Notions Réseau

- Les enregistrements DNS
- Qu'est-ce qu'une DMZ
- Comprendre RADIUS
- La fibre optique : Comprendre FTTH, FTTB et FTTx

Les enregistrements DNS

Les enregistrements DNS (Domain Name System) sont très importants pour le fonctionnement d'Internet, permettant la traduction des noms de domaine faciles à retenir en adresses IP que les machines utilisent pour communiquer entre elles.

Voici un guide compact pour comprendre les types d'enregistrements DNS les plus courants et leur fonction.

1. Enregistrement A (Address Record)

- **Fonction :** Associe un nom de domaine à une adresse IPv4.
- **Usage :** Fondamental pour diriger le trafic vers l'hébergement d'un site web.

2. Enregistrement AAAA

- **Fonction :** Similaire à l'enregistrement A, mais associe un nom de domaine à une adresse IPv6.
- **Usage :** Important pour le routage du trafic dans les réseaux supportant IPv6.

3. Enregistrement CNAME (Canonical Name)

- **Fonction :** Permet à un domaine de faire référence à un autre nom de domaine.
- **Usage :** Utile pour associer des sous-domaines à un domaine principal ou lorsque plusieurs domaines pointent vers le même serveur.

4. Enregistrement MX (Mail Exchange)

- **Fonction :** Dirige les emails envoyés à votre domaine vers les serveurs de messagerie.
- **Usage :** Essentiel pour la configuration de la messagerie électronique pour votre domaine.

5. Enregistrement TXT

- **Fonction :** Permet au propriétaire du domaine d'insérer du texte dans le DNS.
- **Usage :** Souvent utilisé pour la vérification de la propriété du domaine, la configuration des politiques de sécurité email (SPF, DKIM, DMARC).

6. Enregistrement SRV (Service Record)

- **Fonction :** Fournit des informations sur les services disponibles sous un domaine spécifique, incluant le nom du service, le protocole, le port, et le nom d'hôte du serveur.
- **Usage :** Utilisé pour des services spécifiques tels que la VoIP, les services de messagerie instantanée.

7. Enregistrement NS (Name Server)

- **Fonction :** Indique quels serveurs DNS sont autoritatifs pour un domaine.
- **Usage :** Fondamental pour la délégation de sous-domaines et la gestion des réponses DNS.

Bonnes pratiques pour la gestion des enregistrements DNS

- **Planification :** Avant de modifier vos enregistrements DNS, assurez-vous de bien comprendre l'impact de ces changements.
- **Sécurité :** Utilisez des enregistrements TXT pour appliquer des politiques SPF, DKIM, et DMARC afin de réduire le risque de phishing et d'autres formes d'abus email.
- **Redondance :** Assurez-vous que votre domaine est servi par plusieurs serveurs DNS pour améliorer la disponibilité
- **Documentation :** Gardez une trace de tous les changements apportés à vos enregistrements DNS pour faciliter le dépannage et la maintenance futurs.

Les enregistrements DNS sont vitaux pour le bon fonctionnement d'Internet. Ils aident à diriger le trafic web vers les bons endroits, permettant aux gens de trouver ce qu'ils cherchent rapidement et en toute sécurité. Savoir comment ils fonctionnent peut vraiment améliorer la façon dont vous gérez vos sites et services en ligne.

Qu'est-ce qu'une DMZ

Une DMZ (pour *Demilitarized Zone* ou zone démilitarisée) est une partie d'un réseau informatique qui sert d'intermédiaire entre un réseau interne d'une organisation (souvent sécurisée) et un réseau externe (souvent internet).

