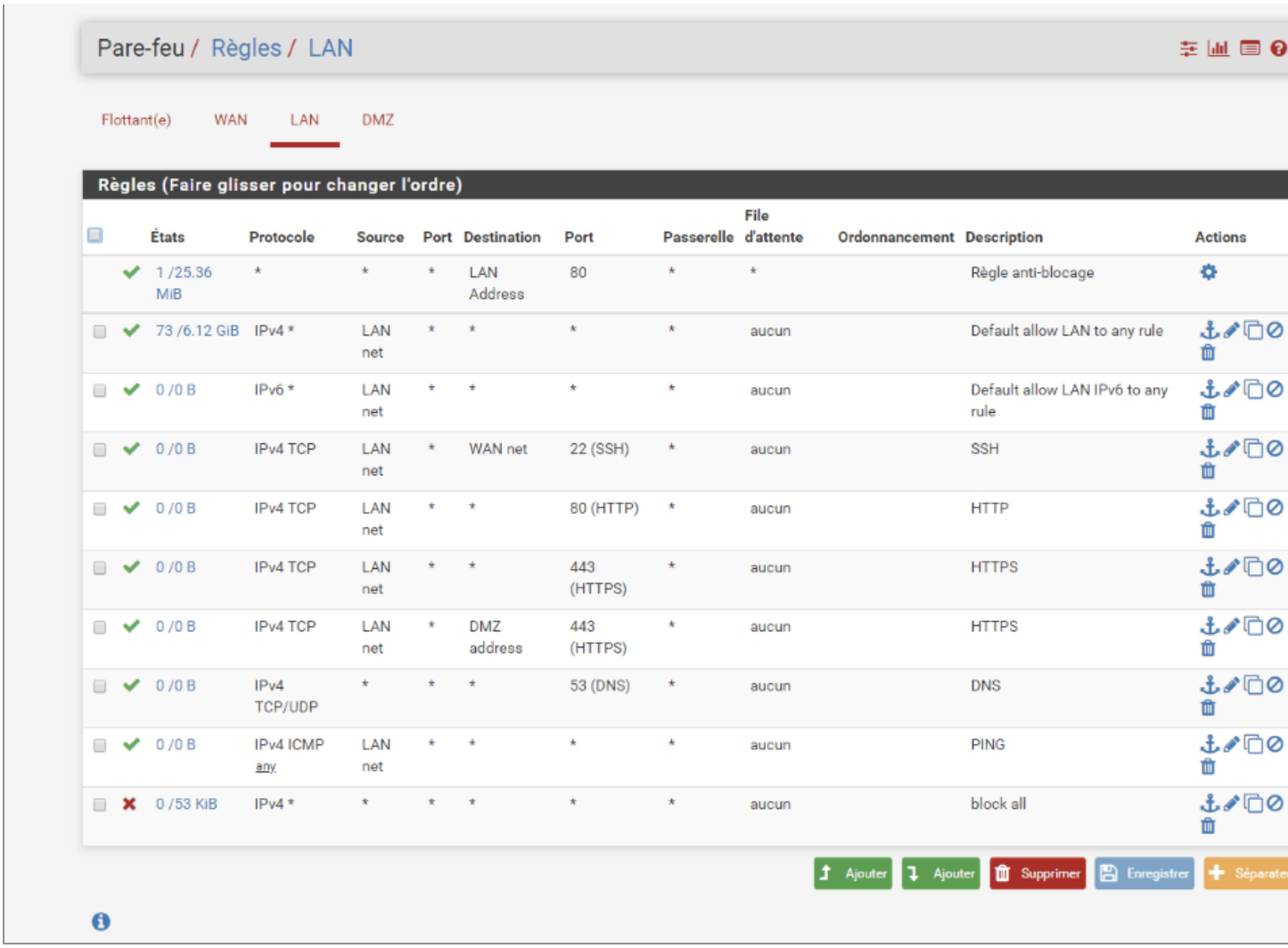
25 Questions CCP3 BIs

1. **Dans la capture d'écran ci-dessous :**



1. **Quel est le rôle de la 1ère règle (en partant du haut) ?**

C'est la règle d'anti-blocage, elle permet de ne pas se couper l'accès à l'interface graphique de pfsense (par exemple).

2. **Quel est le rôle de la 3ème règle (en partant du haut) ?**

Elle autorise tous les paquets provenant du réseau LAN en Ipv6 à transiter sur n'importe quel protocole, vers n'importe quelle destination.

3. **Quel est le rôle de la 4ème règle (en partant du haut) ?**

Elle autorise tous les paquets en provenance du réseau LAN, transitant par le protocole TCP sur le port 22 (SSH) à sortir sur le réseau WAN.

