

3ème année

Sécurité des Systèmes Informatiques

SUPAERO

Rodolphe Ortalo

RSSI - CARSAT Midi-Pyrénées

rodolphe.ortalo@free.fr

(rodolphe.ortalo@carsat-mp.fr)

<http://rodolphe.ortalo.free.fr/ssi.html>

Plan (2/2)

- Protection utilisées dans la pratique
 - Protection réseau et *firewall*
 - Systèmes d'authentification
 - Chiffrement de flux et VPN
- Digressions (RàZ, OpenBSD, 1984)
- Surveiller, analyser et gérer
 - Détection d'intrusion
 - Audit, tests d'intrusion
 - **Administration, exploitation et suivi de la sécurité**
 - Observation et surveillance
- Protection des applications usuelles

Administration

- Configuration cohérente de nombreux éléments
- Correctifs (automatiques)
- Mise à jours (TFTP, etc.)
- Prise en main distante
 - SSH
 - VNC, Patrol, etc.
- Déport des traces (syslog)

Organisation (Fonctions)

- Administration système
 - Monde Unix
 - Monde Windows
- Administration BD
- Administrateurs applications
- Administration réseau
 - Commutation (LAN)
 - Routage (WAN)
- *Administration sécurité*
- Administration services d'infrastructure
 - DHCP, Active Directory
 - DNS
 - Sauvegardes
- Gestion des postes de travail
 - Configurations types, fabrication
 - Mise à disposition
 - Dépannage, incidents

Des éléments différents

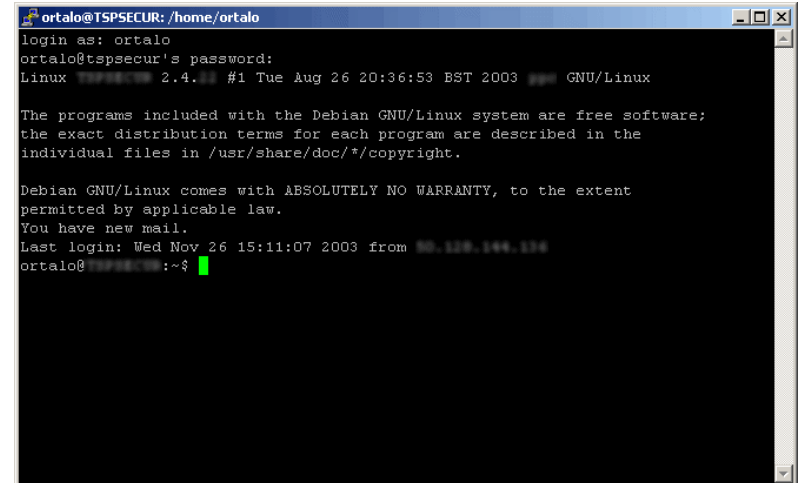
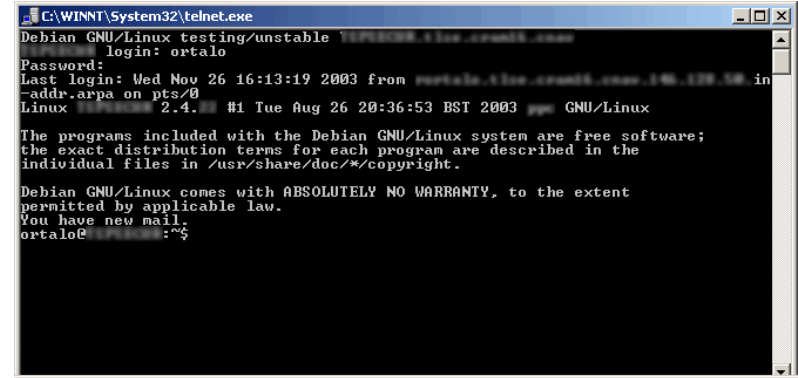
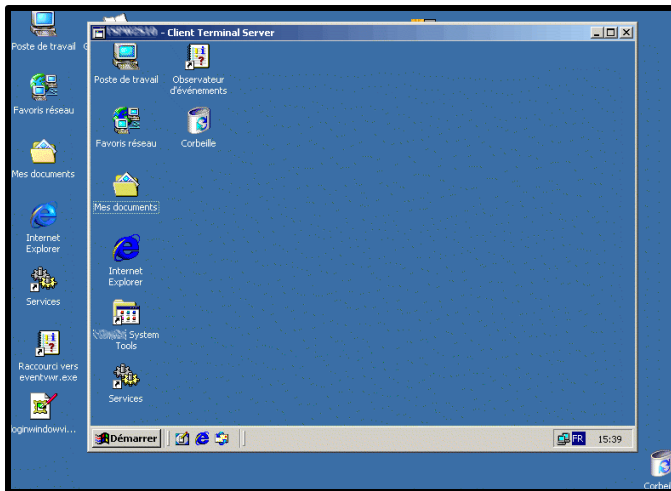
- Serveurs
 - UNIX
 - Solaris
 - Linux
 - RedHat
 - Suse
 - Debian
 - AIX
 - Windows
 - Novell
- Baies de disques
- Routeurs
- *Switches*
- PC Windows
- Macintosh
- Robots (sauvegardes)
- Imprimantes
- Boîtiers caches
- Boîtiers *firewall*
- Éléments logiciels
 - Antivirus
 - SGBD
 - ...
- IDS

Correctifs et mises à jours

- Contraintes : ne pas perturber le fonctionnement normal
- Réagir (notamment à des alertes de sécurité)
- Faciliter les déploiements
 - *patches*
 - *Windows Update, SMS*
 - Lien avec les autres éléments du poste de travail ou des serveurs

Prise en main à distance

- Unix
 - Telnet, RSH *versus* SSH
- HTTP et HTTPS
- Windows
 - *Terminal Server*
 - VNC & co.



Systemes embarqués

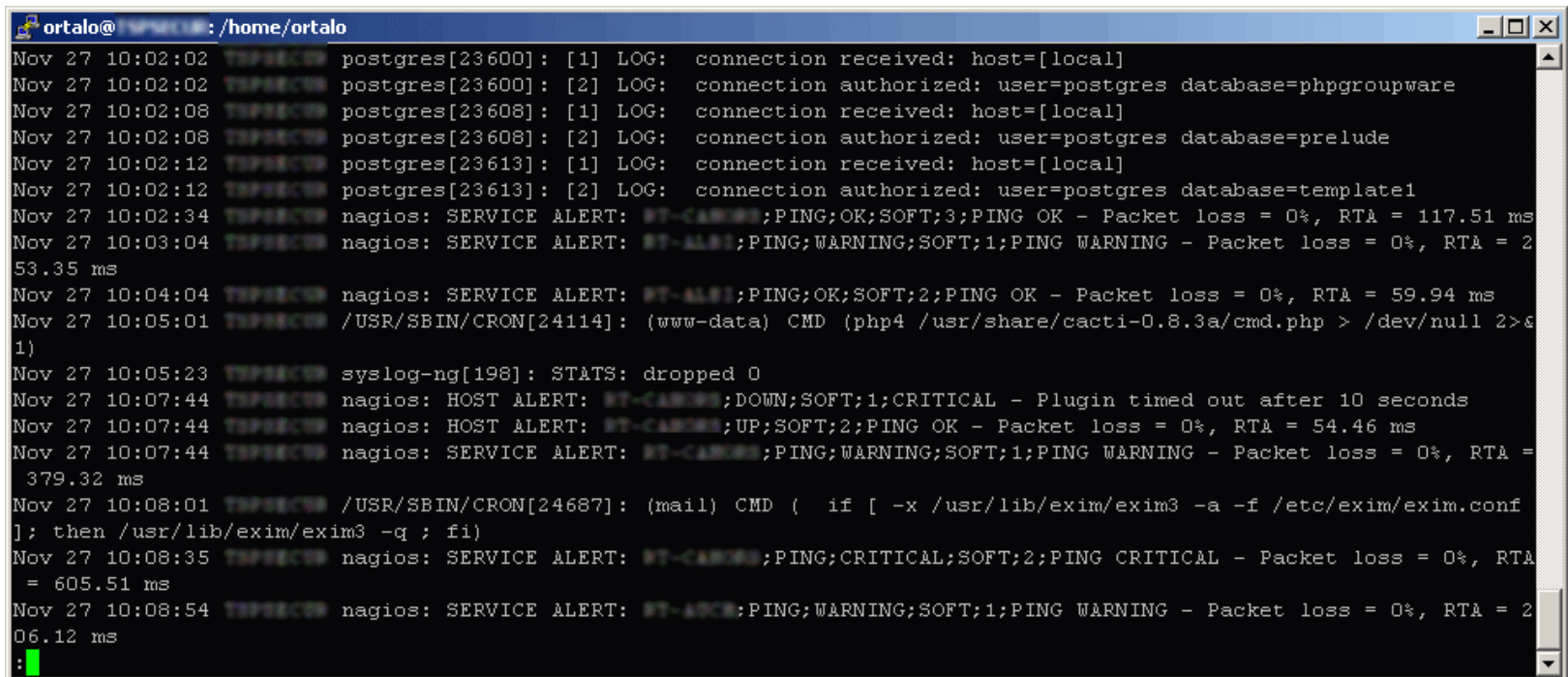
- Il s'agit souvent des équipements associés à *l'infrastructure réseau* (LAN)
- TFTP est largement répandu
 - Mise à jour des OS embarqués (*switch* Cisco, PIX)
 - Sauvegarde des configurations
- HTTP et HTTPS également (IHM)
- SNMP est supporté de manière hétérogène
- SSH apparaît sur les équipements réseau
- Équipements personnels ou PME, et ...

