

**ROYAUME DU MAROC**  
**Maître d'ouvrage : LA SOCIETE FONCIERE CMC S.A.**  
**Maître d'ouvrage délégué : OFFICE DE LA FORMATION PROFESSIONNELLE**  
**ET DE LA PROMOTION DU TRAVAIL**

**AVIS D'APPEL D'OFFRES OUVERT N° 100/2022**

Le **26 Juillet 2022 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, pour le compte de l'office de la Formation Professionnelle et de la Promotion du Travail en maîtrise d'ouvrage déléguée, ayant pour objet **La fourniture, l'installation et la mise en œuvre d'un Firewall Nouvelle Génération destiné aux cités des métiers et des compétences ; réparti en lots suivants :**

- **Lot n°1 : Solution de Firewall Nouvelle Génération NGFW pour la CMC NADOR**
- **Lot n°2 : Solution de Firewall Nouvelle Génération NGFW pour la CMC LAAYOUNE**
- **Lot n°3 : Solution de Firewall Nouvelle Génération NGFW pour la CMC TANGER**
- **Lot n°4 : Solution de Firewall Nouvelle Génération NGFW pour la CMC RABAT**
- **Lot n°5 : Solution de Firewall Nouvelle Génération NGFW pour la CMC BENI MELLAL**
- **Lot n°6 : Solution de Firewall Nouvelle Génération NGFW pour la CMC MARRAKECH**
- **Lot n°7 : Solution de Firewall Nouvelle Génération NGFW pour la CMC CASABLANCA**
- **Lot n°8 : Solution de Firewall Nouvelle Génération NGFW pour la CMC FES**
- **Lot n°9 : Solution de Firewall Nouvelle Génération NGFW pour la CMC ERRACHIDIA**
- **Lot n°10 : Solution de Firewall Nouvelle Génération NGFW pour la CMC GUELMIM**
- **Lot n°11 : Solution de Firewall Nouvelle Génération NGFW pour la CMC DAKHLA**

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 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 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 cautionnements provisoires sont fixés à la somme de :

- **Lot n° 1 : Mille sept cents Dirhams (1 700,00 DH)**
- **Lot n° 2 : Mille sept cents Dirhams (1 700,00 DH)**
- **Lot n° 3 : Mille sept cents Dirhams (1 700,00 DH)**
- **Lot n° 4 : Mille sept cents Dirhams (1 700,00 DH)**
- **Lot n° 5 : Mille sept cents Dirhams (1 700,00 DH)**
- **Lot n° 6 : Mille sept cents Dirhams (1 700,00 DH)**
- **Lot n° 7 : Mille sept cents Dirhams (1 700,00 DH)**
- **Lot n° 8 : Mille sept cents Dirhams (1 700,00 DH)**
- **Lot n° 9 : Mille sept cents Dirhams (1 700,00 DH)**
- **Lot n° 10 : Mille sept cents Dirhams (1 700,00 DH)**
- **Lot n° 11 : Mille sept cents Dirhams (1 700,00 DH)**

L'estimation des coûts des prestations établies par le Maître d'ouvrage est fixée à la somme de

- Lot n°1 : Cent dix mille sept cents Dirhams (110 700,00 DH) en TTC.
- Lot n°2 : Cent dix mille sept cents Dirhams (110 700,00 DH) en TTC.
- Lot n° 3 : Cent dix mille sept cents Dirhams (110 700,00 DH) en TTC.
- Lot n° 4 : Cent dix mille sept cents Dirhams (110 700,00 DH) en TTC.
- Lot n° 5 : Cent dix mille sept cents Dirhams (110 700,00 DH) en TTC.
- Lot n° 6 : Cent dix mille sept cents Dirhams (110 700,00 DH) en TTC.
- Lot n° 7 : Cent dix mille sept cents Dirhams (110 700,00 DH) en TTC.
- Lot n° 8 : Cent dix mille sept cents Dirhams (110 700,00 DH) en TTC.
- Lot n° 9 : Cent dix mille sept cents Dirhams (110 700,00 DH) en TTC.
- Lot n° 10 : Cent dix mille sept cents Dirhams (110 700,00 DH) en TTC.
- Lot n° 11 : Cent dix mille sept cents Dirhams (110 700,00 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'OFPPPT

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°6 du règlement de consultation



## المملكة المغربية

### صاحب المشروع: LA FONCIERE CMC S.A صاحب المشروع مفوض: مكتب التكوين المهني وإنعاش الشغل رقم 2022/100

في يوم 26 يوليوز 2022 على الساعة العاشرة صباحاً، 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 لحساب مكتب التكوين المهني وإنعاش الشغل في إدارة المشاريع بالتفويض ، توريد وتركيب وتنفيذ الجيل الجديد من جدار الحماية لفائدة مدن المهن و الكفاءات، موزعة على الحصص كالتالي:

- الحصة 1: حل جدار الحماية الجيل الجديد NGFW لفائدة مدينة المهن و الكفاءات الناظور.
- الحصة 2: حل جدار الحماية الجيل الجديد NGFW لفائدة مدينة المهن و الكفاءات العيون.
- الحصة 3: حل جدار الحماية الجيل الجديد NGFW لفائدة مدينة المهن و الكفاءات طنجة.
- الحصة 4: حل جدار الحماية الجيل الجديد NGFW لفائدة مدينة المهن و الكفاءات الرباط.
- الحصة 5: حل جدار الحماية الجيل الجديد NGFW لفائدة مدينة المهن و الكفاءات بني ملال.
- الحصة 6: حل جدار الحماية الجيل الجديد NGFW لفائدة مدينة المهن و الكفاءات مراكش.
- الحصة 7: حل جدار الحماية الجيل الجديد NGFW لفائدة مدينة المهن و الكفاءات الدار البيضاء.
- الحصة 8: حل جدار الحماية الجيل الجديد NGFW لفائدة مدينة المهن و الكفاءات فاس.
- الحصة 9: حل جدار الحماية الجيل الجديد NGFW لفائدة مدينة المهن و الكفاءات الراشدية.
- الحصة 10: حل جدار الحماية الجيل الجديد NGFW لفائدة مدينة المهن و الكفاءات كلميم.
- الحصة 11: حل جدار الحماية الجيل الجديد NGFW لفائدة مدينة المهن و الكفاءات الداخلة.

يمكن سحب ملف طلب العروض بمصلحة الصفقات بمديرية 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 1: ألف وسبعمائة (1 700,00) درهم
- الحصة 2: ألف وسبعمائة (1 700,00) درهم
- الحصة 3: ألف وسبعمائة (1 700,00) درهم
- الحصة 4: ألف وسبعمائة (1 700,00) درهم
- الحصة 5: ألف وسبعمائة (1 700,00) درهم
- الحصة 6: ألف وسبعمائة (1 700,00) درهم
- الحصة 7: ألف وسبعمائة (1 700,00) درهم
- الحصة 8: ألف وسبعمائة (1 700,00) درهم
- الحصة 9: ألف وسبعمائة (1 700,00) درهم
- الحصة 10: ألف وسبعمائة (1 700,00) درهم
- الحصة 11: ألف وسبعمائة (1 700,00) درهم

والكلفة التقديرية للأعمال المحددة من طرف صاحب المشروع تبلغ :

- الحصة 1: مائة وعشرة آلاف وسبعمائة درهم (110 700,00) مع احتساب جميع الرسوم
- الحصة 2: مائة وعشرة آلاف وسبعمائة درهم (110 700,00) مع احتساب جميع الرسوم
- الحصة 3 : مائة وعشرة آلاف وسبعمائة درهم (110 700,00) مع احتساب جميع الرسوم
- الحصة 4 : مائة وعشرة آلاف وسبعمائة درهم (110 700,00) مع احتساب جميع الرسوم
- الحصة 5 : مائة وعشرة آلاف وسبعمائة درهم (110 700,00) مع احتساب جميع الرسوم

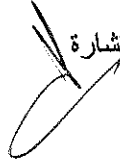
- . الحصة 6 : مائة وعشرة آلاف وسبعمائة درهم (110 700,00) مع احتساب جميع الرسوم
- . الحصة 7 : مائة وعشرة آلاف وسبعمائة درهم (110 700,00) مع احتساب جميع الرسوم
- . الحصة 8 : مائة وعشرة آلاف وسبعمائة درهم (110 700,00) مع احتساب جميع الرسوم
- . الحصة 9 : مائة وعشرة آلاف وسبعمائة درهم (110 700,00) مع احتساب جميع الرسوم
- . الحصة 10 : مائة وعشرة آلاف وسبعمائة درهم (110 700,00) مع احتساب جميع الرسوم
- . الحصة 11 : مائة وعشرة آلاف وسبعمائة درهم (110 700,00) 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 أطرفتهم مقابل وصل، بمكتب مصلحة الصفقات بمديرية التموين واللوجستيك الكائنة بملتقى طريق BO والطريق الوطنية رقم 11 (طريق النواصر – سيدي معروف) - الدار البيضاء؛
- إما تسليمها مباشرة لرئيس لجنة طلب العروض عند بداية الجلسة وقبل فتح الأظرفة.
- إما أن يتم إرسالها إلكترونياً وفقاً لأحكام قرار وزارة الاقتصاد والمالية رقم 14-20 بتاريخ 8 ذي القعدة 1435 (4 سبتمبر 2014) المتعلق بإزالة الطابع المادي لإجراءات المشتريات العامة.

إن الوثائق المثبتة الواجب الإدلاء بها هي تلك المقررة في المادة 6 من نظام الإستشارة





ROYAUME DU MAROC

**MAITRE D'OUVRAGE**

SOCIETE FONCIERE CMC S.A.

**MAITRE D'OUVRAGE DELEGUE**

OFFICE DE LA FORMATION PROFESSIONNELLE  
ET DE LA PROMOTION DU TRAVAIL

**Dossier d'Appel d'offres**

**Ouvert sur offres de prix**  
**N° 100 / 2022**

**Objet de l'Appel d'offres :**

**La fourniture, l'installation et la mise en œuvre d'un Firewall  
Nouvelle Génération destiné aux cités des métiers et des  
compétences ; réparti en lots suivants :**

- Lot 1 : Solution de Firewall Nouvelle Génération NGFW pour la CMC NADOR
- Lot 2 : Solution de Firewall Nouvelle Génération NGFW pour la CMC LAAYOUNE
- Lot 3 : Solution de Firewall Nouvelle Génération NGFW pour la CMC TANGER
- Lot 4 : Solution de Firewall Nouvelle Génération NGFW pour la CMC RABAT
- Lot 5 : Solution de Firewall Nouvelle Génération NGFW pour la CMC BENI MELLAL
- Lot 6 : Solution de Firewall Nouvelle Génération NGFW pour la CMC MARRAKECH
- Lot 7 : Solution de Firewall Nouvelle Génération NGFW pour la CMC CASABLANCA
- Lot 8 : Solution de Firewall Nouvelle Génération NGFW pour la CMC FES
- Lot 9 : Solution de Firewall Nouvelle Génération NGFW pour la CMC ERRACHIDIA
- Lot 10 : Solution de Firewall Nouvelle Génération NGFW pour la CMC GUELMIM
- Lot 11 : Solution de Firewall Nouvelle Génération NGFW pour la CMC DAKHLA

**REGLEMENT DE LA CONSULTATION  
(R. C.)**

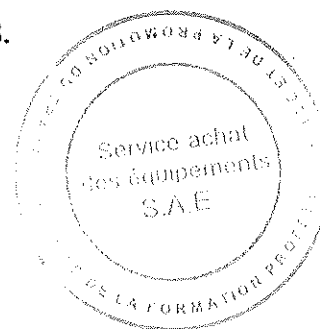


---

## SOMMAIRE

---

ARTICLE 1	: OBJET DU REGLEMENT DE LA CONSULTATION.
ARTICLE 2	: MAITRE D'OUVRAGE
ARTICLE 3	: MAITRE D'OUVRAGE DELEGUE
ARTICLE 4	: DEFINITIONS
ARTICLE 5	: CONDITIONS REQUISES DES CONCURRENTS.
ARTICLE 6	: JUSTIFICATION DES CAPACITES ET DES QUALITES DES CONCURRENTS.
ARTICLE 7	: DOCUMENTS A FOURNIR PAR LES ORGANISMES PUBLICS.
ARTICLE 8	: CONTENU DES DOSSIERS DES CONCURRENTS.
ARTICLE 9	: OFFRE VARIANTE.
ARTICLE 10	: COMPOSITION DU DOSSIER D'APPEL D'OFFRES.
ARTICLE 11	: INFORMATION DES CONCURRENTS.
ARTICLE 12	: MODIFICATION DANS LE DOSSIER D'APPEL D'OFFRES.
ARTICLE 13	: REPARTITION EN LOT.
ARTICLE 14	: PRESENTATION DES DOSSIERS DES CONCURRENTS.
ARTICLE 15	: RETRAIT DU DOSSIER D'APPEL D'OFFRES.
ARTICLE 16	: DEPOT DES PLIS DES CONCURRENTS.
ARTICLE 17	: DELAI DE VALIDITE DES OFFRES.
ARTICLE 18	: LANGUE DE L'OFFRE.
ARTICLE 19	: PRIX PREFERENTIELS POUR LA FORMATION PROFESSIONNELLE.
ARTICLE 20	: MONNAIE DE L'OFFRE.
ARTICLE 21	: DEPENSES ENCOURUES DU FAIT DE L'APPEL D'OFFRES.
ARTICLE 22	: EVALUATION DES OFFRES DES CONCURRENTS.



## REGLEMENT DE LA CONSULTATION

\*\*\*\*\*

### ARTICLE N°1 : OBJET DU REGLEMENT DE LA CONSULTATION.

Le présent règlement de consultation concerne l'appel d'offres ouvert sur offres de prix ayant pour objet la fourniture, l'installation et la mise en œuvre d'un Firewall Nouvelle Génération destiné aux cités des métiers et des compétences ; réparti en lots suivants :

- **Lot 1** : Solution de Firewall Nouvelle Génération NGFW pour la CMC NADOR
- **Lot 2** : Solution de Firewall Nouvelle Génération NGFW pour la CMC LAAYOUNE
- **Lot 3** : Solution de Firewall Nouvelle Génération NGFW pour la CMC TANGER
- **Lot 4** : Solution de Firewall Nouvelle Génération NGFW pour la CMC RABAT
- **Lot 5** : Solution de Firewall Nouvelle Génération NGFW pour la CMC BENI MELLAL
- **Lot 6** : Solution de Firewall Nouvelle Génération NGFW pour la CMC MARRAKECH
- **Lot 7** : Solution de Firewall Nouvelle Génération NGFW pour la CMC CASABLANCA
- **Lot 8** : Solution de Firewall Nouvelle Génération NGFW pour la CMC FES
- **Lot 9** : Solution de Firewall Nouvelle Génération NGFW pour la CMC ERRACHIDIA
- **Lot 10** : Solution de Firewall Nouvelle Génération NGFW pour la CMC GUELMIM
- **Lot 11** : Solution de Firewall Nouvelle Génération NGFW pour la CMC DAKHLA

Il est établi en vertu des dispositions de l'article n°18, du règlement des marchés, approuvé le 18 Chaâbane 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 : MAITRE D'OUVRAGE.

Le maître d'ouvrage du marché qui sera passé suite au présent appel d'offres est : la **Société Foncière CMC S.A.**

### ARTICLE N°3 : MAITRE D'OUVRAGE DELEGUE

Le maître d'ouvrage délégué est l'Office de la Formation Professionnelle et de la Promotion du Travail (OFPPT).

Outre le lancement et le jugement de la procédure des Appels d'offres, la mission de la maîtrise d'ouvrage délégué est portée sur :

- Le suivi d'exécution du marché ;
- Les démarches, éventuelles, nécessaires à l'obtention de l'exonération des droits de douanes ;



- La coordination nécessaire pour La préparation des conditions de livraison, d'installation et de réception des équipements ;
- La signature des bons de dépôt et des livraisons conformément aux dispositions prévues par ce marché ;
- La réception provisoire du marché ;
- La réception définitive du marché ;
- La liquidation et le paiement des dossiers de facturation.

L'OFPPT représente la Société Foncière CMC S.A. à l'égard du titulaire de ce marché dans l'exercice des attributions qui lui sont confiés jusqu'à ce que la Société Foncière des CMC ait constaté l'achèvement de sa mission.

#### **ARTICLE N°4 : DEFINITIONS.**

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°5 : CONDITIONS REQUISES DES CONCURRENTS.**

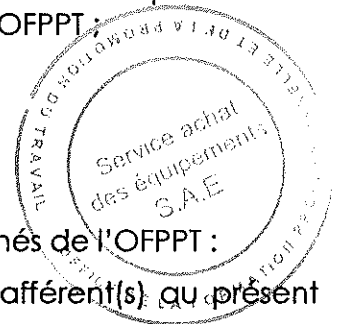
Conformément aux dispositions de l'article n°24 du Règlement des Marchés de l'OFPPT :

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 ;
- 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°6 : JUSTIFICATION DES CAPACITES ET DES QUALITES DES CONCURRENTS.**

Chaque concurrent est tenu de présenter un dossier administratif, un dossier technique et un dossier additif. 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 réalisation ainsi que le nom et la qualité du signataire et son appréciation, établies conformément au modèle joint en annexe.

