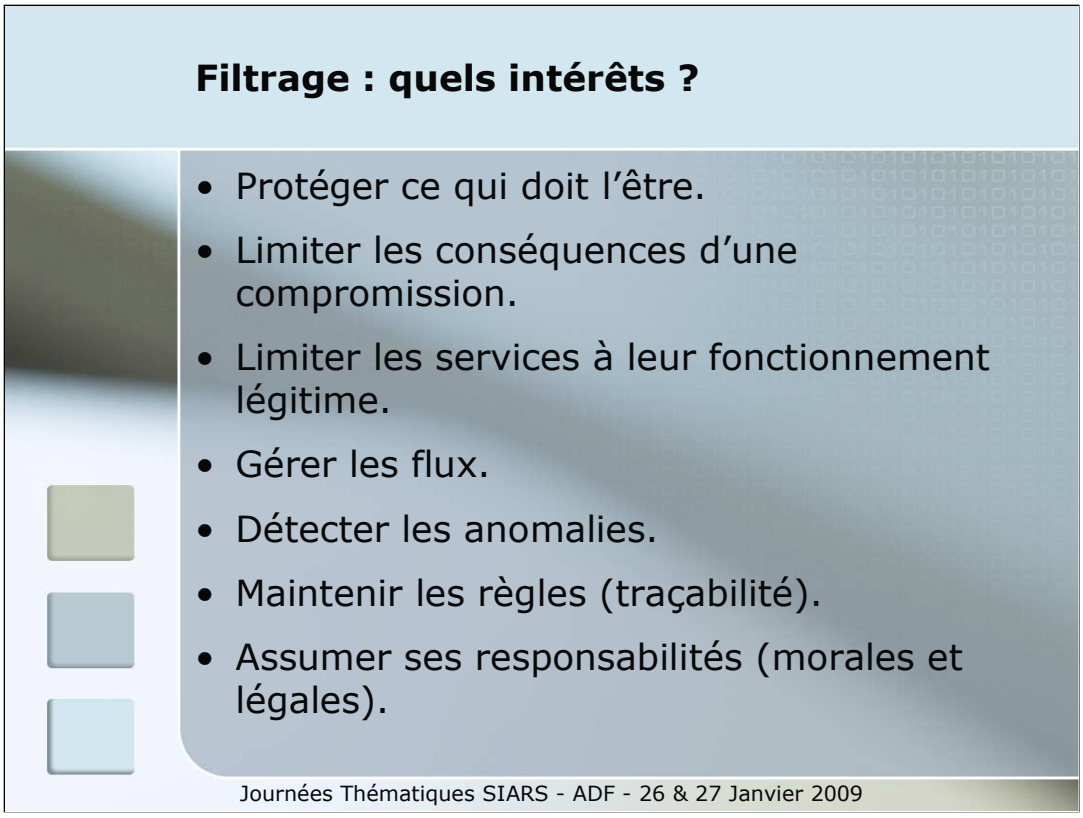
ADF 2009
Architecture réseau avec filtrage

