Institut belge des services postaux et des télécommunications (IBPT)
35 Boulevard du Roi Albert II, 1030 Bruxelles
Personne de contact:
Pascal Vrancken (Fr) tél. : +32 (0)2 226 87 95
e-mail : pascal.vrancken@ibpt.be

CAHIER DES CHARGES n° 2014/SME/Firewall

APPEL D'OFFRES GENERAL

POUR LE COMPTE DE L'INSTITUT BELGE DES SERVICES POSTAUX ET DES TÉLÉCOMMUNICATIONS (IBPT)
POUR LA FOURNITURE DE FIREWALL'S, D'UNE « CENTRAL MANAGMENT» ET D'UN CONTRAT DE MAINTENANCE OPTIONNEL

TABLE DES MATIÈRES

A. DISPOSITIONS GÉNÉRALES

1. **Dérogations aux règles générales d'exécution**

Cet article n'est pas applicable au présent marché.

2. Objet et nature du marché

Le présent marché porte sur la fourniture de Firewall's et d'une « Central Managment », incluant un contrat de support / maintenance annuel optionnel, reconductible pendant 5 ans.

La procédure choisie est celle de l'appel d'offres général au sens de la loi du 15 juin 2006 relative aux marchés publics et à certains marchés de travaux, de fournitures et de services, articles 23 et 25 et de l'A.R. du 15 juillet 2011 relatif à la passation des marchés publics dans les secteurs classiques, article 2, 4° .

Il s'agit d'un marché à forfait (A.R. 8 janvier 1996, art. 86)

Ce marché comporte un lot, ne permet aucune variante et comprend une option.

Il s'agit d'un marché forfaitaire à prix global selon les articles 2 et 13 de l'arrêté royal du 15 juillet 2011 relatif à la passation des marchés publics dans les secteurs classiques.

3. Durée du contrat

Le marché doit impérativement être terminé dans les 2 mois après l'attribution du marché.

Le marché prend cours le premier jour calendrier qui suit le jour où le prestataire de services a reçu la notification d'attribution du marché et dure jusqu'au moment où le marché est complètement exécuté.

Marché optionnel annuel de mise à jour pour les années suivantes (au maximum jusqu'en (2019)

Chaque année (pendant un maximum de cinq années, débutant l'année où le marché sera passé), l'IBPT pourra souscrire à un contrat optionnel de services (support / maintenance) comme d'écrite ci-après (***Cf***. D.3 Services).

Un tel contrat optionnel de Services (Support / Maintenance) sera éventuellement signé pour une année. Chaque année, l'IBPT réévaluera la nécessité de renouvellement. Ce contrat ne sera donc pas prolongé tacitement sans une commande préalable de l'IBPT, sur base d'un courrier de rappel émanant du soumissionnaire.

La durée totale de ce contrat de Services (Support / Maintenance), après reconductions éventuelles, n'excédera pas 5 ans.

4. Pouvoir adjudicateur – Informations complémentaires

Le pouvoir adjudicateur est l'Institut belge des services postaux et des télécommunications (IBPT), représenté par Charles Cuvelliez, Membre du Conseil, mandaté par le Conseil.

Des informations complémentaires relatives à la procédure peuvent être obtenues auprès de :

- Pascal Vrancken, tél. : +32 (0)2 226 87 95, e-mail : pascal.vrancken@ibpt.be
- Steeve Minne, tél. : +32 (0)2 226 89 13, e-mail : steeve.minne@ibpt.be

5. Introduction et ouverture des offres

Les offres doivent être déposées conformément à l'article 90 de l'arrêté royal du 15 juillet 2011 relatif à la passation des marchés publics dans les secteurs classiques.

Pour le dépôt par porteur, les offres devront être remises au bureau d'accueil de l'IBPT durant les heures d'ouverture des bureaux (de 8h30 à 17h00), contre remise d'un accusé de réception.

Les offres doivent être en possession du pouvoir adjudicateur au plus tard le ***vendredi 19 septembre 2014*** à 10 heures.

6. Description des fournitures

Le présent marché se rapporte à la fourniture du matériel et services suivants :

A) 2 Firewall's pour le site Central de l'IBPT (Ellipse Building) ;
B) 5 Firewall's pour les centres provinciaux de Anderlecht, Antwerpen, Gent, Liège et Seneffe ;
C) 1 « Central Managment » pour le site Central de l'IBPT (Ellipse Building) ;
D) Installation, configuration et formation
E) Contrat de Services (Support / Maintenance) annuel optionnel – max. 5 ans.

7. Documents régissant le marché

7.1. Législation

Le présent marché est intégralement soumis aux règles applicables en la matière en Belgique, et notamment la loi du15 juin 2006 relative aux marchés publics et à certains marchés de travaux, fournitures et ses arrêtés d'exécution.

7.2. Documents concernant le marché

- Le présent cahier des charges n° 2014/SME/Firewall.
- L'offre approuvée, sauf toutes les dispositions y figurant contraires au présent cahier des charges, et notamment les conditions générales du soumissionnaire.

8. Offres

8.1. Données à mentionner dans l'offre

L'attention des soumissionnaires est attirée sur l'article 9 de la loi du 15 juin 2006 relatif aux incompatibilités.

Les articles 80 à 82 de l'arrêté royal du 15 juillet 2011 relatif à la passation des marchés publics dans les secteurs classiques sont d'application.

L'offre et toutes les annexes jointes au formulaire d'offre sont rédigées soit intégralement en français, soit intégralement en néerlandais.

Par le dépôt de son offre, le soumissionnaire renonce automatiquement à ses conditions générales ou particulières de vente, même si celles-ci sont mentionnées dans l'une ou l'autre annexe à l'offre.

Le soumissionnaire indique clairement dans son offre quelle information est confidentielle et/ou se rapporte à des secrets techniques ou commerciaux et ne peut donc pas être divulguée par le pouvoir adjudicateur.

