Sécurité : Sécurisation du réseau

Le réseau est soumis à différents types d'attaques et différents types de risques. Les 2 principales attaques concernent le déni de service et l'écoute

L'écoute consiste à porter atteinte à la confidentialité et/ou à l'intégrité des données en transit. Pour cela, 2 types d'écoute :

- L'écoute passive : l'attaquant est en mesure d'écouter les conversations entre A et B, représentant une atteinte à la confidentialité des échanges
- L'écoute active : l'attaquant est en mesure de s'insérer dans la conversation entre A et B sans que ceux-ci le sachent représentant une atteinte à la confidentialité et à l'intégrité des échanges.

Le déni de service, nous l'avons vu, consiste à porter atteinte à la disponibilité du réseau.

Le principe de base est de n'autoriser la connexion au réseau qu'aux équipements maîtrisés. En effet, chaque équipement se connectant au réseau constitue une point d'entrée potentiellement vulnérable. De plus, les équipements personnels (PC portables, tablettes, smartphones, …) sont difficilement maitrisables, tout comme les équipements des visiteurs (clients, fournisseurs, …) échappent à tout contrôle de l'entité.

Pour cela, idéalement, seule la connexion de terminaux maitrisés par l'entité doit être autorisée sur ses différents réseaux d'accès qu'ils soient filaires ou sans fils.

Quelques propositions de mise en place : ……..

Un réseau wifi avec SSID dédié et isolé pourra être mis en place pour les terminaux personnels ou visiteurs

L'authentification des postes sur le réseau standard reposera sur le protocole 802.1X par exemple.

La sécurisation des réseaux repose sur différents composants ainsi que sur une architecture spécifique constitués en 3 zones :

- La zone dangereuse : Internet non maitrisé et non maitrisable par l'entreprise
- La zone à risques : la DMZ
- La zone de confiance : le réseau local maitrisé par l'entreprise

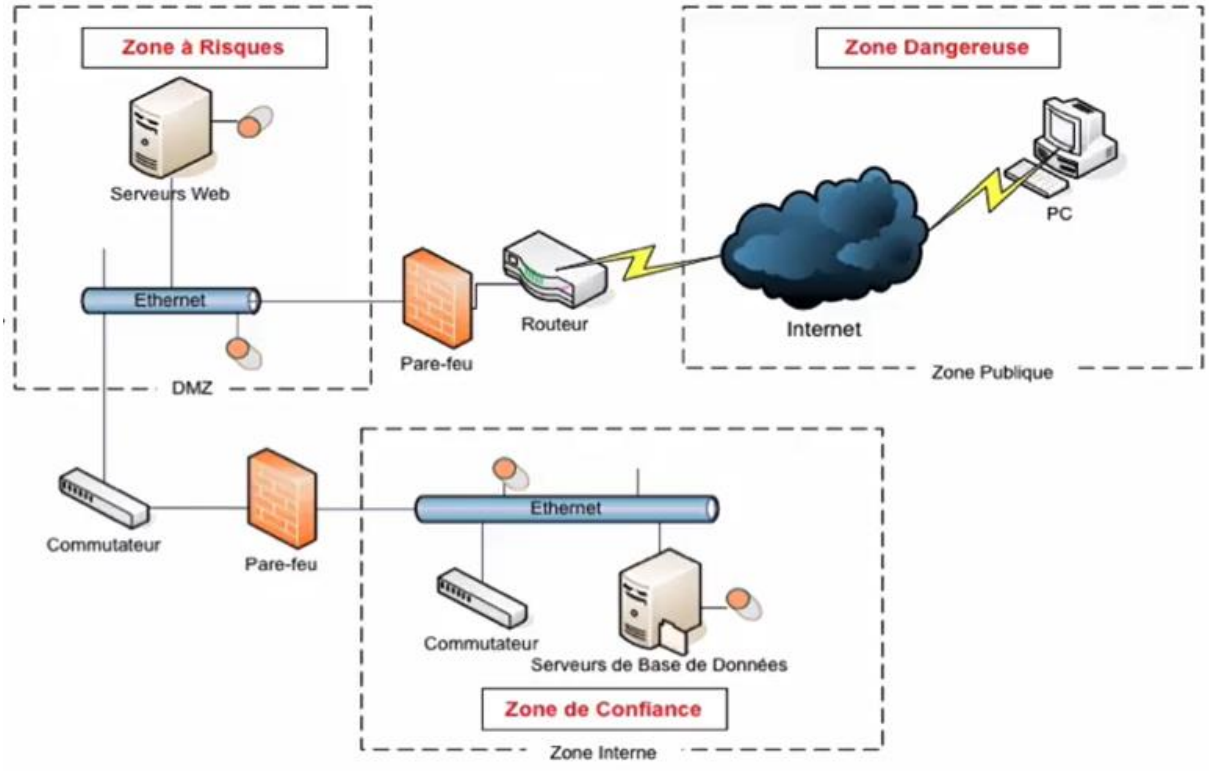
Au départ, les entreprises utilisaient un réseau à plat, avec aucun mécanisme de cloisonnement. Ce qui induisait que chaque machine pouvait accéder à n'importe quelle autre machine. La compromission de l'une d'entre elle mettait alors en péril tout le réseau.

