université de BORDEAUX

Master 1 *Sciences Technologies*

ANNÉE 2022-2023
Étape : Master Sciences Technologies (semestre 2)
Épreuve de : Administration des réseaux
Date : 2 Mai 2023
Heure : 9h00

SESSION DE MAI 2023
UE : 4TIN808
Durée : 1h30
Documents interdits
Épreuve de Monsieur Guermouche

Questions générales

1. Expliquer de manière synthétique le principe de la translation d'adresses dynamique.
2. Expliquer la principale différence entre le protocole d'autonconfigure d'adresses IPv6 (SLAAC) et le protocole DHCP.
3. Quel sont les avantages de l'utilisation des VLANs pour la gestion d'un réseau local. Justifiez votre réponse.
4. Dans le moteur d'authentification linux quel est le rôle joué par NSS (*Name Service Switch*) ? Qu'en est il de PAM (*Pluggable Authentication Modules*) ?
5. Dans un système de stockage (DAS, NAS, SAN), quel est l'intérêt de l'utilisation du RAID ? Quelle sont les fonctions de base sur lesquelles tous les niveaux de RAID sont contruits ?

Exercices

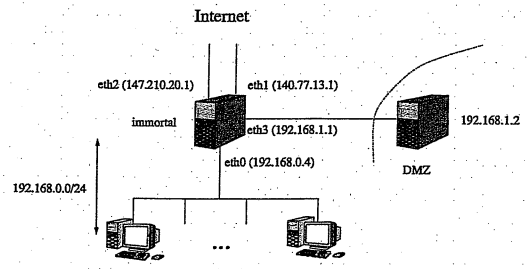
6. Un serveur FTP se trouve dans une DMZ qui est séparée d'Internet par un pare-feu pratiquant la translation d'adresses dynamique. Quel problème risque de survenir lors d'une connexion entre un client et le serveur FTP ? Dans le cas où la connexion serait impossible, proposer une solution. Il vous est demandé de considérer le cas du mode actif ainsi que celui du mode actif.
   Rappel : Le protocole FTP utilise deux connexions. La première dite de contrôle est faite généralement sur le port 21. La seconde, quant à elle sert à transférer les données. Elle est soit ouverte par le client après que le serveur lui ait indiqué le numéro de port correspondant (c'est le mode passif) ou par le serveur sur un port indiqué par le client (c'est le mode actif).
7. Nous nous plaçons dans le contexte d'un jeu en ligne dans lequel un joueur peut se connecter de manière "anonyme" à une partie. Un utilisateur veut pouvoir rejoindre des parties en ligne en utilisant sa connexion ADSL dans laquelle la "box" joue le rôle de passerelle NAT.
   (a) Est ce qu'il sera possible pour l'utilisateur de rejoindre une partie ? Expliquer ce qui se passe au niveau du réseau.
   (b) Supposons maintenant qu'un(e) ami(e) de notre utilisateur veuille rejoindre la partie à partir d'une autre machine utilisant la même passerelle ("box"). Sera-t-il possible pour ce deuxième utilisateur de rejoindre la partie dans le cas où le serveur central du jeu identifie les clients uniquement par leur adresse IP ? Expliquer.
   (c) Dans le cas où le scénario de la question précédente ne fonctionnerait pas, proposer deux solutions.
8. Une entreprise souhaite mettre en place un réseau pour connecter les différentes machines utilisées par ses employés et centraliser la gestion des utilisateurs des ressources informatiques de la société.
   Pour ce faire, un parc de machines, 3 serveurs (dont un avec beaucoup d'espace disque) et un switch de capacité suffisante ont été achetés. De plus, la société a pris un abonnement auprès d'un fournisseur d'accès à internet lui permettant d'avoir 1 adresse IP publique. Le réseau de l'entreprise devra être structuré en deux parties :
   — Les machines de la direction qui ont accès à toutes les ressources de l'entreprise
   — Les autres machines qui ont accès à tout sauf aux machines de la direction
   (a) Proposer une architecture ainsi qu'un schéma d'adressage pour le réseau de l'entreprise (nombre de sous-réseaux, masques de sous-réseaux, mécanisme de translation d'adresses si besoin est,...)
   (b) La société veut disposer d'un serveur WEB et veut donner l'accès au réseau de l'entreprise à partir de l'extérieur à l'aide du service ssh. Étendre l'architecture proposée ci-dessus de manière à isoler un serveur (le serveur ne pourra pas accéder aux machines du réseau interne de l'entreprise autrement que par ssh) qui sera accessible de l'extérieur sur les ports correspondants aux services http et ssh. Il vous est particulièrement demander de détailler la mise en place des mécanismes de sécurité. Il ne vous est pas nécessairement demandé de donner des règles `iptables`. Enfin, pour cette question, il est possible d'ajouter un switch à l'architecture si besoin est.

