ANNEXE A

OUTIL DE CAPTURE DE PAQUETS COMPLETS ET D'ANALYSE DE LA SÉCURITÉ
ÉNONCÉ DES TRAVAUX

1. INTRODUCTION

1.1. Le Centre des opérations de sécurité (COS) de Services partagés Canada (SPC) est chargé de soutenir les fonctions des systèmes de sécurité des technologies de l'information (TI) du gouvernement du Canada (gouvernement du Canada). L'intégration, l'ingénierie, la fourniture et le soutien des systèmes de sécurité applicables à tous les ministères membres de SPC sont inclus dans ce champ des responsabilités. Les systèmes existants et les systèmes de l'état final sont pris en charge en parallèle; cependant, dans le cadre de l'initiative de SPC, ces systèmes passeront progressivement à une adoption pangouvernementale regroupée.

1.2. Le COS de SPC doit remplacer une solution de capture de paquets complets et d'analyse de la sécurité arrivée à la fin de on cycle de vie et de soutien. Il s'agit d'un outil de détection crucial utilisé quotidiennement par le COS de SPC pour détecter et confirmer les menaces.

2. TERMINOLOGIE

Le tableau ci-dessous fournit des renseignements généraux sur les abréviations et acronymes utilisés dans le présent Énoncé des travaux (ÉT).

GC	Gouvernement du Canada
SDI	Système de détection d'intrusion
SPI	Système de prévention d'intrusion
TI	Technologie de l'information
RCN	Région de la capitale nationale
FEO	Fabricant d'équipement d'origine
DP	Demande de proposition
COS	Centre des opérations de sécurité
ÉT	Énoncé des travaux
SPC	Services partagés Canada
RT	Responsable technique

Remarque : Un (1) gigabit = 0,125 gigaoctet ou 125 mégaoctets.

3. CONTEXTE

3.1. L'équipe des opérations de sécurité relève de SPC et a pour mandat d'assurer un soutien interne pour plusieurs applications de systèmes de sécurité de calibre professionnel, y compris les systèmes de gestion principaux de ces applications. À l'heure actuelle, ces applications se trouvent dans plus de 43 réseaux ministériels. Cependant, dans le cadre de l'initiative de SPC, ces systèmes passeront progressivement à une adoption pangouvernementale regroupée.

3.2. Le principal objectif de la présente demande de proposition (DP) consiste à remplacer la solution de capture de paquets complets et d'analyse de la sécurité arrivée à la fin de son cycle de vie et de soutien (au 31 mars 2016). Toute la solution doit être remplacée. Le contrat de base vise les biens et les services requis pour répondre à ce besoin.

3.3. Le deuxième objectif de la DP est d'établir une méthode permettant de développer la solution au fil du temps et d'en élargir progressivement la portée au sein du gouvernement du Canada. Les outils de capture de paquets complets et d'analyse de la sécurité sont employés de façon limitée au gouvernement du Canada; la présente DP est l'une des méthodes adoptées pour normaliser l'utilisation d'un outil commun dans l'ensemble des réseaux opérés par SPC.

3.4. Un ensemble générique d'outils de surveillance de réseau ne suffit pas à répondre à la présente DP. Son principal objectif vise plutôt la capture de paquets dans un contexte d'analyses de sécurité. Les utilisateurs finals de la solution seront les opérateurs du COS. Ces derniers utiliseront l'outil pour confirmer les alertes du système de détection d'intrusion (SDI) et du système de prévention d'intrusion (SPI) en cas d'intrusion par des tiers, pour réexécuter les attaques présumées et dans le cadre d'enquêtes de sécurité.

4. OBJECTIF

4.1. Le principal objectif du contrat consiste à remplacer l'outil de capture de paquets complets et d'analyse de la sécurité à la fin du cycle de soutien au plus tard le 31 mars 2016. Les biens et les services suivants seront requis dans le cadre de cet effort de remplacement :

4.1.1. Le matériel informatique et les logiciels nécessaires pour capturer, stocker et analyser le trafic sur les liens réseau utilisés pour la connexion d'un partenaire de SPC à Internet, par l'entremise d'un port d'accès de test (TAP) réseau existant fourni par l'État, et pour effectuer des analyses de sécurité complexes du trafic capturé.

