# 14 Questions à retenir CCP7

## Quel est l'impact des ACL ci-dessous sur la machine 172.16.0.10 ? Peut-on fusionner ces ACL pour n'en former qu'une seule ? Si oui fais-le.

```bash
access-list 100 deny icmp host 172.16.0.10 172.17.0.0 0.255.255.255
access-list 100 permit ip any any
access-list 101 deny tcp host 172.16.0.10 host 220.0.0.60 eq www
access-list 101 deny tcp host 172.16.0.10 host 220.0.0.60 eq 443
access-list 101 permit ip any any
```

**Pour l'ACL 100 :**

- access-list 100 deny icmp host 172.16.0.10 172.17.0.0 0.255.255.255

=> bloque le trafic ICMP (donc le ping) de la machine 172.16.0.10 vers le réseau 172.17.0.0/24

- access-list 100 permit ip any any

=> Autorise tout le trafic de n'importe quelle source vers n'importe quelle destination

**Pour l'ACL 101 :**

- access-list 101 deny tcp host 172.16.0.10 host 220.0.0.60 eq www

=> bloque tout le trafic TCP de la machine 172.16.0.10 vers la machine 220.0.0.60 sur le port 80 (donc HTTP)

- access-list 101 deny tcp host 172.16.0.10 host 220.0.0.60 eq 443

=> bloque tout le trafic TCP de la machine 172.16.0.10 vers la machine 220.0.0.60 sur le port 443 (donc HTTPS)

- access-list 101 permit ip any any

=> Autorise tout le trafic de n'importe quelle source vers n'importe quelle destination

**Les ACL sont appliquées sur des interfaces, et donc peuvent avoir un objectifs bien precis. On peut théoriquement fusionner ces 2 ACL :**

- access-list 110 deny icmp host 172.16.0.10 172.17.0.0 0.255.255.255
- access-list 110 deny tcp host 172.16.0.10 host 220.0.0.60 eq www
- access-list 110 deny tcp host 172.16.0.10 host 220.0.0.60 eq 443
- access-list 110 permit ip any any

**Pour les commandes ci-dessous les 2 chaînes de caractères en entrée sont de tailles différentes et pourtant la longueur du résultat des commandes est identique. Pourquoi ?**

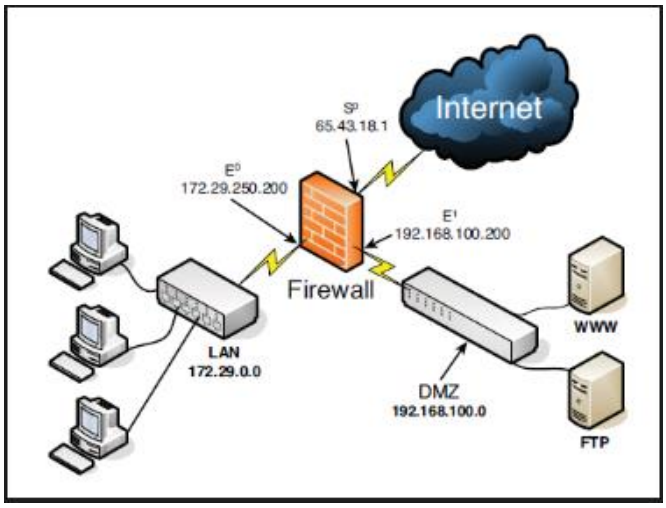
```shell-bash
wilder@Ubuntu:~$ echo -n "test message" | sha512sum
950b2a7effa78f51a63515ec45e03ecebe50ef2f1c41e69629b50778f11bc080002e4db8112b59d09389d10f3558f85bfdeb4f1cc55a34217af0f8547700ebf3 -

wilder@Ubuntu:~$ echo -n "ce message n'a aucun rapport avec le précedent !" | sha512sum
0096a6b7b1ff9714c8a0ecd308e1c952ec2f956f0f5ae28ec29b3e6b68f16a127ea4c379c4aafce2e4f97c029874628f4d3376440ae87c34f83b225c973f1d0a -
```

La commande passé derrière le « pipe » est « sha512sum » qui est une fonction de hachage cryptographiques.

Ce type de fonction de chiffrement produit toujours une sortie de taille fixe, quelle que soit la taille de l'entrée. C'est une caractéristique essentielle qui garantit que la sortie (le hachage) a une longueur constante.

