	TP Matière : Administration Linux Remis par : A. MAZEROLLES	Année : I4
		Date : 2022/2023 Temps : 4h

OBJECTIFS

Mettre en pratique les notions vues en cours et lors du précédent TP.

Installer, configurer et administrer les clients et serveurs nécessaires à la constitution d'un réseau répondant à un cahier des charges.

REMARQUES

Vous êtes une équipe d'administrateurs réseaux envoyés par une SSII dans une PME pour configurer un réseau local.

Cette PME, spécialisée dans le développement de site web emploie actuellement deux personnes mais compte bien embaucher d'autres collaborateurs dès que le budget le permettra.

I. Mise en place d'un parefeu logiciel

Afin de sécuriser l'accès de cette entreprise à l'Internet, vous commencerez par mettre en place un parefeu permettant d'interconnecter le réseau de l'opérateur (WAN) et votre réseau privé (LAN).

L'opérateur vous a transmis les informations de connexion suivantes :

adresse IP : 192.168.101.(100+n°PC) /22

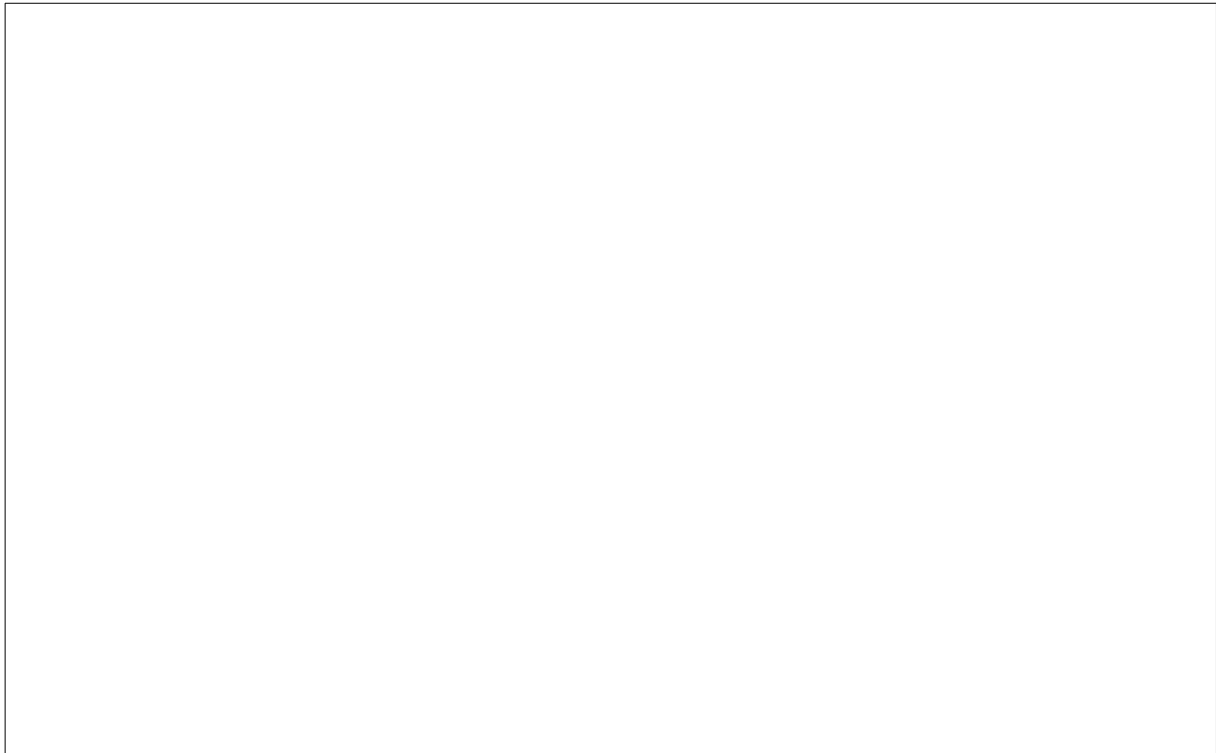
Passerelle par défaut : 192.168.100.254

Serveur DNS : 192.168.100.254

Coté LAN, votre responsable prévoit d'installer un serveur DNS-DHCP, un serveur NFS-LDAP ainsi qu'une connexion SSH avec l'OTP.

