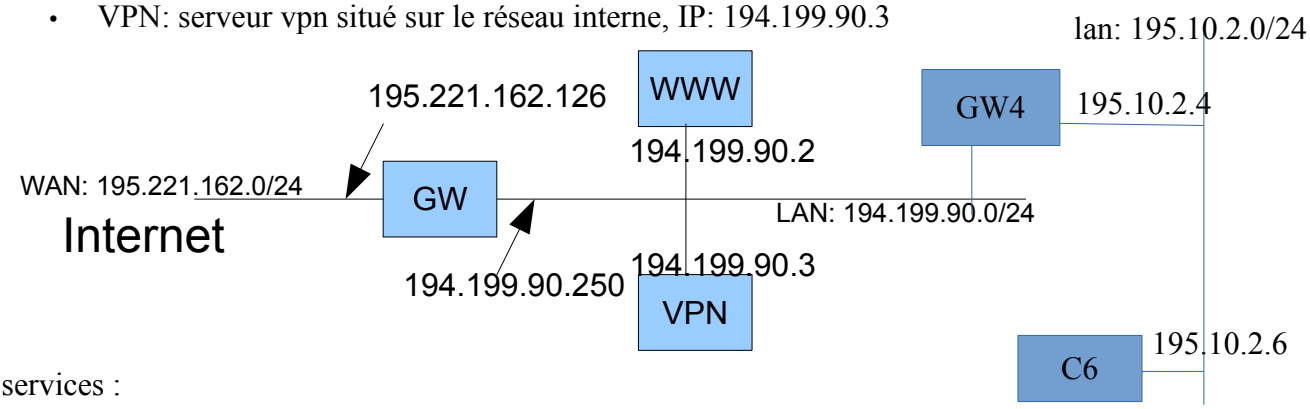
Exercice 1 NetFilter, ipfilter/packet filter: suivi de connexion

Question 1 expliquez la différence entre un simple filtre de paquet et un coupe feu à suivi de connexion.

Question 2 Expliquez à quoi correspond l'état RELATED du firewall netfilter ? Illustrez votre propos par un exemple concret.

Question 3: un administrateur réseau débutant doit configurer le coupe du réseau suivant (ignorez GW4 et C6 qui serviront dans une question ultérieure) où l'on trouve :

- GW: un routeur/coupe feu relié au réseau 195.221.162.0/24 (vers internet, interface eth0, IP 195.221.162.126) et au réseau interne 194.199.90.0/24, interface eth1, IP 194.199.90.250. Il est routeur par défaut des machines WWW, VPN et GW4 (qui ne sert pas dans cette question). le table de routage de GW inclut une route statique vers le lan 195.10.2.0 indiquant que GW4 est le routeur à utiliser dans ce cas.
- WWW: serveur WeB situé sur le réseau interne, IP: 194.199.90.2
- VPN: serveur vpn situé sur le réseau interne, IP: 194.199.90.3



services :

- GW fait office de serveur dns (port 53) et ssh (port 22) tant pour le réseau interne que pour les machines d'internet;
- VPN fournit un service OPENVPN (port 1194) aux hôtes d'internet
- WWW fournit un serveur http (port 80) et https (port 443) à internet.

Notre administrateur réseau souhaite utiliser le coup feu Netfilter pour limiter l'accès à chaque machine à ce qui est utile pour faire fonctionner ce qui est décrit ci-dessus. Pour des questions de temps, on ne s'intéressera qu'aux services suivants:

