**PARCOURS TAI – Réseaux informatique**

**Activité 12 – VLAN, VPN, Pare-feu, DMZ, DHCP et DNS**

**Les bases des VLAN (Virtual LAN)**

* Expliquez en quelques mots ce qu’est un **VLAN** et à quoi il sert dans un réseau d’entreprise.
* Un réseau d’entreprise contient :
* 20 postes du service **Comptabilité**
* 25 postes du service **Informatique**
* 15 postes du service **Ressources Humaines**

Pourquoi est-il préférable d’utiliser des VLAN plutôt que de tout laisser dans un seul réseau local ?

* Quel est l’avantage d’un VLAN par rapport à une séparation physique avec plusieurs switch distincts ?
* Un administrateur configure deux VLAN sur un switch :
* VLAN 10 : Finance
* VLAN 20 : Technique
* Si un poste du VLAN 10 essaie de communiquer avec un poste du VLAN 20, qu’est-ce qui va se passer ?
* Que faut-il mettre en place pour permettre la communication entre les deux VLAN ?
* Citez deux bénéfices majeurs de l’utilisation des VLAN en entreprise.

**Les VPN**

L’entreprise **Alpha** dispose de :

* Un siège avec 50 employés.
* 15 employés en **télétravail régulier**.
* Des ressources internes : un **serveur de fichiers** et un **logiciel métier** accessible uniquement sur le LAN de l’entreprise.

La direction souhaite permettre aux télétravailleurs d’accéder à distance au réseau de l’entreprise **de manière sécurisée**, sans exposer directement les serveurs sur Internet.

* Expliquez pourquoi un **VPN** est la solution adaptée dans ce cas plutôt qu’un simple partage de fichiers sur Internet.
* Dans ce scénario, faut-il mettre en place un **VPN site-à-site** ou un **VPN client-à-site** ? Justifiez votre réponse.
* Citez deux protocoles ou technologies VPN adaptés pour ce besoin et indiquez **un avantage** pour chacun.
* Lors de la configuration, les utilisateurs se plaignent de ne pas pouvoir atteindre le serveur de fichiers après connexion au VPN.  
  Donnez deux hypothèses possibles expliquant cette panne (ex. problème d’adressage IP, routage, pare-feu).
* Proposez les **bonnes pratiques de sécurité** à respecter pour la mise en place d’un VPN en entreprise (au moins 3 recommandations).

**Le Pare-feu**

L’entreprise **Beta Services** dispose d’un LAN de 40 postes, d’un serveur de fichiers et d’un accès Internet via un routeur. La direction souhaite sécuriser le réseau en mettant en place un **pare-feu**.

* Expliquez à quoi sert un pare-feu dans un réseau local d’entreprise et citez **au moins deux menaces** contre lesquelles il protège.
* Dans le cas de l’entreprise Beta Services, où placeriez-vous le pare-feu dans l’architecture du LAN ? Justifiez votre choix.

Le responsable souhaite bloquer tout le trafic **entrant depuis Internet**, sauf :

* le service **HTTP/HTTPS** vers un serveur web,
* et le service **VPN** pour les télétravailleurs.
* Proposez une règle de filtrage correspondante (sous forme simple, pas besoin de syntaxe réelle).
* Quelle est la différence entre un **pare-feu matériel** (appliance dédiée) et un **pare-feu logiciel** (ex. Windows Firewall) ? Donnez un exemple d’utilisation de chaque type en entreprise.
* Quelles **bonnes pratiques** recommanderiez-vous pour la gestion et la mise à jour d’un pare-feu en entreprise (au moins 3 mesures) ?

**Le DHCP, le DNS et le DMZ**

L’entreprise **GammaTech** dispose :

* d’un **LAN interne** avec 80 postes de travail,
* d’un **serveur web** accessible depuis Internet,
* d’un **serveur DHCP** pour attribuer les adresses IP automatiquement,
* d’un **serveur DNS** interne pour résoudre les noms de domaine locaux.

L’administrateur réseau doit sécuriser l’accès au serveur web et s’assurer que les services DHCP et DNS fonctionnent correctement dans le LAN.

* Expliquez pourquoi il est préférable de placer le **serveur web** dans une **DMZ** plutôt que directement dans le LAN interne.
* Un stagiaire propose de configurer toutes les adresses IP des 80 postes manuellement.  
  Expliquez pourquoi l’utilisation d’un **serveur DHCP** est plus adaptée en entreprise.
* Un utilisateur se plaint de ne pas pouvoir accéder à l’intranet via l’adresse <http://intranet.gammatech.local>
* Quels services ou mécanismes de sécurité doit-on mettre en place pour protéger un serveur situé dans une **DMZ** ? (citez au moins 2 mesures).
* Expliquez comment ces trois éléments (**DMZ, DHCP, DNS**) contribuent ensemble au bon fonctionnement et à la sécurité d’un réseau d’entreprise.

**Protocole et port réseaux**

Associez chaque protocole à son **port standard** :

* HTTP
* HTTPS
* DNS
* SMTP
* FTP (contrôle)
* Ports disponibles : **25 – 21 – 443 – 53 – 80**
* Expliquez la différence entre **TCP** et **UDP**. Donnez un exemple de protocole utilisant TCP et un autre utilisant UDP.
* Un utilisateur n’arrive pas à accéder à son **webmail** (accès via HTTPS). Si le port correspondant est bloqué par le pare-feu, lequel est concerné ?
* Dans l’entreprise DeltaInfo, un serveur de fichiers est accessible via **SMB (Server Message Block)**.
* Quel port est utilisé par SMB/CIFS sur TCP/IP ?
* Pourquoi est-il important pour un technicien TAI de connaître les numéros de ports des protocoles les plus courants en entreprise ? Donnez au moins deux raisons.