

# Sécurité et Réseaux

## La défense

# La défense

## Principales technologies de défense

- Protection des locaux et des équipements
- Protection des données sur la machine (Authentification, restrictions d'accès )
- Protection contre les intrusions (Firewalls , Proxy, anti-virus, Anti – spyware, Anti Spam, Suppression des fichiers de travail )
- Sauvegarde des données
- Cryptage des données
- Bonnes pratiques

# 0 - Protection des locaux et des équipements

## **Protection des locaux :**

- Portes solides
- Contrôle des accès, caméras
- Alarmes
- ...

## **Protection des équipements**

- Protection contre le vol
- Protection électriques (onduleurs)
- Climatisation
- ...

# 1 – Protection des données sur la machine

# 1 - Protection des données

## Authentification

Objectif : vérifier la véracité des utilisateurs, du réseau et des documents.

Méthodes :

- Créer un compte d'accès pour chaque utilisateur et lui associer un mot de passe.
- Mettre un mot de passe à l'administrateur par défaut sous Windows
- Supprimer (ou restreindre les droits) du compte invité

Changer votre mot de passe



**Francis**  
Administrateur  
Protégé par mot de passe

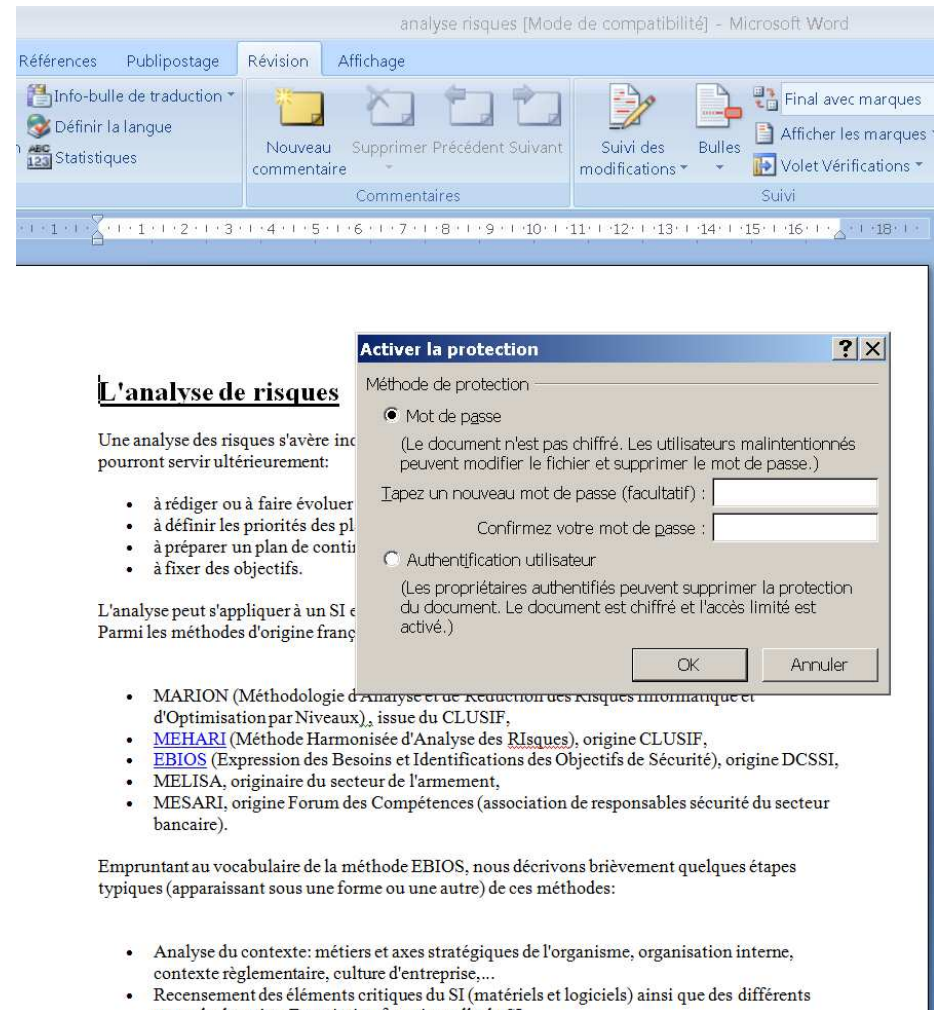
Si votre mot de passe contient des lettres majuscules, voir  
[Conseils pour créer un mot de passe fort](#)

L'indication de mot de passe sera visible à toutes les pers  
[Qu'est-ce qu'une indication de mot de passe ?](#)

# 1 - Protection des données

## Authentification

- Protéger les documents sensibles par code d'accès (par exemple, sous Word il est possible de protéger les documents en leur associant un mot de passe d'accès . Option : Revision → Protéger le document → Mot de passe



# 1 - Protection des données

## Restriction des accès

Objectif : restreindre les accès aux dossiers et documents par un système de droits d'accès.

Méthodes :

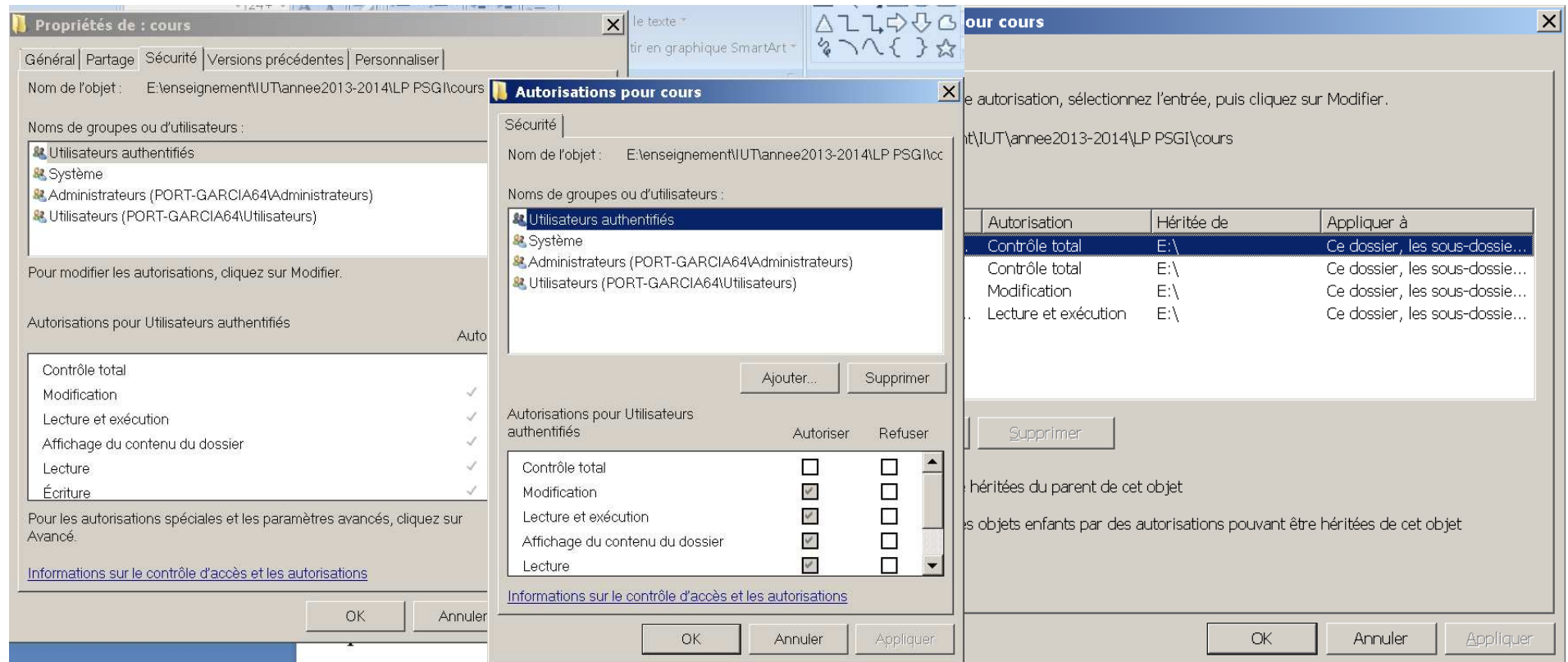
- Sous Linux tout est protégé par défaut, la commande *chmod* permet de modifier les restrictions.

```
nunux@Tux:/mnt/donnees/testt$ ls -la
total 28
drwxr-xr-x  3 nunux users 4096 2005-07-14 16:52 ./
drwxrwxrwx 43 root  root 8192 2005-07-14 16:49 ../
-rw-r--r--  1 nunux users   2 2005-07-14 16:51 .config
drwx----- 2 nunux users 4096 2005-07-14 16:52 images/
-rw-r--r--  1 nunux users  111 2005-07-14 16:51 index.html
lrwxrwxrwx  1 nunux users   23 2005-07-14 16:50 linux -> /usr/src/linux-2.6.11.8
-rw-r--r--  1 nunux users   2 2005-07-14 16:51 readme.txt
```

# 1 - Protection des données

## Restriction des accès

- Sous Windows rien n'est protégé par défaut. Dans les propriétés d'un document ou dossier, l'onglet sécurité permet de réaliser cette action.





## 2 – Protection contre les intrusions

# 1 –Observateurs d'évènements

Les observateurs d'évènements sont des outils avancés qui affichent des informations détaillées sur l'activité du système :

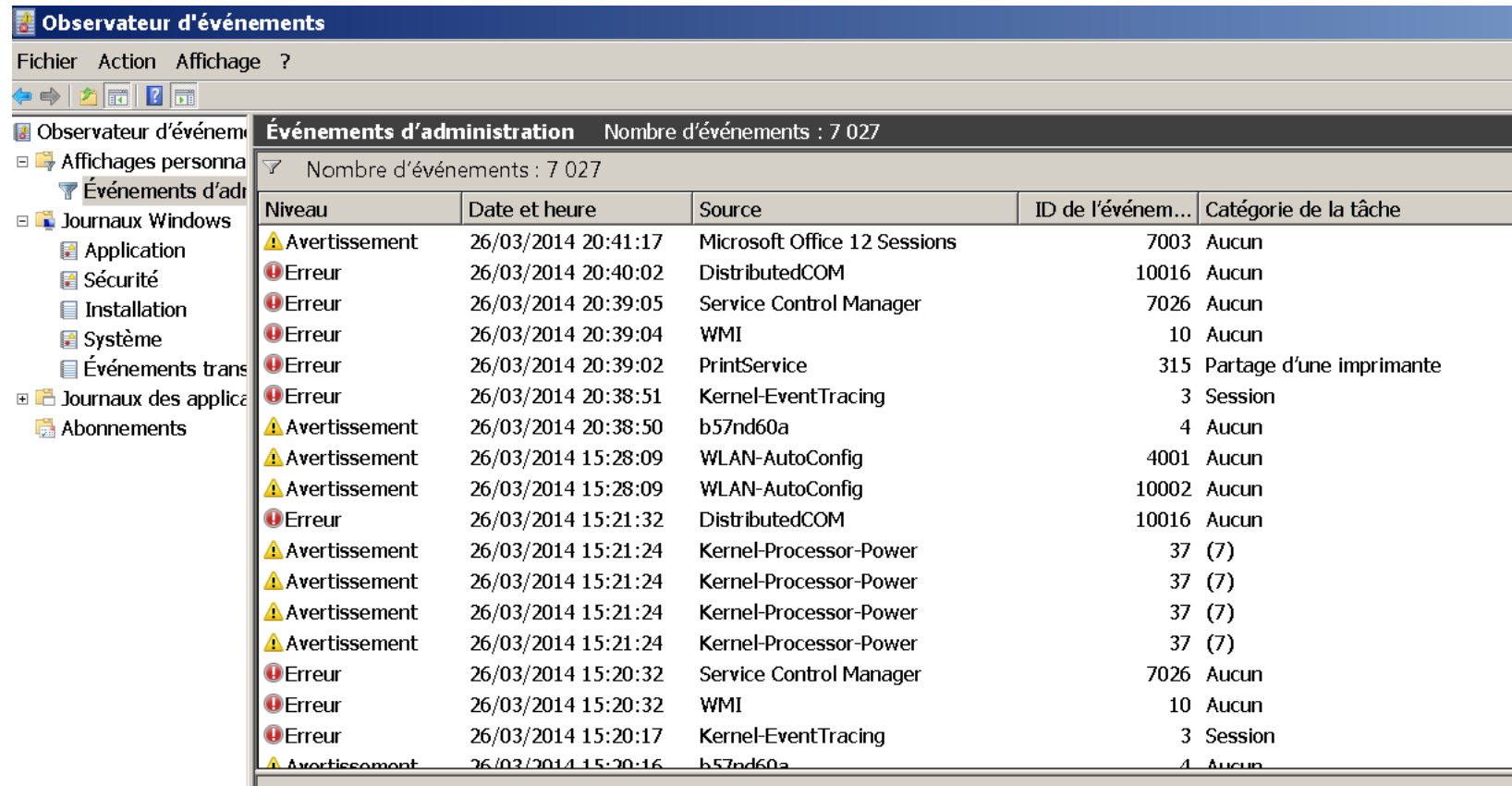
- programmes qui ne démarrent pas comme prévu,
- mises à jour qui sont téléchargées automatiquement,
- ouverture et fermeture d'applications,
- installations d'applications,
- connexions en cours
- ...