- ssh
- openvpn
- http et https

Voici le fichier de configuration du coupe feu qu 'il a écrit :

```
#!/bin/bash
#
IPTABLES="/sbin/iptables"
OPENVPN=1194
HTTP=80
HTTPS=443
```

```
SSH=22
#
#############################################################################
# Connection WAN
INET_IP="195.221.162.126"
INET_IP_RANGE="195.221.162.0/24"
INET_IFACE="eth0"
#############################################################################
# Connection LAN
LAN_IP="194.199.90.250"
LAN_IP_RANGE="194.199.90.0/24"
LAN_IFACE="eth1"
#
# hôtes particuliers
WWW_IP="194.199.90.2"
OPENVPN_IP="194.199.90.3"
#############################################################################
# Module loading.
/sbin/depmod -a
/sbin/modprobe ip_tables
/sbin/modprobe ip_conntrack
/sbin/modprobe iptable_filter
/sbin/modprobe iptable_mangle
/sbin/modprobe iptable_nat
/sbin/modprobe ipt_LOG
/sbin/modprobe ipt_limit
/sbin/modprobe ipt_state
/sbin/modprobe ip_conntrack_ftp
/sbin/modprobe ip_nat_ftp
#
# section 1)
#
echo "0" > /proc/sys/net/ipv4/ip_forward
echo "1" > /proc/sys/net/ipv4/conf/all/rp_filter

#############################################################################
#
# on remet tout à zéro
#
```

```
$IPTABLES --flush
$IPTABLES --delete-chain


#
# section 2)
#
$IPTABLES -P INPUT DROP
$IPTABLES -P OUTPUT DROP
$IPTABLES -P FORWARD DROP
#
# section 2 bis
$IPTABLES -A INPUT -p tcp ! --syn -m state --state NEW -j DROP
$IPTABLES -A OUTPUT -p tcp ! --syn -m state --state NEW -j DROP
$IPTABLES -A FORWARD -p tcp ! --syn -m state --state NEW -j DROP


# section 3)
#
$IPTABLES  -A         -i $INET_IFACE -p tcp -s 0/0 -d $INET_IP --dport $SSH -j
ACCEPT
$IPTABLES  -A         -i $INET_IFACE -p tcp -s 0/0 -d $WWW_IP --dport $HTTP -j
ACCEPT
$IPTABLES  -A         -i $INET_IFACE -p tcp -s 0/0 -d $WWW_IP --dport $HTTPS -j
ACCEPT
$IPTABLES  -A         -i $INET_IFACE -p tcp -s 0/0 -d $OPENVPN_IP --sport
$OPENVPN -j ACCEPT
#
# section 4)
#
echo "1" > /proc/sys/net/ipv4/ip_forward
```

On vous rappelle qu'en script shell, si une variable est définie par TOTO=moi, $TOTO représente la valeur de la variable. Ainsi, dans le script $IPTABLE sera remplacé par le contenu de la variable IPTABLE(/sbin/iptables). Il en sera de même pour les autres variables.

[à faire diretement sur le sujet) : Dans un premier temps, on vous demande de compléter les trous qui suivent le "-A" en section 3 par la chaîne appropriée de netfilter : INPUT, FORWARD ou OUTPUT.

Le reste de l'examen est à faire sur votre copie.

Question 4: section 2

expliquez l'utilité de la section 2

Question 5: Dans cette question, on ne s'intéresse pas au dns. les règles proposées dans ce fichier par notre administrateur réseau débutant permettent-elles d'aboutir au résultat souhaité ? Expliquez pourquoi et proposez, sur votre copie, une version correcte de la section 3 (vous ne devez pas modifier les autres sections).

Question 6: proposez des règles permettant à GW de faire office de serveur dns :

- de dns cache pour les machines internes
- de dns primaire pour la zone de l'entreprise pour les machines externes

Exercice 2 traduction d'adresses (NAPT)

Question 1:

Votre réseau local est le 192.168.4.0/24. Il est relié à internet par un routeur coupe-feu Linux netfilter qui a une ip publique fournie par votre fournisseur d'accès à internet 164.2.3.4. Vous avez installé sur votre réseau un serveur WeB qui écoute sur le port 80 de la machine d'ip 192.168.4.12. Est-il possible de faire en sorte que ce serveur WeB soit joignable depuis internet ? Si oui, vous nommerez et expliquerez comment cela est possible ainsi que le trajet des paquets entre un client situé sur internet et votre serveur WeB. Dans le cas contraire, vous expliquez pourquoi ce n'est pas possible.

Exercice 3 stratégies de groupes

Exercice supprimé car spécifique au programme 2012-2013