Thierry DOSTES
tdostes@ifr88.cnrs-mrs.fr

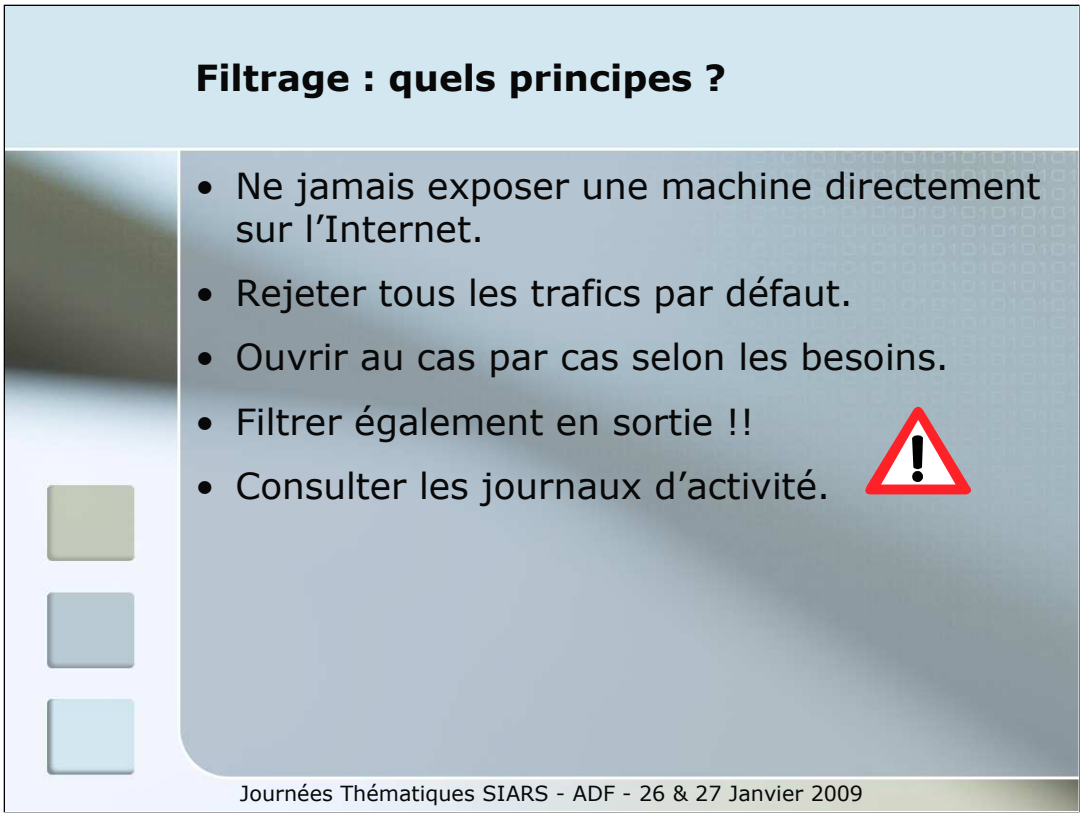
Plan

- Introduction.
- Les différents types de filtrage.
- La journalisation.
- Conclusions.