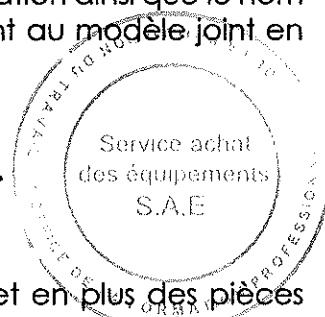
#### **ARTICLE N°7 : DOCUMENTS A FOURNIR PAR LES ETABLISSEMENTS PUBLICS.**

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 6 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 jourmada 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°8 : CONTENU DES DOSSIERS DES CONCURRENTS.**

Les dossiers présentés par les concurrents doivent comporter :

8.1 - **Les dossiers administratifs et techniques**, prévus à l'article 6 ci-dessus.

8.2 - **Une offre technique** :

L'offre technique du concurrent doit comprendre les éléments suivants :

1. Les « spécifications techniques des fournitures » renseignés conformément au canevas prévu à l'annexe : **Lot N°1, Lot N°2, lot n°3, lot n°4, lot n°5, lot n°6, Lot N°7, Lot N°8, lot n°9, lot n°9, lot n°10 et lot n°11** 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 équipements et/ou fournitures » afférents aux équipements et /ou fournitures proposées.

Ces catalogues et/ou documents relatifs aux « spécifications techniques des équipements et/ou fournitures » doivent être cachetés sur toutes les pages et portant le numéro de l'appel d'offres et l'item correspondant.

2. Une proposition d'au moins un (01) chef de projet (bac +4 minimum) ayant une expérience de 5 ans au minimum, un (1) ingénieur expérimenté (bac +4 minimum) ayant une expérience de 5 ans au minimum dans le secteur d'activité objet du présent Appel d'offres pour effectuer les opérations d'installation et mise en marche pour chaque lot.

Cette proposition doit contenir les CV, les diplômes et l'état de déclaration des salaires à la CNSS des 3 derniers mois.

3. Une attestation de(s) constructeur(s) (maison mère, représentant Régional ou local) certifiant que le soumissionnaire est agréé de commercialiser le matériel proposé portant sa marque pour tous les lots.
4. Une attestation d'agrément du service après-vente du soumissionnaire pour réparer le matériel proposé, ou tout autre moyen justifiant la garantie auprès des éditeurs et constructeurs ou son représentant régional ou local (pour la réception)



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.

8.3 - **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'OFPPPT, 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 prix établis par le Maître d'Ouvrage Délégué 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 doivent 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.

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



**ARTICLE N°9 : OFFRE VARIANTE.**

Des offres variantes pourront être proposées par les concurrents.

La présentation des offres 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.

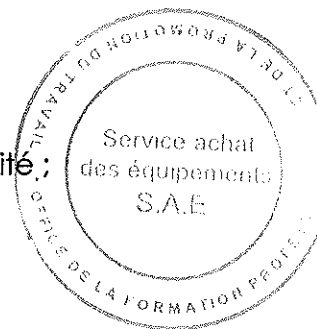
Les offres variantes présentées par les concurrents font l'objet d'un pli distinct de l'offre de base éventuellement proposée. Dans ce cas, les pièces du dossier administratif visées à l'alinéa 1) du paragraphe I-A de l'article 6 et de l'article 7 ci-dessus, le dossier technique est valable aussi bien 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 14 ci-dessous, accompagnée des dossiers prévus à l'article 8 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°10 : 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°11 : INFORMATION DES CONCURRENTS.**

Tout concurrent peut demander au Maître d'Ouvrage Délégué, 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 Délégué au moins sept (7) jours avant la date prévue pour la séance d'ouverture des plis.

Le Maître d'Ouvrage Délégué 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 Délégué 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 Délégué 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°12 : 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 Délégué 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 Délégué, 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 Délégué d'apprécier sa demande de report.

Si le Maître d'Ouvrage Délégué 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 Délégué.

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°13 : REPARTITION EN LOTS.**

- Le jugement des offres, prévu pour le présent appel d'offres, est un jugement **par lot**.
- Le lot fait l'objet d'un seul marché séparé et les quantités indiquées aux différents lots sont indivisibles.
- Le soumissionnaire doit obligatoirement offrir l'ensemble de la quantité indiquée à chaque lot.
- Les offres partielles, techniques et financières, ne sont en aucun cas prises en considération.

Pour l'attribution, le Maître d'Ouvrage Délégué procède à l'ouverture, à l'examen des offres de chaque lot, et à l'attribution par lot.

**ARTICLE N°14 : PRESENTATION 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 :

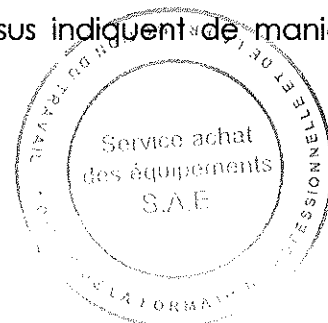
- Le nom et l'adresse du concurrent ;
- L'objet du marché et, éventuellement, l'indication du lot ;
- La date et l'heure de la séance d'ouverture des plis ;
- L'avertissement que " le pli ne doit être ouvert que par le président de la commission d'appel d'offres lors de la séance publique d'ouverture 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 et technique** ».
- b) La deuxième enveloppe comprend l'offre financière du soumissionnaire « Une enveloppe pour chaque lot ». 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 porte 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°15 : 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°16 : DEPOT 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.

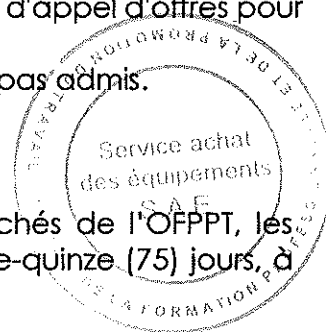
Le délai pour la réception des plis expire à la date et l'heure fixées par l'avis d'appel d'offres pour la séance d'ouverture des plis.

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

**ARTICLE N°17 : DELAI DE VALIDITE 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 Délégué 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 Délégué, avant la date limite fixée par ce dernier, restent engagés pendant ce nouveau délai.



**ARTICLE N°18 : 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°19 : PRIX PREFERENTIELS 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.

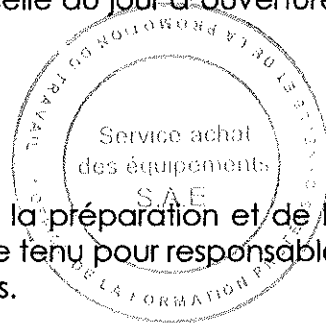
**ARTICLE N°20 : MONNAIE DE L'OFFRE.**

Pour le concurrent national, la monnaie dans laquelle le prix des offres doit être formulé et exprimé en Dirhams.

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°21 : DEPENSES 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°22 : EVALUATION DES DOSSIERS 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 **deux** attestations de références, conformes aux prescriptions de l'article 6-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 des lots concernés, 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 réalisé 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'informations, des données sur leurs offres techniques. Ces éléments qui doivent concerner les documents contenus dans lesdites offres.
- La présence des CV, Diplômes et Attestations CNSS pour les ingénieurs et les techniciens proposés pour l'installation et la mise en marche des équipements objet du présent AO.
- Tout article ne répondant pas aux spécifications techniques demandées sera déclaré non conforme.
- La commission peut, avant de se prononcer, charger une sous-commission technique pour analyser les offres techniques proposées.


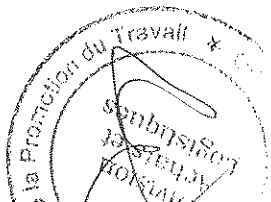

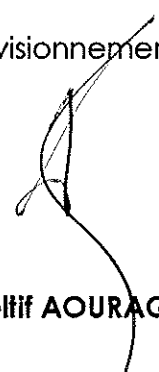
Conformément aux dispositions des articles 39, 40 et 41 du Règlement des Marchés de l'OFPPPT précité, l'examen des offres financières concerne les seuls concurrents admis à l'issue de l'examen de leurs dossiers administratifs et techniques et leur offre technique y compris catalogues, catalogues, et/ou 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 disant par lot.



**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.

<b>Etabli par :</b>  	<b>Vérifié par le Service des Marchés :</b> 
<b>Le Maître d'Ouvrage Délégué</b>	
<p>Le Directeur de l'Approvisionnement et de la Logistique</p>  <p><b>Abdellif AOURAGH</b></p>	





**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 fourniture, l'installation et la mise en œuvre d'un Firewall Nouvelle Génération destiné aux cités des métiers et des compétences ; réparti en lots suivants :**

Lot N° : .....

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**

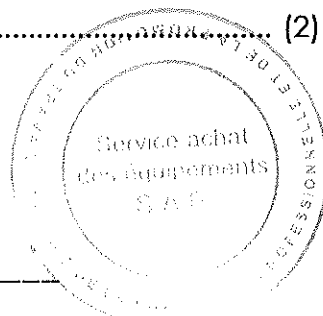
**a) Pour les personnes physiques**

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)

(1) ouvert à mon nom (ou au nom de la société) à..... (Localité), sous relevé d'identification bancaire (RIB) numéro.....

Fait à.....le.....

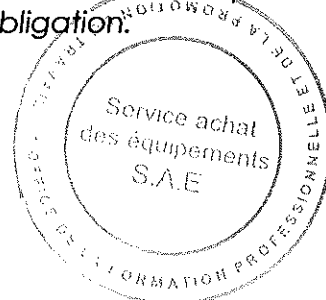
(Signature et cachet du concurrent)

(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 ;

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



**MODELE DE DECLARATION SUR L'HONNEUR**

\*\*\*\*\*

**DECLARATION SUR L'HONNEUR**

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

**Objet du marché : La fourniture, l'installation et la mise en œuvre d'un Firewall Nouvelle Génération destiné aux cités des métiers et des compétences ; réparti en lots suivants :**

**Lot N° :** .....

**A - Pour les personnes physiques**

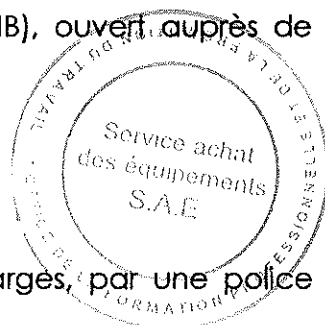
Je, soussigné : ..... (Prénom, nom et qualité)  
 Agissant en mon nom personnel et pour mon propre compte,  
 Adresse du domicile élu : .....  
 Affilié à la CNSS sous le n° : ..... (1)  
 Inscrit au registre du commerce de ..... (Localité) sous le n°  
 ..... (1) n° de patente ..... (1)  
 N° du compte courant postal, bancaire ou à la TGR ..... (RIB), ouvert auprès de  
 .....

**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), ouvert auprès de  
 .....  
 N° d'identification fiscale .....  
 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 remplie les conditions prévues à l'article 24 du règlement des marchés, approuvé le 18 Chaâbane 1435 (16 juin 2014) et fixant les conditions et les formes de passation des marchés de l'office de la formation et de la promotion du travail (OFPPT) ainsi que certaines règles relatives à leur gestion et à leur contrôle ;

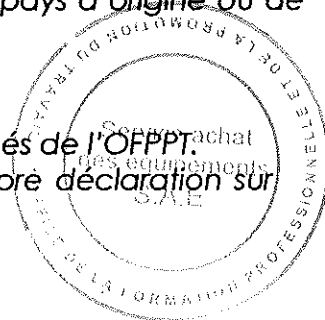


- 3- Etant en redressement judiciaire j'atteste que je suis autorisé par l'autorité judiciaire compétente à poursuivre l'exercice de mon activité (2) ;
- 4- m'engager, si j'envisage de recourir à la sous-traitance :
- à m'assurer que les sous-traitants remplissent également les conditions prévues par 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 Délégué 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 JOUMADA 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

\*\*\*\*\*

### 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

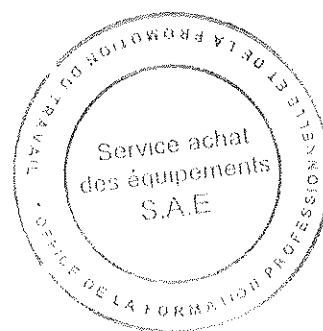
Signature et cachet

Nom et Prénom du signataire

Qualité du signataire

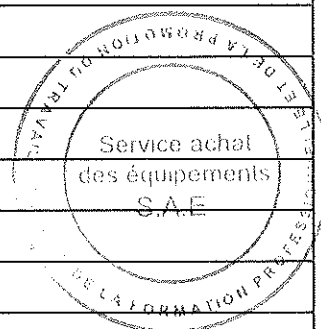


**CAHIER DES PRESCRIPTIONS SPECIALES  
(C. P. S.)**



## SOMMAIRE

ARTICLE 1	:	OBJET DU MARCHE.
ARTICLE 2	:	MAITRISE D'OUVRAGE DELEGUEE ET REGLEMENT DE PASSATION APPLICABLE
ARTICLE 3	:	DOCUMENTS CONSTITUTIFS DU MARCHE.
ARTICLE 4	:	AUTRES TEXTES APPLICABLES.
ARTICLE 5	:	CARACTERE DES PRIX.
ARTICLE 6	:	NATURE DES PRIX.
ARTICLE 7	:	DROITS DE TIMBRES.
ARTICLE 8	:	DELAI D'EXECUTION ET PENALITES DE RETARD.
ARTICLE 9	:	CAUTIONNEMENTS PROVISoire ET DEFINITIF.
ARTICLE 10	:	LIVRAISON DES EQUIPEMENTS AU SITE BENEFICIAIRE
ARTICLE 11	:	MODALITES DE VERIFICATION DE CONFORMITE TECHNIQUE
ARTICLE 12	:	MODALITES DE RECEPTION DES EQUIPEMENTS
ARTICLE 13	:	FORMATION
ARTICLE 14	:	RECEPTIONS PROVISoire ET DEFINITIVE.
ARTICLE 15	:	MODE DE REGLEMENT.
ARTICLE 16	:	MODALITES DE PAIEMENT.
ARTICLE 17	:	UTILISATION DES DOCUMENTS CONTRACTUELS ET DIFFUSION DE RENSEIGNEMENTS.
ARTICLE 18	:	BREVETS.
ARTICLE 19	:	SOUS-TRAITANCE.
ARTICLE 20	:	DOMICILE DU TITULAIRE
ARTICLE 21	:	VALIDITE DU MARCHE.
ARTICLE 22	:	DELAI DE NOTIFICATION DE L'APPROBATION DU MARCHE.
ARTICLE 23	:	GARANTIE.
ARTICLE 24	:	RETENUE DE GARANTIE.
ARTICLE 25	:	DELAI DE GARANTIE.
ARTICLE 26	:	RESTITUTION DES CAUTIONNEMENTS PROVISoire ET DEFINITIF ET PAIEMENT DE LA RETENUE DE GARANTIE
ARTICLE 27	:	ASSURANCE ET RESPONSABILITES.
ARTICLE 28	:	REGLEMENT DES CONTESTATIONS.
ARTICLE 29	:	NANTISSEMENT.
ARTICLE 30	:	RESILIATION DU MARCHE.
ARTICLE 31	:	MESURES COERCITIVES



## 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) ainsi que certaines règles relatives à leur gestion et à leur contrôle.

Entre les soussignés :

**LA SOCIETE FONCIERE CMC S.A.** ou son délégué, représentée par son Directeur Général  
**Mme Loubna TRICHA,**

D'une part

Et,

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° : .....

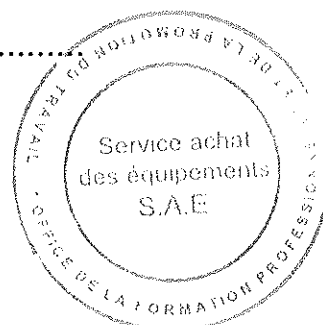
- Patente n° : .....

- N° d'identification fiscale

- n° de l'Identifiant de l'Entreprise : .....

- Représentée par :

Monsieur .....



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

D'autre part

**IL A ETE ARRETE ET CONVENU CE QUI SUIT**



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

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

Le présent marché a pour objet la fourniture, l'installation et la mise en œuvre d'un Firewall Nouvelle Génération destiné aux cités des métiers et des compétences ; réparti en lots suivants :

- Lot 1 : Solution de Firewall Nouvelle Génération NGFW pour la CMC NADOR
- Lot 2 : Solution de Firewall Nouvelle Génération NGFW pour la CMC LAAYOUNE
- Lot 3 : Solution de Firewall Nouvelle Génération NGFW pour la CMC TANGER
- Lot 4 : Solution de Firewall Nouvelle Génération NGFW pour la CMC RABAT
- Lot 5 : Solution de Firewall Nouvelle Génération NGFW pour la CMC BENI MELLAL
- Lot 6 : Solution de Firewall Nouvelle Génération NGFW pour la CMC MARRAKECH
- Lot 7 : Solution de Firewall Nouvelle Génération NGFW pour la CMC CASABLANCA
- Lot 8 : Solution de Firewall Nouvelle Génération NGFW pour la CMC FES
- Lot 9 : Solution de Firewall Nouvelle Génération NGFW pour la CMC ERRACHIDIA
- Lot 10 : Solution de Firewall Nouvelle Génération NGFW pour la CMC GUELMIM
- Lot 11 : Solution de Firewall Nouvelle Génération NGFW pour la CMC DAKHLA

### **ARTICLE 2 : MAITRISE D'OUVRAGE DELEGUEE ET REGLEMENT DE PASSATION APPLICABLE**

SOCIETE FONCIERE CMC S.A. a confié à l'Office de la Formation Professionnelle et de la Promotion de Formation professionnel (OFPPT) la mission globale de maîtrise d'ouvrage déléguée du programme des Cités des Métiers et des Compétences.