Le formulaire d'offre joint au cahier spécial des charges est impérativement présenté en préambule de l'offre.

Conformément à l'article 88 de l'arrêté royal du 15 juillet 2011 précité, tous les montants de l'offre doit être inscrit en toutes lettres dans le formulaire d'offre. L'IBPT exige en outre que ces mêmes montants soient inscrits en chiffres.

En outre, l'IBPT demande que le taux de TVA applicable et les montants calculés après application de ce taux de TVA soient également inscrits dans le formulaire d'offre.

8.2. Durée de validité de l'offre

Conformément à l''article 57 de l'arrêté royal du 15 juillet 2011 relatif à la passation des marchés publics dans les secteurs classiques, l'offre a une validité de 120 jours.

8.3. Echantillons, documents et attestations à joindre à l'offre

Les soumissionnaires joignent à leur offre, outre le formulaire d'offre, tous les documents requis dans le cadre de l'examen des critères de sélection et d'attribution ci-après détaillés.

9. Prix

9.1. Prix

Tous les prix mentionnés dans le formulaire d'offre doivent être obligatoirement libellés en EURO.

L'adjudicataire est censé avoir inclus dans ses prix unitaires tous les frais possibles grevant les services ou les fournitures demandées, à l'exception de la TVA.

9.2. Révision de prix

Pour l'option de support/maintenance demandée, une révision des prix est possible sur la base de l'indice des prix à la consommation. L'indice des prix à la consommation utilisé comme base est celui du mois précédant le début du contrat. La révision a lieu le 1er janvier de chaque année en cours du contrat..

10. Responsabilité de l'adjudicataire

Le prestataire de services assume la pleine responsabilité des fautes et manquements présentés dans les services fournis, en particulier dans les études, les comptes, les plans ou dans toutes les autres pièces déposées par lui en exécution du marché.

Par ailleurs, le prestataire de services garantit le pouvoir adjudicateur des dommages et intérêts dont celui-ci est redevable à des tiers du fait du retard dans l'exécution des services ou de la défaillance du prestataire de services.

Il démontrera en outre, dès le début de sa mission, du respect par lui de l'article 24 de l'arrêté royal du 14 janvier 2013 établissant les règles générales d'exécution des marchés publics et des concessions de travaux publics.

11. Droit d'accès au marché et sélection qualitative particulière

L'IBPT se réfère pour cela aux articles 58 et suivants de l'arrêté royal du 15 juillet 2011 relatif à la passation des marchés publics dans les secteurs classiques.

Par le seul fait de participer à la procédure de passation du présent marché public, le soumissionnaire atteste qu'il ne se trouve pas dans un des cas d'exclusion visés aux articles 58 et suivants de l'arrêté royal du 15 juillet 2011 précité.

L'exactitude de cette déclaration sur l'honneur implicite est vérifiée dans le chef du soumissionnaire dont l'offre sera la mieux classée après l'examen des critères d'attribution.

Pour le présent marché, au titre de sélection qualitative, conformément aux articles 67 et suivants de l'arrêté royal du 15 juillet 2011 précité, l'IBPT vérifiera pour tout

soumissionnaire ayant remis offre les éléments suivants, sur base des documents particuliers requis :

- Une déclaration concernant le chiffre d'affaires global des trois dernières années ;
- La capacité technique ou professionnelle du soumissionnaire :

  1° par l'indication des techniciens ou des organismes techniques, qu'ils soient ou non intégrés à l'entreprise, en particulier de ceux qui sont responsables du contrôle de la qualité;

  2° par la présentation d'une liste des principales livraisons effectuées au cours des trois dernières années, indiquant le montant, la date et le destinataire public ou privé. Les livraisons sont prouvées par des attestations émises ou contresignées par l'autorité compétente ou, lorsque le destinataire a été un acheteur privé par une attestation de l'acheteur ou à défaut simplement par une déclaration du fournisseur;

12. Visite des lieux

Sous peine de voir son offre immédiatement exclue, le soumissionnaire est tenu de participer à une visite des locaux de l'IBPT.

Pour ce faire, il se préinscrira à celle-ci, en renvoyant le formulaire annexé ; ce dernier devant être contre signé par au moins un des participants inscrits, le jour de la visite.

Ce formulaire doit être renvoyé, au plus tard, le vendredi de la semaine précédant celle de la visite

Cette visite des lieux est prévue le ***vendredi 05 septembre 2014*** à 10 heures dans les locaux de l'IBPT situé à Ellipse Building (Bâtiment C) – Boulevard du Roi Albert II, 35 1030 Bruxelles.

Cette visite se tiendra en français et en néerlandais. Chaque candidat aura la possibilité de poser ses questions en français ou en néerlandais.

Une liste des questions – réponses sera établie et sera transmise aux candidats qui en feront la demande lors de cette réunion.

Cette réunion est le seul moment ou des questions pourront être posées en relation avec ce marché

13. Régularité des offres

L'IBPT procèdera à un examen des offres quant à leur régularité, tant formelle que matérielle, conformément à l'article 95 de l'arrêté royal du 15 juillet 2011 relatif à la passation des marchés publics dans les secteurs classiques.

14. Vérification des prix

L'IBPT procèdera à la vérification des prix conformément aux article 21 et 99 de l'arrêté royal du 15 juillet 2011 relatif à la passation des marchés publics dans les secteurs classiques.

15. Critères d'attribution.

Pour le choix de l'offre la plus intéressante d'un point de vue économique, les offres seront confrontées à une série de critères d'attribution.

Ces critères seront pondérés afin d'obtenir un classement final.

