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

## VLAN (Virtual Local Area Network)

C'est un réseau local virtuel qui permet de segmenter un réseau physique en plusieurs réseaux logiques indépendants.

**Pourquoi utiliser des VLAN ?**

Le VLAN permet une :

- Séparation logique des services (Comptabilité, Informatique, RH)
- Meilleure sécurité et contrôle du trafic
- Réduction du broadcast inutile

**Avantage par rapport à plusieurs switchs**

L'avantage c'est que :

- Moins de matériel nécessaire
- Plus flexible : un seul switch peut gérer plusieurs VLAN

**Communication entre VLAN 10 et VLAN 20**

Communication entre VLAN 10 et VLAN 20 :

- Par défaut, les VLAN sont isolés : aucune communication directe.
- Pour permettre la communication : mettre en place un routeur ou un switch de niveau 3 (inter-VLAN routing).

**Deux bénéfices majeurs**

Les bénéfices majeurs :

- ***Sécurité accrue :*** isolation des services sensibles
- ***Optimisation du réseau :*** réduction du trafic inutile

## VPN (Virtual Private Network)

**Pourquoi un VPN ?**

Le VPN, il :

- Chiffre les communications
- Permet un accès sécurisé aux ressources internes sans exposer les serveurs sur Internet

**Type de VPN adapté**

***VPN client-à-site :*** chaque télétravailleur se connecte individuellement au réseau de l'entreprise

***VPN site-à-site*** : connexion sécurisée entre deux réseaux locaux distants via Internet

**Deux protocoles VPN**

| Protocole | Avantage |
|---|---|
| OpenVPN | Très sécurisé et compatible multi-plateforme |
| IPSec | Intégré dans de nombreux équipements réseau |

**Deux hypothèses de panne**

La panne peut être lié à un :

- Mauvais routage ou absence de route vers le serveur
- Pare-feu qui bloque le trafic VPN ou interne

**Bonnes pratiques VPN**

Les bonnes pratiques liées au VPN :

- Authentification forte (certificats ou MFA)
- Chiffrement fort (AES-256)
- Journalisation des connexions et surveillance

## Pare-feu

Le pare-feu filtre le trafic réseau entrant et sortant pour protéger le réseau contre les intrusions.

**Menaces bloquées**

Les menaces possibles qui sont bloqués :

- Attaques externes (ex. scans de ports)
- Accès non autorisés aux ressources internes

**Placement dans le LAN**

Entre le routeur Internet et le réseau interne (LAN) pour filtrer tout le trafic entrant et sortant.

**Règle de filtrage**

Les règles de filtrage sont :

- Autoriser : HTTP/HTTPS vers serveur web, VPN
- Bloquer : tout autre trafic entrant

**Pare-feu matériel vs logiciel**

| Type | Exemple | Usage |
|---|---|---|
| Matériel | Cisco ASA | Protection du réseau entier |
| Logiciel | Windows Firewall | Protection d'un poste individuel |

**Bonnes pratiques**

Les bonnes pratiques du pare-feu :

- Mettre à jour régulièrement les règles et le firmware
- Sauvegarder la configuration
- Surveiller les logs et alertes

## DHCP, DNS et DMZ

**Pourquoi placer le serveur web en DMZ ?**

Placer le serveur web en DMZ permet de :

- Séparer les ressources accessibles depuis Internet du LAN interne
- Limiter les risques en cas de compromission

**DHCP vs IP manuelle**

DHCP : attribution automatique, rapide et sans erreur

IP manuelle : chronophage, source d'erreurs

**Problème d'accès à l'intranet**

En cas de problème d'accès intranet :

- Vérifier le serveur DNS interne
- Vérifier que le nom de domaine est bien configuré

**Sécuriser un serveur en DMZ**

Pour sécuriser un serveur en DMZ, il faut :

- Pare-feu dédié avec règles strictes
- Surveillance et mises à jour régulières

**Contribution des trois éléments**

***DMZ*** : protège le LAN des accès externes

***DHCP*** : simplifie la gestion IP

***DNS*** : facilite l'accès aux ressources internes

## Protocoles et ports

**Association protocole/port**

***HTTP*** = port 80

***HTTPS*** = port 443

***DNS*** = port 53

***SMTP*** = port 25

***FTP*** = port 21

**TCP vs UDP**

***TCP*** : connexion fiable, vérification des paquets (ex : HTTPS)

***UDP*** : rapide, sans vérification (ex : DNS)

**Port bloqué pour le webmail**

Bloquer sur la liaison entre webmail et HTTPS : Port 443 (HTTPS)

**Port SMB/CIFS**

Pour SMB c'est le port 445 (TCP)

**Importance de connaître les ports**

C'est important de connaitre les ports car :

- Pour configurer les pares-feux et les routeurs
- Pour diagnostiquer les problèmes de connexion