Aujourd'hui le réseau doit être segmenté en zones composées de systèmes ayant des besoins de sécurité homogènes. Une zone se caractérise alors par de VLAN dédiés, voire par des infrastructures dédiées selon sa criticité. Des mesures de cloisonnement à l'aide de filtrage peuvent être mis en place.

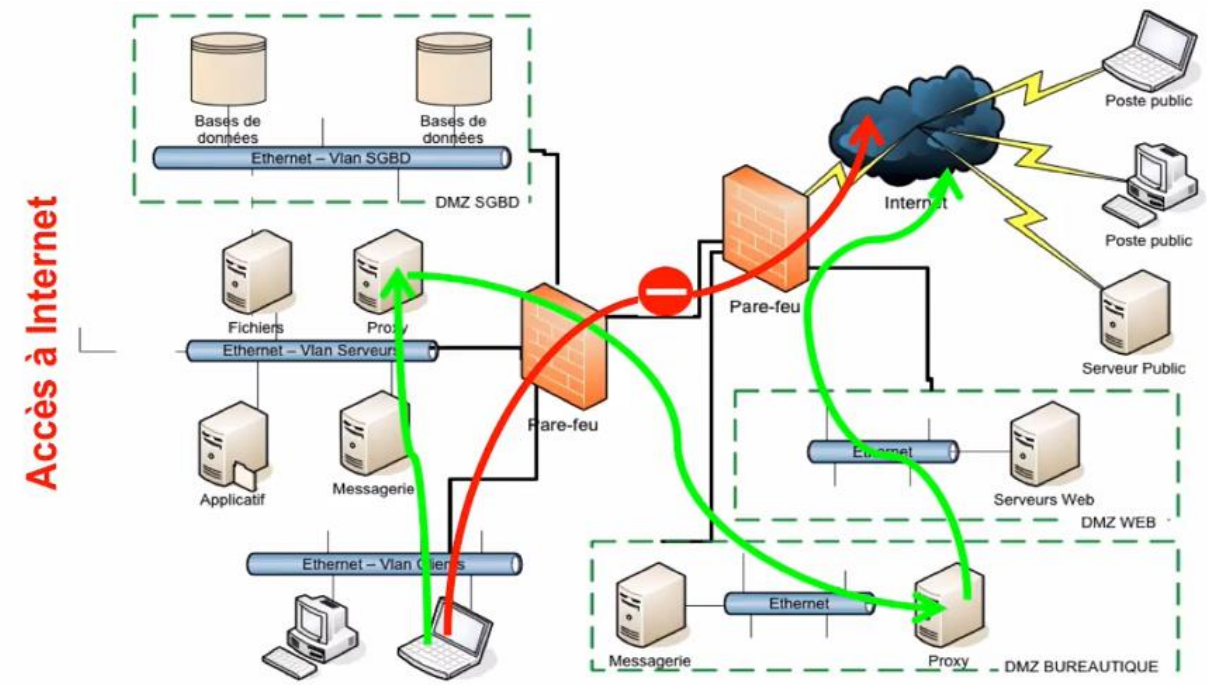
Au niveau sécurité, la base est la mise en place de :