Le parefeu devra avoir **la première adresse**, les serveurs **les dernières adresses** du réseau LAN. Les adresses IP affectées aux PCs des deux personnes composant l'entreprise suivront celle du parefeu. La société souhaite également qu'une **plage de 20 adresses** soit prévu pour permettre à différents utilisateurs de pouvoir se connecter.

Dessiner le schéma du réseau avec les adresses, masques et passerelle par défaut configurés sur les interfaces du parefeu :



→ *Appelez l'enseignant pour vérification et validation.*

Mettez en place un parefeu de type pfsense sous virtualBox respectant les contraintes indiqués précédemment.

Aucun service DNS ou DHCP ne devra être activé sur le parefeu.

BONUS : Afin d'optimiser la sécurité du réseau, le parefeu devra être configuré pour que seuls les ports nécessaires à la navigation internet des postes clients et à la mise à jour de l'ensemble des équipements soit ouvert pour les équipements situés sur le Réseau LAN.

II. Mise en place d'un serveur DNS-DHCP

Pour permettre aux équipements de l'équipe de développement de se connecter au réseau, vous mettrez en place un serveur DHCP coté LAN. Le système d'exploitation devra bien sûr être à jour lors de la démonstration au client.

Le serveur DNS devra gérer une zone, appelée ENT-X.loc dédié à l'entreprise permettant de faire la liaison entre le nom de domaine et l'adresse IP des différents serveurs du réseau.

BONUS : mettre en place une zone reverse du DNS pour les serveurs et la passerelle uniquement.

III. Installation d'un client GNU/Linux

Afin de pouvoir tester la configuration, vous installerez un client bureautique (avec ou sans interface graphique – à votre convenance) Ubuntu, connecté sur le réseau LAN et qui permettra de vérifier le bon fonctionnement des différents services installés.

→ *Appelez l'enseignant pour validation.*

IV. Installation d'un serveur LDAP

Afin de gérer l'accès des utilisateurs aux différents équipements du réseau, vous mettrez en place un serveur LDAP fonctionnant sur GNU/Linux Ubuntu Server 20.04 et installé conformément à la documentation officielle.

Une fois l'installation et la configuration terminée, vous vous assurerez de son bon fonctionnement en permettant au client GNU/Linux installé dans la section précédente d'identifier les utilisateurs renseignés dans l'annuaire LDAP.

Vous mettrez en place un service NFS et le couplerez avec le service LDAP afin d'obtenir l'itinérance des utilisateurs, c'est-à-dire la capacité, pour un utilisateur, de pouvoir se connecter depuis différents PCs tout en retrouvant les documents précédemment modifiés. Les droits d'accès devront être configuré de manière à ce qu'un utilisateur ne puisse pas lister le contenu du répertoire personnel des autres utilisateurs.

→ *Appelez l'enseignant pour validation.*

V. Mise en place d'une connexion SSH 4FA

Un tuto est à votre disposition sur le moodle du cours, section Fiches Techniques > [SSH_4FA_secure_connection.html](#)

Un collègue de votre entreprise a, pendant que vous installiez les précédents services susmentionnés, installé de son côté d'autres services sur une Ubuntu 20.04.

Dans le contrat liant votre SSII avec la PME dans laquelle vous intervenez, il est clairement stipulé que ces services doivent pouvoir être géré par vos soins à distance. Une connexion SSH est donc vitale. Votre collègue souhaite que la connexion soit la plus sécurisée possible mais il n'est pas forcément à l'aise avec cela. Connaissant votre appétence pour les systèmes

bien sécurisés, il vous demande de vous en charger. Vous avez avec vous une documentation très succincte pour vous aider.

Vous allez donc mettre en place sur une Ubuntu 20.04 une connexion SSH 4FA en 2 temps :

- ❖ Un couple login - mot de passe et
- ❖ Un mot de passe à usage unique synchronisé sur l'horloge (et non pas basé sur un compteur) qui se rafraîchit toutes les 30 secondes. Sur l'application de votre téléphone, devra apparaître en plus du login utilisateur, le nom de votre entreprise (ici : testSSII).

Dans un deuxième temps, vous rajouterez :

- ❖ Une connexion par certificat
- ❖ Auquel vous associez un passphrase.