Le filtrage

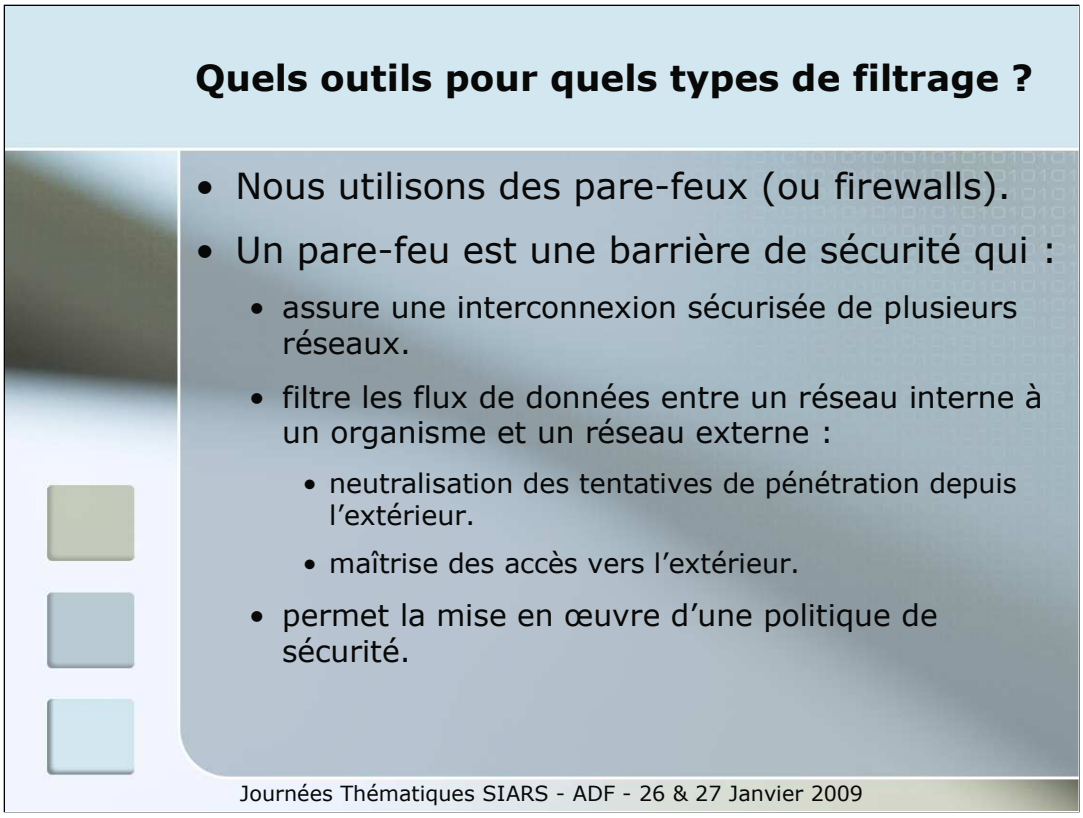


De nombreux incidents pourraient être détectés s'il y avait un bon filtrage, non seulement entrant, mais aussi **sortant**.



NB : De nombreuses attaques peuvent réussir dès lors qu'un agresseur est en mesure d'envoyer des paquets, même s'il n'obtient pas de réponse.

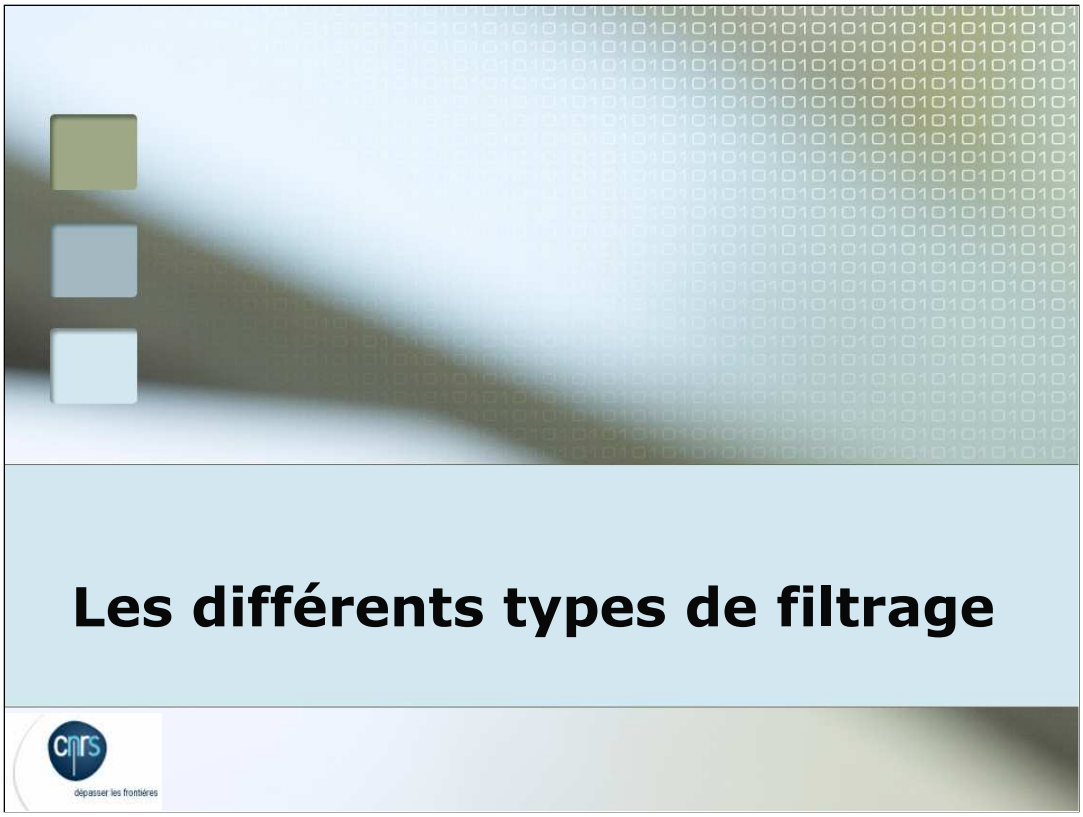
C'est le cas par exemple des attaques par déni de service.