A cet effet, le Maître d'Ouvrage Délégué (OFPPT) agira pour l'accomplissement de la mission qui lui est confiée au nom et pour le compte du Maître d'Ouvrage (SOCIETE FONCIERE CMC S.A.).

A ce titre, le présent marché est passé en application à l'alinéa 2, paragraphe 1 de l'article 16 et paragraphe 1 de l'article 17, du règlement des marchés, approuvé le 18 chaâbane 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 de Travail (OFPPT) ainsi que certaines règles relatives à leur gestion et à leur contrôle.

### **ARTICLE 3 : 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 4 : AUTRES TEXTES APPLICABLES.**

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

- Le règlement des marchés, approuvé le 18 Chaâbane 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).
- Le dahir n°1.85.347 du 20/12/1985 relatif à l'institution générale de la taxe sur la valeur ajoutée (TVA).
- Le dahir n° 1-15-05 du 29 rabii II 1436 (19 février 2015) portant promulgation de la loi n°12-13 relative au nantissement des marchés publics.
- Le décret royal n° 330-66 du 10 moharrem 1387 (21 avril 1967) portant règlement général de comptabilité publique tel qu'il a été modifié et complété.
- L'arrêté 2-3663 du 13 /07/2005 portant Organisation financière et comptable de l'OFPPT.
- 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.
- Les textes officiels réglementant la main d'œuvre et les salaires.

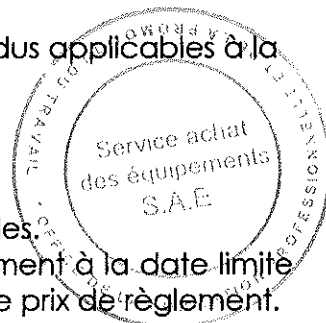
Ainsi que tous les textes réglementaires ayant trait aux marchés publics rendus applicables à la date limite de réception des offres.

#### **ARTICLE N°5 : CARACTERE DES PRIX.**

Les prix des prestations 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°6 : NATURE DES PRIX.**

Le présent marché est à prix unitaires.



Les sommes dues au titulaire sont calculées par application des prix unitaires portés au bordereau des prix - détail estimatif, aux quantités pour les prestations réellement exécutées conformément au marché.

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

#### **ARTICLE N°7 : DROITS DE TIMBRES.**

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

#### **ARTICLE N°8 : FORMALITES DE DOUANES ET DU COMMERCE EXTERIEUR**

Dans le cadre de l'exécution des marchés afférents aux projets des Cités des Métiers et des Compétences (CMC), le titulaire **pourra ou non** opter pour le bénéfice de la franchise tel que précisé ci-après :

##### **a. Le titulaire ayant opté pour bénéficier de la franchise douanière :**

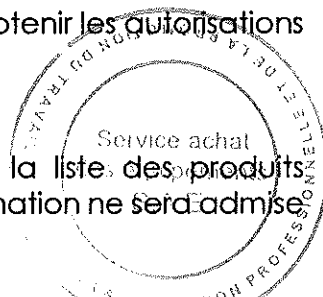
Les équipements du présent marché pourront bénéficier de la franchise des droits de douanes et des taxes à l'importation, sur demande du titulaire, et ce conformément à la convention de l'UNESCO à laquelle le Maroc a adhéré par Dahir n°1.60201 et n°160.202 du 14 Joumada I 1383 (3 Octobre 1963).

Toutes les formalités d'établissement des demandes d'importation et d'obtention des autorisations d'importation délivrées par l'autorité gouvernementale chargée du commerce et de l'industrie (direction du commerce extérieur et Office des changes) ainsi que toutes les formalités douanières seront réalisées par le titulaire et les frais y afférents seront à sa charge.

A cet effet, le titulaire devra prendre toutes les mesures nécessaires pour obtenir les autorisations d'importation dûment visées par les autorités compétentes.

Le titulaire est réputé être au courant des démarches à suivre et de la liste des produits susceptibles d'être non autorisés à l'importation au MAROC. Aucune réclamation ne sera admise à cet effet par l'O.F.P.P.T.

En tant que Maître d'Ouvrage Délégué (MOD), l'O.F.P.P.T. s'engage à fournir au titulaire en temps voulu les documents de son ressort et qui sont nécessaires à l'accomplissement des formalités ci-dessus.



**b. Le titulaire n'ayant pas opté pour bénéficier de la franchise douanière :**

En vertu de l'article 92 (I-6°) du Code Général des impôts, les droits de la TVA sont exonérés au titre du présent marché.

A cet effet, le titulaire devra fournir à l'OFPPT une facture pro-forma globale égale à la valeur du marché pour permettre à l'OFPPT d'obtenir l'attestation d'exonération de la TVA.

Sur la base de l'attestation d'exonération de la TVA délivrée par l'Administration fiscale Marocaine, le titulaire devra fournir les factures en Hors TVA portant la mention « exonération de la taxe sur la valeur ajoutée en vertu de l'article 92 (I-6°) du Code Général des Impôts ».

**ARTICLE N°9 : FORMALITES DE FRANCHISE DOUANIÈRE ET D'EXONERATION DE LA TVA.**

**a. Le titulaire ayant opté pour bénéficier de la franchise douanière :**

Le matériel bénéficiant de la franchise douanière UNESCO bénéficiera d'une exonération de la TVA et ce en application de l'article 8 paragraphe 28 de la loi n°30-85 tel qu'elle a été modifiée et complétée.

L'OFPPT demandera l'exonération de la TVA à la Direction des impôts après avoir reçu du titulaire du marché les pièces suivantes :

-La demande d'attestation d'achat en exonération de la TVA en annexe dûment remplie par le titulaire ;

- La facture pro forma en quatre exemplaires ;

- L'original de la décision soldée de la franchise douanière dûment visée par l'inspecteur douanier ;

-La copie de la déclaration unique de marchandise (DUM) ;

**b. Le titulaire n'ayant pas opté pour bénéficier de la franchise douanière :**

En vertu de l'article 92 (I-6°) du Code Général des impôts, les droits de la TVA sont exonérés au titre du présent marché.

A cet effet, le titulaire devra fournir à l'OFPPT une facture pro-forma globale égale à la valeur du marché pour permettre à l'OFPPT d'obtenir l'attestation d'exonération de la TVA.

Sur la base de l'attestation d'exonération de la TVA délivrée par l'Administration fiscale Marocaine, le titulaire devra fournir les factures en Hors TVA portant la mention « exonération de la taxe sur la valeur ajoutée en vertu de l'article 92 (I-6°) du Code Général des Impôts ».



**ARTICLE N°10 : DELAI D'EXECUTION ET PENALITES DE RETARD.**

**Délai d'exécution :**

Le délai contractuel pour l'exécution des prestations objet du présent marché (par Lot) est de :  
**120 jours (Cent vingt jours).**

Il commence à courir à compter de la date fixée par l'ordre de service prescrivant le commencement des prestations objet du présent marché. 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.

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

L'O.F.P.T. s'engage à fournir au titulaire en temps voulu les documents de son ressort et qui sont nécessaires à l'accomplissement des formalités ci-dessus.

**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 du marché, éventuellement majoré par les montants correspondants aux travaux supplémentaires et à l'augmentation dans la masse et ce, par jour calendaire.

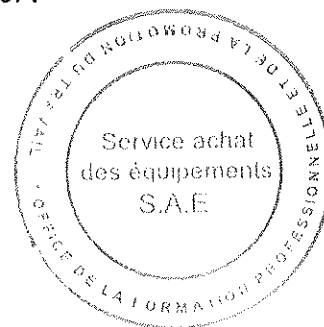
Le montant global des pénalités au titre des retards est plafonné à huit pour cent (8%) du montant initial du marché augmenté le cas échéant du montant des avenants.

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°11 : 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 CCAGT est :

- Lot 1 : Mille sept cents Dirhams (1.700,00 DH)
- Lot 2 : Mille sept cents Dirhams (1.700,00 DH)
- Lot 3 : Mille sept cents Dirhams (1.700,00 DH)
- Lot 4 : Mille sept cents Dirhams (1.700,00 DH)
- Lot 5 : Mille sept cents Dirhams (1.700,00 DH)
- Lot 6 : Mille sept cents Dirhams (1.700,00 DH)
- Lot 7 : Mille sept cents Dirhams (1.700,00 DH)
- Lot 8 : Mille sept cents Dirhams (1.700,00 DH)
- Lot 9 : Mille sept cents Dirhams (1.700,00 DH)



- Lot 10 : Mille sept cents Dirhams (1.700,00 DH)
- Lot 11 : Mille sept cents Dirhams (1.700,00 DH)

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°12 : LIVRAISON DES EQUIPEMENTS EN FAVEUR DU SITE BENEFICIAIRE.**

Les équipements seront livrés aux sites bénéficiaires indiqués dans les tableaux de répartition en annexe. Toutefois, et pour des raisons exceptionnelles dûment justifiées et à la demande de l'OFPPT, la liste des sites bénéficiaires et la répartition peut être modifiée sans impact sur les prix ou autres conditions des marchés.

Si le Site Bénéficiaire est indisponible pour une livraison directe du matériel, l'OFPPT se réserve le droit de demander au Titulaire d'effectuer le Dépôt dans un Entrepôt dédié sur le périmètre urbain de Casablanca.

Toutefois, l'acheminement des équipements vers le Site Bénéficiaire est à la charge du Titulaire. Avant de commencer les livraisons, le titulaire doit transmettre à l'OFPPT :

- Un planning prévisionnel de livraison au moins quinze jours avant le début des livraisons dans les sites bénéficiaires

Toutefois et pour des raisons exceptionnelles dûment justifiées et à la demande de l'OFPPT, la liste des sites bénéficiaires et la répartition dudit planning peut être modifiée sans impact sur les prix ou autres conditions des marchés.

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 et ce dans les sites bénéficiaires et /ou l'entrepôt dédié.

Le responsable du centre bénéficiaire ou de l'entrepôt signe les bons de dépôt des articles livrés en précisant les dates de livraison.

Le titulaire doit communiquer à l'OFPPT le bon de dépôt contre accusé de réception, pour permettre aux services de l'OFPPT de planifier les opérations de vérification de conformité technique.



**ARTICLE N°13 : 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 le site bénéficiaire suivant un planning communiqué au titulaire.

En cas d'indisponibilité du Site bénéficiaire, les opérations de vérification de conformité technique seront effectuées dans l'Entrepôt dédié avant l'acheminement du matériel vers le Site bénéficiaire.

Il est bien entendu qu'en cas de livraison à l'entrepôt dédié, la vérification portera sur la conformité technique et les essais de mise en marche, tandis que l'installation et la mise en marche se feront sur le site bénéficiaire.

Une lettre d'engagement doit être signée par le titulaire afin d'effectuer les opérations d'installation nécessaire après l'acheminement du matériel vers le Site bénéficiaire.

Le retard enregistré dans l'opération de vérification de conformité technique et de réception, après livraison du matériel, sera à la charge de l'OFPPT 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 ;

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 et ce dans les sites bénéficiaires et /ou l'entrepôt dédié.

Le titulaire prend en charge les accessoires, les composants, la matière d'œuvre et toutes sujétions nécessaire à l'installation, la mise en service et aux différents essais de ces équipements.

Les équipements jugés non-conformes sont récupérés séance tenante par le titulaire, ceux présentant des observations doivent faire l'objet de levée de réserves dans un délai maximum de **15 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).

L'OFPPT procédera à la vérification de la conformité technique de l'équipement avec les spécifications du marché) (marque, référence, origine, dimensions, capacités, puissance, alimentation électrique, ...) dans les sites bénéficiaires et /ou l'entrepôt dédié, 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'OFPPT et du titulaire ayant participé à l'opération de vérification.

Toute divergence par rapport au marché 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.

Le titulaire remettra aux représentants du site bénéficiaire 5 exemplaires originales des bons de livraison, afin de renseigner les numéros d'enregistrement dans les livres journal et inventaire dans le site bénéficiaire et /ou l'entrepôt dédié.

#### **ARTICLE N°14 : 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.

La réception n'est prononcée qu'une fois l'équipement, vérifié conforme, satisfait aux essais exigés.

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.

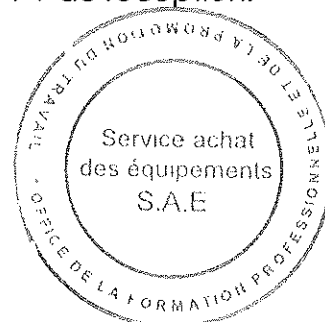
#### **ARTICLE N° 15 : FORMATION.**

Il n'est pas prévu de formation pour ce marché.

#### **ARTICLE N°16 : RECEPTIONS PROVISOIRE ET DEFINITIVE.**

##### **1- 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.





Le titulaire est tenu de présenter une attestation ou tout autre moyen prouvant la souscription de la garantie auprès des éditeurs et constructeurs.

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'OFPPT peut effectuer les réparations ou remplacements aux frais du titulaire de marché ou prendre d'autres mesures correctives.

## **ARTICLE N°17 : MODE DE REGLEMENT.**

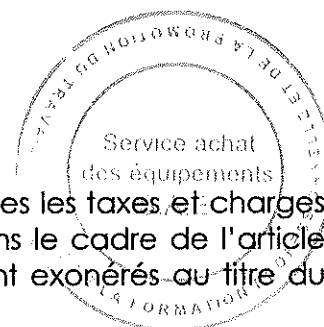
Les prestations faisant l'objet du marché seront réglées par application des prix unitaires définis et établis pour chaque item par le titulaire aux quantités réellement exécutées et réceptionnées, conformément aux descriptions figurant au bordereau des prix-détail estimatif et aux conditions particulières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

## **ARTICLE N°18 : MODALITES DE PAIEMENT.**

Tous les prix du présent marché seront établis en tenant compte de toutes les taxes et charges diverses, y compris la taxe sur la valeur ajoutée "T.V.A". Toutefois et dans le cadre de l'article l'article 92 (I-6°) du Code Générale des impôts, les droits de la TVA sont exonérés au titre du présent marché.

A cet effet, le titulaire devra fournir à l'OFPPT une facture pro-forma globale égale à la valeur du marché pour permettre à l'OFPPT d'obtenir l'attestation d'exonération de la TVA.

Sur la base de l'attestation d'exonération de la TVA délivrée par l'Administration fiscale Marocaine, le titulaire devra fournir les factures en Hors TVA portant la mention « exonération de la taxe sur la valeur ajoutée en vertu de l'article 92 (I-6°) du Code Général des Impôts. ».



Société Foncière CMC S.A. procédera au paiement des articles livrés et réceptionnés conformes.

1) Modalités de paiement pour livraison directe sur le Site bénéficiaire :

Le titulaire adressera à la Société Foncière CMC S.A. les documents constituant le dossier de paiement suivants :

- Les Factures en cinq exemplaires originales portant la date de la facture, le numéro de la facture, l'objet et le numéro du marché, le(s) site(s) bénéficiaire (s), l'arrêté du montant de la facture en chiffre et en lettre.
- Les bons de dépôt portant les dates de livraison dûment signé et cacheté par les représentants du site bénéficiaire
- Les bons de livraison portant la date d'enregistrement et les numéros des livres journal et inventaire.
- Les Copies du PV de vérification de conformité technique.
- Les attestations des polices d'assurances de l'année de l'exécution du marché.
- Le planning prévisionnel de livraison
- Le PV de la formation si le marché le prévoit.

Les sommes dues au titulaire seront réglées sur son compte dont le numéro est précisé dans l'acte d'engagement.

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

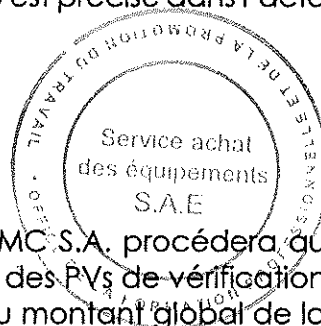
2) Modalités de paiement pour livraison sur l'Entrepôt dédié :

a) Livraison sur l'Entrepôt dédié :

- En cas de livraison dans l'entrepôt dédié, La Société Foncière CMC S.A. procédera au paiement des articles livrés et réceptionnés conformes sur la base des PVs de vérification de conformité technique et essai de marche à hauteur de 65% du montant global de la facture.

Le titulaire adressera à la Société Foncière CMC S.A. les documents constituant le dossier de paiement suivants :

- Les Factures en cinq exemplaires originaux portant la date de la facture, le numéro de la facture, l'objet et le numéro du marché, le(s) site(s) bénéficiaire (s), l'arrêté du montant de la facture en chiffre et en lettre.
- Les bons de dépôt portant les dates de livraison dûment signé et cacheté par le Magasinier de l'entrepôt dédié.
- Les bons de livraison portant la date d'enregistrement et les numéros des livres journal et inventaire.
- Les Copies du PV de vérification de conformité technique et essai de marche
- Les attestations des polices d'assurances de l'année de l'exécution du marché.
- Le planning prévisionnel de livraison



- Une lettre d'engagement signée par le titulaire afin d'effectuer les opérations d'installation et de formation nécessaires après l'acheminement du matériel vers le Site bénéficiaire

Les sommes dues au titulaire seront réglées sur son compte dont le numéro est précisé dans l'acte d'engagement.

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

b) Livraison et acheminement vers le Site Bénéficiaire :

Le reliquat de 35% sera réglé après l'acheminement et l'installation du matériel dans le Site bénéficiaire.

