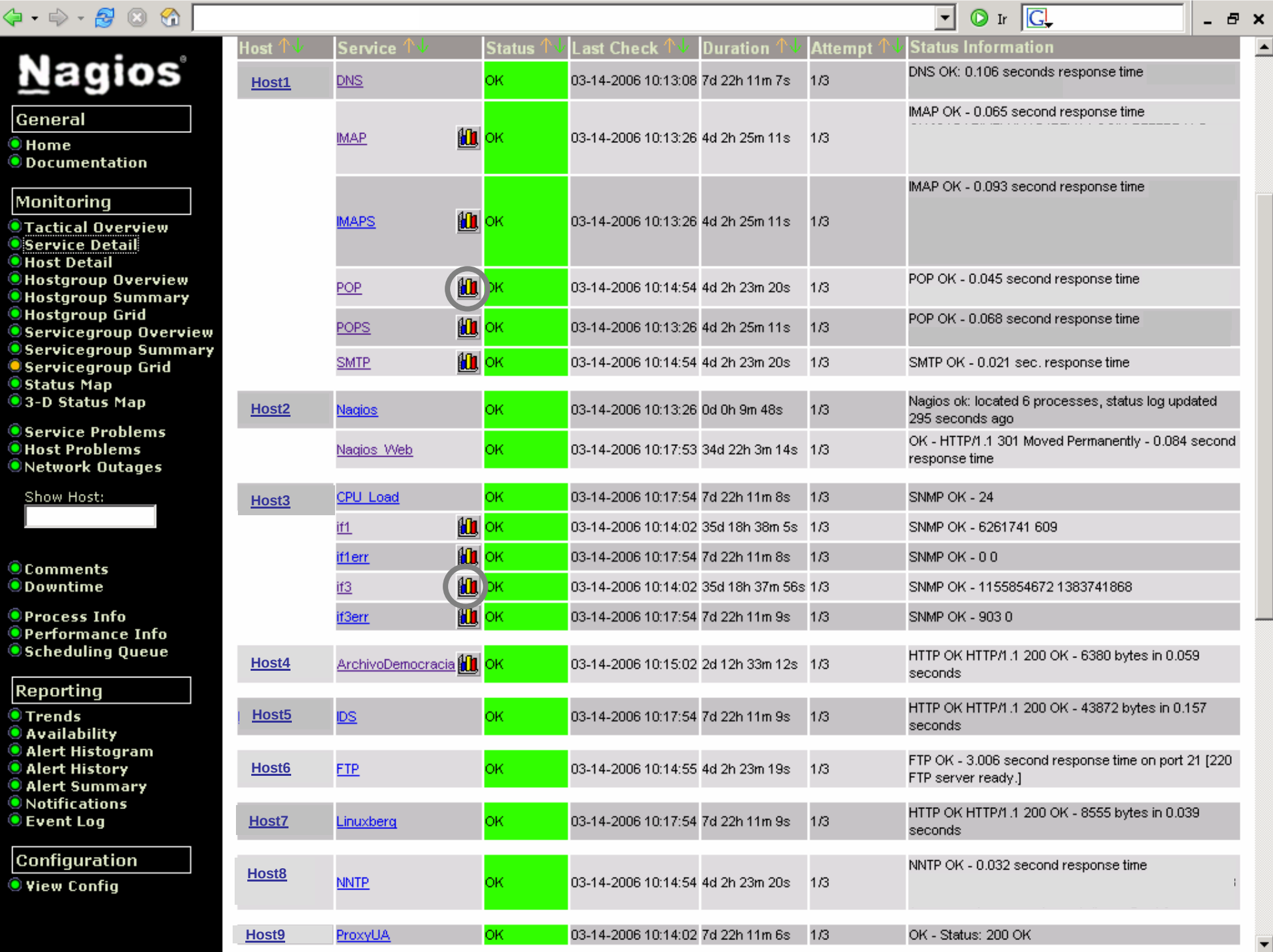
- NAGIOS. Notificaciones (III).
  - Se producen en función de la hora y/o día (ej. backups, mantenimientos, etc)
  - Se elige el método en función del estado del servicio (ej. email para warning, SMS para critical y ok)

Universitat d'Alacant
Universidad de Alicante

- NAGIOS. Interfaz web.





