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

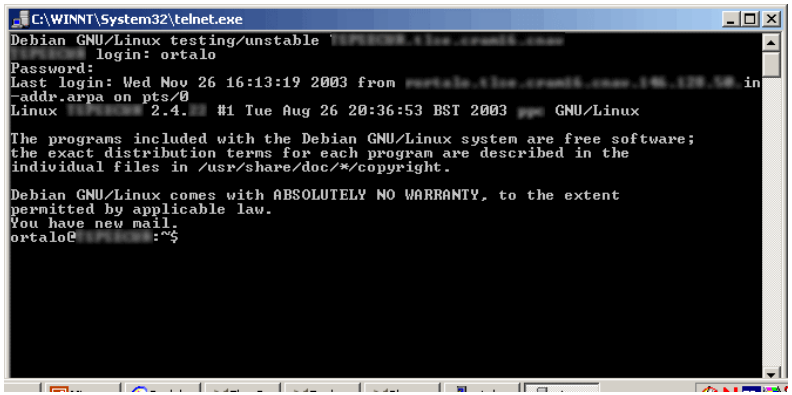
- Serveurs
  - UNIX
    - Solaris
    - Linux
      - RedHat
      - Suse
      - Debian
    - AIX
  - Windows
  - Novell
- Baies de disques
- Routeurs
- *Switches*
- PC Windows
- Macintosh
- Robots (sauvegardes)
- Imprimantes
- Boîtiers caches
- Boîtiers *firewall*
- Éléments logiciels
  - Antivirus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

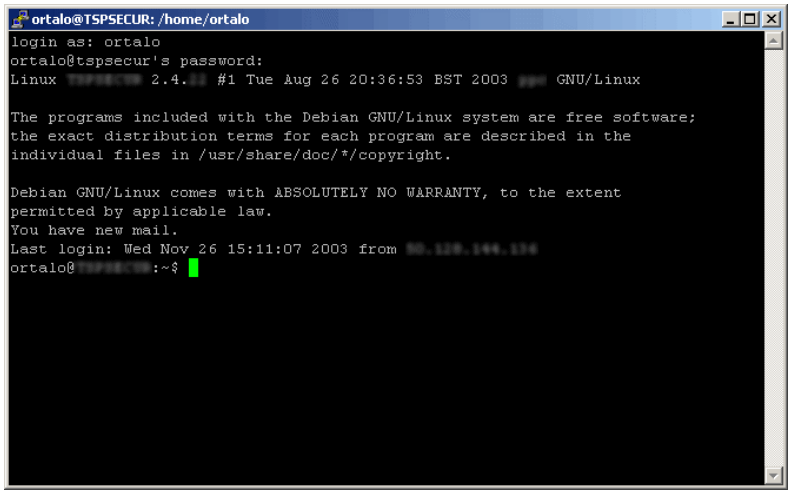
Correctifs et mises à jours

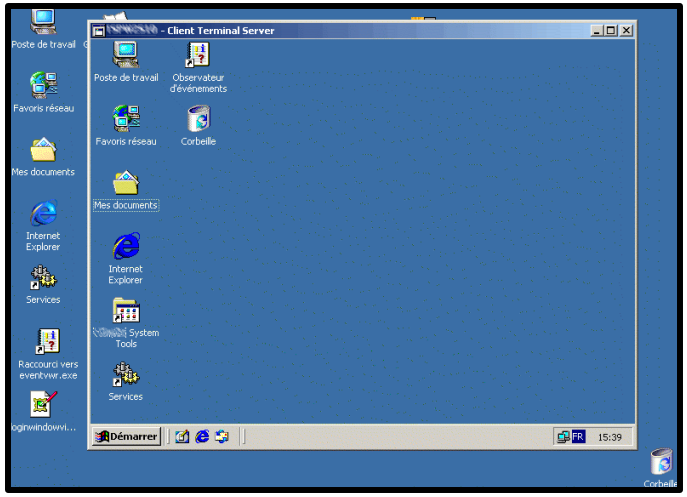
- Contraintes : ne pas perturber le fonctionnement normal
- Réagir (notamment à des alertes de sécurité)
- Faciliter les déploiements
  - *patches*
  - *Windows Update, SMS*
  - Lien avec les autres éléments du poste de travail ou des serveurs