4. **Quel est le rôle de la 7ème règle (en partant du haut) ?**

Elle autorise tous les paquets en provenance du réseau LAN, transitant par le protocole TCP sur le ports 443 (HTTPS) à atteindre la passerelle de la DMZ

5. **Quel est le rôle de la dernière règle (en partant du haut) ?**

Elle bloque le transport de tous les paquets qui n'auraient pas été autorisés à passer dans une autre règle car elles sont lues du haut vers le bas.

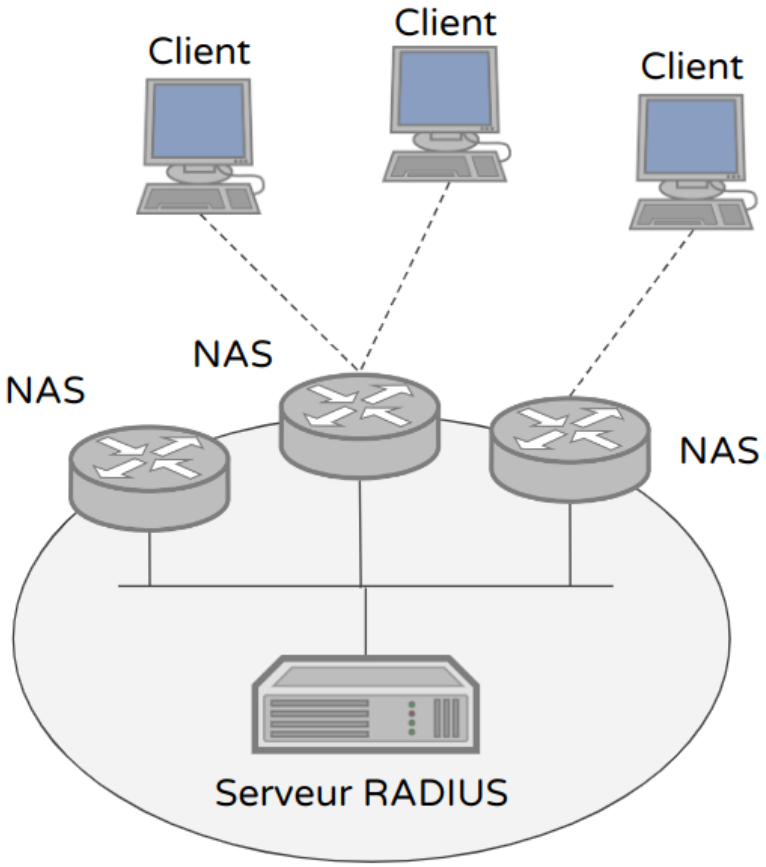
6. **Quelles règles sont redondantes (pour l'ensemble des règles de la capture) ?**

Les règles 4, 5, 6, 7, et 9 (en partant d'en haut) sont redondantes.

2. Qu'est-ce qu'une ACL ?

C'est une liste de règles (Access Control List ou listes de contrôle d'accès) qui servent à autoriser ou non l'accès à un réseau.
On les trouve dans les routeurs ou les switch.

3 . En prenant comme exemple ce schéma, explique le principe du RADIUS :



Radius sert à faire du contrôle d'accès à un réseau en faisant de la centralisation et de l'authentification générique. Il utilise des NAS (Network Access Server) qui vont autoriser des clients à accéder à un réseau (wifi ou ethernet).

4. Explique la différence entre la bande de fréquence 2.4 GHz et 5 GHz en wifi.

Les deux sont des normes de bandes de fréquence.
Concernant la portée maximale, elle sera théoriquement de 100 m pour le wifi 2.4 GHz, et bien moindre pour le wifi 5 GHz.
Concernant le débit, il sera plus important pour le wifi 5 GHz qu'en 2.4 GHz.

5. Quelles méthodes peut-on utiliser pour envoyer un message à un destinataire de manière sécurisée, sans qu'un tiers (non autorisé), puisse lire le message ? Imaginons que Bob veuille envoyer un message à Alice, mais que Stéphane ne doit pas lire le message, explique les différentes procédures.

On peut utiliser de la cryptographie symétrique et asymétrique.
Cryptographie symétrique :

- Bob et Alice doivent convenir d'une clé secrète commune à l'avance. Stéphane n'a pas cette clé.
- Bob utilise cette clé pour chiffrer le message confidentiel.
- Bob envoie le message chiffré à Alice.
- Alice utilise également la même clé pour déchiffrer le message confidentiel.