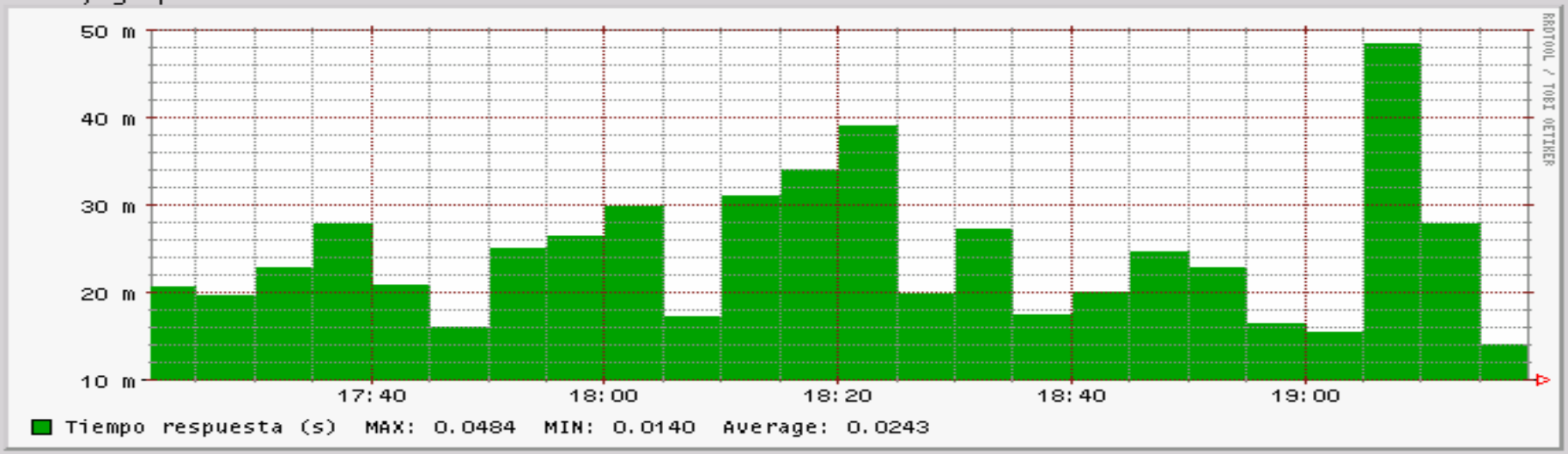


Host	Service	Status	Last Check	Duration	Attempt	Status Information
Host1	DNS	OK	03-14-2006 10:13:08	7d 22h 11m 7s	1/3	DNS OK: 0.106 seconds response time
	IMAP	OK	03-14-2006 10:13:26	4d 2h 25m 11s	1/3	IMAP OK - 0.065 second response time
	IMAPS	OK	03-14-2006 10:13:26	4d 2h 25m 11s	1/3	IMAP OK - 0.093 second response time
	POP	OK	03-14-2006 10:14:54	4d 2h 23m 20s	1/3	POP OK - 0.045 second response time
	POPS	OK	03-14-2006 10:13:26	4d 2h 25m 11s	1/3	POP OK - 0.068 second response time
	SMTP	OK	03-14-2006 10:14:54	4d 2h 23m 20s	1/3	SMTP OK - 0.021 sec. response time
Host2	Nagios	OK	03-14-2006 10:13:26	0d 0h 9m 48s	1/3	Nagios ok: located 6 processes, status log updated 295 seconds ago
	Nagios_Web	OK	03-14-2006 10:17:53	34d 22h 3m 14s	1/3	OK - HTTP/1.1 301 Moved Permanently - 0.084 second response time
Host3	CPU_Load	OK	03-14-2006 10:17:54	7d 22h 11m 8s	1/3	SNMP OK - 24
	if1	OK	03-14-2006 10:14:02	35d 18h 38m 5s	1/3	SNMP OK - 6261741 609
	if1err	OK	03-14-2006 10:17:54	7d 22h 11m 8s	1/3	SNMP OK - 0 0
	if3	OK	03-14-2006 10:14:02	35d 18h 37m 56s	1/3	SNMP OK - 1155854672 1383741868
	if3err	OK	03-14-2006 10:17:54	7d 22h 11m 9s	1/3	SNMP OK - 903 0
Host4	ArchivoDemocracia	OK	03-14-2006 10:15:02	2d 12h 33m 12s	1/3	HTTP OK HTTP/1.1 200 OK - 6380 bytes in 0.059 seconds
Host5	IDS	OK	03-14-2006 10:17:54	7d 22h 11m 9s	1/3	HTTP OK HTTP/1.1 200 OK - 43872 bytes in 0.157 seconds
Host6	FTP	OK	03-14-2006 10:14:55	4d 2h 23m 19s	1/3	FTP OK - 3.006 second response time on port 21 [220 FTP server ready.]
Host7	Linuxberg	OK	03-14-2006 10:17:54	7d 22h 11m 9s	1/3	HTTP OK HTTP/1.1 200 OK - 8555 bytes in 0.039 seconds
Host8	NNTP	OK	03-14-2006 10:14:54	4d 2h 23m 20s	1/3	NNTP OK - 0.032 second response time
Host9	ProxyUA	OK	03-14-2006 10:14:02	7d 22h 11m 6s	1/3	OK - Status: 200 OK

