# POLITIQUE DE FILTRAGE

---

Le présent document définit les règles et procédures à mettre en place dans la gestion des flux de données informatiques. Le filtrage mis en place est réalisé par les firewalls.
Document en version 0.1
Guillaume LEHMANN - 23/05/2003

---

## 1 Définition d'un périmètre de sécurité :

La politique de filtrage va autoriser ou interdire les utilisations de certains services. Pour cela, des firewalls sont disposés aux points d'interconnexion des divers réseaux, et vont filtrer les trames. Ce filtrage va aussi permettre de limiter la diffusion de programmes ou services illicites (virus, logiciels P2P, ...). Par conséquent, la politique de filtrage est techniquement mise en place dans le coeur et la périphérie du réseau informatique de l'organisme, pour filtrer l'utilisation du réseau qu'en font des utilisateurs (internes et externes).

## 2 Besoins :

Le filtrage doit être effectué au niveau de tous les points de routage importants du réseau. Il est également possible de mettre en place des pare-feux personnels :

– **Les points d'entrées/sorties vers Internet :** Ce sont les passerelles vers Internet qui sont généralement de simples routeurs. Il faut que ces routeurs offrent en plus la possibilité de faire du filtrage. Le filtrage mis en place doit être le plus restrictif possible, aussi bien au niveau paquet qu'au niveau suivi de session.

  **Bien identifier les accès vers Internet, et y filtrer les flux.**

– **Les entrées/sorties de VPN :** Les VPN permettent de contourner toutes les solutions de sécurité qui effectuent un contrôle des données, de par le cryptage et l'adressage IP. Ce sont des réseaux point-à-points que l'on établira de préférence entre une paire de routeurs dont au-moins un sera filtrant (routeur-firewall). Cela est d'autant plus important lorsque les VPN sont utilisés par des utilisateurs nomades, depuis Internet.

  **Créer des VPN seulement de firewalls à firewalls, ou entre un routeur et un firewall.**

– **Les ponts d'un réseau sûr à un réseau non sûr (wifi, DMZ, ...) de l'organisme :** Ceci permet de compartimenter un minimum le réseau local de l'organisme. Cela permet de réduire les attaques internes (la plupart des attaques viennent de l'intérieur du réseau local) et la propagation d'incidents de sécurité (virus, troyens, ...). De plus, certains réseaux de part leurs architectures, ou leurs utilisateurs, sont par définition moins sûr (réseau en DHCP, WIFI, ...) et ne peuvent être mieux sécurisés. Ces réseaux sont malgré tout intégrés au réseau de l'organisme, mais sont à considérer comme présentant autant de danger qu'Internet (aucun contrôle réel ne peut être effectué).

  **Après étude des besoins de chaque réseau, et de l'(in)adéquation entre leurs utilisations, étudier la nécessité de filtrer les flux échangés. Documenter les problèmes d'un réseau donné (problèmes de sécurité éventuels, technologies employées, contraintes, ...).**

– **Les points d'interconnexion entre deux réseaux différents :** Nous définisons 2 réseaux différents lorsque les profils utilisateurs sont différents d'un réseau à l'autre, adresses réseaux différentes, ou encore lorsque la sensibilité face à une attaque précise n'est pas la même.

  **Après étude des besoins de chaque réseau, et de l'(in)adéquation entre leurs utilisations, étudier la nécessité de filtrer les flux échangés. Bien identifier les points d'interconnexion entre ces réseaux, pour que le filtrage ne puisse être contourné par reroutage.**

– **Les postes de travail :** Nous définissons ici les ordinateurs personnels ou à la disponibilité du public. Les utilisateurs peuvent installer des applications offrant ou permettant d'accéder à des services non autorisés par la politique de sécurité. L'installation d'un firewall personnel permettra de bien compléter la protection. De plus, ces firewall personnels apportent un filtrage au niveau application, très difficile à mettre en place sur un routeur pour la globalité du réseau.

  **La mise en place d'un firewall personnel diminue beaucoup la propagation des virus et des troyens, et les attaques en internes (et externes) sur les systèmes sont pratiquement toutes bloquées**.

# 3 Procédures :

## 3.1 Installation d'un nouveau firewall :

Un manuel d'installation du firewall a préalablement été écrit. Il explique comment :
– installer/configure/sécuriser le système d'exploitation,
– installer/configurer/sécuriser le module de filtrage,
– ouvrir/fermer le filtrage automatiquement,
– mettre en place du filtrage et que celui-ci soit opérationnel dès le démarrage de la machine, sans intervention,
– administrer le firewall.

