



TERMES DE RÉFÉRENCE

AXE :FORMATION EN SECURITE RESEAUX

(Préparation à la certification Cisco CCNA Sécurité)

« Action dans le cadre du développement et de la mise en place d'une plateforme collaborative au sein de la DGET »

I/CONTEXTE ET JUSTIFICATION

Dans le cadre du second Projet d'Appui à la Réforme de l'Enseignement Supérieur (PARES II), financé en partie par l'accord de prêt n° 7392-TN conclu entre la Banque Internationale pour la Reconstruction et le Développement (BIRD) et le Ministère de l'Enseignement Supérieur et de la Recherche Scientifique (MESRS) et en particulier dans sa composante 3 (Fonds compétitif pour l'amélioration de la Qualité, Programme d'Appui à la Qualité, PAQ), la Direction Générale des Etudes Technologiques (DGET) a bénéficié d'une allocation pour la mise en œuvre de son projet de mise en place d'un système d'information (PAQ2009-CG) intitulé "**Développement et mise en place d'une plateforme collaborative**".

Une des actions à entreprendre dans le cadre de ce projet est la formation des ressources humaines de la DGET et des enseignants des Instituts Supérieurs des Etudes technologiques (ISETs) sur entre autres le thème « sécurité réseaux ».

Cette formation permettra aux bénéficiaires de développer leurs compétences opérationnelles et managériales et contribuera à améliorer la qualité de la gestion courante et le pilotage du projet de « **la mise en place de plateforme collaborative au sein de la DGET** ».

II/ OBJECTIFS GENERAUX

L'action projetée a pour objectif de développer la capacité de la DGET en matière de sécurité réseaux ce qui permettra aux participants d'acquérir les connaissances et les compétences nécessaires pour concevoir, mettre en œuvre et assurer la surveillance d'une politique de sécurité en utilisant les fonctionnalités de sécurité Cisco IOS et diverses autres technologies. Cette formation couvre les contrôles de sécurité des équipements Cisco IOS ainsi que l'introduction à

l'équipement de sécurité Cisco ASA.Elle fournit aux participants les connaissances et les compétences nécessaires pour améliorer les tâches basiques de sécurisation d'un petit réseau branch office en utilisant les fonctionnalités de sécurité Cisco IOS disponibles au travers des GUIs (Cisco Configuration Professional) et CLI sur les routeurs Cisco, les switches et les équipements ASA.

III/ RESULTATS ESCOPMTES

A l'issue cette session de formation, les participants seront capables de :

- Décrire les composants des stratégies de sécurité des réseaux qui peuvent être utilisés pour contrer les menaces contre les systèmes IT, dans un contexte de continuité de services.
- Développer et mettre en œuvre les mesures sécuritaires qui permettent de protéger les éléments du réseau et de l'infrastructure.
- Déployer et maintenir les contrôles de menaces et les technologies de limitation et détection des menaces pour le périmètre de sécurité dans les réseaux de petite et de moyenne envergure.

IV/ PROGRAMME DE FORMATION ET APPROCHE METHODOLOGIQUE

Pour atteindre ces résultats, la formation se déroulera sous forme d'ateliers autour des thèmes suivants sans toutefois suivre forcément le plan suggéré ci-dessous :

- 1. Les menaces de sécurité sur les réseaux modernes de données : Modern Network Security Threats**
Objectifs : Expliquer les menaces réseau, les techniques d'atténuation, et les bases de la sécurisation d'un réseau.
- 2. Sécurisation des routeurs Cisco : Securing Network Devices**
Objectifs : sécuriser l'accès administratif sur les routeurs Cisco.
- 3. Présentation et configuration d'AAA : Authentication, Authorization and Accounting**
Objectifs : Accès administratif sécurisé avec AAA.
- 4. Mise en œuvre des murs pare-feu : Implementing Firewall Technologies**
Objectifs : Mettre en œuvre des technologies de pare-feu pour assurer la sécurité du périmètre du réseau.

5. Mise en œuvre de la prévention d'intrusion : Implementing Intrusion Prevention

Objectifs : Configurer IPS pour atténuer les atteintes à la sécurité du réseau.

6. Sécuriser le réseau local : Securing the Local Area Network

Objectifs : Décrire les considérations de sécurité LAN et mettre en œuvre la sécurité et les caractéristiques des équipements couche.

7. Les systèmes de cryptographie : Cryptographysystems

Objectifs : Décrire les méthodes de mise en œuvre de la confidentialité et de l'intégrité des données.

