

UE Cybersecurité

Cahier des charges du projet

1. Contexte et définition du projet

Le projet consiste à déployer plusieurs réseaux locaux symbolisant des sites et des agences interconnectés par un WAN. Cet interréseau doit être mis en place pour permettre la réalisation des travaux pratiques des cours du bloc 3. Les réseaux doivent être déployés dans les locaux 2/13 et 2/16. Les réseaux doivent pouvoir accéder à Internet via le LAN du département DST. Des UTM Fortigate doivent être déployés pour assurer la sécurité périmétrique de chaque LAN.

Le projet sera commencé au bloc 2 et se terminera l'année suivante en bloc 3.

2. Objectifs du projet

Objectifs généraux du bloc 2 :

- a) Déployer un interréseau (LAN et WAN) dans les locaux 2/13 et 2/16 afin de disposer d'un réseau pour les travaux pratiques des cours du bloc 3.
- b) Sécuriser les LAN en déployant des UTM Fortigate périmétriques.
- c) Chaque LAN inclura un serveur (par exemple un serveur Web) accessible de l'extérieur du site/agence.
- d) Interconnecter les sites et les agences à l'aide de deux WAN (à créer). Ces WAN seront simulés à l'aide de routeurs et commutateurs et les adresses 192.168.0.0/16 seront assimilées à adresses IP publiques le temps du projet.
- e) Déployer des connexions VPN entre les agences et les sites centraux afin de permettre aux serveurs Active Directory de communiquer de manière sécurisée (réplication).
- f) Améliorer la sécurité du réseau en durcissant la configuration des périphériques réseaux selon les fonctionnalités disponibles sur le matériel.
- g) Mettre en œuvre un programme de gestion des vulnérabilités.
- h) Respecter les guides et règles de bonnes pratiques.
- i) Rédiger la documentation.

Objectifs généraux du bloc 3

- a) Améliorer la sécurité des LAN en déployant les fonctionnalités des UTM Fortigate étudiées durant le bloc 3.
- b) Améliorer la sécurité des applications en mettant en œuvre une architecture zero trust.
- c) Améliorer le routage du trafic en routant sur base des applications et de la qualité des liens plutôt que sur base des adresses de destination.
- d) Mise en œuvre d'un monitoring du réseau.

- e) Réaliser un test d'intrusion de son site/agence ou de celui d'un autre groupe (avec leur accord).
- f) Respecter les guides et règles de bonnes pratiques.
- g) Rédiger la documentation.

Hormis quelques tâches indispensables, les éventuelles tâches non réalisées lors du bloc 2 ne seront pas continuées lors du bloc 3.

3. Description fonctionnelle des besoins

Les étudiants devront proposer eux-mêmes les fonctionnalités à implémenter sur les équipements afin de mener à bien le projet.