# Activité iptables

# Objectif de l’activité

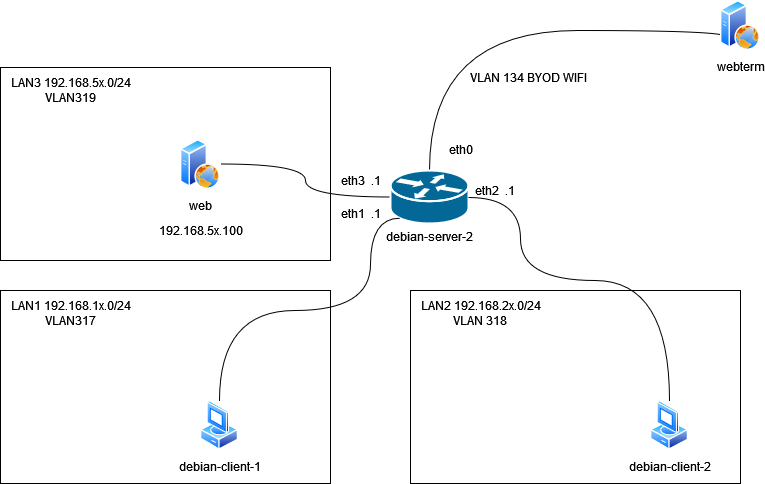
* simuler un petit réseau LAN avec deux sous-réseaux **192.168.1.0/24** et **192.168.2.0/24 relié** par un routeur Debian
* configurer des services réseaux de base :
  + Nat pour accéder à Internet et publier un serveur Web Interne
  + Filtrage du trafic entre les deux sous-réseaux à l’aide d’un pare-feu (iptables).

# Environnement de travail pour le TP

Création de conteneur LXC sur Proxmox

# Activité

## 3.1 Topologie physique



## Configuration IP du routeur (debian-server-2) et des clients

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Périphérique** | **Interface** | **Adresse IP** | **Masque de sous-réseau** | **Passerelle par défaut** |
| web | eth0 | 192.168.5x.100 | 255.255.255.0 | 192.168.5x.1 |
| webterm |  |  |  |  |
| Debian-server-21 | eth0 | 10.187.35. | 255.255.255.0 |  |
| eth1 | 192.168.1x.1 | 255.255.255.0 |  |
|  | eth2 | 192.168.2x.1 | 255.255.255.0 |  |
|  | eth3 | 192.168.5x.1 | 255.255.255.0 |  |
| debian-client-1 | eth0 | 192.168.1x.20 | 255.255.255.0 | 192.168.1x.1 |
| debian-client-2 | eth0 | 192.168.2x.20 | 255.255.255.0 | 192.168.2x.1 |

Configuration des deux interfaces du routeur

* Configure le routage au niveau du routeur

|  |
| --- |
| commande cli debian-server-2  Debian-server-2# |

## NAT et filtrage

## Question 1 : vider les tables filter et nat sur le nœud debian-server-2

* Lancer le terminal
* Vider les tables filter et NAT

|  |
| --- |
| commande cli debian-server-2  root@debian-debian-2:/# iptables -t filter -F  root@debian-debian-2:/# iptables -t filter -X  root@debian-debian-2:/# iptables -t nat -F  root@debian-debian-2:/# iptables -t nat -X |

* Visualiser le contenu des tables filter et nat

Une image contenant texte

Description générée automatiquement

## Question 2 : appliquer les politiques par défaut suivantes sur le nœud debian-server-2

* rejet (silencieux) de tout paquet entrant
* rejet (silencieux) de transfert de paquet
* accepter tous les paquets sortant

|  |
| --- |
| commande cli debian-server-2  root@debian-debian-2:/# iptables -P INPUT DROP  root@debian-debian-2:/# iptables -P FORWARD DROP  root@debian-debian-2:/# iptables -P OUTPUT ACCEPT |

* Visualisation les politiques par défaut

Une image contenant texte

Description générée automatiquement

## Question 3 : vérifier avec des ping l’application des politiques par défaut sur le nœud debian-server-2

|  |
| --- |
| commande cli debian-server-2  root@debian-debian-2:/# ping 192.168.50.100  root@debian-debian-2:/# ping 192.168.122.2 |

Une image contenant texte

Description générée automatiquement

Plus aucune réponse aux requêtes ping car requêtes sont bloquées.

## Question 4 : autoriser le trafic ICMP en entrée sur les interfaces eth0, eth1, eth2 et eth3 sur le nœud debian-server-2

* 1) Accepter les requêtes ICMP en entrée à partir des interfaces eth0, eth1, eth2 et eth3

|  |
| --- |
| commande cli debian-server-2  root@debian-debian-2:/# iptables -A INPUT -p icmp --icmp-type echo-request -m limit --limit 100/s -i eth0 -j ACCEPT  root@debian-debian-2:/# iptables -A INPUT -p icmp --icmp-type echo-request -m limit --limit 100/s -i eth1 -s 192.168.1.0/24 -j ACCEPT  root@debian-debian-2:/# iptables -A INPUT -p icmp --icmp-type echo-request -m limit --limit 100/s -i eth2 -s 192.168.2.0/24 -j ACCEPT  root@debian-debian-2:/# iptables -A INPUT -p icmp --icmp-type echo-request -m limit --limit 100/s -i eth3 -s 192.168.50.0/24 -j ACCEPT |

## Question 5 : créer une règle du SNAT dynamique (masquerade) pour les flux qui sortent par eth0 du nœud debian-server-2

|  |
| --- |
| commande cli debian-server-2  root@debian-debian-2:/# iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE |

## Question 6 : autoriser le transfert des requêtes ICMP après routage vers l’interface de sortie eth0

|  |
| --- |
| commande cli debian-server-2  root@debian-debian-2:/# iptables -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT  root@debian-debian-2:/# iptables -A FORWARD -p icmp -i eth1 -o eth0 -s 192.168.1.0/24 -j ACCEPT  root@debian-debian-2:/# iptables -A FORWARD -p icmp -i eth2 -o eth0 -s 192.168.2.0/24 -j ACCEPT |

* Vérification : debian-client-1 peut réaliser un ping sur les interfaces de debian-server-2, sur Internet mais pas vers un client du LAN2 (debian-client-2 – 192.168.2.2)

## Question 7 : redirection de traffic http et HTTPS à destination du serveur Web

Autoriser les requêtes sur les ports 80 et 443 venant d’internet (interface eth0 de debian-server-2) vers le serveur web internet 192.168.50.100 accessible avec l’interface eth3

|  |
| --- |
| commande cli debian-server-2  root@debian-debian-2:/# iptables -A FORWARD -i eth3 -o eth0 -s 192.168.50.0/24 -j ACCEPT  root@debian-debian-2:/# iptables -A FORWARD -i eth0 -o eth3 -p tcp --dport 80 -j ACCEPT  root@debian-debian-2:/# iptables -A FORWARD -i eth0 -o eth3 -p tcp --dport 443 -j ACCEPT  root@debian-debian-2:/# iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 80 -j DNAT --to-destination 192.168.50.100  root@debian-debian-2:/# iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 443 -j DNAT --to-destination 192.168.50.100 |