Plan (2/2)

- Protection utilisées dans la pratique
 - Protection réseau et *firewall*
 - Systèmes d'authentification
 - Chiffrement de flux et VPN
- Digressions (RàZ, OpenBSD, 1984)
- Surveiller, analyser et gérer
 - Détection d'intrusion
 - Audit, tests d'intrusion
 - Administration, exploitation et suivi de la sécurité
 - **Observation et surveillance**
- Protection des applications usuelles

Centralisation des traces

- Solutions propriétaires
- Syslog
- CNIL



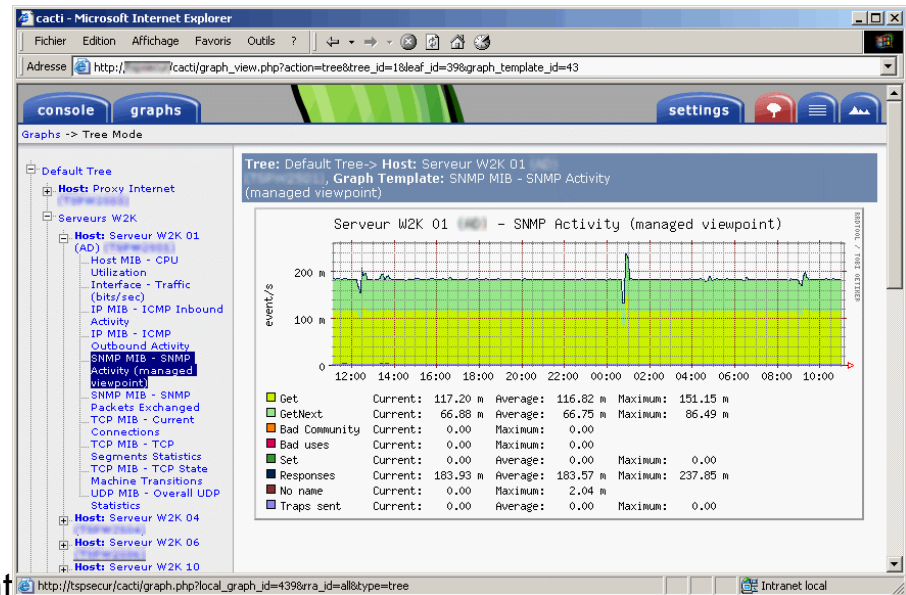
```
ortalo@ortalo: /home/ortalo
Nov 27 10:02:02 postgres[23600]: [1] LOG: connection received: host=[local]
Nov 27 10:02:02 postgres[23600]: [2] LOG: connection authorized: user=postgres database=phpgroupware
Nov 27 10:02:08 postgres[23608]: [1] LOG: connection received: host=[local]
Nov 27 10:02:08 postgres[23608]: [2] LOG: connection authorized: user=postgres database=prelude
Nov 27 10:02:12 postgres[23613]: [1] LOG: connection received: host=[local]
Nov 27 10:02:12 postgres[23613]: [2] LOG: connection authorized: user=postgres database=template1
Nov 27 10:02:34 nagios: SERVICE ALERT: BT-CARIBBE;PING;OK;SOFT;3;PING OK - Packet loss = 0%, RTA = 117.51 ms
Nov 27 10:03:04 nagios: SERVICE ALERT: BT-ALBA;PING;WARNING;SOFT;1;PING WARNING - Packet loss = 0%, RTA = 253.35 ms
Nov 27 10:04:04 nagios: SERVICE ALERT: BT-ALBA;PING;OK;SOFT;2;PING OK - Packet loss = 0%, RTA = 59.94 ms
Nov 27 10:05:01 /USR/SBIN/CRON[24114]: (www-data) CMD (php4 /usr/share/cacti-0.8.3a/cmd.php > /dev/null 2>& 1)
Nov 27 10:05:23 syslog-ng[198]: STATS: dropped 0
Nov 27 10:07:44 nagios: HOST ALERT: BT-CARIBBE;DOWN;SOFT;1;CRITICAL - Plugin timed out after 10 seconds
Nov 27 10:07:44 nagios: HOST ALERT: BT-CARIBBE;UP;SOFT;2;PING OK - Packet loss = 0%, RTA = 54.46 ms
Nov 27 10:07:44 nagios: SERVICE ALERT: BT-CARIBBE;PING;WARNING;SOFT;1;PING WARNING - Packet loss = 0%, RTA = 379.32 ms
Nov 27 10:08:01 /USR/SBIN/CRON[24687]: (mail) CMD ( if [ -x /usr/lib/exim/exim3 -a -f /etc/exim/exim.conf ]; then /usr/lib/exim/exim3 -q ; fi)
Nov 27 10:08:35 nagios: SERVICE ALERT: BT-CARIBBE;PING;CRITICAL;SOFT;2;PING CRITICAL - Packet loss = 0%, RTA = 605.51 ms
Nov 27 10:08:54 nagios: SERVICE ALERT: BT-ALBA;PING;WARNING;SOFT;1;PING WARNING - Packet loss = 0%, RTA = 206.12 ms
:
```

