INFRES_8_2_SR Réseaux informatiques	INFRES	S8

Pourquoi cette UE ?

Ce module permet aux élèves d'acquérir les compétences essentielles pour sécuriser, surveiller et mesurer l'état d'un système d'information. La sécurité réseau leur donne les bases pour protéger les infrastructures. La supervision leur apprend à détecter et anticiper les incidents. La métrologie complète l'ensemble en apportant une vision quantitative pour l'analyse et l'optimisation. Dans une démarche DevOps la fiabilité, la sécurité et la performance des systèmes sont primordiales.

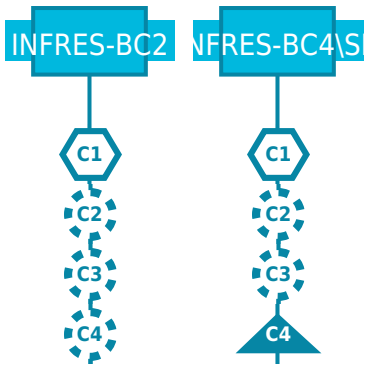
Eléménts constitutifs de l'UE

	coefficient
INFRES_8_2_SR-1 Sécurité des réseaux: outils et équipements dédiés	2
INFRES_8_2_SR-2 Supervision et gestion des réseaux	3

Volume d'heures d'enseignement encadré	Volume d'heures de travail personnel	Nombre d'ECTS
66	22	3

Alignement curriculaire

Parmi les compétences visées par la formation, lesquelles sont développées dans cette UE ?



INFRES_8_2_SR-1 Sécurité des réseaux: outils et équipements dédiés

S8

Contexte et enjeux de l'enseignement

Dans un contexte de multiplication des cybermenaces, les entreprises doivent garantir la sécurité de leurs systèmes d'information. Les pare-feux jouent un rôle central dans cette protection, en assurant un contrôle rigoureux des flux réseau. Le pare-feu Stormshield, certifié par l'ANSSI, est largement utilisé dans les infrastructures sensibles. La maîtrise de son administration est donc un atout stratégique pour les ingénieurs en cybersécurité. Cet enseignement prépare les élèves à configurer, déployer et maintenir ces équipements dans des environnements professionnels exigeants. Il vise également à les amener au niveau requis pour passer la certification CSNA (Certified Stormshield Network Administrator), reconnue dans le secteur.

Prise en compte des dimensions socio-environnementales

Prérequis

Sécurité réseau Cryptographie

Modalités d'enseignement et d'évaluation

	Nb d'heures
Cours	
Cours intégré (cours + TD)	21
TD	
TP	
Projets	
Travail en autonomie encadré	
Contrôles et soutenances	3
Travail personnel	10

Objectifs pédagogiques

(à la fin de cet enseignement, l'étudiant sera capable de ...)

- Déployer un pare-feu Stormshield dans une architecture réseau.
- Configurer les règles de filtrage et les objets de sécurité.
- Gérer les services de journalisation, d'authentification et de VPN.
- Diagnostiquer et résoudre des incidents liés au pare-feu.
- Se préparer efficacement à la certification CSNA.

Activités

(CM, TD, TP, projet, sortie terrain, etc.)

Cours
TP avec des machines virtuelles Stormshield

Évaluations et retours faits aux élèves

(évaluations qui comptent pour la note ou qui permettent à l'étudiant de se situer, corrigés, feedback personnalisé...)

Certification CSNA (QCM)

INFRES_8_2_SR Réseaux informatiques	INFRES
INFRES_8_2_SR-1 Sécurité des réseaux: outils et équipements dédiés	**S8**

Plan de cours

- Introduction à la sécurité réseau et aux pare-feux
Présentation des enjeux de la sécurité périmétrique, typologies d’attaques, rôle des pare-feux dans une architecture réseau, spécificités des solutions Stormshield.
- Installation et prise en main du pare-feu Stormshield
Démarrage initial, interfaces Web et CLI, paramétrage réseau, mise à jour du firmware, configuration de base.
- Filtrage, objets et politiques de sécurité
Création et gestion des objets, configuration des règles de filtrage, inspection des protocoles, gestion des services et des plages d’adresses.
- Fonctionnalités avancées et supervision
VPN site-à-site et mobile, authentification des utilisateurs, journalisation, alertes, supervision en temps réel, outils de diagnostic.
- Mise en pratique et préparation à la certification CSNA
Études de cas, résolution de scénarios techniques, configuration d’un pare-feu en conditions réalistes, conseils pour l'examen CSNA.

Ressources et références

Accès à la plateforme Stormshield

INFRES_8_2_SR Réseaux informatiques	INFRES
INFRES_8_2_SR-2 Supervision et gestion des réseaux	**S8**

Contexte et enjeux de l'enseignement

La supervision et la gestion des réseaux, couplées à la métrologie, jouent un rôle crucial dans l’assurance de performance, de sécurité et de disponibilité des infrastructures numériques. Avec l’augmentation des flux, la diversité des protocoles et la criticité des services, les réseaux doivent être surveillés en temps réel pour anticiper les défaillances, optimiser les ressources et garantir les niveaux de service. La métrologie permet, quant à elle, une mesure fine et continue du comportement du réseau, indispensable à l’analyse de performances, à la détection d’anomalies et à l’aide à la décision. Cet enseignement permet à l’élève de comprendre les mécanismes, outils et pratiques actuels de la supervision, dans un contexte d’évolution vers les réseaux programmables, virtualisés et orientés services.

Prise en compte des dimensions socio-environnementales

Prérequis

Administration des services réseaux Réseaux et Protocoles de communication

Modalités d'enseignement et d'évaluation

	Nb d'heures
Cours	
Cours intégré (cours + TD)	35
TD	
TP	
Projets	7
Travail en autonomie encadré	
Contrôles et soutenances	
Travail personnel	12

Objectifs pédagogiques

(à la fin de cet enseignement, l'étudiant sera capable de ...)

- Mettre en œuvre une solution de supervision réseau.
- Interpréter des métriques issues d’un système de métrologie.-
- Détecter et diagnostiquer des anomalies sur un réseau IP.
- Concevoir un plan de supervision adapté à une architecture.
- Utiliser des protocoles standards de supervision et de collecte de données.

Activités

(CM, TD, TP, projet, sortie terrain, etc.)

Cours
TP

Évaluations et retours faits aux élèves

(évaluations qui comptent pour la note ou qui permettent à l'étudiant de se situer, corrigés, feedback personnalisé...)

Projet en binôme, et contrôle
Copies corrigés et consultables sur demande

INFRES_8_2_SR Réseaux informatiques	INFRES
INFRES_8_2_SR-2 Supervision et gestion des réseaux	**S8**

Plan de cours

- Introduction à la supervision et à la métrologie réseau : définitions, enjeux, panorama des besoins en supervision dans différents contextes (entreprise, opérateur, cloud).
- Protocoles et standards de supervision : SNMP, NetFlow/sFlow/IPFIX, ICMP, syslog, ainsi que les principes d'interrogation active et passive.
- Architecture des systèmes de supervision : agents, collecteurs, bases de données temporelles, interfaces de visualisation, corrélation d'événements.
- Outils et pratiques de supervision : mise en œuvre de solutions open-source (ex. : Zabbix, Prometheus, Grafana, Wireshark), étude de cas et travaux dirigés.
- Analyse de trafic et métrologie avancée : traitement de données de supervision, détection d'anomalies, métrologie appliquée à la sécurité et à l'optimisation du réseau.

Ressources et références

Les supports pédagogiques sont disponibles en ligne sous Campus.