Bob et Alice sont les seuls à avoir la clé secrète, donc ils sont les seuls à pouvoir déchiffrer le message confidentiel.
Stéphane ne peut pas lire le message, car il ne possède pas la clé secrète commune.
Cryptographie asymétrique :

- Alice crée une paire de clés - une clé publique et une clé privée.
- Alice envoie la clé publique à Bob et à Stéphane.
- Bob utilise la clé publique d'Alice pour chiffrer le message confidentiel.
- Bob envoie le message chiffré à Alice (et potentiellement à Stéphane).
- Alice utilise sa clé privée pour déchiffrer le message confidentiel.

Alice est la seule à pouvoir déchiffrer le message confidentiel envoyé par Bob car elle est la seule à posséder la clé privée correspondante à la clé publique utilisée pour le chiffrement.
Stéphane ne peut pas lire le message, car il ne possède pas la clé privée d'Alice.

6. Explique ce que font les ACL suivantes :

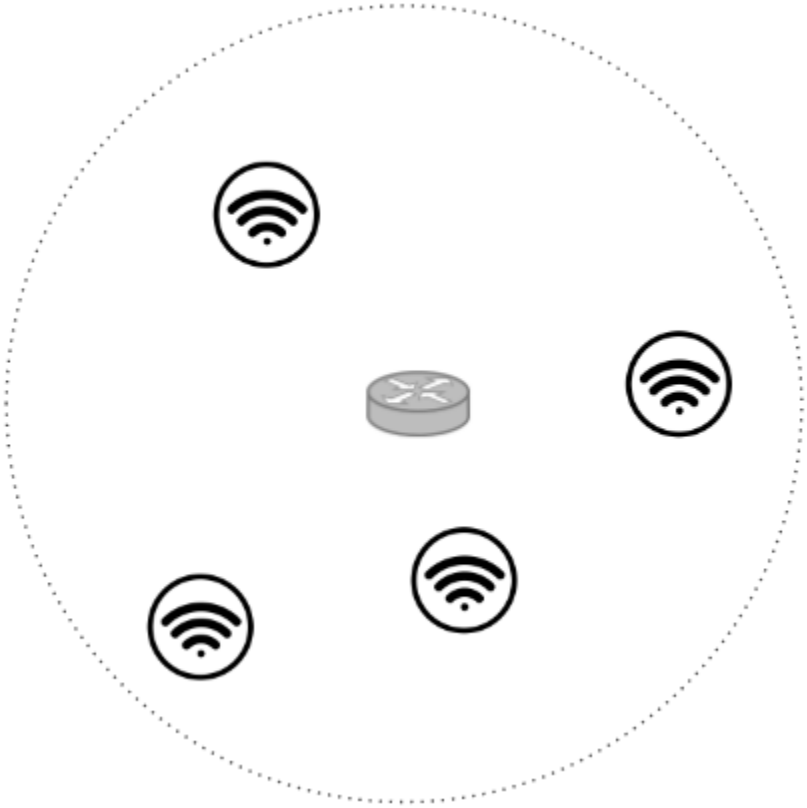
1. **access-list 100 deny icmp 10.1.3.0 0.0.0.255 10.1.2.0 0.0.0.255**

Elle interdit le protocole icmp (donc le ping) du réseau 10.1.3.0/24 vers le réseau 10.1.2.0/24

2. **access-list 100 permit icmp 10.1.1.0 0.0.0.255 10.1.2.0 0.0.0.255**

Elle autorise le protocole icmp (donc le ping) du réseau 10.1.1.0/24 vers le réseau 10.1.2.0/24

7. Dans le schéma ci-dessous :



1. **Indique ce qu'est chaque élément et le type de wifi que l'on peut mettre en place.**

Ce schéma représente un réseau wifi avec différentes entités. On a 4 stations et 1 point d'accès (Access Point).
On peut mettre en place un réseau wifi de type infrastructure (BSS).

2. **Que manque-t-il pour faire de l'ESS ?**

Pour faire de l'ESS, ou infrastructure étendue, il manque un système de distribution (DS).

8. Quelle est la différence entre un VPN type site à site et un VPN point à point ?

Un VPN site à site fait de l'interconnexion de réseaux (les extrémités sont des passerelles de routeurs), alors qu'un VPN point à point permet de communiquer entre 2 machines (qui peuvent être dans des réseaux différents).

9. Donne 2 protocoles de sécurité wifi non-obsolètes.

WPA2-Personnal (ou WPA2-PSK) et WPA2-Entreprise (ou WPA2-EAP).

