8a avenue Maistriau
7000 Mons

www.heh.be

Intitulé de l'UE	**Networks : Connected and secure**
Section(s)	- **(10 ECTS)** Bachelier en Informatique et Systèmes orientation Réseaux et Télécommunications / Cycle 1 Bloc 3 option Sécurité

Responsable(s)	Heures	Période
Denis MANDOUX	95	**Quad 1**

Activités d'apprentissage	Heures	Enseignant(s)
Connecting networks - théorie	30h	**Denis MANDOUX**
Connecting networks - travaux pratiques	40h	**Denis MANDOUX**
Cybersécurité 2	25h	**Denis MANDOUX**

Prérequis	Corequis

Répartition des heures
Connecting networks - théorie : 30h de théorie
Connecting networks - travaux pratiques : 40h d'exercices/laboratoires
Cybersécurité 2 : 20h de théorie, 5h d'exercices/laboratoires

Langue d'enseignement
Connecting networks - théorie : Français, Anglais
Connecting networks - travaux pratiques : Français, Anglais
Cybersécurité 2 : Français, Anglais

Connaissances et compétences préalables

L'UE Cybersécurité 1 est un prérequis.

Il est également fortement conseillé d'avoir réussi les activités d'apprentissage "Télécommunications et réseaux (théorie et travaux pratiques)", "Télécommunications et réseaux avancés (théorie et travaux pratiques)", "Concepts de routage et commutation (théorie et travaux pratiques)".

Objectifs par rapport au référentiel de compétences ARES

Cette UE contribue au développement des compétences suivantes

- Communiquer et informer
  - Choisir et utiliser les moyens d'informations et de communication adaptés

    - Mener une discussion, argumenter et convaincre de manière constructive
    - Utiliser le vocabulaire adéquat
    - Utiliser une langue étrangère
- Collaborer à la conception, à l'amélioration et au développement de projets techniques
    - Elaborer une méthodologie de travail
    - Planifier des activités
    - Analyser une situation donnée sous ses aspects techniques et scientifiques
    - Rechercher et utiliser les ressources adéquates
    - Proposer des solutions qui tiennent compte des contraintes
- S'engager dans une démarche de développement professionnel
    - Développer une pensée critique
    - Travailler tant en autonomie qu'en équipe dans le respect de la structure de l'environnement professionnel
- S'inscrire dans une démarche de respect des réglementations
    - Respecter les normes, les procédures et les codes de bonne pratique
- Collaborer à l'analyse et à la mise en œuvre d'un système informatique
    - Sur base de spécifications issues d'une analyse : (1) développer une solution logicielle ; (2) mettre en œuvre une architecture matérielle
    - Assurer la maintenance, le suivi et l'adaptation des choix technologiques qui ont été implémentés
    - Assurer la sécurité du système
- Intégrer des solutions télécoms sécurisées autour des réseaux locaux en y incluant la qualité de service
    - Mettre en place des solutions sécurisées d'accès aux réseaux (sans fil, ADSL, …)
    - Interconnecter des réseaux de manière sécurisée, en gérant correctement des plans d'adressage et les aspects de sécurité (routage, …)
    - Analyser le comportement d'un réseau en utilisant des outils de supervision et d'audit. mettre en oeuvre des solutions de qualité de service
    - Installer, paramétrer et gérer des solutions de télécommunication incluant les transports des différents flux (voix, données, ..) (téléphonie, VoIP, vidéoconférence, …)

Acquis d'apprentissage spécifiques

A l'issues des activités d'apprentissage, les étudiants seront notamment capable de

- Expliquer le fonctionnement et les avantages des réseaux privés virtuels (VPN) et du tunneling.
- Surveiller les fonctions réseau avec Syslog, SNMP et NetFlow.
- Configurer et dépanner syslog et NTP.
- Configurer et dépanner des connexions série.
- Configurer et dépanner des réseaux et interréseaux
- Configurer et dépanner des VPN.
- Configurer et dépanner la qualité de service dans un réseau.
- Configurer et dépanner différentes fonctions d'un UTM, notamment
    - L'authentification.
    - Les VPN (IPsec, dialup, SSL).
    - La fonction IPS (Intrusion Prevention System).
    - La fonction antivirus.
    - La haute disponibilité.
    - Le filtrage Web.
    - Le Single Sing On.
    - ...
- Communications sans fil (analyse spectrale, modulations, antennes)
- Respecter les méthodologies et règles de bonnes pratiques de l'administrateur réseau et sécurité.
- ...

