

**ROYAUME DU MAROC**  
**OFFICE DE LA FORMATION PROFESSIONNELLE**  
**ET DE LA PROMOTION DU TRAVAIL**

\*==\*==\*==\*

**AVIS RECTIFICATIF DE L'APPEL D'OFFRES**  
**OUVERT N° 191 / 2022**

L'Office de la Formation Professionnelle et de la Promotion du Travail porte à la connaissance du public que des modifications, ci-après, ont été apportées à l'avis d'appel d'offres ouvert n° 191/2022, relatif à **La refonte des solutions réseaux (LAN/WAN) et de sécurité au niveau du siège, annexes du siège et des directions régionales. Réparti en lots suivants :**

- **Lot n°1 : Solutions Switching, Wifi et SDN pour le siège OFPPT, annexes siège et directions régionales**
- **Lot n°2 : Solutions Firewall et SDWAN pour le siège, annexes siège et directions régionales**

- 1. Une modification a été apportée à l'avis d'appel d'offres ; La date de la séance d'ouverture des plis est prévue pour le 31 Janvier 2023 à 12 Heures 30min.**

Le dossier d'appel d'offres rectifié peut être retiré à la Direction de l'Approvisionnement et la Logistique (Service des Marchés), sis Intersection de la Route BO n° 50 et la R.N.11 (Route Nouaceur Sidi Maârouf) Casablanca, il peut être également téléchargé à partir du portail des marchés de l'Etat [www.marchéspublics.gov.ma](http://www.marchéspublics.gov.ma) et du site de l'Office de la Formation Professionnelle et de la Promotion du Travail : [www.ofppt.ma](http://www.ofppt.ma).

\* Les autres termes et conditions restent inchangés.

المملكة المغربية المملكة المغربية  
مكتب التكوين المهني وإنعاش الشغل

\*\*\*\*\*

إعلان تصحيحي لطلب العروض المفتوح  
رقم 191/2022

- ينهي مكتب التكوين المهني وإنعاش الشغل إلى علم العموم أنه قد أجريت تغييرات على طلب العروض المفتوح رقم 191/2022 ، لأجل إصلاح الشبكة ( LAN / WAN ) والحلول الأمنية في المقر الرئيسي وملحقات المقر والإدارات الجهوية. موزعة على الحصص كالتالي:
- الحصة الأولى: حلول التبديل، Wifi و SDN لمقر مكتب التكوين المهني و إنعاش الشغل ومرفقات المقر والإدارات الجهوية.
  - الحصة الثانية: حلول جدار الحماية و SDWAN للمقر الرئيسي وملحقات المقر الرئيسي والإدارات الجهوية.

1- قد أجريت تغييرات على طلب العروض المفتوح تتعلق بتاريخ فتح الأظرفة : في يوم 31 يناير 2023 على الساعة الثانية عشرة و النصف صباحا.

يمكن سحب ملف طلب العروض المصحح بمصلحة الصفقات بمديرية التموين واللوجستيك الكائنة بملتقى طريق 50 BO والطريق الوطنية رقم 11 (طريق النواصر – سيدي معروف) - الدار البيضاء ، كما يمكن كذلك سحبه إلكترونيا من بوابة صفقات الدولة : [www.marchéspublics.gov.ma](http://www.marchéspublics.gov.ma) . وكذا من بوابة مكتب التكوين المهني وإنعاش الشغل على العنوان التالي: [www.ofppt.ma](http://www.ofppt.ma).

- وأن جميع الشروط والمتطلبات الأخرى تبقى بدون تغيير.

**ROYAUME DU MAROC**

**\*\*\_\*\*\_\*\*\_\*\*\_\*\***

**OFFICE DE LA FORMATION PROFESSIONNELLE  
ET DE LA PROMOTION DU TRAVAIL**

**AVIS D'APPEL D'OFFRES OUVERT N° 191/2022**

Le **10 Janvier 2023 à 10 Heures**, Il sera procédé, dans les bureaux de l'office de la Formation Professionnelle et de la Promotion du Travail, sis Intersection de la Route BO n° 50 et la R.N.11 (Route Nouaceur Sidi Maârouf) - Casablanca à l'ouverture des plis relatifs à l'appel d'offres sur offres de prix, ayant pour objet **La refonte des solutions réseaux (LAN/WAN) et de sécurité au niveau du siège, annexes du siège et des directions régionales. Réparti en lots suivants :**

- **Lot n°1 : Solutions Switching, Wifi et SDN pour le siège OFPPT, annexes siège et directions régionales**
- **Lot n°2 : Solutions Firewall et SDWAN pour le siège, annexes siège et directions régionales**

Le dossier d'appel d'offres peut être retiré au service des marchés à la Direction de l'Approvisionnement et la Logistique, sis Intersection de la Route BO n° 50 et la R.N.11 (Route Nouaceur SidiMaârouf) Casablanca, il peut être également téléchargé à partir du portail des marchés de l'Etat [www.marchéspublics.gov.ma](http://www.marchéspublics.gov.ma). Et à partir du site de l'office de la Formation Professionnelle et de la Promotion du Travail : [www.ofppt.ma](http://www.ofppt.ma).

Les cautions provisoires sont fixées à la somme de :

- **Lot n°1 : Cent dix mille Dirhams (110 000.00 DH)**
- **Lot n°2 : Trente-deux mille Dirhams (32 000.00 DH)**

Les estimations des coûts des prestations établies par le Maître d'ouvrage sont fixées à la somme de :

- **Lot n°1 : Six millions neuf cent vingt-cinq mille deux cents Dirhams (6 925 200.00 DH) en TTC.**
- **Lot n°2 : Deux millions cent vingt mille et quatre cent Dirhams (2 120 400.00 DH) en TTC.**

Le contenu, la présentation ainsi que le dépôt des dossiers des concurrents doivent être conformes aux dispositions des articles 27, 29 et 31 du Règlement des Marchés de l'OFPPT.

Les concurrents peuvent :

- ❖ soit envoyer, par courrier recommandé avec accusé de réception, au bureau précité ;
- ❖ soit déposer contre récépissé leurs plis dans le bureau du service des marchés rattaché à la Direction de l'Approvisionnement et la Logistique, sis Intersection de la Route BO n° 50 et la R.N.11 (Route Nouaceur Sidi Maârouf) - Casablanca ;
- ❖ soit les remettre au président de la commission d'appel d'offres au début de la séance et avant l'ouverture des plis.
- ❖ Soit transmis par voie électronique conformément aux dispositions de l'arrêté du ministère de l'économie et des finances n°20-14 du 8 kaada 1435 (4 septembre 2014) relatif à la dématérialisation des procédures de passation des marchés publics.

Les pièces justificatives à fournir sont celles prévues par l'article n° 5 du règlement de consultation

المملكة المغربية  
مكتب التكوين المهني وإنعاش الشغل  
إعلان عن طلب عروض أثمان مفتوح  
رقم 2022/191

في يوم 10 يناير 2023 على الساعة العاشرة صباحا، سيتم في مكتب الإدارة العامة لمكتب التكوين المهني وإنعاش الشغل الكائن بملتقى طريق BO. 50 والطريق الوطنية رقم 11 (طريق النواصر – سيدي معروف) - الدار البيضاء، فتح الأظرفة المتعلقة بطلب عروض الأثمان المفتوح، لأجل إصلاح الشبكة (LAN / WAN) والحلول الأمنية في المقر الرئيسي وملحقات المقر والإدارات الجهوية. موزعة على الحصص كالتالي:

- الحصة الأولى: حلول التبدل، Wifi و SDN لمقر مكتب التكوين المهني وإنعاش الشغل ومرفقات المقر والإدارات الجهوية.
- الحصة الثانية: حلول جدار الحماية و SDWAN للمقر الرئيسي وملحقات المقر الرئيسي والإدارات الجهوية.

يمكن سحب ملف طلب العروض بمصلحة الصفقات بديرية التموين واللوجستيك الكائنة بملتقى طريق BO. 50 والطريق الوطنية رقم 11 (طريق النواصر – سيدي معروف) - الدار البيضاء، كما يمكن كذلك سحبه إلكترونيا من بوابة صفقات الدولة: [www.marchéspublics.gov.ma](http://www.marchéspublics.gov.ma) وكذا من بوابة مكتب التكوين المهني وإنعاش الشغل على العنوان التالي: [www.ofppt.ma](http://www.ofppt.ma).

وتبلغ الضمانة المؤقتة:

- الحصة الأولى: مائة وعشرة آلاف درهم (110 000,00)

- الحصة الثانية: اثنان وثلاثون ألف درهم (32 000,00)

والكلفة التقديرية للأعمال المحددة من طرف صاحب المشروع تبلغ :

- الحصة الأولى: ستة ملايين وتسعمائة وخمسة وعشرون ألفا ومئتان درهم (6 925 200,00) مع احتساب جميع الرسوم.
- الحصة الثانية: مليونان ومائة وعشرون ألف وأربعمائة درهم (2 120 400,00) مع احتساب جميع الرسوم.

يجب أن يكون كل من محتوى وتقديم ملفات المتنافسين مطابقين لمقتضيات المواد 27، 29 و 31 من نظام الصفقات الخاص بمكتب التكوين المهني وإنعاش الشغل.

ويمكن للمتنافسين :

- إما إرسالها عن طريق البريد المضمون بإفادة بالاستلام إلى المكتب المذكور؛
- إما إيداع أظرفتهم مقابل وصل، بمكتب مصلحة الصفقات بديرية التموين واللوجستيك الكائنة بملتقى طريق BO. 50 والطريق الوطنية رقم 11 (طريق النواصر – سيدي معروف) - الدار البيضاء؛
- إما تسليمها مباشرة لرئيس لجنة طلب العروض عند بداية الجلسة وقبل فتح الأظرفة.
- إما إيداع أظرفتهم الكترونيا عبر بوابة الصفقات العمومية وفقا لمقتضيات مرسوم وزارة الاقتصاد و المالية رقم 14-20 (4 شتنبر 2014) ل 8 دوالقعدة 1435 المتعلق بتجريد مساطر الصفقات العمومية من الصفة المادية.

إن الوثائق المثبتة الواجب الإدلاء بها هي تلك المقررة في المادة 5 من نظام الإستشارة.



مكتب التكوين المهني وإنعاش الشغل

Office de la Formation Professionnelle et de la  
Promotion du Travail

Dossier d'Appel  
D'offres

Ouvert sur offres de prix

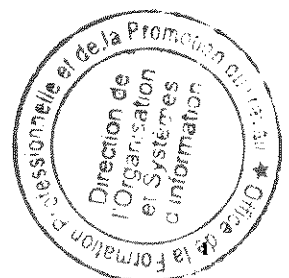
N° 191 / 2022

Financement : Projets OFPPT Hors Coopération

**La refonte des solutions réseaux (LAN/WAN) et de sécurité au niveau  
du siège, annexes du siège et des directions régionales.**

**Réparti en lots suivants :**

- **Lot 1 :** Solutions Switching, Wifi et SDN pour le Siège OFPPT, annexes siège et directions régionales.
- **Lot 2 :** Solutions Firewall et SDWAN pour le siège, annexes siège et directions régionales.



A. Y

## REGLEMENT DE LA CONSULTATION

\*\*\*\*\*

### Article n°1 : Objet du règlement de la consultation

Le présent règlement de consultation concerne l'appel d'offres ouvert sur offres des prix ayant pour objet de :  
La refonte des solutions réseaux (LAN/WAN) et de sécurité au niveau du siège, annexes du siège et des directions régionales. Réparti en lots suivants :

- **Lot 1 : Solutions Switching, Wifi et SDN pour le Siège OFPPT, annexes siège et directions régionales.**
- **Lot 2 : Solutions Firewall et SDWAN pour le siège, annexes siège et directions régionales.**

Il est établi en vertu des dispositions de l'article n°18, du règlement des marchés, approuvé le 18 Chaabane 1435 (16 Juin 2014), relatif aux marchés publics de l'Office de la Formation Professionnelle et de la Promotion du Travail (OFPPT).

Les prescriptions du présent règlement ne peuvent en aucune manière déroger ou modifier les conditions et les formes prévues par le règlement des marchés de l'OFPPT. Toute disposition contraire au règlement des marchés de l'OFPPT est nulle et non avenue. Seules sont valables les précisions et prescriptions complémentaires conformes aux dispositions de l'article n°18 et des autres articles du règlement des marchés de l'OFPPT.

### Article n°2 : Maître d'ouvrage

Le maître d'ouvrages du marché qui sera passé suite au présent appel d'offres est : **l'Office de la Formation Professionnelle et de la Promotion du Travail (OFPPT).**

### Article n°3 : Définitions :

Au sens du règlement des marchés de l'OFPPT on entend par :

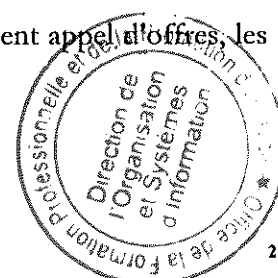
- 1- **Attributaire** : concurrent dont l'offre a été retenue avant la notification de l'approbation du marché ;
- 2- **Autorité compétente** : l'ordonnateur ou la personne déléguée (sous-ordonnateur) par lui pour approuver le marché ;
- 3- **Concurrent** : toute personne physique ou morale qui propose une offre en vue de la conclusion d'un marché ;
- 4- **Groupeement** : deux ou plusieurs concurrents qui souscrivent un engagement unique dans les conditions prévues à l'article 140 du règlement des marchés publics de l'OFPPT ;
- 5- **Titulaire** : attributaire auquel l'approbation du marché a été notifiée.

### Article n°4 : Conditions requises des concurrents

Conformément aux dispositions de l'article n°24 du Règlement des Marchés de l'OFPPT :

Peuvent valablement participer et être attributaire(s) de(s) marché(s) afférent(s) au présent appel d'offres, les personnes physiques ou morales, qui :

- a) Justifient des capacités juridiques, techniques et financières requises ;



2

- b) Sont en situation fiscale régulière, pour avoir souscrit leurs déclarations et réglé les sommes exigibles dûment définitives ou, à défaut de règlement, constitué des garanties jugées suffisantes par le comptable chargé du recouvrement, et ce conformément à la législation en vigueur en matière de recouvrement ;
- c) Sont affiliées à la Caisse Nationale de Sécurité Sociale ou à un régime particulier de prévoyance sociale, et souscrivent de manière régulière leurs déclarations de salaires et sont en situation régulière auprès de ces organismes.

Ne sont pas admises à participer aux appels d'offres :

- Les personnes en liquidation judiciaire ;
- Les personnes en redressement judiciaire, sauf autorisation spéciale délivrée par l'autorité judiciaire compétente ;
- Les personnes ayant fait l'objet d'une exclusion temporaire ou définitive prononcée dans les conditions fixées par l'article n°142 du Règlement des Marchés de l'OFPPT.
- Les personnes qui représentent plus d'un concurrent dans une même procédure de passation de marchés.

#### **Article n°5: Justification des capacités et des qualités des concurrents**

- I- Chaque concurrent est tenu de présenter un dossier administratif et un dossier technique. Chaque dossier peut être accompagné d'un état des pièces qui le constituent.

A- Le dossier administratif comprend :

1. Pour chaque concurrent, au moment de la présentation des offres :

- a) Une déclaration sur l'honneur, en un exemplaire unique, établie conformément au modèle joint en annexe.
- b) L'original du récépissé du cautionnement provisoire ou l'attestation de la caution personnelle et solidaire en tenant lieu, le cas échéant. En cas de groupement, le cautionnement provisoire doit être constitué conformément aux dispositions du § C de l'article n°140 du Règlement des Marchés de l'OFPPT.

**N.B :** 1- Les cautions personnelles et solidaires doivent être choisies parmi les établissements agréés à cet effet par le ministre chargé des finances Marocain (pour les candidats étrangers, ces cautions personnelles et solidaires doivent être avalisées par une banque marocaine).

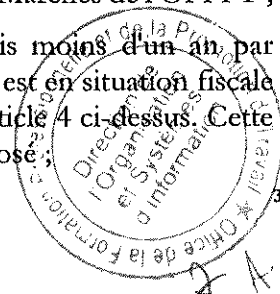
2- Les pièces a et b ne doivent exprimer aucune restriction ou réserve sous peine d'être rejetées par la commission d'appel d'offres.

**Pour les groupements**, il y a lieu de produire :

- + Une copie légalisée de la convention constitutive du groupement prévue à l'article n°140 du Règlement des Marchés de l'OFPPT.
- + Une note indiquant notamment l'objet de la convention, la nature du groupement, le mandataire, la durée de la convention, la répartition des prestations, le cas échéant.

2. Pour le concurrent auquel il est envisagé d'attribuer le marché, dans les conditions fixées à l'article 40 du Règlement des Marchés de l'OFPPT :

- a) La ou les pièces justifiant les pouvoirs conférés à la personne agissant au nom du concurrent et ce conformément à l'alinéa a) du paragraphe 2 de l'article n°25 du Règlement des Marchés de l'OFPPT ;
- b) Une attestation ou sa copie certifiée conforme à l'originale délivrée depuis moins d'un an par l'Administration compétente du lieu d'imposition certifiant que le concurrent est en situation fiscale régulière ou à défaut de paiement qu'il a constitué les garanties prévues à l'article 4 ci-dessus. Cette attestation doit mentionner l'activité au titre de laquelle le concurrent est imposé ;



- c) une attestation ou sa copie certifiée conforme à l'originale délivrée depuis moins d'un an par la Caisse nationale de sécurité sociale certifiant que le concurrent est en situation régulière envers cet organisme conformément aux dispositions prévues à cet effet à l'article 4 ci-dessus ou de la décision du ministre chargé de l'emploi ou sa copie certifiée conforme à l'originale, prévue par le dahir portant loi n° 1-72-184 du 15 joumada II 1392 (27 juillet 1972) relatif au régime de sécurité sociale assortie de l'attestation de l'organisme de prévoyance sociale auquel le concurrent est affilié et certifiant qu'il est en situation régulière vis-à-vis dudit organisme ;

\* La date de production des pièces prévues aux b) et c) ci-dessus sert de base pour l'appréciation de leur validité.

- d) Le certificat d'immatriculation au registre de commerce pour les personnes assujetties à l'obligation d'immatriculation conformément à la législation en vigueur ;

**Pour, les concurrents non installés au Maroc :** l'équivalent des attestations visées aux paragraphes b, c et d ci-dessus, délivrées par les administrations ou les organismes compétents de leurs pays d'origine ou de provenance pour les concurrents non installés au Maroc.

A défaut de la délivrance de tels documents par les administrations ou les organismes compétents de leur pays d'origine ou de provenance, lesdites attestations peuvent être remplacées par une attestation délivrée par une autorité judiciaire ou administrative du pays d'origine ou de provenance certifiant que ces documents ne sont pas produits ou par une déclaration sur l'honneur dûment certifiée par les autorités compétentes du pays d'origine attestant l'impossibilité de produire l'ensemble ou une partie des documents précités.

#### **B - Le dossier technique comprend :**

1. Une note indiquant les moyens humains et techniques du concurrent et mentionnant éventuellement, le lieu, la date, la nature et l'importance des prestations à l'exécution desquelles le concurrent a participé et la qualité de sa participation.
2. Les attestations ou leurs copies certifiées conformes à l'originale délivrées par les maîtres d'ouvrage publics ou privés ou par les hommes de l'art sous la direction desquels le concurrent a exécuté des prestations de mêmes familles. Chaque attestation précise notamment la nature des prestations, leur montant et l'année de la réalisation ainsi que le nom et la qualité du signataire et son appréciation. (Cf pp 15)

#### **C - Le dossier additif comprend :**

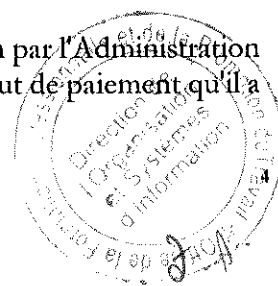
1. Une attestation de(s) constructeur(s) et ou éditeur(s) (maison mère, représentant Régional ou local) certifiant que le soumissionnaire est agréé de commercialiser et d'installer le matériel et logiciel proposés portant sa marque pour les équipements proposés.
2. Une attestation d'agrément du service après-vente du soumissionnaire pour réparer le matériel proposé, fournie par le constructeur ou son représentant régional ou local.
3. Une attestation constructeur de non obsolescence pour le HARDWARE indiquant que les articles proposés ne font l'objet d'aucune annonce de fin de vie et de commercialisation, et que le support sera disponible pour minimum 5 ans.

#### **Article n°6 : Documents à fournir par les établissements publics**

Lorsque le concurrent est un établissement public, il doit fournir :

1. Au moment de la présentation de l'offre, outre le dossier technique et en plus des pièces prévues à l'alinéa 1) du I-A de l'article 5 ci-dessus, une copie du texte l'habilitant à exécuter les prestations objet du marché ;
2. S'il est retenu pour être attributaire du marché :

a) une attestation ou sa copie certifiée conforme à l'original délivrée depuis moins d'un an par l'Administration compétente du lieu d'imposition certifiant qu'il est en situation fiscale régulière ou à défaut de paiement qu'il a





constitué les garanties prévues à l'article 4 ci-dessus. Cette attestation, qui n'est exigée que pour les organismes soumis au régime de la fiscalité, doit mentionner l'activité au titre de laquelle le concurrent est imposé ;

b) une attestation ou sa copie certifiée conforme à l'originale délivrée depuis moins d'un an par la Caisse nationale de sécurité sociale certifiant que le concurrent est en situation régulière envers cet organisme conformément aux dispositions prévues à cet effet à l'article 4 ci-dessus ou de la décision du ministre chargé de l'emploi ou sa copie certifiée conforme à l'originale, prévue par le dahir portant loi n° 1-72-184 du 15 joumada II 1392 (27 juillet 1972) relatif au régime de sécurité sociale assortie de l'attestation de l'organisme de prévoyance sociale auquel le concurrent est affilié et certifiant qu'il est en situation régulière vis-à-vis dudit organisme.

La date de production des pièces prévues aux a) et b) ci-dessus sert de base pour l'appréciation de leur validité.

### **Article n°7 : Contenu des dossiers des concurrents**

Les dossiers présentés par les concurrents doivent comporter :

7.1 - **les dossiers administratifs, techniques et additifs prévus** à l'article 5 ci-dessus.

7.2- **une offre technique** :

Les pièces devant constituer l'offre technique sont :

- a. Les « spécifications techniques des fournitures » renseignés conformément au canevas prévu à l'annexe du cahier des prescriptions spéciales et ce, en faisant ressortir les caractéristiques des fournitures proposées par le concurrent, leurs marques et leurs références. Cette annexe est signée par le concurrent et étayée par les catalogues et/ou documents relatifs aux « spécifications techniques des fournitures » afférents aux fournitures proposées. Ces catalogues et/ou documents relatives aux « spécifications techniques des fournitures » doivent être cachetés sur toutes les pages et portant le numéro de l'appel d'offres et l'item correspondant ;
- b. Une proposition d'au moins (01) un ingénieur de niveau BAC + 4 minimum, ayant une expérience de 5 ans minimum après obtention du diplôme demandé, (02) deux techniciens de niveau BAC + 2 minimum, ayant une expérience de 3 ans minimum après obtention du diplôme demandé et un chef de projet de niveau BAC +4, ayant une expérience de 5 ans minimum dans le secteur d'activité objet du présent Appel d'offres ;
- c. Cette proposition doit contenir les CV, les diplômes et l'état de déclaration des salaires à la CNSS des 3 derniers mois ;
- d. Une note sur le service après-vente avec proposition de profil pour le support ;

Il est à noter que :

- Pour le cas d'un groupement, les documents relatifs à l'offre technique sont à signer par l'ensemble des membres du groupement, soit seulement par le mandataire si celui-ci justifie des habilitations sous forme de procurations légalisées pour représenter les membres du groupement lors de la procédure de passation du marché.
- Pour les pièces de l'offre technique de la solution variante, les mêmes pièces sont exigées et ce, pour les fournitures proposées au titre de la solution variante.

7.3 - **Une offre financière** qui comprend :

a) l'acte d'engagement par lequel le concurrent s'engage à réaliser les prestations objet du marché conformément aux conditions prévues aux cahiers des charges et moyennant un prix qu'il propose. Il est établi en un seul exemplaire conformément au modèle joint au présent règlement.



Cet acte d'engagement dûment rempli, et comportant le relevé d'identité bancaire (RIB), est signé par le concurrent ou son représentant habilité, sans qu'un même représentant puisse représenter plus d'un concurrent à la fois pour le même marché.

Lorsque l'acte d'engagement est souscrit par un groupement tel qu'il est défini à l'article 140 du Règlement des Marchés de l'OFPPT, il doit être signé soit par chacun des membres du groupement ; soit seulement par le mandataire si celui-ci justifie des habilitations sous forme de procurations légalisées pour représenter les membres du groupement lors de la procédure de passation du marché.

b) le bordereau des prix - détail estimatif établi par le maître d'ouvrage et figurant dans le dossier d'appel d'offres.

Le montant total de l'acte d'engagement doit être libellé en chiffres et en toutes lettres.

Le bordereau des prix - détail estimatif doit tenir compte de :

- + La saisie doit se faire par les moyens numériques (non manuscrits).
- + Les prix unitaires doivent être libellés en chiffres.
- + Les montants totaux doivent être libellés en chiffres.

En cas de discordance entre le montant total de l'acte d'engagement, et de celui du bordereau des prix-détail estimatif, le montant de ce dernier document est tenu pour bon pour établir le montant réel de l'acte d'engagement.

7.4 - Le cahier des prescriptions spéciales paraphé et signé par le concurrent ou son représentant dûment habilité à cet effet.

#### **Article n°8 : Offre variante.**

Des variantes pourront être proposées par les concurrents.

La présentation des variantes n'implique pas l'obligation pour le soumissionnaire de présenter une offre pour la solution de base initialement prévue.

Les modalités d'examen des offres de base seront effectuées conformément aux spécifications techniques des fournitures proposées annexé au cahier des prescriptions spéciales.

Les modalités d'examen des offres variantes seront effectuées de la même manière que l'offre technique de base.

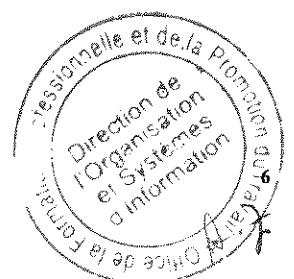
Les offres variantes présentées par les concurrents font l'objet d'un pli distinct de l'offre de base éventuellement proposée. Dans ce cas, les pièces du dossier administratif visées à l'alinéa 1) du paragraphe I-A de l'article 5 et de l'article 6 ci-dessus, le dossier technique est valable aussi bien pour la solution de base que pour les offres variantes.

Dans le cas où le concurrent ne présente qu'une offre variante, le pli contenant celle-ci doit être présentée conformément à l'article 13 ci-dessous, accompagnée des dossiers prévus à l'article 7 ci-dessus, ainsi que le cahier des prescriptions spéciales paraphé et signé par le concurrent ou son représentant dûment habilité à cet effet et doit porter en outre la mention " offre variante".

