Sécurité des Accès

P. Laurençot

Plan d’ensemble

- Technique/parade
  - Filtrage
    - Réseau, Applicatif
  - Translation d’adresse IP (NAT, PAT)
  - Authentification
  - Durcissement des configurations

- Matériels
  - Parefeu
  - Proxy
  - Détecteur d’intrusion
  - Routeurs

Introduction (1)

Pour vivre heureux, vivons caché….

- Quelle information est confidentielle ?
  - Nécessité d'identifier les informations
    - Nom des machines, login utilisateur, informations techniques
    - Plan d'adressage IP
    - Configuration DNS, liens de secours,…
    - Utilisation Wifi,…
  - Nécessité d'informer les utilisateurs de la confidentialité
    - Tous les utilisateurs ayant accès à ses informations

(Attention aux personnes extérieures…)

Défense en profondeur (1)

- Définition :

  Elle consiste à mettre en place plusieurs techniques de sécurité complémentaires afin de réduire l'impact lorsqu'un composant particulier de sécurité est compromise ou défaillant (ANSSI)

- Objectif :
  - *Prévenir* : éviter la présence ou l'apparition de failles de sécurité
  - *Bloquer* : empêcher les attaques de parvenir jusqu'aux composants visés
  - *Contenir* : limiter les conséquences de la compromission
  - *Détecter* : pouvoir identifier les incidents et les compromissions
  - *Réparer* : disposer de moyens pour remettre le système en fonctionnement

- Durcir le travail de l'attaquant
  - Gestion des disques durs
    - Montage des partitions en lecture seule
    - Isolation des partitions pouvant devenir saturés (log, spool, BD de serveur web,…)
    - Limité les droits sur une partition

Défense en profondeur (2)

- Durcir le travail de l'attaquant (suite)
  - Nommage des machines explicites à éviter
    - Router : ISIMA_routeur
    - Parefeu : firewall1_isima
  - Eviter les bannières d'accueil trop précise
    - Pas de « bienvenue sur le routeur »
    - Pas d'information sur l'équipement, ni l'OS
    - Pas d'information sur la société…
  - Mettre en place du filtrage
    - Filtre ICMP,….
  - Hygiène des machines
    - Mettre à jour l'OS, les logiciels, les antivirus…
    - Changer le mot de passe par défaut

Filtrage (1)

- Niveau 2 (Switch)
  - Adresse Mac ou physique
    - Utilisation de VLAN (IEE802.1Q)
      - Mise en place de Private VLAN
        - Mode primaire (ou promiscuous), secondaire (isolé ou communauté)
    - Vérification @Mac émetteur
    - Nombre maximum d'@MAC sur un port
- Niveau 3 (Parefeu et routeur avec ACL)
  - Adresse IP
    - Filtrage IP source (simple) ou Filtrage IP destination (compliqué)
    - Filtrage plus précis pour serveurs internes

Filtrage (2)

- Niveau 4 (Parefeu)
  - TCP/UDP
    - Filtrage au niveau port
    - Filtrage au niveau TCP sur types de segment
    - Filtrage sur le sens des communications
- Filtrage applicatif
    - De plus en plus précis
    - Reconnaissance par mot clef
    - Mise en place de proxy
      - Fonctionnement Black list/ white list
      - Load balancing des serveurs internes
      - Reverse proxy ou proxy

Détection d'intrusion

- Utilisation de sondes IPS/IDS
  - IDS (Intrusion Detection Systems)
    - Passives
    - Alertent, mais n'empêchent pas l'attaque
  - IPS (Intrusion Prevention Systems)
    - En coupure au niveau réseau
    - Agissent si un trafic est considéré malveillant
    - Pb des faux positifs/ faux négatifs

Logiciel gratuit : snort….. (avec des dérivés)