15.1. Liste des critères d'attribution et pondération

Les critères d'attribution, par ordre décroissant d'importance, sont les suivants:

1. Prix pour la fourniture des Firewall's et d'une « Central Managment », incluant l'analyse, l'installation, la configuration, la formation, le support et la maintenance pour 5 ans (critère sur 25 points)
2. Prix pour un Contrat de Services (Support / Maintenance) annuel optionnel - max. 5 ans (critère sur 25 points)
3. Compréhension de la mission et la méthodologie du soumissionnaire (critère sur 10 points)
4. Délais de livraison des fournitures (critère sur 10 points)
5. Le matériel proposé (critère sur 10 points)
6. Contrat de Services (Support / Maintenance) annuel et les qualifications des personnes mises à disposition pour assurer celui-ci (critère sur 10 points)
7. La Formation (critère sur 10 points)

Prix pour la fourniture des Firewall's et d'une « Central Managment », incluant l'analyse, l'installation, la configuration, la formation (critère sur 25 points):

Le prix demandé pour ce marché public est un prix forfaitaire global en ce qui concerne la mission telle que décrite.

Le soumissionnaire avec le prix total le plus bas (P1) se verra attribuer le maximum des points pour ce critère, soit 25 points. Les autres soumissionnaires (Pk) se voient cotés selon la formule suivante :

$$\text{Points} = 25 - \left(25 \times \frac{P_k - P_1}{P_1} \right)$$

Prix pour un Contrat de Services (Support / Maintenance) annuel optionnel - max. 5 ans (critère sur 25 points)

Le prix demandé pour ce marché public est un prix forfaitaire global en ce qui concerne la mission telle que décrite.

Le soumissionnaire avec le prix total le plus bas (P1) se verra attribuer le maximum des points pour ce critère, soit 25 points. Les autres soumissionnaires (Pk) se voient cotés selon la formule suivante :

$$\text{Points} = 25 - \left(25 \times \frac{P_k - P_1}{P_1} \right)$$

Compréhension de la mission et la méthodologie du soumissionnaire (critère sur 10 points) :

Le soumissionnaire devra fournir un document de maximum 5 pages, en français ou en néerlandais, décrivant sa compréhension de la mission et la méthodologie qu'il suivra pour la réaliser

Délais de livraison des fournitures (critère sur 10 points) :

Le soumissionnaire devra fournir les documents suivants en vue de l'évaluation de ce critère :

a) un timing au regard de l'importance de la mission et de la vision réaliste des délais proposés, ce timing devra préciser les délais de livraison.

Le matériel proposé (critère sur 10 points)

En vue de l'évaluation de ce critères, chaque soumissionnaire :

a) pour le matériel proposé, sera tenu d'indiquer très clairement, en quoi celui-ci diffère des critères demandés. Ceci, que les valeurs soient supérieurs, ou inférieurs à ce qui est requis. Il établira, pour chaque composant, un documents énumérant les critères d'origines demandés, et les valeurs réelles du matériel proposé dans son offre ;

b) fournira une documentation détaillées de chaque composant proposé

Contrat de Services (Support / Maintenance) annuel et les qualifications des personnes mises à disposition pour assurer celui-ci (critère sur 10 points)

Le soumissionnaire devra fournir les documents suivants en vue de l'évaluation de ce critère :

a) Une liste de références en relation avec la présente mission pendant les trois dernières années ;

b) Les CV des collaborateurs présentés pour réaliser ce marché ;

La formation (critère sur 10 points)

En vue de l'évaluation de ce critères, le soumissionnaire :

a) fournira un bref descriptif des éléments qui seront développés pendant la formation, en vue de permettre aux participants la prise en main du matériel proposé.

15.2. Cotation finale

Les cotations pour les critères d'attribution seront additionnées.

Le marché sera attribué au soumissionnaire qui obtient la cotation finale la plus élevée, sur 100.

Pour chaque critères, une cote inférieure à la moitié des points maximaux attribuables entraînera l'exclusion du soumissionnaire.

16. Cautionnement

Le cautionnement sera constitué conformément aux articles 25 et suivants de l'arrêté royal du 14 janvier 2013 établissant les règles générales d'exécution des marchés publics et des concessions de travaux public...

17. Réceptions

Les services seront suivis de près pendant leur exécution par un délégué du pouvoir adjudicateur.

Les règles de réception contenues dans l'arrêté royal du 14 janvier 2013 établissant les règles générales d'exécution des marchés publics et des concessions de travaux publics sont d'application pour le présent cahier des charges.

18. Lieu de livraisons des fournitures

Les fournitures seront livrées aux adresse suivantes :

b) Institut belge des services postaux et des télécommunications, 35 Boulevard Albert II, à 1030 Bruxelles.
c) Robert Buyckstraat 48 -52 à 1070 Brussel (Anderlecht)
d) Maria Theresialei 11 à 2000 Antwerpen
e) Burggravenlaan 40 à 9000 Gent
f) Rue Wiertz 34 à 4000 Liège
g) Chaussée de Mons 55 à 7180 Seneffe

19. Facturation et paiement

19.1 Mission Principale : L'adjudicataire enverra sa facture, après l'accomplissement de la mission complète, à l'adresse suivante :

> Institut belge des services postaux et des télécommunications, 35 Boulevard Albert II, à 1030 Bruxelles.

19.2 Mission Secondaire (contrat de support/maintenance optionnel) : L'adjudicataire enverra sa facture à la date d'échéance du contrat, à la même adresse

Dans les 2 cas, le paiement a lieu dans un délai de 30 jours de calendrier à compter de la réception de la déclaration de créance, pour autant que le pouvoir adjudicateur ait été mis dans les délais prévus en possession des autres documents éventuellement exigés.

La facture doit être libellée en EURO.

20. Engagements particuliers pour le prestataire de services

Le prestataire de service s'engage à ce que les Firewall's fournis soient compatibles avec les anciens Firewall's Juniper Netscreen, en terme de fonctionnement, comme décrit en « C. Notice Technique ».