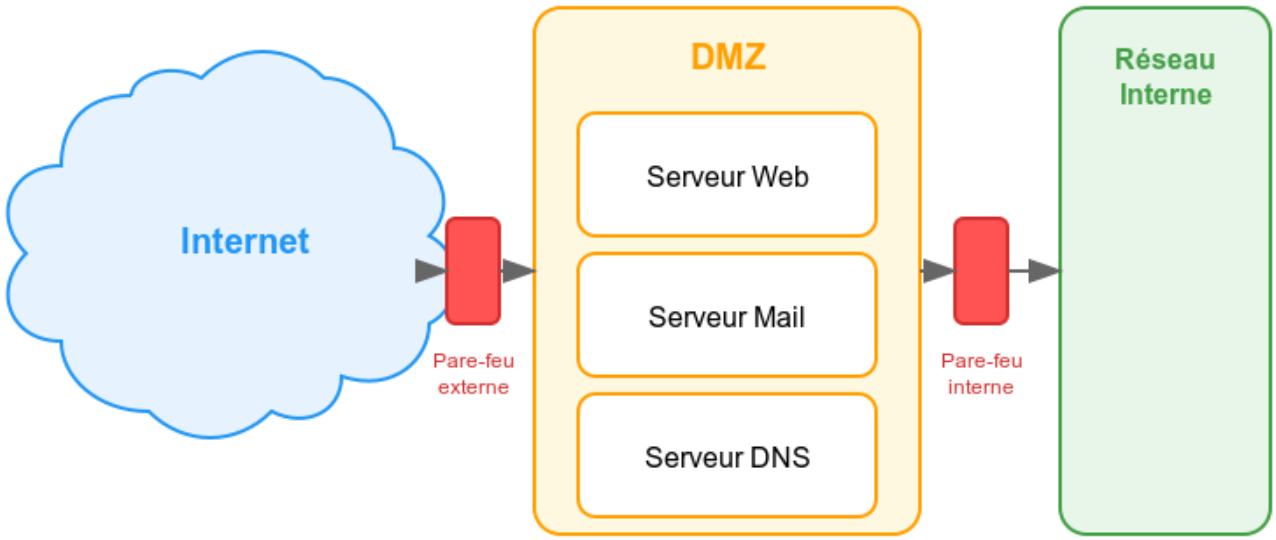
Voici les points importants à retenir :

- **Séparation des environnements :**
  La DMZ permet d'isoler les serveurs exposés (sites internet, serveurs de messagerie, de fichiers, etc.) du réseau interne. Ainsi, même si une personne malveillante compromet un serveur dans la DMZ, il ne peut pas accéder directement aux ressources critiques de l'entreprise.
- **Renforcement de la sécurité**
  En filtrant et en contrôlant le trafic entre le réseau public et le réseau privé, la DMZ ajoute une couche de défense supplémentaire, réduisant les risques d'attaques directes sur le

  réseau interne.

- **Gestion des accès :**
  Des règles de pare-feu strictes sont mises en place pour limiter les communications entre la DMZ, généralement l'on ouvre les accès pour que notre service fonctionne, rien de plus. Cela limite les communications entre la DMZ, le réseau interne et internet et de contrôler précisément qui a accès à quoi.
- **Utilisation typique :**
  On y héberge souvent des serveurs qui doivent être accessibles depuis l'extérieur (sites web, serveurs d'applications publiques, etc.) tout en préservant la sécurité du réseau interne.

Exemple de schéma d'architecture réseau avec DMZ


Internet
Pare-feu externe
DMZ
Serveur Web
Serveur Mail
Serveur DNS
Pare-feu interne
Réseau Interne

Comprendre RADIUS

Le protocole **RADIUS** (*Remote Authentication Dial-In User Service*) est un outil qui aide à gérer qui peut accéder à un réseau et ce qu'il peut y faire. Imaginez que vous ayez un club privé, et que pour entrer, chaque personne doit montrer son badge pour prouver qu'il est membre. RADIUS fonctionne de manière similaire pour les réseaux (c'est un peu le videur musclé devant la porte).

Qu'est-ce que RADIUS ?

RADIUS est un système qui se trouve généralement sur un serveur central et qui gère trois fonctions principales :

1. **Authentification :**
   C'est le processus qui vérifie l'identité de l'utilisateur. Par exemple, quand vous vous connectez à un réseau Wi-Fi, vous entrez votre nom d'utilisateur et votre mot de passe. RADIUS vérifie ces informations pour s'assurer que vous êtes bien celui que vous prétendez être.