→ utilisation de règles de correspondance

Aide à la détection

- Aide aux personnels
  - XDR (eXtended Detection and Response)
    - Collecte les données des EDR
    - Corrélation de ses données + IA
    - Compte-rendu
  - SIEM (security information and event management)
    - Collecte des journaux et des logs de tous les équipements
    - Agrégation de ses données + IA
    - Recherche des menaces et compte-rendu
  - SOAR (Security Orchestration, Automation and Response)
    - Faire des actions automatiques suite à des menaces
    - Reçoit des infos du SIEM ou de l'XDR

Authentification (1)

- Concept
  - Utilisation d'un équipement de sécurité
    - Blocage du flux si non authentifié
    - Une phase d'identification
    - Début de l'authentification
      - Refus ou acceptation
        - par l'équipement de sécurité
        - Par la décision d'un serveur tiers
- Utilisation par beaucoup de protocoles
  - Niveau 2
    - Pour P2P, soit PAP, soit CHAP, soit MS-CHAP2
    - Pour l'ADSL,….

Authentification (2)

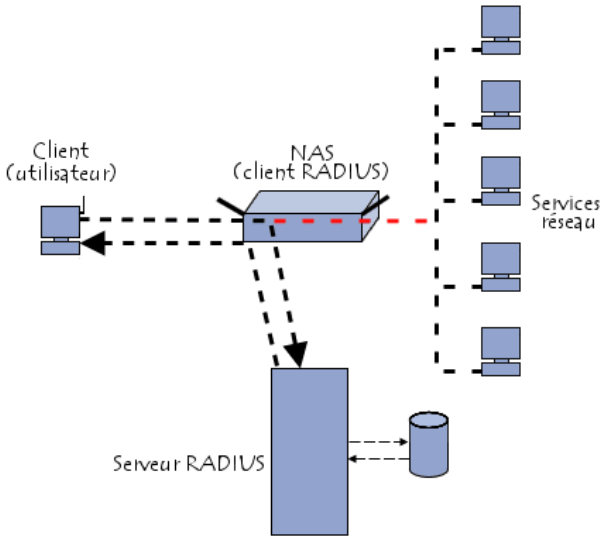
- Utilisation par beaucoup de protocoles
  - Niveau 3
    - Pas nativement pour IPv4, (IPSec),
    - Mise en place pour Ipv6 plus naturel d'IPSec
  - Niveau 4 et plus (ou moins)
    - Norme IEEE 802.1X
      - AAA (Authentication, Authorization, Accounting)
      - Autorise l'accès à un équipement après demande auprès d'un serveur
      - Mise en œuvre : Radius, **Diameter**, TACACS+,….

Radius (1)

Remote Authentication Dial-In User Service

- Plusieurs entités communiquent en UDP:
  - Supplicant (client utilisateur)
  - NAS (Network Access Server) != Network Attached Storage (NAS)
    → client radius
  - Serveur radius (ou proxy radius), basé sur LDAP, …

- 4 Trames possibles vers le serveur radius
  - Access-request : demande d'autorisation
  - Challenge-request : serveur demande plus d'informations au client radius
  - Access-accept : OK + informations
  - Access-Reject : refus de l'accès



Radius (2)

- EAP (Extensible Authentification Protocol)
  - Multitude de méthodes
    - EAP/MD5, EAP/TLS, EAP/TTLS, EAPOL, …
  - Basé sur le niveau 2 pour le chiffrement
    - Avec ou sans certificat
  - Plusieurs sortes de paquets
    - EAP Request / Response : requête/réponse entre supplicant et client
    - EAP success/fail
    - EAPOL –start : début communication EAP over LAN
    - EAPOL-key : passage certificat
    - EAPOL-logout : fin connexion EAP

Durcissement (1)

Minimisation de la surface d'attaque (1)

- Ne lancer que les services nécessaires et n'installer que les programmes nécessaires
  - Définir les services/programmes nécessaires pour un serveur donné
    - Ex : parefeu, DNS : inutile compilateur, Serveur X, zeroconf …
    - Un pgme peut être installé, mais l'exécution désactivée
  - Mettre à jour régulièrement ces services/programmes, désinstaller les autres
  - **Un serveur n'est jamais en DHCP**
  - Vérification via la commande ss (socket statistics) ou netstat -lapute

- Configurer les services si besoin
  - Attention à la configuration par défaut….