Les notions d'intérieur et d'extérieur sont très subjectives puisqu'elles dépendent de l'architecture réseau mise en place. Ces notions sont étrangères à l'équipement.

Les pare-feux

- Il existe deux types de pare-feu :
  - les pare-feux IP ou filtrants qui bloquent tout le trafic sauf celui autorisé.
  - les serveurs mandataires (ou proxies) qui effectuent un filtrage sur la couche application.



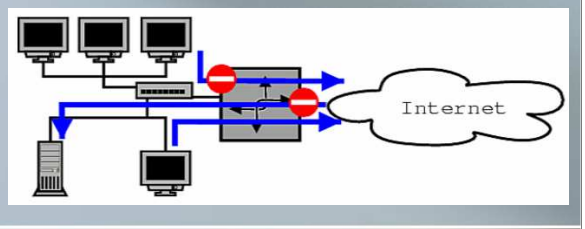
Les différents types de filtrage

Les différents types de filtrage

- Les types de filtrage les plus courants sont :
  - liaison (sur les adresses Mac, la couche Ethernet).
  - réseau (entêtes IP et type/code ICMP).
  - transport (ports TCP/UDP).
  - filtrage adaptatif (stateful inspection) ou dynamique.
  - session.
  - application (serveurs mandataires/relais applicatifs ou « proxies »).

Le filtrage statique (1)

- Il examine les paquets indépendamment les uns des autres.
- Il étudie les entêtes d'un paquet :
  - le protocole.
  - l'adresse et le port source.
  - l'adresse et le port destination.
  - les indicateurs d'état (syn, ack, rst).
  - les options IP.



Le filtrage statique (2)

- Il prend les décisions en fonction de règles préétablies, ordonnées séquentiellement.
- Il existe trois possibilités :
  - accepter le paquet (le laisser passer).
  - refuser le paquet (répondre explicitement à l'émetteur que ce n'est pas possible).
  - rejeter le paquet (faire comme s'il n'était jamais arrivé).
- En l'absence d'historique, beaucoup de ports doivent rester ouverts pour permettre le passage des paquets en retour (ex : FTP).

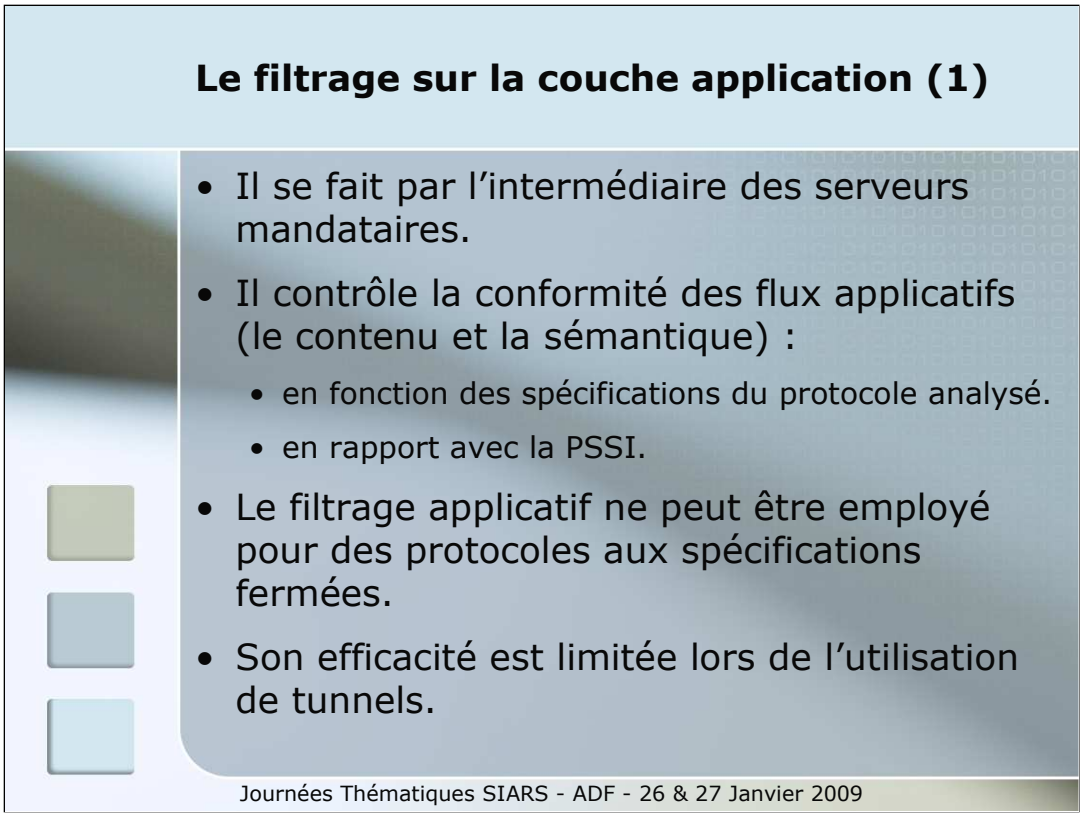
Le filtrage dynamique (1)