2. **Autorisation :**
   Une fois que RADIUS a confirmé votre identité, il décide de ce à quoi vous avez le droit d'accéder. Dans notre exemple du club privé, c'est pour vérifier que vous avez accès à certaines zones réservées ou à certains services une fois que vous êtes entré.

3. **Suivi des connexions (Accounting) :**
   RADIUS garde une trace de ce que vous faites pendant que vous êtes connecté. Cela peut inclure la durée de votre session, les ressources que vous avez utilisées, etc. Cela permet d'aider à surveiller l'utilisation du réseau, à résoudre des problèmes ou même à facturer des services dans certains cas.

Comment ça marche ?

Voici une explication étape par étape, comme si vous assistiez à une petite démonstration :

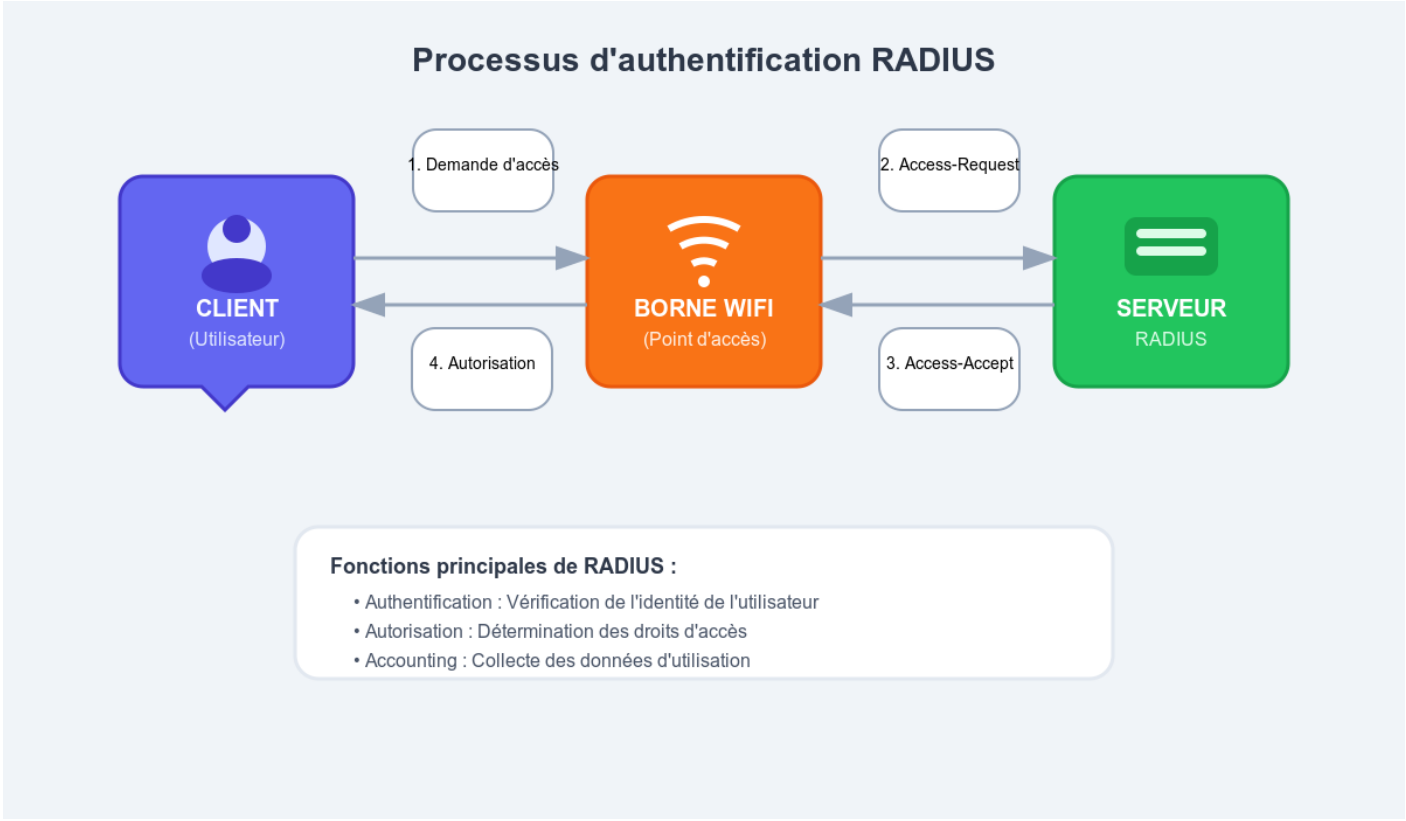
1. **Connexion :**
   Vous (ou votre appareil) essayez de vous connecter au réseau. Vous entrez vos identifiants (nom d'utilisateur et mot de passe).