Le titulaire adressera à la Société Foncière CMC S.A. les documents constituant le dossier de paiement suivants :

- Les Factures en cinq exemplaires originales portant la date de la facture, le numéro de la facture, l'objet et le numéro du marché, le(s) site(s) bénéficiaire (s), l'arrêté du montant de la facture en chiffre et en lettre.
- Les bons de dépôt portant les dates de livraison dûment signé et cacheté par les représentants du site bénéficiaire
- Les bons de livraison portant la date d'enregistrement et les numéros des livres journal et inventaire.
- Les Copies du PV de vérification de conformité technique.
- Les attestations des polices d'assurances de l'année de l'exécution du marché.
- Le planning prévisionnel de livraison
- Le PV de la formation si le marché le prévoit.

Le Maître d'Ouvrage se libérera des sommes dues en exécution du présent marché en faisant donner crédit au compte ouvert au nom du prestataire indiqué sur l'acte d'engagement. Les paiements se feront sur la base du montant Hors Taxes, conformément aux dispositions prévues par la Code Générale des Impôts.

Dans le cas où ladite exonération n'est plus applicable, le Maître d'ouvrage paiera la TVA conformément aux règles de droit commun.

Aussi, les prestations de service réalisées pour le compte du maître d'ouvrage par une entreprise non résidente sont soumises à l'impôt sur les sociétés au taux de 10% de ces prestations. Cet impôt est prélevé du montant desdites prestations sous forme de retenue à la source. Une copie de l'attestation du versement de cet impôt sera remise au prestataire, à sa demande. Pour les entreprises originaires de pays ayant signé avec le Maroc une convention destinée à éviter les doubles impositions, la retenue à la source est déductible des impôts dus dans leur pays d'origine.

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

**ARTICLE N°19 : UTILISATION DES DOCUMENTS CONTRACTUELS ET DIFFUSION DE RENSEIGNEMENTS.**

Le titulaire, sauf consentement préalable donné par écrit par l'OFPPT, ne communiquera le marché, ni aucune de ses clauses, ni aucune des spécifications, des plans, dessins, tracés,

échantillons ou information fournis par l'OFPPT 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'OFPPT, n'utilisera aucun des documents et aucune des informations énumérés dans le paragraphe précédent, si ce n'est pour l'exécution du marché.

Tout document, autre que le marché lui-même, énuméré dans le 1er paragraphe demeurera la propriété de l'OFPPT et tous ses exemplaires seront renvoyés à l'OFPPT sur sa demande, une fois les obligations contractuelles du titulaire exécutées.

#### **ARTICLE N°20 : BREVETS.**

Le titulaire garantira la Société Foncière CMC S.A., 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°21 : 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'OFPPT.

#### **ARTICLE N°22 : 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 Délégué 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 Délégué, par lettre recommandée avec accusé de réception, dans les quinze (15) jours suivant la date d'intervention de ce changement.

#### **ARTICLE N°23 : VALIDITE DU MARCHE.**

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



**ARTICLE N°24 : 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'OFPPT.

**ARTICLE N°25 : 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 la Société Foncière CMC S.A.

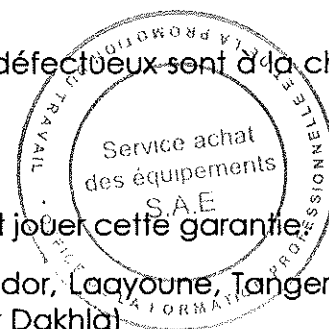
Les frais de récupération ou de remplacement des équipements défectueux sont à la charge exclusive de ce dernier.

**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 au niveau (Nador, Laayoune, Tanger, Beni Mellal, Marrakech, Rabat, Fès, Casablanca, Errachidia, Guelmim et Dakhla).

Le titulaire dispose de 72 heures pour les sites (Nador, Laayoune, Tanger, Beni Mellal, Marrakech, Rabat, Fès, Casablanca, Errachidia, Guelmim et Dakhla) pour réparer ou remplacer l'équipement défectueux avec un équipement équivalent (connectiques incluses).



Site	Délai d'intervention	Délai de réparation
CMC Nador	48 H	72 H
CMC Laayoune		
CMC Tanger		
CMC Rabat		
CMC Beni Mellal		
CMC Marrakech		
CMC Casablanca		
CMC Fès		
CMC Errachidia		
CMC Guelmim		
CMC Dakhla		

**ARTICLE N°26 : 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°27 : DELAI DE GARANTIE.**

Le délai de garantie est fixé à **un (1) an** pour les prestations objet du marché,

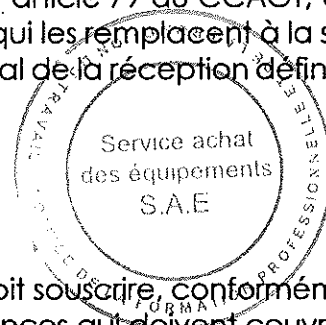
Il court à partir de la date de la dernière réception provisoire de ces équipements sur le Site bénéficiaire.

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°28 : RESTITUTION DES CAUTIONNEMENTS PROVISOIRE ET DEFINITIF ET PAIEMENT DE LA RETENUE DE GARANTIE.**

En application des dispositions de l'article 19 du CCAGT, 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 CCAGT, et le paiement de la retenue de garantie est effectué 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°29 : ASSURANCE ET RESPONSABILITES.**

En application des dispositions de l'article 25 du CCAGT, 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° 30 : 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 (CCAGT). 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 (CCAGT).

**ARTICLE N° 31 : 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 précisé que :

+ La liquidation des sommes dues par la Société Foncière CMC S.A. en exécution du présent marché sera opérée par les soins du Directeur Général de la Société Foncière CMC S.A. ou son délégataire.

+ Le fonctionnaire chargé de fournir au titulaire du futur marché ainsi qu'à bénéficier des nantissemments ou subrogations les renseignements, qui ont été prévus à l'article 8 du dahir susvisé.

+ 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 N°32 : RESILIATION DU MARCHE.**

Le marché peut être résilié par la Société Foncière CMC S.A. en concertation avec 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 Chaâbane 1437 (13 mai 2016) - CCAGT et règlement des marchés de l'OFPPT approuvé le 18 Chaâbane 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 : Solution de Firewall Nouvelle Génération NGFW pour la CMC NADOR**

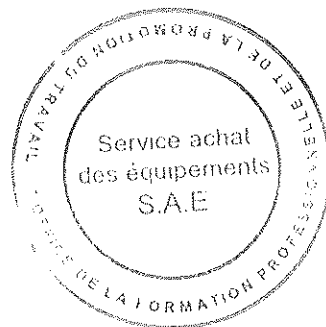
Item	Spécifications techniques
<b>1 .</b>	<b>Solution de Firewall Nouvelle Génération NGFW de type Appliance</b>
<b>1.1</b>	<b>Leader dans Gartner dans la technologie Network Firewall pour les trois années minimum 2019, 2020 et 2021</b>
	<p><b>Fonctions Firewall</b></p> <ul style="list-style-type: none"> <li>- Doit intégrer un système d'exploitation propriétaire sécurisé,</li> <li>- Filtrage de paquets et être doté de la fonction de filtrage dynamique,</li> <li>- Filtrage basé sur les applications niveau 7 en plus des ports/Protocol et par plages de ports UDP ou TCP</li> <li>- Filtrage et inspection en IPv4 et IPv6,</li> <li>- Failover de connexion Internet,</li> <li>- Prise en compte de paramètre Horaire dans les règles de filtrage,</li> <li>- Doit fournir, via sa console d'administration, des statistiques sur le nombre d'accès aux règles de sécurité,</li> <li>- Doit inclure la possibilité de fonctionner en mode transparent ou routé (natté),</li> <li>- 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,</li> <li>- La création de la politique de sécurité basée sur : <ul style="list-style-type: none"> <li>• Geolocation par pays</li> <li>• Zones</li> <li>• Groupes de Zones</li> <li>• Applications, Groupes d'applications</li> <li>• Catégories d'Applications</li> <li>• Technologies d'Applications</li> <li>• Filtres d'Applications</li> <li>• Utilisateurs et Groupes</li> <li>• Adresses IP, Groupes d'adresses IP, Sous-réseaux IP, Groupes de sous-réseaux IP</li> <li>• Services, Groupes de Services</li> </ul> </li> <li>- La solution doit être de type Next Generation Firewall avec capacité de prévention contre les menaces avancées, combinée avec des fonctionnalités de base suivantes (<b>licences incluses</b>) : <ul style="list-style-type: none"> <li>• <b>IPS (prévention des intrusions)</b> 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 : <ul style="list-style-type: none"> <li>- Détection par signatures ;</li> <li>- Détection par anomalies ;</li> <li>- Capable de faire des analyses comportementales de tout type de trafic ;</li> <li>- Possibilité de créer des signatures personnalisées ;</li> <li>- Mise à jour automatique des signatures IPS ;</li> <li>- Création et affectation des politiques IPS par type de zone ou interface ;</li> <li>- 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) ... ;</li> <li>- Gestion de profils IPS avec association à certains trafics dans la politique de filtrage (IP source, IP destination, service, protocole, réseau...) ;</li> </ul> </li> <li>• <b>Filtrage URL</b>, pour assurer le contrôle de l'accès interne aux contenus Web indésirables, non productifs, voire illégaux,</li> </ul> </li> </ul>



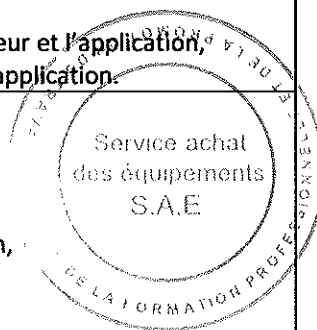
Handwritten marks: a checkmark and the signature 'H2'.



Item	Spécifications techniques
	<ul style="list-style-type: none"> <li>Control Applicatif, afin d'identifier, reconnaître et contrôler les applications dans les flux,</li> </ul>
	<p><b>Spécifications matérielles et performance :</b></p> <ul style="list-style-type: none"> <li>- Format : Appliance Rackable, 19"</li> <li>- Débit de Prevention des menaces (Firewall niveau 7 avec Contrôle applicatif + IPS + Anti Malware + Sandboxing+ Antispyware + filtrage URL, filtrage de contenu et Journalisation) : 2.5 Gbps Minimum</li> <li>- Nombre de sessions inspectées simultanées : 1 Million Minimum</li> <li>- Nombre de nouvelles sessions par seconde : 50 000 Minimum</li> <li>- Stockage Disque dur dédiée de type SSD de 200 GB Minimum</li> <li>- Les ports (en dehors des ports de management et de la haute disponibilité) <ul style="list-style-type: none"> <li>• Minimum 8 ports 10/100/1000 BaseT</li> <li>• Minimum 4 ports 1G/10G SFP/SFP+ dont 4 avec Transceiver SFP+</li> </ul> </li> <li>- Les ports de management et Clustering : <ul style="list-style-type: none"> <li>• Minimum 1 port 10/100/1000 BaseT pour le management</li> <li>• Minimum 1 port console RJ-45</li> <li>• Minimum 1 port USB</li> <li>• Minimum 1 ports 10/100/1000 BaseT pour le HA</li> </ul> </li> <li>- 2 Alimentations électriques Redondantes Minimum (AC),</li> </ul>
	<p><b>Support de la haute disponibilité :</b></p> <ul style="list-style-type: none"> <li>- Actif/Actif avec synchronisation d'état de session,</li> <li>- Actif/Passif,</li> </ul>
	<p><b>Contrôle applicatif :</b></p> <ul style="list-style-type: none"> <li>- Identification des applications en se basant sur : <ul style="list-style-type: none"> <li>• Signatures</li> <li>• Décodage du protocole (respecte la spécification du protocole)</li> <li>• Déchiffrement du trafic encapsulé</li> </ul> </li> <li>- Identification et contrôle des applications partageant la même connexion</li> <li>- Contrôle de la fonction de transfert de fichiers d'une application</li> <li>- Visibilité du trafic applicatif inconnu à travers l'identification de sa nature : <ul style="list-style-type: none"> <li>• Volume du trafic</li> <li>• Utilisateur et/ou adresses IP</li> <li>• Port utilisé</li> <li>• Contenu associé : fichier, menace ou autre.</li> </ul> </li> <li>- La base de données de contrôle des applications doit contenir plus de 3 000 applications connues ;</li> <li>- La solution doit pouvoir créer une règle de filtrage avec plusieurs catégories ;</li> </ul>
	<p><b>Identification, authentification des utilisateurs et protection des identités</b></p> <ul style="list-style-type: none"> <li>- Prise en charge des services d'authentification suivants pour l'identification et authentifications des utilisateurs : <ul style="list-style-type: none"> <li>• Active Directory</li> <li>• Kerberos</li> <li>• LDAP</li> <li>• Radius</li> </ul> </li> </ul>



Item	Spécifications techniques
	<ul style="list-style-type: none"> <li>• Base Locale</li> <li>• SAML</li> <li>• Authentification via SSO Kerberos sans agent</li> <li>• Authentification par Certificat client</li> <li>• Portail captif</li> <li>- Identification des utilisateurs indépendamment : <ul style="list-style-type: none"> <li>• Du terminal (ordinateur, un téléphone intelligent ou une tablette)</li> <li>• Du système d'exploitation utilisé,</li> <li>• Des adresses IP et de la zone (LAN, VPN, hors du périmètre du réseau)</li> </ul> </li> </ul>
	<p><b>Fonctions Réseau :</b></p> <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> <li>- Support de la fonctionnalité <b>SD-WAN</b> pour le routage avancé des flux sur plusieurs liaisons à base d'application afin d'augmenter la disponibilité et la performance WAN en se basant sur les paramètres de performance (Latence, Perte de packets et jitter) que ce soit lors de la navigation Internet et pour la communication inter-sites (<b>fonctionnalité et licence à fournir</b>)</li> </ul>
	<p><b>Fonction VPN :</b></p> <ul style="list-style-type: none"> <li>- VPN IPsec site-site, client-site et hub &amp; Spoke. (<b>Fonctionnalité et licence à fournir</b>)</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>
	<p><b>Gestion de la bande passante :</b></p> <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>
	<p><b>Administration et gestion des journaux :</b></p> <ul style="list-style-type: none"> <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> <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> </ul>



5

H2

Item	Spécifications techniques
	<ul style="list-style-type: none"> <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>
	<p><b>Filtrage URL et Filtrage de contenu</b></p> <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>
1.2	<p><b>PRESTATION DE SERVICE</b></p> <p>Le prestataire doit proposer dans son offre toutes les prestations nécessaires à la mise en œuvre de la solution de sécurité :</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>- Intégration de la solution dans le réseau de la CMC ;</li> <li>- L'interconnexion du NGFW avec les Switch Datacenter ;</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 d'un an 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 ;</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>

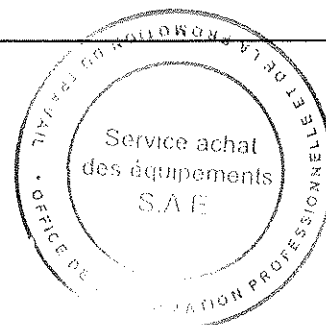
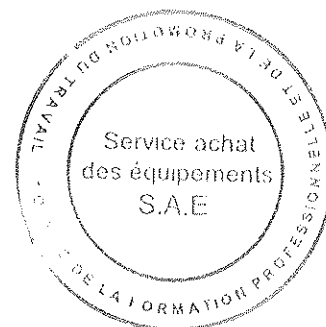


Tableau de répartition

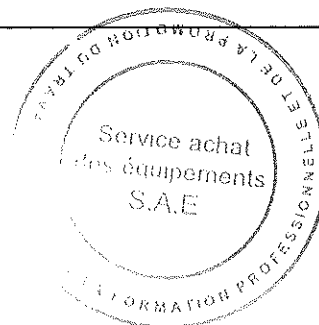
Item	Désignation	Unité	CMC NADOR
1	Solution de Firewall Nouvelle Génération NGFW de type Appliance		
1.1	Firewall	U	1
1.2	PRESTATION DE SERVICE	ens	1

**LOT 2 : Solution de Firewall Nouvelle Génération NGFW pour la CMC LAAYOUNE**

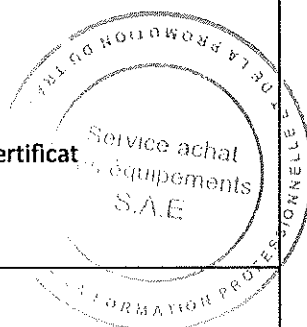
Item	Spécifications techniques
<b>1 .</b>	<b>Solution de Firewall Nouvelle Génération NGFW de type Appliance</b>
<b>1.1</b>	<b>Leader dans Gartner dans la technologie Network Firewall pour les trois années minimum 2019, 2020 et 2021</b>
	<p><b>Fonctions Firewall</b></p> <ul style="list-style-type: none"> <li>- Doit intégrer un système d'exploitation propriétaire sécurisé,</li> <li>- Filtrage de paquets et être doté de la fonction de filtrage dynamique,</li> <li>- Filtrage basé sur les applications niveau 7 en plus des ports/Protocol et par plages de ports UDP ou TCP</li> <li>- Filtrage et inspection en IPv4 et IPv6,</li> <li>- Failover de connexion Internet,</li> <li>- Prise en compte de paramètre Horaire dans les règles de filtrage,</li> <li>- Doit fournir, via sa console d'administration, des statistiques sur le nombre d'accès aux règles de sécurité,</li> <li>- Doit inclure la possibilité de fonctionner en mode transparent ou routé (natté),</li> <li>- 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,</li> <li>- La création de la politique de sécurité basée sur : <ul style="list-style-type: none"> <li>• Geolocation par pays</li> <li>• Zones</li> <li>• Groupes de Zones</li> <li>• Applications, Groupes d'applications</li> <li>• Catégories d'Applications</li> <li>• Technologies d'Applications</li> <li>• Filtres d'Applications</li> <li>• Utilisateurs et Groupes</li> <li>• Adresses IP, Groupes d'adresses IP, Sous-réseaux IP, Groupes de sous-réseaux IP</li> <li>• Services, Groupes de Services</li> </ul> </li> <li>- La solution doit être de type Next Generation Firewall avec capacité de prévention contre les menaces avancées, combinée avec des fonctionnalités de base suivantes (<b>licences incluses</b>) : <ul style="list-style-type: none"> <li>• <b>IPS (prévention des intrusions)</b> 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 : <ul style="list-style-type: none"> <li>- Détection par signatures ;</li> <li>- Détection par anomalies ;</li> <li>- Capable de faire des analyses comportementales de tout type de trafic ;</li> </ul> </li> </ul> </li> </ul>



