

Routage classique

Q1)

Sur la machine FIREWALL, les services actifs sont :

Netstat -a

* :sunrpc, localhost :domain, * :ssh, localhost :smtp, localhost:953, *:53856. Tous sont des protocoles TCP

:::sunrpc, :::domain, :::ssh, localhost:smtp, localhost:953, :::54013. Tous sont des protocoles TCP6

Q2)

Destination	Passerelle	Genmask	Indic	Metric	Ref	Use	Iface
0.0.0.0	192.168.1.1	0.0.0.0	UG				Eth0
192.168.2.0	192.168.2.1	255.255.255.0	U				eth2
195.168.1.0	195.168.1.1	255.255.255.0	U				Eth1
192.168.1.0	192.168.1.1	255.255.255.0	U				Eth0

Configuration du serveur http

Q3) Le port TCP d'écoute standard d'un serveur web sécurisé est 433.

Q4) On observe plusieurs fois le serveur apache pour vérifier si les paramètres ont bien été pris en comptes. Quel que soit le fichier rééditer, il est important de reload le serveur apache et de regarder si les effets désirer sont présents.

Q5) Par défaut la page web qui s'ouvre est index.html avec le contenu « it work »

Q6) cat /etc/debian_version & uname -a

Debian 7.2 | Kernel 3.2

Sur le serveur DMZ

Q7) Après l'installation d'apache, la liste des services actif sont :

22/tcp	Ssh
111/tcp	Rpcbind
8080/tcp	http-proxy
8443/tcp	https-alt

Q8)

```
iptables -P INPUT DROP
iptables -P OUTPUT DROP
iptables -P FORWARD DROP
```

Q9) iptables -L

```
Chain INPUT (policy DROP)
Target    prot opt source      destination
All -- anywhere anywhere
Chain FORWARD (policy DROP)
Target    proto pt source      destination
All -- anywhere anywhere
Chain OUTPUT (policy DROP)
Target    proto pt source      destination
All -- anywhere anywhere
```

Filtrage entre LAN et DMZ

Q10)

```
iptables -A INPUT -s 192.168.2.0/24 -i eth1 -p icmp -j ACCEPT
iptables -A OUTPUT -s 192.168.1.0/24 -p icmp -j ACCEPT
```

Q11)

```
iptables -A INPUT -s 192.168.1.0/24 -i eth2 -p icmp -j ACCEPT
iptables -A OUTPUT -s 192.168.1.0/24 -p icmp -j ACCEPT
```

Q12)

```
iptables -A FORWARD -s 192.168.2.0/24 -d 192.168.1.0/24 -i eth1 -o
eth2 -p icmp -icmp-type echo-request -j ACCEPT
```

```
iptables -A FORWARD -s 192.168.1.0/24 -d 192.168.2.0/ -i eth2 -o
eth1 -p icmp -icmp-type echo-reply -j ACCEPT
```

Q13)

```
ICMP -reply
ICMP -request
```

Q14)

```
iptables -A FORWARD -s 192.168.2.0/24 -d 192.168.1.0/24 -i eth1 -o eth2 -p tcp -dport 8080 -j
ACCEPT
iptables -A FORWARD -s 192.168.2.0/24 -d 192.168.1.0/24 -i eth1 -o eth2 -p tcp -dport 8443 -j
ACCEPT
```

```
iptables -A FORWARD -s 192.168.1.0/24 -d 192.168.2.0/24 -i eth2 -o eth1 -p tcp --dport 8080 -j ACCEPT
```

Q15)

```
iptables -A POSTROUTING -t nat -o eth0 -j MASQUERADE
```

Filtrage (DMZ) et (INTERNET)

Q16)

Configuration DMZ

```
iptables -A FORWARD -t filter -i eth0 -d 192.168.1.1 -p tcp --dport 8080 -j ACCEPT
iptables -A FORWARD -t filter -i eth0 -d 192.168.1.1 -p tcp --dport 8443 -j ACCEPT
iptables -A FORWARD -t filter -o eth0 -s 192.168.1.1 -p tcp --sport 8080 -j ACCEPT
iptables -A FORWARD -t filter -o eth0 -s 192.168.1.1 -p tcp --sport 8443 -j ACCEPT
iptables -A PREROUTING -t nat -i eth0 -p tcp --dport 80 -j DNAT --to-destination 192.168.1.1:8080
iptables -A PREROUTING -t nat -i eth0 -p tcp --dport 443 -j DNAT --to-destination 192.168.1.1:8443
```

Q17)

Accès au serveur web depuis le pc internet

PING 192.168.1.1 (192.168.1.1) 56(84) bytes of data.

--- 192.168.1.2 ping statistics ---

2 packets transmitted, 0 received, 100% packet loss, time 1000ms

#accès au serveur depuis l'ip du routeur qui gère la DMZ

```
curl 195.168.1.1
```

```
<html><body><h1>It works!</h1>
```

```
<p>This is the default web page for this server.</p>
```

```
<p>The web server software is running but no content has been added, yet.</p>
```

```
</body></html>
```

Annexes

Fichier de configuration du PC internet

```
#!/bin/bash

echo "1" > /proc/sys/net/ipv4/ip_forward

function start {

    modprobe ipt_MASQUERADE
    ifconfig eth1 195.168.1.1 netmask 255.255.255.0
    route add -net 192.168.1.0 netmask 255.255.255.0 gw 195.168.1.254
    route add -net 192.168.2.0 netmask 255.255.255.0 gw 195.168.1.254
    iptables -A POSTROUTING -t nat -o eth0 -j MASQUERADE
    iptables -A FORWARD -t filter -i eth1 -o eth0 -j ACCEPT
    echo "hey brownie"
}

function stop {

    iptables -t filter -F
    iptables -t nat -F
    iptables -P INPUT ACCEPT
    iptables -P FORWARD ACCEPT
    iptables -P OUTPUT ACCEPT

    echo "bye brownie"
}

case $1 in
    start ) start ;;
    stop ) stop ;;
    restart ) stop;start;;
esac
```

