

TP02 – Routage, NAT, Filtrage & FTP (with-routers.imn)

tp02.SCR.3.2

0. Rappels sur la topologie & les adresses

Réseaux privés (RFC 1918)

- S1 : 172.16.1.0/24
- S2 : 172.16.2.0/24
- S3 : 172.16.3.0/24

Réseaux publics (routables)

Adresse utilisée	Masque	Réseau CIDR	Plage
37.37.37.1	/22	37.37.36.0/22	37.37.36.0 – 37.37.39.255
45.45.45.254	/21	45.45.40.0/21	45.45.40.0 – 45.45.47.255
62.62.62.253	/19	62.62.48.0/19	62.62.48.0 – 62.62.79.255
37.37.37.254	/22	37.37.36.0/22	même réseau que ci-dessus
45.45.45.253	/21	45.45.40.0/21	même réseau que ci-dessus
62.62.62.254	/19	62.62.48.0/19	même réseau que ci-dessus

PARTIE I – Topologie with-routers.imn

I.1 Construction de la topologie

- Partir d'une copie de `two-gateways.imn` du TP précédent.

- Renommer/adapter pour obtenir `with-routers.imn` avec les mêmes noms / adresses que dans l'énoncé.

I.2 Configuration de GW1 (n10)

```
node n10 {
  type host
  network-config {
    hostname GW1
    !
    interface eth1
      ip address 172.16.2.253/24
      mac address 42:00:aa:00:00:09
    !
    interface eth0
      ip address 172.16.1.253/24
      mac address 42:00:aa:00:00:08
    !
    interface lo0
      type lo
      ip address 127.0.0.1/8
      ipv6 address ::1/128
    !
  }
  canvas c0
  iconcoords {288 240}
  labelcoords {288 276}
  interface-peer {eth0 n0}
  interface-peer {eth1 n1}
  custom-configs {
    custom-config-id default {
      custom-command /bin/sh
      config {
        # --- IP ---
        ip addr add 127.0.0.1/8 dev lo0
        ip addr add 172.16.1.253/24 dev eth0
        ip addr add 172.16.2.253/24 dev eth1
        ip -6 addr add ::1/128 dev lo0

        # --- Forwarding ---
        sysctl -w net.ipv4.ip_forward=1
      }
    }
  }
}
```

```

# --- ROUTES ---
# Route par défaut vers GW2
ip route add 0.0.0.0/0 via 172.16.2.254

# --- NAT ---
# S1 -> S2 (pour les réponses)
iptables -t nat -A POSTROUTING \
    -s 172.16.1.0/24 -d 172.16.2.0/24 \
    -j SNAT --to-source 172.16.2.253

# --- FILTRAGE ---
# 1. Autoriser les connexions déjà établies
iptables -A FORWARD -m state --state
ESTABLISHED,RELATED -j ACCEPT

# 2. S1 <-> S2 : AUTORISÉ
iptables -A FORWARD -s 172.16.1.0/24 -d
172.16.2.0/24 -j ACCEPT
iptables -A FORWARD -s 172.16.2.0/24 -d
172.16.1.0/24 -j ACCEPT

# 3. S1 -> S3 : BLOQUÉ
iptables -A FORWARD -s 172.16.1.0/24 -d
172.16.3.0/24 -j DROP

# 4. Politique par défaut
iptables -P FORWARD DROP

# Services
rpcbind
inetd
}
}
}
custom-enabled true
custom-selected default
}

```

I.3 Configuration de GW2 (n11)

```

node n11 {
    type host

```

```

network-config {
    hostname GW2
    !
    interface eth2
        ip address 45.45.45.254/21
        mac address 42:00:aa:00:00:0c
    !
    interface eth1
        ip address 172.16.3.254/24
        mac address 42:00:aa:00:00:0b
    !
    interface eth0
        ip address 172.16.2.254/24
        mac address 42:00:aa:00:00:0a
    !
    interface lo0
        type lo
        ip address 127.0.0.1/8
        ipv6 address ::1/128
    !
}
canvas c0
iconcoords {624 360}
labelcoords {624 396}
interface-peer {eth0 n1}
interface-peer {eth1 n2}
interface-peer {eth2 n3}
custom-configs {
    custom-config-id default {
        custom-command /bin/sh
        config {
            # --- IP ---
            ip addr add 127.0.0.1/8 dev lo0
            ip addr add 172.16.2.254/24 dev eth0
            ip addr add 172.16.3.254/24 dev eth1
            ip addr add 45.45.45.254/21 dev eth2
            ip -6 addr add ::1/128 dev lo0

            # --- Forwarding ---
            sysctl -w net.ipv4.ip_forward=1
        }
    }
}