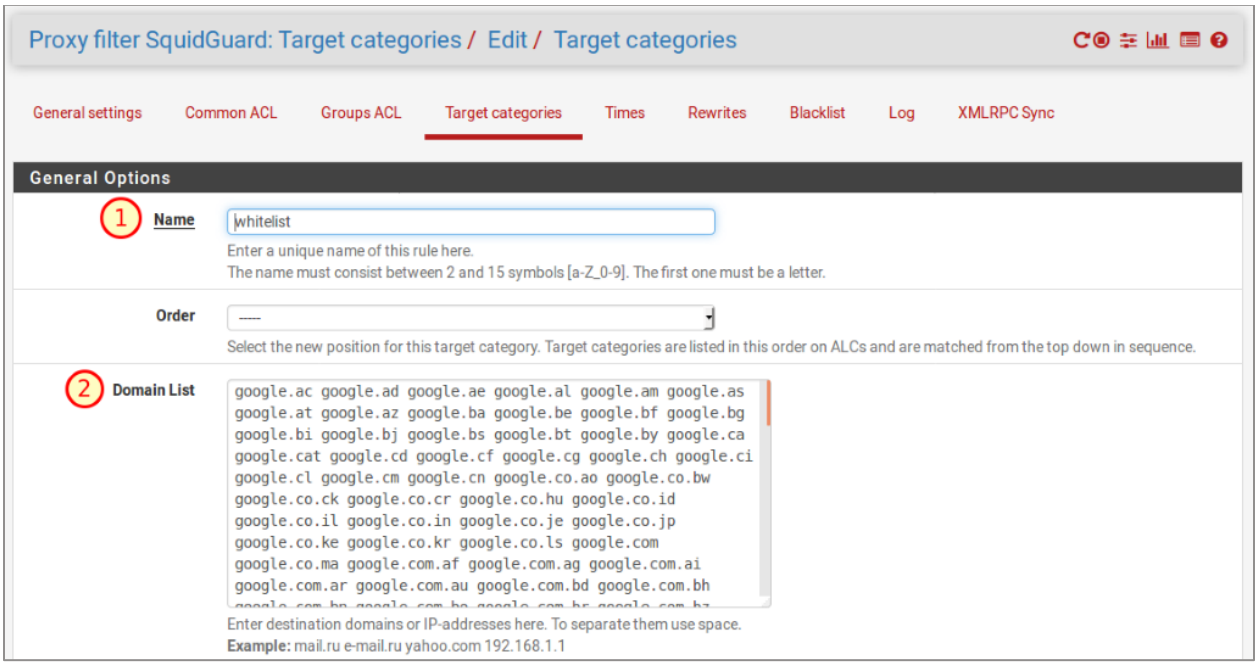
10. A quoi sert SSH ?

SSH sert à faire de l'accès distant sécurisé.

11. Cite un outil ou un logiciel avec lequel tu peux faire du ssh.

Putty sur Windows.

12. Dans la capture d'écran ci-dessous :



1. **Quel logiciel est mis en œuvre ?**

Squid.

2. **Quel est sa fonction ?**

C'est un serveur proxy. Il joue le rôle d'intermédiaire et de cache entre un client et un serveur web. C'est lui qui émet les requêtes web à la place du client.
.

3. **Dans la fenêtre centrale tu peux voir "google.ac google.ad …". A quoi cela sert ?**

C'est une liste blanche, qui autorise les noms de domaines pouvant être consultés par les utilisateurs.

13. Je dois faire communiquer en wifi 2 stations entre elles directement, sans point d'accès. Est-ce qu'utiliser un réseau ad hoc est une bonne idée ?

On peut du had hoc car c'est le principe de ce ce modèle de réseau wifi, mais ce n'est pas une bonne idée.

14. Explique les lignes suivantes :

On demande l'accès à la machine "server".

Le système précise qu'il ne peut pas authentifier la machine "server".

Il demande si on souhaite quand même se connecter.
Après avoir répondu "yes", il est demandé le mot de passe du compte "wilder" sur la machine "server".

15. Est-ce qu'un hash est de la cryptographie symétrique ?

Un hash (ou fonction de hachage) est une fonction mathématique qui sert à calculer une empreinte numérique unique à partir d'un message.
La cryptographie symétrique utilise une seule clé pour chiffrer et déchiffrer les données
ne nécessitent pas de clé
Donc non, un hash n'est pas de la cryptographie symétrique, mais une forme de cryptographie.

