|  |  |  |
| --- | --- | --- |
| *hosts.allow hosts.deny*  http://upload.wikimedia.org/wikipedia/commons/thumb/3/35/Tux.svg/512px-Tux.svg.png |  | *TCP Wrapper*  L'administrateur réseau va pouvoir utiliser 2 fichiers: /etc/hosts.allow et /etc/hosts.deny pour filtrer les accès à sa machine.   * */etc/hosts.deny* on indique dans ce fichier les services et les hôtes pour lesquels l'accès est interdit. * */etc/hosts.allow* on indique dans ce fichier les services et les hôtes pour lesquels l'accès est autorisé.   **Exemples** …  # Fichier /etc/hosts.deny # interdit tous les accès ftp à la machine in.ftpd:ALL  # Fichier /etc/hosts.allow # autorise les accès ftp venant de client1 in.ftpd :client1.profsavard.info  *TCP-Wrapper* utilise l'algorithme suivant …   * si une règle est applicable dans *hosts.allow*,  alors cette règle est appliquée,  sinon … * si une règle est applicable dans *hosts.deny* , alors cette règle est appliquée,  sinon … * l'accès est autorisé.   Ce mode de fonctionnement induit la stratégie de sécurité à adopter :   * décrire toutes les règles pour les couples (services/clients) qui sont autorisés, * interdire systématiquement tout le reste.  Mettre par défaut ALL:ALL dans hosts.deny.   Les tentatives d'accès depuis des machines extérieures sont toutes enregistrées dans des fichiers particuliers.  Ces enregistrements sont effectués par le processus syslogd qui, à son démarrage, lit le fichier /etc/syslog.conf pour trouver dans quel(s) fichier(s) il doit enregistrer les différentes tentatives d'accès.  **Adapté du document original**  <http://doc.ubuntu-fr.org/denyhosts> |
|  |  |  |