(c) Le directeur de l'entreprise constate que la productivité d'un des meilleurs développeurs laisse soudainement à désirer. Il réalise que son employé joue des heures durant à un jeu en ligne. Le directeur, surpris que la configuration du réseau de l'entreprise laisse fonctionner ce jeu, qui utilise un protocole bloqué par les pare-feu, demande des explications à l'administrateur réseau. Ce dernier lui répond que la configuration du réseau de l'entreprise n'est pas mise en cause (les paquets correspondants au protocole utilisé par le jeu sont effectivement détruits). Comment est-il possible de faire fonctionner un tel jeu derrière un pare-feu ? Donner au moins deux possibilités.

Problème

Soit le script de configuration d'`iptables` donné ci-dessous. Il correspond au réseau représenté par la figure fournie ci-dessous (le script étant exécuté sur la machine à trois interfaces réseau).

```
#!/bin/sh
[1] iptables -F
[2] iptables -t nat -F

[3] iptables -P INPUT DROP
[4] iptables -P OUTPUT DROP
[5] iptables -P FORWARD DROP


[6] iptables -A INPUT  -i eth0 -j ACCEPT
[7] iptables -A INPUT  -i lo -j ACCEPT

[8] iptables -A OUTPUT  -o eth0 -j ACCEPT
[9] iptables -A OUTPUT  -o lo -j ACCEPT

[10] iptables -t nat -A POSTROUTING -s 192.168.0.0/16 -o eth1 -j MASQUERADE

[11] iptables -t nat -A POSTROUTING -s 192.168.0.254 -j SNAT --to-source 147.210.20.1
[12] iptables -t nat -A PREROUTING -d 147.210.20.1 -j DNAT --to-destination 192.168.0.254

[13] iptables -A FORWARD -i eth0  -o eth1 -s 192.168.0.0/16 -j ACCEPT
```



9. Est ce que le paquet d'ouverture de connexion envoyé par la machine dont l'adresse IP est 192.168.0.1 vers la machine dont l'adresse IP est 216.58.215.36 (`www.google.com`) arrivera à destination ? Qu'en est-il de la connexion correspondante ? Corriger si nécessaire.
10. Même question que précédemment lorsque c'est la machine 192.168.1.2 qui souhaite ouvrir une connexion vers 216.58.215.36.
11. Que se passe-t-il lorsque la machine dont l'adresse IP est 192.168.0.2 souhaite ouvrir une connexion sur la machine dont l'adresse IP est 147.210.10.1 sur le port 22 ? On supposera dans ce cas que la politique de routage de la passerelle relaiera le paquet via l'interface eth2. Corriger/compléter dans le cas où la connexion ne pourrait pas être établie.
12. Est ce que l'hôte dont l'adresse IP est 209.85.135.99 peut ouvrir une connexion sur le port 21 (ftp) du serveur dont l'adresse IP privée est 192.168.1.2 (on supposera qu'un serveur ftp est exécuté sur la machine correspondante) ? Que faut-il mettre en place dans le cas où cette ouverture de connexion ainsi que l'échange correspondant seraientt impossibles ? Détailler dans ce cas les règles `iptables` correspondantes en les commentant.
13. On souhaite isoler la machine dont l'adresse privée est 192.168.1.2 dans une DMZ. Détailler les règles `iptables` à ajouter pour la mise en place de la DMZ.

    Remarque : À chaque question il est nécessaire de prendre en compte les modifications effectuées dans les questions précédentes.