Pare feu à DMZ

1. Réalisation du réseau

a. Cablage du réseau
   ip a a 192.168.2.17/24 dev eth1
   ip r a 192.168.2.0/24 dev eth1
   ip r a default via 192.168.2.1

b. Configuration du fichier « /etc/inetd.conf »
   ftp stream tcp nowait nobody /usr/sbin/tcpd in.fingerd
   inetd
   Test du fonctionnement :
   Pour le serveur Web : lynx 192.168.2.29
   Pour le serveur FTP : ncftp 192.168.2.17 (anonymous acces)
   Pour le serveur Finger : finger root@192.168.2.5

c. Le ping passe

d. Les machines internes ne peuvent pas accéder au net : l'internet ne peut pas router une IP en 192.168.x.y donc il ne peut pas y avoir de réponse.

2. Mise en œuvre du SNAT

a. *Iptables –t nat –A POSTROUTING –j SNAT –o eth1 –s 192.168.2.29 --to-source 10.40.2.254*

b. Fonctionnement du NAT

c. Pour http

d. *Iptables –t nat –A POSTROUTING –j SNAT –o eth1 –s 192.168.2.0/24 --to-source 10.40.2.254*

e. Ping simultané

f. Fonctionnement du NAT pour le DNS

3. Mise en œuvre du DNAT

a. Dialogue avec internet :
   Message ICMP :
   Génération de ce message :

b. Configuration :
   Iptables –t nat –A PREROUTING –j DNAT –i eth1 –d 10.40.2.254 –p tcp –dport 80 --to-destination 192.168.2.29:80

c. *Iptables –t nat –A PREROUTING –j DNAT –i eth1 –d 10.40.2.254 –p tcp –dport 8080 --to-destination 192.168.2.5:80*

c. Iptables –nL –t nat && iptables –nL –t filter