Prise en main à distance

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







Systèmes embarqués

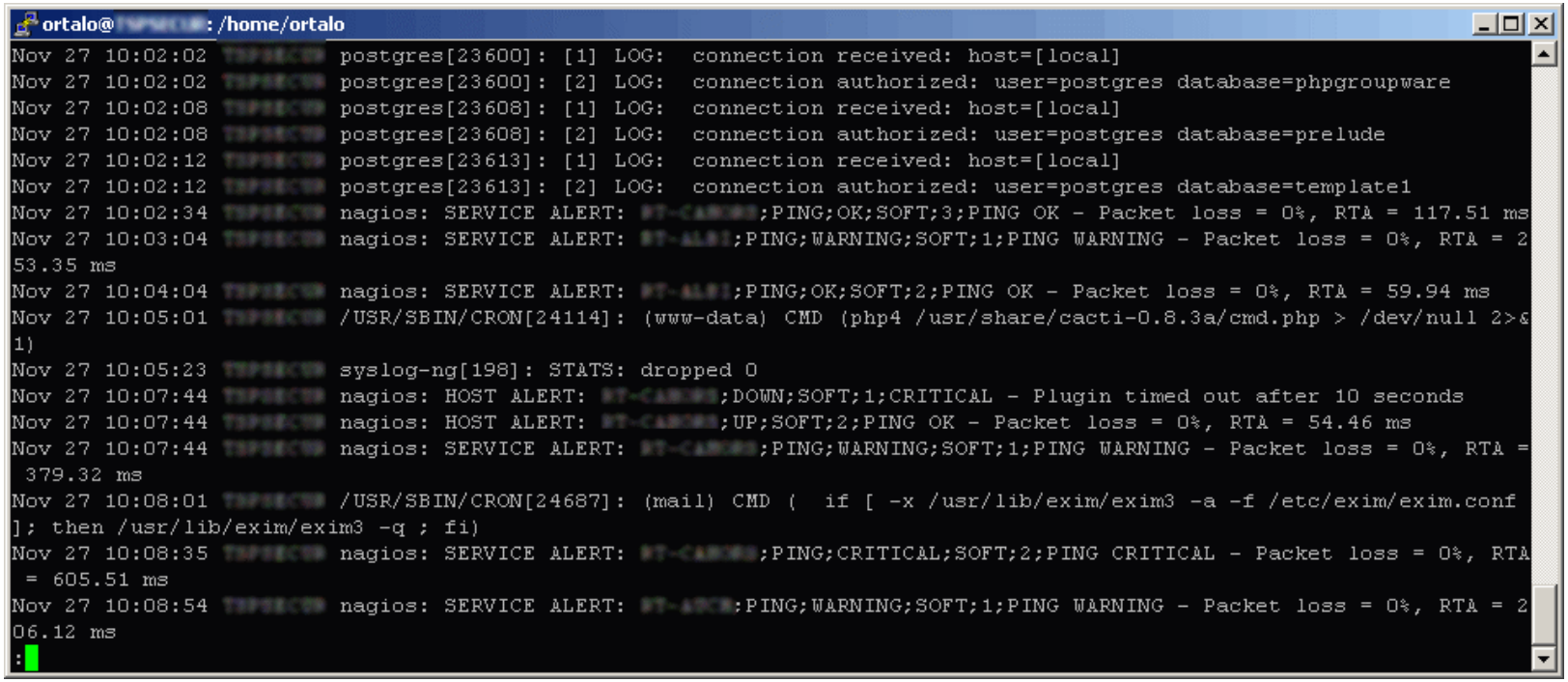
- Il s'agit souvent des équipements associés à *l'infrastructure réseau* (LAN)
- TFTP est largement répandu
  - Mise à jour des OS embarqués (*switch* Cisco, PIX)
  - Sauvegarde des configurations
- HTTP et HTTPS également (IHM)
- SNMP est supporté de manière hétérogène
- SSH apparaît sur les équipements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

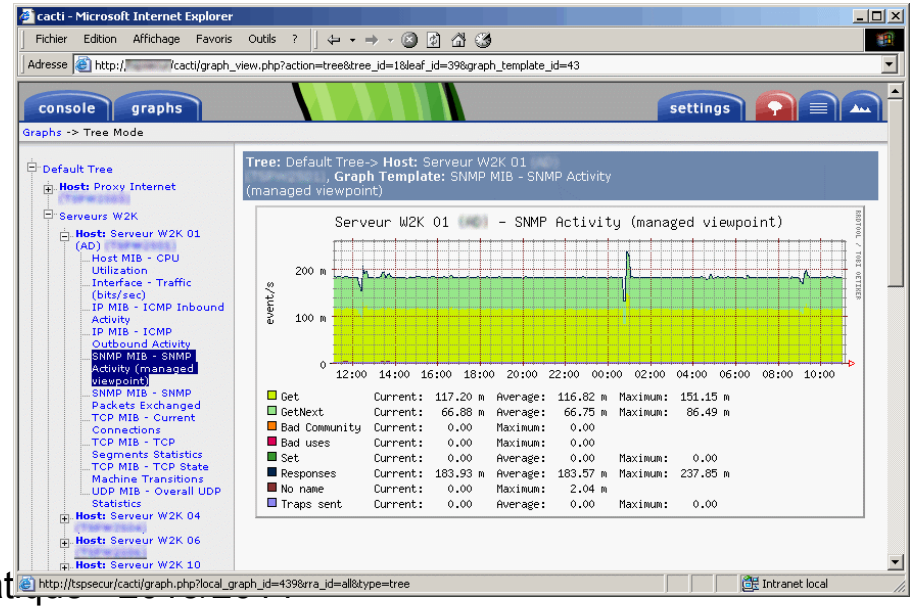


Observation et Surveillance

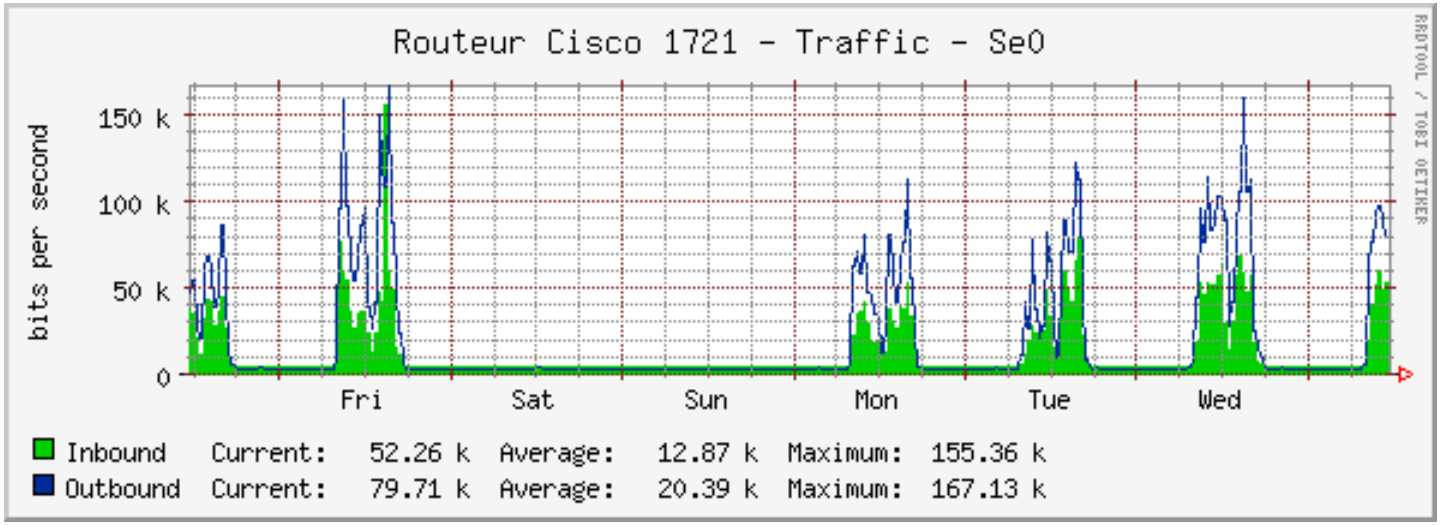
- *Monitoring* réseau
  - Équipements de sécurité
  - Autres équipements (réseaux et QoS par exemple)
- Surveillance système
- Évènements anormaux