8. Mise en œuvre des réseaux privés virtuels : Implementing Virtual Private Networks

Objectifs : Mettre en place des réseaux privés virtuels sécurisés.

9. Gestion d'un réseau sécuritaire : Managing a Secure Network

Objectifs : créer et mettre en œuvre une approche globale d'une politique de sécurité, en tenant compte des besoins de sécurité de l'entreprise.

10. Mise en œuvre du Cisco Adaptive Security Appliance (ASA) : Implementing the Cisco Adaptive Security Appliance

Objectifs : Mettre en œuvre des technologies de pare-feu à l'aide du ASA pour sécuriser le périmètre du réseau.

La formation doit alterner présentations magistrales et parties pratiques. Tous les ateliers pratiques se font directement sur du matériel réseau Cisco, en recréant des situations réelles d'infrastructure réseau. Il est indiqué donc d'intégrer :

- Des séquences en alternance : diaporama, support papier et/ou numérique, classeur personnalisé, extraits de textes et modèles,...
- Transfert d'expertise : échange d'expériences entre le formateur et les participants, problèmes soulevés, entretien et perfectionnement des connaissances,...
- Remise d'une attestation de stage pour chaque participant après un examen blanc sur le contenu de la formation.

V/ BENEFICIAIRES DE LA FORMATION

Comme mentionné plus haut, cette formation est destinée :

Structure :

Le personnel de la DGET, des Instituts Supérieurs des Etudes Technologiques, des institutions de formation des ingénieurs et des instituts préparatoires aux Etudes d'Ingénieurs.

Personnes

28 cadres (personnel administratif et technique) de la DGET et des établissements qui y relèvent.

Le public cible sera réparti sur deux groupes de 14 personnes.

VI/ DUREE, LIEU ET CALENDRIER DES MISSIONS

La durée globale de la formation sera de 12 jours (06 heures/jour), 6 jours pour chacun des 2 groupes. Elle se déroulera après la signature du contrat.

Les interventions du consultant seront assurées dans les locaux qui seront désignés par la DGET.

Le calendrier détaillé va être défini dans le contrat après négociation avec l'expert retenu.

VII/ QUALIFICATIONS ET PROFIL CONSULTANT

Le consultant devra répondre au profil suivant :

- Avoir une certification Cisco CCNA Security valide.
- Etre un Cisco instructeur CCNA.
- Une expérience professionnelle pertinente de 5 ans au minimum en rapport avec le sujet de la formation.
- Avoir participé à des actions et projets similaires.
- Une bonne connaissance des acteurs et des institutions de l'enseignement supérieur.

La connaissance des procédures de la Banque Mondiale et de ses directives en matière de passation des marchés sera un atout supplémentaire.

VIII/ MOYENS ET RESSOURCES A MOBILISER PAR LE CONSULTANT

Le consultant prend à sa charge son transport, son hébergement et tous les frais engendrés lors de son séjour.

Il est tenu de mobiliser par ses soins les moyens logistiques primordiaux pour sa prestation.

IX/ RAPPORTS

Le consultant sera appelé à présenter deux rapports à la Direction Générale des Etudes Technologiques :

Un premier sera réservé à la description du déroulement des séances de formation. Il devra retracer le niveau de participation, la présence des personnes formées (*la fiche de présence signée par les participants*) et leur degré d'assimilation des modules.

Un deuxième rapport décrivant le déroulement de la formation, évaluant la pertinence, l'efficacité et l'efficience de l'action et portant un bilan sur les progrès individuels des personnes formées par rapport à leur niveau de début.

Ces rapports seront validés par le directeur général des études technologiques.

X/ RESPONSABILITE DU CONSULTANT

Le consultant est censé s'acquitter de sa mission avec la diligence voulue et dans les règles de l'art.

La responsabilité du consultant envers la DGET est régie par le droit applicable au marché.

XI/ PIECES CONSTITUTIVES DE LA MANIFESTATION D'INTERET

1. Une lettre de candidature, dûment datée et signée, au nom de Monsieur le Directeur Général des Etudes Technologiques.
2. Toute information indiquant que le candidat atteste de l'expérience et des compétences nécessaires et qu'il est qualifié pour exécuter les dits services selon le modèle de CV joint aux termes de référence.
3. Un programme sommaire de la méthodologie préconisée pour l'exécution de la mission (dûment daté et signé).
4. Une copie de la certification Cisco CCNA.
5. Une copie des documents justifiant l'expérience acquise par le candidat.