21. Litiges

Tous les litiges relatifs à l'exécution de ce marché sont exclusivement tranchés par les tribunaux compétents de l'arrondissement judiciaire de Bruxelles. La langue véhiculaire est le français ou le néerlandais.

Le pouvoir adjudicateur n'est en aucun cas responsable des dommages causés à des personnes ou à des biens qui sont la conséquence directe ou indirecte des activités nécessaires à l'exécution de ce marché. Le prestataire de services garantit le pouvoir adjudicateur contre toute action en dommages et intérêts par des tiers à cet égard.

B. FORMULAIRE D'OFFRE

Institut belge des services postaux et des télécommunications (IBPT)
35 Boulevard du Roi Albert II, 1030 Bruxelles
Personne de contact:
Pascal Vrancken (Fr) tél. : +32 (0)2 226 87 95
e-mail : pascal.vrancken@ibpt.be

CAHIER SPÉCIAL DES CHARGES n°2014/SME/Firewall

APPEL D'OFFRES GENERAL
POUR LE COMPTE DE L'INSTITUT BELGE DES SERVICES POSTAUX ET DES TÉLÉCOMMUNICATIONS (IBPT)
POUR LA FOURNITURE DE FIREWALL'S, D'UNE « CENTRAL MANAGMENT » ET D'UN CONTRAT DE MAINTENANCE OPTIONNEL

La société

(dénomination complète)

dont l'**adresse est:**

(rue)

(code postal et commune)

(pays)

immatriculée à la **Banque Carrefour des Entreprises** sous le numéro

et pour laquelle **Monsieur/Madame *(*)***

(nom)
(fonction)

domicilié(e) à l'adresse:

(rue)

(code postal et commune)

(pays)

agissant comme **soumissionnaire ou fondé de pouvoirs**, signe ci-dessous.

MARCHÉ DE BASE

Le soumissionnaire ou fondé de pouvoirs s'engage à exécuter conformément aux clauses et conditions du cahier des charges **n° 2014/SME/Firewall, l**a livraison des fournitures demandées ci-avant, moyennant le prix forfaitaire global suivant **:** :

[en lettres et en chiffres en EURO]

auquel il y a lieu d'ajouter la T.V.A., soit un montant de:

[en lettres et en chiffres en EURO]

ce qui donne un prix forfaitaire global, T.V.A. incluse, de:

[en lettres et en chiffres en EURO]

MARCHÉ ANNUEL OPTIONNEL DE SERVICES (SUPPORT/MAINTENANCE) POUR LES ANNÉES SUIVANTES (AU MAXIMUM JUSQU'EN 2019)

Dans le cas où l'IBPT en évaluerait la nécessité (annuellement) et m'en ferait la demande, Le soumissionnaire ou fondé de pouvoirs s'engage à exécuter conformément aux clauses et conditions du cahier spécial des charges **n° 2014/SME/Firewall**, moyennant le prix forfaitaire suivant :

[en lettres et en chiffres en EURO]

auquel il y a lieu d'ajouter la T.V.A., soit un montant de:

[en lettres et en chiffres en EURO]

ce qui donne un prix forfaitaire global, T.V.A. incluse, de:

[en lettres et en chiffres en EURO]

L'information confidentielle et/ou l'information qui se rapporte à des secrets techniques ou commerciaux est clairement indiquée dans l'offre.

L'organisme de paiement du pouvoir adjudicateur paiera les sommes dues par virement ou versement

sur le **compte n°**:	
IBAN	
BIC	

Pour l'interprétation du contrat, la langue | française/néerlandaise ***(*)*** | est choisie.

Toute correspondance concernant l'exécution du marché doit être envoyée à l'adresse suivante:

(rue)

(code postal et commune)

(n° de ✆ et de fax)

Fait: **A** **Le** **2014.**

Le soumissionnaire ou le fondé de pouvoirs:

(nom)
(fonction)
(signature)

APPROUVÉ,

(identité et titre de la personne compétente pour approuver l'offre)

POUR MÉMOIRE: DOCUMENTS À JOINDRE OBLIGATOIREMENT À L'OFFRE:

- **Tous les documents et renseignements demandés dans le cadre des critères de sélection et des critères d'attribution.**

  N'oubliez pas de prévoir une numérotation continue et ininterrompue de toutes les pages de votre offre, de votre inventaire et des annexes.

C. FORMULAIRE D'INSCRIPTION À LA VISITE DES LIEUX

CAHIER SPÉCIAL DES CHARGES n°2014/SME/Firewall

APPEL D'OFFRES GENERAL POUR LE COMPTE DE L'INSTITUT BELGE DES SERVICES POSTAUX ET DES TÉLÉCOMMUNICATIONS (IBPT) POUR LA FOURNITURE DE FIREWALL'S, D'UNE « CENTRAL MANAGMENT » ET D'UN CONTRAT DE MAINTENANCE

(Visite des lieux du vendredi 05 septembre 2014 à 10 heures)

La société

(dénomination complète)

dont l'**adresse est:**

(rue)

(code postal et commune)

(pays)

Participera à la visite des lieux prévue le ***vendredi* 05 septembre *2014*** à 10 heures dans les locaux de l'IBPT situé à Ellipse Building (Bâtiment C) – Boulevard du Roi Albert II, 35 1030 Bruxelles, au travers d'au moins une des personnes suivantes :

Non	Prénom	Signature	*Contre-Signature le 12 juin 2014*

Pour l'IBPT :