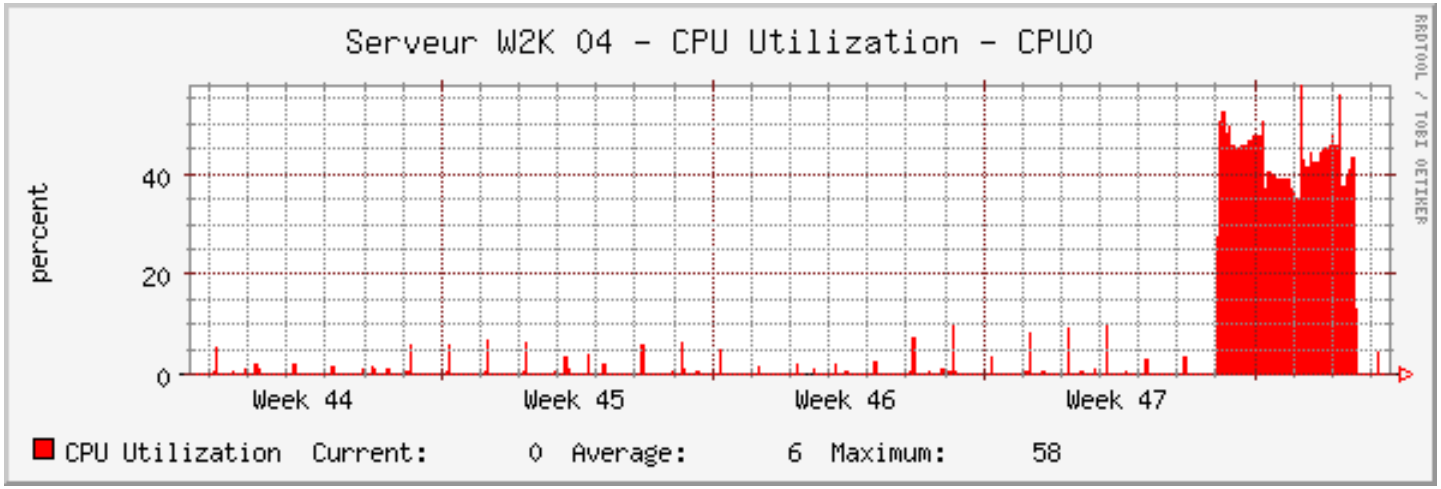
SNMP

- 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

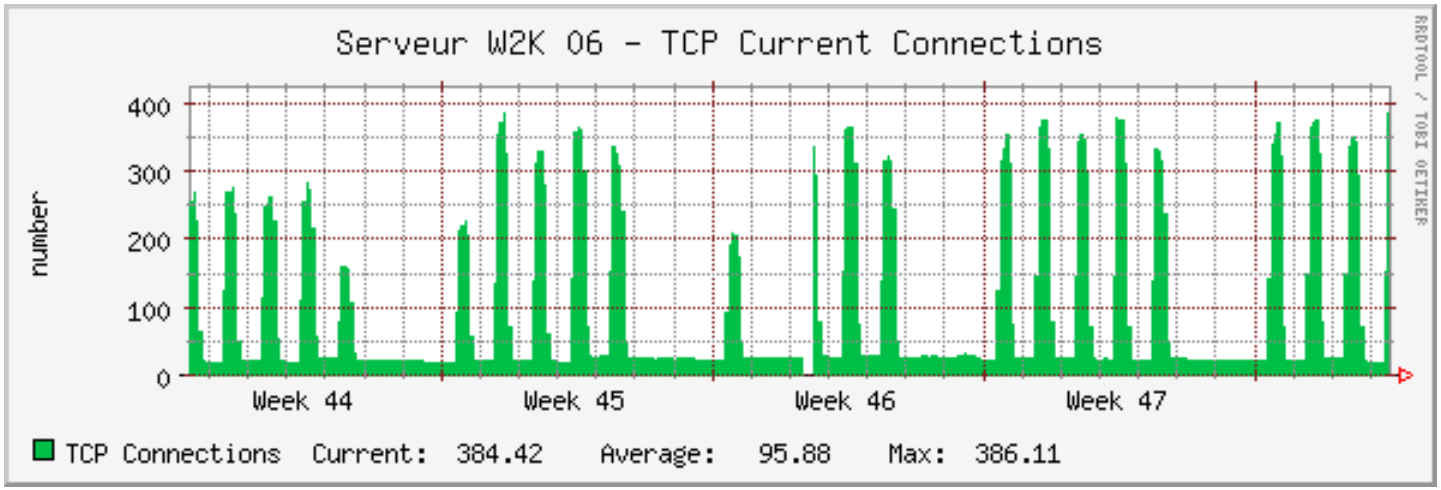