Observation et Surveillance

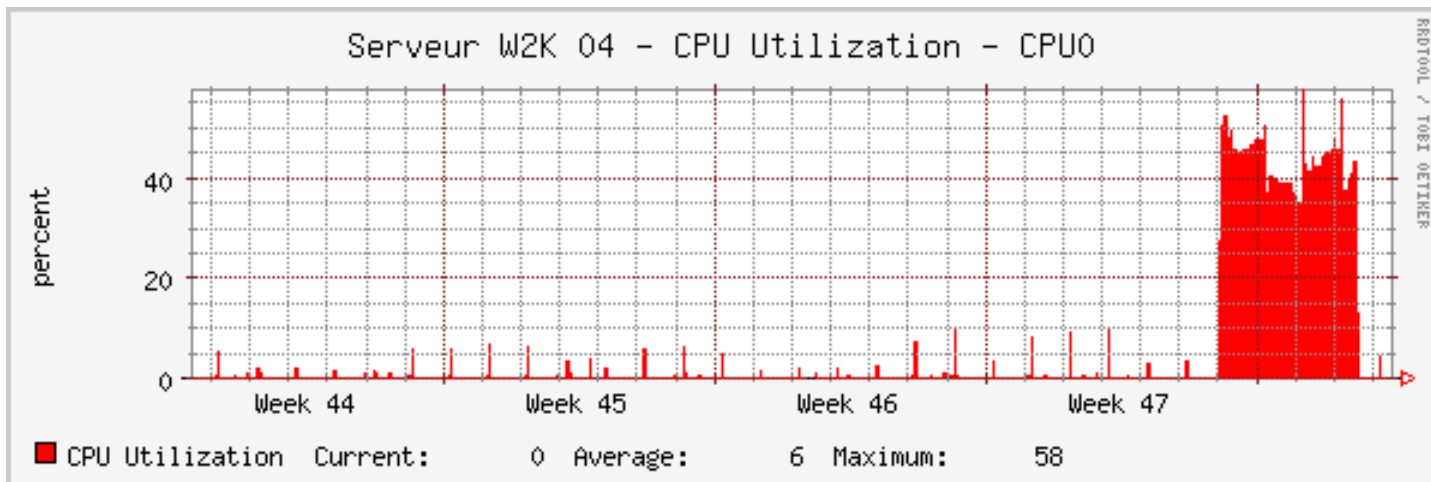
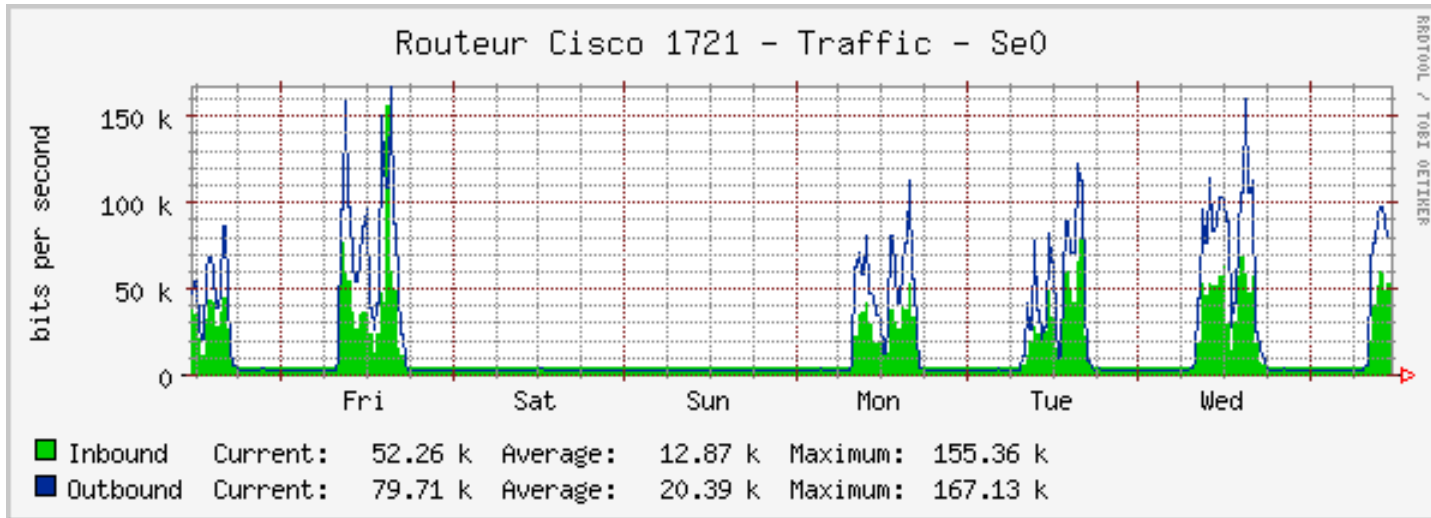
- *Monitoring* réseau
 - Équipements de sécurité
 - Autres équipements (réseaux et QoS par exemple)
- Surveillance système
- Évènements anormaux

SNMP

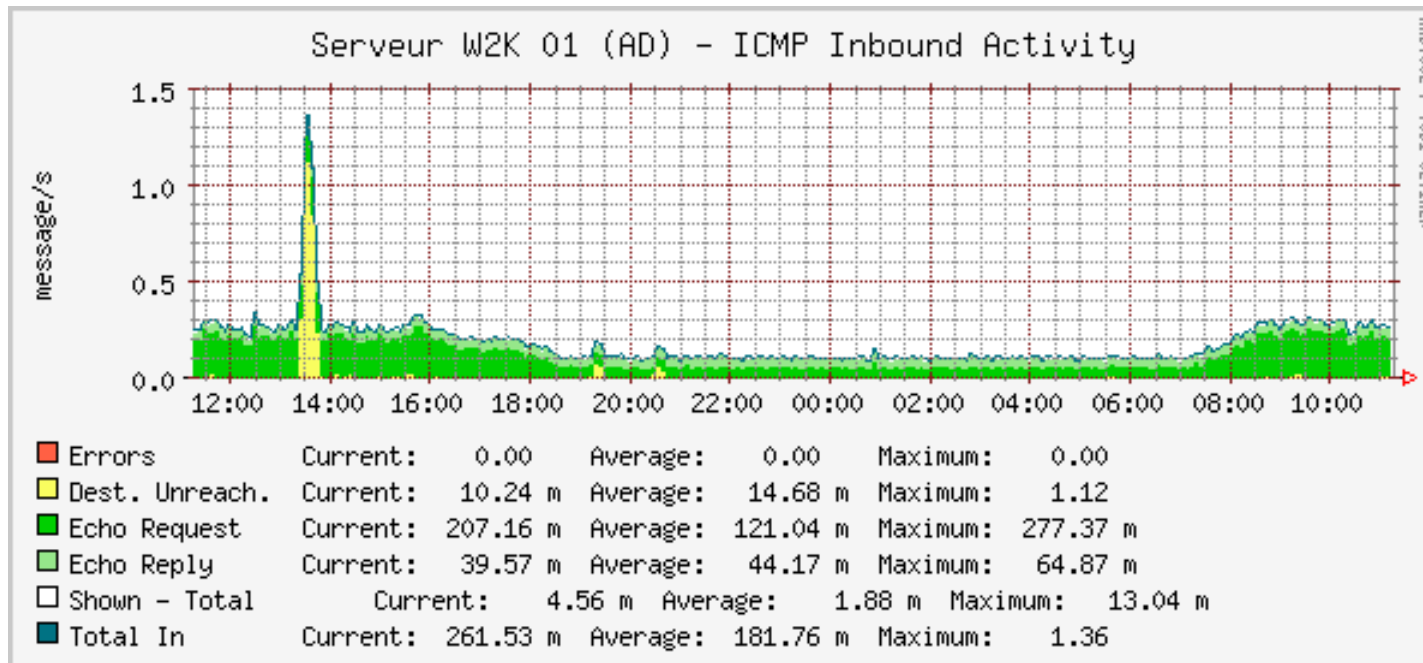
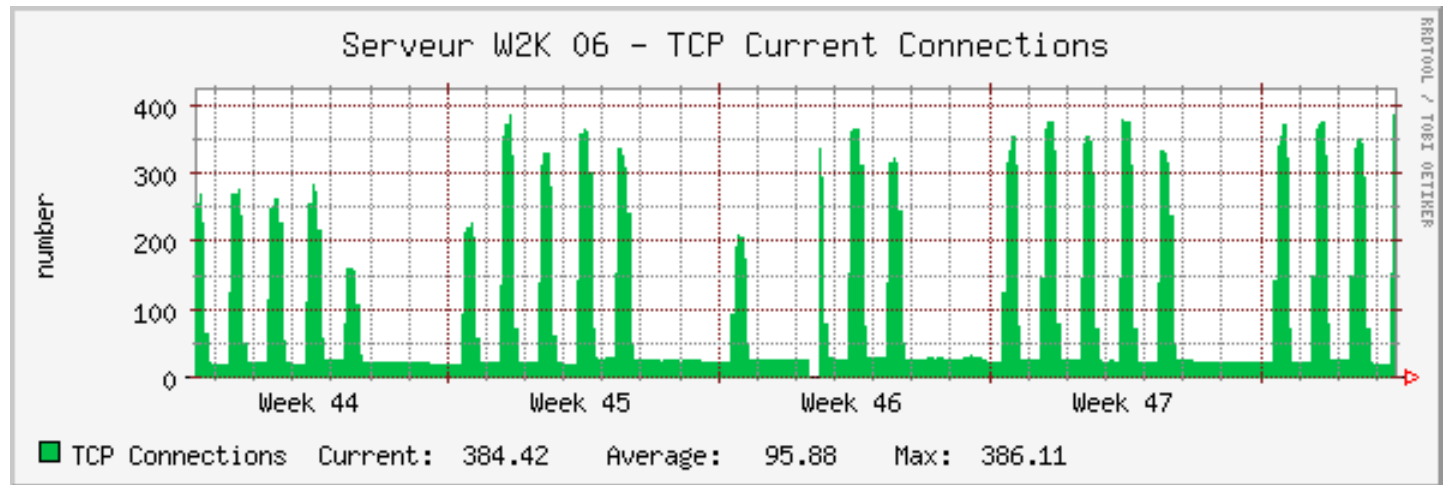
- IF-MIB, HOST-MIB, etc. (www.mibdepot.com)
- NET-SNMP, UCD-SNMP, IETF
Cisco, 3Com, Nortell, IBM, etc.
- RRDTool, MRTG, Cacti, HPoV, Tivoli, etc.
- Requêtes (sur UDP/161 et UDP/162):
 - Get
 - GetNext
 - Set
 - Response
 - Trap



SNMP (Exemples)



SNMP (Exemples)



Surveillance système (exemple)

The screenshot displays the Nagios web interface. The browser window title is "Nagios - Microsoft Internet Explorer" and the address bar shows "http://tspsecur/nagios/". The main content area is a table of monitored services. The left sidebar contains navigation menus for General, Monitoring, Reporting, and Configuration.