- Pare-feu
- Segmentation du réseau
- VLAN
- Répartiteurs de charges

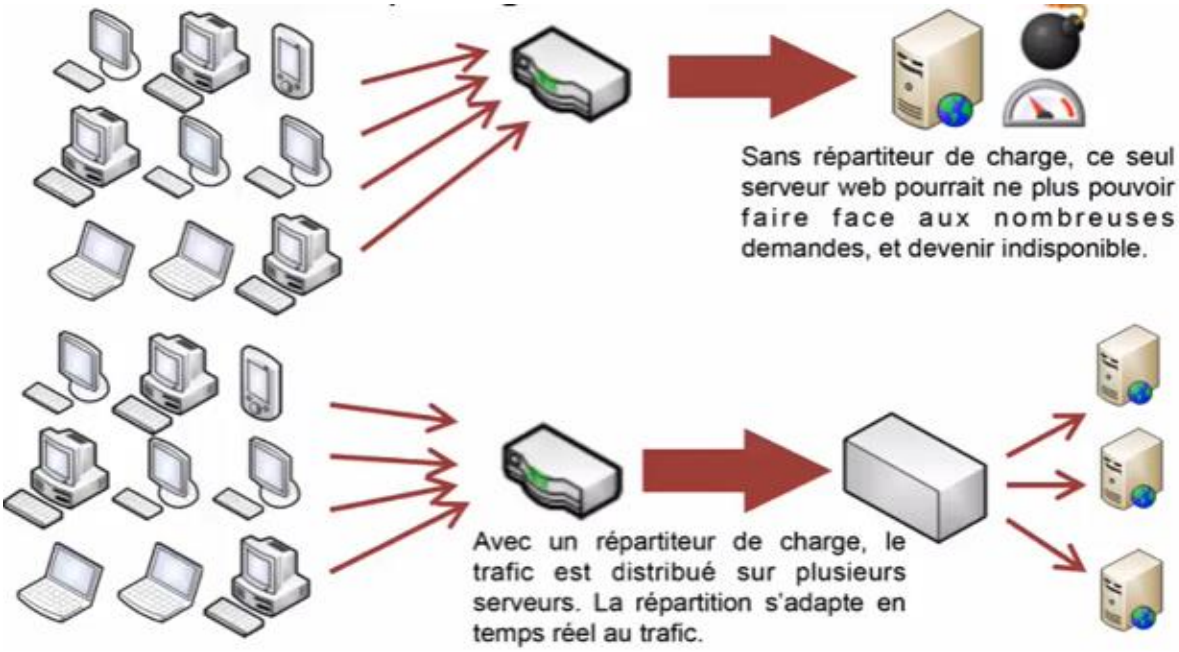
- Antivirus
- Proxy
- Reverse Proxy
- IDS/IPS
- VPN (attention à la disponibilité, seul pilier non maîtrisable)
- Wifi sécurisés (Radius)



Exemple de règles sur les firewalls :



Sur le schéma réseau précédent, le répartiteur de charges n'est pas représenté. Il permet d'optimiser les ressources réseaux, mais aussi de lutter contre le déni de service. On le mettra en place sur les grosses infra où les services doivent faire face à un fort trafic.