Ces outils peuvent s'avérer utiles pour :

- surveiller l'activité du système,
- résoudre des erreurs et des problèmes affectant le système,
- ...

# 1 –Observateurs d'évènements

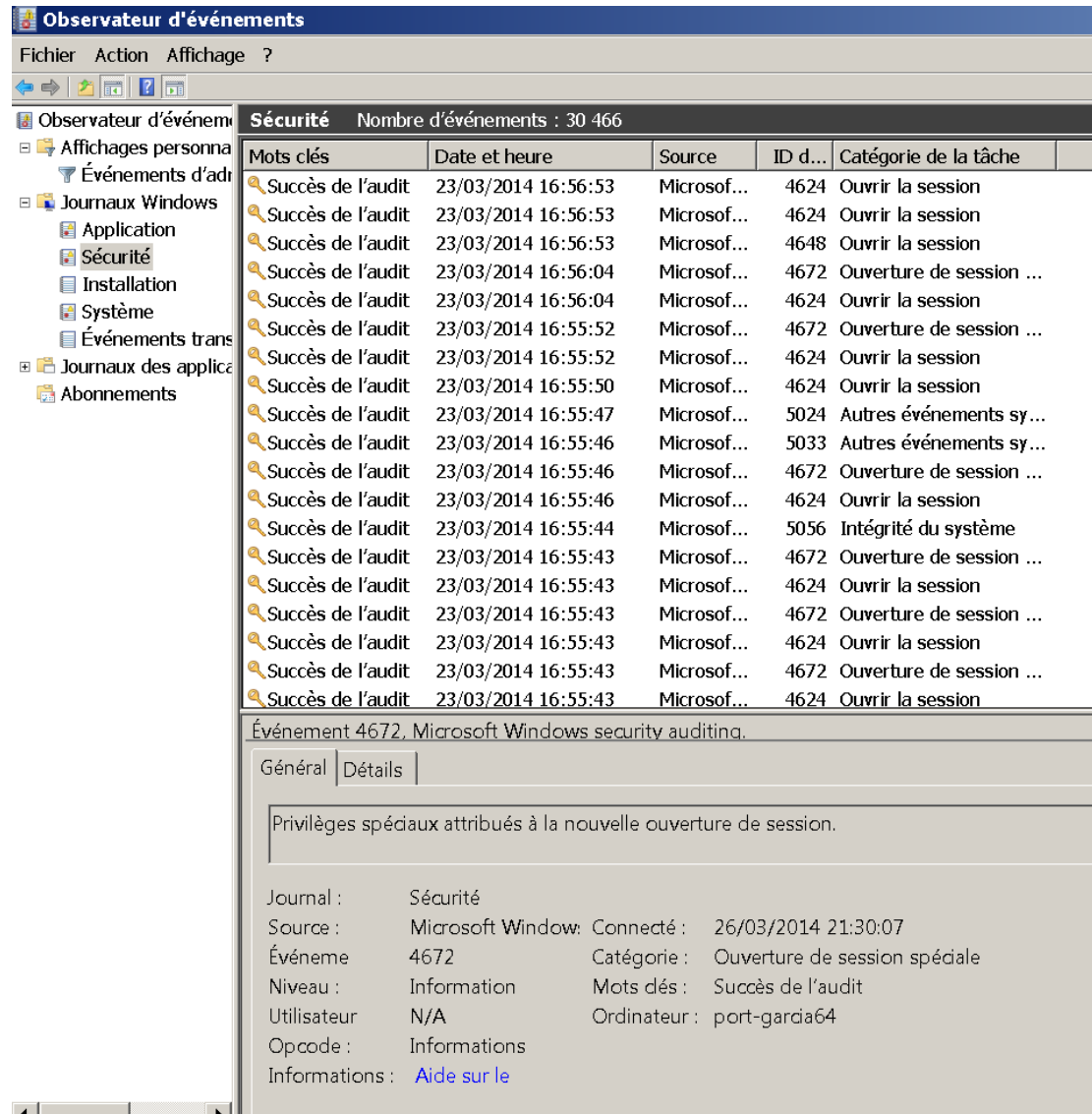
## Exemple : l'observateur d'évènements sous Windows



Observateur d'événements				
Fichier Action Affichage ?				
Observateur d'événements	Événements d'administration Nombre d'événements : 7 027			
Affichages personnels	Nombre d'événements : 7 027			
Événements d'administration				
Journaux Windows				
Application				
Sécurité				
Installation				
Système				
Événements trans				
Journaux des applica				
Abonnements				
Niveau	Date et heure	Source	ID de l'événement...	Catégorie de la tâche
Avertissement	26/03/2014 20:41:17	Microsoft Office 12 Sessions	7003	Aucun
Erreur	26/03/2014 20:40:02	DistributedCOM	10016	Aucun
Erreur	26/03/2014 20:39:05	Service Control Manager	7026	Aucun
Erreur	26/03/2014 20:39:04	WMI	10	Aucun
Erreur	26/03/2014 20:39:02	PrintService	315	Partage d'une imprimante
Erreur	26/03/2014 20:38:51	Kernel-EventTracing	3	Session
Avertissement	26/03/2014 20:38:50	b57nd60a	4	Aucun
Avertissement	26/03/2014 15:28:09	WLAN-AutoConfig	4001	Aucun
Avertissement	26/03/2014 15:28:09	WLAN-AutoConfig	10002	Aucun
Erreur	26/03/2014 15:21:32	DistributedCOM	10016	Aucun
Avertissement	26/03/2014 15:21:24	Kernel-Processor-Power	37	(7)
Avertissement	26/03/2014 15:21:24	Kernel-Processor-Power	37	(7)
Avertissement	26/03/2014 15:21:24	Kernel-Processor-Power	37	(7)
Avertissement	26/03/2014 15:21:24	Kernel-Processor-Power	37	(7)
Erreur	26/03/2014 15:20:32	Service Control Manager	7026	Aucun
Erreur	26/03/2014 15:20:32	WMI	10	Aucun
Erreur	26/03/2014 15:20:17	Kernel-EventTracing	3	Session
Avertissement	26/03/2014 15:20:16	b57nd60a	4	Aucun

# 1 –Observateurs d'évènements

## Exemple : l'observateur d'évènements sous Windows



**Observateur d'événements**

Fichier Action Affichage ?

Observateur d'événements

- Affichages personnalisés
- Événements d'administration
- Journaux Windows
  - Application
  - Sécurité**
  - Installation
  - Système
  - Événements transactiens
- Journaux des applications
- Abonnements

**Sécurité** Nombre d'événements : 30 466

Mots clés	Date et heure	Source	ID d...	Catégorie de la tâche
Succès de l'audit	23/03/2014 16:56:53	Microsof...	4624	Ouvrir la session
Succès de l'audit	23/03/2014 16:56:53	Microsof...	4624	Ouvrir la session
Succès de l'audit	23/03/2014 16:56:53	Microsof...	4648	Ouvrir la session
Succès de l'audit	23/03/2014 16:56:04	Microsof...	4672	Ouverture de session ...
Succès de l'audit	23/03/2014 16:56:04	Microsof...	4624	Ouvrir la session
Succès de l'audit	23/03/2014 16:55:52	Microsof...	4672	Ouverture de session ...
Succès de l'audit	23/03/2014 16:55:52	Microsof...	4624	Ouvrir la session
Succès de l'audit	23/03/2014 16:55:50	Microsof...	4624	Ouvrir la session
Succès de l'audit	23/03/2014 16:55:47	Microsof...	5024	Autres événements sy...
Succès de l'audit	23/03/2014 16:55:46	Microsof...	5033	Autres événements sy...
Succès de l'audit	23/03/2014 16:55:46	Microsof...	4672	Ouverture de session ...
Succès de l'audit	23/03/2014 16:55:46	Microsof...	4624	Ouvrir la session
Succès de l'audit	23/03/2014 16:55:44	Microsof...	5056	Intégrité du système
Succès de l'audit	23/03/2014 16:55:43	Microsof...	4672	Ouverture de session ...
Succès de l'audit	23/03/2014 16:55:43	Microsof...	4624	Ouvrir la session
Succès de l'audit	23/03/2014 16:55:43	Microsof...	4672	Ouverture de session ...
Succès de l'audit	23/03/2014 16:55:43	Microsof...	4624	Ouvrir la session
Succès de l'audit	23/03/2014 16:55:43	Microsof...	4672	Ouverture de session ...
Succès de l'audit	23/03/2014 16:55:43	Microsof...	4624	Ouvrir la session

Événement 4672, Microsoft Windows security auditing.

Général Détails

Privilèges spéciaux attribués à la nouvelle ouverture de session.

Journal : Sécurité

Source : Microsoft Windows Connecté : 26/03/2014 21:30:07

Événement : 4672 Catégorie : Ouverture de session spéciale

Niveau : Information Mots clés : Succès de l'audit

Utilisateur : N/A Ordinateur : port-garcia64

Opcode : Informations

Informations : [Aide sur le](#)

# 1 –Observateurs d'évènements

## Exemple : Commande « netstat »

```
TCP    127.0.0.1:50750      port-garcia64:21322  TIME_WAIT
TCP    127.0.0.1:50766      port-garcia64:21322  TIME_WAIT
TCP    127.0.0.1:50767      port-garcia64:21322  TIME_WAIT
TCP    127.0.0.1:50768      port-garcia64:21322  TIME_WAIT
TCP    127.0.0.1:50769      port-garcia64:21322  TIME_WAIT
TCP    127.0.0.1:50770      port-garcia64:21322  TIME_WAIT
TCP    127.0.0.1:50771      port-garcia64:21322  TIME_WAIT
TCP    127.0.0.1:50772      port-garcia64:21322  TIME_WAIT
TCP    127.0.0.1:50773      port-garcia64:21322  TIME_WAIT
TCP    192.168.1.67:139     port-garcia64:0      LISTENING
TCP    192.168.1.67:50748    65.55.58.184:http    ESTABLISHED
TCP    192.168.1.67:50752    a184-51-148-168:http  TIME_WAIT
TCP    192.168.1.67:50753    a184-51-148-168:http  TIME_WAIT
TCP    192.168.1.67:50754    a184-51-148-168:http  TIME_WAIT
TCP    192.168.1.67:50755    a184-51-148-168:http  TIME_WAIT
TCP    192.168.1.67:50757    68.232.34.200:http    TIME_WAIT
TCP    192.168.1.67:50758    68.232.34.201:http    TIME_WAIT
TCP    192.168.1.67:50760    a184-51-148-115:http  ESTABLISHED
TCP    192.168.1.67:50763    edge-star-shv-10-fra2:http ESTABLISHED
TCP    192.168.1.67:50764    a184-51-148-168:http  TIME_WAIT
TCP    192.168.1.67:50765    95.100.248.147:http   TIME_WAIT
TCP    [::]:135             port-garcia64:0      LISTENING
TCP    [::]:445             port-garcia64:0      LISTENING
TCP    [::]:5357            port-garcia64:0      LISTENING
TCP    [::]:49152           port-garcia64:0      LISTENING
```

Netstat est un outil permettant de connaître les connexions TCP actives sur la machine sur laquelle la commande est activée et ainsi lister l'ensemble des ports TCP et UDP ouverts sur l'ordinateur.

La commande « netstat » permet également d'obtenir des statistiques sur un certain nombre de protocoles (Ethernet, IPv4, TCP, UDP, ICMP et IPv6).

## 2 -Pare-feu ou firewall

**Objectif : filtrer les trames entre le réseau externe et le réseau interne.**

Un firewall intervient au niveau des couches 3 et 4 de l'OSI en filtrant les paquets IP.