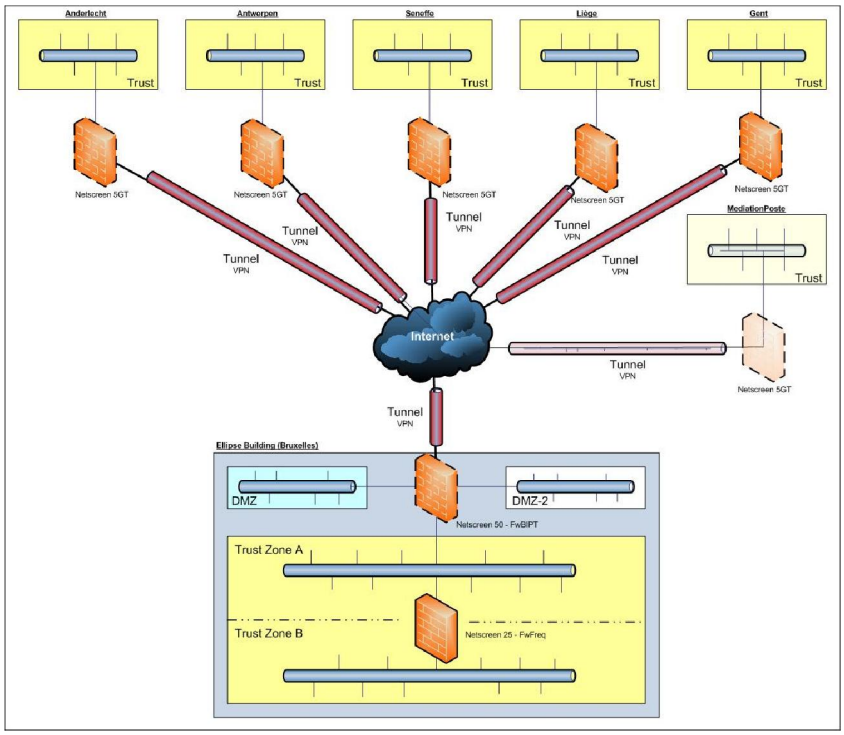
ou	
Vrancken Pascal Premier Informaticien-Conseiller	***Minne Steeve*** Premier Informaticien-Conseiller

A renvoyer, au plus tard, le vendredi 29 août à 15h00 à :
Institut belge des services postaux et des télécommunications (IBPT) - 35 Boulevard du Roi Albert II, 1030 Bruxelles – A l'attention de Pascal Vrancken (Fr) – Premier Informaticien Conseiller

D. NOTICE TECHNIQUE

1. L'existant et son « devenir »

L'IBPT offre dans sa structure réseau actuelle, le schéma suivant :



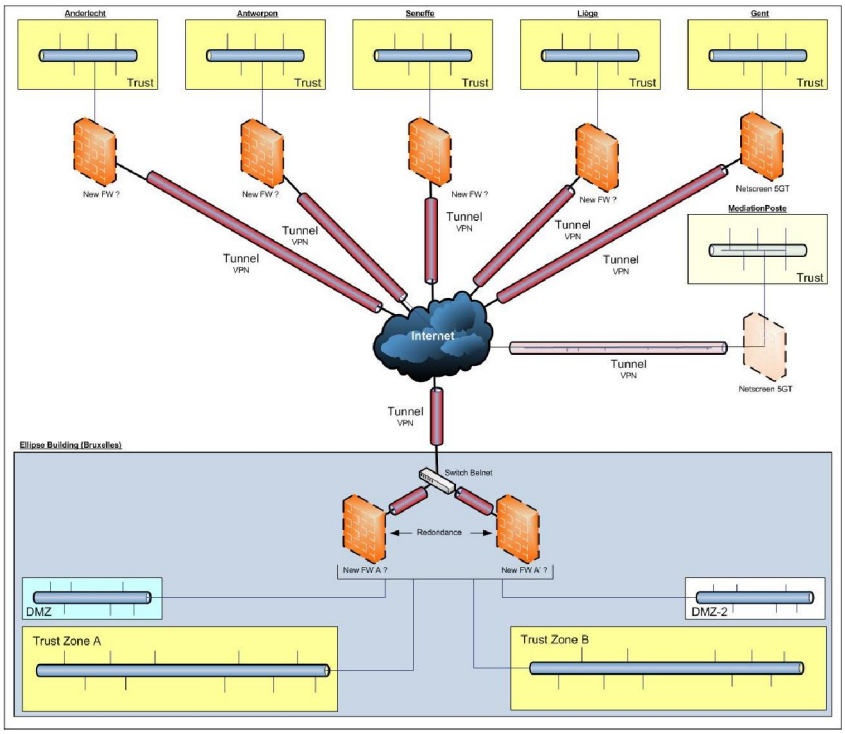
Celui-ci présente sur son site central (Ellipse Building – Bruxelles), une structure en 4 zones, départagées par 2 Firewall's (FW) Juniper ***Netscreen 50 & 25***.

Ce site central est interconnecté avec les centres de contrôles provinciaux de Anderlecht, Antwerpen, Gent, Liège et Seneffe, en tunnels VPN, avec des FW, modèles Juniper ***Netscreen 5GT***.

Ces 5 centres disposent de liaisons 5 Mbps, excepté Anderlecht qui dispose d'une liaison 10 Mbps ; le Site central disposant d'une ligne de 1 Gbps.

La sixième interconnexion VPN, également avec un NetScreen 5GT (*Mediation Poste*) n'est pas concernée par le présent marché.

Ces différents matériels (FW) n'étant plus supportés, le présent marché vise au remplacement de ceux-ci, dans le but d'amener la nouvelle structure suivante :



La différence résidant au niveau du site central, où les deux FW existants sont remplacés par 2 modèles identiques, autorisant la même découpe de zones, mais fonctionnant en « *redondance active – passive* » (HA) ; l'un prenant le relais de l'autre défaillant, vers la ligne d'entrée unique de 1 Gbps.