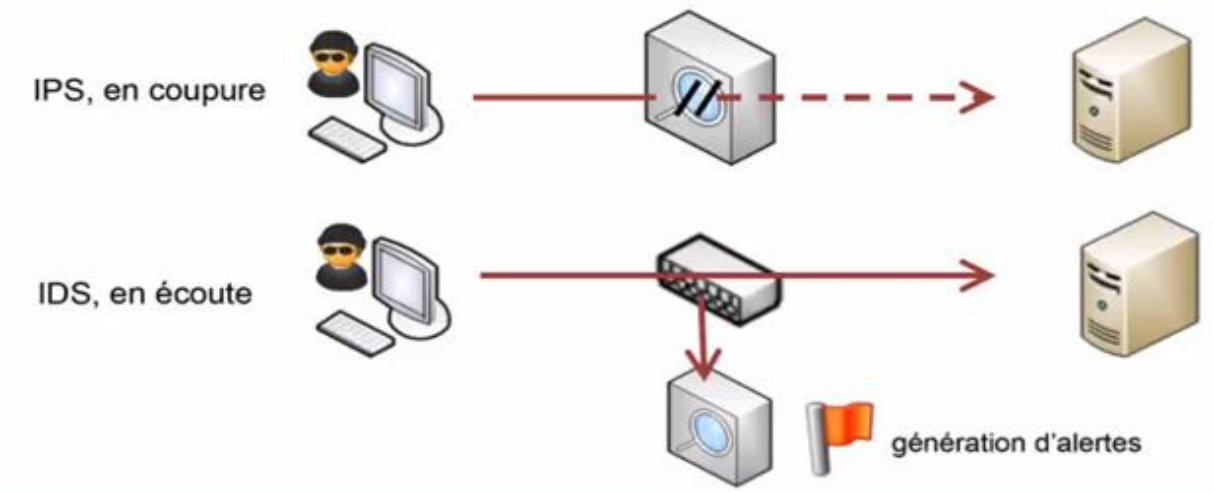


Dans ce schéma, nous pourrons par exemple mettre en œuvre un reverse proxy. Celui-ci permet aux utilisateurs d'Internet d'accéder indirectement à nos ressources. Il peut effectuer du filtrage de certaines IP publiques, mais aussi permet la répartition de charge

- L'antivirus, non présent sur le schéma, est un logiciel chargé d'identifier et de stopper les malwares. Il sera déployé :
    - En local, sur les postes de travail et les serveurs
    - En coupure des flux réseaux, sur les pare feu qui analyseront les flux potentiellement infectés
    - Sur le proxy afin d'analyser l'ensemble des flux http

- Le proxy devra authentifier l'utilisateur accédant aux ressources sur le Web, afin de journaliser les transactions (conservation obligatoire pendant 1 an). Les salariés devront en être avertis de manière juridique.

- Nous l'avons vu en début de formation, l'IDS/IPS permet d'écouter le trafic afin de repérer des activités anormales suspectes. L'IDS est un système passif, positionné soit en coupure de flux réseau, soit positionné en écoute. L'IPS est lui forcément placé en coupure du flux de façon à pouvoir bloquer le trafic lorsque cela est nécessaire. Il existe 2 niveaux, les NIDS/NIPS pour les réseaux et les HIDS/HIPS pour les hôtes.



- Concernant le VPN, nous veillerons particulièrement à la disponibilité, seul pilier de la sécurité non maîtrisable. L'intégrité, la confidentialité, et la preuve sont assuré par le chiffrement et les certificats, mais la disponibilité ne peut être garantie du fait que l'infrastructure de transport utilisé dépend d'Internet. De préférence on choisira IPSEC pour du site2site, tout en considérant le partenaire distant comme non sûr, du filtrage sera donc mis aussi en place, ainsi qu'un IDS/IPS. Pour du VPN site2site, on envisagera la possibilité d'utiliser MPLS faisant appel aux infra spécifiques des opérateurs

- L'utilisation du wifi présente des risques de sécurité bien spécifiques au niveau de la disponibilité (très dépendant de l'environnement), de la zone de couverture (le périmètre n'est pas maitrisé et ne s'arrête pas aux murs de l'entreprise), et de la configuration par défaut (aujourd'hui encore, de nombreuses bornes ont le mdp d'usine admin/admin …). Afin de sécuriser au mieux notre réseau wifi, on veillera à :

