Analyse réflexive – SAE41 : Réalisation d'un réseau sécurisé multi-sites

Introduction

Dans le cadre de la SAE41, il nous a été demandé de concevoir un réseau multi-site sécurisé à l'aide de la plateforme de simulation PnetLab. Ce projet avait pour objectif de reproduire une architecture professionnelle comprenant des VLANs, des équipements de niveau 3, un tunnel IPSec et des règles de sécurité inter-sites. Dès la présentation, cette SAE m'a semblé particulièrement pertinente et stimulante, tant du point de vue technique que pédagogique. Ce retour réflexif retrace les différentes étapes du projet, les compétences mobilisées, les difficultés rencontrées ainsi que les enseignements que j'en ai tirés.

1. Ressenti : entre intérêt technique et surcharge de travail

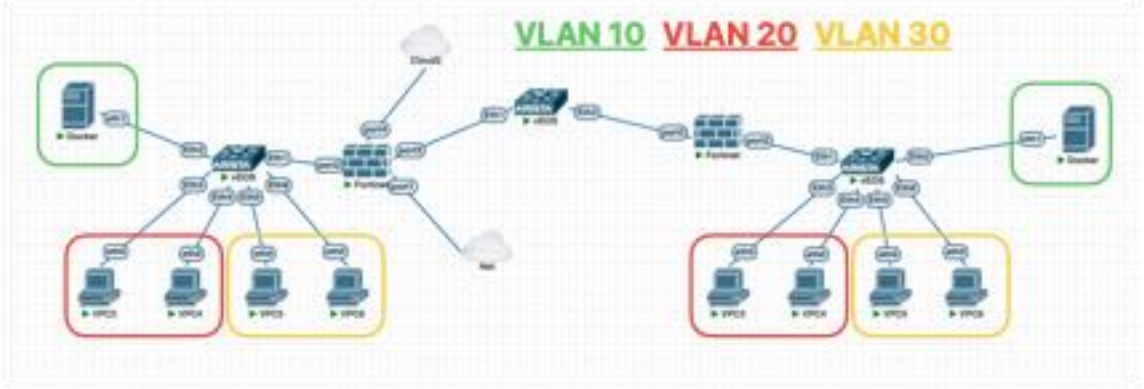
Dès les premières explications du sujet, la SAE m'a semblé très intéressante. Le défi technique qu'elle représentait – créer un réseau sécurisé de bout en bout, réparti sur plusieurs sites – m'a immédiatement motivé. Avec le recul, je considère cette SAE comme extrêmement formatrice. Elle m'a permis de consolider mes compétences en réseaux, d'en acquérir de nouvelles (notamment en sécurité), mais aussi de développer mon autonomie dans la gestion d'un projet technique d'envergure.

2. Analyse du travail mené

Le cœur du projet reposait sur la mise en œuvre d'un réseau multi-site composé de deux infrastructures indépendantes, interconnectées via un tunnel IPSec sécurisé. Chaque site intégrait plusieurs VLANs, avec des règles de filtrage strictes entre eux afin d'assurer une isolation réseau conforme à un environnement professionnel.

Pour construire cette architecture, j'ai dû configurer des équipements ARISTA de niveau 3 (routeurs/switchs) et des firewalls FortiGate. Je n'avais jamais eu l'occasion de configurer un firewall auparavant : j'ai donc dû apprendre en autodidacte à utiliser les FortiGate, d'abord via leur interface graphique, puis, à la suite de déconnexions fréquentes, directement en CLI (ligne de commande). Cette contrainte technique s'est transformée en opportunité d'apprentissage.

L'image illustre les deux sites interconnectés, la segmentation en VLANs (10, 20 et 30), et le tunnel IPSec mis en œuvre pour sécuriser les échanges entre sites.



3. Évaluation : attentes et risques

Aucune grille d'autoévaluation ne nous a été proposée. En me basant sur les critères du cahier des charges et la qualité de l'architecture que j'ai mise en place, j'estime que ce travail mérite une note entre 18 et 19/20. J'ai pris en charge l'intégralité de la configuration du réseau, ainsi que la création du diaporama de présentation.

Cependant, un décalage entre la note espérée et la note finale peut subsister. Cette incertitude s'explique notamment par certaines imprécisions techniques dans le compte rendu final, malgré une relecture approfondie. Ces éléments reflètent une légère défaillance dans l'organisation collective, notamment sur la qualité des livrables et la coordination à l'oral.

4. Bilan et perspectives

Cette SAE a mis en lumière l'importance d'une bonne dynamique de groupe pour garantir la qualité de tous les livrables. Si la configuration technique a été menée de manière fluide, une meilleure coordination dans la rédaction et la restitution aurait permis d'optimiser le résultat final. Pour les projets futurs, je veillerai à renforcer cet aspect collaboratif dès le départ afin de limiter les défaillances organisationnelles.

Sur le plan technique, j'ai acquis des compétences concrètes en sécurisation réseau, en gestion de VLANs, en configuration d'IPSec et en utilisation de firewalls professionnels. Cette SAE m'a préparé à des cas réels que je suis susceptible de rencontrer dans ma carrière, notamment en cybersécurité ou en ingénierie réseau.