Item	Spécifications techniques
	<ul style="list-style-type: none"> <li>- Possibilité de créer des signatures personnalisées ;</li> <li>- Mise à jour automatique des signatures IPS ;</li> <li>- Création et affectation des politiques IPS par type de zone ou interface ;</li> <li>- 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) ... ;</li> <li>- Gestion de profils IPS avec association à certains trafics dans la politique de filtrage (IP source, IP destination, service, protocole, réseau...) ;</li> <li>• <b>Filtrage URL</b>, pour assurer le contrôle de l'accès interne aux contenus Web indésirables, non productifs, voire illégaux,</li> <li>• <b>Control Applicatif</b>, afin d'identifier, reconnaître et contrôler les applications dans les flux,</li> </ul>
	<p><b>Spécifications matérielles et performance :</b></p> <ul style="list-style-type: none"> <li>- Format : Appliance Rackable, 19"</li> <li>- Débit de Prevention des menaces (Firewall niveau 7 avec Contrôle applicatif + IPS + Anti Malware + Sandboxing+ Antispyware + filtrage URL, filtrage de contenu et Journalisation) : <b>2.5 Gbps Minimum</b></li> <li>- Nombre de sessions inspectées simultanées : <b>1 Million Minimum</b></li> <li>- Nombre de nouvelles sessions par seconde : <b>50 000 Minimum</b></li> <li>- Stockage Disque dur dédiée de type SSD de <b>200 GB Minimum</b></li> <li>- Les ports (en dehors des ports de management et de la haute disponibilité) <ul style="list-style-type: none"> <li>• Minimum 8 ports 10/100/1000 BaseT</li> <li>• Minimum 4 ports 1G/10G SFP/SFP+ dont 4 avec Transceiver SFP+</li> </ul> </li> <li>- Les ports de management et Clustering : <ul style="list-style-type: none"> <li>• Minimum 1 port 10/100/1000 BaseT pour le management</li> <li>• Minimum 1 port console RJ-45</li> <li>• Minimum 1 port USB</li> <li>• Minimum 1 ports 10/100/1000 BaseT pour le HA</li> </ul> </li> <li>- 2 Alimentations électriques Redondantes Minimum (AC),</li> </ul>
	<p><b>Support de la haute disponibilité :</b></p> <ul style="list-style-type: none"> <li>- Actif/Actif avec synchronisation d'état de session,</li> <li>- Actif/Passif,</li> </ul>
	<p><b>Contrôle applicatif :</b></p> <ul style="list-style-type: none"> <li>- Identification des applications en se basant sur : <ul style="list-style-type: none"> <li>• Signatures</li> <li>• Décodage du protocole (respecte la spécification du protocole)</li> <li>• Déchiffrement du trafic encapsulé</li> </ul> </li> <li>- Identification et contrôle des applications partageant la même connexion</li> <li>- Contrôle de la fonction de transfert de fichiers d'une application</li> <li>- Visibilité du trafic applicatif inconnu à travers l'identification de sa nature : <ul style="list-style-type: none"> <li>• Volume du trafic</li> <li>• Utilisateur et/ou adresses IP</li> <li>• Port utilisé</li> <li>• Contenu associé : fichier, menace ou autre.</li> </ul> </li> <li>- La base de données de contrôle des applications doit contenir plus de <b>3 000 applications connues</b> ;</li> <li>- La solution doit pouvoir créer une règle de filtrage avec plusieurs catégories ;</li> </ul>
	<p><b>Identification, authentification des utilisateurs et protection des identités</b></p>



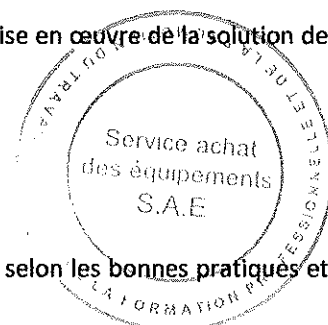
Item	Spécifications techniques
	<ul style="list-style-type: none"> <li>- Prise en charge des services d'authentification suivants pour l'identification et authentifications des utilisateurs : <ul style="list-style-type: none"> <li>• Active Directory</li> <li>• Kerberos</li> <li>• LDAP</li> <li>• Radius</li> <li>• Base Locale</li> <li>• SAML</li> <li>• Authentification via SSO Kerberos sans agent</li> <li>• Authentification par Certificat client</li> <li>• Portail captif</li> </ul> </li> <li>- Identification des utilisateurs indépendamment : <ul style="list-style-type: none"> <li>• Du terminal (ordinateur, un téléphone intelligent ou une tablette)</li> <li>• Du système d'exploitation utilisé,</li> <li>• Des adresses IP et de la zone (LAN, VPN, hors du périmètre du réseau)</li> </ul> </li> </ul>
	<p><b>Fonctions Réseau :</b></p> <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> <li>- Support de la fonctionnalité <b>SD-WAN</b> pour le routage avancé des flux sur plusieurs liaisons à base d'application afin d'augmenter la disponibilité et la performance WAN en se basant sur les paramètres de performance (Latence, Perte de packets et jitter) que ce soit lors de la navigation Internet et pour la communication inter-sites (<b>fonctionnalité et licence à fournir</b>)</li> </ul>
	<p><b>Fonction VPN :</b></p> <ul style="list-style-type: none"> <li>- VPN IPsec site-site, client-site et hub &amp; Spoke. (<b>Fonctionnalité et licence à fournir</b>)</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>
	<p><b>Gestion de la bande passante :</b></p> <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>
	<p><b>Administration et gestion des journaux :</b></p> <ul style="list-style-type: none"> <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> </ul>



5

WZ

Item	Spécifications techniques
	<ul style="list-style-type: none"> <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> <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>
	<p><b>Filtrage URL et Filtrage de contenu</b></p> <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>
1.2	<p><b>PRESTATION DE SERVICE</b></p> <p>Le prestataire doit proposer dans son offre toutes les prestations nécessaires à la mise en œuvre de la solution de sécurité :</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>- Intégration de la solution dans le réseau de la CMC ;</li> <li>- L'interconnexion du NGFW avec les Switch Datacenter ;</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 d'un an 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 ;</li> <li>- Livrables :</li> </ul>



T

12

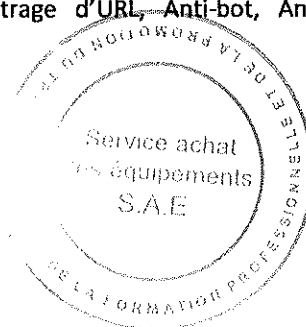
Item	Spécifications techniques
	<ul style="list-style-type: none"> <li>Document d'architecture finale et de configuration de la solution (avec schéma au format exploitable et un fichier de configuration) ;</li> <li>Manuel d'exploitation ;</li> </ul>

Tableau de répartition

Item	Désignation	Unité	CMC LAAYOUNE
1	Solution de Firewall Nouvelle Génération NGFW de type Appliance		
1.1	Firewall	U	1
1.2	PRESTATION DE SERVICE	ens	1

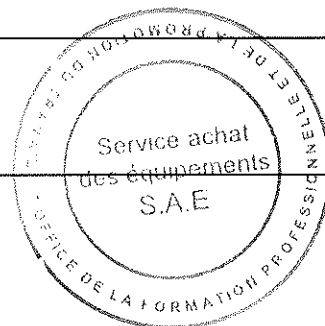
**LOT 3 : Solution de Firewall Nouvelle Génération NGFW pour la CMC TANGER**

Item	Spécifications techniques
1 .	<b>Solution de Firewall Nouvelle Génération NGFW de type Appliance</b>
1.1	<b>Leader dans Gartner dans la technologie Network Firewall pour les trois années minimum 2019, 2020 et 2021</b>
	<p><b>Fonctions Firewall</b></p> <ul style="list-style-type: none"> <li>- Doit intégrer un système d'exploitation propriétaire sécurisé,</li> <li>- Filtrage de paquets et être doté de la fonction de filtrage dynamique,</li> <li>- Filtrage basé sur les applications niveau 7 en plus des ports/Protocol et par plages de ports UDP ou TCP</li> <li>- Filtrage et inspection en IPv4 et IPv6,</li> <li>- Failover de connexion Internet,</li> <li>- Prise en compte de paramètre Horaire dans les règles de filtrage,</li> <li>- Doit fournir, via sa console d'administration, des statistiques sur le nombre d'accès aux règles de sécurité,</li> <li>- Doit inclure la possibilité de fonctionner en mode transparent ou routé (natté),</li> <li>- 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,</li> <li>- La création de la politique de sécurité basée sur : <ul style="list-style-type: none"> <li>• Geolocation par pays</li> <li>• Zones</li> <li>• Groupes de Zones</li> <li>• Applications, Groupes d'applications</li> <li>• Catégories d'Applications</li> <li>• Technologies d'Applications</li> <li>• Filtres d'Applications</li> <li>• Utilisateurs et Groupes</li> <li>• Adresses IP, Groupes d'adresses IP, Sous-réseaux IP, Groupes de sous-réseaux IP</li> <li>• Services, Groupes de Services</li> </ul> </li> <li>- 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) :</li> </ul>

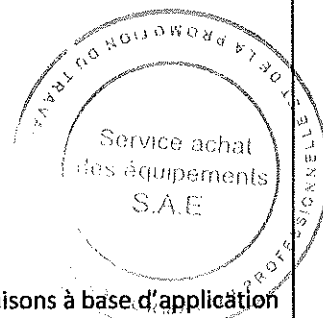




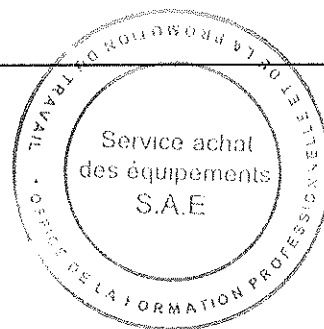
Item	Spécifications techniques
	<ul style="list-style-type: none"> <li>• <b>IPS (prévention des intrusions)</b> pour se protéger contre les menaces réseau telles que vers, chevaux de Troie et autres programmes malveillants. Le système de prévention des intrusions (IPS) doit aussi apporter une protection contre les menaces réseaux existantes et émergentes. Ce module IPS doit avoir deux mécanismes : <ul style="list-style-type: none"> <li>- Détection par signatures ;</li> <li>- Détection par anomalies ;</li> <li>- Capable de faire des analyses comportementales de tout type de trafic ;</li> <li>- Possibilité de créer des signatures personnalisées ;</li> <li>- Mise à jour automatique des signatures IPS ;</li> <li>- Création et affectation des politiques IPS par type de zone ou interface ;</li> <li>- 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) ... ;</li> <li>- Gestion de profils IPS avec association à certains trafics dans la politique de filtrage (IP source, IP destination, service, protocole, réseau...) ;</li> </ul> </li> <li>• <b>Filtrage URL</b>, pour assurer le contrôle de l'accès interne aux contenus Web indésirables, non productifs, voire illégaux,</li> <li>• <b>Control Applicatif</b>, afin d'identifier, reconnaître et contrôler les applications dans les flux,</li> </ul>
	<p><b>Spécifications matérielles et performance :</b></p> <ul style="list-style-type: none"> <li>- Format : Appliance Rackable, 19"</li> <li>- Débit de Prevention des menaces (Firewall niveau 7 avec Contrôle applicatif + IPS + Anti Malware + Sandboxing+ Antispyware + filtrage URL, filtrage de contenu et Journalisation) : 2.5 Gbps Minimum</li> <li>- Nombre de sessions inspectées simultanées : 1 Million Minimum</li> <li>- Nombre de nouvelles sessions par seconde : 50 000 Minimum</li> <li>- Stockage Disque dur dédiée de type SSD de 200 GB Minimum</li> <li>- Les ports (en dehors des ports de management et de la haute disponibilité) <ul style="list-style-type: none"> <li>• Minimum 8 ports 10/100/1000 BaseT</li> <li>• Minimum 4 ports 1G/10G SFP/SFP+ dont 4 avec Transceiver SFP+</li> </ul> </li> <li>- Les ports de management et Clustering : <ul style="list-style-type: none"> <li>• Minimum 1 port 10/100/1000 BaseT pour le management</li> <li>• Minimum 1 port console RJ-45</li> <li>• Minimum 1 port USB</li> <li>• Minimum 1 ports 10/100/1000 BaseT pour le HA</li> </ul> </li> <li>- 2 Alimentations électriques Redondantes Minimum (AC),</li> </ul>
	<p><b>Support de la haute disponibilité :</b></p> <ul style="list-style-type: none"> <li>- Actif/Actif avec synchronisation d'état de session,</li> <li>- Actif/Passif,</li> </ul>
	<p><b>Contrôle applicatif :</b></p> <ul style="list-style-type: none"> <li>- Identification des applications en se basant sur : <ul style="list-style-type: none"> <li>• Signatures</li> <li>• Décodage du protocole (respecte la spécification du protocole)</li> <li>• Déchiffrement du trafic encapsulé</li> </ul> </li> <li>- Identification et contrôle des applications partageant la même connexion</li> <li>- Contrôle de la fonction de transfert de fichiers d'une application</li> <li>- Visibilité du trafic applicatif inconnu à travers l'identification de sa nature : <ul style="list-style-type: none"> <li>• Volume du trafic</li> </ul> </li> </ul>



Item	Spécifications techniques
	<ul style="list-style-type: none"> <li>Utilisateur et/ou adresses IP</li> <li>Port utilisé</li> <li>Contenu associé : fichier, menace ou autre.</li> </ul> <ul style="list-style-type: none"> <li>La base de données de contrôle des applications doit contenir plus de 3 000 applications connues ;</li> <li>La solution doit pouvoir créer une règle de filtrage avec plusieurs catégories ;</li> </ul>
	<p><b>Identification, authentification des utilisateurs et protection des identités</b></p> <ul style="list-style-type: none"> <li>Prise en charge des services d'authentification suivants pour l'identification et authentifications des utilisateurs : <ul style="list-style-type: none"> <li>Active Directory</li> <li>Kerberos</li> <li>LDAP</li> <li>Radius</li> <li>Base Locale</li> <li>SAML</li> <li>Authentification via SSO Kerberos sans agent</li> <li>Authentification par Certificat client</li> <li>Portail captif</li> </ul> </li> <li>Identification des utilisateurs indépendamment : <ul style="list-style-type: none"> <li>Du terminal (ordinateur, un téléphone intelligent ou une tablette)</li> <li>Du système d'exploitation utilisé,</li> <li>Des adresses IP et de la zone (LAN, VPN, hors du périmètre du réseau)</li> </ul> </li> </ul>
	<p><b>Fonctions Réseau :</b></p> <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> <li>Support de la fonctionnalité <b>SD-WAN</b> pour le routage avancé des flux sur plusieurs liaisons à base d'application afin d'augmenter la disponibilité et la performance WAN en se basant sur les paramètres de performance (Latence, Perte de packets et jitter) que ce soit lors de la navigation Internet et pour la communication inter-sites (<b>fonctionnalité et licence à fournir</b>)</li> </ul>
	<p><b>Fonction VPN :</b></p> <ul style="list-style-type: none"> <li>VPN IPSec site-site, client-site et hub &amp; Spoke. (<b>Fonctionnalité et licence à fournir</b>)</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>



Item	Spécifications techniques
	<p><b>Gestion de la bande passante :</b></p> <ul style="list-style-type: none"> <li>- Réservation 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>
	<p><b>Administration et gestion des journaux :</b></p> <ul style="list-style-type: none"> <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> <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>
	<p><b>Filtrage URL et Filtrage de contenu</b></p> <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>
<b>1.2</b>	<p><b>PRESTATION DE SERVICE</b></p> <p>Le prestataire doit proposer dans son offre toutes les prestations nécessaires à la mise en œuvre de la solution de sécurité :</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>- Intégration de la solution dans le réseau de la CMC ;</li> <li>- L'interconnexion du NGFW avec les Switch Datacenter ;</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> </ul>



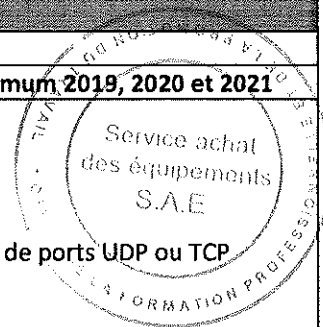
Item	Spécifications techniques
	<ul style="list-style-type: none"> <li>- La définition de la matrice des flux ;</li> <li>- Le prestataire doit réaliser tout essai jugé nécessaire pour s'assurer de la conformité et du bon fonctionnement de la plateforme de sécurité ;</li> <li>- Transfert de compétence ;</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 d'un an 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 ;</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