2. Fournitures

De manière générale, il est recherché une « Nouvelle Génération de FW » :

- Identifiant les applications, indépendamment des ports, du protocole, du chiffrement SSL ou toute autre technique d'évasion (App-ID) et autorisant :
    - un contrôle des différentes fonctions d'une même application (ex. SharePoint Admin & SharePoint Docs) ;
    - une gestion du trafic « inconnu » avec des règles ;
    - Identifiant / Contrôlant les applications partageant une même connexion ;
- Identifiant les utilisateurs, indépendamment de leur adresses IP (User-ID) ;
- Inspectant le contenu en temps réel (Content-ID) avec :
    - Système de prévention des intrusions ;
    - Antivirus réseau ;
    - Filtrage des URL ;

    - Filtrage des fichiers et de données ;

- Disposant d'une gestion simplifiée des stratégies ;
- Permettant une sécurisation de tous les utilisateurs, en déplacement ou en voyage, avec un niveau de sécurité cohérent qui s'étend du périmètre physique au périmètre logique (GlobalProtect) ;
- Fonctionnant par une combinaison de logiciels et de matériel, offrant des performances à faible latence et à haut débit avec tous les services qui seront activés
- Offrant une visibilité et un contrôle des règles, sur l'accès aux applications et leur fonctionnalités.

Ces nouveaux équipements devront néanmoins garantir une compatibilité de fonctionnement avec le FW NetScreen de la Médiation Poste, non repris par le présent marché.

Ceux-ci, afin de faciliter l'intégration des règles actuelles des FW en place, devront pouvoir supporter le « zone base » et « policy base control » ; être compatible IPv6 et supporter des vitesses jusqu'à 1Gb ou plus.

Ils devront pouvoir être gérés / configurés à partir d'un module de centralisation (*Central Managment*), *inclus dans le présent marché* ; et qui permettra à l'administrateur de savoir, en temps réel, ce qui se passe sur le réseau et, le cas échéant, lui permettra de déployer, de façon aisée, de nouvelles stratégies.

Bref, cette « Central Managment » permettra l'analyse, la journalisation, la création de rapports et l'investigation de ce qui se passe sur le réseau.

Détails

Chaque soumissionnaire, pour le matériel proposé, sera tenu d'indiquer très clairement, en quoi celui-ci diffère des critères demandés, énumérés ci-dessous. Ceci, que les valeurs soient supérieurs, ou inférieurs à ce qui est requis.

Il établira, pour chaque composant, un document énumérant les critères d'origines demandés, et les valeurs réelles du matériel proposé dans son offre.

En parallèle, il sera également fourni une documentation détaillées de chaque composant proposés

a) Site Central (nombre : 2)

Il sera fourni deux FW aux caractéristiques équivalentes ou supérieures au plus « gros » des deux Netscreen actuels (*Netscren 50*), permettant une redondance de connectivité en cas de défaillance de l'un d'eux (*HA - active/passive*).

Ceux-ci devront répondre au minimum aux caractéristiques suivantes :

PERFORMANCE AND CAPACITIES	
Firewall throughput (App-ID enabled)	2 Gbps
Threat prevention throughput	1 Gbps
IPSec VPN throughput	500 Mbps
New sessions per second	50,000
Max sessions	250,000
IPSec VPN tunnels/tunnel interfaces	1,000
GlobalProtect (SSL VPN) concurrent users	1,000
SSL decrypt sessions	7,936
SSL inbound certificates	25
Virtual routers	10
Virtual systems (base/max2)	1/6
Security zones	40
Max. number of policies	2500

HARDWARE SPECIFICATION

I/O
- 10/100/1000, SFP optical gigabit

MANAGEMENT I/O
- 10/100/1000 out-of-band management port, 10/100/1000 high availability, RJ-45 console port

STORAGE CAPACITY
- 120GB SSD

INPUT VOLTAGE (INPUT FREQUENCY)
- 100-240VAC (50-60Hz)

RACK MOUNTABLE (DIMENSIONS)
- 1U, 19” standard rack

NETWORKING

INTERFACE MODES
- L2, L3, Tap, Virtual wire (transparent mode)

ROUTING
- Modes: OSPF, RIP, BGP, Static
- Forwarding table size (entries per device/per VR): 2,500/2,500
- Policy-based forwarding
- Point-to-Point Protocol over Ethernet (PPPoE)
- Jumbo frames: 9,210 bytes max frame size
- Multicast: PIM-SM, PIM-SSM, IGMP v1, v2, and v3

HIGH AVAILABILITY
- Modes: Active/Active, Active/Passive
- Failure detection: Path monitoring, Interface monitoring

ADDRESS ASSIGNMENT
- Address assignment for device: DHCP Client/PPPoE/Static
- Address assignment for users: DHCP Server/DHCP Relay/Static

IPV6
- L2, L3, tap, virtual wire (transparent mode)
- Features: App-ID, User-ID, Content-ID, WildFire and SSL decryption

VLANS
- 802.1q VLAN tags per device/per interface: 4,094/4,094
- Max interfaces: 1,024
- Aggregate interfaces (802.3ad)

NAT/PAT
- Max NAT rules: 1,000
- Max NAT rules (DIPP): 200
- Dynamic IP and port pool: 254
- Dynamic IP pool: 16,234
- NAT Modes: 1:1 NAT, n:n NAT, m:n NAT
- DIPP oversubscription (Unique destination IPs per source port and IP): 2
- NAT64

VIRTUAL WIRE
- Max virtual wires: 512
- Interface types mapped to virtual wires: physical and subinterfaces

L2 FORWARDING
- ARP table size/device: 1,500
- MAC table size/device: 1,500
- IPv6 neighbor table size: 1,500

SECURITY

FIREWALL
- Policy-based control over applications, users and content
- Fragmented packet protection
- Reconnaissance scan protection
- Denial of Service (DoS)/Distributed Denial of Services (DDoS) protection
- Decryption: SSL (inbound and outbound), SSH

WILDFIRE
- Identify and analyze targeted and unknown files for more than 100 malicious behaviors
- Generate and automatically deliver protection for newly discovered malware via signature updates
- Signature update delivery in less than 1 hour, integrated logging/ reporting; access to WildFire API for programmatic submission of up to 100 samples per day and up to 1,000 report queries by file hash per day (Subscription Required)

