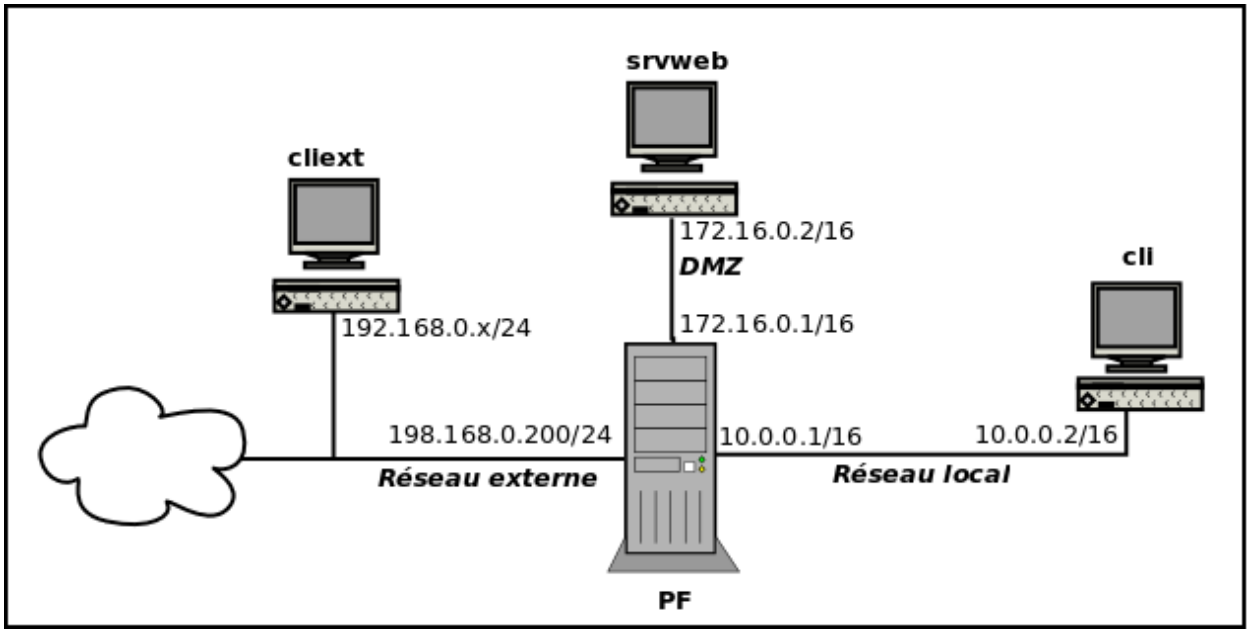
Routage filtrant - DMZ

Mise en œuvre d'un routeur filtrant dans une configuration à 3 réseaux

Prérequis

Schéma



Les machines

- **un routeur Debian 9 (MV VirtualBox) avec 3 cartes réseau *PF* (PareFeu)**
  - ✓ carte 1 (bridgée) : connectée au réseau externe représentant l'internet : 192.168.0.200/24 (adresse fixe à convenir dans le groupe de plot 192.168.0.**100**,192.168.0.**150**,192.168.0.2**00**)
  - ✓ carte 2 (réseau interne **local**) : connectée au réseau interne : 10.0.0.1/16
  - ✓ carte 3 (réseau interne **dmz**) : connectée à la DMZ : 172.16.0.1/16
  - ✓ paquets : links, lynx, tcpdump, nmap (scanner de ports).
- **un client interne Debian 9 *cli***
  - ✓ carte 1 : réseau interne **local**
  - ✓ paquets : links, lynx, tcpdump, nmap
- **un serveur web Debian 9 dans la DMZ *srvweb***
  - ✓ carte 1 : réseau interne **dmz**
  - ✓ paquets : apache2, ssh, links, lynx, tcpdump, nmap,
- **un client externe Debian 9 *cliext***
  - ✓ carte 1 : bridgée : 192.168.0.x en client dhcp
  - ✓ paquets : links, lynx, tcpdump, nmap

Objectifs

- assurer la NAT pour les machines du réseau local
- donner la possibilité d'accéder au serveur **srvweb** en http et ssh depuis partout
- les machines **srvweb** et **PF** doivent être capables de récupérer des paquets sur les dépots debian et de les installer
- autoriser les requêtes DNS sortantes pour toutes les machines
- la machine parefeu **PF** doit être accessible en ssh
- tous les autres flux sont bloqués

Remarques générales

- il est impératif de repérer les chaines concernées par la modification avant d'utiliser **iptables**
- on pourra utiliser **iptables -L** pour vérifier l'effet produit
- on pourra également utiliser **nmap** depuis le bon endroit