Durcissement (2)

- Minimisation de la surface d'attaque (2)
  - Appliquer le principe de moindres privilèges
    - Pas toujours simple à mettre en place
    - Gestion des groupes plus fine (Windows)
    - Restriction des accès : LSM (Linux Security Module)
      - Selinux, Apparmor, seccomp…
  - Faire attention aux programmes lancés en tâche de fond
    - Crontab…
  - Sous Linux, recompiler si nécessaire le noyau en enlevant les modules inutiles
    - ipv6, bluetooth, …

Durcissement (3)

Minimisation de la surface d'attaque (3)

- Chaque service a un compte distinct (pas nobody)
  - Vérifier que c'est le cas
    - Compte postfix, compte www-data, rpcuser…
  - Interdire la connexion pour ces comptes
    - usermod –L compte
- Utilisation du cloisonnement
  - Par conteneur
  - Par hyperviseur
  - Utilisation de la commande chroot (sous unix)
- Restriction des droits d'exécution sous linux
  - Utilisation de la commande sudo

Linux (1)

- DAC/MAC
  - DAC : Discretionary Access Control (par défaut)
  - MAC : Mandatory Access Control
- DAC
  - Chaque utilisateur est maitre de son fichier
    - Il peut en faire ce qu'il veut et donner les droits qu'il veut
    - L'accès aux fichiers dépend de l'owner
    - Changement via chmod, chgrp, etc..
- MAC (exemple : APPARMOR et SELINUX)
  - Rajout des contraintes sur les fichiers
    - Contraintes ajoutées par l'administrateur
    - Même le root subit ces contraintes
    - Noyau interroge apparmor/selinux avant chaque appel système (autorisation)
    - incompatibilité entre apparmor/selinux

Selinux

- Restrictif, et difficile à mettre en œuvre
  - 3 modes : disabled, permissive, enforcing
  - Tous fichiers ou processus à :
    - Un *User* (unconfined_u, system_u, user_u,…)
    - Un *Rôle* (system_r, object_r, …)
    - Un *Type* (httpd_t, user_home_dir_t,..)
  - Un User doit avoir accès au Rôle qui doit pouvoir utiliser Type pour avoir l'autorisation.
  - Les droits sont définis au boot de la machine
    - Fichiers de configuration
    - Possibilité de changer ses droits en live

```
[patrice@testing www]$ ls -lZ
total 20
drwxr-xr-x.  2 root root system_u:object_r:httpd_sys_script_exec_t:s0 4096 Jan  4  2016 cgi-bin
drwxr-xr-x.  3 root root unconfined_u:object_r:httpd_sys_content_t:s0 4096 Jan 29  2018 example
drwxr-xrwx. 14 root root system_u:object_r:httpd_sys_content_t:s0     4096 Sep 23 16:24 html
```

PRA/PCA

- PCA (Plan de Continuité d'Activité)
  - Pour éviter l'interruption des services
    - Mise en place d'un mode dégradé
    - réseau de secours, etc…
- PRA (Plan de Reprise d'Activité)
  - En cas d'incident grave, comment remettre en route le système informatique le plus rapidement possible
    - Procédure à suivre
    - Où trouver les sauvegardes
    - Dans quel ordre remonter les systèmes, etc…

