Jean Saquet – Université de Caen

M1 Informatique

Réseaux

Filtrage

Bureau S3-354
mailto:Jean.Saquet@info.unicaen.fr
http://saquet.users.greyc.fr/M1/rezo

Sécurité - introduction

Au départ, très peu de sécurité dans les accès réseaux (mots de passe, voyageant en clair)

Avec la généralisation d'Internet, plusieurs problèmes :

- tentatives d'intrusion dans les systèmes
- tentatives de dénis de services
- interception des flux de données
- usurpation d'identité

==> nécessité de filtrer les éléments de protocole, de chiffrer, d'authentifier les données

Sécurité – niveau réseau

Les messages transitent dans des datagrammes IP, et doivent traverser les routeurs.
On peut donc au passage décider de l'action à effectuer en fonction des adresses IP (source et destinataire) : accepter de router le DG ou le refuser.

Mais, là encore, il est assez facile d'usurper une adresse IP source. Ceci ne permettra sans doute que l'envoi de DGs, pas l'établissement d'un dialogue, mais peut suffire pour certaines attaques

Sécurité – TCP/IP

Les messages sont le plus souvent des segments TCP ou des DGs UDP (ou messages ICMP).
En analysant au niveau réseau ET transport (ce que font entre autres les NATs) on peut donc contrôler plusieurs paramètres simultanément, de niveau IP et de niveau transport (ou types des messages ICMP).

On va donc définir, en certains endroits du réseau, des règles de filtrage se basant sur ces paramètres.

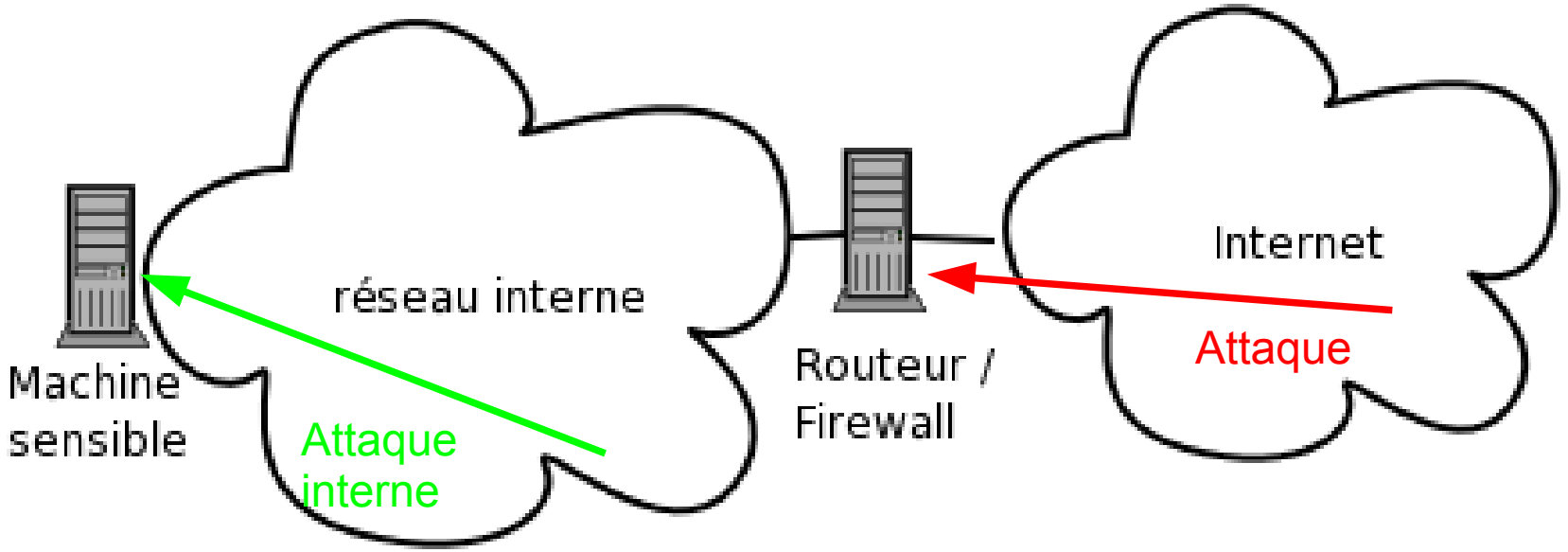
Sécurité – Filtrage

L'analyse des messages TCP/IP sera le plus souvent faite au niveau d'un routeur, d'un traducteur d'adresses en v4.