4.1.2. Le matériel informatique et les logiciels nécessaires pour gérer tous les dispositifs de façon centralisée.

4.1.3. Un forfait de services professionnels à court terme offerts par le fournisseur (ou un partenaire du fournisseur) afin d'aider SPC à déployer la solution de manière efficace.

4.1.4. Un programme de formation de cinq (5) jours sur l'administration de la solution donné par le fournisseur aux employés de SPC.

4.2. Le deuxième objectif consiste à déterminer les options contractuelles dont pourra se prévaloir SPC pour acquérir des biens et services supplémentaires afin de développer la solution au cours des trois (3) prochaines années.

4.3. Quatre (4) catégories de solutions sont requises aux termes de la DP :

4.3.1. Solution d'entreprise. Utilisée pour les plus grands réseaux de SPC (2 gigabits par seconde de débit de données moyen). Cette solution fait partie du contrat de base (deux unités).

4.3.2. Solution de prestataire Internet. Utilisée pour l'infrastructure partagée du gouvernement du Canada comme les connexions Internet pangouvernementales futures. (8 gigabits par seconde de débit de données moyen.)

4.3.3. Solution moyenne. (1 gigabit par seconde de débit de données moyen.)

4.3.4. Solution virtuelle, utilisée pour les besoins des partenaires de capacité moindre.

4.4. Toutes les catégories de solutions doivent avoir une cible de conservation du trafic capturé de 14 à 30 jours. Les fournisseurs doivent offrir une capacité de stockage suffisante pour satisfaire à cette exigence.

4.5. Toutes les catégories de solutions doivent avoir une cible de conservation des métadonnées de 30 à 90 jours. Les fournisseurs doivent offrir une capacité de stockage suffisante pour satisfaire à cette exigence.

4.6. La solution peut être déployée dans un réseau entièrement fermé sans accès à Internet.

4.7. L'état final de la solution est son déploiement à l'échelle du gouvernement du Canada. Cet état final consiste en une solution de gestion centrale située dans un COS du gouvernement. Le système central se connecterait aux télécapteurs par le truchement d'un réseau national de gestion de la sécurité. Un schéma général du type d'utilisation est illustré à la figure 1 :