Contenu de l'AA Connecting networks - théorie

Le contenu de l'activité est principalement basée sur :

- Les connexions séries point à point (protocoles HDLC et PPP).
- La surveillance du réseau (syslog, SNMP, Netflow).
- Configurer et dépanner les connexions série.
- La mise en oeuvre et la sécurisation d'un réseau.
- ...

Contenu de l'AA Connecting networks - travaux pratiques

Projet commun de déploiement et sécurisation d'un réseau mettant en application les notions abordées dans les activités d'apprentissage "télécommunication et réseaux - routing and switching", "Network : Connected and secure" et les AA "Cybersécurité".

Ce projet est la continuité du projet commencé dans l'UE Cybersécurité du bloc 2.

Contenu de l'AA Cybersécurité 2

Ce cours vous apprendra à déployer une solution de sécurité de type UTM/NGFW et à maîtriser les éléments essentiels de sa configuration.

Configurer et dépanner différentes fonctions d'un UTM, notamment :

- L'authentification.
- Les VPN (IPsec, dialup, SSL).
- La fonction IPS (Intrusion Prevention System).
- Le filtrage Web.
- La haute disponibilité.
- La fonction antivirus.
- Le Single Sing On.
- ...

Méthodes d'enseignement

Connecting networks - théorie : cours magistral, approche interactive

Connecting networks - travaux pratiques : travaux de groupes, approche par projets

Cybersécurité 2 : cours magistral, approche interactive

Supports

Connecting networks - théorie : copies des présentations, plateforme elearning

Connecting networks - travaux pratiques : notes d'exercices, protocoles de laboratoires, activités sur eCampus, plateforme elearning

Cybersécurité 2 : copies des présentations, Documentation des éditeurs de solution de sécurité

Ressources bibliographiques de l'AA Connecting networks - théorie

- Support de notes : Mandoux D., *Connecting Networks*, HEH Campus Technique.
- Odom W., *CCNA Routing and Switching 200-125 : Official Cert Guide*, CiscoPress, juillet 2016.
- Santos O. et Stuppi J., *CCNA security 210-260: Official Cert Guide,* CiscoPress, Nov. 2015.
- Hucaby D., *CCNA Wireless 200-355 : Official Cert Guide*, CiscoPress, 2016

Ressources bibliographiques de l'AA Connecting networks - travaux pratiques

- Odom W., *CCNA Routing and Switching 200-125: Official Cert Guide*, CiscoPress, juillet 2016
- Santos O. et Stuppi J., CCNA security 210-260: Official Cert Guide, CiscoPress, Nov. 2015.
- Hucaby D., CCNA Wireless 200-355 : Official Cert Guide, CiscoPress, 2016
- Fortinet, Inc., FortiOS™ Handbook - System Administration VERSION 6.0.6, [En ligne] https://fortinetweb.s3.amazonaws.com /docs.fortinet.com/v2/attachments/4afb0436-a998-11e9-81a4-00505692583a/admin-toc-final.pdf.

Ressources bibliographiques de l'AA Cybersécurité 2

- Support de notes, Mandoux D. *Cybersécurité 2*, HEH Campus Technique.
- Fortinet, Inc., FortiOS™ Handbook - System Administration VERSION 6.0.6, [En ligne] https://fortinetweb.s3.amazonaws.com /docs.fortinet.com/v2/attachments/4afb0436-a998-11e9-81a4-00505692583a/admin-toc-final.pdf.
- O. Santos, J. Stuppi, *CCNA Security 210-260 Official Cert Guide*, Cisco Press, septembre 2015.

Évaluations et pondérations	
Évaluation	Épreuve intégrée
Langue(s) d'évaluation	Français, Anglais
Méthode d'évaluation	Examen théorique (70%) : questionnaire informatisé à compléter sur ordinateur. Evaluation continue (30%) : Evaluation continue pendant les séances de cours et de travaux pratiques de l'UE. Non remédiable en 2e session. Les étudiants n'ayant pas participé au projet ne sont pas autorisé à présenter l'examen théorique.

Année académique : **2021 - 2022**