Pare-feu

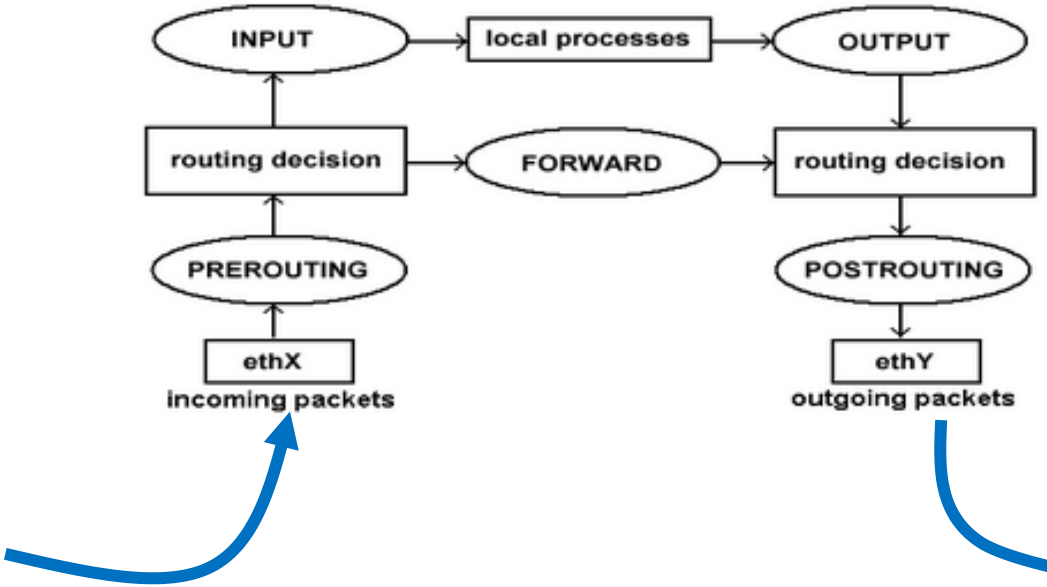
- Elément essentiel dans un réseau
  - Utilise des règles
  - Ne contrôle que ce qui passe par lui
  - N'est pas un antivirus
  - Décision binaire
    - Pare-feu sans état (plus ancien, routeur)
    - Pare-feu avec état (suivi de connexion).
  - Ne peut pas comprendre les flux chiffrés
    - Besoin de plusieurs pare-feux (un sur le réseau, un sur chaque poste)
  - Filtrage au niveau 3 et 4
    - Au-dessus, on parle de proxy ou pare-feu applicatif
    - Filtre @IP, n°port, protocoles, …

Netfilter (1)

- Utiliser par tous les pare-feux linux (iptables)
- Directement intégrer au kernel linux

