Protection des Systèmes d'Informations

Roland Dirlewanger
CNRS - Délégation Aquitaine et Poitou Charentes
rd@dr15.cnrs.fr

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

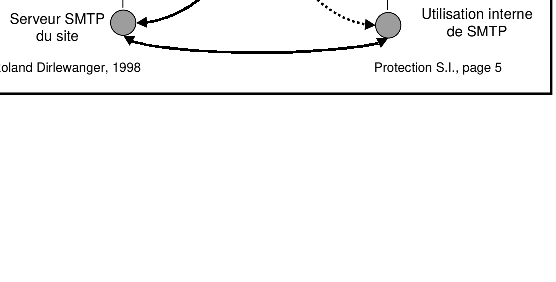
- Protection des données contre leur destruction accidentelle ou intentionnelles
  - sauvegardes
  - disques miroirs
- Protection contre les accès non autorisés venant de l'extérieur ou de l'intérieur
  - filtres IP sur équipements de routage (ACL Cisco)
  - wrappers (tcp_wrappers, TIS)
  - pare-feux
  - chiffrage (mécanismes d'authentification, données en transit)

Les filtres sur les routeurs d'entrée (1)

- Le routeur d'entrée analyse chaque paquet et filtre le paquet en fonction de critères comme :
  - les adresses sources ou destinations
  - les ports sources et destinations
  - le paquet est une demande de connexion
- L'administrateur définit des listes de contrôles (*Access Control Lists*) combinant ces critères. A chaque combinaison il associe le paramètre (permettre/interdire)

Les filtres sur les routeurs d'entrée (2)

- La stratégie : tout ce qui n'est pas explicitement autorisé est interdit
  - autorise l'accès à un service (messagerie, WWW, FTP, etc.) que pour les machines qui réalisent effectivement le service pour l'extérieur du site



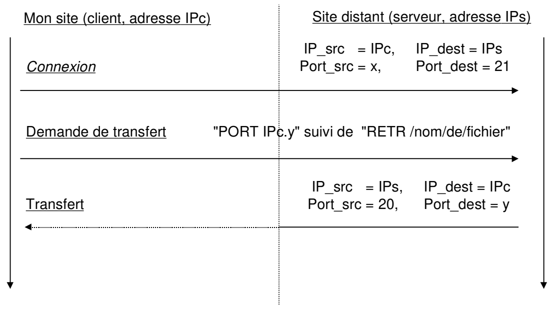
Les filtres sur les routeurs d'entrée (3)

- Dans le sens extérieur vers l'intérieur :
  - autoriser les connexions vers les serveurs de communication (messagerie, WWW, serveurs FTP)
  - interdire les accès (ping) vers l'adresse de broadcast
  - interdire certaines options d'IP (source route par exemple)
  - interdire les accès provenant de l'extérieur et à destination de 127.0.0.1 et des réseaux internes
- Dans le sens intérieur vers extérieur, deux options :
  - tout permettre
  - ne permettre que l'accès depuis des serveurs "proxy" et obliger l'utilisateur à transiter par ces proxys

Les filtres sur les routeurs d'entrée (4)

- Avantages :
  – technique peu coûteuse (standard sur les routeurs) et souvent efficace
- Inconvénients :
  – difficile à mettre en œuvre : demande une parfaite maîtrise des protocoles, configurations fragiles
  – ne protège pas les machines "ouvertes"
  – effets de bord (cas de FTP par exemple)

Les filtres sur les routeurs d'entrée (5)



Les filtres sur les routeurs d'entrée (6)

- Dans le cas d'un transfert FTP (voir ci-dessus), c'est le serveur FTP qui fabrique la connexion de transfert vers un port aléatoire du client. Deux certitudes : en général, le port source est 20, le port aléatoire est supérieur à 1024.
- Solution :
  – Filtrer sur le port source ? pas toujours possible, risqué.
  – Autoriser en entrée tous les ports > 1024 ? attention aux ports 6000 (X11), 2049 (NFS/TCP)
  – Utiliser le mode "passif" (requête PASV) de FTP ? pas toujours implémentée 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 chaque commande et :
  – vérifie si le client du service est autorisé
  – si oui, lance la commande qui implémente le service
  – si non, ferme la connexion

Les wrappers (2)

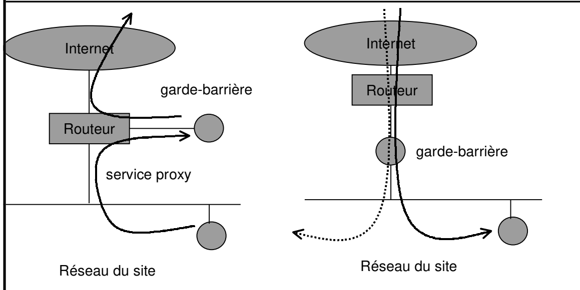
- Plusieurs solutions :
  – solutions propriétaires (inetd.sec sur HP-UX)
  – logiciels du domaine public :
    - TCP Wrapper
    - composant "netacl" de la Firewall Toolkit de TIS
- Avantages comparés :
  – inetd.sec équivalent à TCP Wrapper mais n'existe que sur HP-UX
  – netacl permet de lancer un serveur différent en fonction de l'appelant, pas TCP Wrapper

Les techniques de pare-feux (1)

Deux techniques, ou combinaison des deux :

- pare-feu / garde-barrière filtrant
  – tout trafic transite à travers le pare-feu qui effectue les contrôles de validité des opérations, éventuellement des traductions d'adresses, etc.
- pare-feu / garde-barrière relais ou (*proxy*)
  – le pare-feu accepte tout trafic en entrée et ou en sortie et le relaye vers les serveurs qui implémentent les services
- d'une manière générale : éviter l'accès direct entre les machines 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
  - authentification forte, avec OTP (*One Time Password*) pour les connexions venant de l'extérieur, faible pour les connexions venant de l'intérieur, éventuellement nulle pour FTP anonyme
  - sélection du serveur de destination :
    - par commande "connect" dans le cas du proxy-telnet
    - par utilisateur "login@serveur.destination" dans le cas du proxy-ftp

Les techniques de pare-feux (4)

- Proxy SMTP
  - le courrier à destination du site est envoyé au garde-barrière
  - le serveur SMTP du garde-barrière stocke les messages dans une file d'attente
  - un client SMTP sur le garde barrière scrute la file d'attente et fait suivre chaque message vers la passerelle de messagerie
- Autres proxys dans FWTK
  - HTTP
  - X11
  - proxy générique

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) : pas de possibilité d'utiliser des effets de bords incontrôlés
  - la plupart des services existent sous la forme de proxy : possibilité de configurer l'ensemble des machines du site sans route par défaut, i.e. sans connexion directe vers l'extérieur
  - l'accès aux services du garde-barrière peut se faire soit selon l'adresse du client, soit par authentification de l'utilisateur : on peut autoriser ou pas tel ou tel accès à tel ou tel utilisateur ou machine