#### **Article n°9 : Composition du dossier d'appel d'offres.**

Conformément aux dispositions de l'article 19 du règlement des marchés de l'OFPPT, le dossier d'appel d'offres comprend :

- a) Une copie de l'avis d'appel d'offres ouvert ;
- b) Un exemplaire du cahier des prescriptions spéciales ;
- c) Le modèle de l'acte d'engagement visé à l'article 7 précité ;
- d) Le modèle du bordereau des prix - détail estimatif ;



- e) Le modèle de la déclaration sur l'honneur prévue à l'article 5 précité ;
- f) Le présent règlement de la consultation.

#### **Article n°10 : Information des concurrents**

Tout concurrent peut demander au maître d'ouvrage, par courrier porté avec accusé de réception, par lettre recommandée avec accusé de réception, par fax confirmé ou par voie électronique de lui fournir des éclaircissements ou renseignements concernant l'appel d'offres ou les documents y afférents. Cette demande n'est recevable que si elle parvient au maître d'ouvrage au moins sept (7) jours avant la date prévue pour la séance d'ouverture des plis.

Le maître d'ouvrage doit répondre à toute demande d'information ou d'éclaircissement reçue dans le délai prévu ci-dessus.

Tout éclaircissement ou renseignement, fourni par le maître d'ouvrage à un concurrent à la demande de ce dernier, doit être communiqué le même jour et dans les mêmes conditions aux autres concurrents ayant retiré ou ayant téléchargé le dossier d'appel d'offres et ce par lettre recommandée avec accusé de réception, par fax confirmé ou par voie électronique. Il est également mis à la disposition de tout autre concurrent dans le portail des marchés publics et communiqué aux membres de la commission d'appel d'offres.

Les éclaircissements ou renseignements fournis par le maître d'ouvrage doivent être communiqués au demandeur et aux autres concurrents dans les sept (7) jours suivant la date de réception de la demande d'information ou d'éclaircissement du concurrent. Toutefois, lorsque ladite demande intervient entre le dixième et le septième jour précédant la date prévue pour la séance d'ouverture des plis la réponse doit intervenir au plus tard trois (3) jours avant la date prévue pour la séance d'ouverture des plis.

#### **Article n°11 : Modification dans le dossier d'appel d'offres.**

Conformément aux dispositions de l'article n°19 § 7 du règlement des marchés de l'OFPPT, exceptionnellement, le maître d'ouvrage peut introduire des modifications dans le dossier d'appel d'offres sans changer l'objet du marché. Ces modifications sont communiquées à tous les concurrents ayant retiré ou ayant téléchargé ledit dossier, et introduites dans les dossiers mis à la disposition des autres concurrents.

Lorsque les modifications nécessitent la publication d'un avis rectificatif, celui-ci est publié conformément aux dispositions de l'alinéa 1 du paragraphe I-2 de l'article 20 du Règlement des Marchés de l'OFPPT. Dans ce cas, la séance d'ouverture des plis ne peut être tenue que dans un délai minimum de dix (10) jours à compter du lendemain de la date de la dernière publication de l'avis rectificatif au portail des marchés publics, du site de l'Office le cas échéant et dans le journal paru le deuxième, sans que la date de la nouvelle séance ne soit antérieure à celle prévue par l'avis de publicité initial.

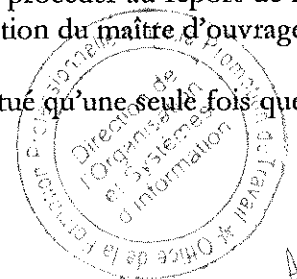
Les concurrents ayant retiré ou téléchargé les dossiers d'appel d'offres doivent être informés des modifications prévues ci-dessus ainsi que de la nouvelle date d'ouverture des plis, le cas échéant.

Lorsqu'un concurrent estime que le délai prévu par l'avis de publicité pour la préparation des offres n'est pas suffisant compte tenu de la complexité des prestations objet du marché, il peut, au cours de la première moitié du délai de publicité, demander au maître d'ouvrage, par courrier porté avec accusé de réception, par fax confirmé ou par courrier électronique confirmé, le report de la date de la séance d'ouverture des plis.

La lettre du concurrent doit comporter tous les éléments permettant au maître d'ouvrage d'apprécier sa demande de report.

Si le maître d'ouvrage reconnaît le bienfondé de la demande du concurrent, il peut procéder au report de la date de la séance d'ouverture des plis. Le report, dont la durée est laissée à l'appréciation du maître d'ouvrage.

Dans ce cas, le report de la date de la séance d'ouverture des plis, ne peut être effectué qu'une seule fois quel que soit le concurrent qui le demande.



**Article n°12 : Répartition**

Le présent appel d'offre est lancé en deux lots.

**Article n°13 : Présentation des dossiers des concurrents.**

Conformément aux dispositions de l'article n°29 du règlement des marchés de l'OFPPT :

A- Le dossier présenté par chaque concurrent est mis dans un pli fermé portant :

- Le nom et l'adresse du concurrent ;
- L'objet du marché et, éventuellement, l'indication du lot ;
- La date et l'heure de la séance d'ouverture des plis ;
- L'avertissement que " le pli ne doit être ouvert que par le président de la commission d'appel d'offres lors de la séance publique d'ouverture des plis ".

B- Ce pli contient trois enveloppes distinctes :

- a) La première enveloppe comprend le dossier administratif, le dossier technique, le dossier additif et le cahier des prescriptions spéciales dûment signé et paraphé par le concurrent ou son représentant dûment habilité à cet effet.

Cette enveloppe doit être cachetée et porter de façon apparente la mention « dossiers administratif, technique et additif ».

- b) La deuxième enveloppe comprend l'offre financière du soumissionnaire. Elle doit être cachetée et porter de façon apparente la mention « offre financière ».

- c) La troisième enveloppe contient l'offre technique. Elle doit être cachetée et porter de façon apparente la mention « offre technique ».

C- Les enveloppes visées aux paragraphes a, b, et c du B ci-dessus indiquent de manière apparente :

- Le nom et l'adresse du concurrent ;
- L'objet du marché et, le cas échéant, l'indication du lot ;
- La date et l'heure de la séance d'ouverture des plis ;

**Article n°14 : Retrait du dossier d'appel d'offres.**

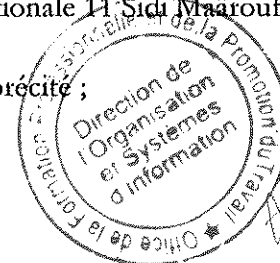
Le dossier d'appel d'offres est mis à la disposition des concurrents dans le bureau du Service des Marchés à la Direction de l'Approvisionnement et la Logistique, sis Intersection de la Route BO n° 50 et la R.N.11 (Route Nouaceur Sidi Maârouf) à Casablanca, dès la première parution de l'avis d'appel d'offres dans l'un des supports de publication prévus à l'article 20 du Règlement des Marchés de l'OFPPT et jusqu'à la date limite de remise des offres. Le dossier d'appel d'offres est remis gratuitement aux concurrents.

Le dossier d'appel d'offres peut être téléchargé à partir du portail des marchés de l'Etat [www.marchéspublics.gov.ma](http://www.marchéspublics.gov.ma) et à partir du site de l'Office de la Formation Professionnelle et de la Promotion du Travail : [www.ofppt.ma](http://www.ofppt.ma).

**Article n°15 : Dépôt des plis des concurrents.**

Conformément aux dispositions de l'article 31 du règlement des marchés de l'OFPPT, les plis sont, au choix des concurrents :

- Soit déposés, contre récépissé, dans le bureau de la Direction des Approvisionnements et Logistique (Service des Marchés), sis Intersection de la Route B.O. n° 50 et la Route Nationale 11 Sidi Maârouf – Casablanca MAROC ;
- Soit envoyés, par courrier recommandé avec accusé de réception, au bureau précité ;



- Soit remis, séance tenante, au président de la commission d'appel d'offres au début de la séance, et avant l'ouverture des plis.
- Soit transmis par voie électronique conformément aux dispositions de l'arrêté du ministère de l'économie et des finances n° 20-14 du 8 kaada 1435 (4 Septembre 2014) relatif à la dématérialisation des procédures de passation des marchés publics.

Le délai pour la réception des plis expire à la date et l'heure fixées par l'avis d'appel d'offres pour la séance d'ouverture des plis.

Les plis déposés ou reçus postérieurement au jour et à l'heure fixés ne sont pas admis.

#### **Article n°16 : Délai de validité des offres**

Conformément aux dispositions de l'article n°33 du règlement des marchés de l'OFPPT, les concurrents restent engagés par leurs offres pendant un délai de soixante-quinze (75) jours, à compter de la date de la séance d'ouverture des plis.

Si la commission d'appel d'offres estime ne pas être en mesure d'effectuer son choix pendant le délai prévu ci-dessus, le maître d'ouvrage saisit les concurrents, avant l'expiration de ce délai par lettre recommandée avec accusé de réception ou par fax confirmé ou par tout autre moyen de communication donnant date certaine et leur propose une prorogation pour un nouveau délai qu'il fixe. Seuls les concurrents ayant donné leur accord par lettre recommandée avec accusé de réception ou par fax ou par tout autres moyens de communication donnant date certaine adressée au maître d'ouvrage, avant la date limite fixée par ce dernier, restent engagés pendant ce nouveau délai.

#### **Article n°17 : Langue de l'Offre.**

L'offre préparée par le concurrent ainsi que toute correspondance et tous documents concernant l'offre échangée entre le candidat et l'OFPPT seront rédigés en Langue Française.

Tout document imprimé fourni par le candidat peut être rédigé en une autre langue dès lors qu'il est accompagné d'une traduction en langue française par une personne/autorité compétente, des passages intéressants l'offre. Dans ce cas et aux fins de l'interprétation de l'offre, la traduction française fait foi.

#### **Article n°18 : Prix préférentiels pour la formation professionnelle.**

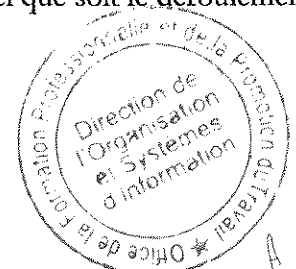
Vu que les prestations objet du présent appel d'offres sont destinées uniquement à la formation professionnelle, il y a lieu de proposer des prix préférentiels pour l'éducation.

#### **Article n°19 : Monnaie de l'offre.**

Pour le concurrent non installé au Maroc, la monnaie dans laquelle le prix des offres doit être formulé et exprimé est l'Euro ou le dollar USA. Dans ce cas, pour être évalués et comparés, les montants des offres exprimées en monnaies étrangères doivent être convertis en dirham. Cette conversion doit s'effectuer sur la base du cours vendeur du dirham en vigueur le premier jour ouvrable de la semaine précédant celle du jour d'ouverture des plis donné par Bank Al-Maghrib.

#### **Article n°20 : Dépenses encourues du fait de l'appel d'offres**

Le soumissionnaire supporte toutes les dépenses encourues du fait de la préparation et de la présentation de son offre à l'OFPPT qui ne pourra, en aucun cas, en être tenu pour responsable, quel que soit le déroulement ou l'issue de la procédure d'appel d'offres.



**Article n°21 : Evaluation des offres des concurrents.**

Les offres des concurrents admissibles sont examinées conformément aux dispositions des articles 36, 38, 39, 40 et 41 du Règlement des Marchés de l'OFPPT.

Les capacités techniques et financières des concurrents seront appréciées comme suit :

- Seuls seront retenus, les concurrents ayant présenté au moins **une attestation** de référence, conformes aux prescriptions de l'article 5-alinéa B-2 du présent règlement de consultation, se rapportant à des prestations de la même famille de celles objet du présent appel d'offres, dont le montant est supérieur ou égal à **25 %** de l'estimation du dit appel d'offres, réalisées au cours des années **(2015 et postérieur)**.
- Aussi, il est précisé qu'en cas d'attestation délivrée à un groupement, celle-ci sera appréciée pour la cote part réalisée par le (s) concurrent(s) ou à défaut de renseignement, pour part égale du montant globale de l'attestation.

Les offres techniques seront évaluées comme suit :

- La conformité technique des offres (de base et / ou des variantes) sera appréciée, sur la base des documents présentés dans l'offre technique du soumissionnaire et par rapport aux spécifications techniques des fournitures demandées au niveau du CPS.
- En cas de discordance des spécifications techniques entre les pièces de l'offre technique d'un ou plusieurs concurrents, la commission d'appel d'offres peut demander par écrit à l'un ou à plusieurs concurrents des précisions, éclaircissements et/ou des compléments d'information, des données sur leurs offres techniques. Ces éléments qui doivent concerner les documents contenus dans lesdites offres.
- Tout article ne répondant pas aux spécifications techniques demandées sera déclaré non conforme.
- La présence des CV, Diplômes et Attestations CNSS pour les ingénieurs proposés pour l'installation et la mise en marche des équipements objet du présent AO.

La commission peut, avant de se prononcer, charger une sous-commission technique pour analyser les offres techniques proposées.

Conformément aux dispositions des articles 39, 40 et 41 du Règlement des Marchés de l'OFPPT précité, l'examen des offres financières concerne les seuls concurrents admis à l'issue de l'examen de leurs dossiers administratifs et techniques et leur offre technique y compris catalogues, catalogues, et/ou documents relatives aux « spécifications techniques des fournitures » présentés.

Le marché sera attribué au concurrent, retenu à l'issue de l'examen des dossiers administratifs et techniques, de l'offre technique et de l'offre financière la moins disante.

NB : En application des dispositions de l'article 27 du règlement des marchés l'OFPPT précité, les corrections des erreurs arithmétiques s'effectueront de la manière suivante :

- En cas de discordance entre les prix unitaires du bordereau des prix et ceux du détail estimatif, les prix du bordereau des prix prévalent ;
- En cas de discordance entre le montant total de l'acte d'engagement et de celui du bordereau des prix-détail estimatif, le montant de ce dernier document est tenu pour bon pour établir le montant réel de l'acte d'engagement

**Le maître d'ouvrage**

Directeur de l'Organisation et  
Systèmes d'Information

  
**Hafid ABLOUHASSANE**

# MODELE DE L'ACTE D'ENGAGEMENT

\*\*\*\*\*

## ACTE D'ENGAGEMENT

### A -Partie réservée à l'Office de la Formation Professionnelle et de la Promotion du Travail

Appel d'offres ouvert sur offres des prix n°..... du .....

**Objet du marché** : La refonte des solutions réseaux (LAN/WAN) et de sécurité au niveau du siège, annexes du siège et des directions régionales. Réparti en lots suivants :

- Lot 1 : Solutions Switching, Wifi et SDN pour le Siège OFPPT, annexes siège et directions régionales.
- Lot 2 : Solutions Firewall et SDWAN pour le siège, annexes siège et directions régionales.

Passé en application de l'alinéa 2, paragraphe 1 de l'article 16 et paragraphe 1 de l'article 17 et alinéa 3 paragraphe 3 de l'article 17, relatif aux marchés publics de l'Office de la Formation Professionnelle et de la Promotion du Travail (OFPPT).

### B - Partie réservée au concurrent

#### a) Pour les personnes physiques

Je (1), soussigné : ..... (prénom, nom et qualité) agissant en mon nom personnel et pour mon propre compte, adresse du domicile élu ..... affilié à la CNSS sous le ..... (2) inscrit au registre du commerce de..... (localité) sous le n° ..... (2) n° de patente..... (2) :

#### b) Pour les personnes morales

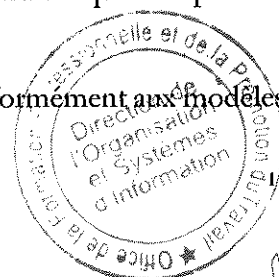
Je (1), soussigné ..... (prénom, nom et qualité au sein de l'entreprise) agissant au nom et pour le compte de..... (raison sociale et forme juridique de la société) au capital de:.....  
 adresse du siège social de la société.....  
 adresse du domicile élu.....  
 affiliée à la CNSS sous le n°.....(2) et (3)  
 inscrite au registre du commerce..... (localité) sous le n°..... (2) et (3)  
 n° de patente.....(2) et (3)  
 n° d'identification fiscale.....  
 n° de l'Identifiant commun de l'Entreprise.....(2) et (3)

En vertu des pouvoirs qui me sont conférés :

après avoir pris connaissance du dossier d'appel d'offres, concernant les prestations précisées en objet de la partie A ci-dessus ;

après avoir apprécié à mon point de vue et sous ma responsabilité la nature et les difficultés que comportent ces prestations :

1) remets, revêtu (s) de ma signature un bordereau de prix - détail estimatif établi (s) conformément aux modèles figurant au dossier d'appel d'offres ;



2) m'engage à exécuter lesdites prestations conformément au cahier des prescriptions spéciales et moyennant les prix que j'ai établis moi-même, lesquels font ressortir :

- Montant total hors T.V.A.:.....(en lettres et en chiffres)
- Taux de la TVA : .....(en pourcentage)
- Montant de la T.V.A.:.....(en lettres et en chiffres)
- Montant total T.V.A. comprise :.....(en lettres et en chiffres)

L'Office de la Formation Professionnelle et de la Promotion du Travail se libérera des sommes dues par lui en faisant donner crédit au compte ..... (à la Trésorerie Générale, bancaire, ou postal) (4) ouvert à mon nom (ou au nom de la société) à.....(localité), sous relevé d'identification bancaire (RIB) numéro.....

Fait à.....le.....

(Signature et cachet du concurrent)

(1) lorsqu'il s'agit d'un groupement, ses membres doivent :

- mettre : «Nous, soussignés..... nous obligeons conjointement/ou solidairement (choisir la mention adéquate et ajouter au reste de l'acte d'engagement les rectifications grammaticales correspondantes) ;
- ajouter l'alinéa suivant : « désignons..... (prénoms, noms et qualité) en tant que mandataire du groupement ».

(2) Pour les concurrents non installés au Maroc, préciser la référence des documents équivalents et lorsque ces documents ne sont pas délivrés par leurs pays d'origine, la référence à l'attestation délivrée par une autorité judiciaire ou administrative du pays d'origine ou de provenance certifiant que ces documents ne sont pas produits.

(3) ces mentions ne concernent que les personnes assujetties à cette obligation.

(4) supprimer les mentions inutiles





# MODELE DE DECLARATION SUR L'HONNEUR

\*\*\*\*\*

## DECLARATION SUR L'HONNEUR

- Mode de passation : Appel d'offres ouvert N°....., sur offres des prix.

**Objet du marché :** La refonte des solutions réseaux (LAN/WAN) et de sécurité au niveau du siège, annexes du siège et des directions régionales. Réparti en lots suivants :

- **Lot 1 :** Solutions Switching, Wifi et SDN pour le Siège OFPPT, annexes siège et directions régionales.
- **Lot 2 :** Solutions Firewall et SDWAN pour le siège, Annexes siège et directions régionales.

### A - Pour les personnes physiques

Je, soussigné : ..... (prénom, nom et qualité)  
 agissant en mon nom personnel et pour mon propre compte,  
 adresse du domicile élu : .....  
 affilié à la CNSS sous le n° : ..... (1)  
 inscrit au registre du commerce de ..... (localité) sous le n° ..... (1) n° de  
 patente ..... (1)  
 n° du compte courant postal, bancaire ou à la TGR ..... (RIB)

### B - Pour les personnes morales

Je, soussigné ..... (prénom, nom et qualité au sein de l'entreprise)  
 agissant au nom et pour le compte de ..... (raison sociale et forme juridique de la société) au  
 capital de: .....  
 adresse du siège social de la société ..... adresse du domicile  
 élu .....  
 affiliée à la CNSS sous le n° ..... (1)  
 inscrite au registre du commerce ..... (localité) sous le n° ..... (1)  
 n° de patente ..... (1)  
 n° du compte courant postal, bancaire ou à la TGR ..... (RIB)  
 n° de l'identifiant Commun de l'Entreprise : ..... (1)

### - Déclare sur l'honneur :

- 1- m'engager à couvrir, dans les limites fixées dans le cahier des charges, par une police d'assurance, les risques découlant de mon activité professionnelle ;
- 2- que je remplit les conditions prévues à l'article 24 du Règlement des Marchés, approuvé le 18 Chaabane 1435 (16 Juin 2014), et fixant les conditions et les formes de passation des marchés de l'office de la formation professionnelle et de la promotion du travail (OFPPT) ainsi que certaines règles relatives à leur gestion et à leur contrôle ;
- 3- Etant en redressement judiciaire j'atteste que je suis autorisé par l'autorité judiciaire compétente à poursuivre l'exercice de mon activité (2) ;
- 4- m'engager, si j'envisage de recourir à la sous-traitance :
  - à m'assurer que les sous-traitants remplissent également les conditions prévues par l'article 24 du Règlement des Marchés de l'OFPPT ;



- que celle-ci ne peut dépasser 50% du montant du marché, ni porter sur les prestations constituant le lot ou le corps d'état principal prévues dans le cahier des prescriptions spéciales, ni sur celles que le maître d'ouvrage a prévues dans ledit cahier ;
- à confier les prestations à sous-traiter à des PME installées au Maroc ; (3)

5- m'engager à ne pas recourir par moi-même ou par personne interposée à des pratiques de fraude ou de corruption de personnes qui interviennent à quelque titre que ce soit dans les différentes procédures de passation, de gestion et d'exécution du présent marché ;

6- m'engage à ne pas faire par moi-même ou par personne interposées, des promesses, des dons ou des présents en vue d'influer sur les différentes procédures de conclusions du présent marché.

7- atteste que je remplis les conditions prévues par l'article 1er du dahir n° 1-02-188 du 12 JOMADA I 1423 (23 juillet 2002) portant promulgation de la loi n°53-00 formant charte de la petite et moyenne entreprises (4).

8- atteste que je ne suis pas en situation de conflit d'intérêt tel que prévu à l'article 151 du Règlement des Marchés de l'OFPPT.

9- je certifie l'exactitude des renseignements contenus dans la présente déclaration sur l'honneur et dans les pièces fournies dans mon dossier de candidature.

10- je reconnais avoir pris connaissance des sanctions prévues par l'article 142 du Règlement des Marchés de l'OFPPT, relatives à l'inexactitude de la déclaration sur l'honneur.

Fait à.....le.....

Signature et cachet du concurrent

**(1)** Pour les concurrents non installés au Maroc, préciser la référence des documents équivalents et lorsque ces documents ne sont pas délivrés par leurs pays d'origine, la référence à l'attestation délivrée par une autorité judiciaire ou administrative du pays d'origine ou de provenance certifiant que ces documents ne sont pas produits.

**(2)** à supprimer le cas échéant.

**(3)** Lorsque le CPS le prévoit.

**(4)** à prévoir en cas d'application de l'article 139 du Règlement des Marchés de l'OFPPT.

(\*) en cas de groupement, chacun des membres doit présenter sa propre déclaration sur l'honneur.



**MODELE DE L'ATTESTATION DE REFERENCE****\*\*\*\*\***

Logo Entreprise

Date

**ATTESTATION DE REFERENCE**

Je soussigné, [Nom et Prénom], [Qualité du signataire], atteste par la présente que la société [Nom de la société], a exécutée les prestations [Détailler les prestations], objet du marché n° ....., d'un montant de : ....., sur un délai d'exécution de : .....

à la date du .....

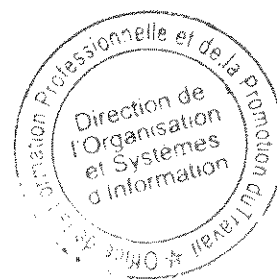
Les prestations mentionnées, ci-dessus, se sont déroulées dans de bonnes conditions et à notre entière satisfaction.

La présente attestation est établie pour servir et valoir ce que de droit

Signature et cachet

Nom et Prénom du signataire

Qualité du signataire



**CAHIER DES PRESCRIPTIONS SPECIALES  
(C. P. S.)**



**CAHIER DES PRESCRIPTIONS SPÉCIALES**

Marché n° ..... / 2022.

Passé en application de l'alinéa 2, paragraphe 1 de l'article 16 et paragraphe 1 de l'article 17 et alinéa 3 paragraphe 3 de l'article 17, du règlement des marchés, approuvé le 18 Chaabane 1435 (16 Juin 2014), relatif aux marchés publics de l'Office de la Formation Professionnelle et de la Promotion du Travail (OFPPT).

Entre les soussignés :

d'une part : .....

L'OFFICE DE LA FORMATION PROFESSIONNELLE ET DE LA PROMOTION DU TRAVAIL (O.F.P.P.T.), représenté par son Directeur Général,

Et,

D'autre part : .....

La société : .....

- Titulaire du compte ..... (à la Trésorerie Générale, bancaire, ou postal) ouvert à mon nom (ou au nom de la société) à ..... (localité), sous relevé d'identification bancaire (RIB) numéro.....

- Adresse du siège social de la société : .....

- Adresse du domicile élu : .....

- Affiliée à la CNSS sous le n° : .....

- Inscrite au registre de commerce de ..... (localité) sous le n° : .....

- Patente n° : .....

- N° d'identification fiscale

- n° de l'identifiant Commun de l'Entreprise : .....

- Représentée par :

Monsieur .....

Agissant au nom et pour le compte de ladite société en vertu des pouvoirs qui lui sont conférés,



## **CHAPITRE I : CLAUSES ADMINISTRATIVES ET FINANCIERES :**

### **ARTICLE 1 : OBJET DU MARCHE**

La refonte des solutions réseaux (LAN/WAN) et de sécurité au niveau du siège, annexes du siège et des directions régionales. Réparti en lots suivants :

- Lot 1 : Solutions Switching, Wifi et SDN pour le Siège OFPPT, annexes siège et directions régionales.
- Lot 2 : Solutions Firewall et SDWAN pour le siège, annexes siège et directions régionales.

### **ARTICLE 2 : DOCUMENTS CONSTITUTIFS DU MARCHE**

Les documents contractuels sont par ordre de priorité :

- 1- L'acte d'engagement,
- 2- Le présent cahier des prescriptions spéciales,
- 3- Le bordereau des prix - détail estimatif,
- 4- L'offre technique du titulaire,
- 5- Le cahier des clauses administratives générales applicables aux marchés de travaux (CCAGT), approuvé par le Décret n° 2-14-394 du 06 Chaabane 1437 (13 mai 2016).

En cas de discordance ou de contradiction entre les documents constitutifs du marché, autres que celles se rapportant à l'offre financière tel que décrit dans règlement relatif aux marchés publics de l'office de l'OFPPT, ceux-ci prévalent dans l'ordre où ils sont énumérés ci-dessus.