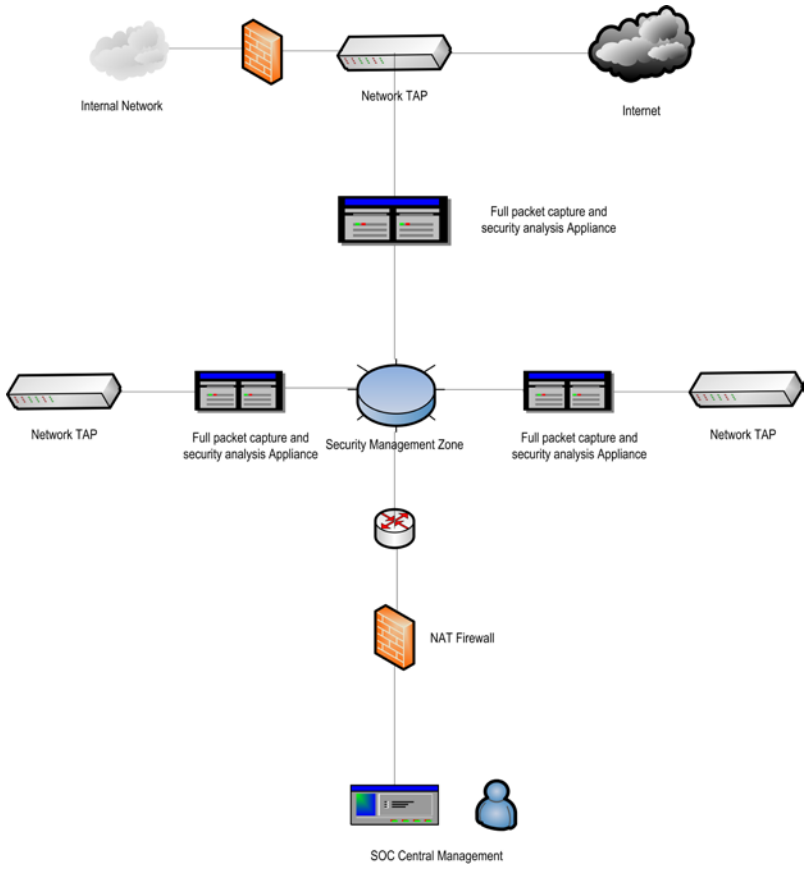

Figure 1 : Type d'utilisation

5. PORTÉE DES TRAVAUX

5.1. Le contrat de base comprend ce qui suit :

5.1.1. Deux (2) solutions d'entreprise pour le matériel et la première année de maintenance et de soutien. Une solution peut être constituée de plusieurs dispositifs ou d'un seul, pourvu qu'ils satisfassent à toutes les exigences obligatoires et aux critères cotés énoncés dans le présent énoncé des travaux. Chaque solution recevra des flux de données d'un TAP réseau existant fourni par l'État. Le débit du flux du trafic devrait se situer entre 2 gigabits par seconde et 10 gigabits par seconde en rafale.

5.1.2. Un (1) système de gestion centrale qui peut être utilisé pour gérer tous les dispositifs et la première année de maintenance et de soutien. Une solution peut être constituée de plusieurs dispositifs ou d'un seul, pourvu qu'ils satisfassent à toutes les exigences obligatoires et aux critères cotés énoncés dans le présent énoncé des travaux. Le système de gestion centrale sera employé pour mettre à niveau les dispositifs et donner un aperçu regroupé des analyses du trafic capturé par les dispositifs.

5.1.3. Une formation donnée par un instructeur sur place à Ottawa, en Ontario, totalisant 35 à 40 heures sur cinq (5) jours ouvrables consécutifs.

5.1.4. Dix (10) jours de services professionnels visant à contribuer au déploiement efficace de la solution de base, y compris les services suivants :

- Génie;
- Essais;
- Optimisation;
- Configuration du système.

5.2. Le volet optionnel du contrat comprend ce qui suit :

5.2.1. L'option d'acquérir les services de maintenance et de soutien pour les deuxième et troisième années suivant l'achat du matériel effectué dans le cadre du contrat de base (deux solutions d'entreprise pour la capture de paquets et un système de gestion centrale).

5.2.2. L'option d'acquérir des solutions d'entreprise supplémentaires pour le matériel pendant au plus trois (3) ans au prix original de la soumission.

5.2.3. L'option d'acquérir une solution de prestataire Internet pour le matériel pendant au plus trois (3) ans au prix établi dans la soumission.

5.2.4. L'option d'acquérir une solution moyenne pour le matériel pendant au plus trois (3) ans au prix établi dans la soumission.

5.2.5. L'option d'acquérir une solution virtuelle pour le matériel pendant au plus trois (3) ans au prix établi dans la soumission.

5.2.6. L'option d'acheter un ou des forfaits de formation de cinq (5) jours supplémentaires pendant au plus trois (3) ans au prix établi dans la soumission.

5.2.7. L'option d'acheter un forfait de services professionnels de dix (10) jours supplémentaire pour le déploiement pendant au plus trois (3) ans au prix établi dans la soumission.

5.2.8. L'option d'acquérir tout module, toute fonction ou toute amélioration qui peuvent être activés dans la solution et qui ne font pas partie des besoins de base.

6. PRODUITS LIVRABLES

6.1. Tous les produits livrables indiqués dans l'énoncé des travaux doivent être présentés au responsable technique (RT).

6.1.1. L'ensemble du matériel et des logiciels inclus dans la solution d'entreprise, la solution de prestataire Internet, la solution moyenne et la solution virtuelle de capture de paquets et d'analyse de la sécurité. Cela comprend l'ensemble des logiciels, des dispositifs, des

adaptateurs de réseau et du stockage requis pour satisfaire à toutes les exigences obligatoires et à tous les critères cotés énoncés dans la soumission.

6.1.2. Le cas échéant, l'abonnement au service de renseignements sur les menaces réseau pendant les 12 premiers mois.

6.1.3. L'ensemble du matériel et des logiciels inclus dans le système de gestion centrale. Cela comprend l'ensemble des logiciels, des dispositifs, des adaptateurs de réseau et du stockage requis pour satisfaire à toutes les exigences obligatoires et à tous les critères cotés énoncés dans la soumission.