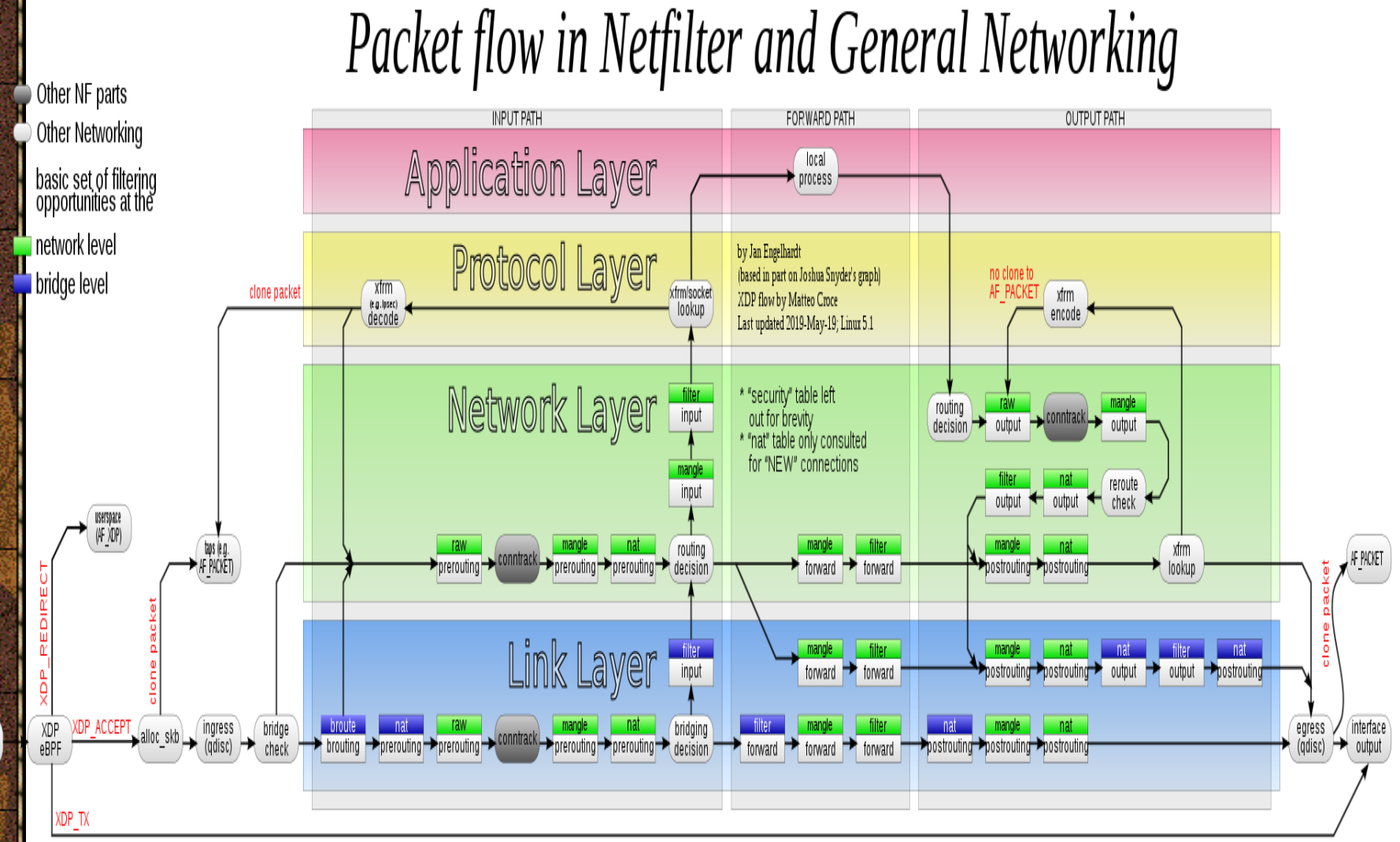
- Flux des informations (très simplifié)

Plusieurs tables
- table filter
- table nat
- table raw
- table mangle



Filter n'existe pas au niveau pre/post routing

Netfilter (2)