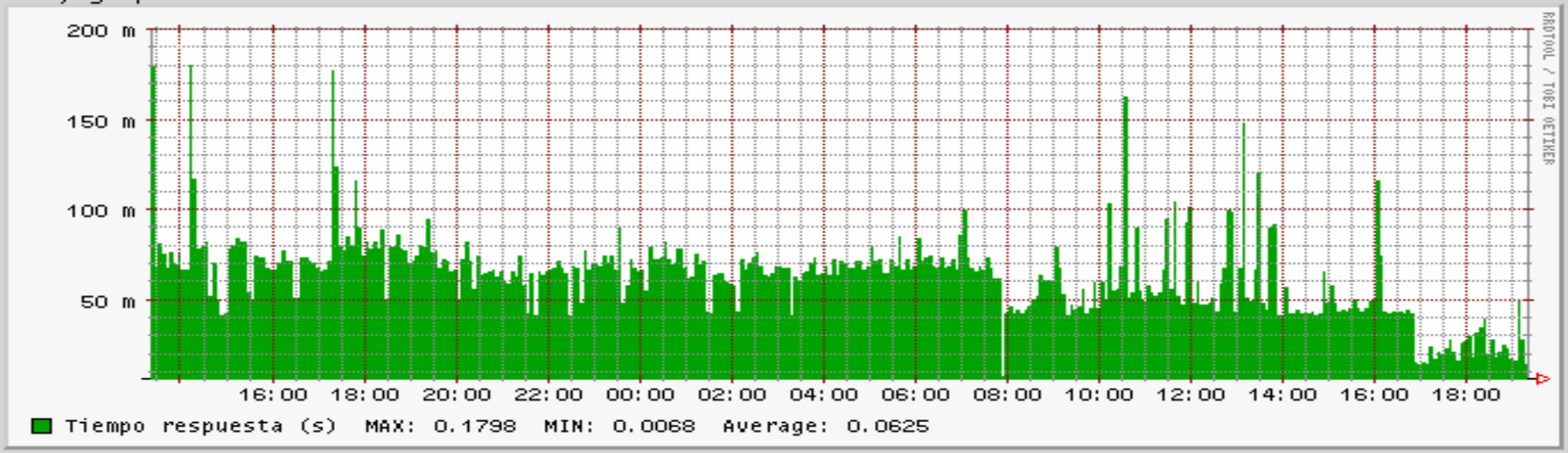
Servidor de Correo

Gráfico generado: Fri Mar 10 19:21:04 2006

Hourly graph



Daily graph

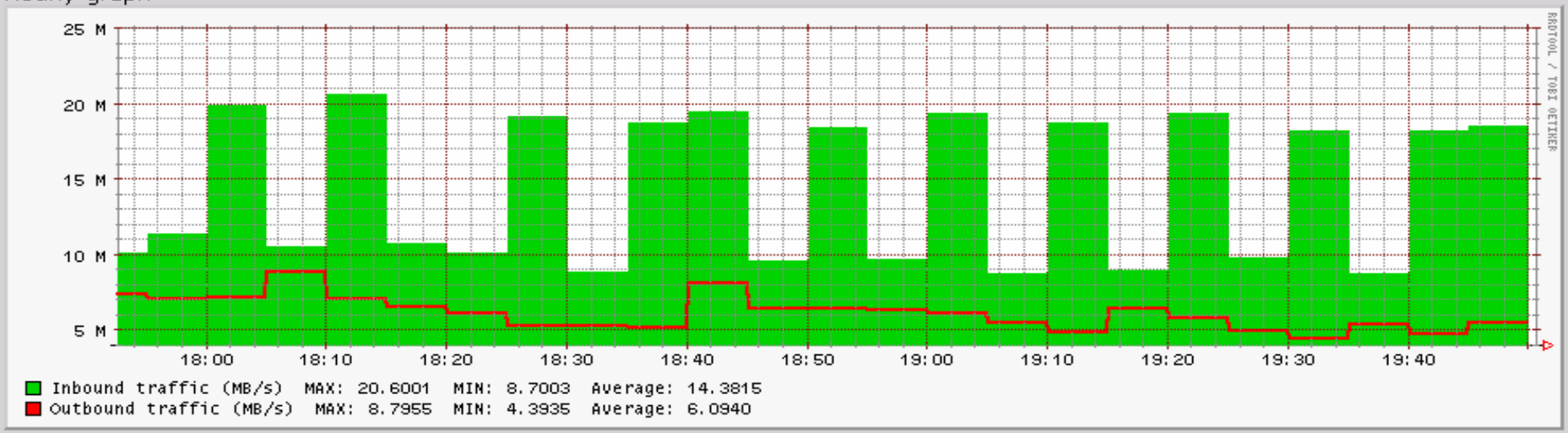


Weekly graph

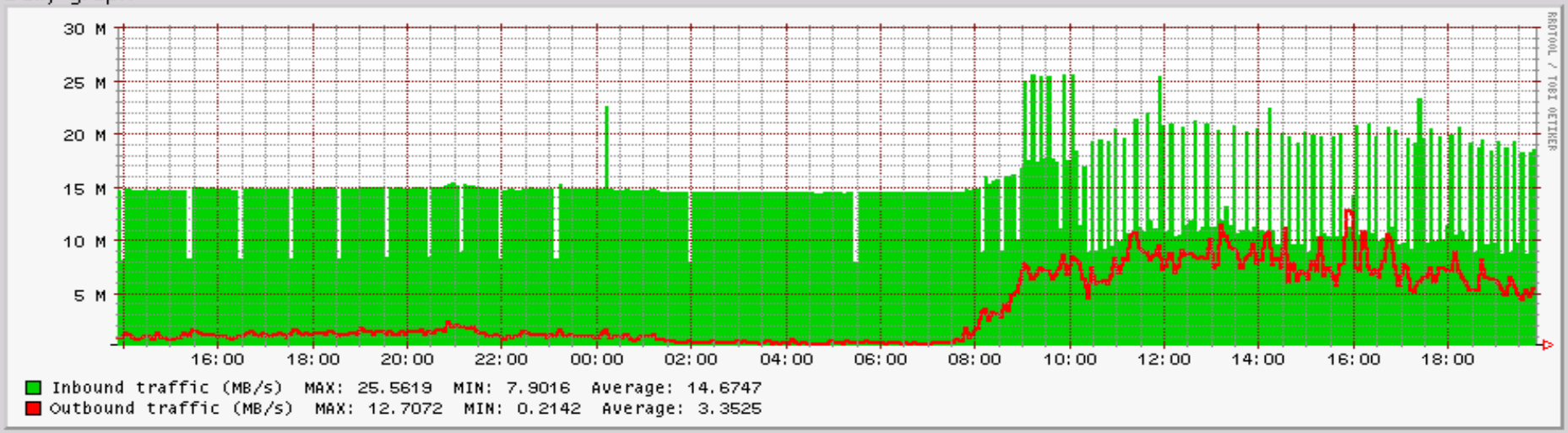
Router

