Julien VADAM
Antonin WITTIG

Audit de l'architecture réseau actuel

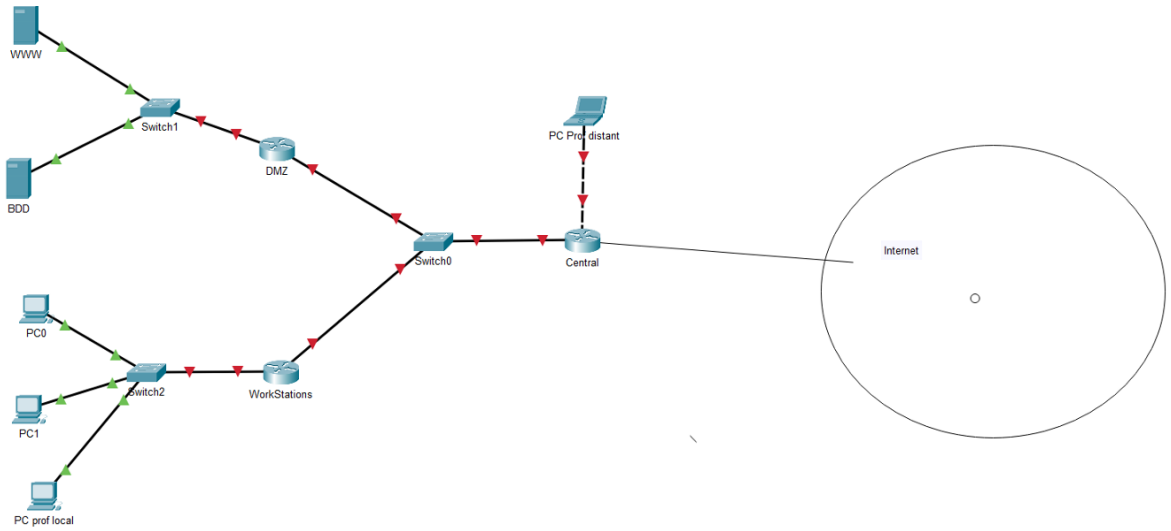

schéma du réseau actuel

Problèmes identifiés

En regardant l'état actuel du réseau, plusieurs failles importantes sautent aux yeux :

1. **Pas de séparation logique :**
   Tout est connecté sans réelle organisation (serveurs, postes utilisateurs, DMZ).
   Résultat :
   - Si un poste est compromis, les serveurs critiques deviennent accessibles.
   - Un virus ou ransomware pourrait se propager partout, sans limite.
2. **Pas d'outils pour surveiller le réseau :**
   - Il n'y a pas de système pour détecter ou bloquer des comportements anormaux (comme un IDS/IPS).
   - Les attaques, comme des exfiltrations de données, pourraient passer inaperçues.
3. **Manque de contrôle des communications internes :**
   - Le routeur central n'a pas de règles pour filtrer les flux entre les différentes parties du réseau.
   - Ça laisse la porte ouverte à des menaces venant de n'importe quel segment.
4. **DMZ mal gérée :**
   - Les serveurs exposés à Internet (comme le serveur web) ne sont pas isolés.
   - Si un attaquant prend le contrôle d'un de ces serveurs, il pourrait facilement accéder au réseau interne.

Proposition de réseau future pour l'Hôpital :