```

```

# --- ROUTES vers autres réseaux publics ---
ip route add 37.37.36.0/22 via 172.16.2.253 dev eth0
ip route add 62.62.48.0/19 via 172.16.2.253 dev eth0

# --- NAT ---
# S1/S2 -> Internet
iptables -t nat -A POSTROUTING \
    -s 172.16.1.0/24 -o eth2 \
    -j SNAT --to-source 45.45.45.254
iptables -t nat -A POSTROUTING \
    -s 172.16.2.0/24 -o eth2 \
    -j SNAT --to-source 45.45.45.254

# S2 <-> S3
iptables -t nat -A POSTROUTING \
    -s 172.16.2.0/24 -d 172.16.3.0/24 \
    -j SNAT --to-source 172.16.3.254
iptables -t nat -A POSTROUTING \
    -s 172.16.3.0/24 -d 172.16.2.0/24 \
    -j SNAT --to-source 172.16.2.254

# --- FILTRAGE ---
# 1. Connexions établies
iptables -A FORWARD -m state --state
ESTABLISHED,RELATED -j ACCEPT

# 2. S2 <-> S3 : AUTORISÉ
iptables -A FORWARD -s 172.16.2.0/24 -d
172.16.3.0/24 -j ACCEPT
iptables -A FORWARD -s 172.16.3.0/24 -d
172.16.2.0/24 -j ACCEPT

# 3. S3 -> S1 : BLOQUÉ
iptables -A FORWARD -s 172.16.3.0/24 -d
172.16.1.0/24 -j DROP

# 4. S1/S2 -> Internet : AUTORISÉ
iptables -A FORWARD -s 172.16.1.0/24 -d
45.45.40.0/21 -j ACCEPT
iptables -A FORWARD -s 172.16.2.0/24 -d
45.45.40.0/21 -j ACCEPT

```

```

        iptables -A FORWARD -s 172.16.1.0/24 -d
37.37.36.0/22 -j ACCEPT
        iptables -A FORWARD -s 172.16.2.0/24 -d
37.37.36.0/22 -j ACCEPT

        # 5. S3 -> Internet : BLOQUÉ
        iptables -A FORWARD -s 172.16.3.0/24 -d
45.45.40.0/21 -j DROP
        iptables -A FORWARD -s 172.16.3.0/24 -d
37.37.36.0/22 -j DROP

        # 6. Politique par défaut
        iptables -P FORWARD DROP

        # Services
        rpcbind
        inetd
    }
}
}
custom-enabled true
custom-selected default
}

```

I.4 Configuration des PCs (routes par défaut)

Exemple pour **pc2 (n7)** :

```

node n7 {
    type pc
    network-config {
        hostname pc2
        !
        interface eth0
            ip address 172.16.2.2/24
            mac address 42:00:aa:00:00:05
        !
        interface lo0
            type lo
            ip address 127.0.0.1/8
            ipv6 address ::1/128
        !
    }
}

```

```

        # Route par défaut vers GW2
        ip route 0.0.0.0/0 172.16.2.254
        !
    }
    # ...
}

```

(Le même principe s'applique aux autres PCs si nécessaire.)

I.5 Tests de connectivité

À lancer après démarrage de la topo :

```

# S1 -> public
sudo himage pc1 ping -c 1 37.37.37.1

# S2 -> public
sudo himage pc2 ping -c 1 37.37.37.1

# public -> public
sudo himage pc ping -c 1 45.45.45.2

# même réseau public
sudo himage host1 ping -c 1 37.37.37.1

# public -> privé (doit échouer)
sudo himage pc ping -c 1 172.16.2.2
# -> Destination Net Unreachable

```

I.6 Analyse NAT avec tcpdump

Ping depuis **pc2** vers l'hôte public :

```

# Sur pc (public)
sudo himage pc tcpdump -i eth0 -n icmp

# Sur pc2 (S2)
sudo himage pc2 tcpdump -i eth0 -n icmp

# Ping
sudo himage pc2 ping -c 2 37.37.37.1

```

- Sur **pc2** : tu vois 172.16.2.2 -> 37.37.37.1
- Sur **pc** : tu vois 45.45.45.254 -> 37.37.37.1

Le routeur GW2 fait du **SNAT** : il remplace la source privée 172.16.2.2 par son IP publique 45.45.45.254.

PARTIE II – Service FTP avec DNAT

II.1 Création de with-ftp-service.imn

```
cp with-routers.imn with-ftp-service.imn
```

II.2 Ajout du serveur FTP (n14) sur S2

```
node n14 {
    type host
    network-config {
        hostname FTP
        !
        interface eth0
            ip address 172.16.2.10/24
            mac address 42:00:aa:00:00:0f
        !
        interface lo0
            type lo
            ip address 127.0.0.1/8
            ipv6 address ::1/128
        !
    }
    canvas c0
    iconcoords {480 120}
    labelcoords {480 156}
    interface-peer {eth0 n1} # switch2
    custom-configs {
        custom-config-id default {
            custom-command /bin/sh
            config {
                # Démarrer le serveur FTP
                /usr/sbin/in.ftpd &
                # (ou autre commande selon l'image)
```



```

        }
    }
}
custom-enabled true
custom-selected default
}

link l14 {
    nodes {n1 n14}
    bandwidth 0
}

