MINISTERE DE LA COMMUNAUTE FRANCAISE

ADMINISTRATION GENERALE DE L'ENSEIGNEMENT ET DE LA RECHERCHE SCIENTIFIQUE

ENSEIGNEMENT DE PROMOTION SOCIALE DE REGIME 1

DOSSIER PEDAGOGIQUE

UNITE DE FORMATION

SECURITE DES RESEAUX

ENSEIGNEMENT SUPERIEUR TECHNIQUE DE TYPE COURT

CODE : 2983 20 U 31 D1
CODE DU DOMAINE DE FORMATION : 206
DOCUMENT DE REFERENCE INTER-RESEAUX

Approbation du Gouvernement de la Communauté française du 30 juin 2009,
sur avis conforme de la Commission de concertation

SECURITE DES RESEAUX

ENSEIGNEMENT SUPERIEUR TECHNIQUE DE TYPE COURT

1. FINALITES DE L'UNITE DE FORMATION

1.1. Finalités générales

Dans le respect de l'article 7 du décret de la Communauté française du 16 avril 1991 organisant l'enseignement de promotion sociale, cette unité doit :

- concourir à l'épanouissement individuel en promouvant une meilleure insertion professionnelle, sociale, culturelle et scolaire ;
- répondre aux besoins et demandes en formation émanant des entreprises, des administrations, de l'enseignement et, d'une manière générale, des milieux socio-économiques et culturels.

1.2. Finalités particulières

L'unité de formation vise à permettre à l'étudiant :

- d'utiliser et de maîtriser les concepts de base de sécurité des réseaux en vue de collaborer efficacement à la maintenance des réseaux informatiques ;
- de maîtriser les concepts d'authentification, d'autorisation et de comptabilisation des accès (AAA) ;
- de protéger un réseau des intrusions malveillantes ;
- de découvrir les grands principes des réseaux privés virtuels ;
- de recourir à la théorie des tunnels IPsec et des techniques de cryptage des données pour sécuriser des échanges de données ;
- de procéder au dépannage d'un réseau privé virtuel ;
- de développer des compétences personnelles d'autoformation dans le domaine informatique et des réseaux privés virtuels ;
- de préparer à une certification en sécurité.

2. CAPACITES PREALABLES REQUISES

2.1. Capacités

En disposant du matériel informatique nécessaire (routeurs, switches, câbles informatiques,...), de la documentation requise et d'une station informatique opérationnelle connectée à Internet,

- configurer un inter-réseau en implémentant PPP, Frame Relay et les listes de contrôle d'accès (ACL) ;
- gérer et contrôler le trafic entre réseaux ;
- remédier à un dysfonctionnement provoqué ;
- résoudre via un laboratoire, une étude de cas pratique consignée dans un cahier des charges.

2.2. Titre pouvant en tenir lieu

Attestation de réussite de l'unité de formation « TECHNOLOGIES WAN » code N°: 2983 13 U31 D1 classée dans l'enseignement technique supérieur de type court.

3. HORAIRE MINIMUM DE L'UNITE DE FORMATION

3.1. Dénomination du cours	Classement	Code U	Nombre de périodes
Laboratoire de maintenance informatique : sécurité des réseaux	CT	S	96
3.2. Part d'autonomie		P	24
Total des périodes			**120**

4. PROGRAMME

L'étudiant sera capable :

en disposant du matériel et du logiciel informatiques nécessaires (routeur et switches, firewall, serveur d'authentification,...), de la documentation requise et de stations informatiques opérationnelles connectées à Internet,

- de décrire et de caractériser les menaces de sécurité des infrastructures réseau en développant les notions suivantes :
  - la détection des attaques dès qu'elles surviennent,
  - l'utilisation d'outils permettant de réaliser un audit de sécurité ;
- de sécuriser les périphériques d'accès réseau en développant les notions suivantes :
  - la sécurisation des accès administratifs (console, telnet, ssh,...) aux routeurs et switches,
  - la création et l'encryption des mots de passe,
  - la gestion des utilisateurs et des privilèges,
  - la création de bannières d'accueil,
  - la collecte, l'enregistrement et l'audit d'activité (syslog, ...) ;
- d'implémenter AAA sur les périphériques réseau en développant les notions suivantes :
  - la configuration de l'authentification locale (par le routeur),
  - la configuration d'une gestion centralisée des authentifications, des autorisations et des comptes sur un serveur RADIUS ;
- de limiter les menaces réseau à l'aide d'ACL (Access Control Lists) en développant les notions suivantes :

- la définition et l'utilisation des ACL basées sur le contexte (CBAC),
- la configuration par zones des politiques et des règles sur le firewall ;

- de mettre en œuvre une gestion sécurisée du réseau ;
- de sécuriser les switches (couche 2) en développant les notions suivantes :
  - la configuration du mode des ports (trunk, access,...),
  - le contrôle de la diffusion des broadcast,
  - les options de sécurité des ports,
  - l'activation et la désactivation de ports,
  - l'utilisation d'outils d'analyse de l'activité et de trafic sur un switch ;
- de mettre en œuvre et de configurer un système de prévention d'intrusions (IPS) ;
- de définir et de caractériser les méthodes de cryptologie en développant les notions suivantes :
  - le codage par substitution (codage de Vigenère,...),
  - la stéganographie,
  - les méthodes et protocoles d'encryption modernes (ESP, AH, IKE, DES, 3DES, IPSEC,...) ;
- d'installer et de configurer un VPN IPSec de site à site en développant les notions suivantes :
  - les types de VPN et leurs caractéristiques,
  - la configuration du client et du serveur,
  - les tests de fonctionnalité ;
- de définir, de caractériser et d'appliquer des politiques de sécurité en développant les notions suivantes :
  - l'activation et la désactivation des services des périphériques,
  - la gestion des images des systèmes d'exploitation des périphériques du réseau,
  - la prévention des attaques.

5. CAPACITES TERMINALES

Pour atteindre le seuil de réussite, l'étudiant sera capable :

en disposant du matériel et du logiciel informatiques nécessaires (routeur et switches, firewall, serveur d'authentification,...), de la documentation requise et de stations informatiques opérationnelles connectées à Internet,

- de décrire des méthodes de sécurisation d'un échange de données au travers d'un inter réseaux ;
- de configurer un VPN de site à site ;
- de remédier à un dysfonctionnement provoqué.

Pour la détermination du degré de maîtrise, il sera tenu compte des critères suivants :

- l'exhaustivité des informations fournies,
- la méthodologie mise en œuvre pour répondre à un dysfonctionnement provoqué,
- la pertinence de l'interprétation des différentes démarches et des résultats,
- les degrés d'autonomie et d'autoformation atteints.

6. CHARGE DE COURS

Le chargé de cours sera un enseignant ou un expert.

L'expert justifiera de compétences particulières issues d'une expérience professionnelle actualisée en relation avec le programme du cours concerné.

7. CONSTITUTION DES GROUPES OU REGROUPEMENT

Il est recommandé de ne pas dépasser plus d'un étudiant par poste de travail.