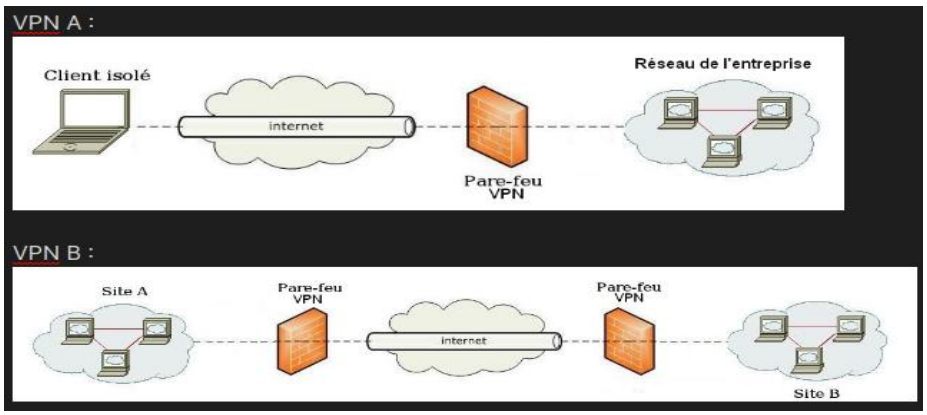
**Sur l'infrastructure réseau représentée par le schéma ci-dessous, que faut-il faire pour que l'on puisse accéder de manière sécurisée au serveur web depuis internet ?**




**Il faut :**

- Créer sur le firewall une redirection du port 443 (HTTPS) vers l'adresse IP du serveur web qui est dans la DMZ.
- Créer une règle pour autoriser le trafic du WAN (Internet) vers l'adresse IP du serveur web qui est dans la DMZ sur le port 443.

## Quels types de VPN sont représentés dans les illustrations suivantes ?




- VPN A :
- VPN type accès distant (host to network)
- VPN B :
- VPN type site à site

## Par rapport au schéma ci-dessous, complète le texte en dessous avec les bons termes.


Pour envoyer un message privé à Bob, Alice utilise **la clé publique** de Bob pour rendre « illisible » le « texte en clair » et Bob utilise **sa clé privée** pour transformer le texte « illisible » en « texte en clair ». Ce processus représente un chiffrement **asymétrique**.

## En matière de sécurité informatique, indique 3 types de menaces (risques et attaques) auxquelles peut être confronté un SI (ne rentre pas dans les détails).

- **Malwares** (virus, ransomwares, chevaux de Troie)
- **Attaques par phishing** (hameçonnage pour voler des identifiants)
- **Intrusions réseau** (accès non autorisé, exploitation de vulnérabilités)
- **Exploitation de vulnérabilités** — Attaques ciblant des failles dans les logiciels ou systèmes.
- **Fuites de données** — Divulgation non autorisée d'informations sensibles.
- **Déni de service (DoS / DDoS)** — Saturation des ressources pour rendre un service indisponible.

## Pourquoi est-ce important de mettre-à-jour le firmware d'un équipement réseau ?

Mettre à jour le firmware d'un équipement réseau est crucial pour plusieurs raisons:

- Corriger des vulnérabilités de sécurité découvertes.

- Améliorer les performances ou la stabilité de l'appareil.
- Ajouter ou mettre à jour des fonctionnalités.

**Explique ce que fais ceci :**

**ssh adminDebian@DebianServer**

**ssh-keygen**

**Enter file in which to save the key (/home/adminDebian/.ssh/id_rsa):**

**Enter passphrase (empty for no passphrase):**

**cat ~/.ssh/id_rsa.pub**

**exit**

**ssh wilder@UbuntuClient**

**mkdir ~/.ssh**

**nano ~/.ssh/authorized_keys**

Ces lignes configurent l'authentification par clé SSH entre deux machines (un serveur DebianServer et un client UbuntuClient).

**Pour le routeur R1 ayant 2 interfaces g0/0 sur le WAN (45.56.12.07/16) et g1/0 sur le LAN (172.16.15.254/24) que représente les ACL suivantes :**

- **access-list 101 permit udp any host 172.16.15.10 eq 67**
- **access-list 101 permit udp any host 172.16.15.10 eq 68**
- **access-list 101 permit tcp any host 172.16.15.10 eq 53**
- **access-list 101 permit udp any host 172.16.15.10 eq 53**

**Que peux-tu déduire de l'hôte 172.16.15.10 ?**

- access-list 101 permit udp any host 172.16.15.10 eq 67

=> autorise le trafic UDP de n'importe quelle source vers l'hôte 172.16.15.10 sur le port 67 (DHCP)

- access-list 101 permit udp any host 172.16.15.10 eq 68

=> autorise le trafic UDP de n'importe quelle source vers l'hôte 172.16.15.10 sur le port 68 (DHCP)

- access-list 101 permit tcp any host 172.16.15.10 eq 53

=> autorise le trafic TCP de n'importe quelle source vers l'hôte 172.16.15.10 sur le port 53 (DNS)

- access-list 101 permit udp any host 172.16.15.10 eq 53

=> autorise le trafic UDP de n'importe quelle source vers l'hôte 172.16.15.10 sur le port 53 (DNS)

La machine 172.16.15.10 est un serveur DHCP et DNS.