XII/ CONFLITS D'INTERÊTS

Les Consultants en conflit d'intérêts, c'est-à-dire qui auraient un intérêt quelconque direct ou indirect au projet ou qui sont en relation personnelle ou professionnelle avec la Banque ou le Ministère doivent déclarer leurs conflits d'intérêts au moment de la transmission de la lettre d'intention pour la mission.

En particulier, tout fonctionnaire exerçant une fonction administrative doit présenter les autorisations nécessaires pour assurer la formation.

XIII/ MODE DE SELECTION

Le mode de sélection de consultant est celui du consultant individuel (personne physique) selon les directives de la Banque Mondiale. Toute candidature émanant d'un bureau ou d'un groupement sera exclue. Cependant, les consultants individuels appartenant à un bureau ou groupement peuvent présenter des candidatures individuelles. Une commission de sélection des candidatures établira un classement des candidatures selon un barème de notation des qualifications techniques de l'expert comme suit :

- Participation à des missions similaires (40).
- Carrière professionnelle pertinente pour la mission (30).
- Diplômes et qualifications pertinents pour la mission (20).
- Expérience générale du consultant (10).

Un Procès-Verbal de classement des candidats sera rédigé au terme de la sélection qui établira une liste restreinte pour la négociation du contrat. Un score minimal de 70/100 est requis pour être éligible.

Avant l'attribution définitive du contrat, celui-ci sera négocié avec le consultant sélectionné. Les négociations portent essentiellement sur :

- Les conditions techniques de mise en œuvre de la mission,
- L'approche méthodologique.
- Le contenu des livrables (toute production émise par le consultant au cours de la formation).
- L'offre financière.

Le candidat le mieux classé sera alors contacté pour présenter son offre financière et assister à la séance de négociation de son contrat.

Tout dossier de candidature arrivé après les délais ou qui ne présente pas les pièces justificatives demandées au paragraphe XI du présent document sera automatiquement écarté.

Développement et mise en place d'une plateforme collaborative au sein de la DGET

(FORMATION EN SECURITE RESEAUX POUR LE PERSONNEL ET ENSEIGNANTS RELEVANT DE LA DGET)

CURRICULUM VITAE

1. **Nom :**
2. **Prénom :**
3. **Date de naissance :**
4. **Nationalité :**
5. **Statut civil :**
6. **Adresse :**
7. **E-mail :**
8. **Téléphone (fixe & mobile):**
9. **Cursus de formation** [indiquer les études universitaires et autres études spécialisées ainsi que les noms des institutions fréquentées, les diplômes obtenus et les dates auxquelles ils l'ont été] :

<i>Institution</i>	
<i>Diplôme</i>	

<i>Institution</i>	
<i>Diplôme</i>	

<i>Institution</i>	
<i>Diplôme</i>	

10. Connaissance des langues :

<i>Langue</i>	<i>Lu</i>	<i>Parlé</i>	<i>Ecrit</i>

11. Affiliation à des organisations / groupements professionnels :

.....
.....
.....
.....
.....
.....
.....

12. Compétences Complémentaires [indiquer toute autre formation reçue ou compétence acquise depuis 9 ci-dessus] :

.....
.....
.....
.....
.....
.....

13. Qualifications clefs :

.....
.....
.....
.....
.....

14. Expériences dans les missions de formation [indiquer la liste des références des missions similaires conduites en indiquant l'organisme bénéficiaire de l'étude, la durée des tâches, l'objet ainsi que la date de début et de fin de la mission ou du projet] :

.....
.....
.....

.....
.....
.....
.....

15. Expériences Professionnelles [en commençant par son poste actuel, donner la liste par ordre chronologique inverse de tous les emplois exercés par l'employé depuis la fin de ses études. Pour chaque emploi, donner les dates, le nom de l'employeur et le poste occupé]

Date :
Pays :
Organisme :
Position / Emploi :
Courte description :

Date :
Pays :
Organisme :
Position / Emploi :
Courte description :

Date :
Pays :
Organisme :
Position / Emploi :
Courte description :

16. Publications et autres informations utiles :

.....
.....
.....
.....
.....
.....
.....

17. Attestations :

Je soussigné, certifie, en toute conscience, que les renseignements ci-dessus rendent fidèlement compte de ma situation, de mes qualifications et de mon expérience. J'accepte que toute déclaration volontairement erronée peut entraîner mon exclusion, ou mon renvoyer si j'ai été engagé.

..... Date :
.....

[Signature du consultant]

Jour/mois/année