### **ARTICLE 3 : AUTRES TEXTES APPLICABLES**

Le titulaire du marché est soumis aux dispositions notamment des textes suivants :

- Le règlement des marchés, approuvé le 18 Chaabane 1435 (16 Juin 2014), relatif aux marchés publics de l'Office de la Formation Professionnelle et de la Promotion du Travail (OFPPT).
- Le Décret n° 2-14-394 du 06 Chaabane 1437 (13 mai 2016) approuvant Le cahier des clauses administratives générales applicables aux marchés de travaux.
- La loi n°69-00 relative au contrôle financier de l'Etat sur les entreprises publiques et autres organismes (B.O. n°5170 du 18/12/2003).
- L'arrêté 2-3663 du 13 /07/2005 portant organisation financière et comptable de l'OFPPT.
- Le dahir n° 1-15-05 du 29 rabii II 1436 (19 février 2015) portant promulgation de la loi n°112-13 relative au nantissement des marchés publics.
- Les textes officiels réglementant la main d'œuvre et les salaires.
- Le dahir n°1.85.347 du 20/12/1985 relatif à l'institution générale de la taxe sur la valeur ajoutée (TVA).
- La décision du Ministre des Finances et de la Privatisation - DEPP n° 2-0610 du 26 Février 2008 fixant le visa préalable du contrôleur d'Etat de l'OFPPT pour les marchés de fournitures et de prestation de service dont le montant est supérieur à 1 000 000,00 DHS.

Ainsi que tous les textes réglementaires ayant trait aux marchés publics rendus applicables à la date limite de réception des offres.



**ARTICLE N°4 : CARACTERE DES PRIX**

Les prix des équipements objet du présent marché sont fermes et non révisables.

Toutefois, si le taux de la taxe sur la valeur ajoutée est modifié postérieurement à la date limite de remise des offres, le maître d'ouvrage répercute cette modification sur le prix de règlement.

**ARTICLE N°5 : NATURE DES PRIX**

Le présent marché est à prix unitaires.

Les sommes dues au titulaire du marché sont calculées par application des prix unitaires portés au bordereau des prix-détail estimatif, joint au présent cahier des prescriptions spéciales, aux quantités réellement exécutées conformément au marché.

Les prix du marché sont réputés comprendre toutes les dépenses résultant de la livraison des fournitures y compris tous les droits, impôts, taxes, frais généraux, faux frais et assurer au titulaire une marge pour bénéfices et risques et d'une façon générale toutes les dépenses qui sont la conséquence nécessaire et directe de la livraison des fournitures.

**ARTICLE N°6 : DROITS DE TIMBRES**

Le titulaire acquitte les droits de timbre dus au titre du marché conformément à la législation en vigueur.

**ARTICLE N°7 : DELAI D'EXECUTION ET PENALITES DE RETARD****Délai d'exécution :**

Le délai contractuel pour l'exécution des prestations objet cet appel d'offre est réparti comme suit :

- **Lot 1 : Huit mois (8 mois)**
- **Lot 2 : Trois mois (3 mois)**

Il commence à courir à compter de la date fixée par l'ordre de service prescrivant le commencement des prestations objet du présent marché pour la partie correspondante. Ce délai s'applique à l'achèvement de la livraison de la totalité des fournitures incombant au titulaire.

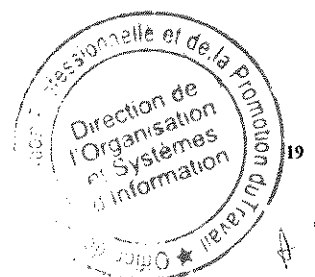
Le délai que se réserve l'OFPPT pour la vérification de la conformité technique, n'est pas inclus dans le délai contractuel susmentionné.

**Pénalités de retard :**

A défaut par le titulaire d'avoir terminé les prestations objet du marché dans le délai contractuel, il lui sera appliqué, sans mise en demeure préalable, une pénalité de un pour mille (1/1000) du montant initial, éventuellement majoré par les montants correspondants aux travaux supplémentaires et à l'augmentation dans la masse et ce, par jour calendaire.

Le montant global des pénalités au titre des retards est plafonné à huit pour cent (8) % du montant initial du marché augmenté le cas échéant du montant des avenants.

Quand le montant des pénalités atteint ce plafond, l'autorité compétente se réserve le droit de résilier le marché dans les conditions prévues par l'article 79 du CCAGT.



**ARTICLE N°8 : CAUTIONNEMENTS PROVISOIRE ET DEFINITIF**

Le cautionnement provisoire qui reste affecté à la garantie des engagements contractuels du titulaire du marché dans les cas prévus par l'article 18 § 1 du CCAOT est :

- Lot 1 : Cent dix milles DIRHAMS (110 000,00 DHS)
- Lot 2 : Trente-deux milles DIRHAMS (32 000,00 DHS)

Le cautionnement provisoire reste acquis au maître d'ouvrage notamment dans les cas cités à l'article 18 du CCAOT.

Le montant du cautionnement définitif est fixé à trois pour cent (3%) du montant du marché arrondi au dirham supérieur.

Le cautionnement définitif doit être constitué dans les vingt (20) jours qui suivent la notification de l'approbation du marché.

**N.B :** Les cautions personnelles et solidaires doivent être choisies parmi les établissements marocains agréés à cet effet conformément à la législation en vigueur

**ARTICLE N°9 : LIVRAISON DES EQUIPEMENTS AU SITE BENEFICIAIRE**

Les équipements seront livrés aux sites bénéficiaires indiqués dans le tableau de répartition.

Avant de commencer les livraisons, le titulaire doit transmettre à l'OFPPT :

- Un planning prévisionnel de livraison une fois l'ordre de service de commencement est signé.
- Le programme des livraisons au moins 15 jours avant le début des livraisons dans le site bénéficiaire(s).

Les opérations de transport, de chargement, de déchargement, de déballage et d'emballage sont à la charge exclusive du titulaire et sont effectuées sous sa responsabilité.

Le responsable du centre bénéficiaire signe les bons de livraison des articles livrés en précisant les dates de livraison.

**ARTICLE N°10 : MODALITES DE VERIFICATION DE CONFORMITE TECHNIQUE**

Sur la base du programme des livraisons, l'OFPPT organise les opérations de vérification de conformité technique du matériel livré dans les sites bénéficiaires suivant un planning communiqué au titulaire.

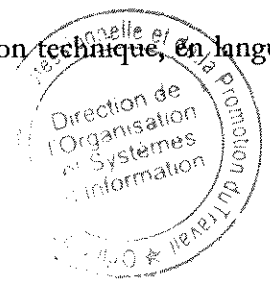
Le retard enregistré dans l'opération de vérification de conformité technique et de réception, après livraison du matériel, sera à la charge de l'O.F.P.P. T et le délai d'exécution du marché sera prorogé en conséquence.

Le titulaire interviendra pour l'installation des différents équipements dans un délai de 7 jours qui commencera à courir à partir du lendemain de la saisie du titulaire par l'OFPPT l'informant du dépôt des équipements en question dans les locaux de ce dernier ;

Le titulaire procédera à l'ouverture des caisses, l'installation et la mise en marches des équipements. La matière d'œuvre nécessaire aux différents essais est à sa charge.

Les équipements jugés non-conformes sont récupérés par le titulaire dans un délai maximum de 30 jours qui commencera à courir à partir du lendemain de la notification au fournisseur par l'OFPPT des équipements concernés. Passé ce délai l'OFPPT n'est plus responsable des équipements en question.

Le titulaire mettra à la disposition du(es) représentant(s) de l'OFPPT la documentation technique, en langue française, nécessaire à la vérification de la conformité technique des équipement(s).





Les opérations de déballage et d'emballage sont à la charge exclusive du titulaire et sont effectuées sous sa responsabilité.

L'O.F.P.P.T. procédera à la vérification de la conformité technique de l'équipement avec les spécifications du marché et avenant(s) (marque, référence, origine, dimensions, capacités, puissance, alimentation électrique,) dans les sites bénéficiaires, à la date prévue, en présence d'un représentant qualifié du titulaire devant être habilité à répondre aux remarques de la commission désignée par l'OFPPT.

La vérification de la conformité technique des articles livrés est sanctionnée par l'établissement d'un procès-verbal qui doit être signé par le(s) représentant(s) de l'O.F.P.P.T. et du titulaire ayant participé à l'opération de vérification.

Toute divergence par rapport au marché et le cas échéant ses avenants doit être consignée dans le procès-verbal de vérification de conformité technique.

Une copie du procès-verbal de vérification de conformité technique est remise au représentant du titulaire séance tenante.

Tout équipement jugé non conforme par l'OFPPT doit être remplacé, par le titulaire, dans le délai contractuel

## **ARTICLE N°11 : MODALITES DE RECEPTION DES EQUIPEMENTS**

L'OFPPT procédera à la réception dans le site bénéficiaire :

- Du matériel sur la base du procès-verbal de vérification de conformité technique
- Des quantités livrées par rapport à celles du marché ou avenant,
- De la mise en marche du matériel si nécessaire.
- De l'attestation ou tout autre moyen prouvant la souscription des licences et de la garantie auprès des éditeurs et constructeurs.

### **Lot 1 :**

La réception du Lot 1 peut être prononcée par partie une fois les prestations de chaque partie sont réalisées, testées ;

### **Lot 2 :**

La réception du Lot 2 est prononcée une fois toutes les prestations des différents sont réalisées, testées ;

Les articles réceptionnés sont enregistrés dans le livre journal et éventuellement dans le livre d'inventaire. Les numéros du livre journal et d'inventaire sont portés sur le PV de réception.

## **ARTICLE N°12 : Formation**

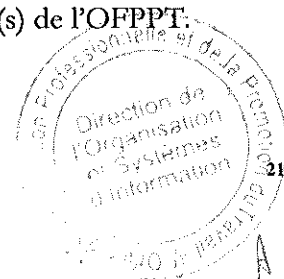
La formation n'est pas prévue ;

## **ARTICLE N°13 : Réceptions provisoire et définitive**

### **2- Réception provisoire**

La réception provisoire du marché n'est prononcée que lorsque tous les équipements sont livrés, vérifiés conformes et une fois tous les essais ont été déclarés satisfaisants par le(s) représentant(s) de l'OFPPT.

La réception provisoire du marché correspondra à la dernière date de réception.



## **2- Réception définitive**

Le titulaire demandera à l'OFPPT d'organiser la réception définitive vingt jours au plus tard avant l'expiration du délai de garantie.

Un planning de réception définitive sera communiqué par l'OFPPT au titulaire en lui précisant les lieux et les dates de réceptions définitives.

Le titulaire prendra les dispositions nécessaires pour se faire représenter à ces opérations qui seront sanctionnées par un procès-verbal de réception définitive locale.

Si au moment de la réception définitive, il est reconnu que certaines réserves concernant la réparation ou le remplacement de l'équipement défectueux ayant fait l'objet d'une notification, le titulaire disposera d'un délai d'un (1) mois maximum pour réparer ou remplacer l'équipement déclaré défectueux.

Le délai de garantie des équipements concernés qui leur est directement lié est prolongé jusqu'à ce que ces réserves soient levées par le titulaire. A défaut, l'O.F.P.P.T. peut effectuer les réparations ou remplacements aux frais du titulaire de marché ou prendre d'autres mesures correctives.

### **ARTICLE N°14 : MODE DE REGLEMENT**

Les prestations faisant l'objet du marché seront réglées par application des prix unitaires définis et établis pour chaque item par le titulaire aux quantités réellement exécutées et réceptionnées, conformément aux descriptions figurant au bordereau des prix-détail estimatif et aux conditions particulières du marché.

### **ARTICLE N°15 : MODALITES DE PAIEMENT**

Le titulaire adressera à l'Office les factures en cinq exemplaires avec les bons de livraisons des articles réceptionnés conformes.

Les sommes dues au titulaire seront réglées à son compte dont le numéro est précisé dans le marché.

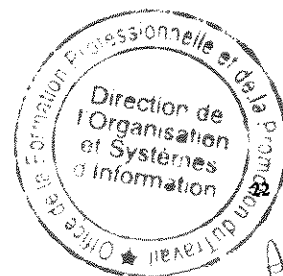
Tout changement du numéro de compte doit faire l'objet d'un avenant.

### **ARTICLE N°16 : UTILISATION DES DOCUMENTS CONTRACTUELS ET DIFFUSION DE RENSEIGNEMENTS.**

Le titulaire, sauf consentement préalable donné par écrit par l'O.F.P.P.T., ne communiquera le marché, ni aucune de ses clauses, ni aucune des spécifications, des plans, dessins, tracés, échantillons ou information fournis par l'O.F.P.P.T. ou en son nom et au sujet du marché à aucune personne autre qu'une personne employée par le titulaire à l'exécution du marché. Les informations transmises à une telle personne le seront confidentiellement et seront limitées à ce qui est nécessaire à ladite exécution.

Le titulaire, sauf consentement préalable donné par écrit par l'O.F.P.P.T., n'utilisera aucun des documents et aucune des informations énumérées dans le paragraphe précédent, si ce n'est pour l'exécution du marché.

Tout document, autre que le marché lui-même, énuméré dans le 1<sup>er</sup> paragraphe demeurera la propriété de l'O.F.P.P.T. et tous ses exemplaires seront renvoyés à l'O.F.P.P.T. sur sa demande, une fois les obligations contractuelles du titulaire exécutées.



**ARTICLE N°17 : BREVETS**

Le titulaire garantira l'O.F.P.P. T, contre toute réclamation des tiers touchant à la contrefaçon ou à l'exploitation non autorisée d'un brevet, d'une marque commerciale ou des droits de création industrielle résultant de l'emploi des équipements ou d'un de leurs éléments au MAROC.

**ARTICLE N°18 : SOUS-TRAITANCE**

Toute sous-traitance éventuelle au titre de ce marché se fera dans les conditions de l'article n°141 du règlement des marchés de l'OFPPPT.

**ARTICLE N°19 : DOMICILE DU TITULAIRE**

Le titulaire du marché est tenu d'élire domicile au Maroc qu'il doit indiquer dans l'acte d'engagement ou le faire connaître au maître d'ouvrage dans le délai de quinze (15) jours à partir de la notification, qui lui est faite, de l'approbation de son marché.

Faute par lui d'avoir satisfait à cette obligation, toutes les notifications qui se rapportent au marché sont valables lorsqu'elles ont été faites au siège de l'entreprise dont l'adresse est indiquée dans le cahier des prescriptions spéciales.

En cas de changement de domicile, le titulaire est tenu d'en aviser le maître d'ouvrage, par lettre recommandée avec accusé de réception, dans les quinze (15) jours suivant la date d'intervention de ce changement.

**ARTICLE N°20 : VALIDITE DU MARCHE**

Le marché ne sera valable, définitif et exécutoire qu'après sa signature par l'autorité compétente de l'Office ou par son délégataire dûment désigné et son visa par le Contrôleur d'Etat, lorsque ledit visa est requis.

**ARTICLE N°21 : DELAI DE NOTIFICATION DE L'APPROBATION DU MARCHE.**

L'approbation du marché doit être notifiée à l'attributaire dans un délai maximum de soixante-quinze (75) jours à compter de la date d'ouverture des plis.

Les conditions de prorogation de ce délai sont fixées par les dispositions de l'article 136 du règlement des marchés de l'OFPPPT.

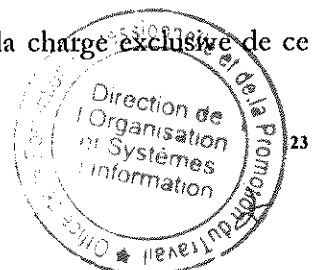
**ARTICLE N°22 : GARANTIE**

Le titulaire garantit que tout l'équipement livré en exécution du marché est neuf, n'a jamais été utilisé, est du modèle le plus récent en service et inclue toutes les dernières améliorations en matière de conception et de matériau sauf si le marché en a disposé autrement.

Le titulaire garantit en outre que tout l'équipement livré en exécution du marché n'aura aucune défectuosité due à sa conception, aux matériaux utilisés ou à sa mise en œuvre (sauf dans le cas où la conception et/ou le matériau requis par les spécifications du marché), qui peut se révéler pendant l'utilisation normale de l'équipement livré, dans les conditions prévalant dans les établissements de formation Professionnelles de l'OFPPPT.

Pendant la période de garantie, les techniciens du fournisseur interviendront dans un délai ne dépassant pas 4h, à partir de la notification de l'OFPPPT suivant la garantie et maintenance définies dans chaque lot.

Les frais de récupération ou de remplacement des équipements défectueux sont à la charge exclusive de ce dernier.



**En cas d'incident :**

L'OFPPT notifiera rapidement au titulaire toutes réclamations faisant jouer cette garantie.

Le titulaire dispose de 48 heures pour l'intervention.

**ARTICLE N°23 : RETENUE DE GARANTIE**

Conformément à l'Article 64 du C.C.A.G-T, une retenue d'un dixième (1/10) sera effectuée sur le montant des acomptes.

La retenue de garantie cessera de croître lorsqu'elle aura atteint sept pour cent (7 %) du montant initial du marché augmenté le cas échéant du montant des avenants.

Toutefois, cette retenue de garantie pourra être remplacée, à la demande du titulaire, par une caution personnelle et solidaire dans les conditions prévues par la réglementation en vigueur.

**N.B :** pour le titulaire étranger, le cautionnement de la retenue de garantie doit être avalisé par une banque marocaine.

**ARTICLE N°24 : DELAI DE GARANTIE**

Le délai de garantie minimal est fixé à :

**Lot 1 : trois années.**

**Lot 2 : trois années.**

Pour les prestations objet du marché. Il court à partir de la date de réception provisoire de ces équipements.

Le délai de garantie suscité concerne tous les items mentionnés dans le bordereau des prix – détail estimatif, et est exigé du titulaire après la date du procès-verbal de réception provisoire.

**ARTICLE N°25 : RESTITUTION DES CAUTIONNEMENTS PROVISOIRE ET DEFINITIF ET PAIEMENT DE LA RETENUE DE GARANTIE**

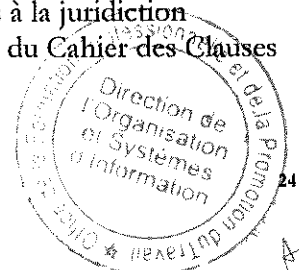
En application des dispositions de l'article 19 du CCA GT, le cautionnement provisoire est restitué au titulaire du marché ou la caution qui le remplace est libérée après que le titulaire aura réalisé le cautionnement définitif. Le cautionnement définitif est restitué, sauf les cas d'application de l'article 79 du CCA GT, et le paiement du la retenu de garantie est effectuée ou bien les cautions qui les remplacent à la suite d'une mainlevée donnée par l'OFPPT dès la signature du procès-verbal de la réception définitive des équipements objet du marché.

**ARTICLE N°26 : ASSURANCE ET RESPONSABILITES**

En application des dispositions de l'article 25 du CCA GT, le titulaire doit souscrire, conformément à la législation et à la réglementation en vigueur, les polices d'assurances qui doivent couvrir les risques inhérents à l'exécution du présent marché.

**ARTICLE N°27 : REGLEMENT DES CONTESTATIONS**

En cas de contestation entre l'administration et le titulaire, il sera fait recours à la procédure prévue par les articles 81, 82 et 84 du Cahier des Clauses Administratives Générales applicables aux marchés de Travaux (CCA GT). Si cette procédure ne permet pas le règlement du litige, celui-ci sera soumis à la juridiction marocaine compétente statuant en matière administrative, conformément à l'article 83 du Cahier des Clauses Administratives Générales applicables aux marchés de Travaux (CCA GT).



**ARTICLE N°28 : NANTISSEMENT**

En cas de nantissement du marché, le Maître d'ouvrage remet au titulaire du marché, sur sa demande et contre récépissé, une copie du marché portant la mention « exemplaire unique » dûment signée et indiquant que ladite copie est délivrée en unique exemplaire destiné à former titre pour le nantissement du marché public, conformément aux dispositions du dahir n° 1-15-05 du 29 rabii II 1436 (19 février 2015) portant promulgation de la loi n° 112-13 relative au nantissement des marchés publics, étant précisé que :

+ La liquidation des sommes dues par l'Office de la formation Professionnelle et de la Promotion du Travail en exécution du présent marché sera opérée par les soins du Directeur Général de l'O.F.P.P.T ou son délégataire.

+ Le fonctionnaire chargé de fournir au titulaire du futur marché ainsi qu'à bénéficiaire des nantissemments ou subrogations les renseignements, qui ont été prévus à l'article 8 du dahir susvisé, est le Directeur Général de l'OFPPT ou son délégataire.

+ Les paiements prévus au présent marché seront effectués par le Trésorier Payeur de l'OFPPT seul qualifié pour recevoir les significations des créanciers du titulaire du présent marché.

Les frais de timbre et d'enregistrement de l'original du présent marché ainsi que de l'exemplaire unique sont à la charge du titulaire du marché.

**ARTICLE 29 : RESILIATION DU MARCHE**

Le marché peut être résilié par l'OFPPT de plein droit dans tous les cas de figure prévus par les textes en vigueur (le Décret n° 2-14-394 du 06 Chaabane 1437 (13 mai 2016) – CCAGT et règlement des marchés de l'OFPPT approuvé le 18 Chaabane 1435 (16 Juin 2014)).

**ARTICLE 30 : MESURES COERCITIVES**

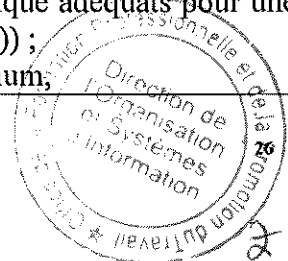
Il sera fait application des mesures coercitives prévues la CCAG-T, notamment celle prévues par son chapitre VIII.



## CHAPITRE II : CLAUSES ET SPECIFICATIONS TECHNIQUES

Lot 1 : Solutions SDN, Switching et Wifi pour le Siège OFPPT, Annexes Sièges et Directions Régionales

| N°<br>ITEM   | Désignation  |
|--|--|
| Partie 1 : Solutions SDN, Switching et Wifi pour le siège, Annexe I-SidiMaarouf et Annexe II-Ain Borja |  |
| 1.   | <p><b><u>Contrôleur SDN :</u></b></p> <p>La solution doit être installée au niveau du Datacenter du siège, elle doit être de même marque que les solutions de switching et wifi proposées dans cet appel d'offre, elle doit permettre :</p> <ul style="list-style-type: none"> <li>• La gestion et l'administration des ressources et équipements réseau LAN objet de cet appel d'offre (Items 2,3,4,5,6,7,9,10 et 11) ;</li> <li>• D'assurer l'intégration avec les modules d'authentification et contrôle d'accès au réseau ;</li> <li>• Le support de l'intégration avec des plateformes Cloud et écosystème tiers via les API ;</li> <li>• D'offrir une cartographie physique et logique des switchs, Points d'accès, équipements connectés aux switchs objet de cet appel d'offres ;</li> <li>• L'administration centralisée LAN et WLAN simplifiée : <ul style="list-style-type: none"> <li>✓ Tagging des ports de plusieurs switchs managés par simple clic ;</li> <li>✓ Supervision centralisée de l'état de santé des switchs ;</li> <li>✓ Vue de la topologie physique des switchs par code couleur (Ring, Uplink, Agrégation des liens, ...) ;</li> <li>✓ Vue du consommation POE au niveau de chaque port et chaque switch ;</li> <li>✓ Permet la gestion de tous les aspects de maintenance et gestion opérationnelle des switchs et des points d'accès : enregistrement, provisionning, upgrade firmware, commande CLI ;</li> <li>✓ Provisionning des SSIDs simplifié et centralisé ;</li> <li>✓ Possibilité d'importer un Plan architecturale du bâtiment et de positionner les points d'accès sur la carte. Cette fonctionnalité permet d'afficher en temps réel l'état, l'emplacement du point d'accès lors de recherches non structurées ;</li> <li>✓ Module d'analyse spectrale permettant de voir les interférences de signal,</li> <li>✓ Module d'analyse applicative : avoir la capacité de lister tout le trafic applicatif des utilisateurs ;</li> </ul> </li> </ul> |
| 2.   | <p><b><u>Switch fédérateur :</u></b></p> <p>Les Switch fédérateurs doivent être de même marque que les contrôleurs SDN / et doivent avoir les caractéristiques <b>minimales</b> suivantes :</p> <ul style="list-style-type: none"> <li>• Marque reconnue mondialement leader Gartner dans les trois dernières années dans le <b>magic quadrant wired and wireless lan</b> ;</li> <li>• Rackable 19" ;</li> <li>• 2 ports de 40 G minimum (face avant du switch) ;</li> <li>• 2 modules QSFP+ 40 G minimum (A prévoir deux câbles fibre optique adéquats pour une distance de 10 mètres minimum ou le câble AOC (actif optique câble)) ;</li> <li>• 48 ports 10 Gigabit SFP+ pour les Uplink des Switchs d'accès minimum;</li> </ul>  |



- **20** Connecteurs **10** Gigabits SFP+ SR nécessaires pour assurer l'interconnexion avec les switchs des sous répartiteurs ;
- **4** Connecteurs **1** Gigabits Base T minimum ;
- Capacité de commutation **2 Tpbs minimum** ;
- Débit de paquet évolutif minimum **900 Mpps** ;
- Switch manageable via SNMP, CLI et interface web ;
- Routage Statique et Dynamique ;
- Modules échangeables à chaud ;
- Alimentation redondante échangeable à chaud ;
- Le commutateur supporte à être contrôlé et surveillé via un gestionnaire réseau/contrôleur, basé sur une architecture définie par logiciel ou matériel ;
- Stacking et SDN ;
- Être livré avec les licences nécessaires ;

### **Garantie et support constructeur de 3 ans pièce et main d'œuvre**

NB : Les Deux Switchs Fédérateurs doivent :

-Fonctionner de façon redondante et en partage de charge ;

-Être équipés de liens d'agrégation de 40 Gbps minimum pour la synchronisation et transfert de données,

-Être livrés avec les câbles et les accessoires nécessaires à leur interconnexion ainsi pour leur pose, raccordement, et mise en service.

### **3. Switch multi Giga (avec PoE+)**

Les commutateurs d'accès auront pour rôle la connectivité au réseau local LAN informatique la totalité des équipements (Points d'accès wifi 6 ; Microordinateurs, IP phone, stations de travail, imprimantes...).

Ils doivent être de même marque que le switch fédérateur et conformes aux spécifications techniques **minimales** suivantes :

- Marque reconnue mondialement **leader Gartner dans les trois dernières années dans le magic quadrant wired and wireless lan** ;
- Rackable 19'' ;
- **8** ports Multi Giga 1/2.5base T PoE/PoE+ minimum ;
- **40** ports **1** Gigabits Base T minimum PoE/PoE+ ;
- **4** ports **10** Gigabit SFP+ minimum (face avant du switch) modulaires pour l'Uplink avec les Switch fédérateurs ;
- **2** connecteurs **10** Gigabit SFP+
- Support SDN ;
- Matrice de commutation **200 Gbps** minimum ;
- Commutation Niveau 2/3, Routage Statique et Dynamique ;
- Throughput **110 Mpps** minimum ;
- Switch manageable via SNMP, CLI et interface web ;



- Support du PoE 802.3af et PoE+ 802.3at ;
- Support VLAN par port ;
- Sécurité et blocage de ports par adresse MAC ;
- Support QoS ;
- Agrégation de liens ;
- Support d'une pile minimum de 8 commutateurs visible sur la console de gestion centralisée ;
- Alimentation redondante échangeable à chaud ;
- Être livré avec les licences nécessaires,

#### **Garantie et support constructeur de 3 ans pièce et main d'œuvre**

Ces commutateurs doivent être livrés avec les câbles et les accessoires nécessaires à leur interconnexion ainsi pour leur pose, raccordement, et mise en service,

#### **4. Switch 48 ports (avec PoE+)**

Les commutateurs d'accès auront pour rôle la connectivité au réseau local LAN informatique la totalité des équipements (Microordinateurs, IP phone, stations de travail, imprimantes...)