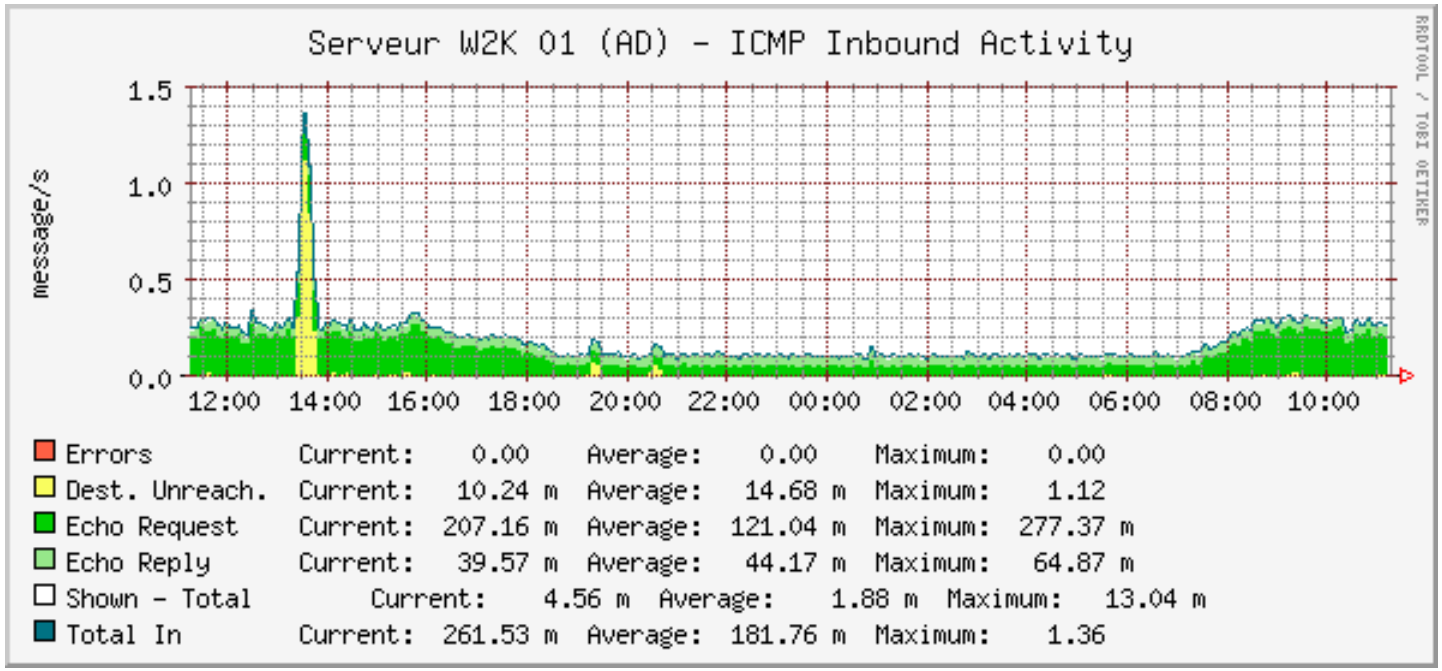
SNMP (Exemples)



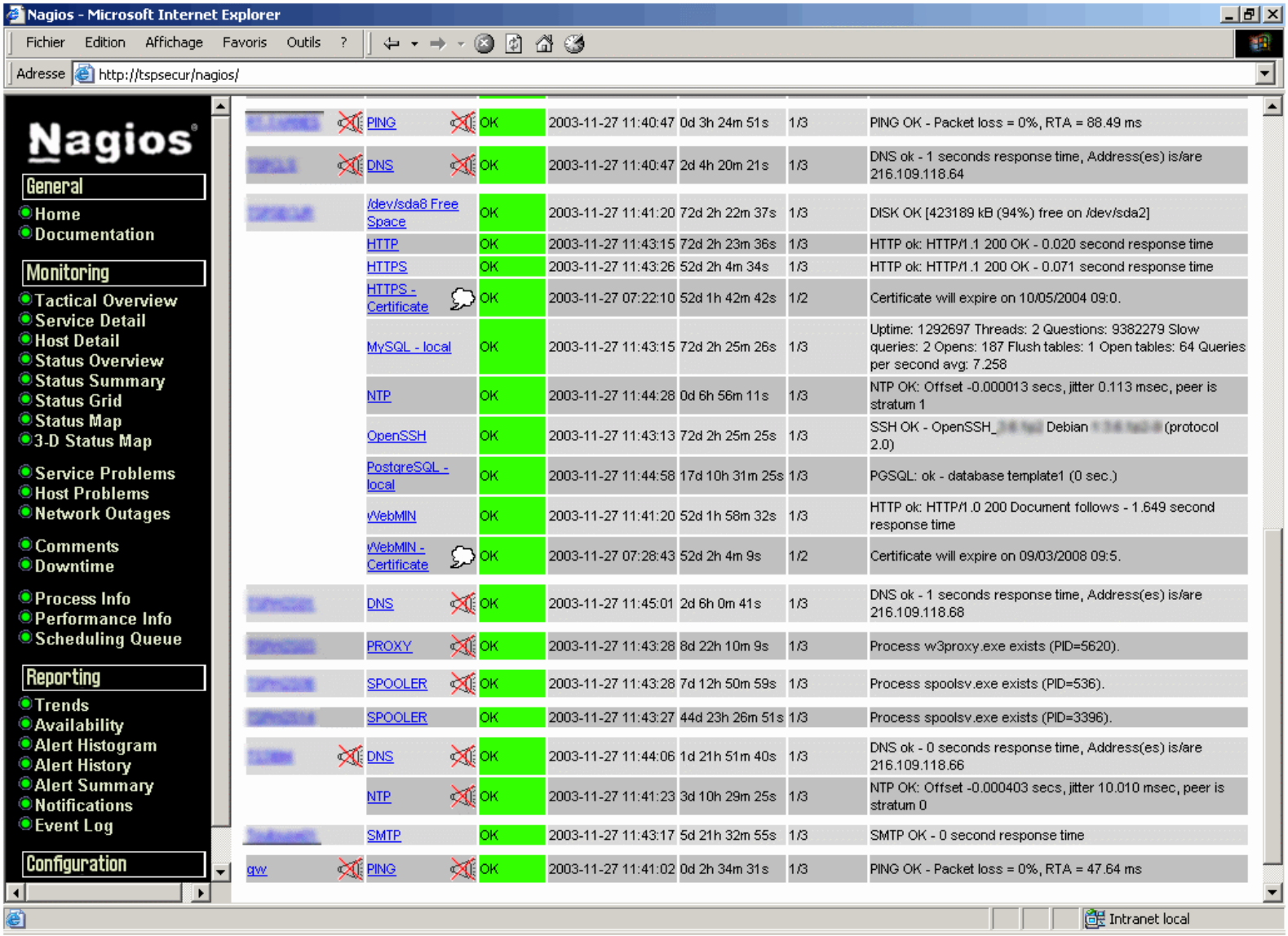


SNMP
(Exemples)





