Ministère de la Communauté française

Administration générale de
l'Enseignement et de la Recherche
scientifique.

Direction générale de l'Enseignement
non obligatoire et de la Recherche
scientifique.

Service de l'enseignement
de promotion sociale.

1080 Bruxelles , le 20 Avr 2005
Rue de Lavallée, 1
02 / 690.87.31

Monsieur Jacques LEFERE
Administrateur délégué
CPEONS

rue des Minimes 87-89
1000 BRUXELLES

Ref.: CC / Document de référence définitif

Objet : Document de référence définitif - Régime 1
----- Unité de formation : SECURITE DES RESEAUX PAR FIREWALL HARDWARE
Classement : ENSEIGNEMENT SUPERIEUR TECHNIQUE DE PROMOTION SOCIALE DE TYPE COURT
Code Référence : 298304U31D1
Domaine : 206 Industrie-SU:électricité,ferronnerie,électronique...

Monsieur l'Administrateur délégué,

J'ai l'honneur de vous faire parvenir le document de référence relatif à l'unité de formation mentionnée sous rubrique, approuvé par le Gouvernement de la Communauté française le 11 Avril 2005 .

Veuillez agréer, Monsieur l'Administrateur délégué, l'assurance de ma considération distinguée.

P.O. La Directrice générale a.i.,

Chantal Kaufmann

Denis VAN LERBERGHE
Directeur

Toute demande de renseignements relative à l'objet de la présente peut être obtenue auprès de
Stéphane Abrassart ou Carine Cacheux (02/690.87.11 ou 02/690.87.10)

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 PAR FIREWALL HARDWARE

ENSEIGNEMENT SUPERIEUR TECHNIQUE DE TYPE COURT

CODE : 29 83 04 U31 D1
CODE DU DOMAINE DE FORMATION : 206
DOCUMENT DE REFERENCE INTER-RESEAUX

Approbation du Gouvernement de la Communauté française du 11/04/2005 ,
sur avis conforme de la Commission de concertation

SECURITE DES RESEAUX PAR FIREWALL HARDWARE

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 découvrir les grands principes des réseaux virtuels privés ;
- de recourir à la théorie des tunnels IPsec et des techniques de cryptage des données pour créer un réseau informatique ;
- de procéder au dépannage d'un réseau virtuel privé de manière analytique ;
- 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,

- décrire les modèles OSI et TCP-IP :
  - associer la fonction des hub, switch et routeur aux couches du modèle OSI ;
  - décrire la structure d'une trame Ethernet ;
  - décrire le principe de l'encapsulation des données ;

- citer les caractéristiques de différents médias utilisés sur un réseau local et comparer ces medias ;
- citer et caractériser le matériel qui constitue le réseau (interface réseau, hub, switch, routeur, ...) ;
- décrire la fonction du protocole ARP et utiliser la commande arp ;
- décrire le principe et le fonctionnement du CSMA-CD ;

- décrire l'adressage de réseaux :
  - décrire la structure de l'adressage IP (classes, masques, sous-réseaux) ;
  - décrire et illustrer le VLSM ;

- décrire et configurer un réseau local commuté :
  - citer les caractéristiques de différents médias utilisés sur un réseau local et comparer ces medias ;
  - citer et caractériser le matériel qui constitue le réseau (interface réseau, hub, switch, routeur, ...) ;
  - décrire la fonction du protocole ARP et utiliser la commande arp ;
  - décrire le principe et le fonctionnement du CSMA-CD ;
  - configurer un réseau local sous IP (adresse, masque, passerelle) ;
  - décrire le fonctionnement des switches (commutateurs) ;
  - définir, décrire et configurer des VLANs ;
  - définir, décrire et configurer le routage inter-VLANs ;

- configurer un inter-réseau :
  - interconnecter un minimum de trois réseaux IP à l'aide de routeurs,

- décrire et configurer le routage :
  - caractériser et configurer des protocoles de routage à vecteur de distance et à états de liens ;

- contrôler le trafic réseau :
  - décrire et configurer des listes de contrôle d'accès basées sur l'adresse IP source, l'adresse IP du destinataire et le service utilisé ;
  - contrôler la diffusion de mises à jour de routage sur une interface (désactivation).

2.2. Titre pouvant en tenir lieu

Attestation de réussite de l'unité de formation « SWITCHING, ROUTAGE et TECHNOLOGIES WANs » CODE N°: 29 83 02 U31 D2 classée dans l'enseignement technique supérieur de type court, **ou** être en possession d'une certification Cisco CCNA.