Ils doivent être de même marque que le switch fédérateur et conformes aux spécifications techniques **minimales** suivantes :

- Marque reconnue mondialement **leader Gartner dans les trois dernières années dans le magic quadrant wired and wireless lan** ;
- Rackable 19'' ;
- **48** ports 10/100/1000 base T PoE/PoE+ minimum ;
- **4** ports **10** Gigabit SFP+ minimum (face avant du switch) modulaires pour l'Uplink avec les Switch fédérateurs ;
- **1** Connecteurs **10** Gigabits minimum connexion nécessaires pour assurer la liaison avec les Switchs fédérateurs ;
- Matrice de commutation **176 Gbps** minimum ;
- Commutation Niveau **2/3**, routage statique et dynamique ;
- Throughput **110 Mpps** minimum ;
- Switch manageable via SNMP, CLI et interface web ;
- Le commutateur supporte à être contrôlé et surveillé via un gestionnaire réseau/contrôleur, basé sur une architecture définie par logiciel ou matériel ;
- Support du PoE 802.3af et PoE+ 802.3at ;
- Support VLAN par port ;
- Sécurité et blocage de ports par adresse MAC ;
- Support QoS ;
- Agrégation de liens ;
- Support SDN ;
- Alimentation redondante échangeable à chaud ;
- Support d'une pile minimum de 8 commutateurs visible sur la console de gestion centralisée ;
- Support Stacking via un câble DAC **10 Gbps minimum** ;
- Câble DAC 10 Gbps de 0.5 m minimum ;
- Être livré avec les licences nécessaires,





**Garantie et support constructeur de 3 ans pièce et main d'œuvre ;**

Les commutateurs d'accès doivent être livrés avec les câbles et accessoires nécessaires à sa mise en pile, leur interconnexion ainsi pour leur pose, raccordement et mise en service.

5

**Switch 24 ports (avec PoE+)**

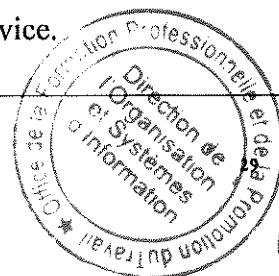
Les commutateurs d'accès auront pour rôle la connectivité au réseau local LAN informatique la totalité des équipements (Microordinateurs, IP phone, stations de travail, imprimantes...).

Ils doivent être de même marque que le switch fédérateur et conformes aux spécifications techniques minimum suivantes :

- Marque reconnue mondialement, **leader Gartner dans les trois dernières années dans le magic quadrant wired and wireless lan** ;
- Rackable 19'' ;
- 24 ports 10/100/1000 base T PoE/PoE+ minimum ;
- 4 ports 10 Gigabit **SFP+** dédiés minimum (face avant du switch) modulaire pour l'Uplink avec les Switch fédérateurs ;
- 1 Connecteurs 10 Gigabits minimum connexion nécessaires pour assurer la liaison avec les Switchs fédérateurs ;
- Matrice de commutation **128 Gbps** ;
- Commutation Niveau **2/3** de **95 Mpps** ;
- Support de la fonction stacking via des câbles DAC 10 Gbps au minimum ;
- Câble DAC 10 Gbps de 0.5m minimum ;
- Switch manageable via SNMP, CLI et interface web ;
- Le commutateur supporte à être contrôlé et surveillé via un gestionnaire réseau/contrôleur, basé sur une architecture définie par logiciel ou matériel ;
- Support du PoE 802.3af et PoE+ 802.3at ;
- Support VLAN par port ;
- Sécurité et blocage de ports par adresse MAC ;
- Support QoS ;
- Agrégation de liens ;
- L'administration doit permettre la gestion du stack comme un seul commutateur logique.
- Support SDN ;
- Alimentation redondante échangeable à chaud ;
- Support d'une pile minimum de 8 commutateurs visible sur la console de gestion centralisée ;
- Rajout/suppression des membres d'une pile à chaud sans arrêt de fonctionnement ;

**Garantie de 3 ans pièce et main d'œuvre ;**

Les commutateurs d'accès doivent être livrés avec les câbles et accessoires nécessaires à leur mise en pile, leur interconnexion ainsi pour leur pose, raccordement et mise en service.



6

**Contrôleur Wifi**

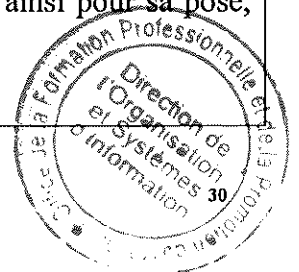
Il s'agit de fourniture, et de mise en service d'un contrôleur WiFi virtuel qui doit contrôler les points d'accès 802.11 ax et permettre d'avoir les spécifications minimales suivantes :

- Marque reconnue mondialement, **leader Gartner dans les trois dernières années dans le magic quadrant wired and wireless lan** ;
- Type virtuel ;
- Le contrôleur prend en charge les dernières normes Wi-Fi Alliance telles que Wi-Fi 6 (802.11ax) et 802.11ad, ainsi que les protocoles de sécurité WPA3.
- Support SNMP ;
- Configuration à distance à travers une interface graphique WEB (Secure WEB GUI) ;
- Support de serveur RADIUS ;
- DNS et SMTP ;
- DHCP ;
- AAA Security ;
- Support de VoWLAN ;
- Support de WIPS ;
- Authentification 802.1x, MAC et WEB (portal captif) ;
- Standards wifi IEEE 802.11ax ;
- Sécurité : AES/WPA2/WPA3 entreprise ;
- La configuration du contrôleur WIFI doit supporter **120** points accès WIFI minimum extensible à **250** ;
- Être livré avec les licences nécessaires pour la gestion de **116** APs, Analyse spectrale, et détection des APs Rogue.
- Nombre client 4 000 minimum ;
- Le contrôleur WIFI doit être automatisable via API
- Le contrôleur doit supporter un mécanisme d'HA en mode cluster Actif/Actif pour assurer une haute disponibilité du service Wifi ;
- L'itinérance des dispositifs d'une borne à l'autre à niveau 2 ainsi qu'à niveau 3 ;
- Le contrôleur WLAN proposé doit avoir la certification FIPS-140 ou équivalent ;
- De gérer des politiques de sécurité individualisées ou aux groupes d'utilisateurs usant l'accès WIFI ;
- D'appliquer les politiques relatives aux configurations et aux comportements clients pour interdire l'accès au réseau aux unités utilisateurs qui ne disposent pas des configurations de sécurité adéquate ;
- D'offrir une sécurité supplémentaire pour l'accès au réseau de l'entreprise par les utilisateurs invités. Il garantit que ces utilisateurs ne pourront pas accéder au réseau sans passer d'abord par le pare-feu ;
- Le contrôleur doit avoir un portail captif afin d'authentifier les utilisateurs,

**Garantie et support constructeur de 3 ans pièce et main d'œuvre**

NB : Le contrôleur WIFI doit :

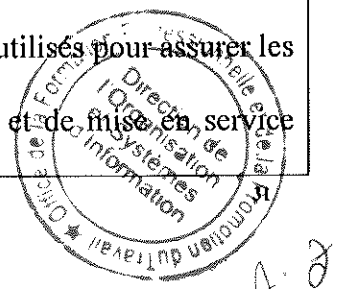
-Être livré avec les câbles et les accessoires nécessaires à son interconnexion ainsi pour sa pose, raccordement, et mise en service,



AQ

9

|    |   |
|----|---|
| 7. | <p><b><u>Point d'accès Wifi</u></b></p> <p>Les points d'accès doivent être des points d'accès haut débit 802.11 ax. Ces derniers doivent répondre aux spécifications minimales suivantes :</p> <ul style="list-style-type: none"> <li>• Marque reconnue mondialement leader <b>Gartner dans les trois dernières années dans le magic quadrant wired and wireless lan</b> ;</li> <li>• Support SNMP v2c, SNMP v3 ;</li> <li>• 802.11a/b/g &amp; 802.11n AP 802.11b/g/802.11 ac /802.11 ax (OFDMA) ;</li> <li>• IEEE 802.3af Power over Ethernet;</li> <li>• Authentification 802.1x ;</li> <li>• Connexion sécurisée avec cryptage AES/WPA/WPA2, TLS, PEAP, TTLS, TKIP;</li> <li>• MU-MIMO 4x4 : 4 ;</li> <li>• Débit doit atteindre jusqu'à <b>2.5 Gbps</b> maximum ;</li> <li>• 1 port PoE+ <b>2.5 Gigabit</b> minimum ;</li> <li>• Minimum quatre antennes intégrées ;</li> <li>• Bluetooth intégré ;</li> <li>• Dual Radio 802.11ax ;</li> <li>• Mode de fonctionnement : avec et sans contrôleur ;</li> <li>• Kit de montage mural,</li> </ul> <p><b>Garantie et support constructeur de 3 ans pièce et main d'œuvre</b></p> <p>Les Points d'accès doivent être livrés avec les câbles et accessoires nécessaires à leur pose, raccordement, fixation et mise en service.</p>   |
| 8. | <p><b><u>Prestation de service : Installation et mise en service (Siège et annexes sièges)</u></b></p> <p>Le soumissionnaire doit assurer à sa charge la livraison, l'installation et la mise en service, clé en main, des différents équipements objet du présent Appel d'offre (Switching et wifi).</p> <p>Le soumissionnaire doit livrer tous les accessoires et connectiques nécessaires pour la mise en rack et la mise en réseau des équipements objet de cet appel d'offre ;</p> <p>Le soumissionnaire doit assurer le tirage de câble (cat 6 minimum) des dites points d'accès, leurs fixations, et leurs mises en service.</p> <p>Dans le cadre des travaux d'installation et de mise en service de la solution clé en main, le soumissionnaire doit réaliser, au préalable une étude d'ingénierie (dossier d'étude détaillée de l'architecture cible) et proposer une configuration cible des éléments actifs réseaux en tenant compte des exigences des services réseaux opérationnels actuellement et ce en concertation avec l'équipe DOSI/OFPPT, et proposer également un plan de migration des anciens switches mis en production vers les nouveaux switches objet de cet AO.</p> <p>Le soumissionnaire doit se baser sur le plan d'adressage IP, de routage, de découpage VLAN et de gestion de la qualité de service existant avec les adaptations nécessaires.</p> <p>Le soumissionnaire doit détailler les procédures et outils de tests qui seront utilisés pour assurer les tests de l'installation de la solution.</p> <p>Les consultants proposés pour la réalisation des prestations d'installation et de mise en service doivent justifier de l'expérience et des compétences nécessaires à cet effet.</p> |



Garantie et maintenance (couvre l'assistance 'sur site ou à distance', l'intervention sur site, les pièces de rechanges et la main d'œuvre) pour une durée de trois ans avec un délai de prise en charge de 2 heures après déclaration de l'incident et un délai de 4 heures de résolution ou de contournement du problème ;

#### **Livrables du projet :**

Le titulaire doit fournir une documentation complète contenant :

Un dossier d'ingénierie contenant l'architecture réseau validée (étude adressage, routage, découpage vlan, ... ;

Un plan de migration de l'ancien système vers la nouvelle solution ;

Une documentation technique des équipements installés en langue Française ;

Procédures d'installation, de configuration et d'administration du matériel ;

Un guide technique d'administration et d'exploitation des équipements ;

L'ensemble de la documentation est à fournir sous format papier en deux exemplaires et sous format électronique (USB).

#### **Transfert de compétences**

Le titulaire doit assurer un transfert de compétence permettant à l'équipe de l'OFPPT d'acquérir les connaissances nécessaires pour assurer l'exploitation des équipements installés objet de l'appel d'offres.

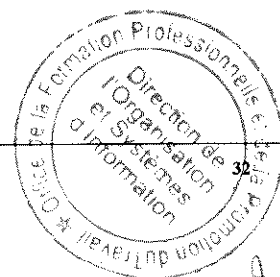
### **Partie 2 : Solutions SDN, Switching et Wifi pour les directions régionales**

#### **9. Switch 24 ports (avec PoE+)**

Les commutateurs d'accès auront pour rôle la connectivité au réseau local LAN informatique la totalité des équipements (Microordinateurs, IP phone, stations de travail, imprimantes...).

Ils doivent être de même marque que le switch fédérateur et conformes aux spécifications techniques minimum suivantes :

- Marque reconnue mondialement, **leader Gartner dans les trois dernières années dans le magic quadrant wired and wireless lan** ;
- Rackable 19'' ;
- 24 ports 10/100/1000 base T PoE/PoE+ minimum ;
- 4 ports 10 Gigabit SFP+ dédiés minimum (face avant du switch) modulaire pour l'Uplink avec les Switch fédérateurs ;
- 1 Connecteurs 10 Gigabits minimum connexion nécessaires pour assurer la liaison avec les Switchs fédérateurs ;
- Matrice de commutation 128 Gbps ;
- Commutation Niveau 2/3 de 95 Mpps ;
- Support de la fonction stacking via des câbles DAC 10 Gbps au minimum ;
- Câble DAC 10 Gbps de 0.5m minimum ;
- Switch manageable via SNMP, CLI et interface web ;
- Le commutateur supporte à être contrôlé et surveillé via un gestionnaire réseau/contrôleur, basé sur une architecture définie par logiciel ou matériel ;
- Support du PoE 802.3af et PoE+ 802.3at ;
- Support VLAN par port ;
- Sécurité et blocage de ports par adresse MAC ;



- Support QoS ;
- Agrégation de liens ;
- L'administration doit permettre la gestion du stack comme un seul commutateur logique.
- Support SDN ;
- Alimentation redondante échangeable à chaud ;
- Support d'une pile minimum de 8 commutateurs visible sur la console de gestion centralisée ;
- Rajout/suppression des membres d'une pile à chaud sans arrêt de fonctionnement ;

**Garantie de 3 ans pièce et main d'œuvre ;**

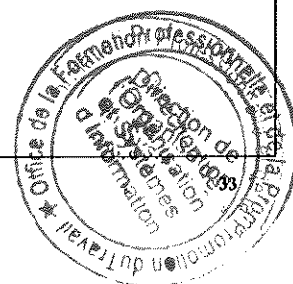
Les commutateurs d'accès doivent être livrés avec les câbles et accessoires nécessaires à leur mise en pile, leur interconnexion ainsi pour leur pose, raccordement et mise en service.

**10. Switch 48 ports (avec PoE+)**

Les commutateurs d'accès auront pour rôle la connectivité au réseau local LAN informatique la totalité des équipements (Microordinateurs, IP phone, stations de travail, imprimantes...)

Ils doivent être de même marque que le switch fédérateur et conformes aux spécifications techniques **minimales** suivantes :

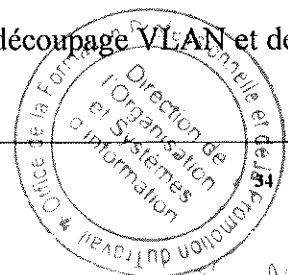
- Marque reconnue mondialement leader **Gartner dans les trois dernières années dans le magic quadrant wired and wireless lan** ;
- Rackable 19'' ;
- **48 ports 10/100/1000 base T PoE/PoE+ minimum** ;
- **4 ports 10 Gigabit SFP+ minimum** (face avant du switch) modulaires pour l'Uplink avec les Switch fédérateurs ;
- **1 Connecteurs 10 Gigabits minimum** connexion nécessaires pour assurer la liaison avec les Switchs fédérateurs ;
- Matrice de commutation **176 Gbps minimum** ;
- Commutation Niveau **2/3**, routage statique et dynamique ;
- Throughput **110 Mpps minimum** ;
- Switch manageable via SNMP, CLI et interface web ;
- Le commutateur supporte à être contrôlé et surveillé via un gestionnaire réseau/contrôleur, basé sur une architecture définie par logiciel ou matériel ;
- Support du PoE 802.3af et PoE+ 802.3at ;
- Support VLAN par port ;
- Sécurité et blocage de ports par adresse MAC ;
- Support QoS ;
- Agrégation de liens ;
- Support SDN ;
- Alimentation redondante échangeable à chaud ;
- Support d'une pile minimum de 8 commutateurs visible sur la console de gestion centralisée ;
- Support Stacking via un câble DAC **10 Gbps minimum** ;
- Câble DAC 10 Gbps de 0.5 m minimum ;
- Être livré avec les licences nécessaires,



AO

Q

|     |  |
|-----|--|
|     | <p><b>Garantie et support constructeur de 3 ans pièce et main d'œuvre ;</b></p> <p>Les commutateurs d'accès doivent être livrés avec les câbles et accessoires nécessaires à sa mise en pile, leur interconnexion ainsi pour leur pose, raccordement et mise en service.</p>   |
| 11. | <p><b><u>Point d'accès Wifi</u></b></p> <p>Les points d'accès doivent être des points d'accès haut débit 802.11 ax. Ces derniers doivent répondre aux spécifications minimales suivantes :</p> <ul style="list-style-type: none"> <li>• Marque reconnue mondialement <b>leader Gartner dans les trois dernières années dans le magic quadrant wired and wireless lan ;</b></li> <li>• Support SNMP v2c, SNMP v3 ;</li> <li>• 802.11a/b/g &amp; 802.11n AP 802.11b/g802.11 ac /802.11 ax (OFDMA) ;</li> <li>• IEEE 802.3af Power over Ethernet;</li> <li>• Authentification 802.1x ;</li> <li>• Connexion sécurisée avec cryptage AES/WPA/WPA2, TLS, PEAP, TTLS, TKIP;</li> <li>• MU-MIMO 4x4 : 4 ;</li> <li>• Débit doit atteindre jusqu'à 2.5 Gbps maximum ;</li> <li>• 1 port PoE+ 2.5 Gigabit minimum ;</li> <li>• Minimum quatre antennes intégrées ;</li> <li>• Bluetooth intégré ;</li> <li>• Dual Radio 802.11ax ;</li> <li>• Mode de fonctionnement : avec et sans contrôleur ;</li> <li>• Kit de montage mural,</li> </ul> <p><b>Garantie et support constructeur de 3 ans pièce et main d'œuvre</b></p> <p>Les Points d'accès doivent être livrés avec les câbles et accessoires nécessaires à leur pose, raccordement, fixation et mise en service.</p>   |
| 12. | <p><b><u>Prestation de service : Installation et mise en service (Directions Régionales)</u></b></p> <p>Le soumissionnaire doit assurer à sa charge la livraison, l'installation et la mise en service, clé en main, des différents équipements objet du présent Appel d'offre (Switching et wifi).</p> <p>Le soumissionnaire doit livrer tous les accessoires et connectiques nécessaires pour la mise en rack et la mise en réseau des équipements objet de cet appel d'offre ;</p> <p>Le soumissionnaire doit assurer le tirage de câble (cat 6 minimum) des dites points d'accès, leurs fixations, et leurs mises en service.</p> <p>Dans le cadre des travaux d'installation et de mise en service de la solution clé en main, le soumissionnaire doit réaliser, au préalable une étude d'ingénierie (dossier d'étude détaillée de l'architecture cible) et proposer une configuration cible des éléments actifs réseaux en tenant compte des exigences des services réseaux opérationnels actuellement et ce en concertation avec l'équipe DOSI/OFPPT, et proposer également un plan de migration des anciens switchs mis en production vers les nouveaux switchs objet de cet AO.</p> <p>Le soumissionnaire doit se baser sur le plan d'adressage IP, de routage, de découpage VLAN et de gestion de la qualité de service existant avec les adaptations nécessaires.</p> |



Le soumissionnaire doit détailler les procédures et outils de tests qui seront utilisés pour assurer les tests de l'installation de la solution.

Les consultants proposés pour la réalisation des prestations d'installation et de mise en service doivent justifier de l'expérience et des compétences nécessaires à cet effet.

Garantie et maintenance (couvre l'assistance 'sur site ou à distance', l'intervention sur site, les pièces de rechanges et la main d'œuvre) pour une durée de trois ans avec un délai de prise en charge de 4 heures après déclaration de l'incident et un délai de 48 heures de résolution ou de contournement du problème ;

#### **Livrables du projet :**

Le titulaire doit fournir une documentation complète contenant :

Un dossier d'ingénierie contenant l'architecture réseau validée (étude adressage, routage, découpage vlan, ... ;

Un plan de migration de l'ancien système vers la nouvelle solution ;

Une documentation technique des équipements installés en langue Française ;

Procédures d'installation, de configuration et d'administration du matériel ;

Un guide technique d'administration et d'exploitation des équipements ;

L'ensemble de la documentation est à fournir sous format papier en deux exemplaires et sous format électronique (USB).

#### **Transfert de compétences**

Le titulaire doit assurer un transfert de compétence permettant à l'équipe de l'OFPPT d'acquérir les connaissances nécessaires pour assurer l'exploitation des équipements installés objet de l'appel d'offres.

Tableau de répartition

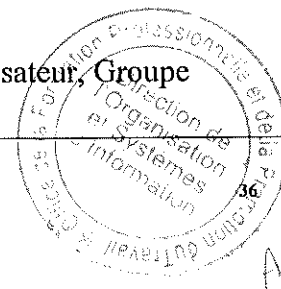
|                     | Siège-<br>SidiMaarouf | Annexe I-<br>SidiMaarouf | Annexe II-Ain<br>Borja | Casablanca- Ain<br>Borja | Béni-Mellal | Laayoune | Er-rachidia | Agadir | Fes | Oujda | Tanger | Rabat | Marrakech | Qte<br>Totale |
|---------------------|-----------------------|--------------------------|------------------------|--------------------------|-------------|----------|-------------|--------|-----|-------|--------|-------|-----------|---------------|
| Switch 48 ports     | 33                    | 1                        | 1                      | 1                        | 0           | 0        | 0           | 1      | 1   | 2     | 0      | 0     | 1         | 41            |
| Switch 24 ports     | 0                     | 2                        | 2                      | 3                        | 1           | 3        | 3           | 2      | 0   | 0     | 2      | 3     | 1         | 22            |
| Points d'accès Wifi | 70                    | 4                        | 6                      | 5                        | 2           | 6        | 2           | 2      | 2   | 3     | 4      | 6     | 4         | 116           |



A. A.

**Lot 2 : Solutions Firewall et SDWAN pour le siège, Annexes siège et directions régionales.**

| <u>Item</u><br><u>N°</u> | <u>Désignation</u>  |
|--------------------------|---|
|                          | <p><b>En vue de renforcer la sécurité du réseau de l'OFPPT, un firewall frontal sera l'objet de ce Lot, il devra être d'une marque différente du firewall dorsal existant (de marque PALOALTO)</b></p> <p><b>Les items N°1 et N°4 doivent être de même marque</b></p>   |
| 1.                       | <p><b>Equipements SDWAN / FIREWALL (Siège)</b></p> <p>La solution cible doit être composée d'une solution SDWAN et Firewall en HA de même marque et respectant au minimum les spécifications techniques cités en bas.</p> <p>La solution proposée peut être composée d'une ou deux Appliances physiques tout en respectant les exigences techniques minimales cumulées des deux solutions suivantes :</p> <p><b><u>Equipement SDWAN :</u></b></p> <ul style="list-style-type: none"> <li>• Marque reconnue mondialement (<b>Leader dans le quadrant magique Gartner « WAN EDGE infrastructure » dans les trois dernières années</b>) ;</li> <li>• Possibilité d'utiliser plusieurs types de liens en actif ; Cuivre Ethernet RJ45, Fibre Ethernet, VLAN, VPN IPsec, 3G/4G Modem USB, ...</li> <li>• Possibilité de créer des tunnels VPN via un assistant graphique sur le Menu SDWan pour une facilité de configuration ;</li> <li>• Offre la possibilité de créer des SLAs intelligentes pour le basculement et le Load Balancing ;</li> <li>• Les SLA doivent se baser sur :             <ul style="list-style-type: none"> <li>✓ L'état de santé du lien avec les protocoles PING, http, TCP et UDP sur deux destinations différentes pour plus de précision</li> <li>✓ SLA basée sur les paramètres de : la latence, la Jitter et la perte de Paquets ;</li> <li>✓ Offrir la visualisation graphique de l'état des SLA par rapport aux paramètres Latence, Jitter et Perte de Paquets ;</li> </ul> </li> <li>• La solution SDWan doit offrir les Méthodes de Load Blancing Suivantes :             <ul style="list-style-type: none"> <li>✓ IP-Source</li> <li>✓ IP-Source-Destination</li> <li>✓ Spillover</li> <li>✓ Sessions</li> <li>✓ Volume</li> </ul> </li> <li>• Offre la possibilité d'utiliser des règles de basculement automatique en se basant sur les paramètres suivant suite au mesure SLA :             <ul style="list-style-type: none"> <li>✓ Best Quality (en se basant sur la : latence, Jitter, Perte de Paquets, Débit Downstream, Débit Upstream et Débit Downstream/Upstream)</li> <li>✓ Lowest Cost</li> <li>✓ Maximize Bandwidth</li> </ul> </li> <li>• Forcer le flux à suivre un lien spécifique manuellement ;</li> <li>• Les règles SDWan doivent se baser sur l'IP Source, IP Destination, Utilisateur, Groupe d'utilisateur, Service Internet, Geo IP, FQDN, Protocol, Application,</li> </ul> |





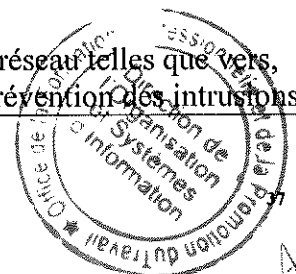
- Doit offrir la possibilité d'associer des politiques QoS pour des flux.
- Offre le contrôle des applications afin d'identifier et reconnaître les applications dans les flux ;
- Management Via interface WEB GUI https ;
- Management via SSH, TELNET et console ;
- Configuration minimale : 8 Ports 1Gbe RJ45 et 2 ports 10Gbe Fibre SFP+ doté de 2 trancivers SFP+ 10Gb) et 2 ports 1Ge SFP (doté de 2 trancivers SFP 1Gbe)
- Throughput VPN IPsec : 20 Gbps minimum
- Support de 1000 tunnels VPN Ipsec Site -to-site ;