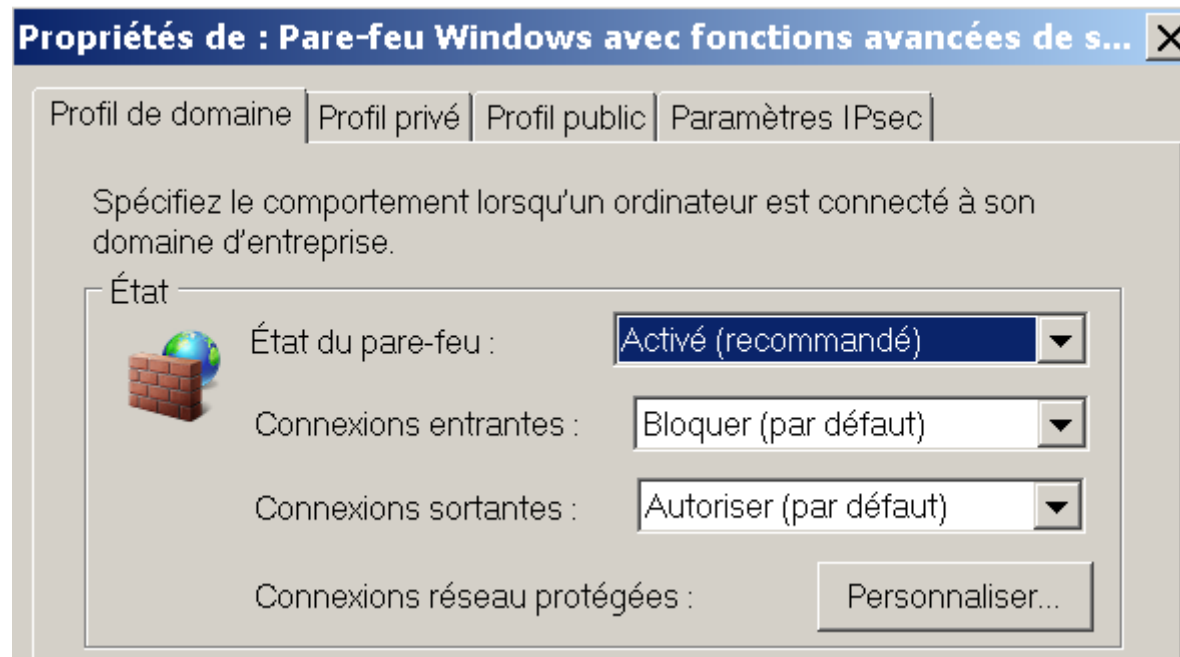
Seule l'en-tête IP d'une trame peut laisser des traces lors de son passage, les rubriques utiles pour le filtrage de paquets sont :

- types de paquets (TCP, UDP, ...)
- adresse IP d'origine
- adresse IP de destination
- le port de destination (TCP, UDP, ...)
- . . .

## 2 -Pare-feu ou firewall

Un système pare-feu contient un ensemble de règles prédéfinies (règles de filtrage) permettant :

- D'autoriser la connexion (*allow*) ;
- De bloquer la connexion (*deny*) ;
- De rejeter la demande de connexion sans avertir l'émetteur (*drop*).



# 2 -Pare-feu ou firewall

## Exemple : Le pare-feu Windows

**Pare-feu Windows avec fonctions avancées de sécurité**

Fichier Action Affichage ?

Pare-feu Windows avec fonctions avancées de sécurité

- Règles de trafic entrant
- Règles de trafic sortant**
- Règles de sécurité de connexion
- Analyse
  - Pare-feu
  - Règles de sécurité de connexion
  - Associations de sécurité
    - Mode principal
    - Mode rapide

Nom	Groupe	Profil	Activée	Action	Programme	Adresse locale	Adresse distante	Protocole	Port local	Port distant
Assistance à distance (PRN...	Assistance à dista...	Public	Non	Autori...	%systemr...	Tout	Tout	UDP	Tout	Tout
Assistance à distance (PRN...	Assistance à dista...	Dom...	Oui	Autori...	%systemr...	Tout	Tout	UDP	Tout	Tout
Assistance à distance (SSD...	Assistance à dista...	Dom...	Oui	Autori...	%SystemR...	Tout	Sous-réseau local	TCP	Tout	Tout
Assistance à distance (SSD...	Assistance à dista...	Dom...	Oui	Autori...	%SystemR...	Tout	Sous-réseau local	UDP	Tout	1900
Assistance à distance (TCP...	Assistance à dista...	Dom...	Oui	Autori...	%SystemR...	Tout	Tout	TCP	Tout	Tout
Assistance à distance (TCP...	Assistance à dista...	Public	Non	Autori...	%SystemR...	Tout	Tout	TCP	Tout	Tout
Assistance à distance (Trafi...	Assistance à dista...	Dom...	Oui	Autori...	%SystemR...	Tout	Tout	TCP	Tout	Tout
Client de mise en cache héb...	BranchCache - Clie...	Tout	Non	Autori...	SYSTEM	Tout	Tout	TCP	Tout	443
Découverte d'homologue de...	BranchCache - Déc...	Tout	Non	Autori...	%systemr...	Tout	Sous-réseau local	UDP	Tout	3702
Extraction du contenu de Br...	BranchCache - Extr...	Tout	Non	Autori...	SYSTEM	Tout	Tout	TCP	Tout	80
Serveur de cache hébergé d...	BranchCache - Ser...	Tout	Non	Autori...	SYSTEM	Tout	Tout	TCP	443	Tout
Connexion à un projecteur r...	Connexion à un pro...	Priv...	Non	Autori...	%SystemR...	Tout	Sous-réseau local	TCP	Tout	Tout
Connexion à un projecteur r...	Connexion à un pro...	Dom...	Non	Autori...	%SystemR...	Tout	Tout	TCP	Tout	Tout
Connexion à un projecteur r...	Connexion à un pro...	Priv...	Non	Autori...	System	Tout	Sous-réseau local	TCP	Tout	5357
Connexion à un projecteur r...	Connexion à un pro...	Dom...	Non	Autori...	System	Tout	Tout	TCP	Tout	5357
Connexion à un projecteur r...	Connexion à un pro...	Dom...	Non	Autori...	System	Tout	Tout	TCP	Tout	5358
Connexion à un projecteur r...	Connexion à un pro...	Priv...	Non	Autori...	System	Tout	Sous-réseau local	TCP	Tout	5358
Connexion à un projecteur r...	Connexion à un pro...	Tout	Non	Autori...	%SystemR...	Tout	Sous-réseau local	UDP	Tout	3702
Coordinateur de transaction...	Coordinateur de tr...	Dom...	Non	Autori...	%SystemR...	Tout	Tout	TCP	Tout	Tout
Coordinateur de transaction...	Coordinateur de tr...	Priv...	Non	Autori...	%SystemR...	Tout	Sous-réseau local	TCP	Tout	Tout
Groupe résidentiel sortant	Groupe résidentiel	Privé	Non	Autori...	%systemr...	Tout	Sous-réseau local	TCP	Tout	3587
Groupement résidentiel sort...	Groupe résidentiel	Privé	Non	Autori...	%systemr...	Tout	Sous-réseau local	UDP	Tout	3540
Infrastructure de gestion Wi...	Infrastructure de g...	Priv...	Non	Autori...	%SystemR...	Tout	Sous-réseau local	TCP	Tout	Tout
Infrastructure de gestion Wi...	Infrastructure de g...	Dom...	Non	Autori...	%SystemR...	Tout	Tout	TCP	Tout	Tout
Lecteur Windows Media (TC...	Lecteur Windows ...	Tout	Non	Autori...	%Program...	Tout	Tout	TCP	Tout	Tout
Lecteur Windows Media (UD...	Lecteur Windows ...	Tout	Non	Autori...	%Program...	Tout	Tout	UDP	Tout	Tout
Lecteur Windows Media x86...	Lecteur Windows ...	Tout	Non	Autori...	%Program...	Tout	Tout	TCP	Tout	Tout
Lecteur Windows Media x86...	Lecteur Windows ...	Tout	Non	Autori...	%Program...	Tout	Tout	UDP	Tout	Tout
Partage de fichiers et d'impr...	Partage de fichiers ...	Dom...	Non	Autori...	Tout	Tout	Tout	ICMPv6	Tout	Tout
Partage de fichiers et d'impr...	Partage de fichiers ...	Public	Oui	Autori...	Tout	Tout	Sous-réseau local	ICMPv6	Tout	Tout
Partage de fichiers et d'impr...	Partage de fichiers ...	Privé	Oui	Autori...	Tout	Tout	Sous-réseau local	ICMPv6	Tout	Tout
Partage de fichiers et d'impr...	Partage de fichiers ...	Dom...	Non	Autori...	Tout	Tout	Tout	ICMPv4	Tout	Tout
Partage de fichiers et d'impr...	Partage de fichiers ...	Public	Oui	Autori...	Tout	Tout	Sous-réseau local	ICMPv4	Tout	Tout

**Actions**

- Nouvelle règle...
- Filtrer par profil
- Filtrer par état
- Filtrer par groupe
- Affichage
- Actualiser
- Exporter la liste...
- Aide



## 2 -Pare-feu ou firewall

### **Politiques de sécurité**

On distingue habituellement deux types de politiques de sécurité :

- On interdit tout, sauf les communications ayant été explicitement autorisées;

- On autorise tout, sauf les échanges qui ont été explicitement interdits.

→ Chaque politique a ces avantages et ces inconvénients.

## 2 -Pare-feu ou firewall

### Types de filtrage

**1 – Filtrage simple de paquets :** On précise la liste les adresses IP, N° de port et le protocole que l'on autorise ou pas.

**2 – Filtrage dynamique :** Si une application ouvre des ports de manière aléatoire, ce type de filtrage acceptera l'ensemble des paquets issus de la connexion initiale.

**3 – Filtrage applicatif :** Ce filtrage permet de filtrer les communications par application. Un firewall effectuant un filtrage applicatif est appelé généralement « passerelle applicative » (ou «proxy »)

## 2 -Pare-feu ou firewall

### Exemple de règles simples

Règle	Direction	@ source	@ dest.	Protocole	Port source	Port dest.	ACK=l	Action
<b>A</b>	Entrant	Externe	Interne	TCP	>1023	21		Permission
<b>B</b>	Sortant	Interne	Externe	TCP	21	>1023		Permission
<b>C</b>	Sortant	Interne	Externe	TCP	>1023	21		Permission
<b>D</b>	Entrant	Externe	Interne	TCP	21	>1023	Oui	Permission
<b>E</b>	Toutes	Toutes	Toutes	Tous	Tous	Tous		Refus


# Exemple pare feu Windows

# Pare feu Windows

Page d'accueil du panneau de configuration

Autoriser un programme ou une fonctionnalité via le Pare-feu Windows

 Modifier les paramètres de notification

 Activer ou désactiver le Pare-feu Windows

 Paramètres par défaut

 Paramètres avancés

Dépanner mon réseau


## Protégez votre ordinateur avec le Pare-feu Windows

Le Pare-feu Windows a pour but d'empêcher les pirates ou les logiciels malveillants d'accéder à votre ordinateur via Internet ou via un réseau.

[Comment un pare-feu protège-t-il mon ordinateur ?](#)

[Qu'est-ce qu'un emplacement réseau ?](#)

  Réseaux domestiques ou d'entreprise (privés) Non connecté 

  Réseaux publics Connecté 

Réseaux dans des lieux publics, tels qu'un aéroport ou un cybercafé

État du Pare-feu Windows :

Activé

Connexions entrantes :

Bloquer toutes les connexions aux programmes ne figurant pas dans la liste des programmes autorisés

Réseaux publics actifs :

 NEUF\_D6BC

État de notification :

M'avertir lorsque le Pare-feu Windows bloque un nouveau programme

# Pare feu Windows

## Autoriser les programmes à communiquer à travers le Pare-feu Windows

Pour ajouter, modifier ou supprimer des programmes et des ports autorisés, cliquez sur Modifier les paramètres.

Quels sont les risques si un programme est autorisé à communiquer ?

 Modifier les paramètres

Programmes et fonctionnalités autorisés :

Nom	Domestique/entreprise (privé)	Public
<input checked="" type="checkbox"/> Assistance à distance	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/> BranchCache - Client de mise en cache hébergé (utilise ...	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> BranchCache - Découverte d'homologue (utilise WSD)	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> BranchCache - Extraction du contenu (utilise HTTP)	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> BranchCache - Serveur de cache hébergé (utilise HTTPS)	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> Bureau à distance	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> Bureau à distance - RemoteFX	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> Communicateur réseau COM HP (HP Deskjet 3050 J610 ...	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> Communicateur réseau HP (HP Deskjet 3050 J610 series)	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> Configuration du périphérique HP (HP Deskjet 3050 J61...	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/> Connexion à un projecteur réseau	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> Coordinateur de transactions distribuées	<input type="checkbox"/>	<input type="checkbox"/>

Détails... Supprimer

Autoriser un autre programme...

# Pare feu Windows

## Pare-feu Windows avec fonctions avancées de sécurité sur Ordinateur local



Le Pare-feu Windows avec sécurité avancée offre une sécurité réseau pour les ordinateurs Windows.

### Vue d'ensemble

#### Profil de domaine

- ✓ Le Pare-feu Windows est activé.
- ✗ Les connexions entrantes qui ne correspondent pas à une règle sont bloquées.
- ✓ Les connexions sortantes qui ne correspondent pas à une règle sont autorisées.

#### Profil privé

- ✓ Le Pare-feu Windows est activé.
- ✗ Les connexions entrantes qui ne correspondent pas à une règle sont bloquées.
- ✓ Les connexions sortantes qui ne correspondent pas à une règle sont autorisées.

#### Le profil public est actif

- ✓ Le Pare-feu Windows est activé.
- ✗ Les connexions entrantes qui ne correspondent pas à une règle sont bloquées.
- ✓ Les connexions sortantes qui ne correspondent pas à une règle sont autorisées.