## En wifi, qu'est-ce qu'une zone blanche ? Comment les détecter et les solutionner ?

En wifi, une zone blanche est un emplacement où il n'y a pas ou peu de couverture réseau.

Pour les détecter on peut analyser la couverture wifi et voir où le signal est très faible, avec des logiciels comme NetSpot ou WiFi Analyzer. Une fois que c'est fait, on peut cartographier le signal sur un plan.

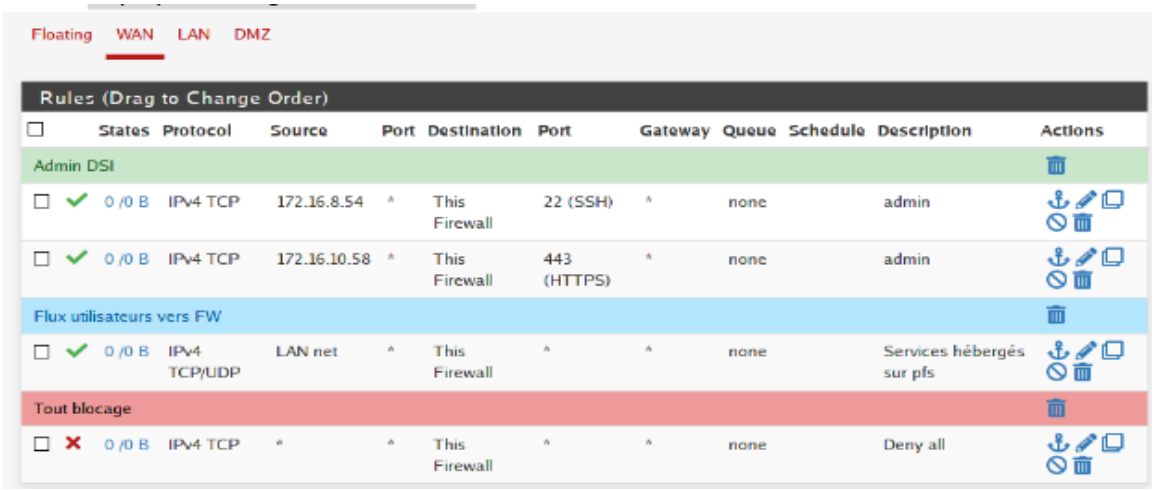
Une solution possible peut être d'utiliser des répéteurs wifi qui vont propager le signal.

## WPA est-il un protocole sécurisé ?

Sur le principe, oui WPA est un protocole sécurisé. Il l'est bien plus que le WEP (obsolète), mais moins que le WPA2 et WPA3.

Donc de nos jours, on peut considérer que WPA n'est pas un protocole sécurisé.

## Explique les règles ci-dessous :




**Règle 1 (en haut) :**

Autorise la machine 172.16.8.54 à se connecter en SSH sur le firewall. On peut supposer que c'est pour l'administration du firewall.

**Règle 2 :**

Autorise la machine 172.16.10.58 à se connecter en HTTPS sur le firewall. On peut supposer que c'est pour l'administration du firewall en mode graphique.

**Règle 3 :**

Autorise les machines du réseau LAN à accéder sur le firewall. Cela peut être pour certains services.

**Règles 4 (en bas) :**

Bloque toutes les connexions TCP vers le firewall.

## Quel est le type de wifi à mettre en place dans des bureaux ayant une surface d'environ 400 m2 ?

Dans un contexte de bureaux situés sur un seul niveau, avec des murs perméables au signal wifi, une ou deux bornes wifi devraient suffire. Dans ce cas, un wifi en mode infrastructure étendue (ESS = Extended Service Set) serait pertinent. Il sera toujours possible d'ajouter des bornes wifi supplémentaires et de les rattacher à cette infrastructure.

## Bob a une clé publique PUB-Bob et une clé privée PRI-Bob. Alice a la même chose avec PUB-Alice et PRI-Alice. Dans le mode de la cryptographie asymétrique, décrit les différentes étapes d'un envoi de message de Bob vers Alice.

- Bob utilise la clé publique d'Alice PUB-Alice pour chiffrer le message et l'envoie à Alice.

- Alice reçoit le message et le déchiffre avec sa clé privée PRI-Alice.