Service	Plugin	Status	Output	Last Check	Next Check	Latency	Current State	Service Description
192.168.1.1	PING	OK	PING OK - Packet loss = 0%, RTA = 88.49 ms	2003-11-27 11:40:47	0d 3h 24m 51s	1/3	OK	
192.168.1.1	DNS	OK	DNS ok - 1 seconds response time, Address(es) is/are 216.109.118.64	2003-11-27 11:40:47	2d 4h 20m 21s	1/3	OK	
192.168.1.1	/dev/sda8 Free Space	OK	DISK OK [423189 kB (94%) free on /dev/sda2]	2003-11-27 11:41:20	72d 2h 22m 37s	1/3	OK	
192.168.1.1	HTTP	OK	HTTP ok: HTTP/1.1 200 OK - 0.020 second response time	2003-11-27 11:43:15	72d 2h 23m 36s	1/3	OK	
192.168.1.1	HTTPS	OK	HTTP ok: HTTP/1.1 200 OK - 0.071 second response time	2003-11-27 11:43:26	52d 2h 4m 34s	1/3	OK	
192.168.1.1	HTTPS - Certificate	OK	Certificate will expire on 10/05/2004 09:0.	2003-11-27 07:22:10	52d 1h 42m 42s	1/2	OK	
192.168.1.1	MySQL - local	OK	Uptime: 1292697 Threads: 2 Questions: 9382279 Slow queries: 2 Opens: 187 Flush tables: 1 Open tables: 64 Queries per second avg: 7.258	2003-11-27 11:43:15	72d 2h 25m 26s	1/3	OK	
192.168.1.1	NTP	OK	NTP OK: Offset -0.000013 secs, jitter 0.113 msec, peer is stratum 1	2003-11-27 11:44:28	0d 6h 56m 11s	1/3	OK	
192.168.1.1	OpenSSH	OK	SSH OK - OpenSSH_3.6.1 Debian 3.6.1-8 (protocol 2.0)	2003-11-27 11:43:13	72d 2h 25m 25s	1/3	OK	
192.168.1.1	PostgreSQL - local	OK	PGSQL: ok - database template1 (0 sec.)	2003-11-27 11:44:58	17d 10h 31m 25s	1/3	OK	
192.168.1.1	WebMIN	OK	HTTP ok: HTTP/1.0 200 Document follows - 1.649 second response time	2003-11-27 11:41:20	52d 1h 58m 32s	1/3	OK	
192.168.1.1	WebMIN - Certificate	OK	Certificate will expire on 09/03/2008 09:5.	2003-11-27 07:28:43	52d 2h 4m 9s	1/2	OK	
192.168.1.1	DNS	OK	DNS ok - 1 seconds response time, Address(es) is/are 216.109.118.68	2003-11-27 11:45:01	2d 6h 0m 41s	1/3	OK	
192.168.1.1	PROXY	OK	Process w3proxy.exe exists (PID=5620).	2003-11-27 11:43:28	8d 22h 10m 9s	1/3	OK	
192.168.1.1	SPOOLER	OK	Process spoolsv.exe exists (PID=536).	2003-11-27 11:43:28	7d 12h 50m 59s	1/3	OK	
192.168.1.1	SPOOLER	OK	Process spoolsv.exe exists (PID=3396).	2003-11-27 11:43:27	44d 23h 26m 51s	1/3	OK	
192.168.1.1	DNS	OK	DNS ok - 0 seconds response time, Address(es) is/are 216.109.118.66	2003-11-27 11:44:06	1d 21h 51m 40s	1/3	OK	
192.168.1.1	NTP	OK	NTP OK: Offset -0.000403 secs, jitter 10.010 msec, peer is stratum 0	2003-11-27 11:41:23	3d 10h 29m 25s	1/3	OK	
192.168.1.1	SMTP	OK	SMTP OK - 0 second response time	2003-11-27 11:43:17	5d 21h 32m 55s	1/3	OK	
192.168.1.1	PING	OK	PING OK - Packet loss = 0%, RTA = 47.64 ms	2003-11-27 11:41:02	0d 2h 34m 31s	1/3	OK	

Plan (2/2)

- Protection utilisées dans la pratique
 - Protection réseau et *firewall*
 - Systèmes d'authentification
 - Chiffrement de flux et VPN
- Digressions (RàZ, OpenBSD, 1984)
- Surveiller, analyser et gérer
 - Détection d'intrusion
 - Audit, tests d'intrusion
 - Administration, exploitation et suivi de la sécurité
 - Observation et surveillance
- **Protection des applications usuelles**

Plan (détailé)

- **Protection des applications (usuelles)**
 - Poste de travail : antivirus
 - *Messagerie, Flux HTTP (entrant) : antivirus*
 - Serveur HTTP
 - Flux HTTP (sortant) : filtrage d'URL
 - *Services Internet : e-* et HTTPS*
 - *Services Internet : e-* Pro (Portal, WebSphere, SOAP & co.)*
 - Signature et messagerie (S/MIME, OpenPGP)
 - DNS (et DNSSEC)
 - *Routage IP (OSPF, RIP, BGP)*
 - Infrastructure SSI : PKI, X.509, LDAP, etc.

