



ADF 2009

Architecture réseau avec filtrage



Thierry DOSTES
tdostes@ifr88.cnrs-mrs.fr



Plan

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



Journées Thématiques SIARS - ADF - 26 & 27 Janvier 2009



Le filtrage



cnrs
dépasser les frontières

Filtrage : quels intérêts ?

- Protéger ce qui doit l'être.
- Limiter les conséquences d'une compromission.
- Limiter les services à leur fonctionnement légitime.
- Gérer les flux.
- Détecter les anomalies.
- Maintenir les règles (traçabilité).
- Assumer ses responsabilités (morales et légales).

Journées Thématiques SIARS - ADF - 26 & 27 Janvier 2009

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

Filtrage : quels principes ?

- Ne jamais exposer une machine directement sur l'Internet.
- Rejeter tous les trafics par défaut.
- Ouvrir au cas par cas selon les besoins.
- Filtrer également en sortie !!
- Consulter les journaux d'activité.



Journées Thématiques SIARS - ADF - 26 & 27 Janvier 2009

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.

Quels outils pour quels types de filtrage ?

- Nous utilisons des pare-feux (ou firewalls).
- Un pare-feu est une barrière de sécurité qui :
 - assure une interconnexion sécurisée de plusieurs réseaux.
 - filtre les flux de données entre un réseau interne à un organisme et un réseau externe :
 - neutralisation des tentatives de pénétration depuis l'extérieur.
 - maîtrise des accès vers l'extérieur.
 - permet la mise en œuvre d'une politique de sécurité.

Journées Thématiques SIARS - ADF - 26 & 27 Janvier 2009

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

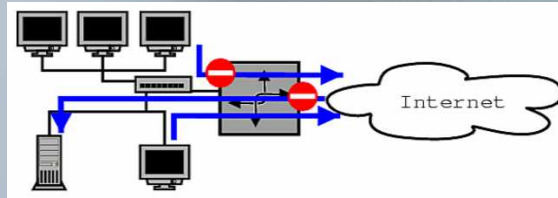


Les différents types de filtrage

- 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.



Journées Thématiques SIARS - ADF - 26 & 27 Janvier 2009

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.

Journées Thématiques SIARS - ADF - 26 & 27 Janvier 2009

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.



Le filtrage sur la couche application (1)

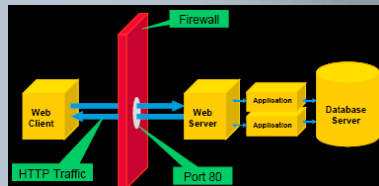
- Il se fait par l'intermédiaire des serveurs mandataires.
- Il contrôle la conformité des flux applicatifs (le contenu et la sémantique) :
 - en fonction des spécifications du protocole analysé.
 - en rapport avec la PSSI.
- Le filtrage applicatif ne peut être employé pour des protocoles aux spécifications fermées.
- Son efficacité est limitée lors de l'utilisation de tunnels.

Journées Thématiques SIARS - ADF - 26 & 27 Janvier 2009

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.



Journées Thématiques SIARS - ADF - 26 & 27 Janvier 2009




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



Conclusions

- Lors de la mise en œuvre d'une politique de filtrage, il est indispensable :
 - de rédiger des procédures / des fiches.
 - de définir une politique la plus restrictive possible.
 - d'éviter les interfaces de configuration.
 - d'anticiper les scénarios d'attaque (voir avis du CERT-A).
 - d'analyser avec précautions les journaux d'activité.
 - **de ne pas oublier de faire du filtrage en sortie ou entre la DMZ et l'Internet !**

Journées Thématiques SIARS - ADF - 26 & 27 Janvier 2009

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 ?