Surveillance système (exemple)



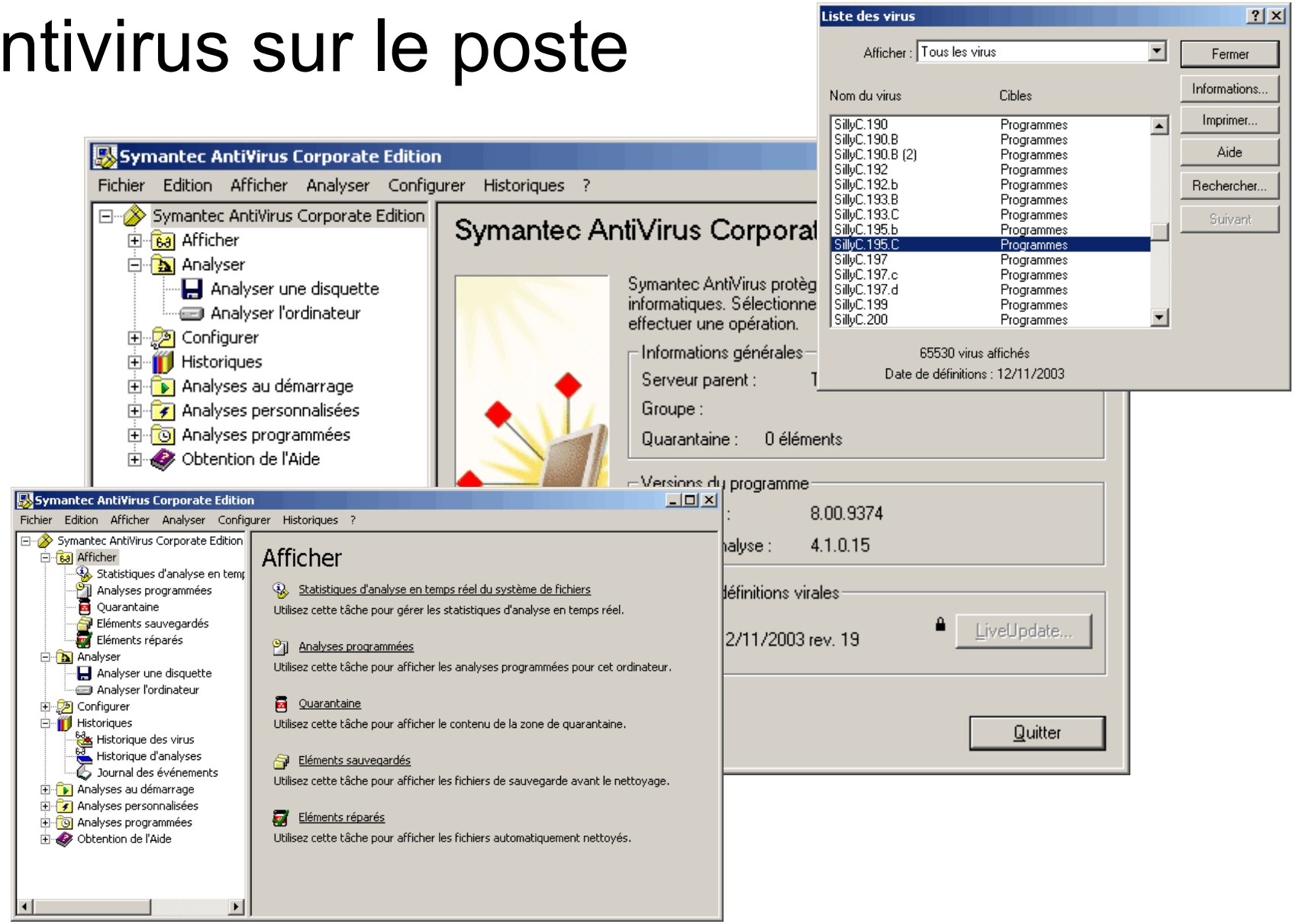
Plan (2/2)