## 3.2 Modification des règles de filtrage d'un ou plusieurs firewall :

Archiver l'ancien ficher de configuration (date), indiquer dans le nouveau script de configuration même, la modification effectuée, et la date (le script doit garder un historique des modifications). Mettre à jour la fiche du firewall, tester le filtrage du firewall. Voir si cette modification a des répercutions importantes sur la politique de filtrage globale.

## 3.3 Un utilisateur demande l'ouverture d'un port :

Étudier l'utilité du service autorisé. Si le service ne peut être autorisé (car diminuant trop le niveau de sécurité global du site) avertir l'utilisateur par email en expliquant le pourquoi. Archiver la demande et la réponse. S'il est par contre utile d'autoriser ce service, archiver la demande et la réponse (qui indiquera simplement à l'utilisateur que sa demande est prise en compte), et appliquer la procédure *Modification des règles de filtrage d'un ou plusieurs firewall*.

## 3.4 Un nouveau ver ou troyen vient d'être découvert (réseau non encore contaminé) :

Ignorer l'alerte si le système d'information n'est pas sensible. Dans le cas contraire, si le firewall peut bloquer ce ver ou troyen, modifier les règles de filtrage. Puis appliquer la procédure*Modification des règles*

*de filtrage d'un ou plusieurs firewall*. Dans le cas contraire, le relais doit être pris par la *protection antivirale*.

### 3.5 Mise en place d'un nouveau firewall :

Prendre en compte sa mise en place au niveau de la *politique de filtrage*, mais aussi dans la *politique d'architecture*.

### 3.6 Un firewall apparaît comme corrompu :

Plusieurs aspects se présentent :
- Le filtrage interdit tout : Remplacer le firewall par un firewall de secours. Ensuite étudier la vulnérabilité exploitée, et parer cette vulnérabilité sur tous les autres firewalls. Pour réutiliser la machine corrompue, il sera nécessaire de la réinstaller entièrement.
- Le filtrage autorise tout : Voir le cas où le firewall interdit tout.
- Le filtrage est déviant :
- La faille exploitée ne vient pas du module du filtrage, mais ... : d'un autre service hébergé par la machine, ou d'une faille du système touchant une autre fonctionnalité. Dans le premier cas, remplacer la machine. Le nouveau firewall NE DOIT PAS héberger d'autres services. Dans le second cas, remplacer le firewall par un firewall de secours. Ensuite étudier la vulnérabilité exploitée, et parer cette vulnérabilité sur tous les autres firewalls. Pour réutiliser la machine corrompue, il sera nécessaire de la réinstaller entièrement.

### 3.7 De nouveaux services, interdits, sont accessibles depuis le réseau local :

Étudier le fonctionnement du nouveau service. On en déduit le filtrage qu'il faudrait réaliser pour le bloquer (et savoir si cela est possible sans effets de bords). Analyser le filtrage pour savoir si le firewall devrait bloquer ce service. Sinon, modifier le script et contrôler intégralement les règles de filtrage du firewall. Dans le cas contraire, cela veut dire que le traffic passe par un autre chemin et contourne le firewall. Il faut alors étudier au niveau de l'architecture réseau logique quel pourrait être ce chemin (découverte du réseau par traceroute, ping avec ttl incrémentés, ...).

### 3.8 Des tentatives d'intrusions sont constatées :

Tant que le firewall les bloque, cela ne pose pas de problème. Si une personne a réussi à s'introduire dans le réseau local sans y avoir le droit, les accès au réseau doivent être coupés après avoir récolté des informations sur l'attaquant, et modifier le script pour que cela ne se reproduise plus. Analyse la machine cible pour savoir si elle est contaminée. Si cela vient d'une mauvaise configuration ou d'une infection du poste de travail, le relais doit être pris par la *politique de maintenance du SI (niveau logiciel)* ou par la *protection antivirale*.

## 4 Communication :

Le filtrage va restreindre l'utilisation du réseau, et c'est donc une solution technique "très voyante". Il est indispensable d'avertir les utilisateurs à l'avance de la mise en place d'un firewall, en leur donnant la possibilité de faire remonter des remarques (adresse e-mail).

# 5 Responsabilité de mise en oeuvre et de maintenance :

À définir.