FILE AND DATA FILTERING
- File transfer: Bi-directional control over more than 60 unique file types
- Data transfer: Bi-directional control over unauthorized transfer of CC# and SSN
- Drive-by download protection

USER INTEGRATION (USER-ID)
- Microsoft Active Directory, Novell eDirectory, Sun One and other LDAP-based directories
- Microsoft Windows Server 2003/2008/2008r2, Microsoft Exchange Server 2003/2007/2010
- Microsoft Terminal Services, Citrix XenApp
- XML API to facilitate integration with non-standard user repositories

IPSEC VPN (SITE-TO-SITE)
- Key Exchange: Manual key, IKE v1
- Encryption: 3DES, AES (128-bit, 192-bit, 256-bit)
- Authentication: MD5, SHA-1, SHA-256, SHA-384, SHA-512
- Dynamic VPN tunnel creation (GlobalProtect)

THREAT PREVENTION (SUBSCRIPTION REQUIRED)
- Application, operating system vulnerability exploit protection
- Stream-based protection against viruses (including those embedded in HTML, Javascript, PDF and compressed), spyware, worms

URL FILTERING (SUBSCRIPTION REQUIRED)
- Pre-defined and custom URL categories
- Device cache for most recently accessed URLs
- URL category as part of match criteria for security policies
- Browse time information

QUALITY OF SERVICE (QOS)

- Policy-based traffic shaping by application, user, source, destination, interface, IPSec VPN tunnel and more
- 8 traffic classes with guaranteed, maximum and priority bandwidth parameters
- Real-time bandwidth monitor
- Per policy diffserv marking
- Physical interfaces supported for QoS: 6

SSL VPN/REMOTE ACCESS (GLOBALPROTECT)

- GlobalProtect Gateway
- GlobalProtect Portal
- Transport: IPSec with SSL fall-back
- Authentication: LDAP, SecurID, or local DB
- Client OS: Mac OS X 10.6, 10.7 (32/64 bit), 10.8 (32/64 bit), Windows XP, Windows Vista (32/64 bit), Windows 7 (32/64 bit)
- Third party client support: Apple iOS, Android 4.0 and greater, VPNC IPSec for Linux

MANAGEMENT, REPORTING, VISIBILITY TOOLS

- Integrated web interface, CLI or central management (Panorama) Multi-language user interface
- Syslog, Netflow v9 and SNMP v2/v3
- XML-based REST API
- Graphical summary of applications, URL categories, threats and data (ACC)
- View, filter and export traffic, threat, WildFire, URL, and data filtering logs
- Fully customizable reporting

b) Site Provinciaux (nombre : 5)

Il sera fourni, par centre, un modèle de FW équivalent ou supérieur aux modèles existants (*Netscreen 5GT*)

Ceux-ci devront répondre au caractéristiques suivantes :

PERFORMANCE AND CAPACITIES	
Firewall throughput (App-ID enabled)	100 Mbps
Threat prevention throughput	50 Mbps
IPSec VPN throughput	50 Mbps
New sessions per second	1,000
Max sessions	64,000
IPSec VPN tunnels/tunnel interfaces	250
IPSEc VPN Tunnels/	
GlobalProtect (SSL VPN) concurrent users	25
SSL decrypt sessions	1000
SSL inbound certificates	25
Virtual routers	3
Security zones	10
Max. number of policies	250

HARDWARE SPECIFICATIONS

I/O
- 10/100/1000

MANAGEMENT I/O
- 10/100 out-of-band management port, RJ-45 console port

STORAGE CAPACITY
- 16GB SSD

INPUT VOLTAGE (INPUT FREQUENCY)
- 100-240VAC (50-60Hz)

NETWORKING

INTERFACE MODES
- L2, L3, Tap, Virtual wire (transparent mode)

ROUTING
- Modes: OSPF, RIP, BGP, Static
- Forwarding table size (entries per device/per VR):1,000/1,000
- Policy-based forwarding
- Point-to-Point Protocol over Ethernet (PPPoE)
- Multicast: PIM-SM, PIM-SSM, IGMP v1, v2, and v3

HIGH AVAILABILITY
- Active/Passive with no session synchronization
- Failure detection: Path monitoring, Interface monitoring

ADDRESS ASSIGNMENT
- Address assignment for device: DHCP Client/PPPoE/Static

• Address assignment for users: DHCP Server/DHCP Relay/Static IPV6
• Features: L2, L3, Tap, Virtual Wire (transparent mode)
• Services: App-ID, User-ID, Content-ID, WildFire and SSL Decryption

VLANS
• 802.1q VLAN tags per device/per interface: 4,094/4,094
• Max interfaces: 100

NAT/PAT
• Max NAT rules: 125
• Max NAT rules (DIPP): 125
• Dynamic IP and port pool: 254
• Dynamic IP pool: 16,234
• NAT Modes: 1:1 NAT, n:n NAT, m:n NAT
• DIPP oversubscription (Unique destination IPs per source port and IP): 1
• NAT64

VIRTUAL WIRE
• Max virtual wires: 50
• Interface types mapped to virtual wires: physical and subinterfaces

L2 FORWARDING
• ARP table size/device: 500
• MAC table size/device: 500
• IPv6 neighbor table size: 500

SECURITY

FIREWALL
• Policy-based control over applications, users and content
• Fragmented packet protection
• Reconnaissance scan protection
• Denial of Service (DoS)/Distributed Denial of Services (DDoS) protection
•Decryption: SSL (inbound and outbound), SSH

WILDFIRE
• Identify and analyze targeted and unknown files for more than 100 malicious behaviors
• Generate and automatically deliver protection for newly discovered malware via signature updates
• Signature update delivery in less than 1 hour, integrated logging/ reporting; access to WildFire API for programmatic submission of up to 100 samples per day and up to 1,000 report queries by file hash per day (Subscription Required)