➔ [Propriétés du Pare-feu Windows](#)

### Démarrer

#### Authentifier les communications entre les ordinateurs

Créez des règles de sécurité de connexion afin de spécifier comment et quand les connexions entre les ordinateurs sont authentifiées et protégées à l'aide de la sécurité du protocole Internet (IPsec).

➔ [Règles de sécurité de connexion](#)

#### Afficher et créer des règles de pare-feu

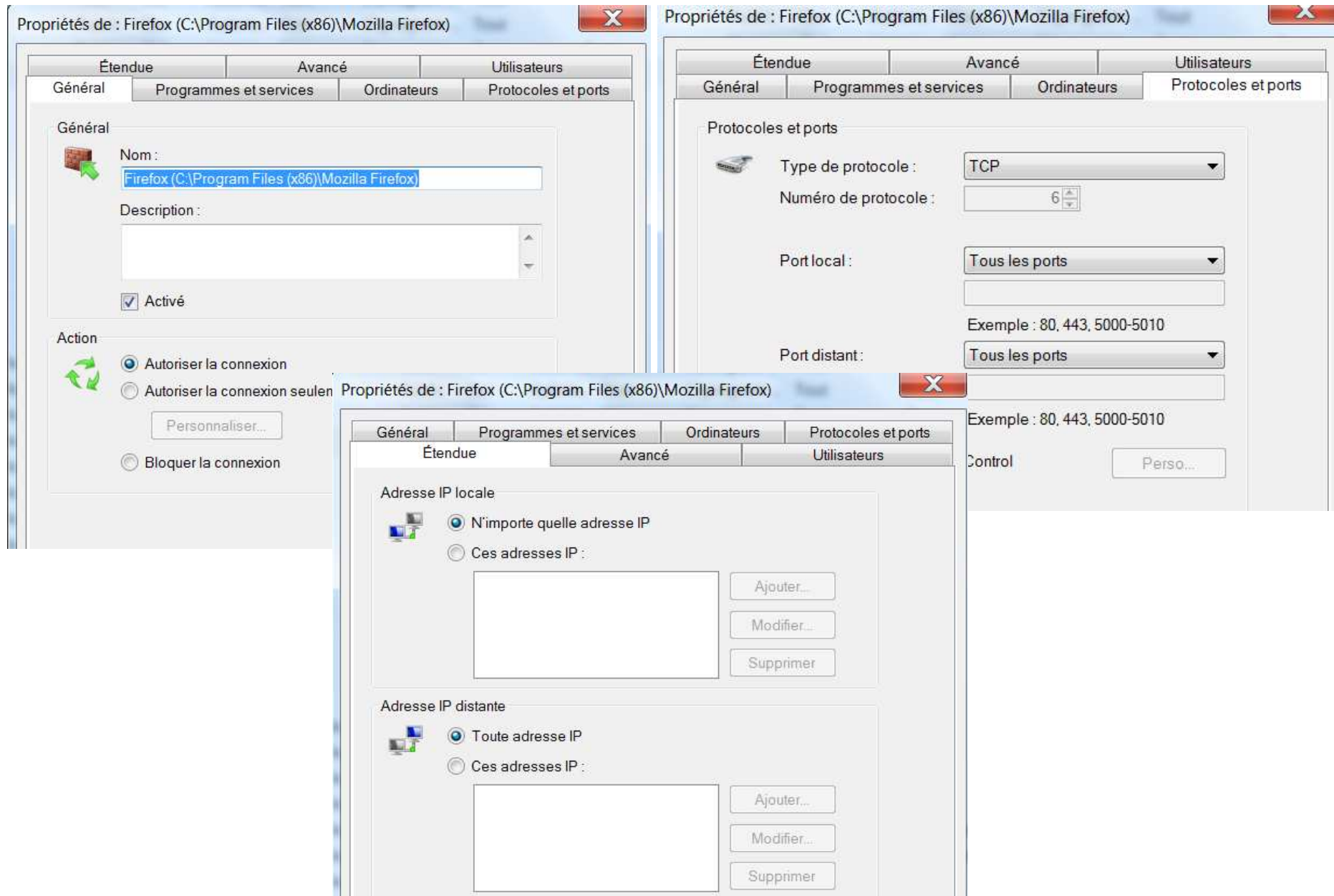
Créez des règles de pare-feu pour autoriser ou bloquer les connexions vers des programmes ou ports spécifiques. Vous ne pouvez autoriser une connexion que si elle est authentifiée ou si elle provient d'un utilisateur, groupe ou ordinateur autorisé. Par défaut, les connexions entrantes sont bloquées si elles ne satisfont pas à une règle qui les autorise, et les connexions sortantes sont autorisées si elles ne satisfont pas à une règle qui les bloque.

# Pare feu Windows

Règles de trafic entrant													
Nom	Groupe	Profil	Activ...	Action	Rempla...	Programme	Adresse loc...	Adresse dist...	Protocole	Port local	Port distant	Utilisateurs...	Ordinateu
✓ Communicateur réseau COM HP ...		Tout	Oui	Autoris...	Non	C:\Program ...	Tout	Sous-réseau...	Tout	Tout	Tout	Tout	Tout
✓ Communicateur réseau HP (HP ...		Tout	Oui	Autoris...	Non	C:\Program ...	Tout	Sous-réseau...	Tout	Tout	Tout	Tout	Tout
✓ Configuration du périphérique H...		Tout	Oui	Autoris...	Non	C:\Program ...	Tout	Sous-réseau...	Tout	Tout	Tout	Tout	Tout
✓ Finder		Public	Oui	Autoris...	Non	C:\program ...	Tout	Tout	TCP	Tout	Tout	Tout	Tout
✓ Finder		Public	Oui	Autoris...	Non	C:\program ...	Tout	Tout	UDP	Tout	Tout	Tout	Tout
✓ Firefox (C:\Program Files (x86)\...		Privé	Oui	Autoris...	Non	C:\Program ...	Tout	Tout	TCP	Tout	Tout	Tout	Tout
✓ Microsoft Office Outlook		Public	Oui	Autoris...	Non	C:\Program ...	Tout	Tout	UDP	6004	Tout	Tout	Tout
✓ Service Bonjour		Public	Oui	Autoris...	Non	C:\Program ...	Tout	Tout	TCP	Tout	Tout	Tout	Tout
✓ Service Bonjour		Public	Oui	Autoris...	Non	C:\Program ...	Tout	Tout	UDP	Tout	Tout	Tout	Tout
✓ Service Bonjour		Public	Oui	Autoris...	Non	C:\Program ...	Tout	Tout	TCP	Tout	Tout	Tout	Tout
✓ Service Bonjour		Public	Oui	Autoris...	Non	C:\Program ...	Tout	Tout	UDP	Tout	Tout	Tout	Tout
✓ Skype		Tout	Oui	Autoris...	Non	C:\Program ...	Tout	Tout	Tout	Tout	Tout	Tout	Tout
✓ Windows Explorer		Public	Oui	Autoris...	Non	C:\Windows...	Tout	Tout	TCP	Tout	Tout	Tout	Tout
✓ Windows Explorer		Public	Oui	Autoris...	Non	C:\Windows...	Tout	Tout	TCP	Tout	Tout	Tout	Tout
✓ Windows Explorer		Public	Oui	Autoris...	Non	C:\Windows...	Tout	Tout	UDP	Tout	Tout	Tout	Tout
✓ Windows Explorer		Public	Oui	Autoris...	Non	C:\Windows...	Tout	Tout	UDP	Tout	Tout	Tout	Tout
✓ Assistance à distance (DCOM-In)	Assista...	Dom...	Oui	Autoris...	Non	%SystemRo...	Tout	Tout	TCP	135	Tout	Tout	Tout
✓ Assistance à distance (DCOM-In)	Assista...	Dom...	Oui	Autoris...	Non	%SystemRo...	Tout	Tout	TCP	135	Tout	Tout	Tout
● Assistance à distance (PNRP-Entr...	Assista...	Public	Non	Autoris...	Non	%systemroo...	Tout	Tout	UDP	3540	Tout	Tout	Tout
✓ Assistance à distance (PNRP-Entr...	Assista...	Dom...	Oui	Autoris...	Non	%systemroo...	Tout	Tout	UDP	3540	Tout	Tout	Tout
✓ Assistance à distance (SSDP TCP ...	Assista...	Dom...	Oui	Autoris...	Non	%SystemRo...	Tout	Sous-réseau...	TCP	2869	Tout	Tout	Tout
✓ Assistance à distance (SSDP UDP...	Assista...	Dom...	Oui	Autoris...	Non	%SystemRo...	Tout	Sous-réseau...	UDP	1900	Tout	Tout	Tout
● Assistance à distance (TCP-Entrée)	Assista...	Public	Non	Autoris...	Non	%SystemRo...	Tout	Tout	TCP	Tout	Tout	Tout	Tout
✓ Assistance à distance (TCP-Entrée)	Assista...	Dom...	Oui	Autoris...	Non	%SystemRo...	Tout	Tout	TCP	Tout	Tout	Tout	Tout
✓ Assistance à distance (Trafic entr...	Assista...	Dom...	Oui	Autoris...	Non	%SystemRo...	Tout	Tout	TCP	Tout	Tout	Tout	Tout
● Découverte d'homologue de Bra...	Branch...	Tout	Non	Autoris...	Non	%systemroo...	Tout	Sous-réseau...	UDP	3702	Tout	Tout	Tout
● Extraction du contenu de Branch...	Branch...	Tout	Non	Autoris...	Non	SYSTEM	Tout	Tout	TCP	80	Tout	Tout	Tout
● Serveur de cache hébergé de Br...	Branch...	Tout	Non	Autoris...	Non	SYSTEM	Tout	Tout	TCP	443	Tout	Tout	Tout
● Bureau à distance (TCP-Entrée)	Bureau...	Tout	Non	Autoris...	Non	System	Tout	Tout	TCP	3389	Tout	Tout	Tout
● Bureau à distance - RemoteFX (T...	Bureau...	Tout	Non	Autoris...	Non	%SystemRo...	Tout	Tout	TCP	3389	Tout	Tout	Tout
● Connexion à un projecteur résea...	Connex...	Privé, ...	Non	Autoris...	Non	%SystemRo...	Tout	Sous-réseau...	TCP	Tout	Tout	Tout	Tout
● Connexion à un projecteur résea...	Connex...	Dom...	Non	Autoris...	Non	%SystemRo...	Tout	Tout	TCP	Tout	Tout	Tout	Tout
● Connexion à un projecteur résea...	Connex...	Privé, ...	Non	Autoris...	Non	System	Tout	Sous-réseau...	TCP	5357	Tout	Tout	Tout
● Connexion à un projecteur résea...	Connex...	Dom...	Non	Autoris...	Non	System	Tout	Tout	TCP	5357	Tout	Tout	Tout
● Connexion à un projecteur résea...	Connex...	Dom...	Non	Autoris...	Non	System	Tout	Tout	TCP	5358	Tout	Tout	Tout