    - Segmenter le réseau wifi de l'architecture filaire
    - Filtrage des flux en provenance des postes connectés
    - Chiffrement robuste et authentification centralisée
    - Protection du wifi par clé pré partagée à proscrire
    - Administration des PA de manière sécurisée
    - Séparation des wifi d'entreprise et des wifi invités (VLAN différents à minima)

Bien entendu on utilisera des protocoles sécurisés pour toutes les connexions (SSH, HTTPS, IMAPS, …)

La messagerie est l'un des principaux vecteurs d'infection du poste de travail (avec le navigateur), par l'ouverture de pièces jointes contenant un code malveillant ou un lien redirigeant vers un site lui-même malveillant.

La première chose à faire est la sensibilisation des utilisateurs :

- L'expéditeur est-il connu ?
- Une information de sa part est-elle attendue ?
- Le lien proposé est-il cohérent avec le sujet ?
- Vérification de l'authenticité du message via un autre canal (téléphone, sms, …)
- La redirection des messages vers une messagerie personnelle est à proscrire

- L'accès distant à la messagerie professionnelle devra être extrêmement sécurisé

Comme bien sûr il ne faut surtout pas faire intégralement confiance à l'utilisateur, des outils seront déployés en amont :

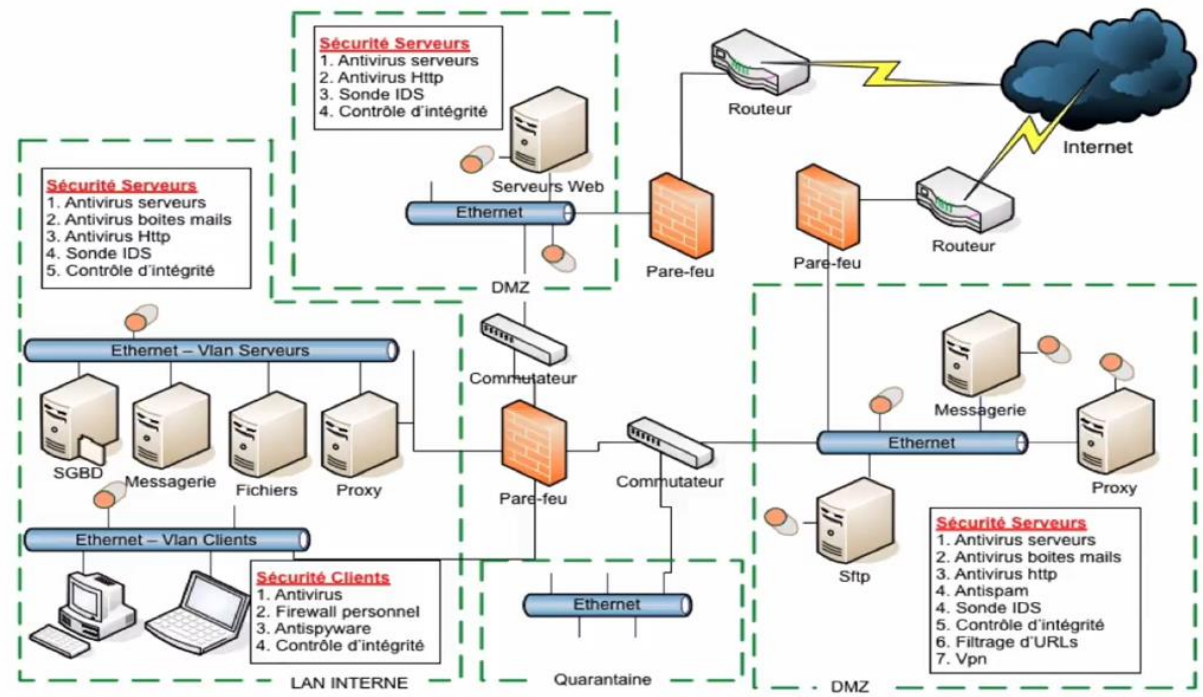
- Un système antiviral des boites aux lettres des utilisateurs
- Le chiffrement TLS entre serveurs de messageries et entre les postes et les serveurs
- Les serveurs de messagerie ne doivent pas être directement exposés sur Internet, mais au travers de relais dans une DMZ
- Déploiement d'un service anti-spam
- Vérification d'authenticité et de la bonne configuration des enregistrements DNS publics