16. Qu'est-ce que le MIMO ?

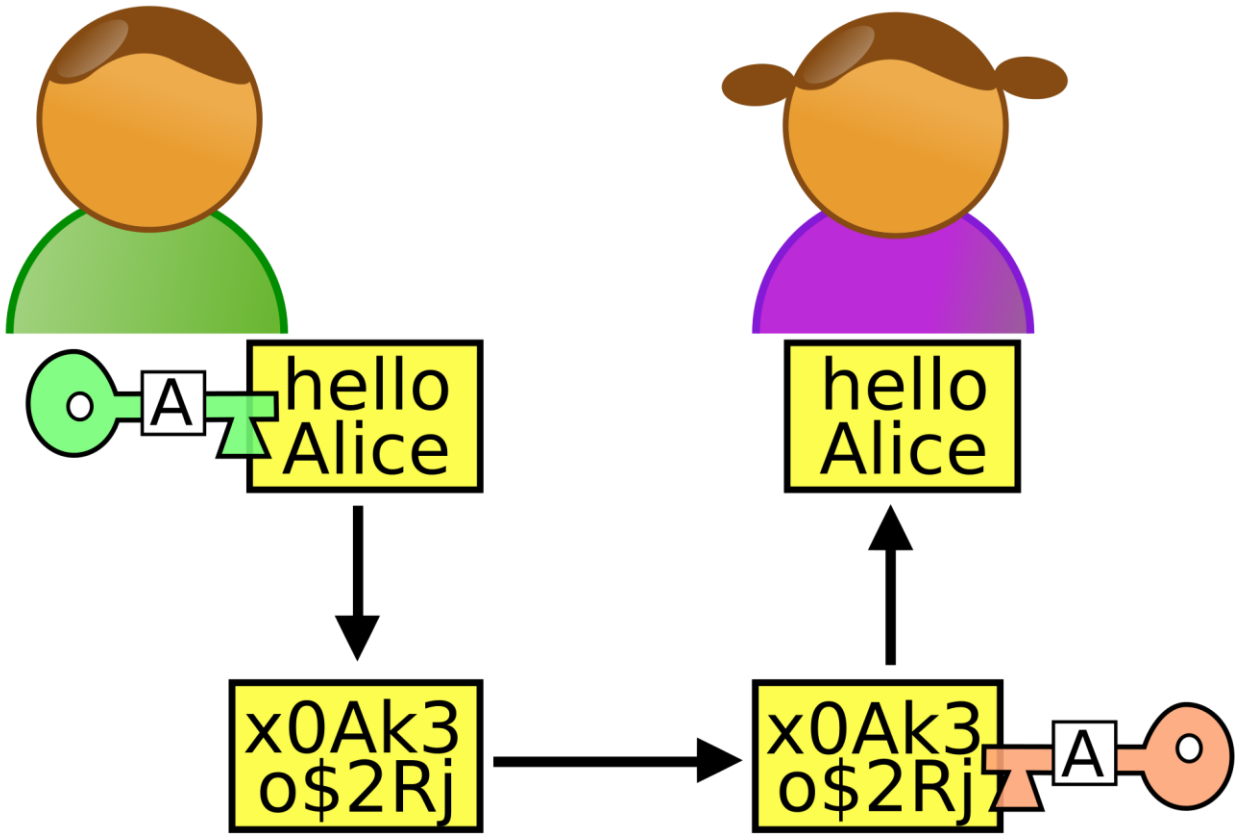
Le MIMO (Multiple-Input Multiple-Output), dans le domaine de la transmission sans fil, en particulier en wifi, est une technique qui permet d'utiliser plusieurs antennes en même temps.
Cela permet d'augmenter le flux des données et la qualité.

17 . Pour un RADIUS, qu'est-ce qu'un NAS ? A quoi sert ce NAS ?

Un NAS (Network Access Server) est un point d'entrée sur un réseau.
Son rôle est d'autoriser (ou pas) l'accès à des clients sur un réseau.