### Next-Generation Firewall

- Marque reconnue mondialement (**Leader dans le quadrant magique Gartner « Network Firewalls » dans les trois dernières années**) ;
- Doit intégrer un système d'exploitation propriétaire sécurisé ;
- Filtrage de paquets et être doté de la fonction de filtrage dynamique ;
- Filtrage basé sur les applications niveau 7 en plus des ports/Protocol et par plages de ports UDP ou TCP ;
- Filtrage et inspection en IPv4 et IPv6 ;
- Failover de connexion Internet ;
- Prise en compte de paramètre Horaire dans les règles de filtrage ;
- Doit fournir, via sa console d'administration, des statistiques sur le nombre d'accès aux règles de sécurité ;
- Doit inclure la possibilité de fonctionner en mode transparent ou routé (natté) ;
- Doit fournir la possibilité de définir des instances firewall virtuels sur la même Appliance, et capable d'activer les fonctionnalités de protection IPS, Sandboxing, Control Applicatif, filtrage d'URL, Anti-bot, Anti-virus/Antimalware ;
- La création de la politique de sécurité basée sur :
  - ✓ Geolocation par pays
  - ✓ Zones
  - ✓ Groupes de Zones
  - ✓ Applications, Groupes d'applications
  - ✓ Catégories d'Applications
  - ✓ Technologies d'Applications
  - ✓ Filtres d'Applications
  - ✓ Utilisateurs et Groupes
  - ✓ Adresses IP, Groupes d'adresses IP, Sous-réseaux IP, Groupes de sous-réseaux IP
  - ✓ Services, Groupes de Services

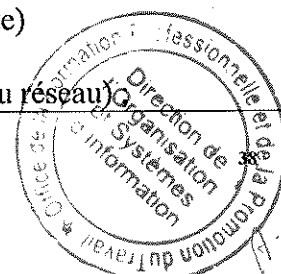
La solution doit être de type Next Generation Firewall avec capacité de prévention contre les menaces avancées, combinée avec des fonctionnalités de base suivantes (**licences incluses**) :

- **IPS (prévention des intrusions)** pour se protéger contre les menaces réseau telles que vers, chevaux de Troie et autres programmes malveillants. Le système de prévention des intrusions



(IPS) doit aussi apporter une protection contre les menaces réseaux existantes et émergentes. Ce module IPS doit avoir deux mécanismes :

- ✓ Détection par signatures ;
- ✓ Détection par anomalies ;
- ✓ Capable de faire des analyses comportementales de tout type de trafic ;
- ✓ Possibilité de créer des signatures personnalisées ;
- ✓ Mise à jour automatique des signatures IPS ;
- ✓ Création et affectation des politiques IPS par type de zone ou interface ;
- ✓ Pour chaque événement d'attaque, il sera possible de laisser passer ou bloquer, de faire une mise en quarantaine automatique (IP totalement bloquée pendant un temps donné) ... ;
- ✓ Gestion de profils IPS avec association à certains trafics dans la politique de filtrage (IP source, IP destination, service, protocole, réseau...) ;
- **Module Antivirus / Antimalware (à fournir)** pour traquer en temps réel les virus, vers, chevaux de Troie, Botnet et autres menaces Internet ;
- **Filtrage URL**, pour assurer le contrôle de l'accès interne aux contenus Web indésirables, non productifs, voire illégaux,
- **Contrôle Applicatif**, afin d'identifier, reconnaître et contrôler les applications dans les flux,
- **Support de la haute disponibilité** :
  - ✓ Actif/Actif avec synchronisation d'état de session,
  - ✓ Actif/Passif,
- **Contrôle applicatif** :
  - ✓ Identification des applications en se basant sur :
    - ✓ Signatures
    - ✓ Décodage du protocole (respecte la spécification du protocole)
    - ✓ Déchiffrement du trafic encapsulé
- Identification et contrôle des applications partageant la même connexion
- Contrôle de la fonction de transfert de fichiers d'une application
- Visibilité du trafic applicatif inconnu à travers l'identification de sa nature :
  - ✓ Volume du trafic
  - ✓ Utilisateur et/ou adresses IP
  - ✓ Port utilisé
  - ✓ Contenu associé : fichier, menace ou autre.
- La base de données de contrôle des applications doit contenir plus de 3 000 applications connues ;
- La solution doit pouvoir créer une règle de filtrage avec plusieurs catégories ;
- **Identification, authentification des utilisateurs et protection des identités**  
Prise en charge des services d'authentification suivants pour l'identification et authentifications des utilisateurs :
  - ✓ Active Directory
  - ✓ Kerberos
  - ✓ LDAP
  - ✓ Radius
  - ✓ Base Locale
  - ✓ SAML
  - ✓ Authentification via SSO Kerberos sans agent
  - ✓ Authentification par Certificat client
  - ✓ Portail captif
- Identification des utilisateurs indépendamment :
  - ✓ Du terminal (ordinateur, un téléphone intelligent ou une tablette)
  - ✓ Du système d'exploitation utilisé,
  - ✓ Des adresses IP et de la zone (LAN, VPN, hors du périmètre du réseau)



- **Fonctions Réseau :**

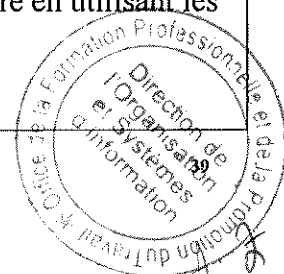
- ✓ Support mode Routage, mode transparent, TAP ou SPAN,
- ✓ Support IPv4 et IPv6
- ✓ Routage IPv4 : Statique et Dynamique, RIPv2, OSPFv3 et BGP au minimum
- ✓ Agrégation des liens 802.3ad, LACP
- ✓ Support des VLAN 802.1q
- ✓ Support des modes de translations NAT et PAT
- ✓ Nat dynamique, Nat Statique, Nat par port, Nat64
- ✓ Support de Multicast

- **Fonction VPN :**

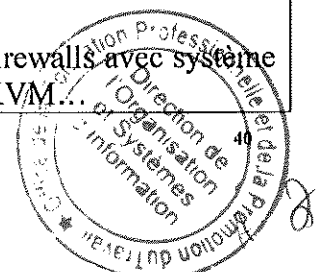
- ✓ VPN IPSec site-site, client-site et hub & Spoke. (Fonctionnalité et licence à fournir)
- ✓ Support du VPN SSL mode portail et mode tunnel (avec ou sans agent)
- ✓ Support du Tunnel GRE
- ✓ Support de IKEv1 et IKEv2 avec authentification à base de clé pré-partagée (PSK) ou certificat
- ✓ Standard de Chiffrement : 3DES, AES 256 au minimum
- ✓ Algorithme de contrôle d'intégrité : MD5, SHA-256, SHA-384, SHA-512,

- **Gestion de la bande passante :**

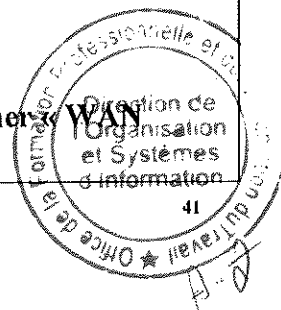
- ✓ Réserve et Priorisation des flux en fonction de la source, la destination, l'utilisateur et l'application,
- ✓ Limitation de la bande passante par source, destination, application ou catégorie d'application.
- ✓ Administration et gestion des journaux :
- ✓ Administration via une interface web intuitive et sécurisée en HTTPS,
- ✓ Administration en ligne de commande SSH et Telnet,
- ✓ Interface d'administration graphique multi-langues : Français et Anglais au minimum,
- ✓ Support de l'administration par rôle,
- ✓ Permettre l'export et l'importation de la configuration,
- ✓ Suivre et visibilité en temps réel sur les flux transitant par le firewall avec possibilité de filtrage,
- ✓ Outil de filtrage et recherche multicritère dans les journaux pour faciliter l'identification des incidents de sécurité.
- ✓ Prise en charge de balises (tags) pour l'organisation des règles et des objets.
- ✓ Différente vue pour les journaux : Flux, Menaces, Filtrage de contenu, Authentification, Systèmes
- ✓ Vue synthétique des applications, menaces et URL,
- ✓ Export des journaux vers des systèmes externes en Syslog et Intégration avec des solutions SIEM
- ✓ Support de SNMPv3
- ✓ Journalisation locale dans le disque du NGFW sans dégradation des performances.
- ✓ La solution doit inclure une autorité de certification x.509 interne qui peut générer des certificats pour les passerelles et les utilisateurs pour permettre une authentification facile sur les VPN,
- ✓ La solution doit inclure la possibilité d'utiliser des autorités de certification externes,
- ✓ La visionneuse de journaux doit avoir la possibilité de créer un filtre en utilisant les noms d'objets prédéfinis (hôtes, réseau, groupes, utilisateurs...) ;



|    |  |
|----|--|
|    | <ul style="list-style-type: none"> <li>• <b>Module Antivirus / Antimalware (licence à fournir) :</b> <ul style="list-style-type: none"> <li>- scan d'un grand nombre de protocoles : <ul style="list-style-type: none"> <li>✓ HTTP</li> <li>✓ HTTPS (Avec déchiffrement SSL)</li> <li>✓ SMTP</li> <li>✓ POP3</li> <li>✓ IMAP</li> <li>✓ MAPI</li> <li>✓ FTP</li> <li>✓ NNTP</li> <li>✓ CIFS</li> <li>✓ SSH (Mode proxy uniquement)</li> </ul> </li> <li>- Support du scan antivirus en mode Flow ou Proxy.</li> <li>- Possibilité de désarmer un fichier Office ou PDF de tout lien hypertexte actif, macros, objets liés ...tout en conservant la lisibilité de son contenu à son destinataire, diminuant ainsi le risque lié aux attaques avancées.</li> </ul> </li> <li>• <b>Filtrage URL et Filtrage de contenu</b> <ul style="list-style-type: none"> <li>✓ Filtrage HTTP, HTTPS, HTTP2 ;</li> <li>✓ Filtrage URL à base de catégories ;</li> <li>✓ Inspection des flux chiffrés TLS 1.3 ;</li> <li>✓ Validation des certificats des serveurs (CRL, Algorithm, Cipher...) ;</li> <li>✓ Filtrage URL à base de l'adresse IP ;</li> <li>✓ Filtrage des liens de phishing dans les e-mails, des sites de phishing ;</li> <li>✓ Filtrage des commandes et contrôles basés sur HTTP et les pages contenant des kits d'exploits ;</li> <li>✓ Filtrage des données en fonction du type de fichier, propriété de fichier, Metadata, mot clés...</li> <li>✓ Mise à jour de la base des URL.</li> </ul> </li> <li>• <b>Licence à fournir : IPS, Antivirus, Filtrage URL, Contrôle applicatif et sandbox cloud pendant une durée de 3 années</b></li> <li>• <b>Performances minimales :</b> <ul style="list-style-type: none"> <li>✓ Dôté de 6 ports 10gbe SFP+ (doté de 6 trancivers SFP+ 10Gb) et 8 ports 1ge RJ45 et 2 ports 1Ge SFP (doté de 2 trancivers SFP 1Gbe)</li> <li>✓ Nombre de sessions simultanées : 7 Millions au minimum</li> <li>✓ Nombre de nouvelles sessions par secondes : 500 000</li> <li>✓ Débit FULL protection : avec activation Firewalling + contrôle applicatif + IPS + inspection antivirus + filtrage URL entreprise MIX (IMIX) de 8 Gbps minimum</li> <li>✓ Double alimentation ;</li> </ul> </li> <li>• Support et Licences pour une durée de 3 ans ;</li> </ul> |
| 2. | <p><b><u>Solution de management centralisé des firewalls</u></b></p> <p>Le soumissionnaire doit proposer une solution logicielle (pour besoin d'évolutivité futur) de gestion et administration centralisée compatible a 100% avec les Firewalls proposés et devant répondre aux spécifications techniques suivantes :</p> <p><b>Performances minimales :</b></p> <ul style="list-style-type: none"> <li>• Solution sous format d'<b>Appliance virtuelle</b> de même marque que les Firewalls avec système d'exploitation auto-protégée compatible avec Vmware ESxi, Hyper-V, KVM...</li> </ul>  |



|    |   |
|----|---|
|    | <ul style="list-style-type: none"> <li>• Permet la gestion centralisée des Firewalls proposés</li> <li>• Permet la gestion des configurations des Firewalls</li> <li>• Permet la gestion des MAJ Firmware des Firewalls</li> <li>• Doté d'au moins de 4 interfaces réseau Giga Ethernet</li> <li>• Espace de stockage Minimum 100 GB extensible pour évolution futur</li> <li>• Licence pour gestion de 20 Firewalls au minimum</li> <li>• Permet de créer des profils et des domaines d'administration différents</li> <li>• Support et Licences pour une durée de 3 ans ;</li> </ul>  |
| 3. | <p><b><u>Solution de gestion centralisée des Logs et de reporting des Firewalls :</u></b></p> <p>Le soumissionnaire doit proposer une solution de gestion logs et de reporting compatible a 100% avec les Firewalls proposés et devant répondre aux spécifications techniques suivantes :</p> <ul style="list-style-type: none"> <li>• Appliance physique Rackable de même marque que les Firewalls ;</li> <li>• L'outil de Reporting doit assumer la collecte et la valorisation des logs générés par les firewalls proposés</li> <li>• Envoyer des alertes par rapport à un évènement bien défini</li> <li>• Disposer d'une interface de consultation des journaux avec un moteur de recherche permettant de filtrer les logs sur de multiples critères. Les filtres supportent le caractère Wildcard ainsi que des opérateurs booléens.</li> <li>• Générer à la demande ou de manière planifiée des rapports dont le contenu sera adapté au profil de leurs destinataires (opérationnel, sécurité, direction, etc.). Ils peuvent être sauvegardés sur un serveur tiers ou être envoyés à leur destinataire par e-mail.</li> <li>• Interface Web de gestion et de consultation des logs et des journaux</li> <li>• Dashboard : afin de rendre compte très synthétiquement de l'activité logging dans l'environnement administré. L'exploitant peut visualiser ainsi à chaque accès, le nombre de logs/sec moyen en cours, ainsi que le nombre et le volume de logs collectés jour par jour, sur une semaine (Ces informations sont très importantes pour déterminer la politique de conservation des logs sur le système et les travaux de capacity planning)</li> <li>• Possibilité de création de plusieurs profils d'administration afin d'y affecter des Firewalls par profil</li> <li>• Affichage d'une carte de menace « Threat Map » afin de montrer les origines des attaques sur une carte géographique mondiale</li> <li>• Module d'indice de compromission.</li> <li>• Capacité de traitement des Logs : <b>25 GB</b> de logs par jour</li> <li>• Espace de stockage : <b>4 TB</b> ;</li> <li>• 4 interfaces GE RJ45 et 2 ports GE SFP ;</li> <li>• Support et Licences pour une durée de 3 ans ;</li> </ul> |
| 4. | <p><b>Equipement SDWAN/FIREWALL (Annexes sièges /Directions régionales)</b></p> <p>La solution cible doit être composée d'une solution SDWAN et Firewall en HA de même marque et respectant au minimum les spécifications techniques cités en bas.</p> <p>La solution proposée peut être composée d'une ou deux Appliances physiques tout en respectant les exigences techniques minimales cumulées des deux solutions suivantes :</p> <p><b><u>Equipement SDWAN :</u></b></p> <ul style="list-style-type: none"> <li>• Marque reconnue mondialement (<b>Leader dans le quadrant magique Gartner « WAN EDGE infrastructure » dans les trois dernières années</b>) : <b>A préciser</b></li> </ul>  |

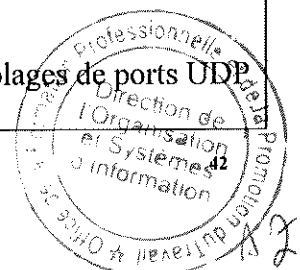


- Possibilité d'utiliser plusieurs types de liens en actif ; Cuivre Ethernet RJ45, Fibre Ethernet, VLAN, VPN IPsec, 3G/4G Modem USB, ...
- Possibilité de créer des tunnels VPN via un assistant graphique sur le Menu SDWan pour une facilité de configuration ;
- Offre la possibilité de créer des SLAs intelligentes pour le basculement et le Load Balancing ;
- Les SLA doivent se baser sur :
  - ✓ L'état de santé du lien avec les protocoles PING, http, TCP et UDP sur deux destinations différentes pour plus de précision
  - ✓ SLA basée sur les paramètres de : la latence, la Jitter et la perte de Paquets ;
  - ✓ Offrir la visualisation graphique de l'état des SLA par rapport aux paramètres Latence, Jitter et Perte de Paquets ;
- La solution SDWan doit offrir les Méthodes de Load Blancing Suivantes :
  - ✓ IP-Source
  - ✓ IP-Source-Destination
  - ✓ Spillover
  - ✓ Sessions
  - ✓ Volume
- Offre la possibilité d'utiliser des règles de basculement automatique en se basant sur les paramètres suivant suite au mesure SLA :
  - ✓ Best Quality (en se basant sur la : latence, Jitter, Perte de Paquets, Débit Downstream, Débit Upstream et Débit Downstream/Upstream)
  - ✓ Lowest Cost
  - ✓ Maximize Bandwidth
- Forcer le flux à suivre un lien spécifique manuellement ;
- Les règles SDWan doivent se baser sur l'IP Source, IP Destination, Utilisateur, Groupe d'utilisateur, Service Internet, Geo IP, FQDN, Protocol, Application,
- Doit offrir la possibilité d'associer des politiques QoS pour des flux.
- Offre le contrôle des applications afin d'identifier et reconnaître les applications dans les flux ;
- Management Via interface WEB GUI https ;
- Management via SSH, TELNET et console ;
- Configuration minimale : **4 Ports 1Gbe RJ45 et 4 ports 1Gbe Fibre**
- Throughput VPN IPsec: **7 Gbps minimum**
- Support de 200 tunnels VPN Ipsec Site -2-site

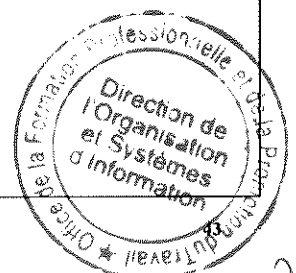
#### Next-Generation Firewall :

##### Fonctions Firewall

- Marque reconnue mondialement (**Leader dans le quadrant magique Gartner « Network Firewalls » dans les trois dernières années**) ;
- Doit intégrer un système d'exploitation propriétaire sécurisé,
- Filtrage de paquets et être doté de la fonction de filtrage dynamique,
- Filtrage basé sur les applications niveau 7 en plus des ports/Protocol et par plages de ports UDP ou TCP

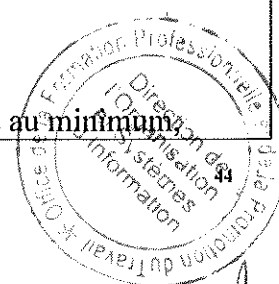


- Filtrage et inspection en IPv4 et IPv6,
- Failover de connexion Internet,
- Prise en compte de paramètre Horaire dans les règles de filtrage,
- Doit fournir, via sa console d'administration, des statistiques sur le nombre d'accès aux règles de sécurité,
- Doit inclure la possibilité de fonctionner en mode transparent ou routé (natté),
- Doit fournir la possibilité de définir des instances firewall virtuels sur la même Appliance, et capable d'activer les fonctionnalités de protection IPS, Sandboxing, Control Applicatif, filtrage d'URL, Anti-bot, Anti-virus/Antimalware,
- La création de la politique de sécurité basée sur :
  - Geolocation par pays
  - Zones
  - Groupes de Zones
  - Applications, Groupes d'applications
  - Catégories d'Applications
  - Technologies d'Applications
  - Filtres d'Applications
  - Utilisateurs et Groupes
  - Adresses IP, Groupes d'adresses IP, Sous-réseaux IP, Groupes de sous-réseaux IP
  - Services, Groupes de Services
- La solution doit être de type Next Generation Firewall avec capacité de prévention contre les menaces avancées, combinée avec des fonctionnalités de base suivantes (**licences incluses**) :
  - **IPS (prévention des intrusions)** pour se protéger contre les menaces réseau telles que vers, chevaux de Troie et autres programmes malveillants. Le système de prévention des intrusions (IPS) doit aussi apporter une protection contre les menaces réseaux existantes et émergentes. Ce module IPS doit avoir deux mécanismes :
    - Détection par signatures ;
    - Détection par anomalies ;
    - Capable de faire des analyses comportementales de tout type de trafic ;
    - Possibilité de créer des signatures personnalisées ;
    - Mise à jour automatique des signatures IPS ;
    - Création et affectation des politiques IPS par type de zone ou interface ;
    - Pour chaque événement d'attaque, il sera possible de laisser passer ou bloquer, de faire une mise en quarantaine automatique (IP totalement bloquée pendant un temps donné) ... ;
    - Gestion de profils IPS avec association à certains trafics dans la politique de filtrage (IP source, IP destination, service, protocole, réseau...) ;
  - **Module Antivirus / Antimalware (à fournir)** pour traquer en temps réel les virus, vers, chevaux de Troie, Botnet et autres menaces Internet ;
  - **Filtrage URL**, pour assurer le contrôle de l'accès interne aux contenus Web indésirables, non productifs, voire illégaux,
  - **Contrôle Applicatif**, afin d'identifier, reconnaître et contrôler les applications dans les flux,
  - **Support de la haute disponibilité** :
    - Actif/Actif avec synchronisation d'état de session,
    - Actif/Passif,
  - **Contrôle applicatif** :
    - Identification des applications en se basant sur :
      - Signatures
      - Décodage du protocole (respecte la spécification du protocole)
      - Déchiffrement du trafic encapsulé
    - Identification et contrôle des applications partageant la même connexion
    - Contrôle de la fonction de transfert de fichiers d'une application



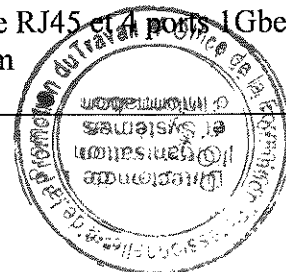
A. 2

- Visibilité du trafic applicatif inconnu à travers l'identification de sa nature :
  - o Volume du trafic
  - o Utilisateur et/ou adresses IP
  - o Port utilisé
  - o Contenu associé : fichier, menace ou autre.
- La base de données de contrôle des applications doit contenir plus de 3 000 applications connues ;
- La solution doit pouvoir créer une règle de filtrage avec plusieurs catégories ;
- **Identification, authentification des utilisateurs et protection des identités**
  - Prise en charge des services d'authentification suivants pour l'identification et authentifications des utilisateurs :
    - ✓ Active Directory
    - ✓ Kerberos
    - ✓ LDAP
    - ✓ Radius
    - ✓ Base Locale
    - ✓ SAML
    - ✓ Authentification via SSO Kerberos sans agent
    - ✓ Authentification par Certificat client
    - ✓ Portail captif
  - Identification des utilisateurs indépendamment :
    - ✓ Du terminal (ordinateur, un téléphone intelligent ou une tablette)
    - ✓ Du système d'exploitation utilisé,
    - ✓ Des adresses IP et de la zone (LAN, VPN, hors du périmètre du réseau)
- **Fonctions Réseau :**
  - ✓ Support mode Routage, mode transparent, TAP ou SPAN,
  - ✓ Support IPv4 et IPv6
  - ✓ Routage IPv4 : Statique et Dynamique, RIPv2, OSPFv3 et BGP au minimum
  - ✓ Agrégation des liens 802.3ad, LACP
  - ✓ Support des VLAN 802.1q
  - ✓ Support des modes de translations NAT et PAT
  - ✓ Nat dynamique, Nat Statique, Nat par port, Nat64
  - ✓ Support de Multicast
- **Fonction VPN :**
  - ✓ VPN IPsec site-site, client-site et hub & Spoke. (Fonctionnalité et licence à fournir)
  - ✓ Support du VPN SSL mode portail et mode tunnel (avec ou sans agent)
  - ✓ Support du Tunnel GRE
  - ✓ Support de IKEv1 et IKEv2 avec authentification à base de clé pré-partagée (PSK) ou certificat
  - ✓ Standard de Chiffrement : 3DES, AES 256 au minimum
  - ✓ Algorithme de contrôle d'intégrité : MD5, SHA-256, SHA-384, SHA-512,
- **Gestion de la bande passante :**
  - ✓ Réserve et Priorisation des flux en fonction de la source, la destination, l'utilisateur et l'application,
  - ✓ Limitation de la bande passante par source, destination, application ou catégorie d'application.
- Administration et gestion des journaux :
- Administration via une interface web intuitive et sécurisée en HTTPS,
- Administration en ligne de commande SSH et Telnet,
- Interface d'administration graphique multi-langues : Français et Anglais au minimum,





