TD – Firewall

Le fait de se connecter à Internet sur un lien haut débit ADSL a pour inconvénient d’augmenter le risque d’attaques de pirates.

Un serveur Linux fera office de pare-feu.



Les règles de sécurité suivantes sont mises en œuvre :

Ces règles sont traitées **séquentiellement** jusqu’à ce que l’une d’entre elles soit vérifiée.

Adresses MAC des cartes Ethernet du Pare feu :

* Réseau interne : 00-10-5A-A6-42-A4
* Côté ADSL : 00-40-05-56-B0-D9
1. Déterminer l’action du pare-feu à la réception des trames suivantes. Justifier en indiquant la règle qui vérifie chacune d’entre elles.

ATTENTION les nombres sont en hexadécimal ! ! !

Trame 1

Des: 00-10-5A-A6-42-A4 Src : 00-60-08-1F-F7-4E Type:0800 Ethernet\_II

IP Ver=4 Service=00 LenHead=5 TotalLen=005C Number=C605 frag=0000 TTL=0x01

Des=193.252. 19. 3 Src=192.168.106. 99

Prot=ICMP Demande d'écho

00 E8 FF 01 00 0E 00 00 00 00 00 00 00 00 00 00

Trame 2

Des: 00-10-5A-A6-42-A4 Src : 00-60-08-1F-F7-4E Type:0800 Ethernet\_II

IP Ver=4 Service=00 LenHead=5 TotalLen=003C Number=B905 frag=0000 TTL=0x80

Des=193.252. 19. 1 Src=192.168.106. 99

Prot=UDP Ports Des=0035 Src=0448 len=0028

00 01 01 00 00 01 00 00 00 00 00 00 03 70 6F 70

Trame 3

Des: 00-40-05-56-B0-D9 Src : 00-02-3B-00-22-6F Type:8864 Ethernet\_II

PPP over Ethernet . Ver=01 Type=01. Etape = PPP Session

SessionID=0484 Longueur=003E Protocole=0021

IP Ver=4 Service=00 LenHead=5 TotalLen=003C Number=29DC frag=4000 TTL=0x30

Des=217.128. 50.102 Src=216.239. 39.101

Prot=TCP Ports Des=EE4C Src=0050 seqNum=F648FC38 AckNum=E8D1F0C7

Win=7EDC Control=00010010 Accepte Connexion. SYN Len entete TCP=28

Options =

Taille maxi d'un segment=1412

2.Quelle règle faut-il ajouter (et entre quelles règles) pour que la trame suivante ne soit pas refusée ?

Trame 4

Des: 00-10-5A-A6-42-A4 Src : 00-60-08-1F-F7-4E Type:0800 Ethernet\_II

IP Ver=4 Service=00 LenHead=5 TotalLen=002C Number=1D06 frag=4000 TTL=0x80

Des=216.239. 39.101 Src=192.168.106. 99

Prot=TCP Ports Des=0017 Src=0452 seqNum=00AA442E

Win=2000 Control=00000010 Demande de Connexion. SYN Len entete TCP=18

Options =

Taille maxi d'un segment=1460