Gráfico generado: Mon Mar 13 19:52:36 2006

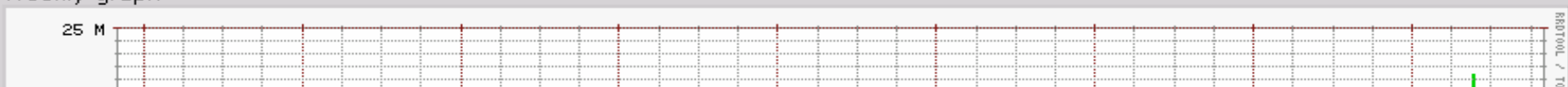
Hourly graph



Daily graph



Weekly graph



Universitat d'Alacant
Universidad de Alicante

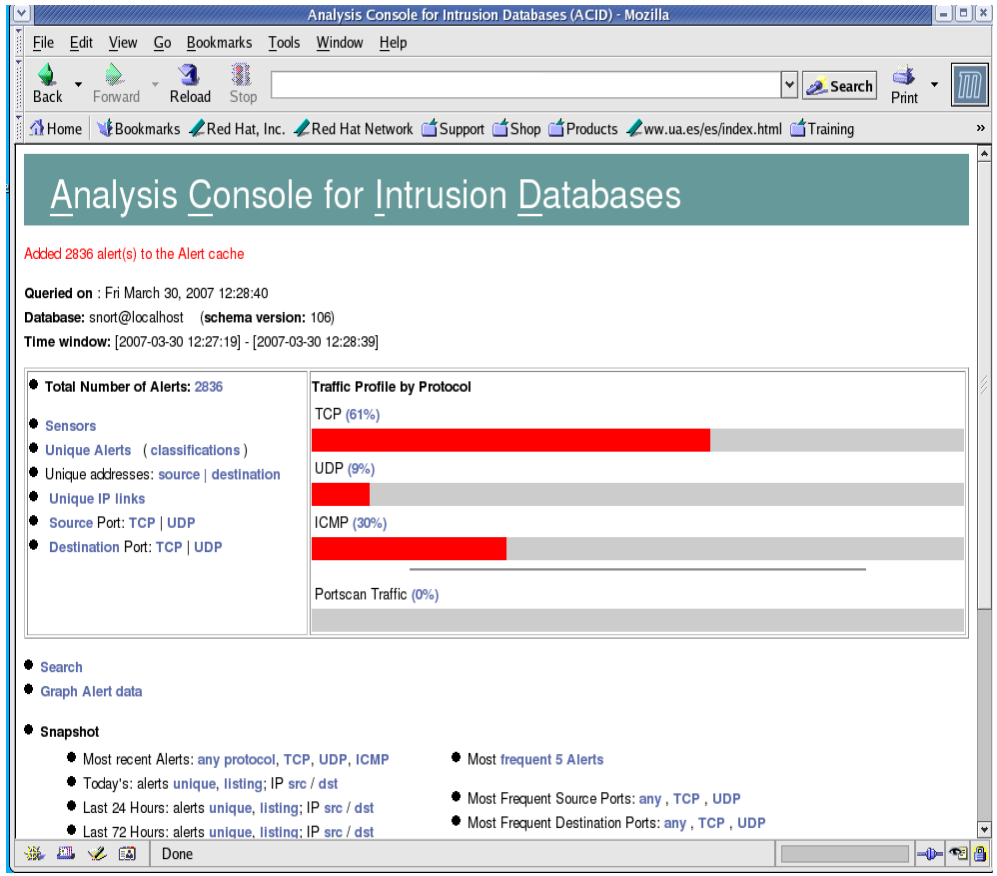
- SNORT - ACID. Características (I).
  - Sistema de detección de intrusos (IDS) en la red.
  - Analiza el tráfico de paquetes IP en tiempo real.
  - Realiza análisis de protocolo y búsqueda de patrones en el contenido de los paquetes para detectar una gran variedad de ataques.