- 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**

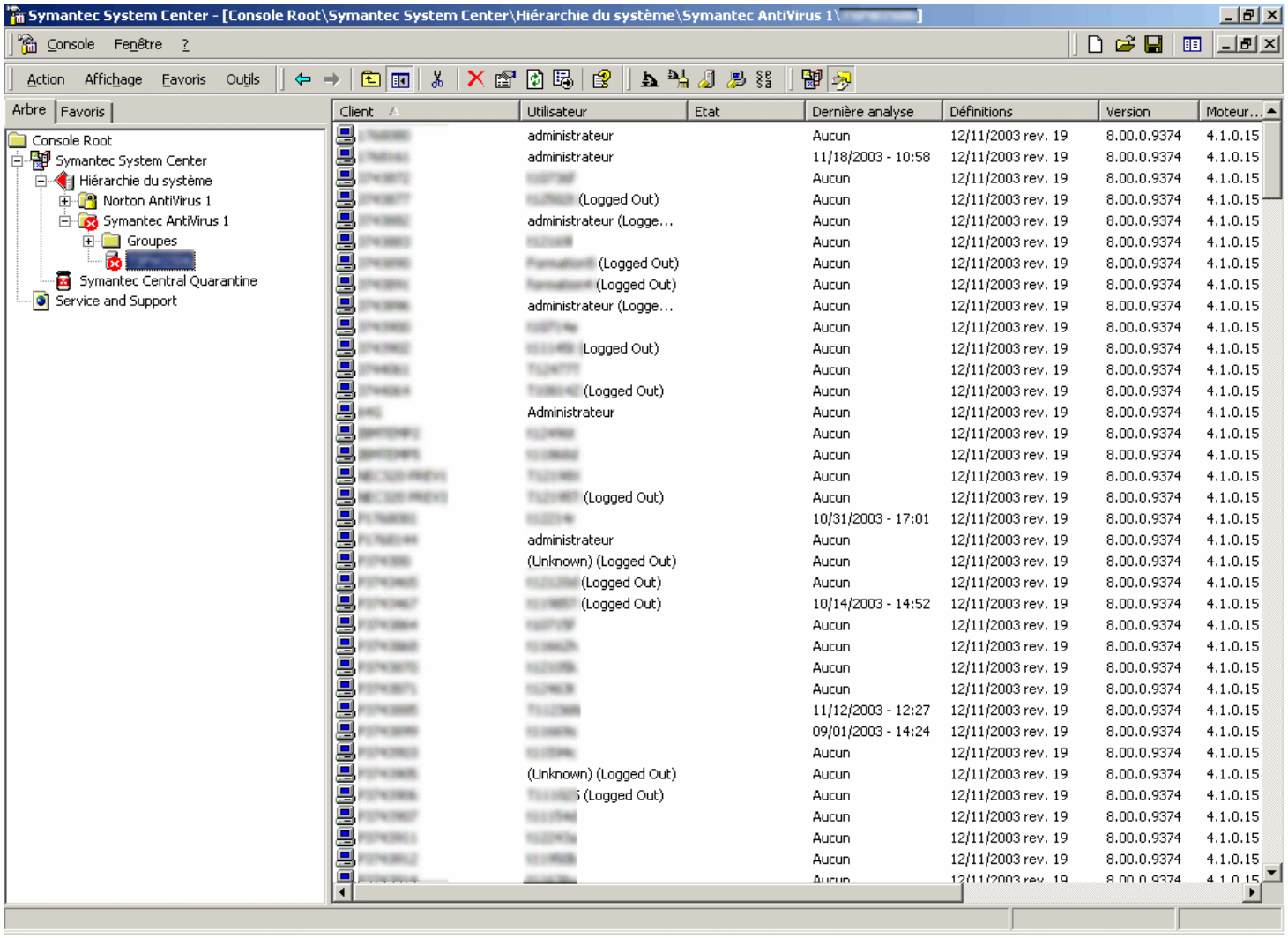
Plan (détaillé)

- **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.

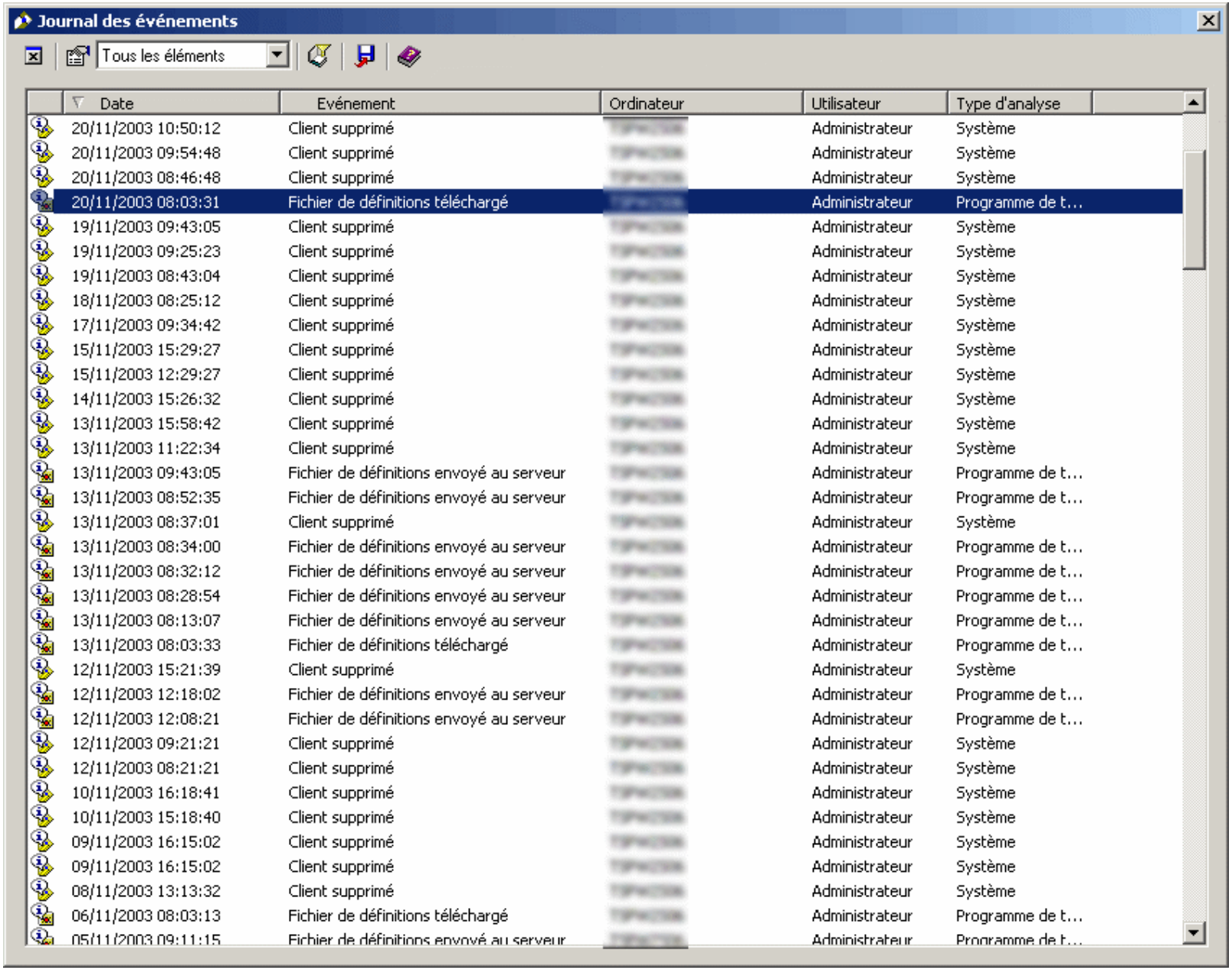
Antivirus sur le poste



Console Antivirus (1)