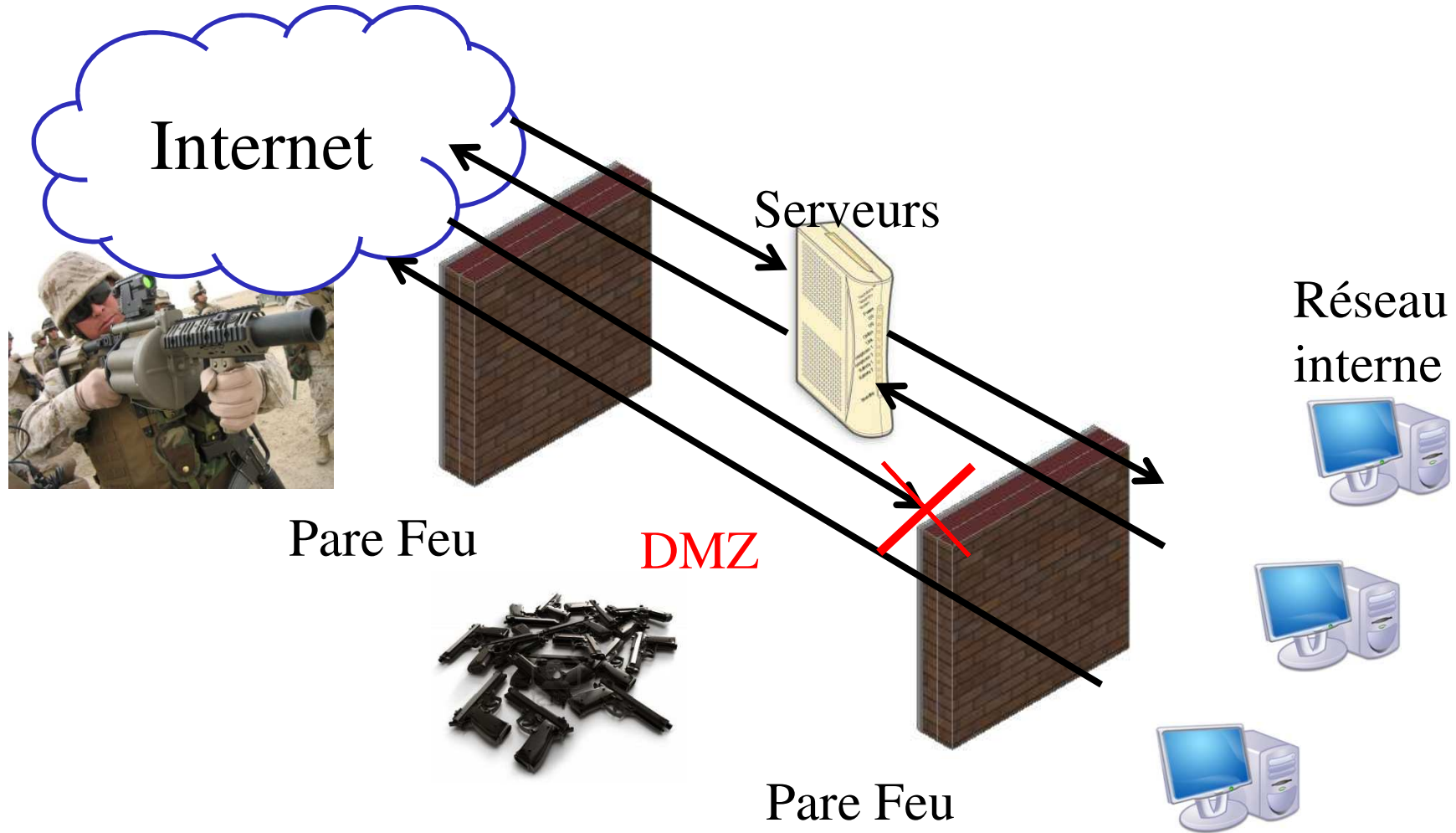
# Pare feu Windows



## 2 -Pare-feu ou firewall

Exemple d'utilisation des pare-feu

la DMZ (Zone Démilitarisée)



## 2 -Pare-feu ou firewall

Les réactions des firewalls aux attaques classiques :

### 1 - IP spoofing

L'IP spoofing consiste à modifier les paquets IP afin de faire croire au firewall qu'ils proviennent d'une adresse IP considérée comme « de confiance ». Les derniers firewalls peuvent offrir une protection contre ce type d'attaque, notamment en utilisant un protocole VPN, par exemple IPSec

## 2 -Pare-feu ou firewall

Les réactions des firewalls aux attaques classiques :

### 2 – DOS et DDOS

Les firewalls ici n'ont que peu d'utilité car une attaque DOS ou DDOS utilise le plus souvent des adresses sources différentes et souvent, impossible de distinguer ces paquets des autres...

Cette attaque brute reste un des gros problèmes actuels, car elle est très difficilement évitable.

## 2 -Pare-feu ou firewall

Les réactions des firewalls aux attaques classiques :

### 3 – Port scanning

Le firewall va, dans quasiment tous les cas, pouvoir bloquer ces scans en annonçant le port comme « fermé ».

### 4 – Virus

Le firewall n'est d'aucune utilité

## 2 -Pare-feu ou firewall

Les réactions des firewalls aux attaques classiques :

### 5 - Exploit

Il est quasiment impossible au firewall d'intercepter ces attaques, qui sont considérées comme des requêtes normales au système, mais exploitant un bug du serveur le plus souvent.

La seule solution est la mise à jour périodique des logiciels utilisés afin de barrer cette voie d'accès au fur et à mesure qu'elles sont découvertes.

## 3 -Proxy

Un proxy est un composant logiciel qui joue le rôle d'intermédiaire en se plaçant entre deux autres machines pour faciliter ou surveiller les échanges entre applications.

Dans le cas des réseaux informatiques, un proxy est un programme servant d'intermédiaire pour accéder à internet.

Les fournisseurs d'accès à internet (FAI) peuvent proposer des proxys pour la connexion de leurs abonnés.

Souvent, le fournisseur d'accès utilise un proxy transparent (sans configuration par l'utilisateur), pour réduire le nombre d'accès effectifs aux sites distants, mais aussi pour connaître les habitudes de navigation de leurs abonnés.

# 3 -Proxy

Les serveurs proxys sont notamment utilisés pour assurer les fonctions suivantes :

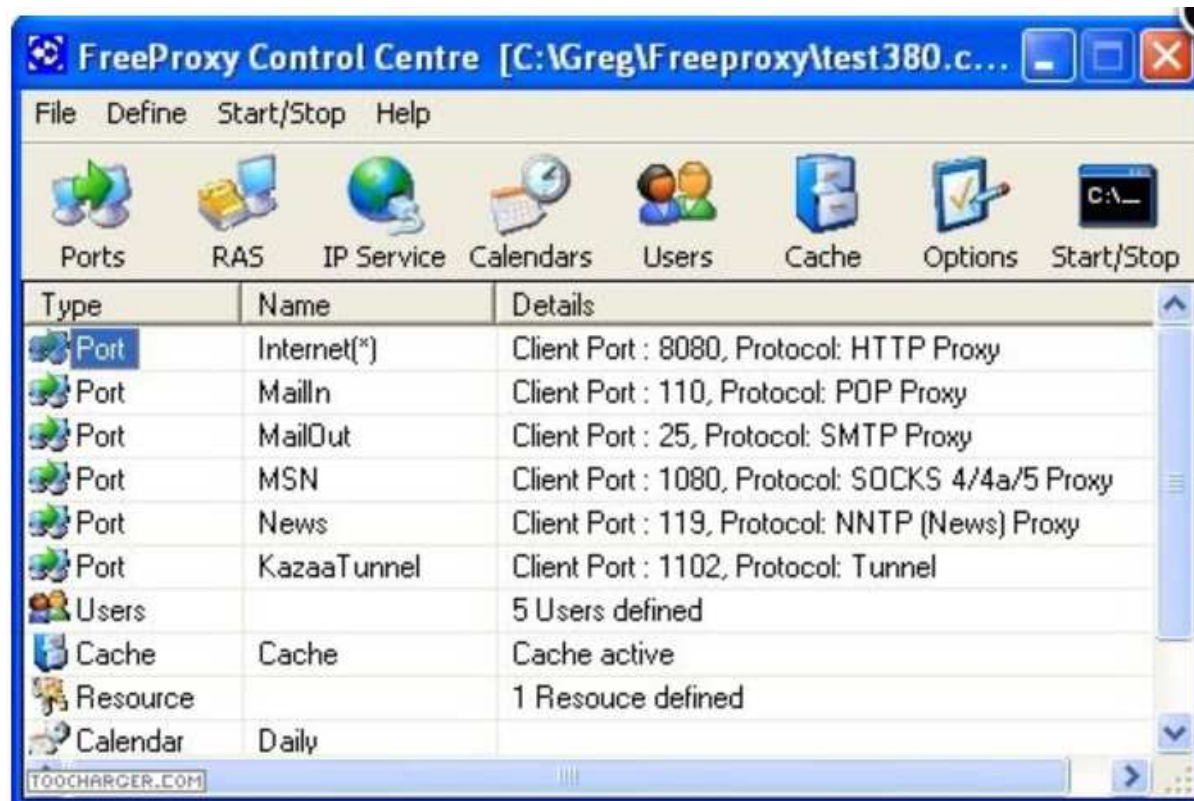
- accélération de la navigation : mémoire cache, compression de données, filtrage des publicités ou des contenus lourds (java, flash);
- journalisation des requêtes ;
- sécurité du réseau local ;
- filtrage et l'anonymat.



# 3 -Proxy

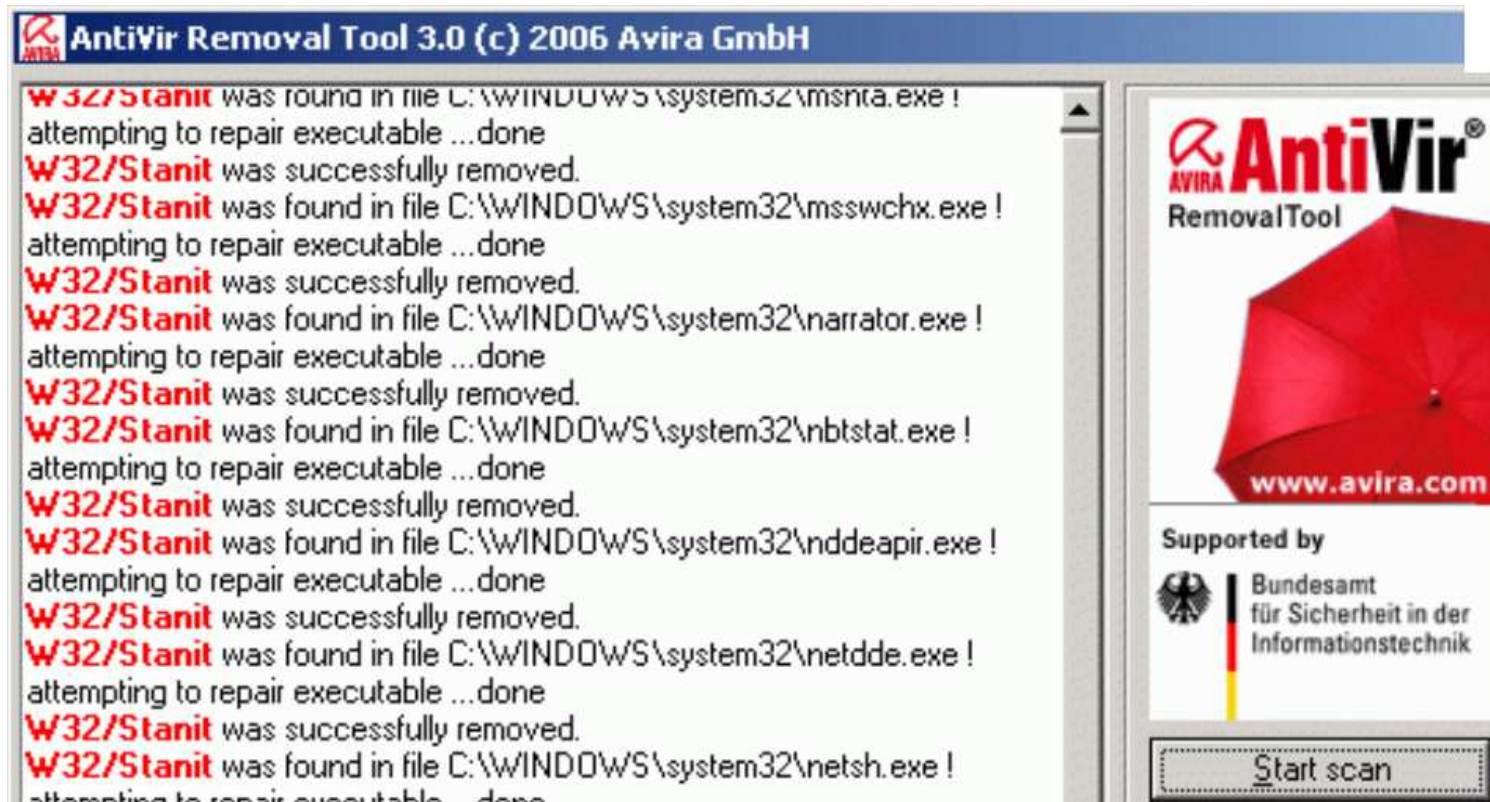
Proxy et sécurité :

Le Proxy fait office de « mémoire cache », il peut ainsi filtrer les requêtes en fonction de certaines règles.



## 4 - Anti-virus

Objectif : détecter et mettre hors d'état de nuire les virus



# 4 - Anti-virus

Il existe trois grandes techniques de détection :

- La signature ;**
- L'analyse heuristique ;**
- L'analyse de comportement .**

# 4 - Anti-virus

Techniques de détection :

## **-La signature :**

Principe = Analyser le disque dur à la recherche de la signature du virus, qui est présente dans la base de données du logiciel.

La signature est un morceau de code du virus qui permet de l'identifier.



# 4 - Anti-virus

Techniques de détection :

## **-La signature - Méthode :**

Rappel : Un virus est un programme exécutable.

A chaque nouvelle découverte de virus, les éditeurs d'antivirus enregistrent dans la base de données de leur logiciel ces codes appelés « signatures ».

