Livrable Sprint 3 : : Mise en place des services réseau et sécurisation

1/ Objectif du sprint

Pour ce Sprint 3, notre objectif était de compléter l'infrastructure déjà fonctionnelle réalisée lors des sprints précédents, en ajoutant les services réseau essentiels et les premiers mécanismes de sécurité.
Après la configuration des VLANs, du routage inter-VLAN et du DHCP au Sprint 2, ce sprint devait permettre :

- d'activer la résolution interne via le serveur DNS,
- de mettre en place la journalisation centralisée (Syslog),
- d'héberger un premier site Web interne en DMZ,
- d'appliquer une première couche de sécurité via ACL,
- et enfin de tester le NAT/PAT pour simuler une connexion Internet.

Ce sprint marque la transition entre un réseau fonctionnel et un réseau avec des services intégrés et contrôlés.

2/ Tâches réalisées

Ce sprint contenait un ensemble de tâches techniques découpées et suivies via Trello. Voici ce que nous avons réalisé :

Configuration du serveur DNS :

- Ajout de l'adresse IP statique : 192.168.30.10
- Ajout d'enregistrements A (serveur Web DMZ, routeur, serveurs internes…)
- Ajout d'un enregistrement interne web.local
- Test via ping web.local et nslookup → Résultat : Fonctionnel

Vérification du DHCP :

- Ajout de l'option DNS sur les pools VLAN 10 et VLAN 20

- Tests réalisés sur plusieurs postes → renouvellement OK (ipconfig /renew)

Mise en place du serveur Web en DMZ (VLAN 99) :

- Configuration de l'adresse statique 192.168.99.10
- Installation du service HTTP + création du site web du projet
- Tests d'accès ACL

Mise en place du Syslog :

- Serveur Syslog configuré (192.168.30.20)
- Activation du logging sur routeur + switches
- Génération volontaire d'événements (shutdown interface, VLAN up…)
  → Les logs sont bien reçus et horodatés sur le serveur.

Configuration d'ACL de sécurité :

- Blocage de l'accès au serveur Web depuis les VLAN Users et Servers
- Autorisation uniquement pour le VLAN Admin
  (Test : ping + HTTP) → Fonctionnel.

Configuration du NAT / PAT :

- NAT configuré sur le routeur (Gig0/0/1 en outside)
- Tests non concluants car Packet Tracer ne permet pas la configuration avancée du Cloud → enjeu identifié

3/ Méthodologie et outils utilisés

Comme pour les sprints précédents, nous avons continué à appliquer la démarche Agile.

Nous avons utilisé :

- Trello pour suivre notre avancement (Backlog → Doing → À tester → Done),
- GitHub pour versionner le fichier Packet Tracer ainsi que les captures utilisées pour la documentation,
- Cisco Packet Tracer pour simuler l'ensemble du réseau,
- Google Docs et Agenda pour organiser notre travail et rédiger les comptes rendus.

Au sein du groupe, nous avions un Lead Network, un Scrum Master, et deux membres chargés du support configuration et de la documentation.
Chaque membre a participé activement aux tests et à la validation des configurations.

4/ Livrables produits

À la fin de ce sprint, nous avons obtenu :

- Serveur DNS fonctionnel avec résolution interne
- Serveur Web en DMZ avec page projet opérationnelle
- Serveur Syslog configuré et recevant correctement les logs
- ACL fonctionnelles contrôlant l'accès aux ressources sensibles
- NAT configuré (non validé à cause des limites Packet Tracer)
- Mise à jour GitHub avec documentation, config et captures

5/ Résultats obtenus

À l'issue de ce Sprint, nous avons obtenu un réseau qui fonctionne de manière stable et conforme à nos attentes. Le routage inter-VLAN est opérationnel grâce au Router-on-Stick, ce qui permet la communication entre les différentes zones du réseau. Les VLANs sont propagés correctement sur l'ensemble des switches, et les tests effectués avec les commandes show interfaces trunk et show vlan brief nous ont permis de valider la cohérence de la segmentation réseau.

Les postes utilisateurs situés dans les VLANs Users et Admin reçoivent correctement leurs adresses IP via DHCP, ce qui confirme que les pools et le relay DHCP ont été configurés correctement via ip helper-address. Le DNS interne fonctionne également, notamment avec la résolution locale de web.local, que nous avons vérifiée avec nslookup et ping.
Le serveur web en DMZ est accessible, mais uniquement depuis le VLAN Admin,

conformément aux politiques de sécurité définies. Cette restriction est appliquée via les ACL configurées sur le routeur, ce qui confirme que le contrôle d'accès fonctionne comme prévu. Enfin, la journalisation centralisée est opérationnelle : les logs provenant du routeur et des switches sont bien reçus par le serveur Syslog, ce que nous avons pu confirmer par l'apparition d'événements horodatés à chaque modification ou changement d'état.

Même si le NAT n'a pas pu être testé entièrement en raison de limitations techniques liées à Packet Tracer, sa configuration est en place et documentée pour la suite. Globalement, ce sprint nous permet donc de disposer d'un réseau complet, segmenté, sécurisé et supervisé.

6/ Difficultés rencontrées et solutions

Durant ce sprint, nous avons rencontré plusieurs difficultés qui nous ont obligés à revoir notre approche et à réaliser des tests supplémentaires. La première difficulté concernait la propagation du DNS : dans un premier temps, certains postes ne parvenaient pas à résoudre les noms, car l'option DNS n'avait pas été ajoutée dans les pools DHCP. Une fois cette configuration corrigée, les tests ipconfig /renew ont permis de confirmer que la résolution fonctionnait correctement.

Nous avons également rencontré un problème avec le Syslog, car aucun log ne parvenait au serveur dans les premières tentatives. Après vérification, nous avons constaté que le logging n'avait pas été activé sur tous les équipements, ce que nous avons corrigé avec la commande logging host <ip> puis à l'aide de tests (shutdown/no shutdown d'une interface).

Une autre difficulté concernait la mise en place du NAT. Bien que la configuration soit techniquement correcte, Packet Tracer ne permet pas une configuration avancée du Cloud, ce qui nous empêche de tester la traduction d'adresse. Nous avons donc classé ce point comme enjeu et amélioration future, faute de pouvoir le valider dans cet environnement.

Enfin, la configuration des ACL a nécessité plusieurs ajustements, notamment parce que certains flux essentiels étaient bloqués lors des premiers essais. Après plusieurs tests successifs, nous avons finalement défini des règles cohérentes permettant d'assurer l'isolement de la DMZ tout en maintenant les services internes accessibles au VLAN Admin.