Plan de l'atelier

- Etape 0 : vérification de la connectivité
- Etape 0-bis : activation du routage sur PF
- Etape 1 : configuration de base du parefeu – Tout bloquer
- Etape 2 : autoriser l'accès SSH à la machine PF
- Etape 3 : autoriser les requêtes DNS et les installations de paquets (HTTP et FTP) depuis la machine PF
- Etape 4 : mettre en oeuvre la NAT pour le réseau local
- Etape 5 : autoriser les requêtes DNS sortantes pour toutes les machines
- Etape 6 : rendre le serveur srvweb accessible en web et ssh
- Etape 6bis : vérifier que l'accès au réseau local intérieur est interdit (ssh, http)
- Etape 7 : permettre l'installation de paquets sur le serveur srvweb
- Etape 8 : autoriser tous les pings sauf ceux venant de l'extérieur

Etape 0 : vérification de la connectivité

- pas de filtrage sur PF, vidage des tables Filter et Nat :
  - ✓ créer le répertoire **tppf** dans **/root**
  - ✓ créer le script **fw0.sh** dans **/root/tppf** et le rendre exécutable pour le tester.
  - ✓ l'exécuter ./fw0.sh
  - ✓ vérifier avec **iptables -L** et **iptables -L -t nat**
- chacune des 3 machines doit être capable de pinguer l'interface de **PF** située sur le même réseau

Etape 0-bis : activation du routage sur PF

- vérifier les passerelles par défaut pour chacune des machines
  - ✓ cli :
  - ✓ srvweb :
  - ✓ cliext :
  - ✓ PF :
- activer le routage :
- tester les ping
  - ✓ cli → srvweb
  - ✓ cli → cliext
  - ✓ srvweb → cli
  - ✓ srvweb → cliext
  - ✓ cliext → cli
  - ✓ cliext → srvweb

Etape 1 : configuration de base du parefeu – Tout bloquer (fichier fw1.sh)

- modifier le script précédent en **fw1.sh** dans **/root/tppf** et le rendre exécutable pour le tester.
- politique par défaut (DROP pour toutes les chaînes), remise à zéro des tables **filter** et **nat**
- vérifier avec **iptables -L** et **iptables -L -t nat**
- vérifier les ping

Etape 2 : autoriser l'accès en SSH à la machine PF

- modifier le script précédent en **fw2.sh** dans **/root/tppf**
- indiquer les chaines concernées
- tester en se connectant en ssh depuis **cli**, **cliext** et **srvweb**

Etape 3 : autoriser les requêtes DNS et les installations de paquets (HTTP et FTP) depuis la machine PF

- modifier le script précédent en **fw3.sh** dans **/root/tppf**
- indiquer les chaines concernées
- autoriser les requêtes DNS depuis **PF**, vérifier avec **host** ou **nslookup** (paquet net-tools).
- autoriser les requêtes http et ftp sortantes, tester avec **aptitude update**

Etape 4 : mettre en oeuvre la NAT pour le réseau local 10.0.0.0/16

- modifier le script en **fw4.sh** dans **/root/tppf**
- depuis **cli**, vérifier l'accès à une page web avec **lynx** http://www.google.fr
-  la NAT doit être mise en oeuvre sur l'interface **extérieure**

Etape 5 : autoriser les requêtes DNS sortantes pour toutes les machines

- modifier le script précédent en **fw5.sh** dans **/root/tppf**
- indiquer les chaînes concernées
- autoriser les requêtes DNS depuis le réseau **local**, tester avec host ou nslookup depuis **cli**
- autoriser les requêtes DNS depuis le réseau **dmz**, tester avec host ou nslookup depuis **srvweb**

Etape 6 : rendre le serveur srvweb accessible en web et ssh

- modifier le script précédent en **fw6.sh** dans **/root/tppf**
- vérifier l'accès à une page web avec **lynx http://172.16.0.2** depuis **cli**
- vérifier l'accès à une page web avec **lynx http://172.16.0.2** depuis **cliext**
- même chose pour ssh sur le port 22

Etape 6bis : vérifier que l'accès au réseau local intérieur est interdit

- depuis l'extérieur :
- depuis la DMZ :
- modifier si nécessaire le script **fw6.sh** en **fw6b.sh**

Etape 7 : permettre l'installation de paquets sur le serveur srvweb (dns, http)

- modifier le script précédent en **fw7.sh** dans **/root/tppf**
- vérifier avec **apt-get update**

Etape 8 : autoriser tous les pings sauf ceux venant de l'extérieur

- modifier le script précédent en **fw8.sh** dans **/root/tppf**
- tester