Universitat d'Alacant
Universidad de Alicante

- SNORT - ACID. Características (II).
  - Informa mediante su interfaz web (ACID) del tráfico analizado.
  - Se bloquea el tráfico por la red de programas nocivos como virus, programas espía, etc.
  - Dota de mayor seguridad a la intranet de la Universidad de Alicante.

Universitat d'Alacant
Universidad de Alicante

- SNORT - ACID. Interfaz Web.



Analysis Console for Intrusion Databases

Added 2836 alert(s) to the Alert cache

Queried on : Fri March 30, 2007 12:28:40

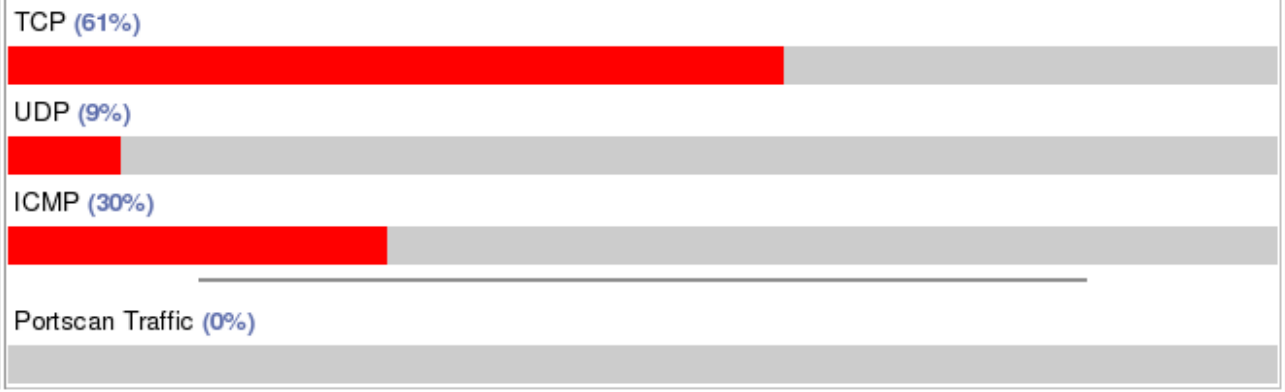
Database: snort@localhost (**schema version:** 106)

Time window: [2007-03-30 12:27:19] - [2007-03-30 12:28:39]

- **Total Number of Alerts:** 2836

- Sensors
- Unique Alerts (classifications)
- Unique addresses: source | destination
- Unique IP links
- Source Port: TCP | UDP
- Destination Port: TCP | UDP

Traffic Profile by Protocol



- Search
- Graph Alert data

- **Snapshot**
  - Most recent Alerts: any protocol, TCP, UDP, ICMP
  - Today's: alerts unique, listing; IP src / dst
  - Last 24 Hours: alerts unique, listing; IP src / dst
  - Last 72 Hours: alerts unique, listing; IP src / dst
  - Most frequent 5 Alerts
  - Most Frequent Source Ports: any , TCP , UDP
  - Most Frequent Destination Ports: any , TCP , UDP

