MASTER RÉSEAUX ET TÉLÉCOMMUNICATIONS

## PARCOURS TÉLÉCOMMUNICATIONS, RÉSEAUX ET CYBERSÉCURITÉ

**Semestre 7**

# Cyber-protection des systèmes d'information

## Présentation

**6 crédits ECTS**

Volume horaire

Cours Magistral : 16h
Travaux Dirigés : 16h
Travaux Pratiques : 20h

La cyber-protection nécessite en la conception d'une architecture réseau sécurisée. C'est la première barrière de défense d'une entité qui consiste à réduire au maximum sa surface d'attaque. Bien que différentes stratégies de protection existent, la stratégie de défense en profondeur est aujourd'hui la plus pragmatique. Cependant l'application d'une telle stratégie nécessite de connaître quelles contre-mesures peuvent faire face à un ou plusieurs types de menaces, savoir comment les déployer et les configurer et enfin pouvoir être en capacité de les maintenir dans le temps.

Cet enseignement se focalise sur la conception d'une architecture complexe qui repose sur le principe de la défense en profondeur. Deux concepts sont principalement abordés :

> Segmenter le réseau : la segmentation d'un réseau est probablement un des concepts les plus importants pour pouvoir réduire la surface d'attaque. Une méthodologie est présentée afin de pouvoir segmenter de manière optimale un système d'information tout en tenant compte de diverses contraintes opérationnelles et techniques.
> Réaliser la ségrégation entre zones : la ségrégation consiste à fournir des communications sécurisées entre zones segmentées d'un système. Cet enseignement propose des concepts pour sélectionner efficacement les mécanismes de sécurité et garantir leur bonne configuration.

La mise en place de la défense en profondeur est autant recommandée pour les systèmes d'information des technologies de l'information que pour ceux des technologies d'opération. Les spécificités de chacune de ces systèmes sont également abordées et les méthodologies adaptées au contexte d'application.

## Pré-requis nécessaires

Bonne connaissance des réseaux, Bonne connaissance des systèmes d'opération

## Compétences visées

> Pouvoir segmenter un réseau efficacement
> Assurer la ségrégation entre diverses zones d'un système d'information
> Savoir positionner les mécanismes de sécurité aux bons endroits et en minimiser le nombre
> Configurer les équipements de sécurité et les maintenir dans le temps
> Ecrire une politique de sécurité

## Modalités de contrôle des connaissances

### Session 1 ou session unique - Contrôle de connaissances

| Nature de l'enseignement | Modalité | Nature | Durée (min.) | Coefficient | Remarques |
|---|---|---|---|---|---|
| UE | CT | Ecrit - devoir surveillé | 120 | 100% | |

### Session 2 : Contrôle de connaissances

| Nature de l'enseignement | Modalité | Nature | Durée (min.) | Coefficient | Remarques |
|---|---|---|---|---|---|
| UE | CT | Ecrit - devoir surveillé | 120 | 100% | |