Fichier configuration du routeur

```
#!/bin/bash

echo "1" > /proc/sys/net/ipv4/ip_forward

function start {

# conf des interfaces
  modprobe ipt_MASQUERADE

  ifconfig eth0 195.168.1.254 netmask 255.255.255.0 up
  route add default gw 195.168.1.1

  ifconfig eth1 192.168.2.254 netmask 255.255.255.0 up
  ifconfig eth2 192.168.1.254 netmask 255.255.255.0 up

# Policy par default
  iptables -P INPUT DROP
  iptables -P OUTPUT DROP
  iptables -P FORWARD DROP

# on en casse pas les connexions existantes
  iptables -A FORWARD -t filter -m state --state ESTABLISHED,RELATED
  #iptables -A INPUT -t filter -m state --state ESTABLISHED,RELATED
  #iptables -A OUTPUT -t filter -m state --state ESTABLISHED,RELATED

# on autorise le ping vers la passerelle
  iptables -A INPUT -t filter -s 192.168.2.0/24 -d 192.168.2.254 -i eth1 -p icmp --icmp-type echo-request -j ACCEPT
  iptables -A INPUT -t filter -s 192.168.1.0/24 -d 192.168.1.254 -i eth2 -p icmp --icmp-type echo-request -j ACCEPT
  iptables -A OUTPUT -t filter -p icmp --icmp-type echo-reply -j ACCEPT

# Autorise le ping sur l'interface web, utilie pour tester la connectivité externe.
  iptables -A INPUT -t filter -s 195.168.1.0/24 -d 195.168.1.254 -i eth0 -p icmp --icmp-type echo-request -j ACCEPT

# On autorise le ping depuis le LAN vers la DMZ
  iptables -A FORWARD -t filter -s 192.168.2.0/24 -d 192.168.1.0/24 -i eth1 -o eth2 -p icmp --icmp-type echo-request -j ACCEPT
  iptables -A FORWARD -t filter -s 192.168.1.0/24 -d 192.168.2.0/24 -i eth2 -o eth1 -p icmp --icmp-type echo-reply -j ACCEPT

# On autorise le LAN a contacter le serveur web
  iptables -A FORWARD -t filter -s 192.168.2.0/24 -d 192.168.1.0/24 -i eth1 -o eth2 -p tcp --dport 8080 -j ACCEPT
```

```
iptables -A FORWARD -t filter -s 192.168.2.0/24 -d 192.168.1.0/24 -i eth1 -o eth2 -p tcp --dport 8443 -j ACCEPT
```

```
iptables -A FORWARD -t filter -s 192.168.1.0/24 -d 192.168.2.0/24 -i eth2 -o eth1 -j ACCEPT
```

```
#ping et http sur le net
```

```
#iptables -A POSTROUTING -t nat -o eth0 -j MASQUERADE
```

```
iptables -A POSTROUTING -t nat -s 192.168.2.0/24 -j SNAT --to-source 195.168.1.254
```

```
iptables -A FORWARD -t filter -s 192.168.2.0/24 -i eth1 -o eth0 -p tcp --dport 80 -j ACCEPT
```

```
iptables -A FORWARD -t filter -s 192.168.2.0/24 -i eth1 -o eth0 -p tcp --dport 443 -j ACCEPT
```

```
iptables -A FORWARD -t filter -s 192.168.2.0/24 -i eth1 -o eth0 -p icmp --icmp-type echo-request -j ACCEPT
```

```
iptables -A FORWARD -t filter -i eth0 -o eth1 -p icmp --icmp-type echo-reply -j ACCEPT
```

```
iptables -A FORWARD -t filter -i eth0 -d 192.168.2.0/24 -p tcp --sport 443 -j ACCEPT
```

```
iptables -A FORWARD -t filter -i eth0 -d 192.168.2.0/24 -p tcp --sport 80 -j ACCEPT
```

```
# Configuration DMZ
```

```
iptables -A FORWARD -t filter -i eth0 -d 192.168.1.1 -p tcp --dport 8080 -j ACCEPT
```

```
iptables -A FORWARD -t filter -i eth0 -d 192.168.1.1 -p tcp --dport 8443 -j ACCEPT
```

```
iptables -A FORWARD -t filter -o eth0 -s 192.168.1.1 -p tcp --sport 8080 -j ACCEPT
```

```
iptables -A FORWARD -t filter -o eth0 -s 192.168.1.1 -p tcp --sport 8443 -j ACCEPT
```

```
iptables -A PREROUTING -t nat -i eth0 -p tcp --dport 80 -j DNAT --to-destination 192.168.1.1:8080
```

```
iptables -A PREROUTING -t nat -i eth0 -p tcp --dport 443 -j DNAT --to-destination 192.168.1.1:8443
```

```
echo "hey brownie"
```

```
}
```

```
function stop {
```

```
iptables -t filter -F
```

```
iptables -t nat -F
```

```
iptables -P INPUT ACCEPT
```

```
iptables -P FORWARD ACCEPT
```

```
iptables -P OUTPUT ACCEPT
```

```
echo " bye brownie"
```

```
}
```

```
case $1 in
```

```
start ) start ;;
```

```
stop ) stop ;;
```

```
restart ) stop;start;;
```

```
esac
```

```
#!/bin/bash
```