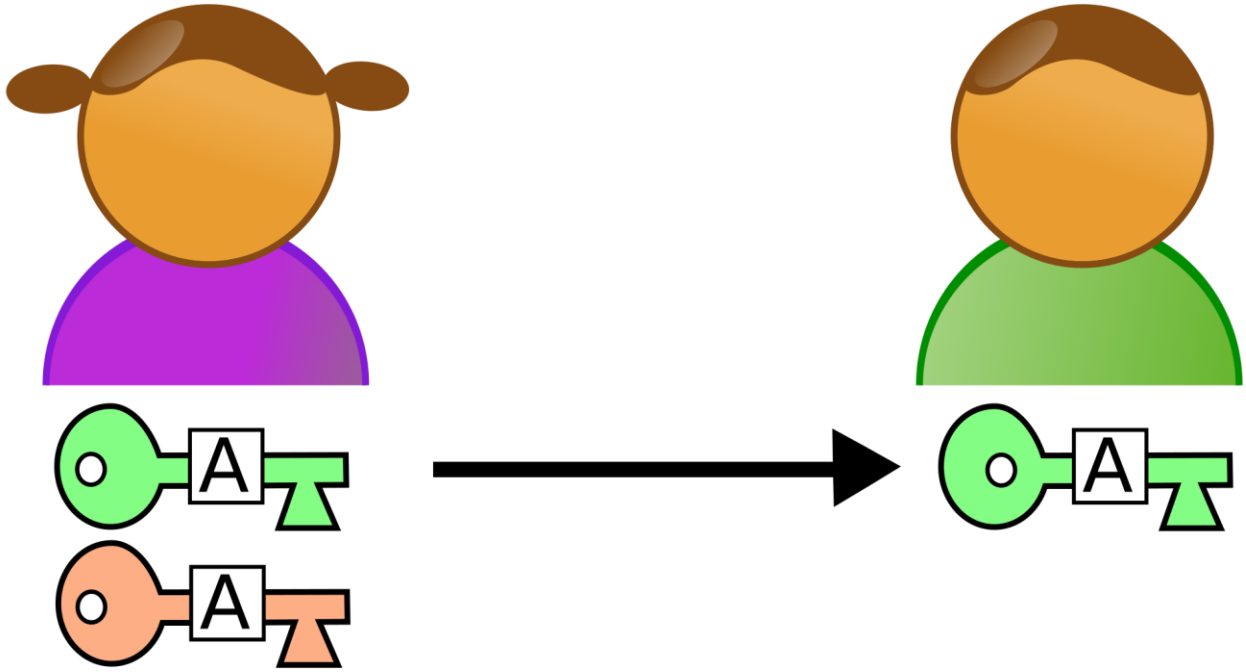
18. Est-ce que le schéma suivant, avec les étapes 1 et 2 est correct ?

Etape 1 :



Bob chiffre le message avec la clé publique d'Alice et envoie le texte chiffré. Alice déchiffre le message grâce à sa clé privée.

Etape 2 :



Alice génère deux clés: Sa clé publique (verte) qu'elle envoie à Bob et sa clé privée (rouge) qu'elle conserve précieusement sans la divulguer à quiconque.
Les 2 étapes sont inversées, d'abord c'est l'étape 2, puis la 1.

19. Quel est le principe de l'attaque Man in the middle ?

L'attaque Man in the middle est une attaque informatique où un attaquant intercepte la communication entre deux entités, par exemple un utilisateur et un site web.

20. Qu'est-ce que l'EAP et dans quel contexte est-il utilisé ?

L'EAP (Extensible Authentication Protocol) ou protocole d'authentification extensible sert à faire de l'authentification.
Il y a par exemple l'EAP-PSK, l'EAP-TLS, l'EAP-SIM, …
Il est utilisé avec RADIUS et en Wifi.

21. Décrit chaque ligne des commandes shell ci-dessous :

Connection en SSH au serveur "Server" avec le compte "wilder" à partir d'une machine "Ubuntu".