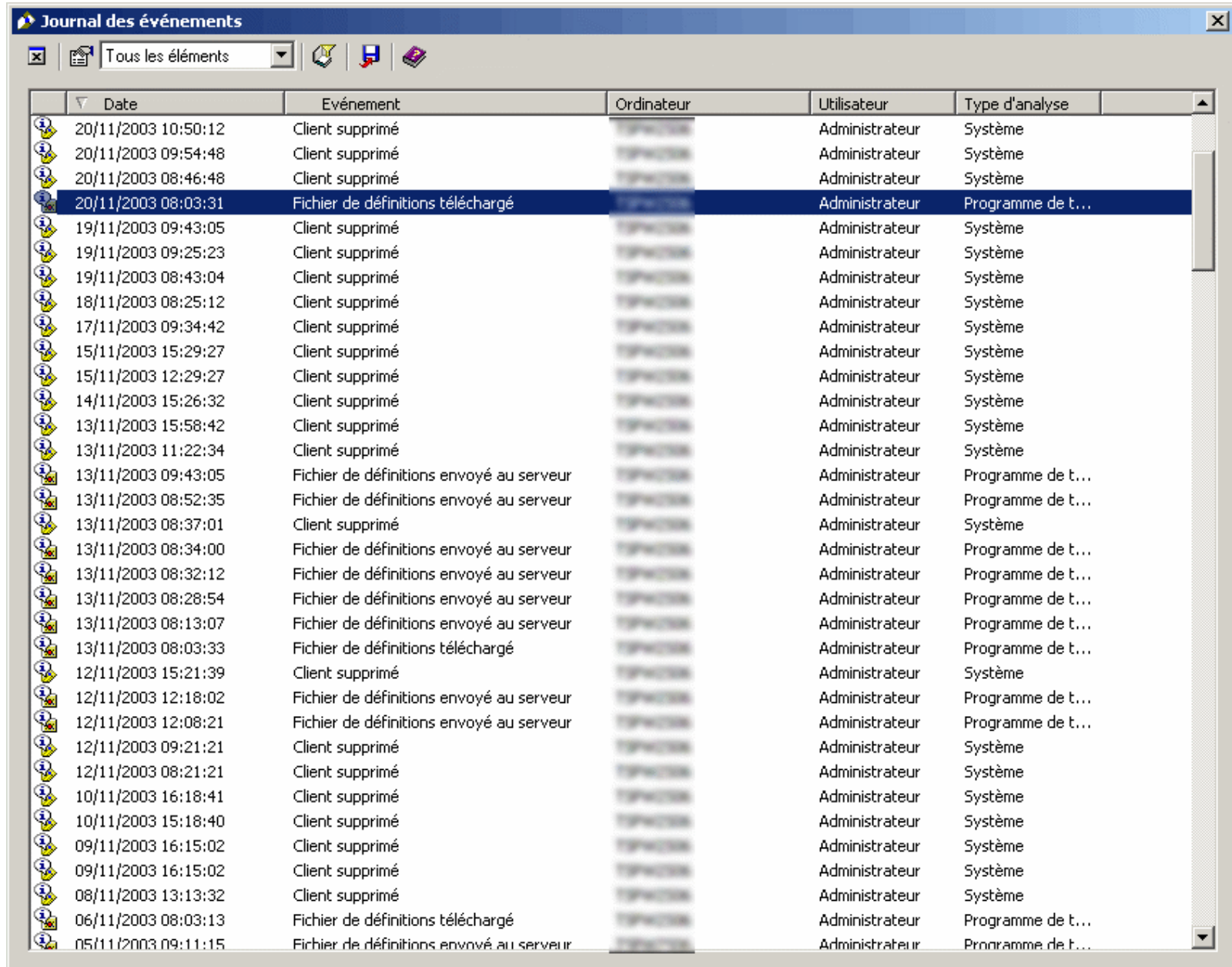
Antivirus sur le poste

The image displays the Symantec AntiVirus Corporate Edition interface. The main window is titled 'Symantec AntiVirus Corporate Edition' and features a menu bar with 'Fichier', 'Edition', 'Afficher', 'Analyser', 'Configurer', and 'Historiques'. The left sidebar contains a tree view with options like 'Afficher', 'Analyser', 'Configurer', 'Historiques', 'Analyses au démarrage', 'Analyses personnalisées', 'Analyses programmées', and 'Obtention de l'Aide'. The main content area shows a welcome message and a list of tasks under the 'Afficher' menu, including 'Statistiques d'analyse en temps réel du système de fichiers', 'Analyses programmées', 'Quarantaine', 'Eléments sauvegardés', and 'Eléments réparés'. A 'Liste des virus' dialog box is open in the foreground, showing a table of detected viruses.

Nom du virus	Cibles
SillyC.190	Programmes
SillyC.190.B	Programmes
SillyC.190.B (2)	Programmes
SillyC.192	Programmes
SillyC.192.b	Programmes
SillyC.193.B	Programmes
SillyC.193.C	Programmes
SillyC.195.b	Programmes
SillyC.195.C	Programmes
SillyC.197	Programmes
SillyC.197.c	Programmes
SillyC.197.d	Programmes
SillyC.199	Programmes
SillyC.200	Programmes

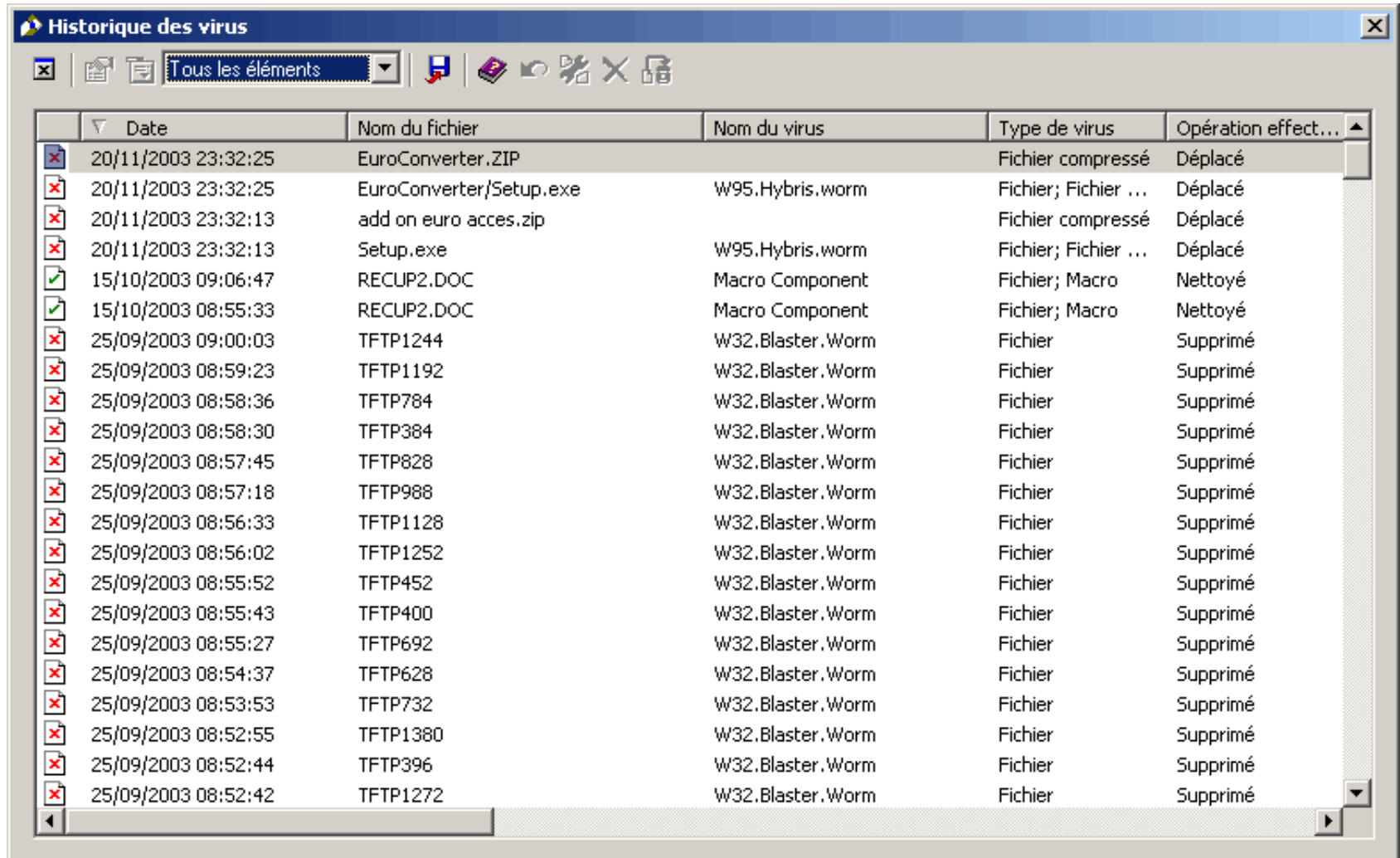
65530 virus affichés
Date de définitions : 12/11/2003

Console Antivirus (2)



Date	Événement	Ordinateur	Utilisateur	Type d'analyse
20/11/2003 10:50:12	Client supprimé		Administrateur	Système
20/11/2003 09:54:48	Client supprimé		Administrateur	Système
20/11/2003 08:46:48	Client supprimé		Administrateur	Système
20/11/2003 08:03:31	Fichier de définitions téléchargé	Ordinateur	Administrateur	Programme de t...
19/11/2003 09:43:05	Client supprimé		Administrateur	Système
19/11/2003 09:25:23	Client supprimé		Administrateur	Système
19/11/2003 08:43:04	Client supprimé		Administrateur	Système
18/11/2003 08:25:12	Client supprimé		Administrateur	Système
17/11/2003 09:34:42	Client supprimé		Administrateur	Système
15/11/2003 15:29:27	Client supprimé		Administrateur	Système
15/11/2003 12:29:27	Client supprimé		Administrateur	Système
14/11/2003 15:26:32	Client supprimé		Administrateur	Système
13/11/2003 15:58:42	Client supprimé		Administrateur	Système
13/11/2003 11:22:34	Client supprimé		Administrateur	Système
13/11/2003 09:43:05	Fichier de définitions envoyé au serveur		Administrateur	Programme de t...
13/11/2003 08:52:35	Fichier de définitions envoyé au serveur		Administrateur	Programme de t...
13/11/2003 08:37:01	Client supprimé		Administrateur	Système
13/11/2003 08:34:00	Fichier de définitions envoyé au serveur		Administrateur	Programme de t...
13/11/2003 08:32:12	Fichier de définitions envoyé au serveur		Administrateur	Programme de t...
13/11/2003 08:28:54	Fichier de définitions envoyé au serveur		Administrateur	Programme de t...
13/11/2003 08:13:07	Fichier de définitions envoyé au serveur		Administrateur	Programme de t...
13/11/2003 08:03:33	Fichier de définitions téléchargé		Administrateur	Programme de t...
12/11/2003 15:21:39	Client supprimé		Administrateur	Système
12/11/2003 12:18:02	Fichier de définitions envoyé au serveur		Administrateur	Programme de t...
12/11/2003 12:08:21	Fichier de définitions envoyé au serveur		Administrateur	Programme de t...
12/11/2003 09:21:21	Client supprimé		Administrateur	Système
12/11/2003 08:21:21	Client supprimé		Administrateur	Système
10/11/2003 16:18:41	Client supprimé		Administrateur	Système
10/11/2003 15:18:40	Client supprimé		Administrateur	Système
09/11/2003 16:15:02	Client supprimé		Administrateur	Système
09/11/2003 16:15:02	Client supprimé		Administrateur	Système
08/11/2003 13:13:32	Client supprimé		Administrateur	Système
06/11/2003 08:03:13	Fichier de définitions téléchargé		Administrateur	Programme de t...
05/11/2003 09:11:15	Fichier de définitions envoyé au serveur		Administrateur	Programme de t...