< Signature >	< Classification >	< Total # >	Sensor #	< Src. Addr. >	< Dest. Addr. >	< First >	< Last >
url[snort] BLEEDING-EDGE P2P BitTorrent peer sync	policy-violation	245 (7%)	1	47	71	2007-03-30 12:27:19	2007-03-30 12:29:02
[arachNIDS][snort] ICMP PING NMAP	attempted-recon	371 (10%)	1	172	25	2007-03-30 12:27:19	2007-03-30 12:29:05
[snort] ICMP PING	misc-activity	421 (11%)	1	173	26	2007-03-30 12:27:19	2007-03-30 12:29:05
[snort] (http_inspect) BARE BYTE UNICODE ENCODING	*unclassified*	603 (16%)	1	331	254	2007-03-30 12:27:19	2007-03-30 12:29:02
nessus[cve][icat][bugtraq][snort] WEB-PHP viewtopic.php access	web-application-attack	12 (0%)	1	4	7	2007-03-30 12:27:19	2007-03-30 12:28:17
[snort] (http_inspect) DOUBLE DECODING ATTACK	*unclassified*	89 (2%)	1	25	20	2007-03-30 12:27:19	2007-03-30 12:28:58
url[arachNIDS][snort] POLICY SMTP relaying denied	misc-activity	227 (6%)	1	2	157	2007-03-30 12:27:19	2007-03-30 12:29:02
[snort] (http_inspect) OVERSIZE REQUEST-URI DIRECTORY	*unclassified*	8 (0%)	1	5	5	2007-03-30 12:27:19	2007-03-30 12:28:59
url[snort] BLEEDING-EDGE Malware Hotbar Agent Activity	trojan-activity	4 (0%)	1	4	2	2007-03-30 12:27:19	2007-03-30 12:28:28
url[snort] BLEEDING-EDGE MALWARE Alexa Search Toolbar	trojan-activity	44 (1%)	1	2	5	2007-03-30 12:27:19	2007-03-30 12:28:59
[snort] MISC Tiny Fragments	bad-unknown	203 (5%)	1	4	1	2007-03-30 12:27:19	2007-03-30 12:29:03
url[snort] BLEEDING-EDGE MALWARE Suspicious User Agent	trojan-activity	6 (0%)	1	4	4	2007-03-30 12:27:20	2007-03-30 12:28:55
[snort] ICMP Destination Unreachable Port Unreachable	misc-activity	29 (1%)	1	2	13	2007-03-30	2007-03-30