Sur le serveur : mise-à-jour des dépôts et du système

Sur le serveur : installation du logiciel openvpn à partir des dépots

Sur le serveur : edition du fichier de configuration

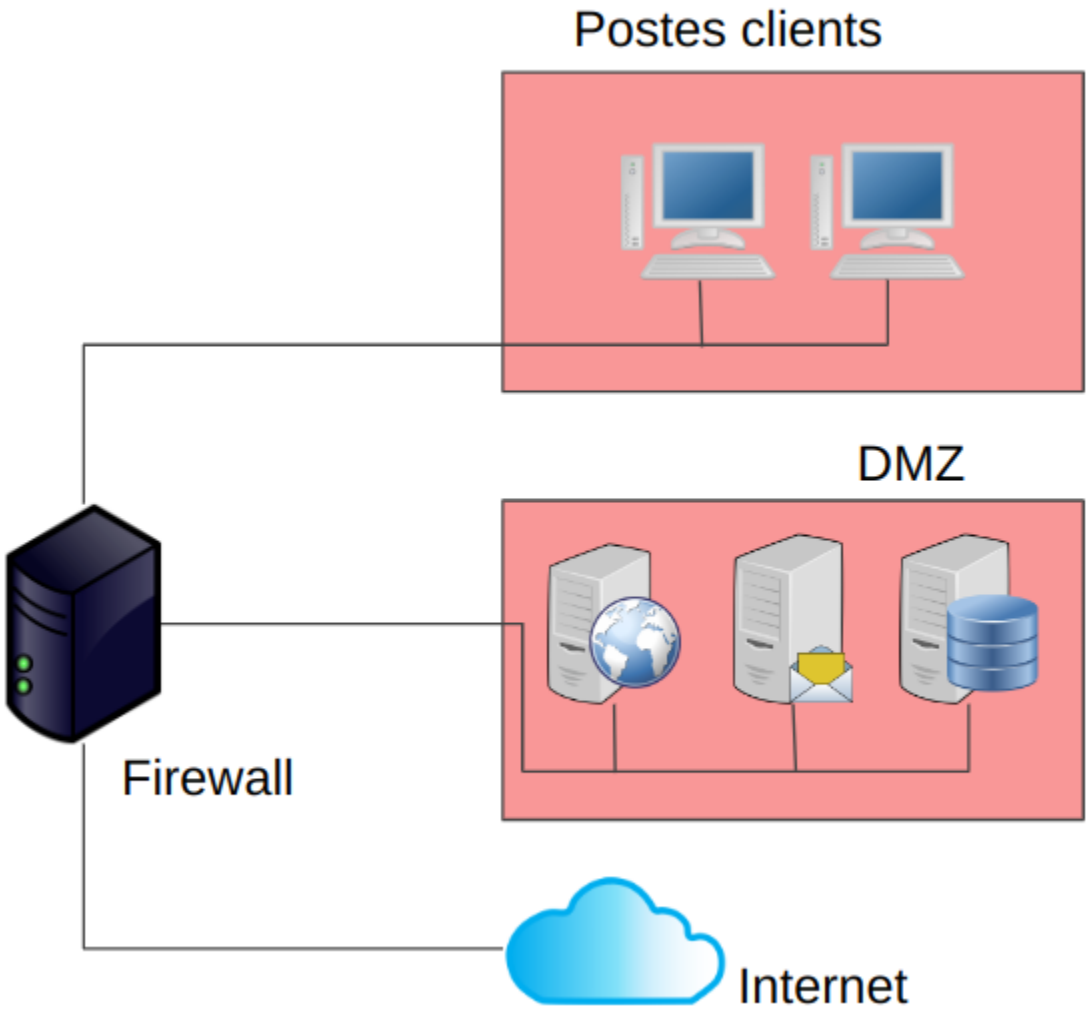
Sur le serveur : démarrage du service openVPN

Sur le serveur : vérification de l'état du service openVPN

Sur le serveur : déconnexion de la session SSH

Retour sur la machine Ubuntu.

22. Sur le schéma ci-dessous :



1. **L'administrateur systèmes et réseaux de ce réseau a choisi de placer un NIDS entre le pare-feu et l'accès internet. Quels sont les avantages et les inconvénients de ce choix ?**

Placer un NIDS (système de détection d'intrusion réseau) entre le pare-feu et l'accès internet permet d'analyser le trafic entrant (internet) et sortant de l'ensemble du réseau interne.
Avantage de cet emplacement :

- Détection des tentatives d'intrusion avant qu'elles ne puissent causer des dommages au réseau interne.
- Sécurité globale du réseau.

Inconvénients :

- Charge supplémentaire sur le réseau en entrée due à la surveillance du trafic, donc qui peut amener des ralentissement pour l'ensemble du réseau
- Possibilité de détection de trafic légitime comme malveillant (faux positifs)

- Avoir des compétences d'analyse importantes.

2. **Il souhaite également placer un NIPS au même endroit. Est-ce une bonne idée ?**

En mettant un NIPS au même emplacement, cela permet de prendre des mesures immédiates pour bloquer les attaques détectées par le NIDS. Donc c'est une bonne idée.
Néanmoins, il serait plus judicieux de le mettre juste derrière le pare-feu car de cette manière beaucoup de flux malveillant seront arrêtés par le pare-feu.

3. **Ce NIPS sera en mode fail close. Que se passera-t-il s'il y a un problème sur ce NIPS ?**

S'il y a un problème, le mode fail close va entraîner une interruption de service.
Dans ce cas, le trafic sera bloqué et les utilisateurs ne pourront pas accéder aux ressources du réseau.

23. Pour le shell ci-dessous :

1. **Explique la phrase en rouge**

La commande ssh-keygen -t ecdsa -b 256 génère une paire de clés SSH de type ECDSA (Elliptic Curve Digital Signature Algorithm) avec une taille de clé de 256 bits.