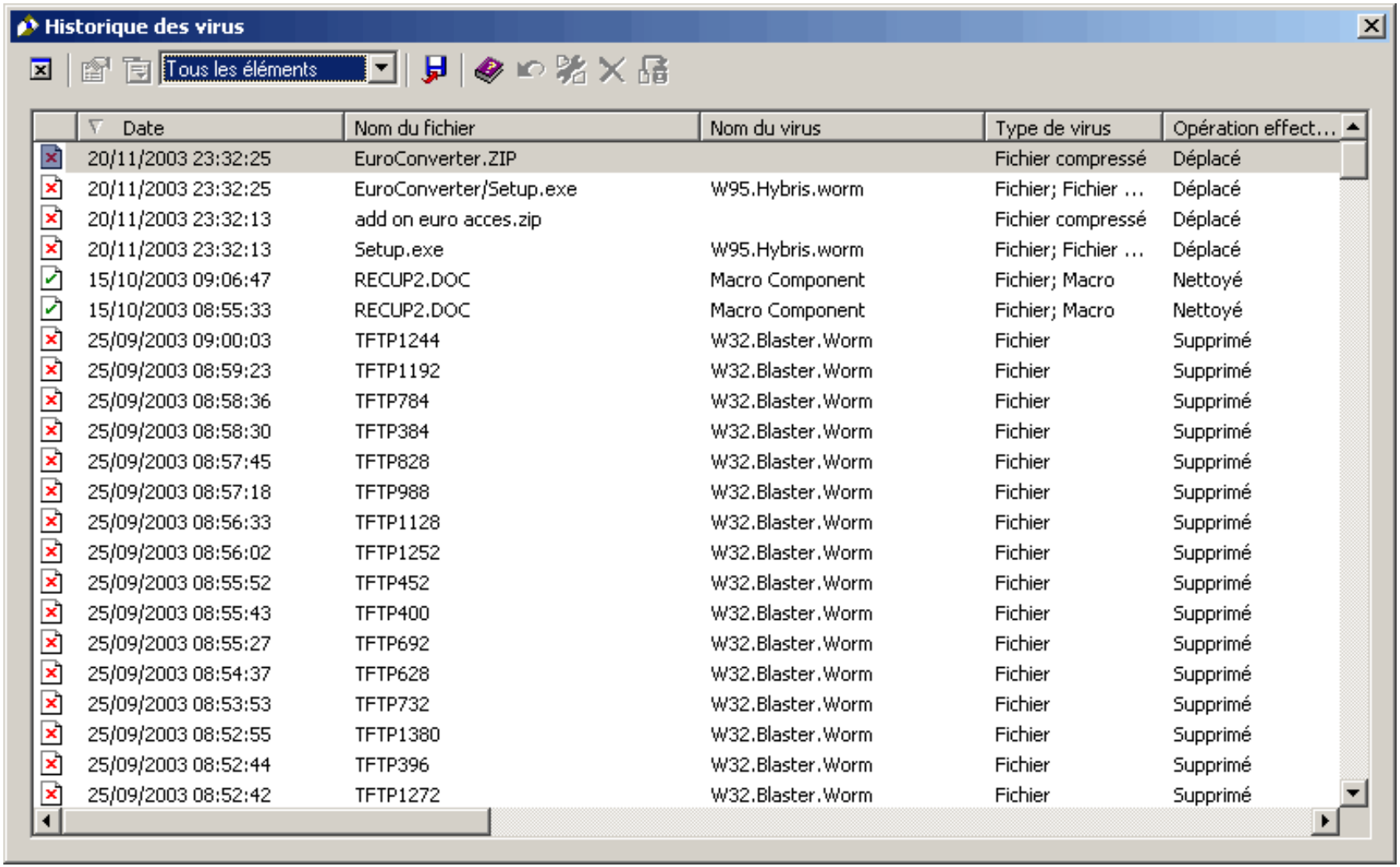


Console Antivirus (2)



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

Console Antivirus (3)



Date	Nom du fichier	Nom du virus	Type de virus	Opération effect...
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)