2. **Envoi de la demande :**
   Votre appareil envoie ces informations à un dispositif d'accès (comme un point d'accès Wi-Fi), qui à son tour les transmet au serveur RADIUS.

3. **Vérification :**
   Le serveur RADIUS reçoit la demande et la compare avec ses données (qui peuvent provenir d'une base de données, d'un annuaire Active Directory ou d'un autre système de gestion des utilisateurs). Si vos informations correspondent, il vous authentifie.

4. **Définition des droits d'accès :**
   Une fois authentifié, RADIUS vérifie également à quelles ressources vous avez le droit d'accéder (par exemple, accéder à certains services ou sections du réseau).

5. **Suivi de la session :**
   Pendant que vous êtes connecté, le serveur enregistre les informations sur votre session. Cela peut aider l'administrateur du réseau à surveiller l'activité ou à détecter des comportements malveillants ou inhabituels



Pourquoi utiliser RADIUS ?

Pour résumer, RADIUS est très utile, car il permet de :

- **Centraliser la gestion des accès :**
  Au lieu de devoir configurer chaque point d'accès ou service séparément, toutes les demandes sont gérées par un seul serveur. Cela simplifie la vie de l'administrateur réseau.

- **Renforcer la sécurité :**
  En vérifiant l'identité des utilisateurs et en limitant ce qu'ils peuvent faire, RADIUS aide à protéger le réseau contre les accès non autorisés.

- **Suivre l'utilisation du réseau :**
  Grâce aux données enregistrées, il est plus facile de comprendre comment le réseau est utilisé et d'identifier rapidement les problèmes ou les tentatives d'intrusion.

La fibre optique : Comprendre FTTH, FTTB et FTTx

Le déploiement de la fibre optique a révolutionné la connectivité Internet en offrant des débits bien supérieurs aux technologies comme l'ADSL. Il existe plusieurs types de fibre optique selon le mode de raccordement ?

Qu'est-ce que la fibre optique ?

La fibre optique est une technologie de transmission de données basée sur des fils en verre ou en plastique ultra-fins, capable de transporter des signaux lumineux sur de longues distances. Contrairement aux câbles en cuivre de l'ADSL, la fibre permet des vitesses bien plus élevées et une meilleure stabilité.

Pourquoi la fibre est-elle plus performante que l'ADSL ?

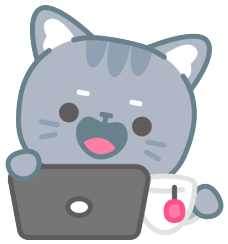
- L'ADSL utilise des câbles en cuivre qui subissent une atténuation du signal sur de longues distances, car le cuivre transporte des signaux électriques qui se dégradent progressivement à mesure qu'ils parcourent le câble. Cette atténuation est due à la résistance du matériau et aux interférences électromagnétiques, ce qui réduit la vitesse et la qualité du signal,
  notamment au-delà de quelques kilomètres.
  À l'inverse, la fibre optique utilise des impulsions lumineuses transmises à travers un noyau en verre ou en plastique. La lumière étant beaucoup moins sujette aux pertes d'énergie que le courant électrique, elle peut parcourir plusieurs dizaines, voire centaines de kilomètres sans dégradation significative.
- La fibre optique offre des **débits symétriques**, c'est-à-dire que les vitesses d'envoi et de réception des données sont similaires, contrairement à l'ADSL où l'envoi est plus lent que

la réception.
- La latence est bien plus faible avec la fibre optique, car les signaux lumineux qu'elle transporte se déplacent beaucoup plus rapidement que les signaux électriques utilisés dans les câbles en cuivre, ce qui améliore les performances pour les jeux en ligne et la visioconférence.