2. **Explique ce qu'est la partie bleue**

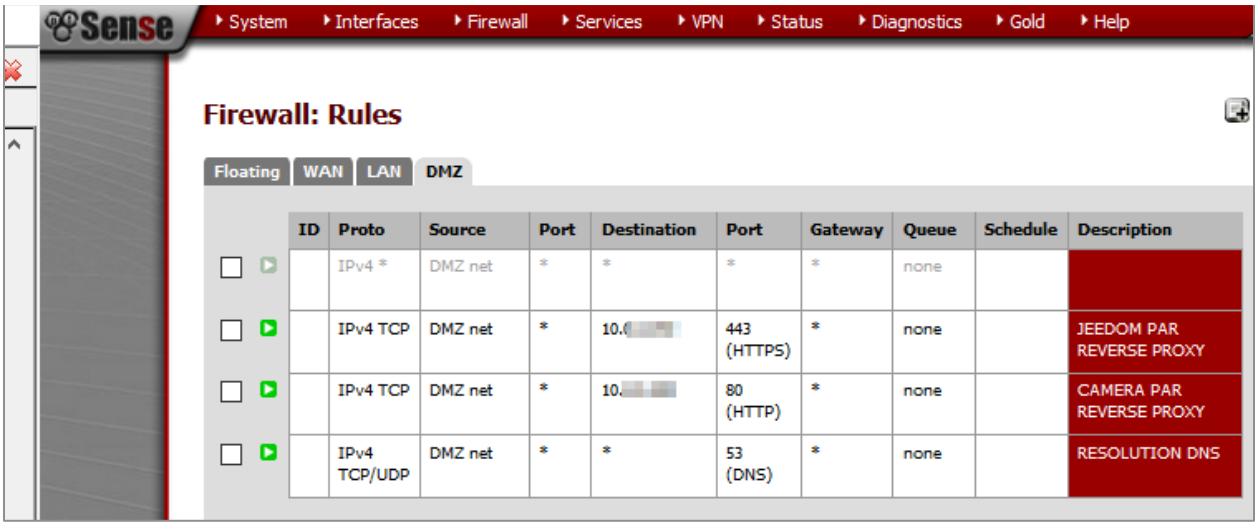
La première ligne indique le type de clé (ECDSA 256), ensuite on a un dessin qui représente la clé publique générée sous forme graphique. La clé publique est représentée par une série de points, de croix et de lettres qui ont été générés à partir de la paire de clés.
La dernière ligne indique l'algorithme de hachage utilisé pour la signature, le SHA-256.

3. **Quels sont les fichiers créés et à quoi servent-ils ?**

Il y a 2 fichiers : id_ecdsa et id_ecdsa.pub.
Ce sont des clés d'authentification pour SSH :

- id_ecdsa est la clé privée (pour s'authentifier auprès d'un serveur SSH distant)
- id_ecdsa.pub est la clé publique correspondante (partagée avec les serveurs pour permettre l'authentification de l'utilisateur)

24. Dans la capture suivante :



1. **Explique la règle 1 (en partant du haut)**

Elle autorise, en Ipv4, les paquets à transiter grâce à n'importe quel protocole, en provenance de la DMZ, vers n'importe quelle destination et via n'importe quel port.
Elle est grisée donc désactivée.

2. **Explique la règle 2 (en partant du haut)**

Elle autorise, en Ipv4, tous les paquets à transiter grâce au protocole TCP, en provenance de la DMZ via n'importe quel port mais seulement à destination du réseau 10.[...] via le port HTTPS.

3. **Explique la règle 3 (en partant du haut)**

Elle autorise, en Ipv4, tous les paquets à transiter grâce au protocole TCP, en provenance de la DMZ via n'importe quel port mais seulement à destination du réseau 10.[...] via le port HTTP.

4. **Explique la règle 4 (en partant du haut)**

Autorise, en Ipv4, tous les paquets à transiter grâce aux protocoles TCP et UDP, en provenance de la DMZ vers n'importe quelle destination et via n'importe quel port via le port DNS.

5. **A quel réseau, ou zone du réseau, ces règles s'appliquent-elles ?**

A la DMZ.

6. **Quelles règles sont redondantes en production ?**

Aucune. La règle 1 est grisée, donc non active. Si elle était active, aucune autre règle ne serait utile car les règles sont lues du haut vers le bas.

25. Qu'est-ce que x.509 ? A quoi cela sert ?

X.509 est une norme ITU-T pour le format des certificats numériques. Ils sont composés d'informations sur l'entité à qui le certificat est délivré (nom, adresse, …) et la clé publique associée.
Cela sert à authentifier des serveurs (en général web), des applications, ainsi que des utilisateurs.