

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

Responsable(s)	Heures	Période
Denis MANDOUX	94	Quad 1

Activités d'apprentissage	Heures	Enseignant(s)
Connecting networks - théorie	30h	Denis MANDOUX
Connecting networks - travaux pratiques	40h	Denis MANDOUX
Cybersécurité 2	24h	Denis MANDOUX

Prérequis	Corequis

Répartition des heures
Connecting networks - théorie : 30h de théorie
Connecting networks - travaux pratiques : 40h d'exercices/laboratoires
Cybersécurité 2 : 24h de théorie

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
<ul style="list-style-type: none"> • Communiquer et informer <ul style="list-style-type: none"> ◦ Choisir et utiliser les moyens d'informations et de communication adaptés

- Mener une discussion, argumenter et convaincre de manière constructive
- Utiliser le vocabulaire adéquat
- Présenter des prototypes de solution et d'application techniques
- 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, ...)

Objectifs de développement durable



Education de qualité

Objectif 4 Assurer l'accès de tous à une éducation de qualité, sur un pied d'égalité, et promouvoir les possibilités d'apprentissage tout au long de la vie

- 4.3 D'ici à 2030, faire en sorte que les femmes et les hommes aient tous accès dans des conditions d'égalité à un enseignement technique, professionnel ou tertiaire, y compris universitaire, de qualité et d'un coût abordable.
- 4.4 D'ici à 2030, augmenter considérablement le nombre de jeunes et d'adultes disposant des compétences, notamment techniques et professionnelles, nécessaires à l'emploi, à l'obtention d'un travail décent et à l'entrepreneuriat.
- 4.5 D'ici à 2030, éliminer les inégalités entre les sexes dans le domaine de l'éducation et assurer l'égalité d'accès des personnes vulnérables, y compris les personnes handicapées, les autochtones et les enfants en situation vulnérable, à tous les niveaux d'enseignement et de formation professionnelle.



Egalité entre les sexes

Objectif 5 Parvenir à l'égalité des sexes et autonomiser toutes les femmes et les filles

- 5.b Renforcer l'utilisation des technologies clefs, en particulier l'informatique et les communications, pour promouvoir l'autonomisation des femmes.



Travail décent et croissance économique

Objectif 8 Promouvoir une croissance économique soutenue, partagée et durable, le plein emploi productif et un travail décent pour tous

- 8.8 Défendre les droits des travailleurs, promouvoir la sécurité sur le lieu de travail et assurer la protection de tous les travailleurs, y compris les migrants, en particulier les femmes, et ceux qui ont un emploi précaire.

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 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 Single Sing On.
 - ...
- Respecter les méthodologies et règles de bonnes pratiques de l'administrateur réseau et sécurité.
- Connaitre et savoir expliquer les différentes étapes de la méthodologie de pentesting PTES.
- Mettre en oeuvre les différentes étapes de la méthodologie de pentesting PTES en utilisant différents outils.
- ...

Contenu de l'AA Connecting networks - théorie

Le contenu de l'activité est principalement basée sur :

- La mise en oeuvre, la gestion et la sécurisation d'un réseau.
 - AAA (Authentication, Authorization, Accounting)
 - VRF (Virtual Routing and Forwarding)
 - Port mirroring
 - Compléments Wi-Fi
 - ...
- La mise en oeuvre d'un test de pénétration via la méthode PTES.
 - Engagement avec le client, collecte de renseignements, modélisation des menaces, analyse de vulnérabilités, ...
- La surveillance du réseau (syslog, SNMP, Netflow, monitoring).
- ...

Contenu de l'AA Connecting networks - travaux pratiques

Projet commun de déploiement et sécurisation d'un interréseau 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 consistant à mettre en oeuvre un interréseau sur du matériel physique :

- Déploiement d'une infrastructure réseau constituées de sites et agences localisées dans deux classes différentes..
- Sécurisation de l'infrastructure.
- Test de pénétration de l'infrastructure.

Contenu de l'AA Cybersécurité 2

Ce cours est la continuité de l'UE Cybersécurité du bloc 2. 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).
- La haute disponibilité.
- La fonction antivirus.
- Le Single Sing On.
- Le ZTNA (Zero Trust Network Access)
- ...

Méthodes d'enseignement

Connecting networks - théorie : cours magistral, approche interactive
Connecting networks - travaux pratiques : travaux de groupes, approche par projets, approche par situation problème, utilisation de logiciels
Cybersécurité 2 : cours magistral, approche interactive

Supports

Connecting networks - théorie : copies des présentations, activités sur eCampus
Connecting networks - travaux pratiques : Documentation technique relative au matériel et logiciel utilisés
Cybersécurité 2 : copies des présentations, notes d'exercices, activités sur eCampus, FortiGate administration guide

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

Ressources bibliographiques de l'AA Cybersécurité 2

- Support de notes, Mandoux D. *Cybersécurité 2*, HEH Campus Technique.
- Fortinet, Inc., *FortiGate/FortiOS™ 7.2 Administration guide*, [En ligne] <https://docs.fortinet.com/product/fortigate/7.2>.

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 ayant participé à moins de 75% des séances de travaux pratiques ne sont pas autorisé à présenter l'examen théorique.

Année académique : **2024 - 2025**