- Le filtrage dynamique introduit, au simple filtrage de paquets, la notion de session.
- Le système de filtrage mémorise les paquets (historique).
- Il adapte dynamiquement ses règles de filtrage.
- Un flux de retour sera autorisé uniquement si un paquet similaire est déjà passé dans l'autre sens.
- Le filtrage dynamique permet de laisser moins de ports ouverts.

Le filtrage dynamique (2)

- Exemple d'utilisation : protection d'un serveur Web avec IPTABLES.
  - en entrée : règles permettant uniquement l'accès au serveur Apache.
  - en sortie :
    - autoriser les réponses aux requêtes des clients distants (sessions).
    - interdire au serveur Web d'initier des connexions vers l'extérieur pour télécharger des données.

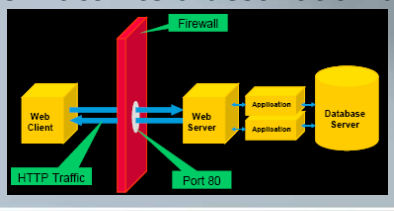
      exemple : exploitation des failles d'inclusion.
    - permettre au système d'exploitation de se mettre à jour.



Toute la difficulté consiste alors à détecter l'utilisation de tunnels HTTP(s). Exemple : certaines applications de P2P.

Le filtrage sur la couche application (3)

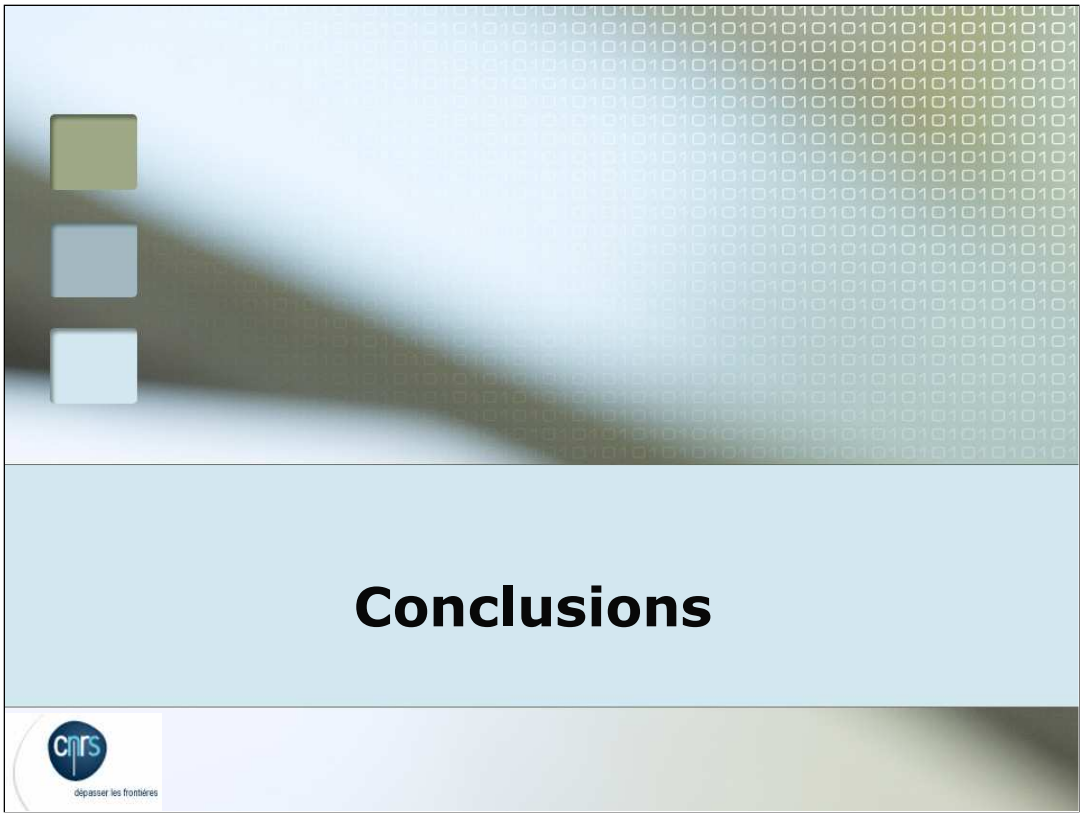
- Exemple d'utilisation : les modules Reverse Proxy et ModSecurity du serveur Apache.
  - centraliser et analyser le contenu des requêtes HTTP.
  - réagir à la découverte d'une faille de sécurité:
    - ajouter une nouvelle règle lors de la découverte d'une faille de sécurité ;
    - « temporiser » en attendant un correctif de sécurité.
  - enregistrer l'activité à destination des sites Web.