En effet, les messages devant être analysés à ces niveaux, autant en profiter pour pousser plus loin cette analyse et éliminer les messages indésirables.

Il est donc commode de grouper les systèmes de filtrage sur par exemple un routeur d'accès à l'Internet. Attention toutefois à la charge de ce dernier.

Sécurité – Interne/externe



Les règles de filtrage du firewall sont sans effet contre une attaque venant de l'intérieur

Sécurité – autofirewalls

La centralisation du firewall est pratique au niveau de la gestion, mais ne protège pas contre les risques internes.
En v4, le couplage avec NAT semble offrir une sécurité (adresses privées non accessibles de l'extérieur), mais, là encore, effet nul contre les attaques internes.
==> auto-firewalls sur machines sensibles, adaptés à chaque cas.

Sécurité – protections

Une possibilité est d'essayer de profiter d'une faille d'un logiciel.
Pour éviter ceci au maximum, bien mettre à jour tous les serveurs publics, interdire l'accès aux autres personnes non autorisées.
Les connexions entrantes seront donc filtrées.
Le filtrage des connexions sortantes est plus du domaine des autorisations accordées aux membres de l'entreprise.

Sécurité – firewalls

Principe de base : suite ordonnée de règles :
de la plus particulière à la plus générale
la dernière : refuser tout ce qui n'est pas explicitement autorisé !
Filtres basés sur paramètres TCP/IP : adresses, ports sources et destination (ou fonction ICMP), connexions entrantes ou sortantes, protocole de transport, interface physique utilisée.

Sécurité – IPtables

Iptables est le logiciel de commande du système de filtrage intégré au noyau Linux.
Il utilise – d'où son nom – des tables avec en particulier "filter" et "nat". Chacune comporte des "chaînes" (listes de règles) se positionnant à un moment bien précis de l'analyse des paquets : en entrée, sortie, ou traversée pour filter, avant ou après routage pour nat, ...

Sécurité – IPtables

Les instructions permettent d'ajouter ou supprimer des règles à chaque chaîne. Exemples :

iptables -A INPUT -p tcp --dport 22 -j ACCEPT
accepte les connexions aux ports 22 (ssh)

iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
masque (traduit) les adresses à la sortie par eth0

Sécurité – IPtables

La syntaxe générale est :
iptables [-t table] command [match] [target/jump]

- command ajoute, supprime, liste, ... les règles
- match : suite de critères de filtrage (adresse, port source/dest, proto, interface, ...)
- target/jump : action à effectuer si la règle s'applique

Si la règle ne s'applique pas, on passe à la suivante dans la chaîne

Sécurité – IPtables

L'ordre des règles est fondamental. Exemple :

- autoriser la machine d'@ip x à se connecter au port 22 de la machine d'@ip y
- interdire à toute machine de se connecter au port 22 de la machine d'@ip y

Si on inverse l'ordre, la machine x ne pourra pas se connecter car la règle générale (devenue la première) se sera appliquée.

Sécurité – firewalls

Le positionnement, la configuration des firewalls est un exercice difficile. Idéalement :

- configurer un auto-firewall "standard" pour les postes de travail ordinaires
- configurer un auto-firewall particulier pour chaque serveur, chaque machine ayant une fonction particulière
- configurer un ou des firewalls généraux entre réseaux internes et externe, pour l'accès à la zone des serveurs publics (DMZ)

Sécurité – firewalls

À éviter :

- Compter uniquement sur un firewall d'accès au réseau public
- Se baser sur les adresses privées (et le NAT) pour la sécurité
- Refuser toute requête sous prétexte de sécurité

(nécessité de dialogue avec les utilisateurs, de mémoriser tous les cas particuliers)

Sécurité – applications

Des filtres applicatifs peuvent également être mis en place :

- filtres de courrier (virus, spam)
- filtres de contenus des messages d'application

Il est en effet possible d'encapsuler des messages indésirables dans du http par exemple, ou autre protocole couramment non filtré.