Console Antivirus (3)



Date	Nom du fichier	Nom du virus	Type de virus	Opération effectuée
20/11/2003 23:32:25	EuroConverter.ZIP		Fichier compressé	Déplacé
20/11/2003 23:32:25	EuroConverter/Setup.exe	W95.Hybris.worm	Fichier; Fichier ...	Déplacé
20/11/2003 23:32:13	add on euro acces.zip		Fichier compressé	Déplacé
20/11/2003 23:32:13	Setup.exe	W95.Hybris.worm	Fichier; Fichier ...	Déplacé
15/10/2003 09:06:47	RECUP2.DOC	Macro Component	Fichier; Macro	Nettoyé
15/10/2003 08:55:33	RECUP2.DOC	Macro Component	Fichier; Macro	Nettoyé
25/09/2003 09:00:03	TFTP1244	W32.Blaster.Worm	Fichier	Supprimé
25/09/2003 08:59:23	TFTP1192	W32.Blaster.Worm	Fichier	Supprimé
25/09/2003 08:58:36	TFTP784	W32.Blaster.Worm	Fichier	Supprimé
25/09/2003 08:58:30	TFTP384	W32.Blaster.Worm	Fichier	Supprimé
25/09/2003 08:57:45	TFTP828	W32.Blaster.Worm	Fichier	Supprimé
25/09/2003 08:57:18	TFTP988	W32.Blaster.Worm	Fichier	Supprimé
25/09/2003 08:56:33	TFTP1128	W32.Blaster.Worm	Fichier	Supprimé
25/09/2003 08:56:02	TFTP1252	W32.Blaster.Worm	Fichier	Supprimé
25/09/2003 08:55:52	TFTP452	W32.Blaster.Worm	Fichier	Supprimé
25/09/2003 08:55:43	TFTP400	W32.Blaster.Worm	Fichier	Supprimé
25/09/2003 08:55:27	TFTP692	W32.Blaster.Worm	Fichier	Supprimé
25/09/2003 08:54:37	TFTP628	W32.Blaster.Worm	Fichier	Supprimé
25/09/2003 08:53:53	TFTP732	W32.Blaster.Worm	Fichier	Supprimé
25/09/2003 08:52:55	TFTP1380	W32.Blaster.Worm	Fichier	Supprimé
25/09/2003 08:52:44	TFTP396	W32.Blaster.Worm	Fichier	Supprimé
25/09/2003 08:52:42	TFTP1272	W32.Blaster.Worm	Fichier	Supprimé

Serveur Web

- Serveur HTTP et serveur HTTPS
- Sélection des utilisateurs
 - Plages d'adresses
 - Certificats
- Sélection des destinations
 - Chemin d'accès
 - Type d'extension
- Maîtrise des extensions dynamiques
- Contrôle du processus serveur
 - Confinement
 - Lien avec le système de fichiers

Apache 1.3 (1)

- Configuration réseau fondamentale

```
#Listen 3000
```

[Debian 3.1]

```
#Listen 12.34.56.78:80
```

```
#BindAddress *
```

```
Port 80 (?)
```

- Extensions (modules)

```
LoadModule cgi_module /usr/lib/apache/1.3/mod_cgi.so
```

```
# LoadModule asis_module /usr/lib/apache/1.3/mod_asis.so
```

```
LoadModule alias_module /usr/lib/apache/1.3/mod_alias.so
```

```
LoadModule access_module
```

```
    /usr/lib/apache/1.3/mod_access.so
```

```
LoadModule php4_module /usr/lib/apache/1.3/libphp4.so
```

- Processus

```
User www-data
```

```
Group www-data
```

Apache 1.3 (2)

- Configuration conditionnelle
 <IfModule mod_status.c>
 ExtendedStatus On
 </IfModule>
- Configuration modulaire
 Include /etc/phpmyadmin/apache.conf
 Include /etc/phpgroupware/apache.conf
- Directives de contexte
 <Directory> et **<DirectoryMatch>**
 <Files> et **<FilesMatch>**
 <Location> et **<LocationMatch>**
 <VirtualHost>

Apache 1.3 (3)

- Contrôle des chemins d'accès (fichiers)

```
<Directory />
  Options
  SymLinksIfOwnerMatch
  AllowOverride None
</Directory>
...
<Directory /var/www/>
  Options Indexes Includes
  FollowSymLinks MultiViews
  AllowOverride None
  Order allow,deny
  Allow from all
</Directory>
...
```

```
<Directory /home/*/public_html>
  AllowOverride FileInfo
  AuthConfig Limit
  Options MultiViews Indexes
  SymLinksIfOwnerMatch
  IncludesNoExec
  <Limit GET POST OPTIONS
  PROPFIND>
    Order allow,deny
    Allow from all
  </Limit>
  <Limit PUT DELETE PATCH
  PROPPATCH MKCOL COPY
  MOVE LOCK UNLOCK>
    Order deny,allow
    Deny from all
  </Limit>
</Directory>
```

Apache 1.3 (4)

- Contrôle des noms de fichiers

```
<Files ~ "^\.ht">  
    Order allow,deny  
    Deny from all  
</Files>
```

- A vérifier

```
# If the perl module is installed,  
    this will be enabled.  
<IfModule mod_perl.c>  
    Alias /perl/ /var/www/perl/  
    <Location /perl>  
        SetHandler perl-script  
        PerlHandler  
        Apache::Registry  
        Options +ExecCGI  
    </Location>  
</IfModule>
```

Apache 1.3 (5)

- Contrôle des chemins d'accès (URL)

```
Alias /doc/ /usr/share/doc/  
<Location /doc>  
  order deny,allow  
  deny from all  
  allow from  
    127.0.0.0/255.0.0.0  
  allow from  
    AA.BB.CC.0/255.255.XX.  
    0  
  Options Indexes  
    FollowSymLinks  
    MultiViews  
</Location>  
...
```

```
# For Prelude PIWI  
Alias /piwi  
  /home/xxxx/prelude/piwi  
ScriptAlias /piwi  
  /home/xxxx/prelude/piwi  
<DirectoryMatch  
  /home/xxxx/prelude/piwi/>  
order allow,deny  
allow from all  
Options +ExecCGI  
AddHandler cgi-script .pl  
DirectoryIndex index.pl  
</DirectoryMatch>
```

Apache 1.3 (6)

- /etc/phpgroupware/apache.conf
Alias /phpgroupware /usr/share/phpgroupware
<Directory /usr/share/phpgroupware/>
Options +FollowSymLinks
AllowOverride None
order allow,deny
allow from all
DirectoryIndex index.html **index.php**
<IfModule mod_php3.c>
 php3_magic_quotes_gpc On
 php3_track_vars On
 php3_include_path **./etc/phpgroupware**
</IfModule>
<IfModule mod_php4.c>
 php_flag **magic_quotes_gpc** On
 php_flag track_vars On
 php_flag session.save_path /var/tmp/phpgroupware
 php_value include_path **./etc/phpgroupware**
</IfModule>
</Directory>
- Exemple de fichier de configuration secondaire

Apache 1.3 (7)

- *Virtual hosts*
 - # VirtualHost example:
 - # *Almost* any Apache directive may go into a VirtualHost container.
 - #
 - #<**VirtualHost** ip.address.of.host.some_domain.com>
 - # ServerAdmin webmaster@host.some_domain.com
 - # **DocumentRoot** /www/docs/host.some_domain.com
 - # **ServerName** host.some_domain.com
 - # ErrorLog logs/host.some_domain.com-error.log
 - # CustomLog logs/host.some_domain.com-access.log
common
 - #</VirtualHost>
- Consulter la documentation
- N'oubliez pas Apache-SSL

Le *proxy* Web

- Le relais le plus utilisé dans un système d'information
- Couplé à du filtrage d'URL (nécessairement)
- Liaison souhaitable avec l'authentification du poste de travail
- Fonction de cache

Squid – Règles de contrôle d'accès

www.squid-cache.org

- Deux composants
 - Éléments (*ACL elements*)
 - Règles (*access lists rules*)
- Combinaison
 - `acl_type {allow|deny} acl AND acl AND ...`
 - OR `acl_type {allow|deny} acl AND acl AND ...`
 - OR ...
- Exemples (utiles)
 - `acl all src 0/0`
`http_access deny all`
 - `acl myclients src 1.2.3.0/24`
`http_access allow myclients`