6.1.4. Cinq (5) jours de formation, y compris :

- Des salles de classe accueillant dix (10) personnes pourvues par le fournisseur.
- Un instructeur approuvé par le fabricant d'équipement d'origine (FEO) donnant le cours sur place.
- Tout le matériel de cours, y compris les postes de travail pour effectuer les activités de laboratoire.

6.1.5. Un forfait de dix (10) jours de services professionnels, y compris :

- La documentation sur le système et la version, sous format papier et sous format électronique, au besoin.
- La documentation sur le projet, au besoin.
- Le code source de tous les scripts personnalisés requis pour mettre en œuvre la solution, y compris les commentaires sur le codage.
- Le transfert des connaissances aux ressources désignées par l'État, au besoin.

7. BIENS LIÉS AUX SERVICES PROFESSIONNELS RENDUS SUR PLACE

7.1. Lieu de travail

Les ressources doivent être en mesure de travailler dans les locaux du gouvernement du Canada situés dans la région de la capitale nationale (RCN). Des postes de travail informatisés seront fournis.

Les déplacements dans la RCN seront fréquents. Les frais de déplacement dans la RCN ne seront pas remboursés.

7.2. Supervision du travail

Les ressources qui fournissent des services professionnels travailleront sous la supervision d'un responsable technique ou d'un gestionnaire.

7.3. Rapports d'étape

Le fournisseur doit joindre des rapports d'étape à toutes ses factures.

7.4. Ressources de soutien

Des ressources de bureau seront fournies aux ressources.

7.5. Attestation de sécurité

Les ressources fournissant des services professionnels dans le cadre du forfait de dix (10) jours doivent avoir une attestation de sécurité de niveau 2 (secret). Le soumissionnaire doit préciser le numéro de dossier de l'attestation de sécurité et sa date d'échéance.

7.6. Heures normales de travail

Les ressources travailleront aux heures normales de travail, soit pas avant 7 h et pas plus tard que 18 h, heure de l'Est, du lundi au vendredi. Pendant les dix (10) jours de ce forfait de services professionnels, les ressources doivent travailler 7,5 heures par jour au cours de ces heures normales, à moins d'ententes différentes conclues au préalable avec le responsable technique.

7.7. Exigences linguistiques

Les ressources doivent être capables de communiquer efficacement en anglais, tant à l'oral qu'à l'écrit.

8. BIENS LIÉS AUX SERVICES DE FORMATION

8.1. Lieu de travail

Les ressources donnant la formation doivent être en mesure de travailler dans les locaux du gouvernement du Canada situés dans la RCN.

8.2. Supervision du travail

Les ressources donnant la formation travailleront sous la supervision d'un responsable technique ou d'un gestionnaire.

8.3. Ressources de soutien

Des ressources de bureau seront fournies aux ressources mais ces dernières devront fournir leur ordinateur.

8.4. Autorisation de sécurité

Les ressources donnant la formation ne sont pas tenues d'être dotées d'une autorisation de sécurité du gouvernement du Canada.

8.5. Heures normales de travail

Les ressources travailleront aux heures normales de travail, soit pas avant 7 h et pas plus tard que 18 h, heure de l'Est, du lundi au vendredi.

8.6. Exigences linguistiques

Les ressources doivent être capables de communiquer efficacement en anglais, tant à l'oral qu'à l'écrit. Le bilinguisme (anglais et français) est souhaitable, mais pas obligatoire.

9. AVIS DE PROPRIÉTÉ

9.1. Non-divulgation

9.1.1. Tous les travaux exécutés par l'entrepreneur dans le cadre du présent énoncé des travaux demeureront la propriété de l'État. Les rapports, documents et prolongations afférentes demeurent la propriété de l'État et l'entrepreneur ne peut divulguer ou diffuser de tels

rapports ou documents à une autre personne, ni les reproduire, sans l'autorisation écrite préalable de l'État.

9.1.2. Tous les renseignements et les documents mis à la disposition de l'entrepreneur dans le cadre du présent projet sont jugés exclusifs et doivent être restitués à l'État une fois les tâches décrites dans le présent énoncé des travaux réalisés ou à la résiliation du contrat.

10. INTERPRÉTATION

10.1. En cas de différends dans l'interprétation du présent énoncé des travaux ou de la terminologie qu'il contient, la décision du responsable technique a préséance.