Exemple : X5O!P%@AP[4\PZX54(P^)7CC)7}\$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!\$H+H\*

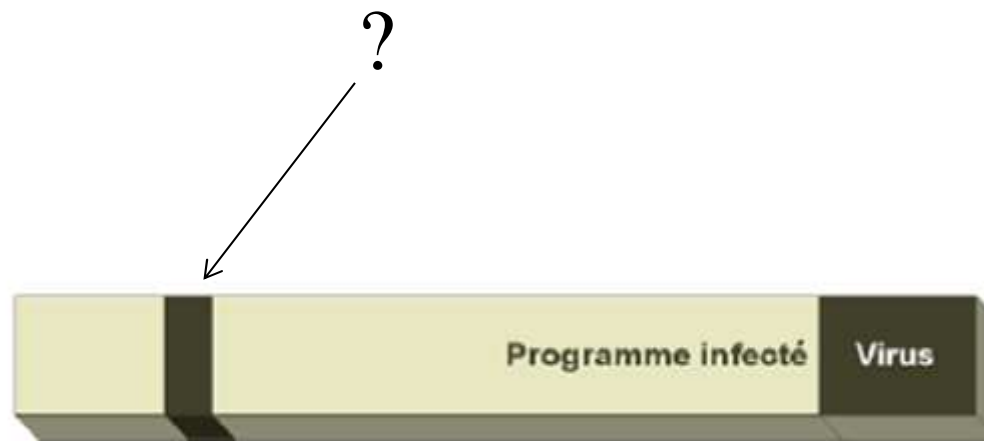
Il suffit alors de vérifier si le début du code du programme scanné est dans la base de données.

# 4 - Anti-virus

Techniques de détection :

**-La signature : La limite de cette méthode :**

Si un virus s'implante de manière aléatoire dans le programme (point d'entrée obscur) , il est pratiquement impossible de le détecter.



# 4 - Anti-virus

Techniques de détection :

## **-L'analyse heuristique :**

Cette méthode permet de détecter d'éventuels virus inconnus de l'antivirus.

Elle cherche à détecter la présence d'un virus en analysant le code d'un programme inconnu (en simulant son fonctionnement ).

L'analyse se base sur les codes des instructions en langage machine.

Exemple :      MOV AH, 01H  
                  INT 21H

# 4 - Anti-virus

Techniques de détection :

## **-L'analyse heuristique – Exemple :**

Au démarrage un programme normal commence par rechercher la ligne de commande des options.

Par contre les virus cherchent des fichiers exécutables pour se multiplier, essayent d'écrire directement sur le disque ou déchiffrent leur code qui était crypté à l'origine (dans le cas des virus polymorphes) etc..

Si l'antivirus détecte une application qui montre plusieurs anomalies (contenir un code permettant de formater le disque dur, par exemple), il déclenchera une alerte virus.



# 4 - Anti-virus

Techniques de détection :

## **-L'analyse heuristique : Limite de la méthode**

Si un programme légitime exécute des fonctions bas niveau il peut être pris pour un virus.

Cette méthode provoque parfois de fausses alertes voire peut bloquer un programme légitime.

## 4 - Anti-virus

Technique de détection :

- **L'analyse de comportement :**

L'antivirus actif surveille en permanence le comportement des logiciels en cours d'exécution.

Il analyse tous les fichiers modifiés et créés et en cas d'anomalie, il avertit l'utilisateur par un message explicite.

Cette méthode n'est jamais utilisée seule et vient en complément de l'une des deux premières.

## 4 - Anti-virus

Technique de détection :

**-L'analyse de comportement :**

**Exemple : Le contrôleur d'intégrité :**

Cet outil vérifie régulièrement certains éléments invariables des logiciels (comme la taille, la date de création etc..).

La modification de ces données est le signe de la présence d'un virus.

## 4 - Anti-virus

Techniques de détection :

### **-L'analyse comportement : Limite de la méthode**

Même problème que pour le cas précédent, si un programme légitime exécute des fonctions bas niveau (changement de date, changement de propriétaire, ...) il peut être pris pour un virus.

Cette méthode provoque parfois de fausses alertes voire peut bloquer un programme légitime.

# 4 - Anti-virus

Techniques de correction :

**-Réparation du fichier :** L'antivirus doit être capable de réparer un fichier atteint. Mais ce n'est pas toujours possible.

**-Suppression du fichier :** L'antivirus peut supprimer les fichiers infectés si vous le demandez, s'il n'est pas capable de le faire il est conseillé de supprimer manuellement.

**-Mise en quarantaine :** C'est une solution d'attente dans le cas où le fichier ne peut être réparé. L'antivirus place le fichier dans un dossier sûr du disque dur en attendant de pouvoir faire la réparation.

# 4 - Anti-virus

Limites des anti-virus :

- La signature n'est connue que lorsque le virus s'est diffusé,
- La détection d'un virus dans un programme exécutable n'est possible que si l'on connaît leurs caractéristiques,
- L'apparition des virus polymorphes, qui changent de signature à chaque infection. Ce type de virus est difficilement détectable à l'aide des signatures,
- Les antivirus ralentissent le système.

## 4 - Anti-virus

En conséquence :

→ Il est nécessaire d'actualiser en permanence les anti-virus.

→ Un antivirus ne peut assurer seul la sécurité de l'ensemble du système d'information, des mesures techniques et humaines doivent également l'accompagner.

## 5 - Anti-spyware

La principale difficulté avec les spywares est de les détecter.

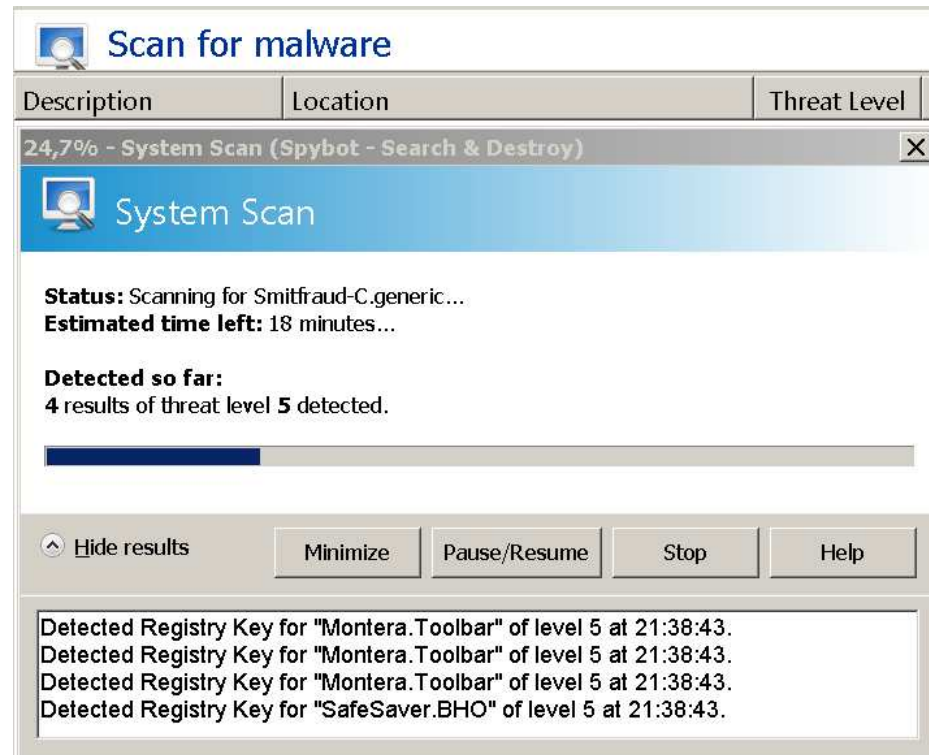
La meilleure façon de se protéger est encore de ne pas installer de logiciels dont on n'est pas sûr à 100% de la provenance et de la fiabilité (notamment les freewares, les sharewares et plus particulièrement les logiciels d'échange de fichiers en peer-to-peer).

La solution consiste à traiter les « spywares » comme des virus et à installer des logiciels, nommés **anti-spywares** permettant de détecter et de supprimer les fichiers, processus et entrées de la base de registres créés par des spywares.



# 5 - Anti-spyware

Les antispywares sont conçus comme les antivirus, ils travaillent sur la base de signatures.

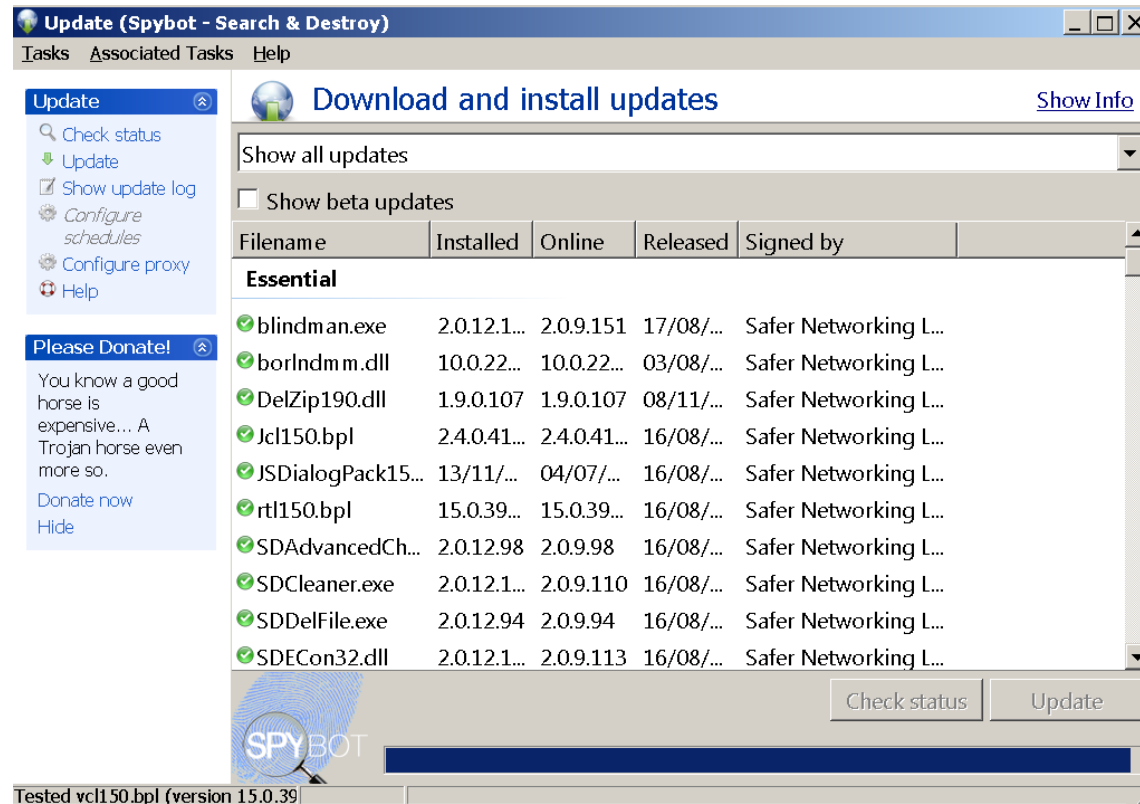


Ces protections, permettent de détecter un spyware même s'il n'est pas actif, mais restent dépendantes de la mise à jour du fichier des signatures.

Cependant , il n'est pas recommandé d'utiliser plusieurs logiciels de détection ou de désinfection car cela augmente les risques de plantage et de ralentissement de l'ordinateur.

# 5 - Anti-spyware

À l'instar des antivirus, les logiciels anti-espions utilisent des bases de données fréquemment mises à jour . Cependant certaines mises à jour restent manuelles.



# 5 - Anti-spyware

La plupart des anti-spywares gratuits (comme Ad-Aware ou Spybot - Search & Destroy) sont bridés dans leur version gratuite (pas de protection en temps réel par exemple).



Certains anti-spywares payants (comme Terminator, Spyware Doctor, Webroot, etc.), sont aussi complets que les antivirus classiques.

## 6 – L'Anti-spam

★	🔍	📧	Sujet	⏮	⏭	🔥	Date	Expéditeur
☆			*** SPAM possible *** (score = 20.3) *** 【無料】4月度の、投資モニターを募集します。	•	🔥		01/04/2014 15:27	ご参加ください
☆			*** SPAM possible *** (score = 30.2) *** こすこいわwwIDもアドレスも丸見えww skzpoivrojqt	•	🔥		03/04/2014 09:11	ebsfxziejxgim@softbank.ne.jp
☆			*** SPAM possible *** (score = 32.2) *** マジですこいとこ見つけたんだけどwww sffdaot	•	🔥		03/04/2014 15:05	ausyoewsdex@ezweb.ne.jp
☆			*** SPAM possible *** (score = 33.3) *** マジですこいとこ見つけたんだけどwww sspjeekpvt	•	🔥		03/04/2014 12:20	mhtukqprdg@docomo.ne.jp
☆			*** SPAM possible *** (score = 37.5) *** これはマジですこいわwww sndbwquvtdwdzrt	•	🔥		03/04/2014 09:25	jvboaleazghuw@docomo.ne.jp
☆			*** SPAM possible *** (score = 45.8) *** これは...アドもIDも丸見えとかヤバ過ぎ!! scbkwckpjfkmzit	•	🔥		03/04/2014 10:26	hvvhi@ezweb.ne.jp
☆			*** SPAM possible *** (score = 6.9) *** Re: OMG ... C'est incroyable	•	•		01/04/2014 14:27	Sarah

Les technologies antispam, se basent sur les éléments disponibles lors de la réception d'un email :

- Le serveur de messagerie,
- L'adresse IP,
- Le protocole SMTP ,
- Le port TCP/25.