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 par firewall hardware	CT	S	64
3.2. Part d'autonomie		P	16
Total des périodes			**80**

4. PROGRAMME

L'étudiant sera capable :

en disposant du matériel informatique nécessaire (firewall hardware, matériel de sécurité, ...), de la documentation requise et d'une station informatique opérationnelle connectée à Internet, par l'intermédiaire de travaux pratiques,

- de caractériser et de mettre en oeuvre la sécurité des réseaux utilisant du matériel hardware en développant les notions suivantes :
  - les firewalls et leurs technologies, la sécurité, les labels de certification VPN et firewall, le marché actuel,
  - le matériel de sécurité : introduction au matériel de sécurité, spécificités de l'operating system, algorithme de sécurité adaptatif, fonctionnement en proxy Cut-through, failover, translation d'adresses réseaux (NAT), familles de matériels de sécurité, services firewall, types de licences et possibilités VPN,
  - l'environnement de démarrage : interface utilisateur, commandes de base de configuration du matériel de sécurité, examen des statuts du matériel de sécurité,
  - le routage et la configuration multicast : routes statiques et dynamiques, routage multicast, permission des hôtes pour recevoir des transmissions multicast, transfert multicast à partir d'une source de transmission, debuggage SMR (Sub Multicast Routing),
  - DHCP (Dynamic Host Configuration Protocol) pour matériel de sécurité : serveur et client, DHCP serveur, configuration d'un matériel de sécurité comme DHCP serveur ;
- d'utiliser les concepts de base de la translation des services (PAT et NAT) du matériel de sécurité et leurs connexions en développant les notions suivantes :
  - les protocoles de transport : sessions dans l'environnement IP, révision détaillée de TCP, caractéristiques de TCP et UPD et interaction avec le matériel de sécurité,
  - la translation d'adresses réseaux (NAT) : compréhension de NAT, traductions statiques et dynamiques internes, traductions statiques et dynamiques externes, identification NAT,
  - la configuration du support DNS : vue d'ensemble et commande « alias », procédé de dépannage DNS, destination translatée avec la commande « alias », traduction et relais provenant de serveurs DNS,
  - les connections : contrôle du trafic entrant et sortant (validité des requêtes des utilisateurs qui traversent le matériel de sécurité, contrôle du flux entre 2 interfaces « conduit »,...),
  - la translation d'adresses et de ports (PAT) : translation d'adresses et de ports relative au matériel de sécurité, utilisant les adresses extérieures d'interface, mapping des adresses internes de sous-réseaux en adresses externes, effets de l'utilisation de multiples adresses externes, augmentation du pool d'adresses translatées par l'utilisation de PAT, redirection de ports,

- les interfaces multiples du matériel de sécurité : support et configuration d'interfaces additionnelles (3 ou 4 interfaces) ;

- d'élaborer les listes d'accès (ACLs) en développant les notions suivantes :
  - Les ACLs dans le matériel de sécurité : ACLs, configuration des ACLs, ACLs turbo, utilisation des ACLs comparée au contrôle du flux entre 2 interfaces (« conduit »), vérification et dépannage des ACLs,
  - l'utilisation des ACLs : blocage des accès web, filtrage d'applets malveillantes et d'URLs, permission des accès web vers la DMZ, contrôle de paquets ICMP (PING),
  - les groupes d'objets : groupement d'objets (hôtes ou services) de types similaires, utilisation et configuration des groupes dans les ACLs, vérification et suppression,
  - l'imbrication des groupes d'objets : configuration et utilisation des groupes imbriqués au sein d'une liste d'accès ;

- de maîtriser et d'utiliser les concepts de « Authorization », « Authentication » et « Accounting » (AAA) dans le matériel de sécurité en développant les notions suivantes :
  - AAA : définition des concepts d'authentification, d'autorisation et de compte d'accès, fonctionnement en proxy Cut-through, TACACS+ et RADIUS, interaction entre des programmes d'administration (ex : CISCO secure ACS) et firewall hardware ;
  - la configuration de l'« authentication » : configuration du matériel de sécurité pour supporter l'« authentication », « authentication » de services autres que Telnet (FTP, HTTP de manière directe ou par Telnet virtuel), authentification par l'accès console, modification des paramètres d'authentification (timeout, invite d'authentification, ...),
  - la configuration de l' «Authorization» et l'«Accounting» : configuration du matériel de sécurité, usage et définition des ACLs téléchargeables, définition des comptes, gestion du trafic, surveillance de la configuration AAA,
  - PPPoE (Point to Point Protocol over Ethernet) et le matériel de sécurité : description et configuration du support de PPPoE, surveillance et dépannage d'un client PPPoE ;