Elle est utilisée pour divers types de raccordement, dont les plus courants sont :

- **FTTH (Fiber To The Home) :** Fibre jusqu'au domicile
- **FTTB (Fiber To The Building) :** Fibre jusqu'à l'immeuble
- **FTTO (Fiber To The Office) :** Fibre jusqu'aux bureaux
- **FTTA (Fiber To The Antenna) :** Fibre jusqu'aux antennes relais (4G/5G)

FTTH : La fibre jusqu'à la maison



Le FTTH est la technologie de fibre la plus répandue pour les particuliers. C'est très probablement celle que vous avez actuellement à la maison si vous êtes équipés de la fibre. Elle permet un raccordement direct de la fibre optique jusqu'à l'intérieur du logement. Cette connexion offre des débits élevés pouvant atteindre **1Gbit/s, voire 10Gbit/s dans certaines offres avancées,** garantissant ainsi une connexion stable et fluide.

Le principal avantage du FTTH est qu'il ne dépend pas du réseau cuivre existant. Ainsi, même si vous habitez loin du nœud de raccordement, votre connexion ne subira pas de perte de performances.

FTTB : La fibre jusqu'à l'immeuble

Le FTTB est principalement utilisé pour raccorder les immeubles collectifs. La fibre arrive dans la cave ou un local technique, puis des câbles en cuivre ou coaxiaux distribuent la connexion aux logements. Cette solution est souvent mise en place dans les grandes villes où il est plus simple

d'amener la fibre à un bâtiment plutôt qu'à chaque logement individuellement.

Les débits offerts en FTTB sont généralement **compris entre 100 Mbit/s et 1Gbit/s,** selon la qualité des câbles utilisés dans l'immeuble.

Le FTTB est une alternative intéressante lorsque le déploiement du FTTH est complexe. Toutefois, la présence de câbles en cuivre sur le dernier segment peut réduire légèrement la performance par rapport à une connexion entièrement en fibre.

FTTO : La fibre pour les entreprises

La FTTO est une solution dédiée aux entreprises, offrant un débit garanti et une qualité de service supérieure.
Contrairement à la FTTH, la bande pa[illegible]pas partagée avec d'autres abonnés grâce à

l'utilisation d'une **fibre dédiée.**

La FTTO repose majoritairement sur une liaison **point-à-point** entre l'entreprise et le nœud de raccordement de l'opérateur.

Les débits proposés en FTTO varient généralement de **10Mbits/s à plusieurs Gbit/s,** avec des garanties de services adaptées aux besoins professionnels.

Ce type de connexion est particulièrement adapté aux structures nécessitant une connexion fiable et sécurisée, comme les bureaux et les centres de données. Il permet également d'obtenir une **garantie de temps de rétablissement (GTR)**, c'est-à-dire une intervention rapide en cas de panne.

FTTA : La fibre jusqu'aux antennes mobiles :

La FTTA est utilisée pour relier les antennes 4G et 5G aux réseaux des opérateurs. Cela permet d'améliorer la couverture mobile et la qualité des connexions sans fil.

Sans fibre optique, le réseau mobile dépendrait uniquement de liaisons hertziennes, moins rapides et plus sensibles aux interférences. La FTTA garantit ainsi une meilleure expérience pour les

utilisateurs de smartphone, en réduisant la latence et en augmentant les débits qui peuvent atteindre **plusieurs Gbit/s** pour assurer une bonne connectivité de la 5G.

Le futur de la fibre optique :

Le déploiement de la fibre continue à s'étendre, avec des innovations comme :

- **La fibre 10G PON,** qui permettra des débits encore plus élevés pour les particuliers et les entreprises.
- **Le développement de la fibre quantique,** qui pourrait révolutionner la cybersécurité en offrant des communications ultra-sécurisées.
- **Une couverture plus large dans les zones rurales**, grâce aux investissements des opérateurs ou des gouvernements.

Avec ces différentes technologies, la fibre optique s'adapte aux besoins variés des particuliers, des entreprises et des infrastructures mobiles.