Item	Désignation	Unité	CMC TANGER
1	Solution de Firewall Nouvelle Génération NGFW de type Appliance		
1.1	Firewall	U	1
1.2	PRESTATION DE SERVICE	ens	1

**LOT 4 : Solution de Firewall Nouvelle Génération NGFW pour la CMC RABAT**

Item	Spécifications techniques
<b>1 .</b>	<b>Solution de Firewall Nouvelle Génération NGFW de type Appliance</b>
<b>1.1</b>	<b>Leader dans Gartner dans la technologie Network Firewall pour les trois années minimum 2019, 2020 et 2021</b>
	<p><b>Fonctions Firewall</b></p> <ul style="list-style-type: none"> <li>- Doit intégrer un système d'exploitation propriétaire sécurisé,</li> <li>- Filtrage de paquets et être doté de la fonction de filtrage dynamique,</li> <li>- Filtrage basé sur les applications niveau 7 en plus des ports/Protocol et par plages de ports UDP ou TCP</li> <li>- Filtrage et inspection en IPv4 et IPv6,</li> <li>- Failover de connexion Internet,</li> <li>- Prise en compte de paramètre Horaire dans les règles de filtrage,</li> <li>- Doit fournir, via sa console d'administration, des statistiques sur le nombre d'accès aux règles de sécurité,</li> <li>- Doit inclure la possibilité de fonctionner en mode transparent ou routé (natté),</li> <li>- 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,</li> <li>- La création de la politique de sécurité basée sur : <ul style="list-style-type: none"> <li>• Geolocation par pays</li> <li>• Zones</li> <li>• Groupes de Zones</li> <li>• Applications, Groupes d'applications</li> <li>• Catégories d'Applications</li> </ul> </li> </ul>

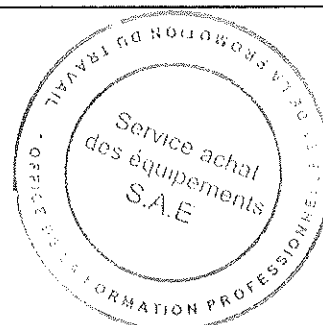


Item	Spécifications techniques
	<ul style="list-style-type: none"> <li>Technologies d'Applications</li> <li>Filtres d'Applications</li> <li>Utilisateurs et Groupes</li> <li>Adresses IP, Groupes d'adresses IP, Sous-réseaux IP, Groupes de sous-réseaux IP</li> <li>Services, Groupes de Services</li> </ul> <p>- 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) :</p> <ul style="list-style-type: none"> <li><b>IPS (prévention des intrusions)</b> 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 : <ul style="list-style-type: none"> <li>Détection par signatures ;</li> <li>Détection par anomalies ;</li> <li>Capable de faire des analyses comportementales de tout type de trafic ;</li> <li>Possibilité de créer des signatures personnalisées ;</li> <li>Mise à jour automatique des signatures IPS ;</li> <li>Création et affectation des politiques IPS par type de zone ou interface ;</li> <li>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) ... ;</li> <li>Gestion de profils IPS avec association à certains trafics dans la politique de filtrage (IP source, IP destination, service, protocole, réseau...) ;</li> </ul> </li> <li><b>Filtrage URL</b>, pour assurer le contrôle de l'accès interne aux contenus Web indésirables, non productifs, voire illégaux,</li> <li><b>Control Applicatif</b>, afin d'identifier, reconnaître et contrôler les applications dans les flux,</li> </ul>
	<p><b>Spécifications matérielles et performance :</b></p> <ul style="list-style-type: none"> <li>Format : Appliance Rackable, 19"</li> <li>Débit de Prévention des menaces (Firewall niveau 7 avec Contrôle applicatif + IPS + Anti Malware + Sandboxing+ Antispyware + filtrage URL, filtrage de contenu et Journalisation) : <b>2.5 Gbps Minimum</b></li> <li>Nombre de sessions inspectées simultanées : <b>1 Million Minimum</b></li> <li>Nombre de nouvelles sessions par seconde : <b>50 000 Minimum</b></li> <li>Stockage Disque dur dédiée de type SSD de <b>200 GB Minimum</b></li> <li>Les ports (en dehors des ports de management et de la haute disponibilité) <ul style="list-style-type: none"> <li>Minimum 8 ports 10/100/1000 BaseT</li> <li>Minimum 4 ports 1G/10G SFP/SFP+ dont 4 avec Transceiver SFP+</li> </ul> </li> <li>Les ports de management et Clustering : <ul style="list-style-type: none"> <li>Minimum 1 port 10/100/1000 BaseT pour le management</li> <li>Minimum 1 port console RJ-45</li> <li>Minimum 1 port USB</li> <li>Minimum 1 ports 10/100/1000 BaseT pour le HA</li> </ul> </li> <li>2 Alimentations électriques Redondantes Minimum (AC),</li> </ul>
	<p><b>Support de la haute disponibilité :</b></p> <ul style="list-style-type: none"> <li>Actif/Actif avec synchronisation d'état de session,</li> <li>Actif/Passif,</li> </ul>
	<p><b>Contrôle applicatif :</b></p> <ul style="list-style-type: none"> <li>Identification des applications en se basant sur :</li> </ul>



4  
H2

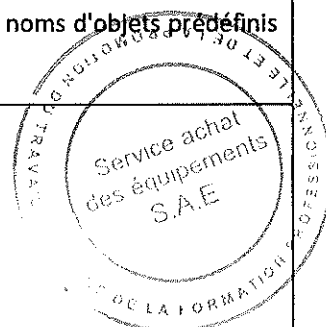
Item	Spécifications techniques
	<ul style="list-style-type: none"> <li>• Signatures</li> <li>• Décodage du protocole (respecte la spécification du protocole)</li> <li>• Déchiffrement du trafic encapsulé</li> <li>- Identification et contrôle des applications partageant la même connexion</li> <li>- Contrôle de la fonction de transfert de fichiers d'une application</li> <li>- Visibilité du trafic applicatif inconnu à travers l'identification de sa nature : <ul style="list-style-type: none"> <li>• Volume du trafic</li> <li>• Utilisateur et/ou adresses IP</li> <li>• Port utilisé</li> <li>• Contenu associé : fichier, menace ou autre.</li> </ul> </li> <li>- La base de données de contrôle des applications doit contenir plus de 3 000 applications connues ;</li> <li>- La solution doit pouvoir créer une règle de filtrage avec plusieurs catégories ;</li> </ul>
	<p><b>Identification, authentification des utilisateurs et protection des identités</b></p> <ul style="list-style-type: none"> <li>- Prise en charge des services d'authentification suivants pour l'identification et authentifications des utilisateurs : <ul style="list-style-type: none"> <li>• Active Directory</li> <li>• Kerberos</li> <li>• LDAP</li> <li>• Radius</li> <li>• Base Locale</li> <li>• SAML</li> <li>• Authentification via SSO Kerberos sans agent</li> <li>• Authentification par Certificat client</li> <li>• Portail captif</li> </ul> </li> <li>- Identification des utilisateurs indépendamment : <ul style="list-style-type: none"> <li>• Du terminal (ordinateur, un téléphone intelligent ou une tablette)</li> <li>• Du système d'exploitation utilisé,</li> <li>• Des adresses IP et de la zone (LAN, VPN, hors du périmètre du réseau)</li> </ul> </li> </ul>
	<p><b>Fonctions Réseau :</b></p> <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> <li>- Support de la fonctionnalité <b>SD-WAN</b> pour le routage avancé des flux sur plusieurs liaisons à base d'application afin d'augmenter la disponibilité et la performance WAN en se basant sur les paramètres de performance (Latence, Perte de packets et jitter) que ce soit lors de la navigation Internet et pour la communication inter-sites (<b>fonctionnalité et licence à fournir</b>)</li> </ul>
	<p><b>Fonction VPN :</b></p> <ul style="list-style-type: none"> <li>- VPN IPSec site-site, client-site et hub &amp; Spoke. (<b>Fonctionnalité et licence à fournir</b>)</li> <li>- Support du VPN SSL mode portail et mode tunnel (avec ou sans agent)</li> </ul>



5

112

Item	Spécifications techniques
	<ul style="list-style-type: none"> <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>
	<p><b>Gestion de la bande passante :</b></p> <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>
	<p><b>Administration et gestion des journaux :</b></p> <ul style="list-style-type: none"> <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> <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>
	<p><b>Filtrage URL et Filtrage de contenu</b></p> <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>
1.2	<p><b>PRESTATION DE SERVICE</b></p> <p>Le prestataire doit proposer dans son offre toutes les prestations nécessaires à la mise en œuvre de la solution de sécurité :</p> <ul style="list-style-type: none"> <li>- Ingénierie et définition de l'architecture finale ;</li> </ul>



Item	Spécifications techniques
	<ul style="list-style-type: none"> <li>- Analyse du plan d'adressage IP, de routage et de découpage VLAN ;</li> <li>- Intégration de la solution dans le réseau de la CMC ;</li> <li>- L'interconnexion du NGFW avec les Switch Datacenter ;</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 (couvrir l'assistance (sur site ou à distance), l'intervention sur site, les pièces de rechanges et la main d'œuvre) pour une durée d'un an 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 ;</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**

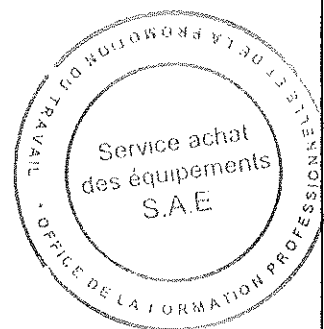
Item	Désignation	Unité	CMC RABAT
1	Solution de Firewall Nouvelle Génération NGFW de type Appliance		
1.1	Firewall	U	Service achat
1.2	PRESTATION DE SERVICE	ens	des équipements S.A.E

**LOT 5 : Solution de Firewall Nouvelle Génération NGFW pour la CMC BENI MELLAL**

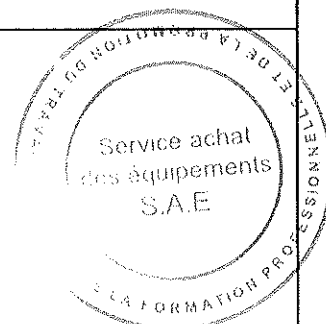
Item	Spécifications techniques
<b>1 .</b>	<b>Solution de Firewall Nouvelle Génération NGFW de type Appliance</b>
<b>1.1</b>	<b>Leader dans Gartner dans la technologie Network Firewall pour les trois années minimum 2019, 2020 et 2021</b>
	<p><b>Fonctions Firewall</b></p> <ul style="list-style-type: none"> <li>- Doit intégrer un système d'exploitation propriétaire sécurisé,</li> <li>- Filtrage de paquets et être doté de la fonction de filtrage dynamique,</li> <li>- Filtrage basé sur les applications niveau 7 en plus des ports/Protocol et par plages de ports UDP ou TCP</li> <li>- Filtrage et inspection en IPv4 et IPv6,</li> <li>- Failover de connexion Internet,</li> <li>- Prise en compte de paramètre Horaire dans les règles de filtrage,</li> <li>- Doit fournir, via sa console d'administration, des statistiques sur le nombre d'accès aux règles de sécurité,</li> <li>- Doit inclure la possibilité de fonctionner en mode transparent ou routé (natté),</li> <li>- 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,</li> <li>- La création de la politique de sécurité basée sur : <ul style="list-style-type: none"> <li>• Geolocation par pays</li> </ul> </li> </ul>



Item	Spécifications techniques
	<ul style="list-style-type: none"> <li>• Zones</li> <li>• Groupes de Zones</li> <li>• Applications, Groupes d'applications</li> <li>• Catégories d'Applications</li> <li>• Technologies d'Applications</li> <li>• Filtres d'Applications</li> <li>• Utilisateurs et Groupes</li> <li>• Adresses IP, Groupes d'adresses IP, Sous-réseaux IP, Groupes de sous-réseaux IP</li> <li>• Services, Groupes de Services</li> </ul> <p>- La solution doit être de type Next Generation Firewall avec capacité de prévention contre les menaces avancées, combinée avec des fonctionnalités de base suivantes (<b>licences incluses</b>) :</p> <ul style="list-style-type: none"> <li>• <b>IPS (prévention des intrusions)</b> 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 : <ul style="list-style-type: none"> <li>- Détection par signatures ;</li> <li>- Détection par anomalies ;</li> <li>- Capable de faire des analyses comportementales de tout type de trafic ;</li> <li>- Possibilité de créer des signatures personnalisées ;</li> <li>- Mise à jour automatique des signatures IPS ;</li> <li>- Création et affectation des politiques IPS par type de zone ou interface ;</li> <li>- 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) ... ;</li> <li>- Gestion de profils IPS avec association à certains trafics dans la politique de filtrage (IP source, IP destination, service, protocole, réseau...) ;</li> </ul> </li> <li>• <b>Filtrage URL</b>, pour assurer le contrôle de l'accès interne aux contenus Web indésirables, non productifs, voire illégaux,</li> <li>• <b>Control Applicatif</b>, afin d'identifier, reconnaître et contrôler les applications dans les flux,</li> </ul>
	<p><b>Spécifications matérielles et performance :</b></p> <ul style="list-style-type: none"> <li>- Format : Appliance Rackable, 19"</li> <li>- Débit de Prevention des menaces (Firewall niveau 7 avec Contrôle applicatif + IPS + Anti Malware + Sandboxing+ Antispyware + filtrage URL, filtrage de contenu et Journalisation) : <b>2.5 Gbps Minimum</b></li> <li>- Nombre de sessions inspectées simultanées : <b>1 Million Minimum</b></li> <li>- Nombre de nouvelles sessions par seconde : <b>50 000 Minimum</b></li> <li>- Stockage Disque dur dédiée de type SSD de <b>200 GB Minimum</b></li> <li>- Les ports (en dehors des ports de management et de la haute disponibilité) <ul style="list-style-type: none"> <li>• Minimum 8 ports 10/100/1000 BaseT</li> <li>• Minimum 4 ports 1G/10G SFP/SFP+ dont 4 avec Transceiver SFP+</li> </ul> </li> <li>- Les ports de management et Clustering : <ul style="list-style-type: none"> <li>• Minimum 1 port 10/100/1000 BaseT pour le management</li> <li>• Minimum 1 port console RJ-45</li> <li>• Minimum 1 port USB</li> <li>• Minimum 1 ports 10/100/1000 BaseT pour le HA</li> </ul> </li> <li>- 2 Alimentations électriques Redondantes Minimum (AC),</li> </ul>
	<p><b>Support de la haute disponibilité :</b></p> <ul style="list-style-type: none"> <li>- Actif/Actif avec synchronisation d'état de session,</li> </ul>

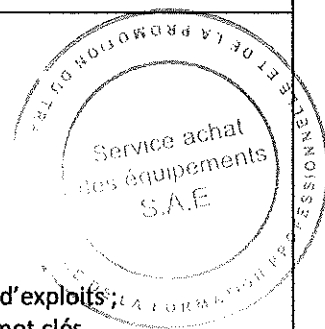


Item	Spécifications techniques
	<ul style="list-style-type: none"> <li>- Actif/Passif,</li> </ul>
	<p><b>Contrôle applicatif :</b></p> <ul style="list-style-type: none"> <li>- Identification des applications en se basant sur : <ul style="list-style-type: none"> <li>• Signatures</li> <li>• Décodage du protocole (respecte la spécification du protocole)</li> <li>• Déchiffrement du trafic encapsulé</li> </ul> </li> <li>- Identification et contrôle des applications partageant la même connexion</li> <li>- Contrôle de la fonction de transfert de fichiers d'une application</li> <li>- Visibilité du trafic applicatif inconnu à travers l'identification de sa nature : <ul style="list-style-type: none"> <li>• Volume du trafic</li> <li>• Utilisateur et/ou adresses IP</li> <li>• Port utilisé</li> <li>• Contenu associé : fichier, menace ou autre.</li> </ul> </li> <li>- La base de données de contrôle des applications doit contenir plus de 3 000 applications connues ;</li> <li>- La solution doit pouvoir créer une règle de filtrage avec plusieurs catégories ;</li> </ul>
	<p><b>Identification, authentification des utilisateurs et protection des identités</b></p> <ul style="list-style-type: none"> <li>- Prise en charge des services d'authentification suivants pour l'identification et authentifications des utilisateurs : <ul style="list-style-type: none"> <li>• Active Directory</li> <li>• Kerberos</li> <li>• LDAP</li> <li>• Radius</li> <li>• Base Locale</li> <li>• SAML</li> <li>• Authentification via SSO Kerberos sans agent</li> <li>• Authentification par Certificat client</li> <li>• Portail captif</li> </ul> </li> <li>- Identification des utilisateurs indépendamment : <ul style="list-style-type: none"> <li>• Du terminal (ordinateur, un téléphone intelligent ou une tablette)</li> <li>• Du système d'exploitation utilisé,</li> <li>• Des adresses IP et de la zone (LAN, VPN, hors du périmètre du réseau)</li> </ul> </li> </ul>
	<p><b>Fonctions Réseau :</b></p> <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> <li>- Support de la fonctionnalité <b>SD-WAN</b> pour le routage avancé des flux sur plusieurs liaisons à base d'application afin d'augmenter la disponibilité et la performance WAN en se basant sur les paramètres de performance (Latence, Perte de packets et jitter) que ce soit lors de la navigation Internet et pour la communication inter-sites (<b>fonctionnalité et licence à fournir</b>)</li> </ul>



5  
H2

Item	Spécifications techniques
	<p><b>Fonction VPN :</b></p> <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>
	<p><b>Gestion de la bande passante :</b></p> <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>
	<p><b>Administration et gestion des journaux :</b></p> <ul style="list-style-type: none"> <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> <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>
	<p><b>Filtrage URL et Filtrage de contenu</b></p> <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>
1.2	PRESTATION DE SERVICE



Handwritten marks: a checkmark and the signature 'H2'.

