Séminaire sur le pare-feu

Yann Duplouy

Cachan Réseau à Normale Sup'

Mardi 22 janvier 2013

Sommaire

Un pare-feu, vous dites ?

- Permet de limiter les échanges réseau entre l'extérieur et la machine ou le réseau local, suivant divers critères
- Windows en intègre un (de base)...
- ...tout comme Linux, avec *netfilter*, un module du noyau Linux (qu'on verra ultérieurement)

Le pare-feu sur l'ordinateur «de tout le monde»

Sous Windows, depuis quelques temps, un Pare-feu est intégré de base.

- Permet de bloquer certains ports en entrée/sortie
- Permet de bloquer la connexion réseau des programmes
- . . . par défaut, le pare-feu de Windows bloque les PING. . .

Sommaire

Limitation du routage

- *komaz* est la passerelle du Cr@ns
- Les réseaux non routables sont bloqués : `10.0.0.0/8`, `172.16.0.0/12`, `169.254.0.0/16`, `192.168.0.0/16`, `224.0.0.0/4`

Filtrage

- Association MAC-IP
- Filtrage des ports
- Filtrage du peer-to-peer
- Détection des flood dus aux virus

Sommaire

Présentation

- Netfilter est un module du noyau de Linux qui permet de contrôler, modifier, et filtrer les paquets IP (et de suivre les connexions).
  - Pare-feu
  - Partage de connexion
  - Autorisation du trafic réseau
- Iptables est une interface permettant de le configurer.

Présentation (2)

- Les paquets IP passent dans différentes tables (Raw, Mangle, Nat et Filter)
- Dans ces tables, ils passent dans différentes chaînes, sur lesquelles on applique des règles.

Architecture

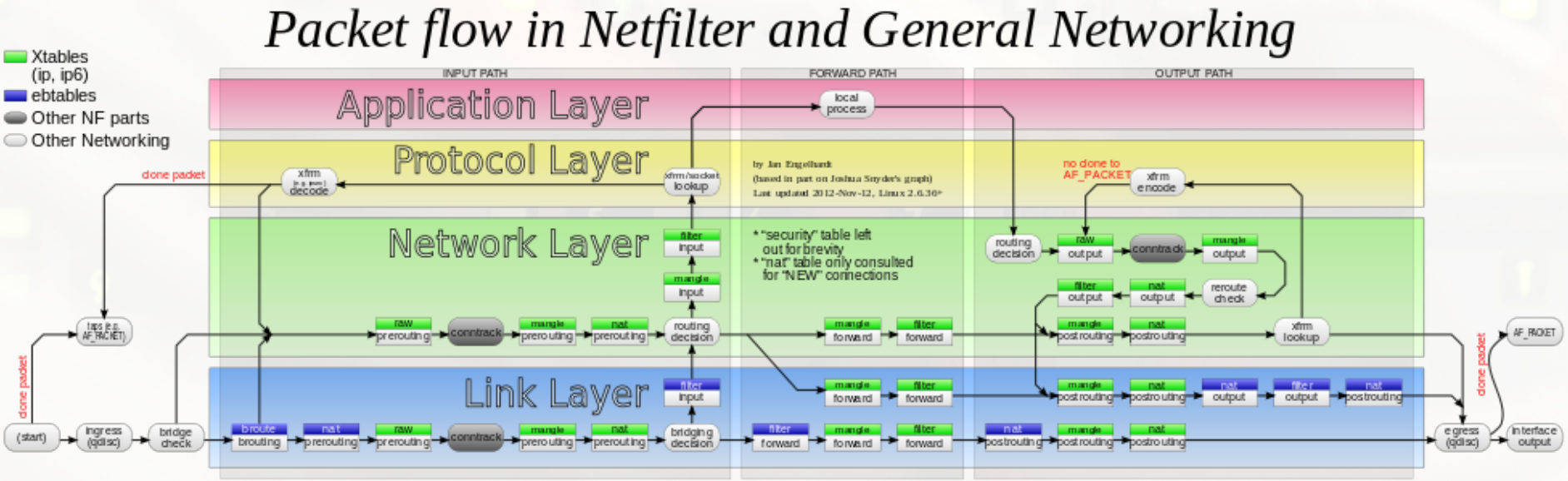

Table Raw

- Sert à modifier des paquets (ToS, TTL...)
- On peut y utiliser toutes les chaînes de base :
  - *Prerouting* : permet de modifier les paquets entrants, avant le routage
  - *Postrouting* : permet de modifier les paquets locaux avant le re-routage vers la destination
  - *Input*
  - *Output*
  - *Forward*