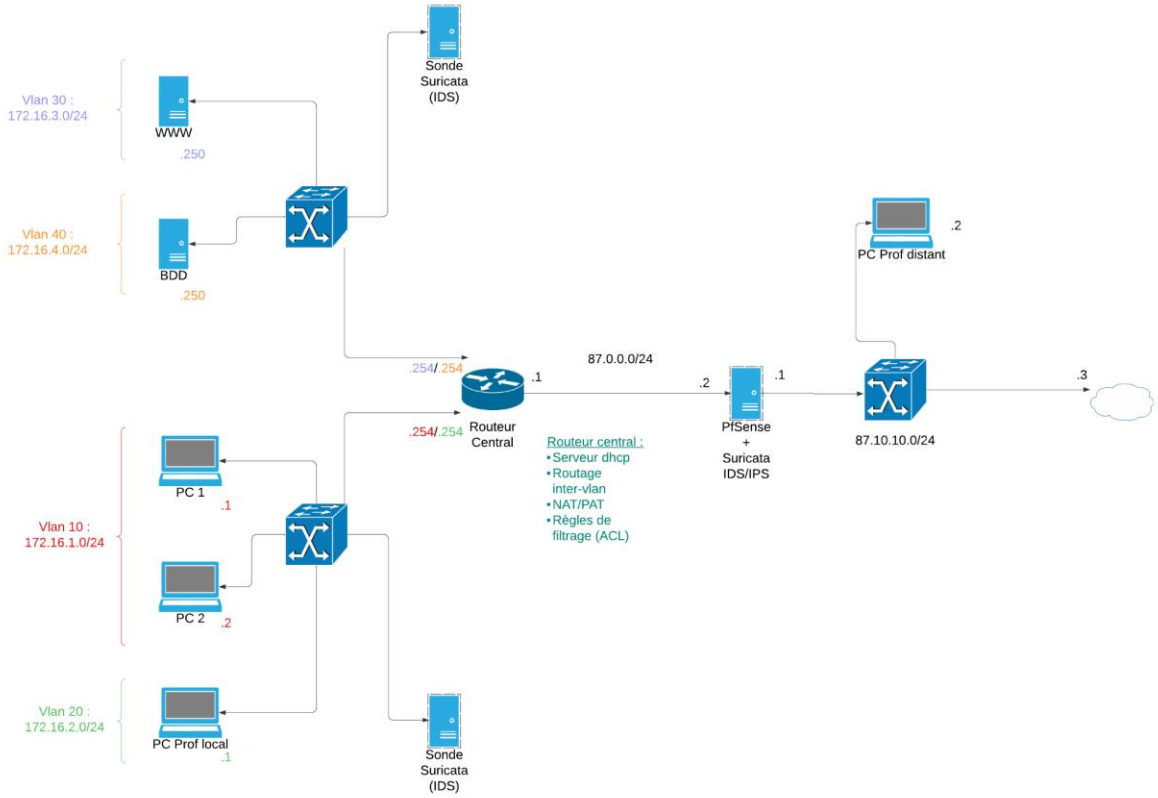

Schéma mis à jour

Nouvel état du réseau

Voici ce qui pourrait être fait pour résoudre les problèmes et renforcer la sécurité :

1. **Créer des VLAN :**
   - Séparer le réseau en segments logiques pour chaque type d'équipement (ex. : VLAN pour les utilisateurs, un autre pour les serveurs).
   - Résultat : une attaque reste limitée à un segment, et les communications entre les parties sont mieux contrôlées.
2. **Ajouter un IDS/IPS :**
   - Installer des sondes comme **Suricata** pour surveiller le réseau et détecter les comportements bizarres (ex. : tentative d'attaque).
   - Ça permet de bloquer les menaces avant qu'elles ne se propagent.
3. **Installer un pare-feu efficace :**
   - Utiliser **PfSense** pour gérer les accès depuis l'extérieur et les communications internes.
   - Le pare-feu s'assure que seules les communications autorisées passent.
4. **Réorganiser la DMZ :**
   - La mettre dans un VLAN spécifique, isolé du reste du réseau.

- Toutes les connexions entre la DMZ et l’interne passeront par des règles strictes définies sur le routeur.

Conclusion :

Le premier schéma illustre une infrastructure réseau vulnérable, où l’absence de segmentation, de filtrage et d’outils de surveillance expose l’organisation à des attaques potentielles. En revanche, le second schéma apporte des solutions concrètes à ces problématiques. Il met en place une segmentation efficace avec des VLANs, intègre des outils de détection et de prévention d’intrusion, et ajoute un pare-feu performant pour protéger les communications avec l’extérieur. Ces améliorations permettent de limiter les risques de propagation des menaces et renforcent la sécurité globale de l’infrastructure, tout en offrant une meilleure gestion du réseau. Ce travail illustre une approche réfléchie pour transformer un réseau vulnérable en une infrastructure plus robuste et résiliente face aux cybermenaces.