Item	Spécifications techniques
	<p>Le prestataire doit proposer dans son offre toutes les prestations nécessaires à la mise en œuvre de la solution de sécurité :</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>- Intégration de la solution dans le réseau de la CMC ;</li> <li>- L'interconnexion du NGFW avec les Switch Datacenter ;</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 d'un an 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 ;</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>

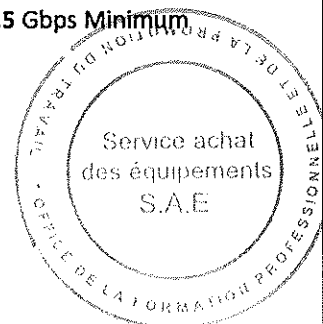
Tableau de répartition

Item	Désignation	Unité	CMC BENI MELLAL A.E
1	Solution de Firewall Nouvelle Génération NGFW de type Appliance		
1.1	Firewall	U	1
1.2	PRESTATION DE SERVICE	ens	1

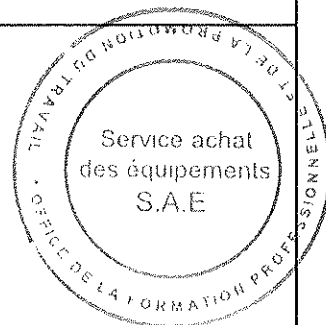
**LOT 6 : Solution de Firewall Nouvelle Génération NGFW pour la CMC MARRAKECH**

Item	Spécifications techniques
1 .	<b>Solution de Firewall Nouvelle Génération NGFW de type Appliance</b>
1.1	<b>Leader dans Gartner dans la technologie Network Firewall pour les trois années minimum 2019, 2020 et 2021</b>
	<p><b>Fonctions Firewall</b></p> <ul style="list-style-type: none"> <li>- Doit intégrer un système d'exploitation propriétaire sécurisé,</li> <li>- Filtrage de paquets et être doté de la fonction de filtrage dynamique,</li> <li>- Filtrage basé sur les applications niveau 7 en plus des ports/Protocol et par plages de ports UDP ou TCP</li> <li>- Filtrage et inspection en IPv4 et IPv6,</li> <li>- Failover de connexion Internet,</li> <li>- Prise en compte de paramètre Horaire dans les règles de filtrage,</li> <li>- Doit fournir, via sa console d'administration, des statistiques sur le nombre d'accès aux règles de sécurité,</li> <li>- Doit inclure la possibilité de fonctionner en mode transparent ou routé (natté),</li> </ul>

Item	Spécifications techniques
	<ul style="list-style-type: none"> <li>- 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,</li> <li>- La création de la politique de sécurité basée sur : <ul style="list-style-type: none"> <li>• Geolocation par pays</li> <li>• Zones</li> <li>• Groupes de Zones</li> <li>• Applications, Groupes d'applications</li> <li>• Catégories d'Applications</li> <li>• Technologies d'Applications</li> <li>• Filtres d'Applications</li> <li>• Utilisateurs et Groupes</li> <li>• Adresses IP, Groupes d'adresses IP, Sous-réseaux IP, Groupes de sous-réseaux IP</li> <li>• Services, Groupes de Services</li> </ul> </li> <li>- La solution doit être de type Next Generation Firewall avec capacité de prévention contre les menaces avancées, combinée avec des fonctionnalités de base suivantes (<b>licences incluses</b>) : <ul style="list-style-type: none"> <li>• <b>IPS (prévention des intrusions)</b> 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 : <ul style="list-style-type: none"> <li>- Détection par signatures ;</li> <li>- Détection par anomalies ;</li> <li>- Capable de faire des analyses comportementales de tout type de trafic ;</li> <li>- Possibilité de créer des signatures personnalisées ;</li> <li>- Mise à jour automatique des signatures IPS ;</li> <li>- Création et affectation des politiques IPS par type de zone ou interface ;</li> <li>- 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) ... ;</li> <li>- Gestion de profils IPS avec association à certains trafics dans la politique de filtrage (IP source, IP destination, service, protocole, réseau...) ;</li> </ul> </li> <li>• <b>Filtrage URL</b>, pour assurer le contrôle de l'accès interne aux contenus Web indésirables, non productifs, voire illégaux,</li> <li>• <b>Control Applicatif</b>, afin d'identifier, reconnaître et contrôler les applications dans les flux,</li> </ul> </li> </ul>
	<p><b>Spécifications matérielles et performance :</b></p> <ul style="list-style-type: none"> <li>- Format : Appliance Rackable, 19"</li> <li>- Débit de Prévention des menaces (Firewall niveau 7 avec Contrôle applicatif + IPS + Anti Malware + Sandboxing+ Antispyware + filtrage URL, filtrage de contenu et Journalisation) : <b>2.5 Gbps Minimum</b></li> <li>- Nombre de sessions inspectées simultanées : <b>1 Million Minimum</b></li> <li>- Nombre de nouvelles sessions par seconde : <b>50 000 Minimum</b></li> <li>- Stockage Disque dur dédiée de type SSD de <b>200 GB Minimum</b></li> <li>- Les ports (en dehors des ports de management et de la haute disponibilité) <ul style="list-style-type: none"> <li>• Minimum 8 ports 10/100/1000 BaseT</li> <li>• Minimum 4 ports 1G/10G SFP/SFP+ dont <b>4 avec Transceiver SFP+</b></li> </ul> </li> <li>- Les ports de management et Clustering : <ul style="list-style-type: none"> <li>• Minimum 1 port 10/100/1000 BaseT pour le management</li> <li>• Minimum 1 port console RJ-45</li> <li>• Minimum 1 port USB</li> <li>• Minimum 1 ports 10/100/1000 BaseT pour le HA</li> </ul> </li> </ul>

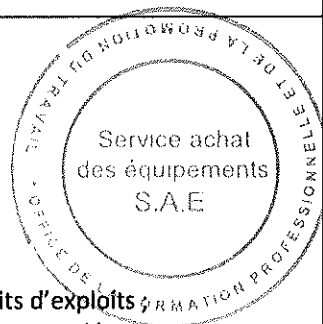


Item	Spécifications techniques
	<ul style="list-style-type: none"> <li>- 2 Alimentations électriques Redondantes Minimum (AC),</li> </ul>
	<p><b>Support de la haute disponibilité :</b></p> <ul style="list-style-type: none"> <li>- Actif/Actif avec synchronisation d'état de session,</li> <li>- Actif/Passif,</li> </ul>
	<p><b>Contrôle applicatif :</b></p> <ul style="list-style-type: none"> <li>- Identification des applications en se basant sur : <ul style="list-style-type: none"> <li>• Signatures</li> <li>• Décodage du protocole (respecte la spécification du protocole)</li> <li>• Déchiffrement du trafic encapsulé</li> </ul> </li> <li>- Identification et contrôle des applications partageant la même connexion</li> <li>- Contrôle de la fonction de transfert de fichiers d'une application</li> <li>- Visibilité du trafic applicatif inconnu à travers l'identification de sa nature : <ul style="list-style-type: none"> <li>• Volume du trafic</li> <li>• Utilisateur et/ou adresses IP</li> <li>• Port utilisé</li> <li>• Contenu associé : fichier, menace ou autre.</li> </ul> </li> <li>- La base de données de contrôle des applications doit contenir plus de 3 000 applications connues ;</li> <li>- La solution doit pouvoir créer une règle de filtrage avec plusieurs catégories ;</li> </ul>
	<p><b>Identification, authentification des utilisateurs et protection des identités</b></p> <ul style="list-style-type: none"> <li>- Prise en charge des services d'authentification suivants pour l'identification et authentifications des utilisateurs : <ul style="list-style-type: none"> <li>• Active Directory</li> <li>• Kerberos</li> <li>• LDAP</li> <li>• Radius</li> <li>• Base Locale</li> <li>• SAML</li> <li>• Authentification via SSO Kerberos sans agent</li> <li>• Authentification par Certificat client</li> <li>• Portail captif</li> </ul> </li> <li>- Identification des utilisateurs indépendamment : <ul style="list-style-type: none"> <li>• Du terminal (ordinateur, un téléphone intelligent ou une tablette)</li> <li>• Du système d'exploitation utilisé,</li> <li>• Des adresses IP et de la zone (LAN, VPN, hors du périmètre du réseau)</li> </ul> </li> </ul>
	<p><b>Fonctions Réseau :</b></p> <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>



7  
A2

Item	Spécifications techniques
	<ul style="list-style-type: none"> <li>- Support de la fonctionnalité SD-WAN pour le routage avancé des flux sur plusieurs liaisons à base d'application afin d'augmenter la disponibilité et la performance WAN en se basant sur les paramètres de performance (Latence, Perte de packets et jitter) que ce soit lors de la navigation Internet et pour la communication inter-sites (fonctionnalité et licence à fournir)</li> </ul>
	<p><b>Fonction VPN :</b></p> <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>
	<p><b>Gestion de la bande passante :</b></p> <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>
	<p><b>Administration et gestion des journaux :</b></p> <ul style="list-style-type: none"> <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> <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>
	<p><b>Filtrage URL et Filtrage de contenu</b></p> <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>



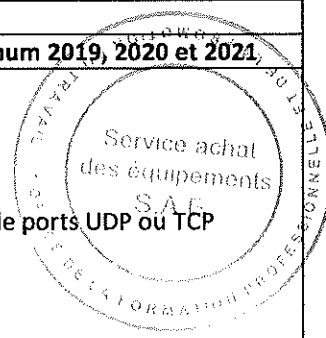
Item	Spécifications techniques
1.2	<p><b>PRESTATION DE SERVICE</b></p> <p>Le prestataire doit proposer dans son offre toutes les prestations nécessaires à la mise en œuvre de la solution de sécurité :</p> <ul style="list-style-type: none"> <li>- Ingénierie et définition de l'architecture finale ;</li> <li>- Analyse du plan d'adressage IP, de routage et de découpage VLAN ;</li> <li>- Intégration de la solution dans le réseau de la CMC ;</li> <li>- L'interconnexion du NGFW avec les Switch Datacenter ;</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 d'un an 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 ;</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

Item	Désignation	Unité	CMC MARRAKECH
1	Solution de Firewall Nouvelle Génération NGFW de type Appliance		
1.1	Firewall	U	1
1.2	PRESTATION DE SERVICE	ens	1

**LOT 7 : Solution de Firewall Nouvelle Génération NGFW pour la CMC CASABLANCA**

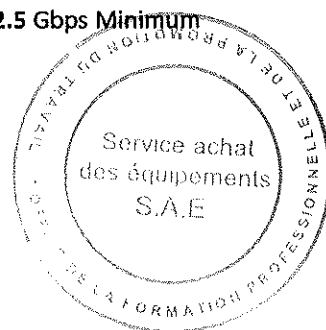
Item	Spécifications techniques
1 .	<b>Solution de Firewall Nouvelle Génération NGFW de type Appliance</b>
1.1	<b>Leader dans Gartner dans la technologie Network Firewall pour les trois années minimum 2019, 2020 et 2021.</b>
	<p><b>Fonctions Firewall</b></p> <ul style="list-style-type: none"> <li>- Doit intégrer un système d'exploitation propriétaire sécurisé,</li> <li>- Filtrage de paquets et être doté de la fonction de filtrage dynamique,</li> <li>- Filtrage basé sur les applications niveau 7 en plus des ports/Protocol et par plages de ports UDP ou TCP</li> <li>- Filtrage et inspection en IPv4 et IPv6,</li> <li>- Failover de connexion Internet,</li> <li>- Prise en compte de paramètre Horaire dans les règles de filtrage,</li> <li>- Doit fournir, via sa console d'administration, des statistiques sur le nombre d'accès aux règles de sécurité,</li> </ul>



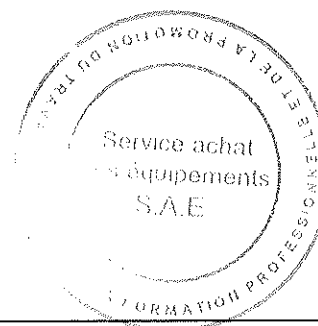
✓  
A\*



Item	Spécifications techniques
	<ul style="list-style-type: none"> <li>- Doit inclure la possibilité de fonctionner en mode transparent ou routé (natté),</li> <li>- 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,</li> <li>- La création de la politique de sécurité basée sur : <ul style="list-style-type: none"> <li>• Geolocation par pays</li> <li>• Zones</li> <li>• Groupes de Zones</li> <li>• Applications, Groupes d'applications</li> <li>• Catégories d'Applications</li> <li>• Technologies d'Applications</li> <li>• Filtres d'Applications</li> <li>• Utilisateurs et Groupes</li> <li>• Adresses IP, Groupes d'adresses IP, Sous-réseaux IP, Groupes de sous-réseaux IP</li> <li>• Services, Groupes de Services</li> </ul> </li> <li>- 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) : <ul style="list-style-type: none"> <li>• <b>IPS (prévention des intrusions)</b> 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 : <ul style="list-style-type: none"> <li>- Détection par signatures ;</li> <li>- Détection par anomalies ;</li> <li>- Capable de faire des analyses comportementales de tout type de trafic ;</li> <li>- Possibilité de créer des signatures personnalisées ;</li> <li>- Mise à jour automatique des signatures IPS ;</li> <li>- Création et affectation des politiques IPS par type de zone ou interface ;</li> <li>- 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) ... ;</li> <li>- Gestion de profils IPS avec association à certains trafics dans la politique de filtrage (IP source, IP destination, service, protocole, réseau...) ;</li> </ul> </li> <li>• <b>Filtrage URL</b>, pour assurer le contrôle de l'accès interne aux contenus Web indésirables, non productifs, voire illégaux,</li> <li>• <b>Control Applicatif</b>, afin d'identifier, reconnaître et contrôler les applications dans les flux,</li> </ul> </li> </ul>
	<p><b>Spécifications matérielles et performance :</b></p> <ul style="list-style-type: none"> <li>- Format : Appliance Rackable, 19"</li> <li>- Débit de Prévention des menaces (Firewall niveau 7 avec Contrôle applicatif + IPS + Anti Malware + Sandboxing+ Antispyware + filtrage URL, filtrage de contenu et Journalisation) : <b>2.5 Gbps Minimum</b></li> <li>- Nombre de sessions inspectées simultanées : <b>1 Million Minimum</b></li> <li>- Nombre de nouvelles sessions par seconde : <b>50 000 Minimum</b></li> <li>- Stockage Disque dur dédiée de type SSD de <b>200 GB Minimum</b></li> <li>- Les ports (en dehors des ports de management et de la haute disponibilité) <ul style="list-style-type: none"> <li>• Minimum 8 ports 10/100/1000 BaseT</li> <li>• Minimum 4 ports 1G/10G SFP/SFP+ dont 4 avec Transceiver SFP+</li> </ul> </li> <li>- Les ports de management et Clustering : <ul style="list-style-type: none"> <li>• Minimum 1 port 10/100/1000 BaseT pour le management</li> <li>• Minimum 1 port console RJ-45</li> </ul> </li> </ul>

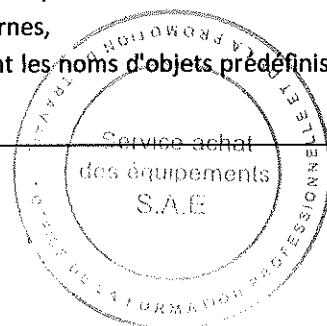


Item	Spécifications techniques
	<ul style="list-style-type: none"> <li>• Minimum 1 port USB</li> <li>• Minimum 1 ports 10/100/1000 BaseT pour le HA</li> <li>- 2 Alimentations électriques Redondantes Minimum (AC),</li> </ul>
	<b>Support de la haute disponibilité :</b> <ul style="list-style-type: none"> <li>- Actif/Actif avec synchronisation d'état de session,</li> <li>- Actif/Passif,</li> </ul>
	<b>Contrôle applicatif :</b> <ul style="list-style-type: none"> <li>- Identification des applications en se basant sur : <ul style="list-style-type: none"> <li>• Signatures</li> <li>• Décodage du protocole (respecte la spécification du protocole)</li> <li>• Déchiffrement du trafic encapsulé</li> </ul> </li> <li>- Identification et contrôle des applications partageant la même connexion</li> <li>- Contrôle de la fonction de transfert de fichiers d'une application</li> <li>- Visibilité du trafic applicatif inconnu à travers l'identification de sa nature : <ul style="list-style-type: none"> <li>• Volume du trafic</li> <li>• Utilisateur et/ou adresses IP</li> <li>• Port utilisé</li> <li>• Contenu associé : fichier, menace ou autre.</li> </ul> </li> <li>- La base de données de contrôle des applications doit contenir plus de 3 000 applications connues ;</li> <li>- La solution doit pouvoir créer une règle de filtrage avec plusieurs catégories ;</li> </ul>
	<b>Identification, authentification des utilisateurs et protection des identités</b> <ul style="list-style-type: none"> <li>- Prise en charge des services d'authentification suivants pour l'identification et authentifications des utilisateurs : <ul style="list-style-type: none"> <li>• Active Directory</li> <li>• Kerberos</li> <li>• LDAP</li> <li>• Radius</li> <li>• Base Locale</li> <li>• SAML</li> <li>• Authentification via SSO Kerberos sans agent</li> <li>• Authentification par Certificat client</li> <li>• Portail captif</li> </ul> </li> <li>- Identification des utilisateurs indépendamment : <ul style="list-style-type: none"> <li>• Du terminal (ordinateur, un téléphone intelligent ou une tablette)</li> <li>• Du système d'exploitation utilisé,</li> <li>• Des adresses IP et de la zone (LAN, VPN, hors du périmètre du réseau)</li> </ul> </li> </ul>
	<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> </ul>