Layer 4 Criteria	*none*
Payload Criteria	*any*

- Source Port: TCP | UDP
- Destination Port: TCP | UDP
- Time profile of alerts

Displaying alerts 1-50 of 408 total

ID	< Signature >	< Timestamp >	< Source Address >	< Dest. Address >	< Layer 4 Proto >
#0-(1-1)	url[snort] BLEEDING-EDGE P2P BitTorrent peer sync	2007-03-30 12:27:19			TCP
#1-(1-6)	url[snort] BLEEDING-EDGE P2P BitTorrent peer sync	2007-03-30 12:27:19			TCP
#2-(1-18)	url[snort] BLEEDING-EDGE P2P BitTorrent peer sync	2007-03-30 12:27:19			TCP
#3-(1-68)	url[snort] BLEEDING-EDGE P2P BitTorrent peer sync	2007-03-30 12:27:21			TCP
#4-(1-79)	url[snort] BLEEDING-EDGE P2P BitTorrent peer sync	2007-03-30 12:27:21			TCP
#5-(1-88)	url[snort] BLEEDING-EDGE P2P BitTorrent peer sync	2007-03-30 12:27:22			TCP
#6-(1-132)	url[snort] BLEEDING-EDGE P2P BitTorrent peer sync	2007-03-30 12:27:23			TCP
#7-(1-133)	url[snort] BLEEDING-EDGE P2P BitTorrent peer sync	2007-03-30 12:27:23			TCP
#8-(1-135)	url[snort] BLEEDING-EDGE P2P BitTorrent peer sync	2007-03-30 12:27:23			TCP
#9-(1-150)	url[snort] BLEEDING-EDGE P2P BitTorrent peer sync	2007-03-30 12:27:24			TCP
#10-(1-164)	url[snort] BLEEDING-EDGE P2P BitTorrent peer sync	2007-03-30 12:27:25			TCP
#11-(1-194)	url[snort] BLEEDING-EDGE P2P BitTorrent peer sync	2007-03-30 12:27:25			TCP
#12-(1-197)	url[snort] BLEEDING-EDGE P2P BitTorrent peer sync	2007-03-30 12:27:25			TCP
#13-(1-206)	url[snort] BLEEDING-EDGE P2P BitTorrent peer sync	2007-03-30 12:27:26			TCP
#14-(1-213)	url[snort] BLEEDING-EDGE P2P BitTorrent peer sync	2007-03-30 12:27:26			TCP
#15-(1-234)	url[snort] BLEEDING-EDGE P2P BitTorrent peer sync	2007-03-30 12:27:27			TCP
#16-(1-262)	url[snort] BLEEDING-EDGE P2P BitTorrent peer sync	2007-03-30 12:27:28			TCP
#17-(1-264)	url[snort] BLEEDING-EDGE P2P BitTorrent peer sync	2007-03-30 12:27:28			TCP
#18-(1-281)	url[snort] BLEEDING-EDGE P2P BitTorrent peer sync	2007-03-30 12:27:28			TCP
#19-(1-283)	url[snort] BLEEDING-EDGE P2P BitTorrent peer sync	2007-03-30 12:27:28			TCP
#20-(1-287)	url[snort] BLEEDING-EDGE P2P BitTorrent peer sync	2007-03-30 12:27:29			TCP
#21-(1-314)	url[snort] BLEEDING-EDGE P2P BitTorrent peer sync	2007-03-30 12:27:30			TCP
#22-(1-319)	url[snort] BLEEDING-EDGE P2P BitTorrent peer sync	2007-03-30 12:27:30			TCP
#23-(1-334)	url[snort] BLEEDING-EDGE P2P BitTorrent peer sync	2007-03-30 12:27:30			TCP
#24-(1-341)	url[snort] BLEEDING-EDGE P2P BitTorrent peer sync	2007-03-30 12:27:31			TCP
#25-(1-346)	url[snort] BLEEDING-EDGE P2P BitTorrent peer sync	2007-03-30 12:27:31			TCP
#26-(1-355)	url[snort] BLEEDING-EDGE P2P BitTorrent peer sync	2007-03-30 12:27:31			TCP
#27-(1-361)	url[snort] BLEEDING-EDGE P2P BitTorrent peer sync	2007-03-30 12:27:31			TCP
#28-(1-369)	url[snort] BLEEDING-EDGE P2P BitTorrent peer sync	2007-03-30 12:27:32			TCP
#29-(1-399)	url[snort] BLEEDING-EDGE P2P BitTorrent peer sync	2007-03-30 12:27:33			TCP
#30-(1-400)	url[snort] BLEEDING-EDGE P2P BitTorrent peer sync	2007-03-30 12:27:33			TCP
#31-(1-403)	url[snort] BLEEDING-EDGE P2P BitTorrent peer sync	2007-03-30 12:27:33			TCP

Payload Criteria	*any*

Added 239 alert(s) to the Alert cache

Alert #1

[First] >> Next #1-(1-6)

Meta

ID #	Time	Triggered Signature
1 - 1	2007-03-30 12:27:19	url[snort] BLEEDING-EDGE P2P BitTorrent peer sync

Sensor	name	interface	filter
		eth1	*none*

Alert Group	*none*

IP

source addr	dest addr	Ver	Hdr Len	TOS	length	ID	flags	offset	TTL	chksum
		4	5	0	66	32668	0	0	124	558

Options	*none*

TCP

source port	dest port	R 1	R 0	U R G	A C K	P S H	R S T	S Y N	F I N	seq #	ack	offset	res	window	urp	chksum
1177	56065				X	X				2835646537	2390715498	5	0	17520	0	52329

Options	*none*

Payload

```
 length = 26

000 : 00 00 00 0D 06 00 00 00 06 00 02 00 00 00 02 00   ................
010 : 00 00 00 00 05 04 00 00 01 09                     ..........
```

[First] >> Next #1-(1-6)

Action

{ action } Selected