Enfin nous ferons extrêmement attention aux architectures spontanées. Celle-ci désigne les dispositifs informatiques en place directement par les utilisateurs sans en référer à la DSI. Nous trouvons par exemple :

- Les périphériques de stockage : clé USB, disques portables
- Bornes Wifi : Ad-Hoc ou partage de connexion avec mobile
- Accès Internet : certains services n'hésitent pas à commander des accès internet grand public afin de contourner les limitations de l'accès officiel
- Services Cloud : Prise à distance des équipements, partage de fichiers, messageries, …
- Serveurs non gérés par la DSI

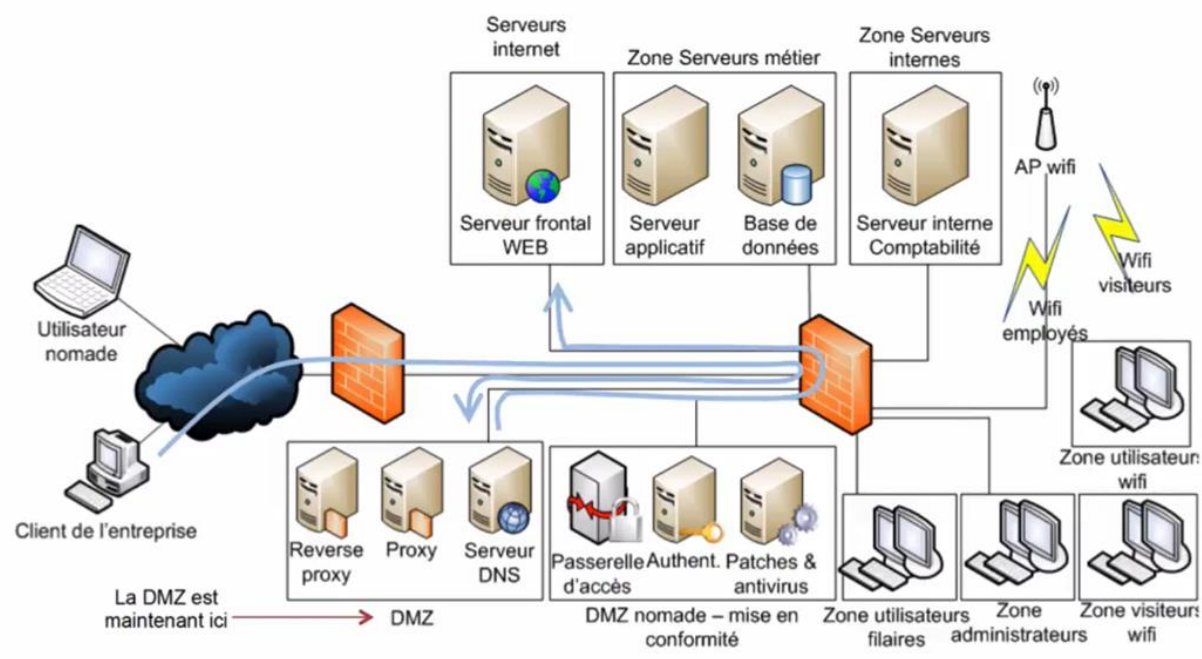
EXERCICES :

Exemple d'architecture mise en place



- Commentez et argumentez la sécurité mise en place dans ce réseau
- Expliquez l'intérêt d'une zone de quarantaine

- Mettant en avant la sécurité mise en place dans le schéma suivant



-