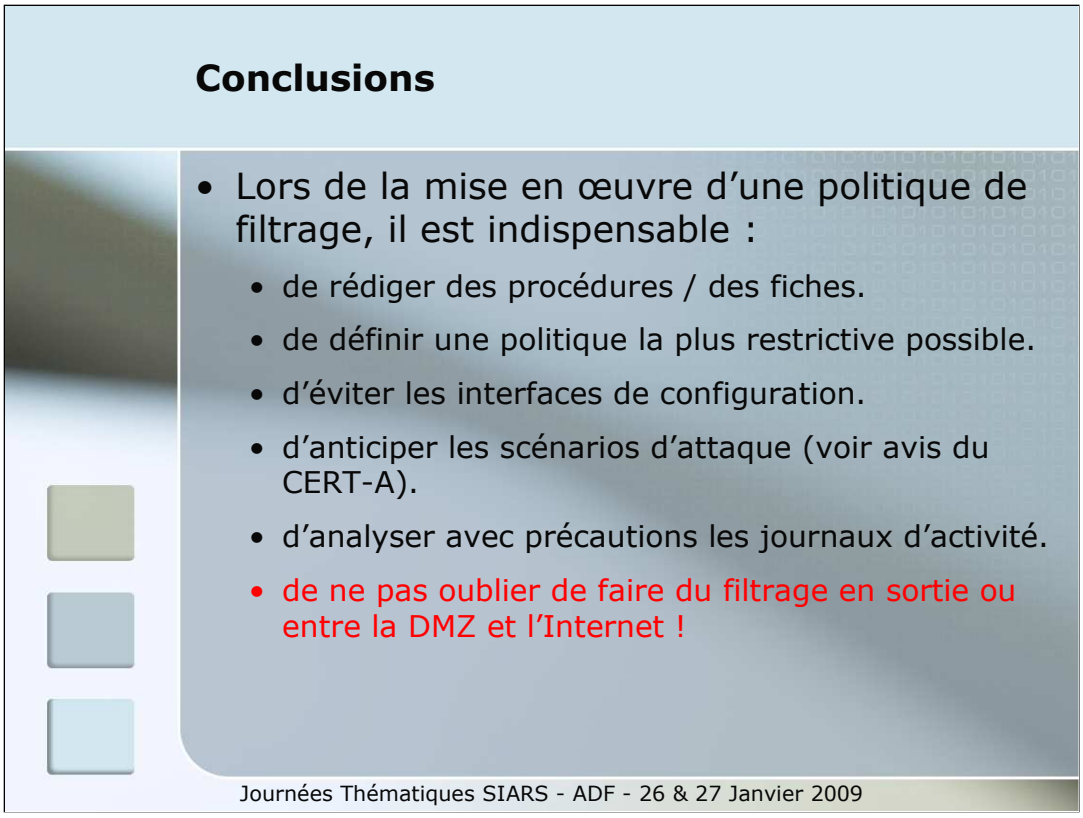
La journalisation

La journalisation

- Elle peut inciter à mettre en place un élément de filtrage spécifique pour :
  - récapituler les opérations réalisées par ce filtre.
  - recenser les problèmes ou attaques rencontrés.
- Il est recommandé de dupliquer les journaux vers une machine fédérant l'ensemble des traces du SI.
- Il est indispensable de privilégier un format de journalisation réellement exploitable (texte brut, XML).



Conclusions