Table Nat

- Permet de faire du changement d'IP sur les requêtes
- Cette fois-ci, on est limité à trois chaînes :
  - *Prerouting*, qui permet de modifier la destination des paquets
  - *Postrouting*, qui permet de modifier la source des paquts
  - *Output* : de même que *prerouting*, mais pour les connexions provenant d'un processus du système

Table Filter

- Permet de filtrer les paquets (DROP, LOG, ACCEPT, REJECT)
- On peut agir sur trois chaînes :
  - *Input*
  - *Output*
  - *Forward*, pour les paquets en transit d'une interface à une autre.

Sommaire

Principe général

- On récupère, dans la base ldap, les informations nécessaires (machines, ports ouverts...)
- La correspondance Mac-IP est assurée par *ipset*
- Un script python génère les règles iptables nécessaires
- Le pare-feu est ensuite mis en place sur :
  - komaz
  - zamok
  - gordon
  - et normalement tous les serveurs ayant adm//adhérents

Table Mangle

Utilisée en *prerouting*. Par défaut : ACCEPT

- Si elle passe par un sous réseau de l'ip Cr@ns : SUBNET
  - Classe les paquets : par groupe de /24 (138.231.136. , 138.231.137. ...), par adhérent.

Table Nat

Elle ne concerne que les nouvelles connexions.
Elle est utilisée dans le cas d'un passage sur connexion de secours, ou dans le cas d'une déconnexion "soft"

Table Filter (1/2)

- Pour les non serveurs : passage par TEST_VIRUS_FLOOD
- Puis passage par RESEAUX_NON_ROUTABLES_DST
- Puis passage des paquets venant de l'extérieur par RESEAUX_NON_ROUTABLES_SRC
- Les paquets passant par TEST_MAC-IP, sauf les suivants :
  - Ceux qui ont pour source ou destination les serveurs de serveur_crans
  - Les paquets provenant de l'extérieur

Table Filter (1/2) – Chaînes utilisées

- TEST_VIRUS_FLOOD : droppe les paquets semblant provenir de virus, ou de flood
- RESEAUX_NON_ROUTABLES_DST : droppe les paquets allant vers des réseaux non routables
  - `10.0.0.0/8`, `172.16.0.0/12`, `169.254.0.0/16`, `192.168.0.0/16`, `224.0.0.0/4`
- RESEAUX_NON_ROUTABLES_SRC : même chose, mais pour ceux provenant de réseaux non routables
- TEST_MAC-IP : envoie les bons paquets vers CRANS_VERS_EXT.

Table Filter (2/2)

On l'utilise en *forward*, par défaut : ACCEPT

1. passage par BLACKLIST
2. ce qui a pour source un serveur de serveur_crans est dirigé vers SERVEURS_VERS_EXT
3. ce qui a pour destination un de ces serveurs est dirigé vers EXT_VERS_SERVEURS
4. ce qui vient de l'interface externe est dirigé vers EXT_VERS_CRANS
5. ce qui vient de l'interface interne est dirigé vers CRANS_VERS_EXT
6. et on termine par un passage par INGRESS_FILTERING

Table Filter (2/2) – Chaînes utilisées

- BLACKLIST filtre les ip blacklistées ⇒ REJECT
- FILTRE_P2P filtre le trafic peer-to-peer :
  - log les paquets correspondant aux protocoles de filtres_p2p
  - et rejette les paquets correspondants aux protocoles filtres_p2p_bloq une fois la limite atteinte
- EXT_VERS_CARNS et CRANS_VERS_EXT :
  - Les paquets vers les machines du Crans : ACCEPT (selon le test port-ip)
  - REJECT pour le reste
- EXT_VERS_SERVEURS et SERVEURS_VERS_EXT :
  - Si le test MAC-IP et IP-Port réussit : ACCEPT
  - Sinon : REJECT
- INGRESS_FILTERING : ne laisse sortir que les paquets dans l'adresse IP source appartient au Cr@ns.