Squid – ACL *elements*

Squid knows about the following types of ACL elements :

- **src**: source (client) IP addresses
- **dst**: destination (server) IP addresses
- **myip**: the local IP address of a client's connection
- **srcdomain**: source (client) domain name
- **dstdomain**: destination (server) domain name
- **srcdom_regex**: source (client) regular expression pattern matching
- **dstdom_regex**: destination (server) regular expression pattern matching
- **time**: time of day, and day of week
- **url_regex**: URL regular expression pattern matching
- **urlpath_regex**: URL-path regular expression pattern matching, leaves out the protocol and hostname
- **port**: destination (server) port number
- **myport**: local port number that client connected to
- **proto**: transfer protocol (http, ftp, etc)
- **method**: HTTP request method (get, post, etc)
- **browser**: regular expression pattern matching on the request's user-agent header
- **ident**: string matching on the user's name
- **ident_regex**: regular expression pattern matching on the user's name
- **src_as**: source (client) Autonomous System number
- **dst_as**: destination (server) Autonomous System number
- **proxy_auth**: user authentication via external processes
- **proxy_auth_regex**: user authentication via external processes
- **snmp_community**: SNMP community string matching
- **maxconn**: a limit on the maximum number of connections from a single client IP address
- **req_mime_type**: regular expression pattern matching on the request content-type header
- **arp**: Ethernet (MAC) address matching
- **rep_mime_type**: regular expression pattern matching on the reply (downloaded content) content-type header. This is only usable in the *http_reply_access* directive, not *http_access*.
- **external/**: lookup via external acl helper defined by *external_acl_type*

Note: The information here is current for version 2.5

Squid – *Access lists types*

There are a number of different access lists:

- **http_access**: Allows HTTP clients (browsers) to access the HTTP port. This is the primary access control list.
- **http_reply_access**: Allows HTTP clients (browsers) to receive the reply to their request. This further restricts permissions given by `http_access`, and is primarily intended to be used together with the `rep_mime_type` acl type for blocking different content types.
- **icp_access**: Allows neighbor caches to query your cache with ICP.
- **miss_access**: Allows certain clients to forward cache misses through your cache. This further restricts permissions given by `http_access`, and is primarily intended to be used for enforcing sibling relations by denying siblings from forwarding cache misses through your cache.
- **no_cache**: Defines responses that should not be cached.
- **redirector_access**: Controls which requests are sent through the redirector pool.
- **ident_lookup_access**: Controls which requests need an Ident lookup.
- **always_direct**: Controls which requests should always be forwarded directly to origin servers.
- **never_direct**: Controls which requests should never be forwarded directly to origin servers.
- **snmp_access**: Controls SNMP client access to the cache.
- **broken_posts**: Defines requests for which squid appends an extra CRLF after POST message bodies as required by some broken origin servers.
- **cache_peer_access**: Controls which requests can be forwarded to a given neighbor (peer).

SquidGuard (1)

www.squidguard.org

- Un redirecteur pour Squid
- Recherche efficace pour des listes de grandes tailles (>100 000 entrées)
- Définition de listes de contrôle d'accès
- Prise en compte des plages horaires
- Propose des listes noires d'URL et de sites (et un robot)

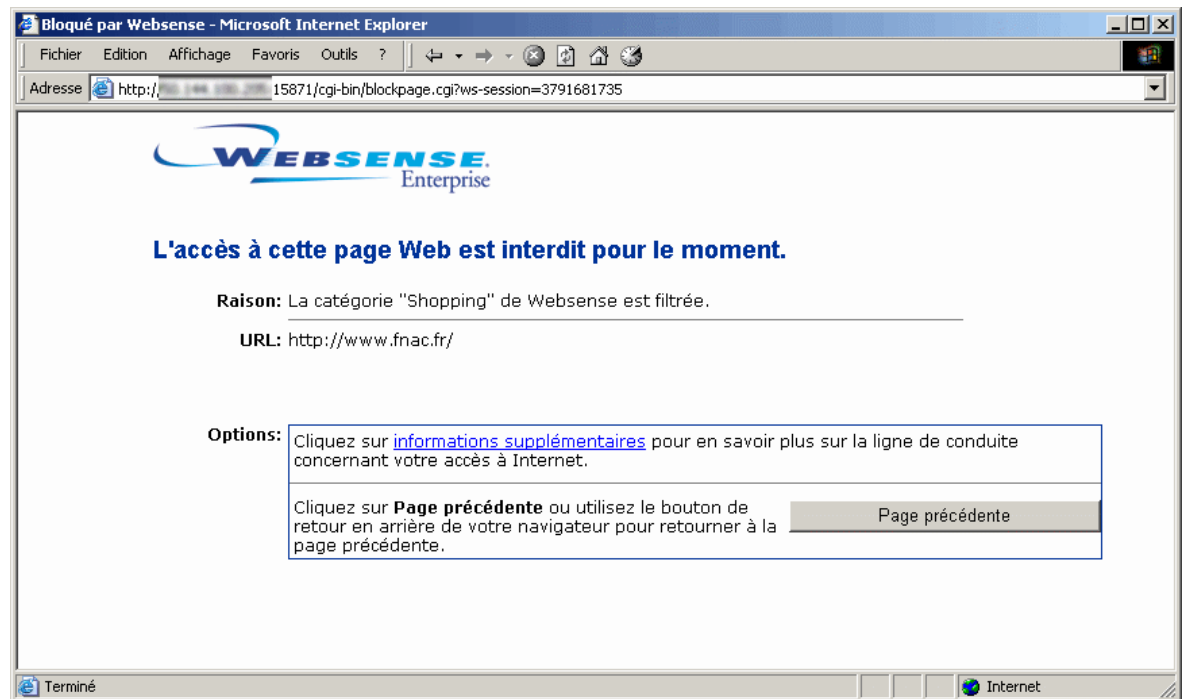
SquidGuard (2)

- Exemple:

```
logdir /usr/local/squidGuard/log
dbhome /usr/local/squidGuard/db
src grownups { ip 10.0.0.0/24 user foo bar }
src kids { ip 10.0.1.0/24 }
dest porn { domainlist porn/domains urllist porn/urls }
acl {
    grownups { pass all }
    kids { pass !porn all }
    default {
        pass none
        redirect http://info.foo.bar/cgi/blocked?clientaddr=
        %a&clientname=%n&
        clientuser=%i&clientgroup=%s&targetgroup=%t&url=%u
    }
}
```