# 6 – L'Anti-spam

## **Quelques remarques sur ces champs :**

1 - L'IP émettrice du serveur: permet d'identifier le pays émetteur, ainsi que le propriétaire de l'IP (souvent le FAI).

2 - Dans le protocole SMTP , le champ HELO, est utilisé par le serveur de messagerie lors de l'initialisation de la communication pour indiquer son nom complet : exemple : `"/etc/hosts"`.

3 – L'adresse email et nom de domaine émetteur: L'adresse email émettrice n'a que très peu d'intérêt dans la détection d'un spam, mais le domaine émetteur permet d'effectuer quelques vérifications ou de pouvoir véhiculer via le DNS quelques informations utiles.

## 6 – L'Anti-spam

4 – L'en-tête du mail : Au niveau de la détection antispam, les champs les plus intéressants sont : "Received", "Subject", "Message-Id" et "Date". Pour rappel, le champ "Received" assure la traçabilité d'un email : chaque serveur par lequel un mail transite ajoute un champ "Received", en indiquant au minimum l'identifiant interne du message, le serveur d'origine du mail et la date de traitement.

**→ A partir de ces divers éléments d'identification d'un message, différentes technologies de détection ont été développées.**

# 6 – L'Anti-spam

## **Analyse heuristique**

Constitue un ensemble de règles représentées sous forme d'expressions régulières. Elle permet de rechercher les mails dont les entêtes et/ou les corps correspondent à des caractéristiques très particulières connues pour avoir une forte probabilité d'être un spam.

## **Listes noires**

Sont des listes de serveurs ou de réseaux connus pour accueillir, produire ou retransmettre des spams ou fournir un service pouvant être utilisé comme support pour l'expédition de spam : OpenSMTP Relay, Open Proxy List (OPL).

# 6 – L'Anti-spam

## **Bases collaboratives de spams**

Ce sont des bases de signatures de spams, utilisées de la même manière que les bases de signatures de virus. Ces bases sont alimentées par les utilisateurs de solutions antispam.

## **Enregistrement DNS**

Vérifie la corrélation entre l'adresse IP du serveur source et son nom via une requête DNS inverse (in-addr.arpa).



# 6 – L'Anti-spam

## **Filtres bayésiens**

Méthode probabiliste de filtrage des courriers électroniques fonctionnant par apprentissage. Ce type d'algorithme s'auto-adapte en s'appuyant sur l'analyse des emails connus comme étant ou n'étant pas des spams.

## **Liste blanche**

Liste de sites, hôtes, domaines ou adresses sûres. Mais par défaut très peu d'hôtes sont considérés comme sûrs car leurs adresses peuvent être usurpées par les spammeurs.

# 6 – L'Anti-spam

## **Historique des transactions**

Des individus ayant l'habitude de s'envoyer des emails légitimes, n'ont pas de raison de s'envoyer des spams.

## **Adresses URL**

Cette technique consiste à rechercher dans le mail des URL de sites suspects et/ou des url suspectes

# 6 – L'Anti-spam

## **OS fingerprint**

Consiste à reconnaître le système d'exploitation utilisé par le serveur émetteur, par analogie d'empreinte des trames émises par le système distant. Combinée à l'analyse comportementale du serveur distant, cette technique permet de retrouver les spams émis par des botnet. (Ensemble de pc zombies exploités de manière malveillante).

## **Analyse des images et des PDF**

Consiste à examiner les propriétés des images et les fichiers PDF contenus dans un email (nombre, type, taille, format et dimensions) et à les comparer aux caractéristiques d'images utilisées par les spammeurs.

# 6 – L'Anti-spam

## **Le greylisting**

Technique très récente qui consiste à rejeter temporairement un message, par émission d'un code de refus temporaire au serveur émetteur. Le serveur émetteur réexpédie le mail après quelques minutes, la plupart des serveurs de spams ne prennent pas cette peine!

# 6 – L'Anti-spam

## Quelques Anti-spam connus

SpamAssassin : analyse les entêtes, le texte, le filtre Bayezien, des listes de blocage DNS, des bases de données collaboratives de filtrages et d'autres techniques pratiques.

SpamBayes : se concentre sur les filtres Bayeziens.

ASSP – Création automatique de listes blanches, il propose aussi des filtres Bayesiens.

SPAMfighter : créé une liste noire d'adresses et de domaines, ainsi qu'une liste blanche. Procède aussi par analyse heuristique.

Vade retro : Liste noire et liste blanche avec importation/exportation  
Mise en place de règles personnalisées (e-mails, domaine, expéditeur)

# 6 – L' Anti-spam

## **Limites des Anti-spam**

Bien que le but général de ces technologies est d'identifier de manière la plus correcte possible si le message reçu est un spam, certaines de ces technologies apportent de la crédibilité à l'émetteur mais ne permettent pas pour autant de qualifier le message.

D'autre part, chacune de ces technologies ne donne pas les mêmes résultats en termes de détection et d'erreur d'analyse.

# 6 – L'Anti-spam

## En conclusion

La « lutte » contre le Spam est difficile , on peut cependant le limiter en adoptant quelques principes :

- Utiliser un logiciel anti-spam qui lui aussi filtre les messages à partir de mots clés.
- Ne donner l'adresse e-mail qu'à des personnes de confiance et utiliser une seconde adresse « fictive » que l'on diffuse.
- Supprimer les messages dès leur arrivé dans la boite aux lettres en utilisant les filtres du logiciel de messagerie.

## 7 -Suppression des fichiers de travail

Pour des raisons de performances le système garde dans une multitude de fichiers toute l'activité du système et en particulier les traces des visites des sites web.

Il convient de supprimer régulièrement ou de réduire l'espace de stockage des fichiers qui suivent :

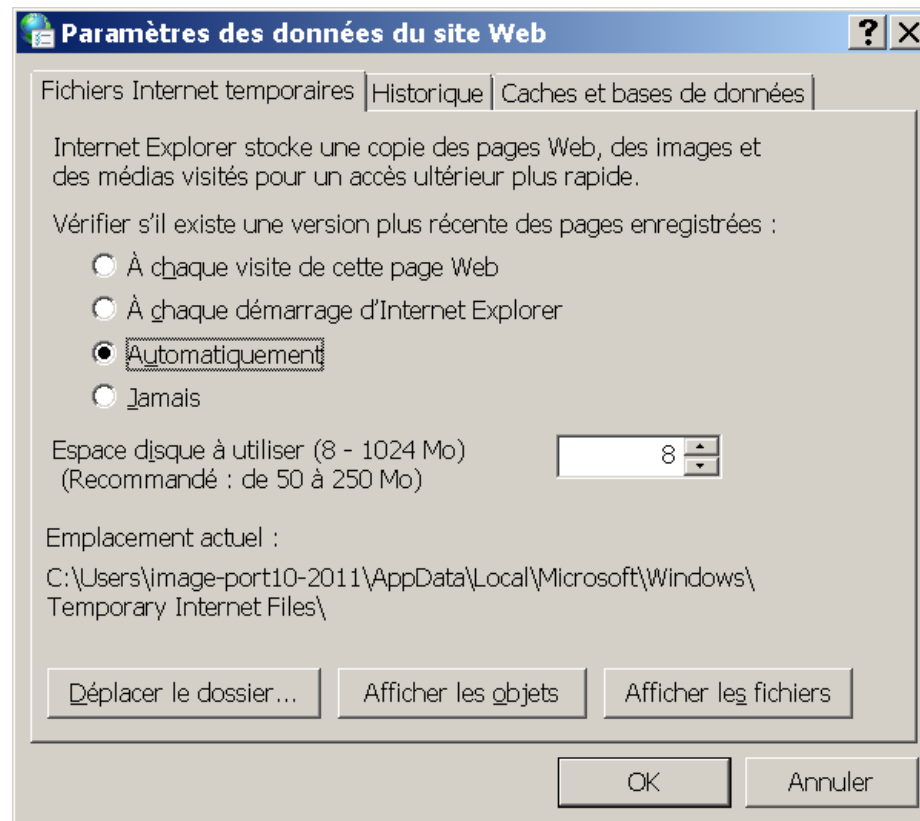
- Les fichiers temporaires d'internet
- L'historique du navigateur internet
- Les cookies
- La saisie semi-automatique
- Les favoris



# 7 -Suppression des fichiers de travail

Avant tout il est recommandé de paramétrer les « caches » utilisées par le web

Exemple : panneau de configuration → options d'internet



# 7 -Suppression des fichiers de travail

Pour vider ces caches, plusieurs techniques existent :

## 1 - Vider systématiquement la corbeille

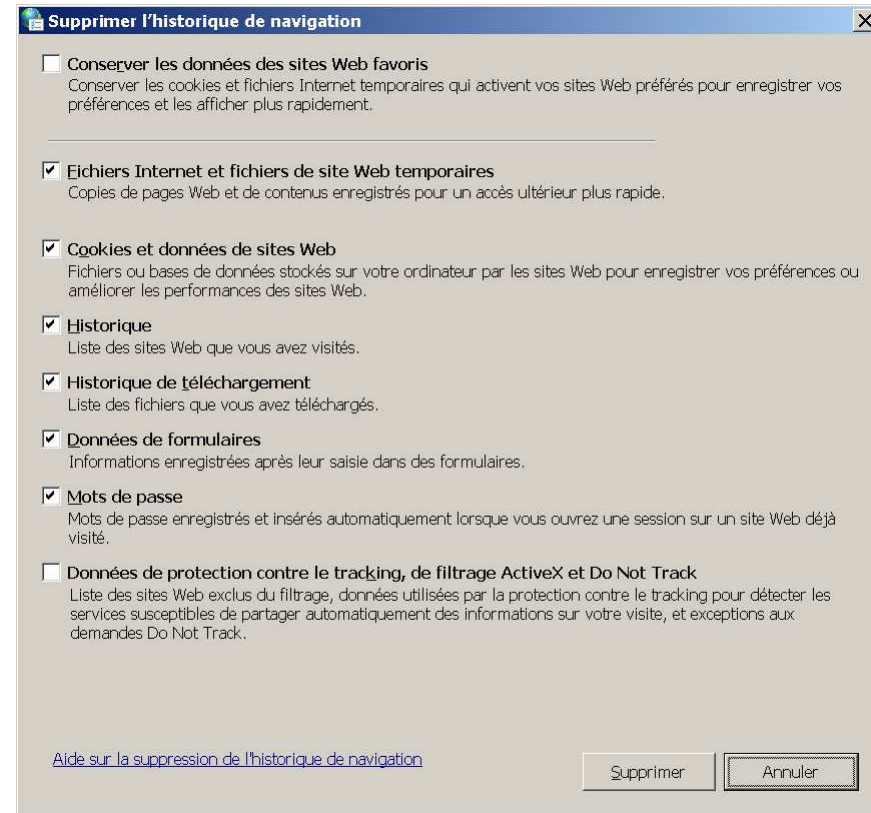


# 7 -Suppression des fichiers de travail

## 2 - Supprimer les fichiers de travail via le système.

Il est possible de choisir les types de fichiers à supprimer →

Et aussi de supprimer les fichiers issus de la navigation



### Historique de navigation

Supprimer les fichiers temporaires, l'historique, les cookies, les mots de passe enregistrés et les données de formulaires Web.