```

II.3 DNAT sur GW2 pour exposer FTP

Dans la config de GW2 (n11), ajouter :

```

# --- DNAT FTP depuis Internet vers le serveur interne ---

# Port 21 (contrôle)
iptables -t nat -A PREROUTING \
    -d 45.45.45.254 -p tcp --dport 21 \
    -j DNAT --to-destination 172.16.2.10:21

# Port 20 (données, mode actif)
iptables -t nat -A PREROUTING \
    -d 45.45.45.254 -p tcp --dport 20 \
    -j DNAT --to-destination 172.16.2.10:20

# Autoriser le forwarding vers le serveur FTP
iptables -A FORWARD -d 172.16.2.10 -p tcp --dport 21 -j ACCEPT
iptables -A FORWARD -d 172.16.2.10 -p tcp --dport 20 -j ACCEPT

# Autoriser FTP depuis S1 et S2 (accès direct à 172.16.2.10)
iptables -A FORWARD -s 172.16.1.0/24 -d 172.16.2.10 -p tcp --dport 21 -j ACCEPT
iptables -A FORWARD -s 172.16.2.0/24 -d 172.16.2.10 -p tcp --dport 21 -j ACCEPT

```

Rappel :

- **PREROUTING** : avant le routage, on peut faire du **DNAT** (changer la destination).

- Ici on publie le service FTP interne 172.16.2.10 sur l'IP publique 45.45.45.254.

II.4 Vérification du serveur FTP

```
# Le service écoute bien sur 21/tcp
sudo himage FTP ss -na --tcp
# Doit montrer : LISTEN sur *:21

# Port FTP dans /etc/services
sudo himage FTP cat /etc/services | grep ftp
# -> ftp 21/tcp
```

II.5 Tests d'accès FTP

```
# 1. Depuis pc (public) vers IP publique : OK
sudo himage pc ftp 45.45.45.254

# 2. Depuis pc (public) vers IP privée : NON routable
sudo himage pc ftp 172.16.2.10
# -> Network is unreachable

# 3. Depuis pc1 (S1) vers IP privée : OK
sudo himage pc1 ftp 172.16.2.10

# 4. Depuis pc2 (S2) vers IP privée : OK
sudo himage pc2 ftp 172.16.2.10

# 5. Depuis host1 (réseau public 45.45.45.0/21) : OK
sudo himage host1 ftp 45.45.45.254
```

II.6 Analyse FTP avec tcpdump

```
# Sur pc (public)
sudo himage pc tcpdump -i eth0 -n tcp port 21

# Sur FTP (serveur interne)
sudo himage FTP tcpdump -i eth0 -n tcp port 21

# Connexion FTP
sudo himage pc ftp 45.45.45.254
```

- Côté **pc** : connexion 37.37.37.1 -> 45.45.45.254:21
- Côté **FTP** : connexion 172.16.2.254 -> 172.16.2.10:21

GW2 fait :

- **DNAT** : 45.45.45.254:21 → 172.16.2.10:21 (destination modifiée)
- **SNAT** : 37.37.37.1 → 172.16.2.254 (source modifiée pour que les réponses repartent bien via GW2)

Récapitulatif des règles essentielles

Sur GW1

```
# NAT S1 -> S2
iptables -t nat -A POSTROUTING \
    -s 172.16.1.0/24 -d 172.16.2.0/24 \
    -j SNAT --to-source 172.16.2.253

# Filtrage
iptables -A FORWARD -s 172.16.1.0/24 -d 172.16.2.0/24 -j ACCEPT #
S1 -> S2
iptables -A FORWARD -s 172.16.2.0/24 -d 172.16.1.0/24 -j ACCEPT #
S2 -> S1
iptables -A FORWARD -s 172.16.1.0/24 -d 172.16.3.0/24 -j DROP    #
S1 -> / S3
```

Sur GW2

```
# NAT S1/S2 -> Internet
iptables -t nat -A POSTROUTING -s 172.16.1.0/24 -o eth2 \
    -j SNAT --to-source 45.45.45.254
iptables -t nat -A POSTROUTING -s 172.16.2.0/24 -o eth2 \
    -j SNAT --to-source 45.45.45.254

# DNAT FTP
iptables -t nat -A PREROUTING -d 45.45.45.254 -p tcp --dport 21 \
    -j DNAT --to-destination 172.16.2.10:21

# Filtrage (extraits)
```

```
iptables -A FORWARD -s 172.16.2.0/24 -d 172.16.3.0/24 -j ACCEPT #  
S2 -> S3  
iptables -A FORWARD -s 172.16.3.0/24 -d 172.16.1.0/24 -j DROP #  
S3 -> S1  
iptables -A FORWARD -s 172.16.1.0/24 -d 45.45.40.0/21 -j ACCEPT #  
S1 -> Internet  
iptables -A FORWARD -s 172.16.3.0/24 -d 45.45.40.0/21 -j DROP #  
S3 -> Internet
```