- de définir la détection d'intrusions sur les protocoles « avancés » en développant les notions suivantes :
  - la modification des paramètres (numéro de port, nom, ...) des principaux services tels que FTP, HTTP, SCCP (Skinny Client Control Protocol), SIP (Session Initiation Protocol), RSh (Remote Shell), ...,
  - les problèmes liés au support multimédia, le protocole RTSP (Real Time Streaming Protocol), le standard H.323, les télécommunications IP et le serveur DHCP pour le matériel de sécurité,
  - les attaques massives AAA et SYN, l'interception TCP, la surveillance des attaques de DNS ou par mails, l'utilisation d'outils tels que FragGuard et Virtual Reassembly ou la commande floodguard,
  - la détection d'intrusions : information et la signature des attaques, configuration de la détection d'intrusions sur un firewall,
  - le shunning : blocage d'un interface en cas d'attaque,
  - la configuration et l'utilisation d'un serveur SYSLOG, l'interprétation des messages SYSLOG,
  - la description et la configuration de SNMP (Simple Network Management Protocol) avec support des MIB (Management Information Base) ;

- de mettre en œuvre des concepts de base permettant d'assurer la sécurité du réseau suite à une intrusion ou à un problème technique en appliquant les notions suivantes :

- la description et la mise en place de solutions « failover » (gestion des incidents) : redondance en cas de panne, redéfinition d'adresses IP, réplication des configurations, ... sur un LAN ou sur un WAN (au moyen de câbles série),
- l'utilisation de commandes additionnelles permettant la création d'adresses MAC virtuelles, la réplication d'adresses HTTP, et la réinitialisation du firewall,
- le test de validation du « failover »,
- la télé-maintenance : configuration TELNET pour accéder à la console du matériel de sécurité, connections SSH (Secure SHell), configuration du client et du serveur, définition des commandes utilisables à distance,
- la récupération du mot de passe du firewall (password recovery),
- la mise à jour du système d'exploitation du firewall et de la clé d'activation ;

- de configurer un VPN (Virtual Private Network) sur un firewall hardware en appliquant les notions suivantes :
  - le matériel de sécurité et la sécurité VPN : fonctions et topologies du VPN sur le matériel de sécurité, caractéristiques IPsec (IP Security Protocol), standards IPsec supportés par le matériel de sécurité,
  - la configuration d'un VPN : détermination des règles IKE, des méthodes de distribution et d'identification, configuration des paramètres IKE et IPsec, tests et vérifications (IKE, IPsec, crypto map, ACL et trafic échangé, ...), suppression des IPsec et IKE,
  - le client VPN : caractéristiques, assignation d'une adresse IP au client VPN par le firewall, configuration du matériel de sécurité et du client pour réaliser un tunnel VPN,
  - les certifications externes : requêtes des clients et du firewall vers les serveurs d'organismes de certification (Certification Authority, CA) ;

- d'assurer la gestion du matériel de sécurité en appliquant les notions suivantes :
  - les politiques générales de sécurité (règlements d'ordre intérieur, ...), le gestionnaire du matériel de sécurité,
  - la mise en œuvre, la configuration des firewalls (règles d'accès, de translation, VPN, la surveillance, ...) à l'aide d'un gestionnaire du matériel de sécurité,
  - l'utilisation d'un gestionnaire de matériel de sécurité pour créer :
    - des VPNs site à site : configuration IKE, support de certifications externes, transform sets, crypto map, lrègles IPsec,
    - un accès à distance par VPN : matériel à mettre en œuvre, clients et serveur sur divers environnements ;
  - la gestion du matériel de sécurité en entreprise : gestion centralisée des firewalls, concepts clés, serveurs de mises à jour automatiques.

5. CAPACITES TERMINALES

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

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

- de démontrer la compréhension des concepts et notions développés dans le cadre de cette unité de formation en répondant à un questionnaire ;

- de résoudre via un laboratoire, une étude de design composé d'un site primaire et d'un site secondaire sans ramification comprenant au moins :
  - la configuration des composants informatiques,
  - la mise en place d'un firewall hardware entre deux sites distants à l'aide d'un tunnel VPN ;
- de remédier à un dysfonctionnement provoqué.

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

- l'exhaustivité des informations contenues dans l'étude du design,
- 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,
- l'utilisation judicieuse du vocabulaire informatique.

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.