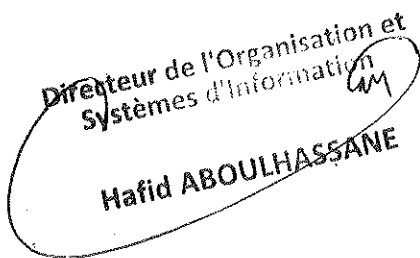
- Support de l'administration par rôle,
- Permettre l'export et l'importation de la configuration,
- Suivre et visibilité en temps réel sur les flux transitant par le firewall avec possibilité de filtrage,
- Outil de filtrage et recherche multicritère dans les journaux pour faciliter l'identification des incidents de sécurité.
- Prise en charge de balises (tags) pour l'organisation des règles et des objets.
- Différente vue pour les journaux : Flux, Menaces, Filtrage de contenu, Authentification, Systèmes
- Vue synthétique des applications, menaces et URL,
- Export des journaux vers des systèmes externes en Syslog et Intégration avec des solutions SIEM
- Support de SNMPv3
- Journalisation locale dans le disque du NGFW sans dégradation des performances.
- La solution doit inclure une autorité de certification x.509 interne qui peut générer des certificats pour les passerelles et les utilisateurs pour permettre une authentification facile sur les VPN,
- La solution doit inclure la possibilité d'utiliser des autorités de certification externes,
- La visionneuse de journaux doit avoir la possibilité de créer un filtre en utilisant les noms d'objets prédéfinis (hôtes, réseau, groupes, utilisateurs...),
- **Module Antivirus / Antimalware (à fournir) :**
  - scan d'un grand nombre de protocoles :
    - ✓ HTTP
    - ✓ HTTPS (Avec déchiffrement SSL)
    - ✓ SMTP
    - ✓ POP3
    - ✓ IMAP
    - ✓ MAPI
    - ✓ FTP
    - ✓ NNTP
    - ✓ CIFS
    - ✓ SSH (Mode proxy uniquement)
  - Support du scan antivirus en mode Flow ou Proxy.
  - Possibilité de désarmer un fichier Office ou PDF de tout lien hypertexte actif, macros, objets liés ...tout en conservant la lisibilité de son contenu à son destinataire, diminuant ainsi le risque lié aux attaques avancées.
- **Filtrage URL et Filtrage de contenu**
  - ✓ Filtrage HTTP, HTTPS, HTTP2 ;
  - ✓ Filtrage URL à base de catégories ;
  - ✓ Inspection des flux chiffrés TLS 1.3 ;
  - ✓ Validation des certificats des serveurs (CRL, Algorithm, Cipher...) ;
  - ✓ Filtrage URL à base de l'adresse IP ;
  - ✓ Filtrage des liens de phishing dans les e-mails, des sites de phishing ;
  - ✓ Filtrage des commandes et contrôles basés sur HTTP et les pages contenant des kits d'exploits ;
  - ✓ Filtrage des données en fonction du type de fichier, propriété de fichier, Metadata, mot clés...
  - ✓ Mise à jour de la base des URL.
- **Licence à fournir :** IPS, Antivirus, Filtrage URL, Contrôle applicatif et sandbox cloud pendant une durée de 3 années
- **Performances minimales :**
  - ✓ Doté au minimum de 2 ports 10Gb SFP+ et de 8 ports 1gbe RJ45 et 4 ports 1Gbe SFP
  - ✓ Nombre de sessions simultanées : 1.5 Millions au minimum
  - ✓ Nombre de nouvelles sessions par secondes : 50 000



|    |   |
|----|---|
|    | ✓ Débit FULL protection : avec activation Firewalling + contrôle applicatif + IPS + inspection antivirusale + filtrage URL entreprise MIX ( IMIX) de 1 Gbps minimum   |
| 5. | <p><b><u>Prestation de service :</u></b></p> <p>Le prestataire doit proposer dans son offre toutes les prestations nécessaires à la mise en œuvre des solutions SDWAN et Firewall au niveau du siège OFPPT, annexes siège et directions régionales.</p> <ul style="list-style-type: none"> <li>• Ingénierie et définition de l'architecture finale ;</li> <li>• Analyse du plan d'adressage IP, de routage et de découpage VLAN ;</li> <li>• L'interconnexion des différents sites ;</li> <li>• Assurer une communication WAN entre les différents sites OFPPT ;</li> <li>• L'installation et la configuration des fonctions du pare feu nouvelle génération selon les bonnes pratiques et les standards de la sécurité ;</li> <li>• La définition de la matrice des flux ;</li> <li>• Le prestataire doit réaliser tout essai jugé nécessaire pour s'assurer de la conformité et du bon fonctionnement de la plateforme de sécurité ;</li> <li>• Transfert de compétence ;</li> <li>• Garantie et maintenance (couvre l'assistance 'sur site ou à distance', l'intervention sur site, les pièces de rechanges et la main d'œuvre) pour une durée de 3 ans avec un délai de prise en charge de 2 heures après déclaration de l'incident et un délai de 4 heures de résolution ou de contournement du problème et 48 h en cas de remplacement ;</li> <li>• Livrables : <ul style="list-style-type: none"> <li>✓ Document d'architecture finale et de configuration de la solution (avec schéma au format exploitable et un fichier de configuration) ;</li> <li>✓ Manuel d'exploitation ;</li> </ul> </li> </ul> |

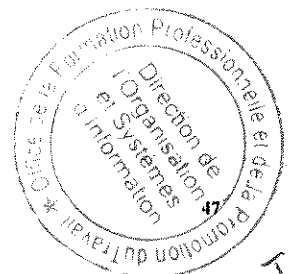
Tableau de répartition

|                | Siège-<br>SidiMaarouf | Annexe I-<br>SidiMaarouf | Annexe II-Ain<br>Borja | Casablanca-<br>Ain Borja | Béni-Mellal | Laayoune | Er-Rachidia | Agadir | Fès | Oujda | Tanger | Rabat | Marrakech |
|----------------|-----------------------|--------------------------|------------------------|--------------------------|-------------|----------|-------------|--------|-----|-------|--------|-------|-----------|
| SDWAN-Firewall | 2                     | 1                        | 1                      | 1                        | 1           | 1        | 1           | 1      | 1   | 1     | 1      | 1     | 1         |

| LE SOUMISSIONNAIRE | LE MAÎTRE D'OUVRAGE   |
|--------------------|---|
| Lu et accepté      |  <p>Directeur de l'Organisation et<br/>Systèmes d'Information</p> <p>Hafid ABLOUHASSANE</p> |

## **ANNEXE :**

### **Spécifications techniques des fournitures proposées par le concurrent**



A. J.

# La refonte des solutions réseaux (LAN/WAN) et de sécurité au niveau du siège, annexes du siège et des directions régionales.

## Lot 1 : Solutions Switching, Wifi et SDN pour le Siège OFPPT, annexes siège et directions régionales.

N.B : les soumissionnaires sont invités à remplir la case <<Proposition du soumissionnaire >> en précisant les caractéristiques du matériel proposé.

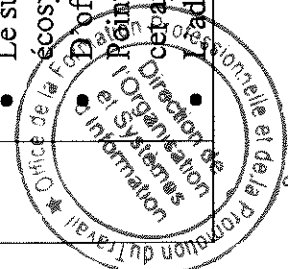
Tout article ne répondant pas aux spécifications demandées sera déclaré non-conforme.

Les colonnes « Désignations et caractéristiques techniques » et « Appréciation de l'administration » >> ne doivent pas être renseignées ou modifiées.

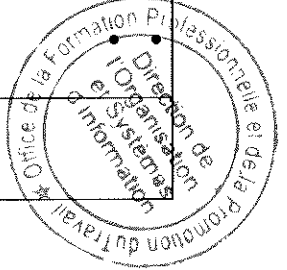
Le concurrent est tenu de renseigner pour chaque item, la marque, la référence et les caractéristiques des fournitures proposées et ce, dans le cadre de la colonne « Proposition du soumissionnaire » et la ligne correspondante à l'item.

Les valeurs des dimensions, longueurs, capacités, ..... Doivent être renseignées d'une manière précise dans la colonne « Proposition du soumissionnaire ».

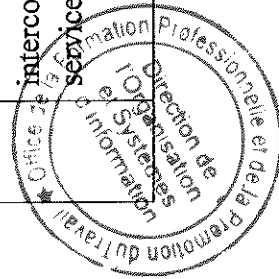
| N°<br>ITEM   | Désignation et caractéristiques techniques minimales   | Qte | Proposition du soumissionnaire | Appréciation<br>de<br>l'administration |
|--|--|-----|--------------------------------|--|
| Partie 1 : Solutions SDN, Switching et Wifi pour le siège, Annexe I-SidiMaarouf et Annexe II-Ain Borja |  |     |                                |  |
| 1.   | <p><u>Contrôleur SDN :</u></p> <p>La solution doit être installée au niveau du Datacenter du siège, elle doit être de même marque que les solutions de switching et wifi proposées dans cet appel d'offre, elle doit permettre :</p> <ul style="list-style-type: none"> <li>• La gestion et l'administration des ressources et équipements réseau LAN objet de cet appel d'offre (Items 2,3,4,5,6,7,9,10 et 11) ;</li> <li>• D'assurer l'intégration avec les modules d'authentification et contrôle d'accès au réseau ;</li> <li>• Le support de l'intégration avec des plateformes Cloud et écosystème tiers via les API ;</li> <li>• D'offrir une cartographie physique et logique des switches, Points d'accès, équipements connectés aux switches objet de cet appel d'offres ;</li> <li>• L'administration centralisée LAN et WLAN simplifiée :</li> </ul> |     |                                |  |



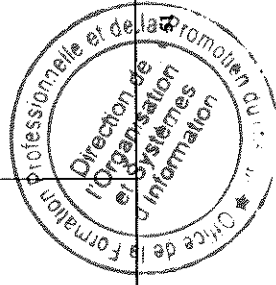
|           |   |  |  |
|-----------|---|--|--|
|           | <ul style="list-style-type: none"> <li>✓ Tagging des ports de plusieurs switches managés par simple clic ;</li> <li>✓ Supervision centralisée de l'état de santé des switches ;</li> <li>✓ Vue de la topologie physique des switches par code couleur (Ring, Uplink, Agrégation des liens, ...) ;</li> <li>✓ Vue du consommation POE au niveau de chaque port et chaque switch ;</li> <li>✓ Permet la gestion de tous les aspects de maintenance et gestion opérationnelle des switches et des points d'accès : enregistrement, provisionning, upgrade firmware, commande CLI ;</li> <li>✓ Provisionning des SSIDs simplifié et centralisé ;</li> <li>✓ Possibilité d'importer un Plan architecturale du bâtiment et de positionner les points d'accès sur la carte. Cette fonctionnalité permet d'afficher en temps réel l'état, l'emplacement du point d'accès lors de recherches non structurées ;</li> <li>✓ Module d'analyse spectrale permettant de voir les interférences de signal,</li> <li>✓ Module d'analyse applicative : avoir la capacité de lister tout le trafic applicatif des utilisateurs ;</li> </ul> |  |  |
| <p>2.</p> | <p><b><u>Switch fédérateur :</u></b></p> <p>Les Switch fédérateurs doivent être de même marque que les contrôleurs SDN / et doivent avoir les caractéristiques minimales suivantes :</p> <ul style="list-style-type: none"> <li>• Marque reconnue mondialement leader Gartner dans les trois dernières années dans le magic quadrant wired and wireless lan ;</li> <li>• Rackable 19" ;</li> <li>• 2 ports de 40 G minimum (face avant du switch) ;</li> </ul>  |  |  |



|  |   |  |
|--|---|--|
|  | <ul style="list-style-type: none"> <li>• 2 modules QSFP+ 40 G minimum (A prévoir deux câbles fibre optique adéquats pour une distance de 10 mètres minimum ou le câble AOC (actif optique câble)) ;</li> <li>• 48 ports 10 Gigabit SFP+ pour les Uplink des Switchs d'accès minimum,</li> <li>• 20 Connecteurs 10 Gigabits SFP+ SR nécessaires pour assurer l'interconnexion avec les switchs des sous répartiteurs ;</li> <li>• 4 Connecteurs 1 Gigabits Base T minimum ;</li> <li>• Capacité de commutation 2 Tpbs minimum ;</li> <li>• Débit de paquet évolutif minimum 900 Mpps ;</li> <li>• Switch manageable via SNMP, CLI et interface web ;</li> <li>• Routage Statique et Dynamique ;</li> <li>• Modules échangeables à chaud ;</li> <li>• Alimentation redondante échangeable à chaud ;</li> <li>• Le commutateur supporte à être contrôlé et surveillé via un gestionnaire réseau/contrôleur, basé sur une architecture définie par logiciel ou matériel ;</li> <li>• Stacking et SDN ;</li> <li>• Être livré avec les licences nécessaires ;</li> </ul> <p><b>Garantie et support constructeur de 3 ans pièce et main d'œuvre</b></p> <p>NB : Les Deux Switchs Fédérateurs doivent :</p> <ul style="list-style-type: none"> <li>-Fonctionner de façon redondante et en partage de charge ;</li> <li>-Être équipés de liens d'agrégation de 40 Gbps minimum pour la synchronisation et transfert de données,</li> <li>-Être livrés avec les câbles et les accessoires nécessaires à leur interconnexion ainsi pour leur pose, raccordement, et mise en service.</li> </ul> |  |
|--|---|--|

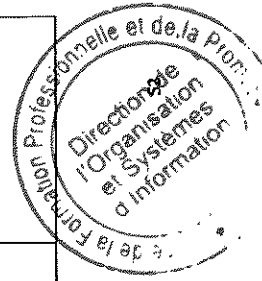


|    |  |  |                 |
|----|--|--|-----------------|
| 3. | <p><b><u>Switch multi Giga (avec PoE+)</u></b></p> <p>Les commutateurs d'accès auront pour rôle la connectivité au réseau local LAN informatique la totalité des équipements (Points d'accès wifi 6 ; Microordinateurs, IP phone, stations de travail, imprimantes...).</p> <p>Ils doivent être de même marque que le switch fédérateur et conformes aux spécifications techniques minimales suivantes :</p> <ul style="list-style-type: none"> <li>• Marque reconnue mondialement <b>leader Gartner dans les trois dernières années dans le magic quadrant wired and wireless lan</b> ;</li> <li>• Rackable 19" ;</li> <li>• 8 ports Multi Giga 1/2.5base T PoE/PoE+ minimum ;</li> <li>• 40 ports 1 Gigabits Base T minimum PoE/PoE+ ;</li> <li>• 4 ports 10 Gigabit SFP+ minimum (face avant du switch) modulaires pour l'Uplink avec les Switch fédérateurs ;</li> <li>• 2 connecteurs 10 Gigabit SFP+ ;</li> <li>• Support SDN ;</li> <li>• Matrice de commutation <b>200 Gbps</b> minimum ;</li> <li>• Commutation Niveau 2/3, Routage Statique et Dynamique ;</li> <li>• Throughput <b>110 Mpps</b> minimum ;</li> <li>• Switch manageable via SNMP, CLI et interface web ;</li> <li>• Support du PoE 802.3af et PoE+ 802.3at ;</li> <li>• Support VLAN par port ;</li> <li>• Sécurité et blocage de ports par adresse MAC ;</li> <li>• Support QoS ;</li> <li>• Agrégation de liens ;</li> <li>• Support d'une pile minimum de 8 commutateurs visible sur la console de gestion centralisée ;</li> </ul> |  | <p><b>p</b></p> |
|----|--|--|-----------------|



01. 2

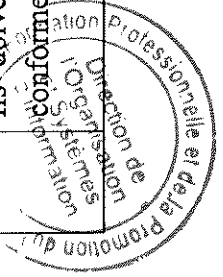
|    |  |  |  |
|----|--|--|--|
|    | <ul style="list-style-type: none"> <li>Alimentation redondante échangeable à chaud ;</li> <li>Être livré avec les licences nécessaires,</li> </ul> <p><b>Garantie et support constructeur de 3 ans pièce et main d'œuvre</b></p> <p>Ces commutateurs doivent être livrés avec les câbles et les accessoires nécessaires à leur interconnexion ainsi pour leur pose, raccordement, et mise en service,</p>  |  |  |
| 4. | <p><b><u>Switch 48 ports (avec PoE+)</u></b></p> <p>Les commutateurs d'accès auront pour rôle la connectivité au réseau local LAN informatique la totalité des équipements (Microordinateurs, IP phone, stations de travail, imprimantes...)</p> <p>Ils doivent être de même marque que le switch fédérateur et conformes aux spécifications techniques <b>minimales</b> suivantes :</p> <ul style="list-style-type: none"> <li>Marque reconnue mondialement <b>leader Gartner</b> dans les <b>trois dernières années dans le magic quadrant wired and wireless lan</b> ;</li> <li>Rackable 19" ;</li> <li>48 ports 10/100/1000 base T PoE/PoE+ minimum ;</li> <li>4 ports 10 Gigabit SFP+ minimum (face avant du switch) modulaires pour l'Uplink avec les Switch fédérateurs ;</li> <li>1 Connecteurs 10 Gigabits minimum connexion nécessaires pour assurer la liaison avec les Switchs fédérateurs ;</li> <li>Matrice de commutation <b>176 Gbps</b> minimum ;</li> <li>Commutation Niveau 2/3, routage statique et dynamique ;</li> <li>Throughput <b>110 Mpps</b> minimum ;</li> <li>Switch manageable via SNMP, CLI et interface web ;</li> </ul> |  |  |



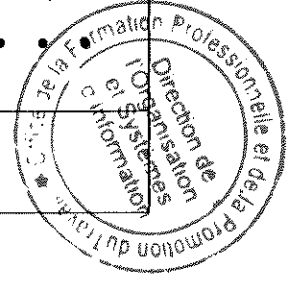
Signature



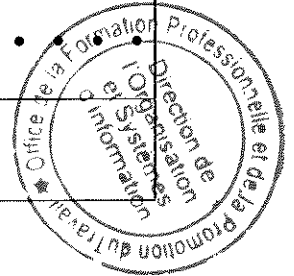
|   |   |  |  |
|---|---|--|--|
|   | <ul style="list-style-type: none"> <li>Le commutateur supporte à être contrôlé et surveillé via un gestionnaire réseau/contrôleur, basé sur une architecture définie par logiciel ou matériel ;</li> <li>Support du PoE 802.3af et PoE+ 802.3at ;</li> <li>Support VLAN par port ;</li> <li>Sécurité et blocage de ports par adresse MAC ;</li> <li>Support QoS ;</li> <li>Agrégation de liens ;</li> <li>Support SDN ;</li> <li>Alimentation redondante échangeable à chaud ;</li> <li>Support d'une pile minimum de 8 commutateurs visible sur la console de gestion centralisée ;</li> <li>Support Stacking via un câble DAC 10 Gbps minimum ;</li> <li>Câble DAC 10 Gbps de 0.5 m minimum ;</li> <li>Être livré avec les licences nécessaires,</li> </ul> <p><b>Garantie et support constructeur de 3 ans pièce et main d'œuvre ;</b></p> <p>Les commutateurs d'accès doivent être livré avec les câbles et accessoires nécessaires à sa mise en pile, leur interconnexion ainsi pour leur pose, raccordement et mise en service.</p> |  |  |
| 5 | <p><b><u>Switch 24 ports (avec PoE+)</u></b></p> <p>Les commutateurs d'accès auront pour rôle la connectivité au réseau local LAN informatique la totalité des équipements (Microordinateurs, IP phone, stations de travail, imprimantes...).</p> <p>Ils doivent être de même marque que le switch fédérateur et conformes aux spécifications techniques minimum suivantes :</p>  |  |  |



|  |  |  |  |
|--|--|--|--|
|  | <ul style="list-style-type: none"> <li>• Marque reconnue mondialement, leader Gartner dans les trois dernières années dans le magic quadrant wired and wireless lan ;</li> <li>• Rackable 19" ;</li> <li>• 24 ports 10/100/1000 base T PoE/PoE+ minimum ;</li> <li>• 4 ports 10 Gigabit SFP+ dédiés minimum (face avant du switch) modulaire pour l'Uplink avec les Switch fédérateurs ;</li> <li>• 1 Connecteurs 10 Gigabits minimum connexion nécessaires pour assurer la liaison avec les Switchs fédérateurs ;</li> <li>• Matrice de commutation 128 Gbps ;</li> <li>• Commutation Niveau 2/3 de 95 Mpps ;</li> <li>• Support de la fonction stacking via des câbles DAC 10 Gbps au minimum ;</li> <li>• Câble DAC 10 Gbps de 0.5m minimum ;</li> <li>• Switch manageable via SNMP, CLI et interface web ;</li> <li>• Le commutateur supporte à être contrôlé et surveillé via un gestionnaire réseau/contrôleur, basé sur une architecture définie par logiciel ou matériel ;</li> <li>• Support du PoE 802.3af et PoE+ 802.3at ;</li> <li>• Support VLAN par port ;</li> <li>• Sécurité et blocage de ports par adresse MAC ;</li> <li>• Support QoS ;</li> <li>• Agrégation de liens ;</li> <li>• L'administration doit permettre la gestion du stack comme un seul commutateur logique.</li> <li>• Support SDN ;</li> <li>• Alimentation redondante échangeable à chaud ;</li> <li>• Support d'une pile minimum de 8 commutateurs visible sur la console de gestion centralisée ;</li> </ul> |  |  |
|--|--|--|--|



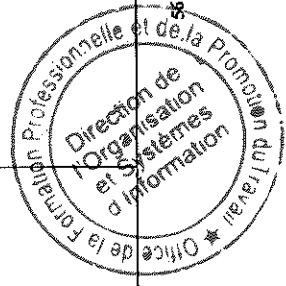
|   |  |  |  |
|---|--|--|--|
|   | <ul style="list-style-type: none"> <li>Rajout/suppression des membres d'une pile à chaud sans arrêt de fonctionnement ;</li> </ul> <p><b>Garantie de 3 ans pièce et main d'œuvre ;</b></p> <p>Les commutateurs d'accès doivent être livré avec les câbles et accessoires nécessaires à leur mise en pile, leur interconnexion ainsi pour leur pose, raccordement et mise en service.</p>   |  |  |
| 6 | <p><b><u>Contrôleur Wifi</u></b></p> <p>Il s'agit de fourniture, et de mise en service d'un contrôleur WiFi virtuel qui doit contrôler les points d'accès 802.11 ax et permettre d'avoir les spécifications minimales suivantes :</p> <ul style="list-style-type: none"> <li>Marque reconnue mondialement, <b>leader Gartner dans les trois dernières années dans le magic quadrant wired and wireless lan ;</b></li> <li>Type virtuel ;</li> <li>Le contrôleur prend en charge les dernières normes Wi-Fi Alliance telles que Wi-Fi 6 (802.11ax) et 802.11ad, ainsi que les protocoles de sécurité WPA3.</li> <li>Support SNMP ;</li> <li>Configuration à distance à travers une interface graphique WEB (Secure WEB GUI) ;</li> <li>Support de serveur RADIUS ;</li> <li>DNS et SMTP ;</li> <li>DHCP ;</li> <li>AAA Security ;</li> <li>Support de Vo WLAN ;</li> <li>Support de WIPS ;</li> <li>Authentification 802.1x, MAC et WEB (portal captif) ;</li> <li>Standards wifi IEEE 802.11ax ;</li> <li>Sécurité : AES/WPA2/WPA3 entreprise ;</li> </ul> |  |  |



- La configuration du contrôleur WIFI doit supporter **120** points accès WIFI minimum extensible à **250** ;
- Être livré avec les licences nécessaires pour la gestion de **116** APs, Analyse spectrale, et détection des APs Rogue.
- Nombre client 4 000 minimum ;
- Le contrôleur WIFI doit être automatisable via API
- Le contrôleur doit supporter un mécanisme d'HA en mode cluster Actif/Actif pour assurer une haute disponibilité du service Wifi ;
- L'itinérance des dispositifs d'une borne à l'autre à niveau 2 ainsi qu'à niveau 3 ;
- Le contrôleur WLAN proposé doit avoir la certification FIPS-140 ou équivalent ;
- De gérer des politiques de sécurité individualisées ou aux groupes d'utilisateurs usant l'accès WIFI ;
- D'appliquer les politiques relatives aux configurations et aux comportements clients pour interdire l'accès au réseau aux unités utilisateurs qui ne disposent pas des configurations de sécurité adéquate ;
- D'offrir une sécurité supplémentaire pour l'accès au réseau de l'entreprise par les utilisateurs invités. Il garantit que ces utilisateurs ne pourront pas accéder au réseau sans passer d'abord par le pare-feu ;
- Le contrôleur doit avoir un portail captif afin d'authentifier les utilisateurs,

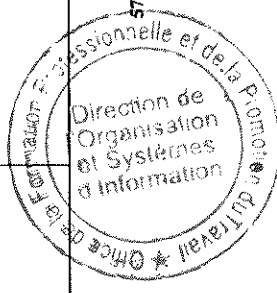
**Garantie et support constructeur de 3 ans pièce et main d'œuvre**

NB : Le contrôleur WIFI doit :



Q A

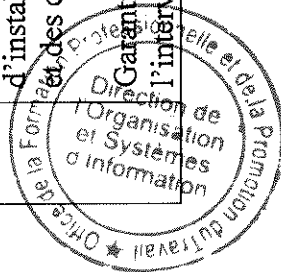
|    |   |  |  |
|----|---|--|--|
|    | -Être livré avec les câbles et les accessoires nécessaires à son interconnexion ainsi pour sa pose, raccordement, et mise en service,   |  |  |
| 7. | <p><b><u>Point d'accès Wifi</u></b></p> <p>Les points d'accès doivent être des points d'accès haut débit 802.11 ax. Ces derniers doivent répondre aux spécifications minimales suivantes :</p> <ul style="list-style-type: none"> <li>• Marque reconnue mondialement <b>leader Gartner dans les trois dernières années dans le magic quadrant wired and wireless lan ;</b></li> <li>• Support SNMP v2c, SNMP v3 ;</li> <li>• 802.11a/b/g &amp; 802.11n AP 802.11b/g802.11 ac /802.11 ax (OFDMA) ;</li> <li>• IEEE 802.3af Power over Ethernet;</li> <li>• Authentification 802.1x ;</li> <li>• Connexion sécurisée avec cryptage AES/WPA/WPA2, TLS, PEAP, TTLS, TKIP;</li> <li>• MU-MIMO 4x4 : 4 ;</li> <li>• Débit doit atteindre jusqu'à 2.5 Gbps maximum ;</li> <li>• 1 port PoE+ 2.5 Gigabit minimum ;</li> <li>• Minimum quatre antennes intégrées ;</li> <li>• Bluetooth intégré ;</li> <li>• Dual Radio 802.11ax ;</li> <li>• Mode de fonctionnement : avec et sans contrôleur ;</li> <li>• Kit de montage mural,</li> </ul> <p><b>Garantie et support constructeur de 3 ans pièce et main d'œuvre</b></p> <p>Les Points d'accès doivent être livré avec les câbles et accessoires nécessaires à leur pose, raccordement, fixation et mise en service.</p> |  |  |



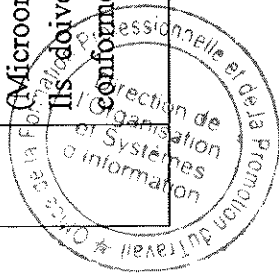
①

2

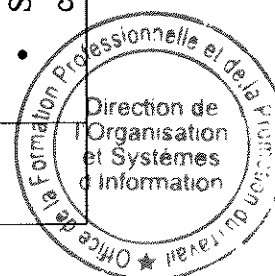
|    |  |  |
|----|--|--|
| 8. | <p><b>Prestation de service : Installation et mise en service (Siège et annexes sièges)</b></p> <p>Le soumissionnaire doit assurer à sa charge la livraison, l'installation et la mise en service, clé en main, des différents équipements objet du présent Appel d'offre (Switching et wifi).</p> <p>Le soumissionnaire doit livrer tous les accessoires et connectiques nécessaires pour la mise en rack et la mise en réseau des équipements objet de cet appel d'offre ;</p> <p>Le soumissionnaire doit assurer le tirage de câble (cat 6 minimum) des dites points d'accès, leurs fixations, et leurs mises en service.</p> <p>Dans le cadre des travaux d'installation et de mise en service de la solution clé en main, le soumissionnaire doit réaliser, au préalable une étude d'ingénierie (dossier d'étude détaillée de l'architecture cible) et proposer une configuration cible des éléments actifs réseaux en tenant compte des exigences des services réseaux opérationnels actuellement et ce en concertation avec l'équipe DOSI/OFPPT, et proposer également un plan de migration des anciens switches mis en production vers les nouveaux switches objet de cet AO.</p> <p>Le soumissionnaire doit se baser sur le plan d'adressage IP, de routage, de découpage VLAN et de gestion de la qualité de service existant avec les adaptations nécessaires.</p> <p>Le soumissionnaire doit détailler les procédures et outils de tests qui seront utilisés pour assurer les tests de l'installation de la solution.</p> <p>Les consultants proposés pour la réalisation des prestations d'installation et de mise en service doivent justifier de l'expérience et des compétences nécessaires à cet effet.</p> |  |
|----|--|--|



|    |  |  |  |
|----|--|--|--|
|    | <p>pour une durée de 3 ans avec un délai de prise en charge de 2 heures après déclaration de l'incident et un délai de 4 heures de résolution ou de contournement du problème ;</p> <p><b>Livrables du projet :</b><br/>         Le titulaire doit fournir une documentation complète contenant :<br/>         Un dossier d'ingénierie contenant l'architecture réseau validée (étude adressage, routage, découpage vlan, ... ;<br/>         Un plan de migration de l'ancien système vers la nouvelle solution ;<br/>         Une documentation technique des équipements installés en langue Française ;<br/>         Procédures d'installation, de configuration et d'administration du matériel ;<br/>         Un guide technique d'administration et d'exploitation des équipements ;<br/>         L'ensemble de la documentation est à fournir sous format papier en deux exemplaires et sous format électronique (USB).</p> <p><b>Transfert de compétences</b><br/>         Le titulaire doit assurer un transfert de compétence permettant à l'équipe de l'OFPPT d'acquérir les connaissances nécessaires pour assurer l'exploitation des équipements installés objet de l'appel d'offres.</p> |  |  |
|    | <b>Partie 2 : Solutions SDN, Switching et Wifi pour les directions régionales</b>  |  |  |
| 9. | <p><b>Switch 24 ports (avec PoE+)</b><br/>         Les commutateurs d'accès auront pour rôle la connectivité au réseau local LAN informatique la totalité des équipements (Microordinateurs, IP phone, stations de travail, imprimantes...).<br/>         Ils doivent être de même marque que le switch fédérateur et conformes aux spécifications techniques minimum suivantes :</p>  |  |  |