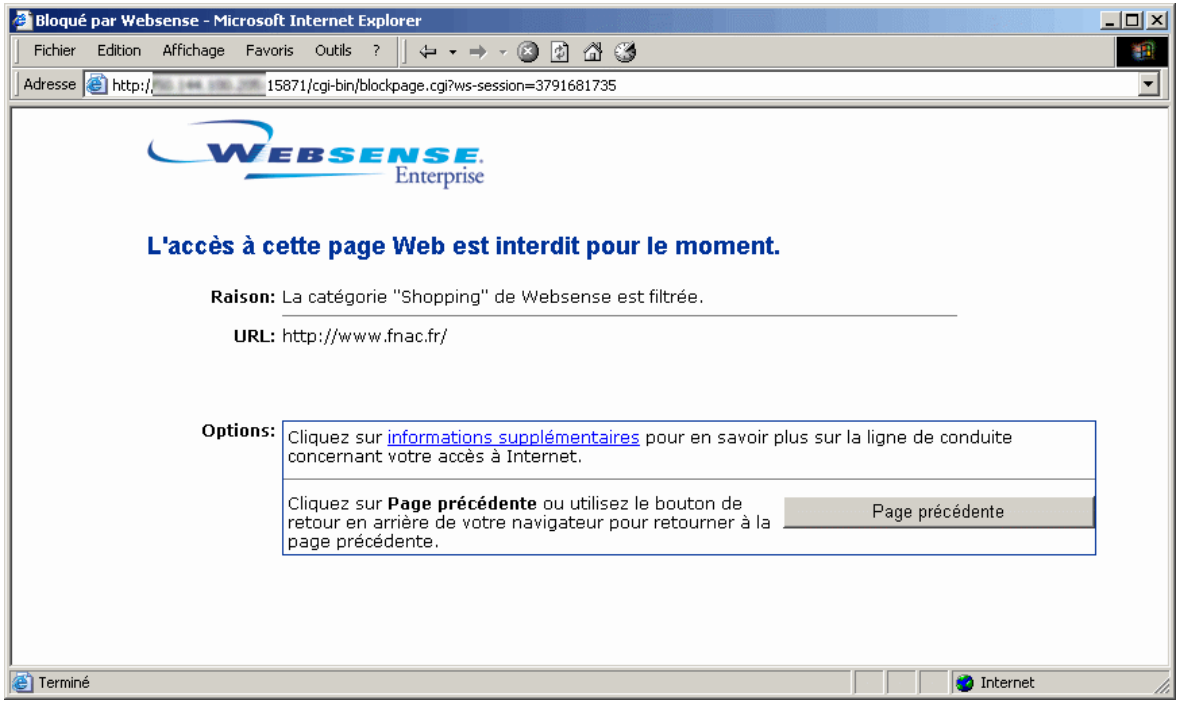
SquidGuard (2)

- 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

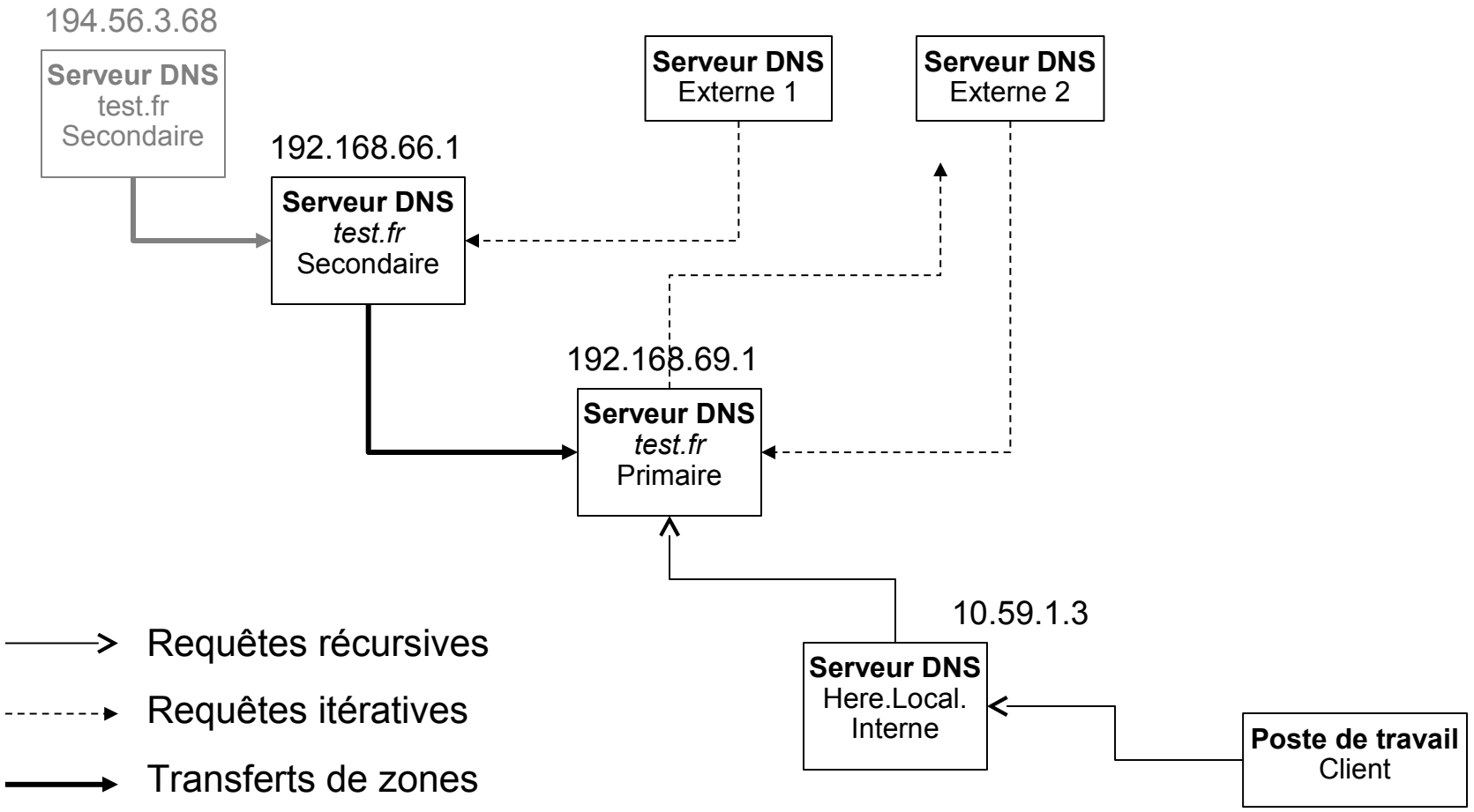
- Les offres commerciales incluent la classification des sites
- Exemple : WebSense



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.


194.56.3.68
Serveur DNS
test.fr
Secondaire
Serveur DNS
Externe 1
Serveur DNS
Externe 2
192.168.66.1
Serveur DNS
test.fr
Secondaire
192.168.69.1
Serveur DNS
test.fr
Primaire
10.59.1.3
Serveur DNS
Here.Local.
Interne
Poste de travail
Client
Requêtes récursives
Requêtes itératives
Transferts de zones

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