Protection des Systèmes

élégation Aquitaine et Poitou Charentes

Bibliographie *(1)*

- Acces control lists sur Cisco : http://www.dr15.cnrs.fr/Cours/ACL-Cisco, 1996.
- Kit de garde-barrière : http://www.urec.fr/KGB, 1996-1997.

Les techniques

- Protection des données contre leur destruction accidentelle

ès non autorisés venant de
érieur ou de l'intérieur
équipements de routage (ACL Cisco)

écanismes d'authentification, données en transit)

Les filtres sur les routeurs d'entrée (1)

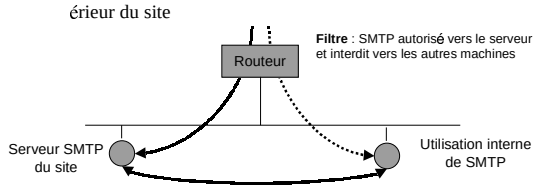
ée analyse chaque paquet et filtre
ères comme :

éfinit des listes de contrôles
ères. A
être

Les filtres sur les routeurs d'entrée (2)

égie : tout ce qui n'est pas explicitement autorisé

ès à un service (messagerie, WWW, FTP, etc.) que
éalisent effectivement le service pour
érieur du site



Les filtres sur les routeurs d'entrée (3)

érieur vers l'intérieur :

cès (ping) vers l'adresse de broadcast

cès provenant de l'extérieur et à destination de
éseaux internes

érieur vers extérieur, deux options :

ccès depuis des serveurs "proxy" et obliger
à transiter par ces proxys

Les filtres sur les routeurs d'entrée (4)

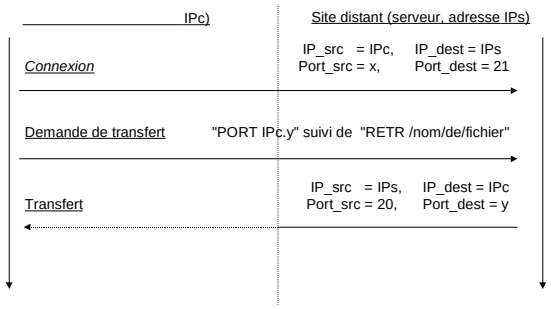
ûteuse (standard sur les routeurs) et

énients :

e à mettre en œuvre : demande une parfaite
îtrise des protocoles, configurations fragiles

ège pas les machines "ouvertes"

Les filtres sur les routeurs d'entrée (5)



Les filtres sur les routeurs d'entrée (6)

éatoire du client. Deux certitudes : en général, le
éatoire est supérieur à 1024.

é.

ée tous les ports > 1024 ? attention aux ports

ête PASV) de FTP ? pas toujours
émentée sur les clients et serveurs

Les wrappers (1)

- S'intercalent entre la demande de connexion d'un client vers un service et l'ouverture de ce service pour ce client
- Sur Unix : la plupart des services se lancent via *inetd*, configurable par *inetd.conf*. A chaque demande de connexion vers un service, *inetd* lance la commande qui implémente ce service. Le "wrapper" prend la place de

érifie si le client du service est autorisé

émente le service

Les wrappers (2)

- Plusieurs solutions :
  - solutions propriétaires (inetd.sec sur HP-UX)

és :

ec équivalent à TCP Wrapper mais n'existe que sur HP-

érent en fonction de

Les techniques de pare-feux (1)

Deux techniques, ou combinaison des deux :

- pare-feu / garde-barrière filtrant

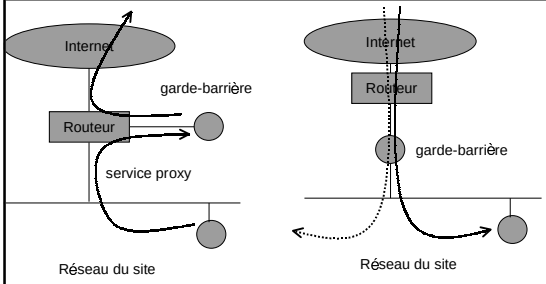
e à travers le pare-feu qui effectue les contrôles
é des opérations, éventuellement des traductions

ère relais ou (*proxy*)

ée et ou en sortie et le relaye
émentent les services

ère générale : éviter l'accès direct entre les
à protéger et le reste du monde

Les techniques de pare-feux (2)



Les techniques de pare-feux (3)

Les services "proxys". Exemple : Firewall Toolkit (TIS)

- Proxy Telnet et FTP
  - connexion sur garde-barrière

érieur, faible pour les connexions
érieur, éventuellement nulle pour FTP anonyme
élection du serveur de destination :

Les techniques de pare-feux (4)

- Proxy SMTP
  - le courrier à destination du site est envoyé au garde-barrière
    ère stocke les messages dans une
    ère scrute la file d'attente et fait

énérique

Les techniques de pare-feux (5)

- Avantages :
  - le code des proxys est simple : plus un programme est simple, moins il contient d'anomalies
  - tout proxy s'exécute dans un environnement restreint (chroot) :
    é d'utiliser des effets de bords incontrôlés

é de configurer l'ensemble des machines du site sans
éfaut, i.e. sans connexion directe vers l'extérieur
ccès aux services du garde-barrière peut se faire soit selon

ès à tel ou tel utilisateur ou