☒ Supprimer l'historique de navigation en quittant le navigateur

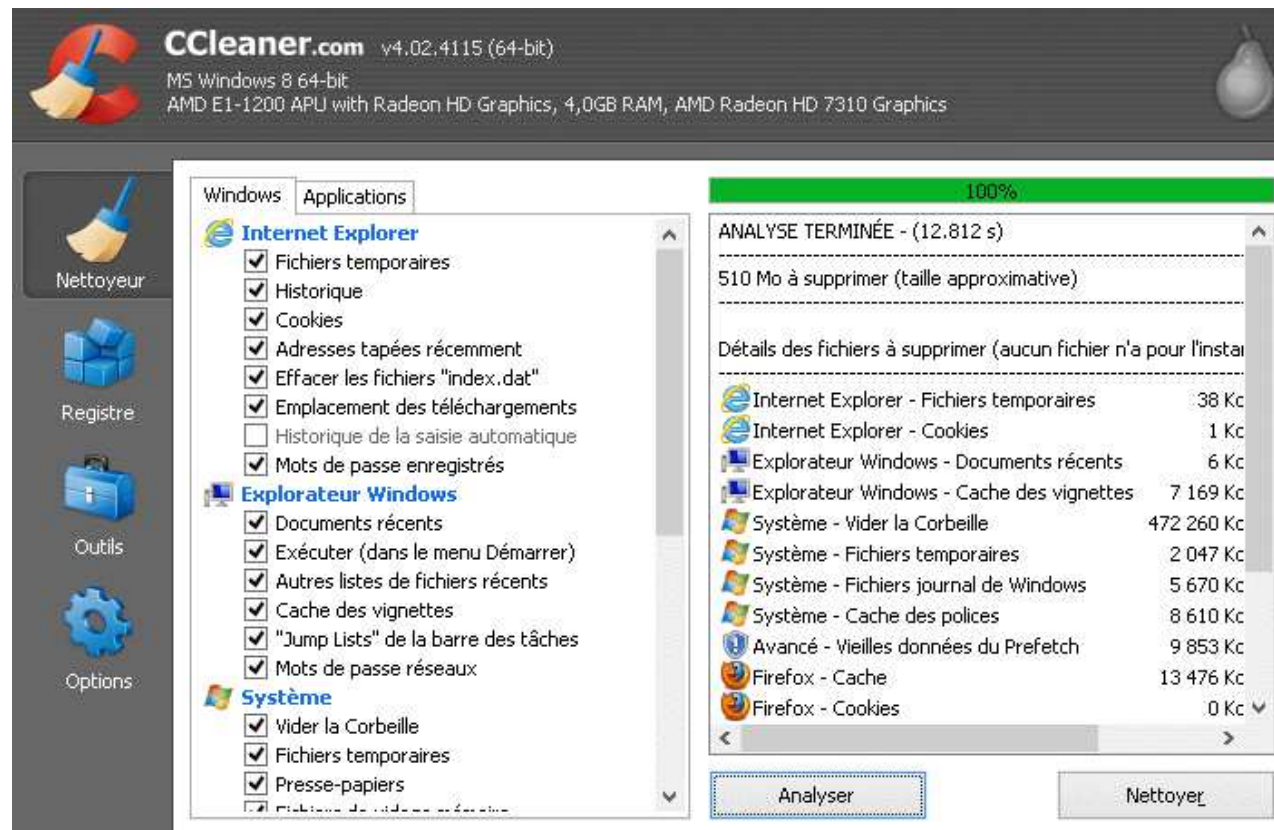
Supprimer...

Paramètres

# 7 -Suppression des fichiers de travail

## 3 - Utiliser des logiciels du marché

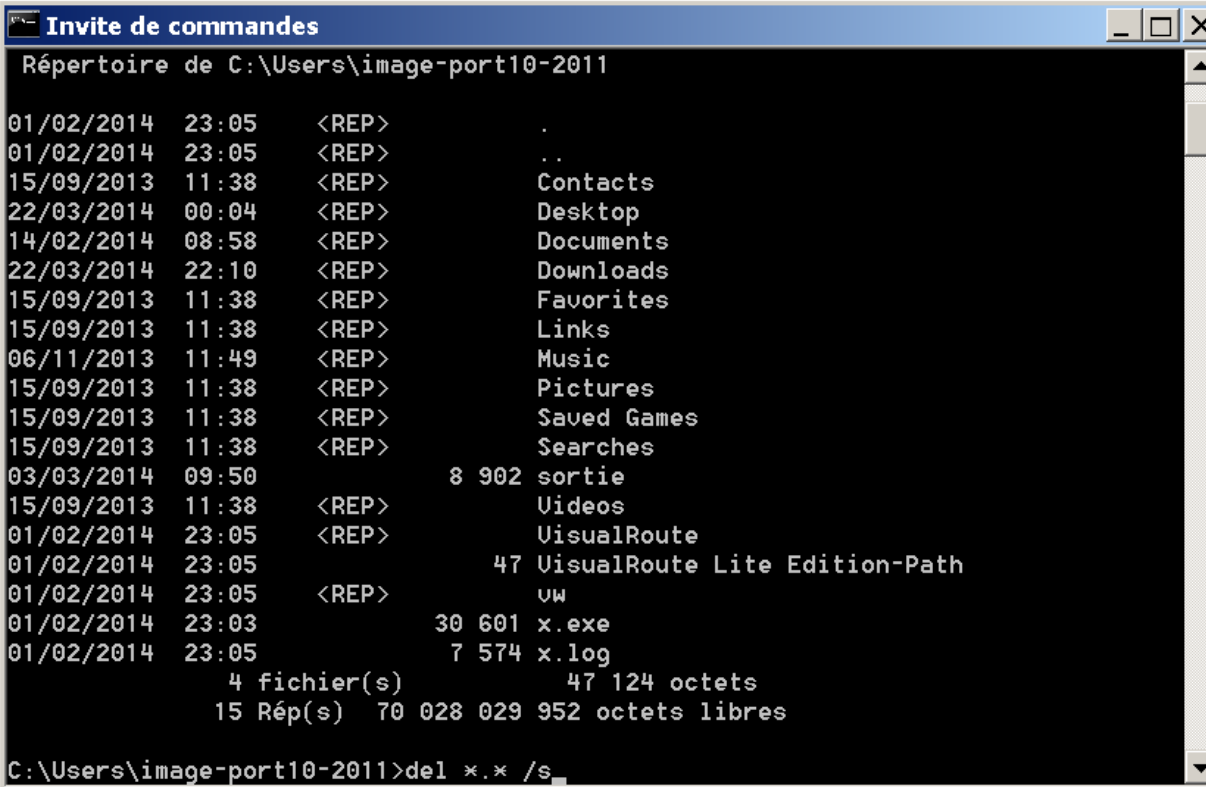
Comme Ccleaner qui proposent de choisir les de fichiers à supprimer.



# 7 -Suppression des fichiers de travail

## 4 - Le faire manuellement

Cette technique reste la meilleure, encore faut-il connaître les commandes de base du système et savoir quels fichiers supprimer...



```
Invite de commandes
Répertoire de C:\Users\image-port10-2011

01/02/2014  23:05    <REP>      .
01/02/2014  23:05    <REP>      ..
15/09/2013  11:38    <REP>      Contacts
22/03/2014  00:04    <REP>      Desktop
14/02/2014  08:58    <REP>      Documents
22/03/2014  22:10    <REP>      Downloads
15/09/2013  11:38    <REP>      Favorites
15/09/2013  11:38    <REP>      Links
06/11/2013  11:49    <REP>      Music
15/09/2013  11:38    <REP>      Pictures
15/09/2013  11:38    <REP>      Saved Games
15/09/2013  11:38    <REP>      Searches
03/03/2014  09:50      8 902 sortie
15/09/2013  11:38    <REP>      Videos
01/02/2014  23:05    <REP>      VisualRoute
01/02/2014  23:05      47 VisualRoute Lite Edition-Path
01/02/2014  23:05    <REP>      vw
01/02/2014  23:03     30 601 x.exe
01/02/2014  23:05      7 574 x.log
               4 fichier(s)             47 124 octets
              15 Rép(s)  70 028 029 952 octets libres

C:\Users\image-port10-2011>del *.* /s
```

## 8 – Sauvegarde des données

Suite à une attaque, un crash système, une défaillance matérielle, seule une sauvegarde permet de restaurer entièrement le système dans son état originel

Encore faut-il qu'elles soient bien faites !

Faire de bonnes sauvegardes consiste à :

- Bien paramétrer son outil,
- L'utiliser de manière correcte,
- Protéger ses sauvegardes.

→ Il est nécessaire de s'imposer quelques règles élémentaires

# 8 - Sauvegarde des données

## **1 – Ne pas tout sauvegarder à chaque fois**

Tout n'est pas important à sauvegarder à chaque instant, comme par exemple le système et les applications.

Ainsi, il peut être judicieux d'effectuer une sauvegarde quotidienne des données importantes et une sauvegarde mensuelle (si possible bootable) du système.

La sauvegarde bootable du système permettra une restauration automatique de celui-ci. La sauvegarde des données permettra leur restauration à tout instant.

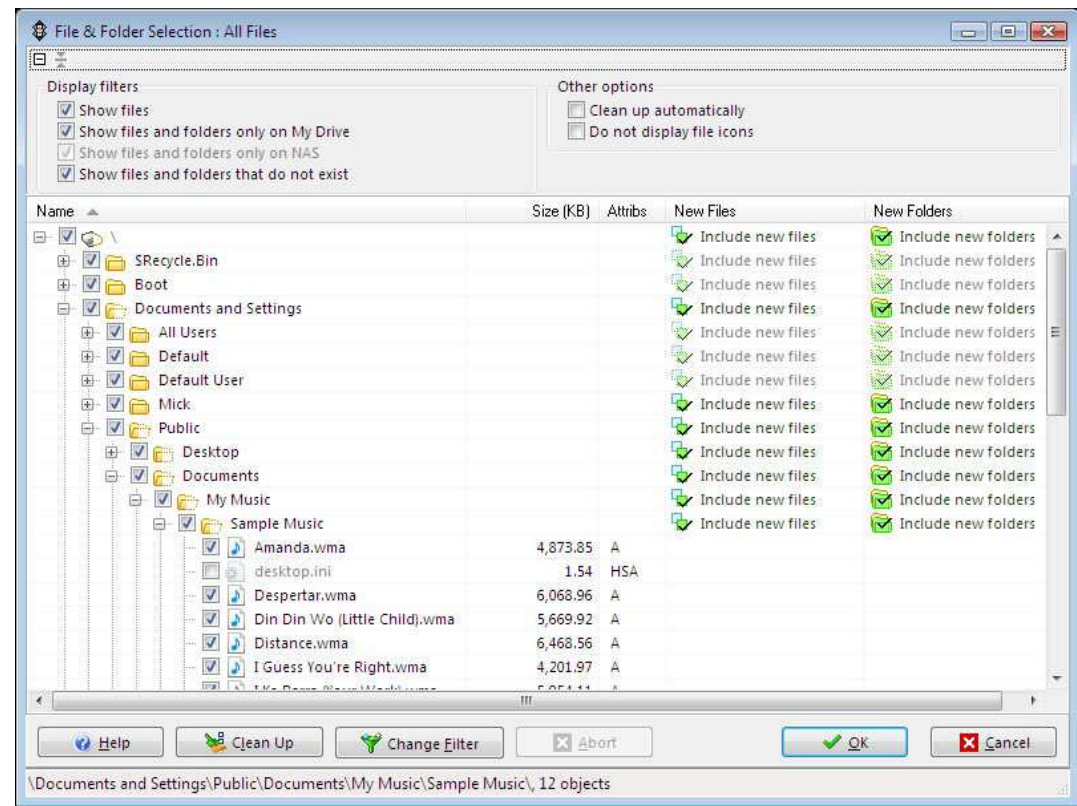
# 8 - Sauvegarde des données

## 2 – Ne pas oublier de données dans la sauvegarde

La plus part des logiciels de sauvegarde sont paramétrables.

Le paramétrage est souvent difficile pour un non initié, ce qui génère souvent des oublis.

Par exemple la messagerie.





# 8 - Sauvegarde des données

## 3 - Faire des sauvegardes régulières.

Il faut faire des sauvegardes quotidiennes des données de travail ou du moins à chaque fois que des modifications ont été faites.

Problème : Le volume des données à sauvegarder est important et la copie est très longue.

Solutions :

- Les sauvegardes incrémentales
- Le CDB (Continus Data Backup), sauvegarde permanente.

# 8 - Sauvegarde des données

## 4 - Faire des sauvegardes fiables.

La fiabilité des sauvegardes dépend de la qualité du support et des vérifications faites.

Dans la sauvegarde effectuée, on doit vérifier deux choses :

- le contenu de cette sauvegarde pour les supports CD et DVD : on se méfiera des lecteurs , certains sont mal réglés et sont alors les seuls à pouvoir relire ce qu'ils ont écrit.
- la lisibilité du support : Il suffit de relire le support après la copie. Il est conseillé de faire cette opération sur un machine différente.

# 8 - Sauvegarde des données

## **5 – Protéger les sauvegardes.**

Les sauvegardes qui sont conservées à proximité de la machine représentent un risque en cas de vol, d'incendie, inondations, ...

Il est important de les stocker dans un lieu différent de la machine.

Certaines entreprises font systématiquement deux copies. L'une reste sur le site et l'autre est transférée sur un site différent.

Toutes ces procédures étant lourdes à mettre en place, depuis des années se sont développées des solutions de sauvegarde à distance.

# 8 - Sauvegarde des données

## **Les sauvegardes à distance.**

Après configuration , ce type de sauvegarde ne nécessite plus aucune manipulation de la part de l'utilisateur de la machine, elles réalisent de manière automatique une copie des données du système sur une machine distante (data center)

Il existe aujourd'hui plusieurs solutions de sauvegarde à distance :

- Mozy (Dell)
- Iperius Backup
- Norton Online Backup
- BullGuard
- IBM Tivoli

Exemple de tarif (mozy) : 10€/mois 10Go à 50€/mois 100 Go

# 8 - Sauvegarde des données

## **Les sauvegardes sur le « Cloud »**

Ce type de service se développe mais attention au prix :

**Amazon cloud drive** : 70 €/an espace illimité

**Dropbox** : 30€/mois 2 To de stockage, 45 €/mois espace illimité

**Google Drive** : 9,99€/mois 1 To : 19,99/mois 2 To : 99,99€/mois 10 To

**Hubic OVH** : 10€/an 100 Go : 50€/an 10To

**OneDrive (Microsoft)** : 5€/mois 1To : 10€/mois illimité