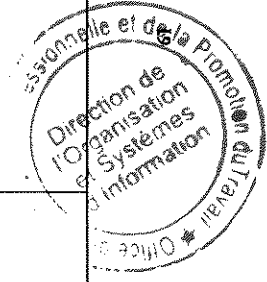


|  |   |  |
|--|---|--|
|  | <ul style="list-style-type: none"> <li>• Marque reconnue mondialement, leader Gartner dans les trois dernières années dans le magic quadrant wired and wireless lan ;</li> <li>• Rackable 19’’ ;</li> <li>• 24 ports 10/100/1000 base T PoE/PoE+ minimum ;</li> <li>• 4 ports 10 Gigabit SFP+ dédiés minimum (face avant du switch) modulaire pour l’Uplink avec les Switch fédérateurs ;</li> <li>• 1 Connecteurs 10 Gigabits minimum connexion nécessaires pour assurer la liaison avec les Switchs fédérateurs ;</li> <li>• Matrice de commutation 160 Gbps ;</li> <li>• Commutation Niveau 2/3 de 95 Mpps ;</li> <li>• Support de la fonction stacking via des câbles DAC 10 Gbps au minimum ;</li> <li>• Câble DAC 10 Gbps de 0.5m minimum ;</li> <li>• Switch manageable via SNMP, CLI et interface web ;</li> <li>• Le commutateur supporte à être contrôlé et surveillé via un gestionnaire réseau/contrôleur, basé sur une architecture définie par logiciel ou matériel ;</li> <li>• Support du PoE 802.3af et PoE+ 802.3at ;</li> <li>• Support VLAN par port ;</li> <li>• Sécurité et blocage de ports par adresse MAC ;</li> <li>• Support QoS ;</li> <li>• Agrégation de liens ;</li> <li>• L’administration doit permettre la gestion du stack comme un seul commutateur logique.</li> <li>• Support SDN ;</li> <li>• Alimentation redondante échangeable à chaud ;</li> <li>• Support d’une pile minimum de 8 commutateurs visible sur la console de gestion centralisée ;</li> </ul> |  |
|--|---|--|





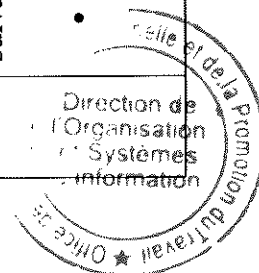
|     |   |  |  |
|-----|---|--|--|
|     | <ul style="list-style-type: none"> <li>Rajout/suppression des membres d'une pile à chaud sans arrêt de fonctionnement ;</li> </ul> <p><b>Garantie de 3 ans pièce et main d'œuvre ;</b><br/>Les commutateurs d'accès doivent être livré avec les câbles et accessoires nécessaires à leur mise en pile, leur interconnexion ainsi pour leur pose, raccordement et mise en service.</p>   |  |  |
| 10. | <p><b><u>Switch 48 ports (avec PoE+)</u></b></p> <p>Les commutateurs d'accès auront pour rôle la connectivité au réseau local LAN informatique la totalité des équipements (Microordinateurs, IP phone, stations de travail, imprimantes...)</p> <p>Ils doivent être de même marque que le switch fédérateur et conformes aux spécifications techniques <b>minimales</b> suivantes :</p> <ul style="list-style-type: none"> <li>Marque reconnue mondialement <b>leader Gartner dans les trois dernières années dans le magic quadrant wired and wireless lan ;</b></li> <li>Rackable 19" ;</li> <li>48 ports 10/100/1000 base T PoE/PoE+ minimum ;</li> <li>4 ports 10 Gigabit SFP+ minimum (face avant du switch) modulaires pour l'Uplink avec les Switch fédérateurs ;</li> <li>1 Connecteurs 10 Gigabits minimum connexion nécessaires pour assurer la liaison avec les Switchs fédérateurs ;</li> <li>Matrice de commutation <b>176 Gbps</b> minimum ;</li> <li>Commutation Niveau 2/3, routage statique et dynamique ;</li> <li>Throughput <b>110 Mpps</b> minimum ;</li> <li>Switch manageable via SNMP, CLI et interface web ;</li> </ul> |  |  |



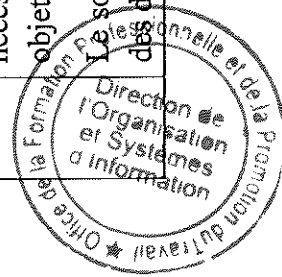
Signature

Signature

|     |   |  |  |
|-----|---|--|--|
|     | <ul style="list-style-type: none"> <li>Le commutateur supporte à être contrôlé et surveillé via un gestionnaire réseau/contrôleur, basé sur une architecture définie par logiciel ou matériel ;</li> <li>Support du PoE 802.3af et PoE+ 802.3at ;</li> <li>Support VLAN par port ;</li> <li>Sécurité et blocage de ports par adresse MAC ;</li> <li>Support QoS ;</li> <li>Agrégation de liens ;</li> <li>Support SDN ;</li> <li>Alimentation redondante échangeable à chaud ;</li> <li>Support d'une pile minimum de 8 commutateurs visible sur la console de gestion centralisée ;</li> <li>Support Stacking via un câble DAC 10 Gbps minimum ;</li> <li>Câble DAC 10 Gbps de 0.5 m minimum ;</li> <li>Être livré avec les licences nécessaires,</li> </ul> <p><b>Garantie et support constructeur de 3 ans pièce et main d'œuvre ;</b></p> <p>Les commutateurs d'accès doivent être livré avec les câbles et accessoires nécessaires à sa mise en pile, leur interconnexion ainsi pour leur pose, raccordement et mise en service.</p> |  |  |
| 11. | <p><b><u>Point d'accès Wifi</u></b></p> <p>Les points d'accès doivent être des points d'accès haut débit 802.11 ax. Ces derniers doivent répondre aux spécifications minimales suivantes :</p> <ul style="list-style-type: none"> <li>Marque reconnue mondialement leader Gartner dans les trois dernières années dans le magic quadrant wired and wireless lan ;</li> </ul>  |  |  |



|     |   |  |
|-----|---|--|
|     | <ul style="list-style-type: none"> <li>• Support SNMP v2c, SNMP v3 ;</li> <li>• 802.11a/b/g &amp; 802.11n AP 802.11b/g802.11 ac /802.11 ax (OFDMA) ;</li> <li>• IEEE 802.3af Power over Ethernet;</li> <li>• Authentification 802.1x ;</li> <li>• Connexion sécurisée avec cryptage AES/WPA/WPA2, TLS, PEAP, TTLS, TKIP;</li> <li>• MU-MIMO 4x4 : 4 ;</li> <li>• Débit doit atteindre jusqu'à 2.5 Gbps maximum ;</li> <li>• 1 port PoE+ 2.5 Gigabit minimum ;</li> <li>• Minimum quatre antennes intégrées ;</li> <li>• Bluetooth intégré ;</li> <li>• Dual Radio 802.11ax ;</li> <li>• Mode de fonctionnement : avec et sans contrôleur ;</li> <li>• Kit de montage mural,</li> </ul> <p><b>Garantie et support constructeur de 3 ans pièce et main d'œuvre</b><br/>Les Points d'accès doivent être livré avec les câbles et accessoires nécessaires à leur pose, raccordement, fixation et mise en service.</p> |  |
| 12. | <p><b>Prestation de service : Installation et mise en service (Directions Régionales)</b></p> <p>Le soumissionnaire doit assurer à sa charge la livraison, l'installation et la mise en service, clé en main, des différents équipements objet du présent Appel d'offre (Switching et wifi).</p> <p>Le soumissionnaire doit livrer tous les accessoires et connectiques nécessaires pour la mise en rack et la mise en réseau des équipements objet de cet appel d'offre ;</p> <p>Le soumissionnaire doit assurer le tirage de câble (cat 6 minimum) des dites points d'accès, leurs fixations, et leurs mises en service.</p>  |  |



A.2

Dans le cadre des travaux d'installation et de mise en service de la solution clé en main, le soumissionnaire doit réaliser, au préalable une étude d'ingénierie (dossier d'étude détaillée de l'architecture cible) et proposer une configuration cible des éléments actifs réseaux en tenant compte des exigences des services réseaux opérationnels actuellement et ce en concertation avec l'équipe DOSI/QFPPT, et proposer également un plan de migration des anciens switchs mis en production vers les nouveaux switchs objet de cet AO.

Le soumissionnaire doit se baser sur le plan d'adressage IP, de routage, de découpage VLAN et de gestion de la qualité de service existant avec les adaptations nécessaires.

Le soumissionnaire doit détailler les procédures et outils de tests qui seront utilisés pour assurer les tests de l'installation de la solution.

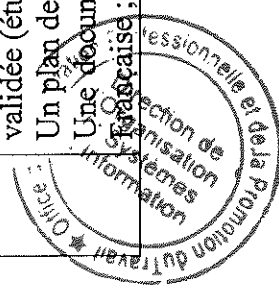
Les consultants proposés pour la réalisation des prestations d'installation et de mise en service doivent justifier de l'expérience et des compétences nécessaires à cet effet.

Garantie et maintenance (couvrir l'assistance 'sur site ou à distance', l'intervention sur site, les pièces de rechanges et la main d'œuvre) pour une durée de 3 ans avec un délai de prise en charge de 4 heures après déclaration de l'incident et un délai de 48 heures de résolution ou de contournement du problème ;

#### Livrables du projet :

Le titulaire doit fournir une documentation complète contenant :

- Un dossier d'ingénierie contenant l'architecture réseau validée (étude adressage, routage, découpage vlan, ... ;
- Un plan de migration de l'ancien système vers la nouvelle solution ;
- Une documentation technique des équipements installés en langue française ;



|  |   |  |  |
|--|---|--|--|
|  | <p>Procédures d'installation, de configuration et d'administration du matériel ;</p> <p>Un guide technique d'administration et d'exploitation des équipements ;</p> <p>L'ensemble de la documentation est à fournir sous format papier en deux exemplaires et sous format électronique (USB).</p> <p><b>Transfert de compétences</b></p> <p>Le titulaire doit assurer un transfert de compétence permettant à l'équipe de l'OFPPT d'acquérir les connaissances nécessaires pour assurer l'exploitation des équipements installés objet de l'appel d'offres.</p> |  |  |
|--|---|--|--|



## Lot 2 : Solutions Firewall et SDWAN pour le siège, Annexes siège et directions régionales.

N.B : les soumissionnaires sont invités à remplir la case << Proposition du soumissionnaire >> en précisant les caractéristiques du matériel proposé.

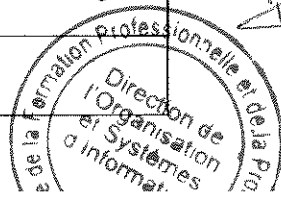
Tout article ne répondant pas aux spécifications demandées sera déclaré non-conforme.

Les colonnes « Désignations et caractéristiques techniques » et « Appréciation de l'Administration » >> ne doivent pas être renseignées ou modifiées.

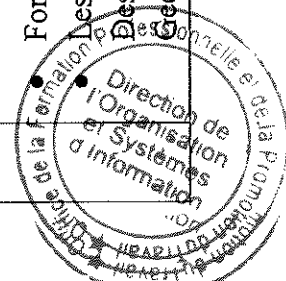
Le concurrent est tenu de renseigner pour chaque item, la marque, la référence et les caractéristiques des fournitures proposées et ce, dans le cadre de la colonne « Proposition du soumissionnaire » et la ligne correspondante à l'item.

Les valeurs des dimensions, longueurs, capacités ,..... Doivent être renseignées d'une manière précise dans la colonne « Proposition du soumissionnaire ».

| Item<br>N°   | Désignation et caractéristiques techniques minimales  | Qte | Proposition du soumissionnaire | Appréciation de<br>l'Administration |
|--|---|-----|--------------------------------|-------------------------------------|
| <b>En vue de renforcer la sécurité du réseau de l'OFPPT, un firewall frontal sera l'objet de ce Lot, il devra être d'une marque différente du firewall dorsal existant (de marque Palo Alto)</b> |   |     |                                |                                     |
| <b>Les items N°1 et N°4 doivent être de même marque</b>  |   |     |                                |                                     |
| 1.   | <p><b>Equipements SDWAN / FIREWALL (Siège)</b></p> <p>La solution cible doit être composée d'une solution SDWAN et Firewall en HA de même marque et respectant au minimum les spécifications techniques cités en bas.</p> <p>La solution proposée peut être composée d'une ou deux Appliances physiques tout en respectant les exigences techniques minimales cumulées des deux solutions suivantes :</p> <p><b>Equipement SDWAN :</b></p> <ul style="list-style-type: none"> <li>• Marque reconnue mondialement (Leader dans le quadrant magique Gartner « wan edge infrastructure » dans les trois dernières années) ;</li> <li>• Possibilité d'utiliser plusieurs types de liens en actif ; Cuivre Ethernet RJ45, Fibre Ethernet, VLAN, VPN IPsec, 3G/4G Modem USB, ...</li> <li>• Possibilité de créer des tunnels VPN via un assistant graphique sur le Menu SDWAN pour une facilité de configuration ;</li> </ul> |     |                                |                                     |



|  |  |  |  |
|--|--|--|--|
|  | <ul style="list-style-type: none"> <li>• Offre la possibilité de créer des SLAs intelligentes pour le basculement et le Load Balancing ;</li> <li>• Les SLA doivent se baser sur :             <ul style="list-style-type: none"> <li>✓ L'état de santé du lien avec les protocoles PING, http, TCP et UDP sur deux destinations différentes pour plus de précision</li> <li>✓ SLA basée sur les paramètres de : la latence, la Jitter et la perte de Paquets ;</li> <li>✓ Offrir la visualisation graphique de l'état des SLA par rapport aux paramètres Latence, Jitter et Perte de Paquets ;</li> </ul> </li> <li>• La solution SDWan doit offrir les Méthodes de Load Blancing Suivantes :             <ul style="list-style-type: none"> <li>✓ IP-Source</li> <li>✓ IP-Source-Destination</li> <li>✓ Spillover</li> <li>✓ Sessions</li> <li>✓ Volume</li> </ul> </li> <li>• Offre la possibilité d'utiliser des règles de basculement automatique en se basant sur les paramètres suivant suite au mesure SLA :             <ul style="list-style-type: none"> <li>✓ Best Quality (en se basant sur la : latence, Jitter, Perte de Paquets, Débit Downstream, Débit Upstream et Débit Downstream/Upstream)</li> <li>✓ Lowest Cost</li> <li>✓ Maximize Bandwidth</li> </ul> </li> </ul> <p>Forcer le flux à suivre un lien spécifique manuellement ;</p> <p>Les règles SDWan doivent se baser sur l'IP Source, IP Destination, Utilisateur, Groupe d'utilisateur, Service Internet, Geo IP, FQDN, Protocol, Application,</p> |  |  |
|--|--|--|--|



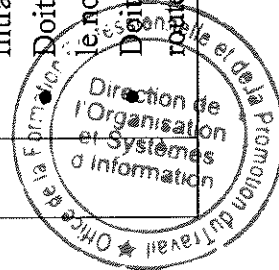
- Doit offrir la possibilité d'associer des politiques QoS pour des flux.
- Offre le contrôle des applications afin d'identifier et reconnaître les applications dans les flux ;
- Management Via interface WEB GUI https ;
- Management via SSH, TELNET et console ;
- Configuration minimale : 8 Ports 1Gbe RJ45 et 2 ports 10Gbe Fibre SFP+ doté de 2 trancivers SFP+ 10Gb) et 2 ports 1Ge SFP (doté de 2 trancivers SFP 1 Gbe)
- Throughput VPN IPsec : 20 Gbps minimum
- Support de 1000 tunnels VPN Ipsec Site -to-site ;

#### Next-Generation Firewall

- Marque reconnue mondialement Marque reconnue mondialement (**Leader dans le quadrant magique Gartner « Network Firewalls » dans les trois dernières années**) ;
- Doit intégrer un système d'exploitation propriétaire sécurisé ;
- Filtrage de paquets et être doté de la fonction de filtrage dynamique ;
- Filtrage basé sur les applications niveau 7 en plus des ports/Protocol et par plages de ports UDP ou TCP ;
- Filtrage et inspection en IPv4 et IPv6 ;
- Failover de connexion Internet ;
- Prise en compte de paramètre Horaire dans les règles de filtrage ;

Doit fournir, via sa console d'administration, des statistiques sur le nombre d'accès aux règles de sécurité ;

Doit inclure la possibilité de fonctionner en mode transparent ou nat (naté) ;

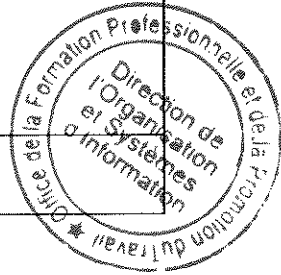




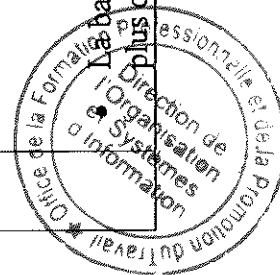
- Doit fournir la possibilité de définir des instances firewall virtuels sur la même Appliance, et capable d'activer les fonctionnalités de protection IPS, Sandboxing, Control Applicatif, filtrage d'URL, Anti-bot, Anti-virus/Antimalware ;
- La création de la politique de sécurité basée sur :
  - ✓ Geolocation par pays
  - ✓ Zones
  - ✓ Groupes de Zones
  - ✓ Applications, Groupes d'applications
  - ✓ Catégories d'Applications
  - ✓ Technologies d'Applications
  - ✓ Filtres d'Applications
  - ✓ Utilisateurs et Groupes
  - ✓ Adresses IP, Groupes d'adresses IP, Sous-réseaux IP, Groupes de sous-réseaux IP
  - ✓ Services, Groupes de Services

La solution doit être de type Next Generation Firewall avec capacité de prévention contre les menaces avancées, combinée avec des fonctionnalités de base suivantes (**licences incluses**) :

- **IPS (prévention des intrusions)** pour se protéger contre les menaces réseau telles que vers, chevaux de Troie et autres programmes malveillants. Le système de prévention des intrusions (IPS) doit aussi apporter une protection contre les menaces réseaux existantes et émergentes. Ce module IPS doit avoir deux mécanismes :
  - ✓ Détection par signatures ;
  - ✓ Détection par anomalies ;
  - ✓ Capable de faire des analyses comportementales de tout type de trafic ;
  - ✓ Possibilité de créer des signatures personnalisées ;
  - ✓ Mise à jour automatique des signatures IPS ;



- ✓ Création et affectation des politiques IPS par type de zone ou interface ;
  - ✓ Pour chaque événement d'attaque, il sera possible de laisser passer ou bloquer, de faire une mise en quarantaine automatique (IP totalement bloquée pendant un temps donné) ... ;
  - ✓ Gestion de profils IPS avec association à certains trafics dans la politique de filtrage (IP source, IP destination, service, protocole, réseau...) ;
  - **Module Antivirus / Antimalware (à fournir)** pour traquer en temps réel les virus, vers, chevaux de Troie, Botnet et autres menaces Internet ;
  - **Filtrage URL**, pour assurer le contrôle de l'accès interne aux contenus Web indésirables, non productifs, voire illégaux,
  - **Contrôle Applicatif**, afin d'identifier, reconnaître et contrôler les applications dans les flux,
  - **Support de la haute disponibilité :**
    - ✓ Actif/Actif avec synchronisation d'état de session,
    - ✓ Actif/Passif,
  - **Contrôle applicatif :**
    - ✓ Identification des applications en se basant sur :
    - ✓ Signatures
    - ✓ Décodage du protocole (respecte la spécification du protocole)
    - ✓ Déchiffrement du trafic encapsulé
  - Identification et contrôle des applications partageant la même connexion
  - Contrôle de la fonction de transfert de fichiers d'une application
  - Visibilité du trafic applicatif inconnu à travers l'identification de sa nature :
    - ✓ Volume du trafic
    - ✓ Utilisateur et/ou adresses IP
    - ✓ Port utilisé
    - ✓ Contenu associé : fichier, menace ou autre.
- La base de données de contrôle des applications doit contenir plus de 3 000 applications connues ;



- La solution doit pouvoir créer une règle de filtrage avec plusieurs catégories ;

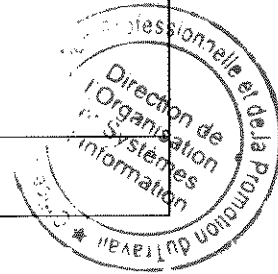
- **Identification, authentification des utilisateurs et protection des identités**

Prise en charge des services d'authentification suivants pour l'identification et authentifications des utilisateurs :

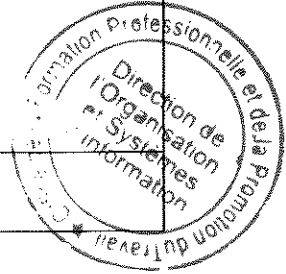
- ✓ Active Directory
- ✓ Kerberos
- ✓ LDAP
- ✓ Radius
- ✓ Base Locale
- ✓ SAML
- ✓ Authentification via SSO Kerberos sans agent
- ✓ Authentification par Certificat client
- ✓ Portail captif
- Identification des utilisateurs indépendamment :
  - ✓ Du terminal (ordinateur, un téléphone intelligent ou une tablette)
  - ✓ Du système d'exploitation utilisé,
  - ✓ Des adresses IP et de la zone (LAN, VPN, hors du périmètre du réseau) ;

- **Fonctions Réseau :**

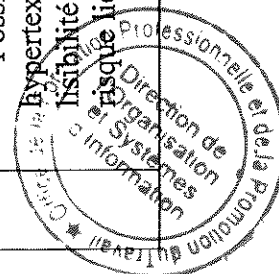
- ✓ Support mode Routage, mode transparent, TAP ou SPAN,
- ✓ Support IPv4 et IPv6
- ✓ Routage IPv4 : Statique et Dynamique, RIPv2, OSPFv3 et BGP au minimum
- ✓ Agrégation des liens 802.3ad, LACP
- ✓ Support des VLAN 802.1q
- ✓ Support des modes de translations NAT et PAT
- ✓ Nat dynamique, Nat Statique, Nat par port, Nat64
- ✓ Support de Multicast



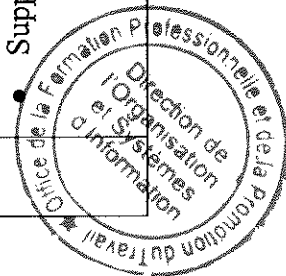
|  |  |  |  |
|--|--|--|--|
| <ul style="list-style-type: none"> <li>• <b>Fonction VPN :</b> <ul style="list-style-type: none"> <li>✓ VPN IPsec site-site, client-site et hub &amp; Spoke. (Fonctionnalité et licence à fournir)</li> <li>✓ Support du VPN SSL mode portail et mode tunnel (avec ou sans agent)</li> <li>✓ Support du Tunnel GRE</li> <li>✓ Support de IKEv1 et IKEv2 avec authentification à base de clé pré-partagée (PSK) ou certificat</li> <li>✓ Standard de Chiffrement : 3DES, AES 256 au minimum</li> <li>✓ Algorithme de contrôle d'intégrité : MD5, SHA-256, SHA-384, SHA-512,</li> </ul> </li> <li>• <b>Gestion de la bande passante :</b> <ul style="list-style-type: none"> <li>✓ Réserve et Priorisation des flux en fonction de la source, la destination, l'utilisateur et l'application,</li> <li>✓ Limitation de la bande passante par source, destination, application ou catégorie d'application.</li> <li>✓ Administration et gestion des journaux :</li> <li>✓ Administration via une interface web intuitive et sécurisée en HTTPS,</li> <li>✓ Administration en ligne de commande SSH et Telnet,</li> <li>✓ Interface d'administration graphique multi-langues : Français et Anglais au minimum,</li> <li>✓ Support de l'administration par rôle,</li> <li>✓ Permettre l'export et l'importation de la configuration,</li> <li>✓ Suivre et visibilité en temps réel sur les flux transitant par le firewall avec possibilité de filtrage,</li> <li>✓ Outil de filtrage et recherche multicritère dans les journaux pour faciliter l'identification des incidents de sécurité.</li> <li>✓ Prise en charge de balises (tags) pour l'organisation des règles et des objets.</li> <li>✓ Différente vue pour les journaux : Flux, Menaces, Filtrage de contenu, Authentification, Systèmes</li> </ul> </li> </ul> |  |  |  |
|--|--|--|--|