FILE AND DATA FILTERING
• File transfer: Bi-directional control over more than 60 unique file types
• Data transfer: Bi-directional control over unauthorized transfer of CC# and SSN

- Drive-by download protection

USER INTEGRATION (USER-ID)

- Microsoft Active Directory, Novell eDirectory, Sun One and other LDAP-based directories
- Microsoft Windows Server 2003/2008/2008r2, Microsoft Exchange Server 2003/2007/2010
- Microsoft Terminal Services, Citrix XenApp
- XML API to facilitate integration with non-standard user repositories

IPSEC VPN (SITE-TO-SITE)

- Key Exchange: Manual key, IKE v1
- Encryption: 3DES, AES (128-bit, 192-bit, 256-bit)
- Authentication: MD5, SHA-1, SHA-256, SHA-384, SHA-512
- Dynamic VPN tunnel creation (GlobalProtect)

THREAT PREVENTION (SUBSCRIPTION REQUIRED)

- Application, operating system vulnerability exploit protection
- Stream-based protection against viruses (including those embedded in HTML, Javascript, PDF and compressed), spyware, worms

URL FILTERING (SUBSCRIPTION REQUIRED)

- Pre-defined and custom URL categories
- Device cache for most recently accessed URLs
- URL category as part of match criteria for security policies
- Browse time information

QUALITY OF SERVICE (QOS)

- Policy-based traffic shaping by application, user, source, destination, interface, IPSec VPN tunnel and more
- 8 traffic classes with guaranteed, maximum and priority bandwidth parameters
- Real-time bandwidth monitor
- Per policy diffserv marking
- Physical interfaces supported for QoS: 4

SSL VPN/REMOTE ACCESS (GLOBALPROTECT)

- GlobalProtect Gateway
- GlobalProtect Portal
- Transport: IPSec with SSL fall-back
- Authentication: LDAP, SecurID, or local DB
- Client OS: Mac OS X 10.6, 10.7 (32/64 bit), 10.8 (32/64 bit), Windows XP, Windows Vista (32/64 bit), Windows 7 (32/64 bit)
- Third party client support: Apple iOS, Android 4.0 and greater, VPNC IPSec for Linux

MANAGEMENT, REPORTING, VISIBILITY TOOLS

- Integrated web interface, CLI or central management
- Multi-language user interface
- Syslog, Netflow v9 and SNMP v2/v3
- XML-based REST API
- Graphical summary of applications, URL categories, threats and data (ACC)

• View, filter and export traffic, threat, WildFire, URL, and data filtering logs
• Fully customizable reporting

c) « Central Managment » (nombre : 1)

SPECIFICATIONS

Number of devices supported : Up to 1,000
High Availability : Active/Passive
Administrator authentication : Local database, RADIUS

MANAGEMENT APPLIANCE SPECIFICATIONS

I/O
• 10/100/1000, 10/100/1000 (for future use), DB9 Console serial port
STORAGE
• M-100 1TB RAID: 2 x 1TB RAID Certified HDD for 1TB of RAID Storage
• M-100 4TB RAID: 8 x 1TB RAID Certified HDD for 4TB of RAID Storage
INPUT VOLTAGE (INPUT FREQUENCY)
• 100-240VAC (50-60Hz)
RACK MOUNTABLE (DIMENSIONS)
• 1U, 19" standard rack

3. Services (Support / Maintenance)

1. A la commande, le soumissionnaires procèdera à une analyse de la sécurité existante et procédera, après amélioration éventuelle, en accord avec les responsable du service IT, à sa mise en place sur les nouveaux appareillages ; l'installation sur site faisant partie intégrante de la mission du soumissionnaire.

   Il configurera également la partie « HA » des deux éléments du site central, ainsi que le « Central Managment ».

   Le tout, en perturbation minime sur le fonctionnement des services de l'Institut.

2. Le soumissionnaire fournira une formation sur la nouvelle technologie mise en place, en mettant l'accent sur les méthodes de réflexion à adopter pour améliorer la sécurité de l'Institut. Il fournira une méthode de sauvegarde de la configuration en place, avec également un plan de restauration en cas de désastre.

   Cette formation de 1 jours maximum, concernera 5 membres de l'IBPT, en français ou en néerlandais.

3. Le soumissionnaire proposera au maître d'ouvrage, un contrat optionnel de services (Support / Maintenance)– max. 5 ans, couvrant la réparation des pannes, les entretiens et la maintenance de l'infrastructure FW ; voir aussi, le remplacement intégral d'un « Device » en cas de défectuosité de l'un d'eux .

   Le soumissionnaire s'engage à intervenir pendant les heures de bureau, dans les 24 heures (un jour) et fournira un numéro de téléphone unique permettant de faire un appel d'intervention. Cet appel permettra de mettre à disposition un expert au téléphone dans les deux minutes après l'appel. La langue utilisée pour cet appel téléphonique sera soit le français ou le néerlandais.

   Ce contrat de services comprendra également la mise à disposition d'un expert pour toutes questions de sécurité, pour une durée maximale de 10 heures par an, reconductible pour les heures non utilisées.

   Tout upgrade critique du matériels, mettant en jeu la sécurité de l'Institut, fera l'objet d'une installation dans un délai maximum de 3 jours ouvrables.

4. Le soumissionnaire y réalisera également, bi-annuellement, une analyse globale de la sécurité (flux). Les résultats de cette analyse feront l'objet d'un rapport qui comprendra au minimum une analyse de la situation existante ainsi que les améliorations de « stratégies » conseillées.

Ce rapport sera remis et commenté à l'Institut lors d'une réunion fixée avec les responsables informatiques. Après approbation, le soumissionnaire en configurera les éléments concernés par ces améliorations.

Ces différents services de Support /Maintenance seront proposé annuellement, et reconductible pendant maximum 5 ans.