Sécurisez le réseau avec un Raspberry pi

Durée	2 périodes
Format	Par groupe de 2
Matériel	PC individuel, Une VM Ubuntu server, une VM Ubuntu desktop, Un raspberry pi, un mini Switch, une carte SD

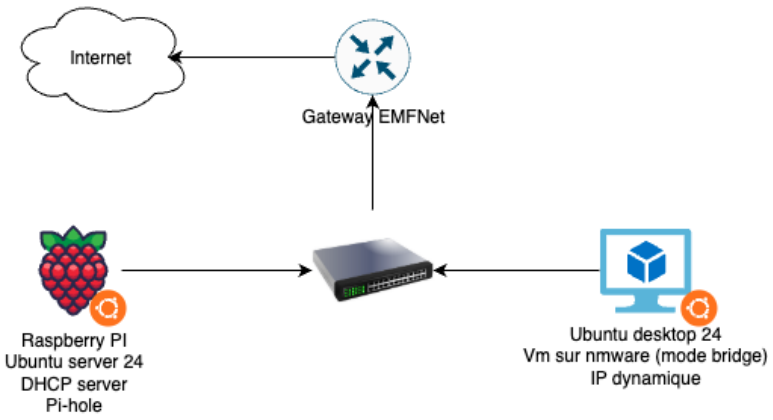
Objectifs pédagogiques

À la fin de cet exercice, l'apprenant sera capable de :

- Installer et configurer un système Linux sur Raspberry Pi
- Configurer une IP statique avec Netplan
- Installer et configurer Pi-hole
- Configurer un poste client pour utiliser Pi-hole comme DNS
- Utiliser SSH pour administrer à distance
- Lire et filtrer des logs sous Linux
- Configurer un pare-feu avec UFW
- Utiliser l'interface graphique de Pi-hole pour gérer les listes de blocage

Scénario

Vous êtes l'administrateur réseau d'un petit lycée. Votre mission est de déployer un Raspberry Pi avec Ubuntu Server pour filtrer la publicité et les domaines indésirables sur tout le réseau grâce à **Pi-hole**.



Travail à réaliser

Préparation du Raspberry Pi

1. Télécharge Raspberry Pi Imager sur internet
2. Avec ce logiciel, flasher l'image « Ubuntu server » sur la carte SD du Raspberry Pi
3. Démarrer le Raspberry Pi avec écran/clavier

Configuration du Raspberry Pi

1. Configure le réseau du Raspberry Pi, il faut lui mettre une ip statique
2. Effectue les mises à jour système sur le Raspberry Pi
3. Installe un serveur DHCP sur le Raspberry Pi et configure-le, comme ça les clients pourront l'utiliser (il n'y a pas de DHCP dans ton VLAN EMFNet). L'adresse DNS que les clients recevront doit être celle du Raspberry Pi.
4. Installe l'application pi-hole et assure-toi que le service tourne au redémarrage
5. Dans l'assistant, retiens bien les informations d'accès (notamment l'url de l'interface web admin et le password)

Configuration du client Ubuntu, accès SSH et observation des logs

1. Sur ta machine ubuntu desktop, utilise le serveur dhcp précédemment installé
2. Vérifie que l'ip du DNS reçue est bien celle du Raspberry Pi
3. Sur la vm Ubuntu, lance un navigateur et accède à la console admin
    1. Sur la console admin, ajoute une liste de noms de domaine à bloquer, par exemple : https://raw.githubusercontent.com/StevenBlack/hosts/master/hosts
    2. Observe le dashboard et son évolution lorsque tu navigues sur internet
4. Connecte-toi en SSH sur le Raspberry Pi
    1. Désormais plus besoin d'écran et de clavier sur le Raspberry Pi, il est possible d'y accéder à distance !
    2. Vérifie que le service pi-hole est fonctionnel en commande
    3. Observe les logs au niveau des fichiers de pi-hole
    4. Trouve une ligne qui contient « blocked » dans le fichier de log (en utilisant le pipe |)
    5. *S'il y a un problème et qu'aucun site n'a été bloqué, essaye la commande « pihole -g » et dans la console web admin, tu devrais voir ta liste apparaitre*

Observation des journaux et configuration de pare-feu

1. Sur le Raspberry Pi ainsi que sur la vm Ubuntu desktop, configure le pare-feu pour qu'il soit activé, qu'il laisse passer le protocole ssh ainsi que le traffic sur le port 80, 443 et 53. Il faut également que le pare-feu soit activé au redémarrage.
2. Observe les logs système et les logs de connexion SSH du raspberry Pi

Exercice avancé : Grafana et visualisation des données

L'administration du lycée souhaite avoir une vision en temps réel de l'efficacité du filtrage DNS. Vous devez utiliser prometheus (pour exporter les données de pi-hole) et grafana (pour les afficher en graphique).

Vous trouverez l'exporter avec des dashboard grafana ici :
https://github.com/eko/pihole-exporter

Exercice avancé 2 : fail2ban

Des tentatives d'intrusion ont été détectées sur le Raspberry Pi du lycée.
Vous devez mettre en place un mécanisme de défense **automatique** qui bloque les IP effectuant trop de tentatives de connexion.

Travail à réaliser :

- Installer Fail2Ban
- Configurer fail2ban pour le service ssh
- Tester en simulant des mauvais password plusieurs fois au login depuis votre vm ubuntu desktop.
- Observez les logs et documentez l'exercice.