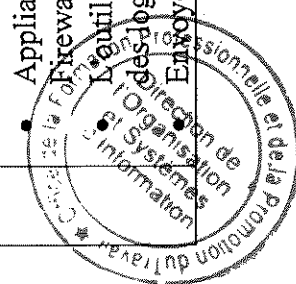
|  |   |  |
|--|---|--|
|  | <ul style="list-style-type: none"> <li>✓ Vue synthétique des applications, menaces et URL,</li> <li>✓ Export des journaux vers des systèmes externes en Syslog et Intégration avec des solutions SIEM</li> <li>✓ Support de SNMPv3</li> <li>✓ Journalisation locale dans le disque du NGFW sans dégradation des performances.</li> <li>✓ La solution doit inclure une autorité de certification x.509 interne qui peut générer des certificats pour les passerelles et les utilisateurs pour permettre une authentification facile sur les VPN,</li> <li>✓ La solution doit inclure la possibilité d'utiliser des autorités de certification externes,</li> <li>✓ La visionneuse de journaux doit avoir la possibilité de créer un filtre en utilisant les noms d'objets prédéfinis (hôtes, réseau, groupes, utilisateurs...);</li> </ul> <ul style="list-style-type: none"> <li>• <b>Module Antivirus / Antimalware (licence à fournir) :</b> <ul style="list-style-type: none"> <li>- scan d'un grand nombre de protocoles : <ul style="list-style-type: none"> <li>✓ HTTP</li> <li>✓ HTTPS (Avec déchiffrement SSL)</li> <li>✓ SMTP</li> <li>✓ POP3</li> <li>✓ IMAP</li> <li>✓ MAPI</li> <li>✓ FTP</li> <li>✓ NNTP</li> <li>✓ CIFS</li> <li>✓ SSH (Mode proxy uniquement)</li> </ul> </li> <li>- Support du scan antivirus en mode Flow ou Proxy.</li> <li>- Possibilité de désarmer un fichier Office ou PDF de tout lien hypertexte actif, macros, objets liés ... tout en conservant la lisibilité de son contenu à son destinataire, diminuant ainsi le risque lié aux attaques avancées.</li> </ul> </li> </ul> |  |
|--|---|--|



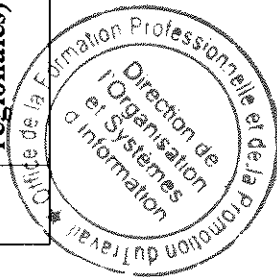
|   |  |  |
|---|--|--|
| <ul style="list-style-type: none"> <li>• <b>Filtrage URL et Filtrage de contenu</b> <ul style="list-style-type: none"> <li>✓ Filtrage HTTP, HTTPS, HTTP2 ;</li> <li>✓ Filtrage URL à base de catégories ;</li> <li>✓ Inspection des flux chiffrés TLS 1.3 ;</li> <li>✓ Validation des certificats des serveurs (CRL, Algorithm, Cipher...);</li> <li>✓ Filtrage URL à base de l'adresse IP ;</li> <li>✓ Filtrage des liens de phishing dans les e-mails, des sites de phishing ;</li> <li>✓ Filtrage des commandes et contrôles basés sur HTTP et les pages contenant des kits d'exploits ;</li> <li>✓ Filtrage des données en fonction du type de fichier, propriété de fichier, Metadata, mot clés...</li> <li>✓ Mise à jour de la base des URL.</li> </ul> </li> <li>• <b>Licence à fournir</b> : IPS, Antivirus, Filtrage URL, Contrôle applicatif et sandbox cloud pendant une durée de 3 années</li> <li>• <b>Performances minimales</b> : <ul style="list-style-type: none"> <li>✓ Dôté de 6 ports 10gbe SFP+ (doté de 6 trancieveurs SFP+ 10Gb) et 8 ports 1ge RJ45 et 2 ports 1Ge SFP (doté de 2 trancieveurs SFP 1Gbe)</li> <li>✓ Nombre de sessions simultanées : 7 Millions au minimum</li> <li>✓ Nombre de nouvelles sessions par secondes : 500 000</li> <li>✓ Débit FULL protection : avec activation Firewalling + contrôle applicatif + IPS + inspection antivirale + filtrage URL entreprise MIX ( IMIX) de 8 Gbps minimum</li> <li>✓ Double alimentation ;</li> </ul> </li> <li>• Support et Licences pour une durée de 3 ans ;</li> </ul> |  |  |
|---|--|--|



|    |   |  |  |
|----|---|--|--|
| 2. | <p><b><u>Solution de management centralisé des firewalls</u></b></p> <p>Le soumissionnaire doit proposer une solution logicielle (pour besoin d'évolutivité futur) de gestion et administration centralisée compatible a 100% avec les Firewalls proposés et devant répondre aux spécifications techniques suivantes :</p> <p><b>Performances minimales :</b></p> <ul style="list-style-type: none"> <li>• Solution sous format <b>d'Appliance virtuelle</b> de même marque que les Firewalls avec système d'exploitation auto-protégée compatible avec VMware ESXi, Hyper-V, KVM...</li> <li>• Permet la gestion centralisée des Firewalls proposés</li> <li>• Permet la gestion des configurations des Firewalls</li> <li>• Permet la gestion des MAJ Firmware des Firewalls</li> <li>• Doté d'au moins de 4 interfaces réseau Giga Ethernet</li> <li>• Espace de stockage Minimum 100 GB extensible pour évolution futur</li> <li>• Licence pour gestion de 20 Firewalls au minimum</li> <li>• Permet de créer des profils et des domaines d'administration différents</li> <li>• Support et Licences pour une durée de 3 ans ;</li> </ul> |  |  |
| 3. | <p><b><u>Solution de gestion centralisée des Logs et de reporting des Firewalls :</u></b></p> <p>Le soumissionnaire doit proposer une solution de gestion logs et de reporting compatible a 100% avec les Firewalls proposés et devant répondre aux spécifications techniques suivantes :</p> <ul style="list-style-type: none"> <li>• Appliance physique Rackable de même marque que les Firewalls ;</li> <li>• Le outil de Reporting doit assumer la collecte et la valorisation des logs générés par les firewalls proposés</li> <li>• Envoyer des alertes par rapport à un évènement bien définit</li> </ul>  |  |  |



|    |   |  |  |
|----|---|--|--|
|    | <ul style="list-style-type: none"> <li>• Disposer d'une interface de consultation des journaux avec un moteur de recherche permettant de filtrer les logs sur de multiples critères. Les filtres supportent le caractère Wildcard ainsi que des opérateurs booléens.</li> <li>• Générer à la demande ou de manière planifiée des rapports dont le contenu sera adapté au profil de leurs destinataires (opérationnel, sécurité, direction, etc.). Ils peuvent être sauvegardés sur un serveur tiers ou être envoyés à leur destinataire par e-mail.</li> <li>• Interface Web de gestion et de consultation des logs et des journaux</li> <li>• Dashboard : afin de rendre compte très synthétiquement de l'activité logging dans l'environnement administré. L'exploitant peut visualiser ainsi à chaque accès, le nombre de logs/sec moyen en cours, ainsi que le nombre et le volume de logs collectés jour par jour, sur une semaine (Ces informations sont très importantes pour déterminer la politique de conservation des logs sur le système et les travaux de capacity planning)</li> <li>• Possibilité de création de plusieurs profils d'administration afin d'y affecter des Firewalls par profil</li> <li>• Affichage d'une carte de menace « Threat Map » afin de montrer les origines des attaques sur une carte géographique mondiale</li> <li>• Module d'indice de compromission.</li> <li>• Capacité de traitement des Logs : <b>25 GB</b> de logs par jour</li> <li>• Espace de stockage : <b>4 TB</b> ;</li> <li>• 4 interfaces GE RJ45 et 2 ports GE SFP ;</li> <li>• Support et Licences pour une durée de 3 ans ;</li> </ul> |  |  |
| 4. | <b>Equipement SDWAN/FIREWALL (Annexes sièges /Directions régionales)</b>  |  |  |





La solution cible doit être composée d'une solution SDWAN et Firewall en HA de même marque et respectant au minimum les spécifications techniques cités en bas.

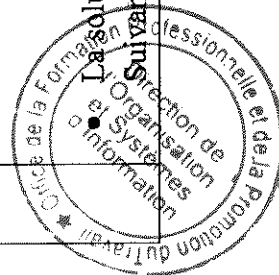
La solution proposée peut être composée d'une ou deux Appliances physiques tout en respectant les exigences techniques minimales cumulées des deux solutions suivantes :

**Equipement SDWAN : (Leader dans Gartner dans les trois dernières années)**

- Marque reconnue mondialement (Leader dans le quadrant magique Gartner « wan edge infrastructure » dans les trois dernières années) : A préciser
- Possibilité d'utiliser plusieurs types de liens en actif ; Cuivre Ethernet RJ45, Fibre Ethernet, VLAN, VPN IPsec, 3G/4G Modem USB, ...
- Possibilité de créer des tunnels VPN via un assistant graphique sur le Menu SDWan pour une facilité de configuration ;
- Offre la possibilité de créer des SLAs intelligentes pour le basculement et le Load Balancing ;
- Les SLA doivent se baser sur :
  - ✓ L'état de santé du lien avec les protocoles PING, http, TCP et UDP sur deux destinations différentes pour plus de précision
  - ✓ SLA basée sur les paramètres de : la latence, la Jitter et la perte de Paquets ;
  - ✓ Offrir la visualisation graphique de l'état des SLA par rapport aux paramètres Latence, Jitter et Perte de Paquets ;

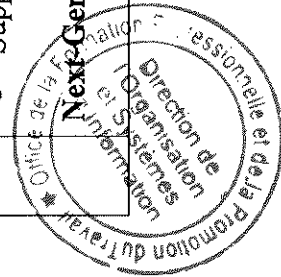
La solution SDWan doit offrir les Méthodes de Load Balancing

Suivantes :



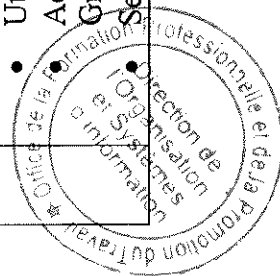
- ✓ IP-Source
- ✓ IP-Source-Destination
- ✓ Spillover
- ✓ Sessions
- ✓ Volume
- Offre la possibilité d'utiliser des règles de basculement automatique en se basant sur les paramètres suivant suite au mesure SLA :
  - ✓ Best Quality (en se basant sur la : latence, Jitter, Perte de Paquets, Débit Downstream, Débit Upstream et Débit Downstream/Upstream)
  - ✓ Lowest Cost
  - ✓ Maximize Bandwidth
- Forcer le flux à suivre un lien spécifique manuellement ;
- Les règles SDWan doivent se baser sur l'IP Source, IP Destination, Utilisateur, Groupe d'utilisateur, Service Internet, Geo IP, FQDN, Protocol, Application,
- Doit offrir la possibilité d'associer des politiques QoS pour des flux.
- Offre le contrôle des applications afin d'identifier et reconnaître les applications dans les flux ;
- Management Via interface WEB GUI https ;
- Management via SSH, TELNET et console ;
- Configuration minimale : **4 Ports 1Gbe RJ45 et 4 ports 1Gbe Fibre**
- Throughput VPN IPsec: **7 Gbps minimum**
- Support de 200 tunnels VPN Ipsec Site -2-site

#### Next-Generation Firewall :

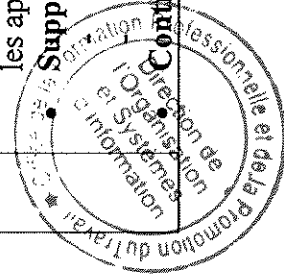


### Fonctions Firewall

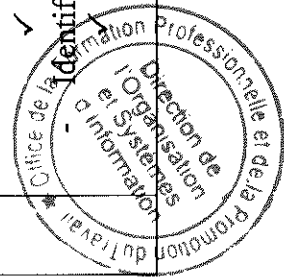
- Marque reconnue mondialement (**Leader dans le quadrant magique Gartner « Network Firewalls » dans les trois dernières années**)
- Doit intégrer un système d'exploitation propriétaire sécurisé,
- Filtrage de paquets et être doté de la fonction de filtrage dynamique,
- Filtrage basé sur les applications niveau 7 en plus des ports/Protocol et par plages de ports UDP ou TCP
- Filtrage et inspection en IPv4 et IPv6,
- Failover de connexion Internet,
- Prise en compte de paramètre Horaire dans les règles de filtrage,
- Doit fournir, via sa console d'administration, des statistiques sur le nombre d'accès aux règles de sécurité,
- Doit inclure la possibilité de fonctionner en mode transparent ou routé (natté),
- Doit fournir la possibilité de définir des instances firewall virtuels sur la même Appliance, et capable d'activer les fonctionnalités de protection IPS, Sandboxing, Control Applicatif, filtrage d'URL, Anti-bot, Anti-virus/Antimalware,
- La création de la politique de sécurité basée sur :
  - Geolocation par pays
  - Zones
  - Groupes de Zones
  - Applications, Groupes d'applications
  - Catégories d'Applications
  - Technologies d'Applications
  - Filtres d'Applications
  - Utilisateurs et Groupes
  - Adresses IP, Groupes d'adresses IP, Sous-réseaux IP, Groupes de sous-réseaux IP
  - Services, Groupes de Services



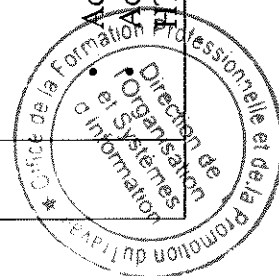
- La solution doit être de type Next Generation Firewall avec capacité de prévention contre les menaces avancées, combinée avec des fonctionnalités de base suivantes (**licences incluses**) :
  - **IPS (prévention des intrusions)** pour se protéger contre les menaces réseau telles que vers, chevaux de Troie et autres programmes malveillants. Le système de prévention des intrusions (IPS) doit aussi apporter une protection contre les menaces réseaux existantes et émergentes. Ce module IPS doit avoir deux mécanismes :
    - Détection par signatures ;
    - Détection par anomalies ;
    - Capable de faire des analyses comportementales de tout type de trafic ;
    - Possibilité de créer des signatures personnalisées ;
    - Mise à jour automatique des signatures IPS ;
    - Création et affectation des politiques IPS par type de zone ou interface ;
    - Pour chaque événement d'attaque, il sera possible de laisser passer ou bloquer, de faire une mise en quarantaine automatique (IP totalement bloquée pendant un temps donné) ... ;
    - Gestion de profils IPS avec association à certains trafics dans la politique de filtrage (IP source, IP destination, service, protocole, réseau...) ;
  - **Module Antivirus / Antimalware (à fournir)** pour traquer en temps réel les virus, vers, chevaux de Troie, Botnet et autres menaces Internet ;
  - **Filtrage URL**, pour assurer le contrôle de l'accès interne aux contenus Web indésirables, non productifs, voire illégaux,
  - **Contrôle Applicatif**, afin d'identifier, reconnaître et contrôler les applications dans les flux,
  - **Support de la haute disponibilité** :  
Actif/Actif avec synchronisation d'état de session, Actif/Passif,
  - **Contrôle applicatif** :



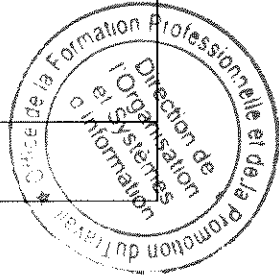
- Identification des applications en se basant sur :
    - o Signatures
    - o Décodage du protocole (respecte la spécification du protocole)
    - o Déchiffrement du trafic encapsulé
  - Identification et contrôle des applications partageant la même connexion
  - Contrôle de la fonction de transfert de fichiers d'une application
  - Visibilité du trafic applicatif inconnu à travers l'identification de sa nature :
    - o Volume du trafic
    - o Utilisateur et/ou adresses IP
    - o Port utilisé
    - o Contenu associé : fichier, menace ou autre.
  - La base de données de contrôle des applications doit contenir plus de 3 000 applications connues ;
  - La solution doit pouvoir créer une règle de filtrage avec plusieurs catégories ;
- **Identification, authentification des utilisateurs et protection des identités**
    - Prise en charge des services d'authentification suivants pour l'identification et authentifications des utilisateurs :
      - ✓ Active Directory
      - ✓ Kerberos
      - ✓ LDAP
      - ✓ Radius
      - ✓ Base Locale
      - ✓ SAML
      - ✓ Authentification via SSO Kerberos sans agent
      - ✓ Authentification par Certificat client
      - ✓ Portail captif
- Identification des utilisateurs indépendamment :**  
Du terminal (ordinateur, un téléphone intelligent ou une tablette)



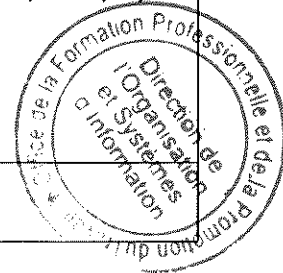
|  |  |  |
|--|--|--|
|  | <ul style="list-style-type: none"> <li>✓ Du système d'exploitation utilisé,</li> <li>✓ Des adresses IP et de la zone (LAN, VPN, hors du périmètre du réseau)</li> <li>• <b>Fonctions Réseau :</b> <ul style="list-style-type: none"> <li>✓ Support mode Routage, mode transparent, TAP ou SPAN,</li> <li>✓ Support IPv4 et IPv6</li> <li>✓ Routage IPv4 : Statique et Dynamique, RIPv2, OSPFv3 et BGP au minimum</li> <li>✓ Agrégation des liens 802.3ad, LACP</li> <li>✓ Support des VLAN 802.1q</li> <li>✓ Support des modes de translations NAT et PAT</li> <li>✓ Nat dynamique, Nat Statique, Nat par port, Nat64</li> <li>✓ Support de Multicast</li> </ul> </li> <li>• <b>Fonction VPN :</b> <ul style="list-style-type: none"> <li>✓ VPN IPsec site-site, client-site et hub &amp; Spoke. (Fonctionnalité et licence à fournir)</li> <li>✓ Support du VPN SSL mode portail et mode tunnel (avec ou sans agent)</li> <li>✓ Support du Tunnel GRE</li> <li>✓ Support de IKEv1 et IKEv2 avec authentification à base de clé pré-partagée (PSK) ou certificat</li> <li>✓ Standard de Chiffrement : 3DES, AES 256 au minimum</li> <li>✓ Algorithme de contrôle d'intégrité : MD5, SHA-256, SHA-384, SHA-512,</li> </ul> </li> <li>• <b>Gestion de la bande passante :</b> <ul style="list-style-type: none"> <li>✓ Réserve et Priorisation des flux en fonction de la source, la destination, l'utilisateur et l'application,</li> <li>✓ Limitation de la bande passante par source, destination, application ou catégorie d'application.</li> </ul> </li> </ul> <p>Administration et gestion des journaux :<br/>Administration via une interface web intuitive et sécurisée en HTTPS,</p> |  |
|--|--|--|



- Administration en ligne de commande SSH et Telnet,
- Interface d'administration graphique multi-langues : Français et Anglais au minimum,
- Support de l'administration par rôle,
- Permettre l'export et l'importation de la configuration,
- Suivre et visibilité en temps réel sur les flux transitant par le firewall avec possibilité de filtrage,
- Outil de filtrage et recherche multicritère dans les journaux pour faciliter l'identification des incidents de sécurité.
- Prise en charge de balises (tags) pour l'organisation des règles et des objets.
- Différente vue pour les journaux : Flux, Menaces, Filtrage de contenu, Authentification, Systèmes
- Vue synthétique des applications, menaces et URL,
- Export des journaux vers des systèmes externes en Syslog et Intégration avec des solutions SIEM
- Support de SNMPv3
- Journalisation locale dans le disque du NGFW sans dégradation des performances.
- La solution doit inclure une autorité de certification x.509 interne qui peut générer des certificats pour les passerelles et les utilisateurs pour permettre une authentification facile sur les VPN,
- La solution doit inclure la possibilité d'utiliser des autorités de certification externes,
- La visionneuse de journaux doit avoir la possibilité de créer un filtre en utilisant les noms d'objets prédéfinis (hôtes, réseau, groupes, utilisateurs...),
- **Module Antivirus / Antimalware (à fournir) :**
  - scan d'un grand nombre de protocoles :
    - ✓ HTTP
    - ✓ HTTPS (Avec déchiffrement SSL)
    - ✓ SMTP
    - ✓ POP3
    - ✓ IMAP



|  |   |  |  |
|--|---|--|--|
|  | <ul style="list-style-type: none"> <li>✓ MAPI</li> <li>✓ FTP</li> <li>✓ NNTP</li> <li>✓ CIFS</li> <li>✓ SSH (Mode proxy uniquement)</li> <li>- Support du scan antivirus en mode Flow ou Proxy.</li> <li>- Possibilité de désarmer un fichier Office ou PDF de tout lien hypertexte actif, macros, objets liés ... tout en conservant la lisibilité de son contenu à son destinataire, diminuant ainsi le risque lié aux attaques avancées.</li> <li>• <b>Filtrage URL et Filtrage de contenu</b> <ul style="list-style-type: none"> <li>✓ Filtrage HTTP, HTTPS, HTTP2 ;</li> <li>✓ Filtrage URL à base de catégories ;</li> <li>✓ Inspection des flux chiffrés TLS 1.3 ;</li> <li>✓ Validation des certificats des serveurs (CRL, Algorithm, Cipher...) ;</li> <li>✓ Filtrage URL à base de l'adresse IP ;</li> <li>✓ Filtrage des liens de phishing dans les e-mails, des sites de phishing ;</li> <li>✓ Filtrage des commandes et contrôles basés sur HTTP et les pages contenant des kits d'exploits ;</li> <li>✓ Filtrage des données en fonction du type de fichier, propriété de fichier, Metadata, mot clés...</li> <li>✓ Mise à jour de la base des URL.</li> </ul> </li> <li>• <b>Licence à fournir</b> : IPS, Antivirus, Filtrage URL, Contrôle applicatif et sandbox cloud pendant une durée de 3 années</li> <li>• <b>Performances minimales</b> : <ul style="list-style-type: none"> <li>✓ Doté au minimum de 2 ports 10Gb SFP+ et de 8 ports 1gbe RJ45 et 4 ports 1Gbe SFP</li> <li>✓ Nombre de sessions simultanées : 1.5 Millions au minimum</li> <li>✓ Nombre de nouvelles sessions par secondes : 50 000</li> <li>✓ Débit FULL protection : avec activation Firewalling + contrôle applicatif + IPS + inspection antivirusale +</li> </ul> </li> </ul> |  |  |
|--|---|--|--|





filtrage URL entreprise MIX ( IMIX) de 1 Gbps minimum

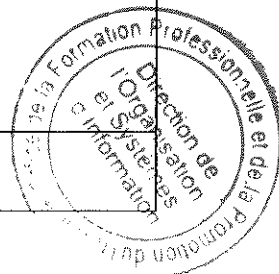
### 5. Prestation de service :

Le prestataire doit proposer dans son offre toutes les prestations nécessaires à la mise en œuvre des solutions SDWAN et Firewall au niveau du siège OFPPT, annexes siège et directions régionales.

- Ingénierie et définition de l'architecture finale ;
- Analyse du plan d'adressage IP, de routage et de découpage VLAN ;
- L'interconnexion des différents sites ;
- Assurer une communication WAN entre les différents sites OFPPT ;
- L'installation et la configuration des fonctions du pare feu nouvelle génération selon les bonnes pratiques et les standards de la sécurité ;
- La définition de la matrice des flux ;
- Le prestataire doit réaliser tout essai jugé nécessaire pour s'assurer de la conformité et du bon fonctionnement de la plateforme de sécurité ;
- Transfert de compétence ;
- Garantie et maintenance (couvre l'assistance 'sur site ou à distance', l'intervention sur site, les pièces de rechanges et la main d'œuvre) pour une durée de 3 ans avec un délai de prise en charge de 2 heures après déclaration de l'incident et un délai de 4 heures de résolution ou de contournement du problème et 48 h en cas de remplacement

#### • Livrables :

- ✓ Document d'architecture finale et de configuration de la solution (avec schéma au format exploitable et un fichier de configuration) ;
- ✓ Manuel d'exploitation ;



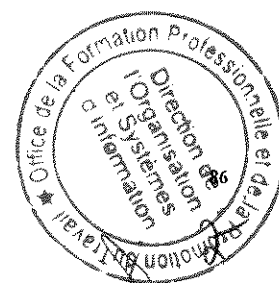
## BORDEREAU DES PRIX – DETAIL ESTIMATIF

**Lot 1 : Solutions SDN, Switching et Wifi pour le Siège OFPPT, Annexes Sièges et Directions Régionales**

| Items<br>N°   | Désignations                                   | Unité | QTE | Prix Unitaire<br>En HTVA<br>En chiffre | Prix Total<br>En HTVA<br>En chiffre |
|---|--|-------|-----|--|-------------------------------------|
| <b>Partie 1 : Solutions SDN, Switching et Wifi pour le siège, Annexe I-SidiMaarouf et Annexe II-Ain Borja</b> |  |       |     |  |                                     |
| 1.  | Solution SDN                                   | U     | 1   |  |                                     |
| 2.  | Switch Fédérateur 48 ports                     | U     | 2   |  |                                     |
| 3.  | Switch MultiGiga                               | U     | 7   |  |                                     |
| 4.  | Switch 48 ports                                | U     | 36  |  |                                     |
| 5.  | Swicth 24 ports                                | U     | 4   |  |                                     |
| 6.  | Contrôleur WIFI                                | U     | 1   |  |                                     |
| 7.  | Points d'accès wifi                            | U     | 80  |  |                                     |
| 8.  | Prestation de service (Siège et annexes siège) | F     | F   |  |                                     |
| <b>Partie 2 : Solutions Switching et Wifi pour les directions régionales</b>                                  |  |       |     |  |                                     |
| 9.  | Switch 24 ports                                | U     | 18  |  |                                     |
| 10.   | Switch 48 ports                                | U     | 5   |  |                                     |
| 11.   | Points d'accès wifi                            | U     | 36  |  |                                     |
| 12.   | Prestation de service (Directions régionales)  | F     | F   |  |                                     |
| <b>MONTANT TOTAL EN HTVA</b>  |  |       |     |  |                                     |
| <b>MONTANT TOTAL EN HTVA</b>  |  |       |     |  |                                     |
| <b>TOTAL DE LA TVA (TAUX %)</b>   |  |       |     |  |                                     |

Fait à ..... le .....

Signature et cachet du concurrent



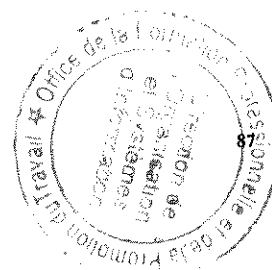
## BORDEREAU DES PRIX – DETAIL ESTIMATIF

Lot 2 : Solutions Firewall et SDWAN pour le siège, Annexes siège et directions régionales.

| Items<br>N°              | Désignations   | Unité | QTE | Prix Unitaire<br>En HTVA<br>En chiffre | Prix Total<br>En HTVA<br>En chiffre |
|--------------------------|--|-------|-----|--|-------------------------------------|
| 1.                       | Equipements SDWAN / FIREWALL (Siège)                                   | U     | 2   |  |                                     |
| 2.                       | Solution de management centralisé des firewalls                        | U     | 1   |  |                                     |
| 3.                       | Solution de gestion centralisée des Logs et de reporting des Firewalls | U     | 1   |  |                                     |
| 4.                       | Equipement SDWAN/FIREWALL (Annexes sièges /Directions régionales)      | U     | 12  |  |                                     |
| 5.                       | Prestation de service  | U     | F   |  |                                     |
| MONTANT TOTAL EN HTVA    |  |       |     |  |                                     |
| MONTANT TOTAL EN HTVA    |  |       |     |  |                                     |
| TOTAL DE LA TVA (TAUX %) |  |       |     |  |                                     |

Fait à ..... le .....

Signature et cachet du concurrent



A 2