Filtrage d'URL

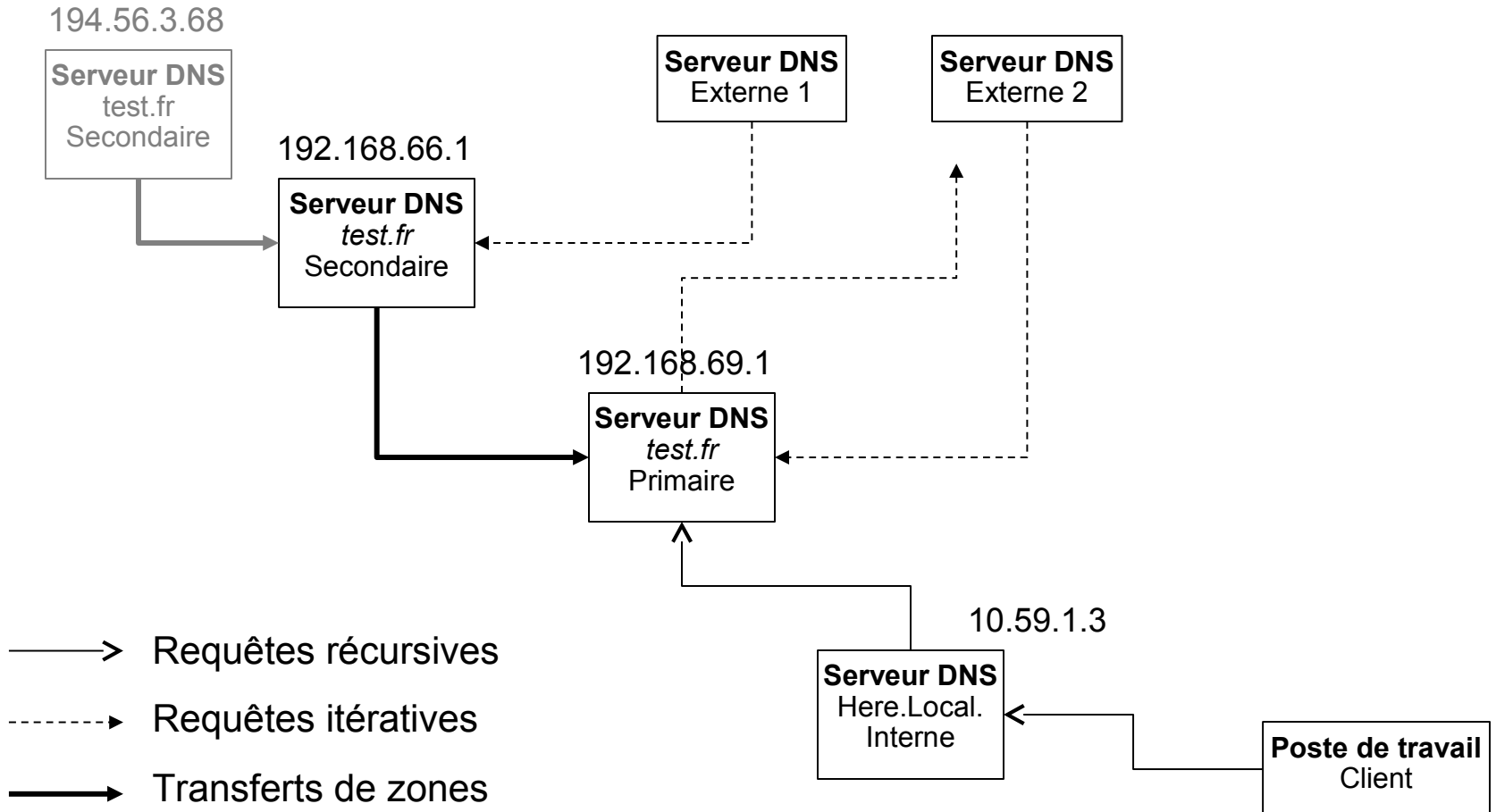
- Les offres commerciales incluent la classification des sites
- Exemple : WebSense



DNS

- Sécuriser les échanges entre les serveurs eux-mêmes
- Contrôler correctement les clients
- Émettre efficacement les requêtes
- Organiser précisément la diffusion de l'information gérée (notamment en présence de translation d'adresses)

DNS : test.fr.



DNS et BIND

- BIND 8
- BIND 9
 - Possibilités d'authentification forte
 - Échanges entre serveurs
 - Administration
 - Transferts de zone incrémentaux
 - DNSSEC

BIND 9 (1)

- Limiter les transferts de zones

```
zone "test.fr" {  
    type master;  
    file "/etc/bind/db.test.fr";  
    allow-transfer {  
        192.168.66.1;  
    };  
};
```

- Même sur un secondaire

```
zone "test.fr" {  
    type slave;  
    masters { 192.168.69.1; };  
    file "/etc/bind/bak.db.test.fr";  
    allow-transfer {  
        194.56.3.68; // or "none"  
    };  
};
```


BIND 9 (2)

- Contrôler les accès aux zones gérées
 - requêtes directes : autres serveurs
 - requêtes itératives : pour les clients finaux

```
// We allow only recursive queries from the internal nameserver  
and self
```

```
acl "ns_rzo" { 192.168.66.1; 10.59.1.3; 127.0.0.1; };
```

```
// We also allow the admin. station to do queries here directly
```

```
acl "admin" { 192.168.65.1; };
```

```
...
```

```
allow-query { any; }; // or "slaves_ns"  
allow-recursion { "ns_rzo"; "admin"; };
```

BIND 9 (2)

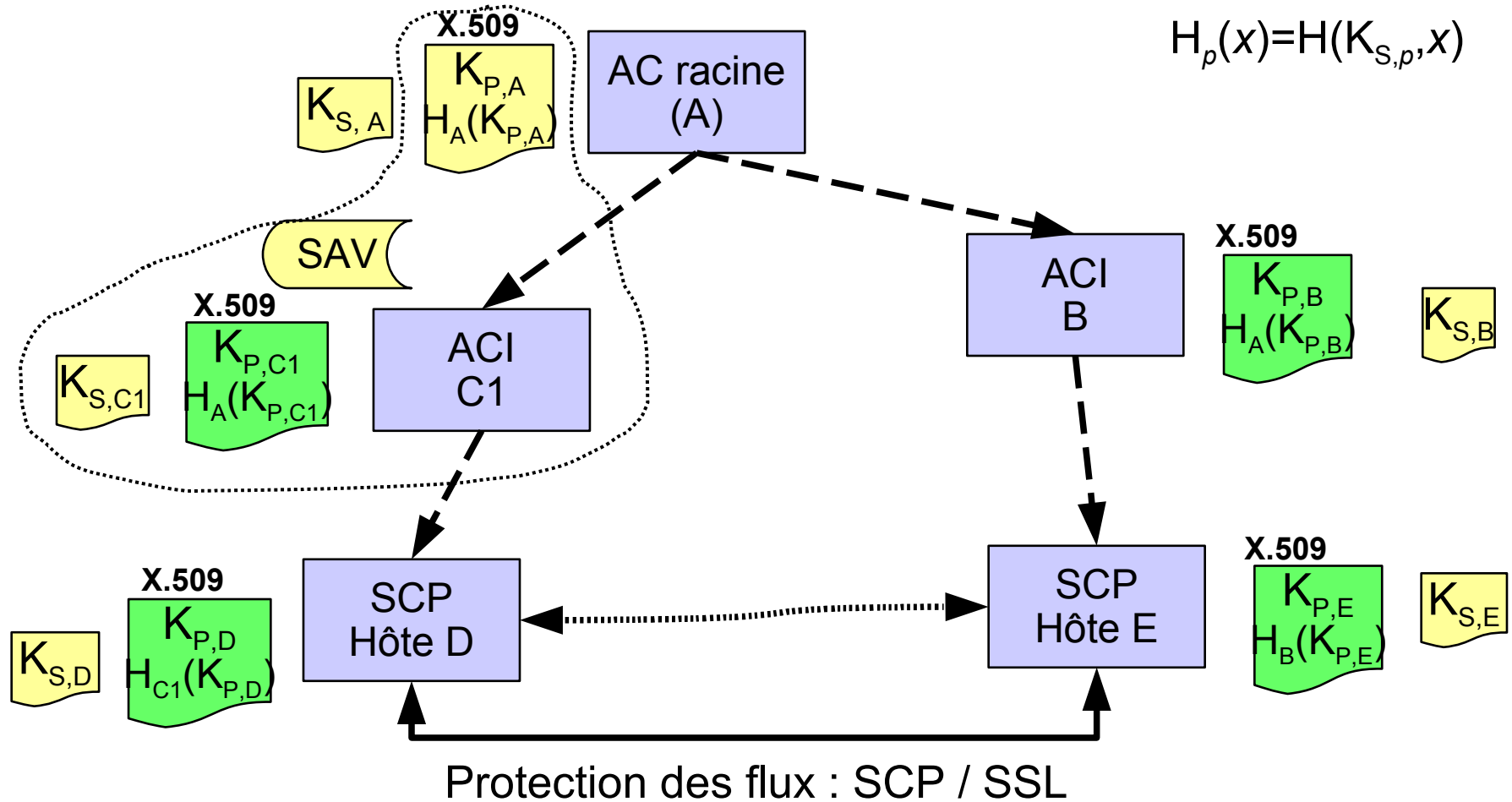
- Fonctionner en mode relais pur

```
options {  
  ...  
  // Allowed forwarders (only the DMZ nameservers)  
  forwarders {  
    192.168.69.1; 192.168.66.1;  
  };  
  
  // We *always* forward  
  forward only;  
  ...  
};
```

PGP et la confiance

- Un protocole : OpenPGP (RFC 2440)
- Deux principales implémentations : PGP et GnuPG
- Le conteneur contient : un bi-clef, un ensemble de signatures et des informations « administratives »
- Signer une clef
 - Cela signifie que vous avez pu vérifier *directement* l'identité du détenteur de la clef publique (par exemple à l'aide d'une empreinte de cette clef communiquée en personne et d'une carte d'identité)
 - Cela ne signifie rien d'autre
- Pour signer ou chiffrer des fichiers et des messages
- *Trust* : permet de limiter la transitivité (et indiquer ceux qui ne définissent pas « signer une clef » comme vous)

PKI – Autorités de certification



$$H_p(x) = H(K_{S,p}, x)$$

- - -> Certification
- Authentication mutuelle
- ↔ Échange de données