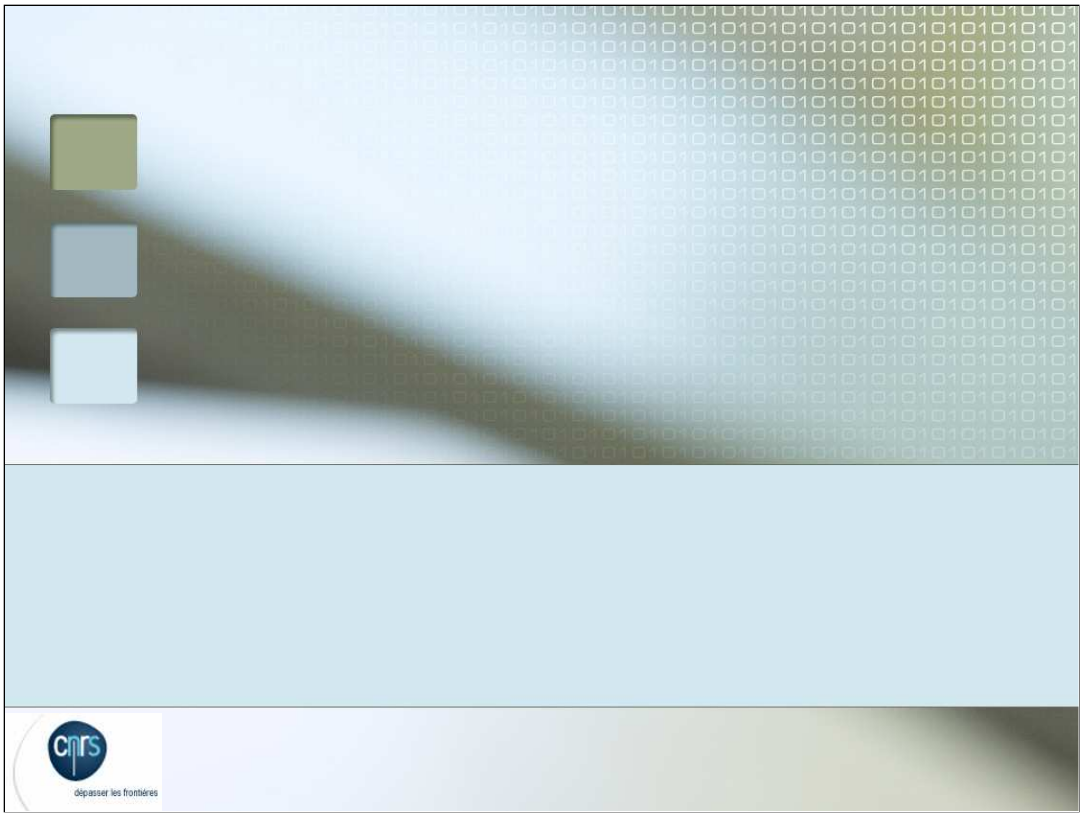
La mise en œuvre d'une politique de filtrage n'est pas une fin en soi. Nous devons absolument analyser avec précaution les journaux de filtrage pour nous assurer que les filtres sont pertinents.

Les activités rejetées par le dispositif de filtrage sont-elles :

-celles qui ne correspondent pas à la politique de configuration;

-l'indication d'une mauvaise configuration du filtre;

-le signe d'une compromission ?


dépasser les frontières