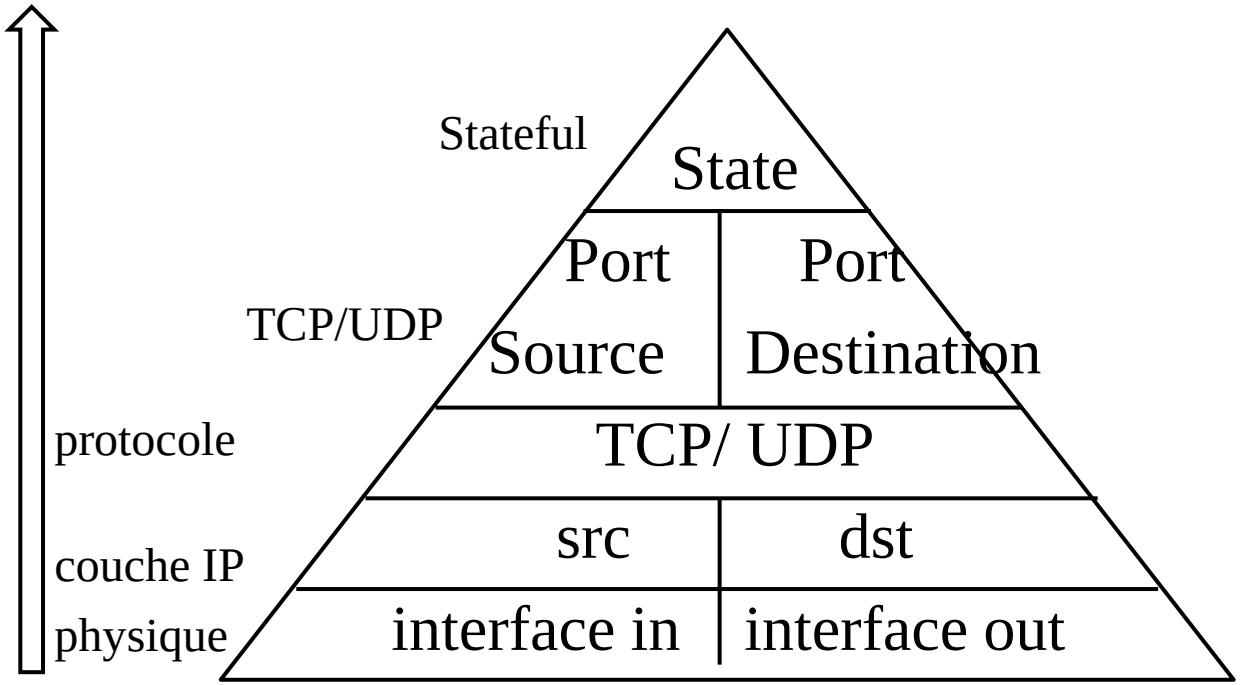

Packet flow in Netfilter and General Networking
Other NF parts
Other Networking
basic set of filtering opportunities at the
network level
bridge level
INPUT PATH
FORWARD PATH
OUTPUT PATH
Application Layer
Protocol Layer
Network Layer
Link Layer
local process
by Jan Engelhardt
(based in part on Joshua Snyder's graph)
XDP flow by Matteo Croce
Last updated 2019-May-19, Linux 5.1
* "security" table left out for brevity
* "nat" table only consulted for "NEW" connections
clone packet
no clone to AF_PACKET
xfrm (e.g. ipsec) decode
xfrm/socket lookup
xfrm encode
filter input
mangle input
routing decision
raw output
conntrack
mangle output
filter output
nat output
reroute check
raw prerouting
mangle prerouting
nat prerouting
mangle forward
filter forward
mangle postrouting
nat postrouting
xfrm lookup
broute brouting
bridging decision
nat output
filter output
nat postrouting
egress (qdisc)
interface output
AF_PACKET
userspace (AF_XDP)
taps (e.g. AF_PACKET)
XDP_REDIRECT
clone packet
(start)
XDP eBPF
XDP_ACCEPT
alloc_skb
ingress (qdisc)
bridge check
XDP_TX

Netfilter (3)

- 3 tables couramment utilisées
  - Filter : input, forward, output
  - Nat : prerouting, input, output, postrouting
  - Mangle : tout, mais opération particulière
- Chaque chaine est indépendante, et ordonnée
- 4 états possibles : ACCEPT, DROP, REJECT, LOG
- Netfilter est un pare-feu avec état, certifié par l'ANSSI
- Différents logiciels l'utilisent :
  - Iptables, ip6tables, arptables,…
  - Nftables utilisent une partie

Iptables (1)

- Gestion d'une règle



Pour être complet, toutes ces informations….

Ex : iptables -A forward -i eth0 -o eth1 -s 195.10.15.0 -d 192.120.10.2 -p tcp
--sport 1024: --dport 80 --syn -m state --state NEW -j ACCEPT

Iptables (2)

- Quelques règles
  - -A : append : ajoute la règle
  - -D : delete : supprime une règle
  - -L : list
  - - F : flush vide toutes les règles d'une chaine
  - -N : créer une nouvelle chaine
  - -P : règle à appliquer par défaut

- Script par défaut (Attention, c'est un parefeu….)

  iptables –P INPUT drop
  iptables –P OUTPUT drop
  iptables –P FORWARD drop

  - Accès à l'interface l0
    - iptables –A input –i lo –j ACCEPT
      iptables –A output –o lo –j ACCEPT