5  
A0

Item	Spécifications techniques
	<ul style="list-style-type: none"> <li>- Nat dynamique, Nat Statique, Nat par port, Nat64</li> <li>- Support de Multicast</li> <li>- Support de la fonctionnalité SD-WAN pour le routage avancé des flux sur plusieurs liaisons à base d'application afin d'augmenter la disponibilité et la performance WAN en se basant sur les paramètres de performance (Latence, Perte de packets et jitter) que ce soit lors de la navigation Internet et pour la communication inter-sites (<b>fonctionnalité et licence à fournir</b>)</li> </ul>
	<p><b>Fonction VPN :</b></p> <ul style="list-style-type: none"> <li>- VPN IPSec site-site, client-site et hub &amp; Spoke. (<b>Fonctionnalité et licence à fournir</b>)</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>
	<p><b>Gestion de la bande passante :</b></p> <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>
	<p><b>Administration et gestion des journaux :</b></p> <ul style="list-style-type: none"> <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> <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 <b>nom d'objets prédéfinis</b> (hôtes, réseau, groupes, utilisateurs...),</li> </ul>
	<p><b>Filtrage URL et Filtrage de contenu</b></p> <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> </ul>



Item	Spécifications techniques
	<ul style="list-style-type: none"> <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>
1.2	<p><b>PRESTATION DE SERVICE</b></p> <p>Le prestataire doit proposer dans son offre toutes les prestations nécessaires à la mise en œuvre de la solution de sécurité :</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>- Intégration de la solution dans le réseau de la CMC ;</li> <li>- L'interconnexion du NGFW avec les Switch Datacenter ;</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 d'un an 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 ;</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

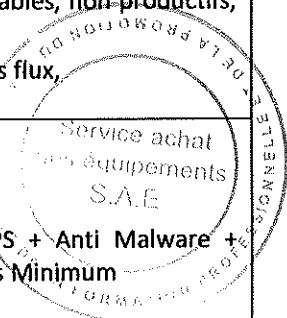
Item	Désignation	Unité	CMC CASABLANCA
1	Solution de Firewall Nouvelle Génération NGFW de type Appliance		
1.1	Firewall	U	1
1.2	PRESTATION DE SERVICE	ens	1

**LOT 8 : Solution de Firewall Nouvelle Génération NGFW pour la CMC FES**

Item	Spécifications techniques
1.	Solution de Firewall Nouvelle Génération NGFW de type Appliance
1.1	Leader dans Gartner dans la technologie Network Firewall pour les trois années minimum 2019, 2020 et 2021
	<p>Fonctions Firewall</p> <ul style="list-style-type: none"> <li>- Doit intégrer un système d'exploitation propriétaire sécurisé,</li> </ul>

✓  
A2

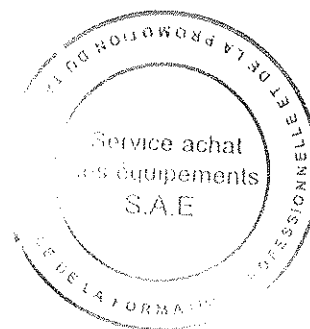
Item	Spécifications techniques
	<ul style="list-style-type: none"> <li>- Filtrage de paquets et être doté de la fonction de filtrage dynamique,</li> <li>- Filtrage basé sur les applications niveau 7 en plus des ports/Protocol et par plages de ports UDP ou TCP</li> <li>- Filtrage et inspection en IPv4 et IPv6,</li> <li>- Failover de connexion Internet,</li> <li>- Prise en compte de paramètre Horaire dans les règles de filtrage,</li> <li>- Doit fournir, via sa console d'administration, des statistiques sur le nombre d'accès aux règles de sécurité,</li> <li>- Doit inclure la possibilité de fonctionner en mode transparent ou routé (natté),</li> <li>- 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,</li> <li>- La création de la politique de sécurité basée sur : <ul style="list-style-type: none"> <li>• Geolocation par pays</li> <li>• Zones</li> <li>• Groupes de Zones</li> <li>• Applications, Groupes d'applications</li> <li>• Catégories d'Applications</li> <li>• Technologies d'Applications</li> <li>• Filtres d'Applications</li> <li>• Utilisateurs et Groupes</li> <li>• Adresses IP, Groupes d'adresses IP, Sous-réseaux IP, Groupes de sous-réseaux IP</li> <li>• Services, Groupes de Services</li> </ul> </li> <li>- 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) : <ul style="list-style-type: none"> <li>• <b>IPS (prévention des intrusions)</b> 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 : <ul style="list-style-type: none"> <li>- Détection par signatures ;</li> <li>- Détection par anomalies ;</li> <li>- Capable de faire des analyses comportementales de tout type de trafic ;</li> <li>- Possibilité de créer des signatures personnalisées ;</li> <li>- Mise à jour automatique des signatures IPS ;</li> <li>- Création et affectation des politiques IPS par type de zone ou interface ;</li> <li>- 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) ... ;</li> <li>- Gestion de profils IPS avec association à certains trafics dans la politique de filtrage (IP source, IP destination, service, protocole, réseau...) ;</li> </ul> </li> <li>• <b>Filtrage URL</b>, pour assurer le contrôle de l'accès interne aux contenus Web indésirables, non-productifs, voire illégaux,</li> <li>• <b>Control Applicatif</b>, afin d'identifier, reconnaître et contrôler les applications dans les flux,</li> </ul> </li> </ul>
	<p><b>Spécifications matérielles et performance :</b></p> <ul style="list-style-type: none"> <li>- Format : Appliance Rackable, 19"</li> <li>- Débit de Prevention des menaces (Firewall niveau 7 avec Contrôle applicatif + IPS + Anti Malware + Sandboxing+ Antispyware + filtrage URL, filtrage de contenu et Journalisation) : <b>2.5 Gbps Minimum</b></li> <li>- Nombre de sessions inspectées simultanées : <b>1 Million Minimum</b></li> <li>- Nombre de nouvelles sessions par seconde : <b>50 000 Minimum</b></li> <li>- Stockage Disque dur dédiée de type SSD de <b>200 GB Minimum</b></li> </ul>



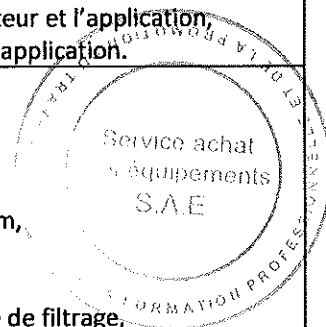
5

1/2

Item	Spécifications techniques
	<ul style="list-style-type: none"> <li>- Les ports (en dehors des ports de management et de la haute disponibilité) <ul style="list-style-type: none"> <li>• Minimum 8 ports 10/100/1000 BaseT</li> <li>• Minimum 4 ports 1G/10G SFP/SFP+ dont 4 avec Transceiver SFP+</li> </ul> </li> <li>- Les ports de management et Clustering : <ul style="list-style-type: none"> <li>• Minimum 1 port 10/100/1000 BaseT pour le management</li> <li>• Minimum 1 port console RJ-45</li> <li>• Minimum 1 port USB</li> <li>• Minimum 1 ports 10/100/1000 BaseT pour le HA</li> </ul> </li> <li>- 2 Alimentations électriques Redondantes Minimum (AC),</li> </ul>
	<p><b>Support de la haute disponibilité :</b></p> <ul style="list-style-type: none"> <li>- Actif/Actif avec synchronisation d'état de session,</li> <li>- Actif/Passif,</li> </ul>
	<p><b>Contrôle applicatif :</b></p> <ul style="list-style-type: none"> <li>- Identification des applications en se basant sur : <ul style="list-style-type: none"> <li>• Signatures</li> <li>• Décodage du protocole (respecte la spécification du protocole)</li> <li>• Déchiffrement du trafic encapsulé</li> </ul> </li> <li>- Identification et contrôle des applications partageant la même connexion</li> <li>- Contrôle de la fonction de transfert de fichiers d'une application</li> <li>- Visibilité du trafic applicatif inconnu à travers l'identification de sa nature : <ul style="list-style-type: none"> <li>• Volume du trafic</li> <li>• Utilisateur et/ou adresses IP</li> <li>• Port utilisé</li> <li>• Contenu associé : fichier, menace ou autre.</li> </ul> </li> <li>- La base de données de contrôle des applications doit contenir plus de 3 000 applications connues ;</li> <li>- La solution doit pouvoir créer une règle de filtrage avec plusieurs catégories ;</li> </ul>
	<p><b>Identification, authentification des utilisateurs et protection des identités</b></p> <ul style="list-style-type: none"> <li>- Prise en charge des services d'authentification suivants pour l'identification et authentifications des utilisateurs : <ul style="list-style-type: none"> <li>• Active Directory</li> <li>• Kerberos</li> <li>• LDAP</li> <li>• Radius</li> <li>• Base Locale</li> <li>• SAML</li> <li>• Authentification via SSO Kerberos sans agent</li> <li>• Authentification par Certificat client</li> <li>• Portail captif</li> </ul> </li> <li>- Identification des utilisateurs indépendamment : <ul style="list-style-type: none"> <li>• Du terminal (ordinateur, un téléphone intelligent ou une tablette)</li> <li>• Du système d'exploitation utilisé,</li> <li>• Des adresses IP et de la zone (LAN, VPN, hors du périmètre du réseau)</li> </ul> </li> </ul>
	<p><b>Fonctions Réseau :</b></p>



Item	Spécifications techniques
	<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> <li>- Support de la fonctionnalité <b>SD-WAN</b> pour le routage avancé des flux sur plusieurs liaisons à base d'application afin d'augmenter la disponibilité et la performance WAN en se basant sur les paramètres de performance (Latence, Perte de packets et jitter) que ce soit lors de la navigation Internet et pour la communication inter-sites (<b>fonctionnalité et licence à fournir</b>)</li> </ul>
	<p><b>Fonction VPN :</b></p> <ul style="list-style-type: none"> <li>- VPN IPsec site-site, client-site et hub &amp; Spoke. (<b>Fonctionnalité et licence à fournir</b>)</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>
	<p><b>Gestion de la bande passante :</b></p> <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>
	<p><b>Administration et gestion des journaux :</b></p> <ul style="list-style-type: none"> <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> <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>



Item	Spécifications techniques
	<p><b>Filtrage URL et Filtrage de contenu</b></p> <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>
1.2	<p><b>PRESTATION DE SERVICE</b></p> <p>Le prestataire doit proposer dans son offre toutes les prestations nécessaires à la mise en œuvre de la solution de sécurité :</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>- Intégration de la solution dans le réseau de la CMC ;</li> <li>- L'interconnexion du NGFW avec les Switch Datacenter ;</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 d'un an avec un délai de prise en charge de <b>2 heures</b> après déclaration de l'incident et un délai de <b>4 heures</b> de résolution ou de contournement du problème ;</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>

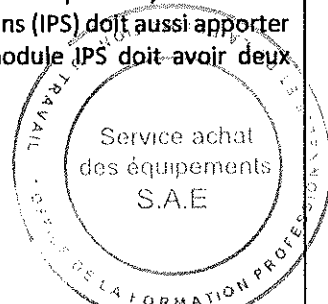
Tableau de répartition

Item	Désignation	Unité	CMC FES
1	Solution de Firewall Nouvelle Génération NGFW de type Appliance		
1.1	Firewall	U	1
1.2	PRESTATION DE SERVICE	ens	1

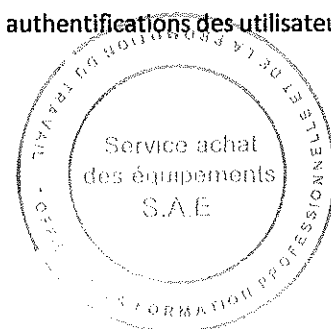


LOT 9 : Solution de Firewall Nouvelle Génération NGFW pour la CMC ERRACHIDIA

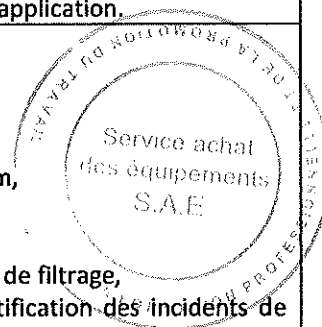
Item	Spécifications techniques
1 .	<b>Solution de Firewall Nouvelle Génération NGFW de type Appliance</b>
1.1	<b>Leader dans Gartner dans la technologie Network Firewall pour les trois années minimum 2019, 2020 et 2021</b>
	<p><b>Fonctions Firewall</b></p> <ul style="list-style-type: none"> <li>- Doit intégrer un système d'exploitation propriétaire sécurisé,</li> <li>- Filtrage de paquets et être doté de la fonction de filtrage dynamique,</li> <li>- Filtrage basé sur les applications niveau 7 en plus des ports/Protocol et par plages de ports UDP ou TCP</li> <li>- Filtrage et inspection en IPv4 et IPv6,</li> <li>- Failover de connexion Internet,</li> <li>- Prise en compte de paramètre Horaire dans les règles de filtrage,</li> <li>- Doit fournir, via sa console d'administration, des statistiques sur le nombre d'accès aux règles de sécurité,</li> <li>- Doit inclure la possibilité de fonctionner en mode transparent ou routé (natté),</li> <li>- 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,</li> <li>- La création de la politique de sécurité basée sur : <ul style="list-style-type: none"> <li>• Geolocation par pays</li> <li>• Zones</li> <li>• Groupes de Zones</li> <li>• Applications, Groupes d'applications</li> <li>• Catégories d'Applications</li> <li>• Technologies d'Applications</li> <li>• Filtres d'Applications</li> <li>• Utilisateurs et Groupes</li> <li>• Adresses IP, Groupes d'adresses IP, Sous-réseaux IP, Groupes de sous-réseaux IP</li> <li>• Services, Groupes de Services</li> </ul> </li> <li>- 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) : <ul style="list-style-type: none"> <li>• <b>IPS (prévention des intrusions)</b> 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 : <ul style="list-style-type: none"> <li>- Détection par signatures ;</li> <li>- Détection par anomalies ;</li> <li>- Capable de faire des analyses comportementales de tout type de trafic ;</li> <li>- Possibilité de créer des signatures personnalisées ;</li> <li>- Mise à jour automatique des signatures IPS ;</li> <li>- Création et affectation des politiques IPS par type de zone ou interface ;</li> <li>- 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) ... ;</li> <li>- Gestion de profils IPS avec association à certains trafics dans la politique de filtrage (IP source, IP destination, service, protocole, réseau...) ;</li> </ul> </li> <li>• <b>Filtrage URL</b>, pour assurer le contrôle de l'accès interne aux contenus Web indésirables, non productifs, voire illégaux,</li> <li>• <b>Control Applicatif</b>, afin d'identifier, reconnaître et contrôler les applications dans les flux,</li> </ul> </li> </ul>



Item	Spécifications techniques
	<p><b>Spécifications matérielles et performance :</b></p> <ul style="list-style-type: none"> <li>- Format : Appliance Rackable, 19"</li> <li>- Débit de Prevention des menaces (Firewall niveau 7 avec Contrôle applicatif + IPS + Anti Malware + Sandboxing+ Antispyware + filtrage URL, filtrage de contenu et Journalisation) : 2.5 Gbps Minimum</li> <li>- Nombre de sessions inspectées simultanées : 1 Million Minimum</li> <li>- Nombre de nouvelles sessions par seconde : 50 000 Minimum</li> <li>- Stockage Disque dur dédiée de type SSD de 200 GB Minimum</li> <li>- Les ports (en dehors des ports de management et de la haute disponibilité) <ul style="list-style-type: none"> <li>• Minimum 8 ports 10/100/1000 BaseT</li> <li>• Minimum 4 ports 1G/10G SFP/SFP+ dont 4 avec Transceiver SFP+</li> </ul> </li> <li>- Les ports de management et Clustering : <ul style="list-style-type: none"> <li>• Minimum 1 port 10/100/1000 BaseT pour le management</li> <li>• Minimum 1 port console RJ-45</li> <li>• Minimum 1 port USB</li> <li>• Minimum 1 ports 10/100/1000 BaseT pour le HA</li> </ul> </li> <li>- 2 Alimentations électriques Redondantes Minimum (AC),</li> </ul>
	<p><b>Support de la haute disponibilité :</b></p> <ul style="list-style-type: none"> <li>- Actif/Actif avec synchronisation d'état de session,</li> <li>- Actif/Passif,</li> </ul>
	<p><b>Contrôle applicatif :</b></p> <ul style="list-style-type: none"> <li>- Identification des applications en se basant sur : <ul style="list-style-type: none"> <li>• Signatures</li> <li>• Décodage du protocole (respecte la spécification du protocole)</li> <li>• Déchiffrement du trafic encapsulé</li> </ul> </li> <li>- Identification et contrôle des applications partageant la même connexion</li> <li>- Contrôle de la fonction de transfert de fichiers d'une application</li> <li>- Visibilité du trafic applicatif inconnu à travers l'identification de sa nature : <ul style="list-style-type: none"> <li>• Volume du trafic</li> <li>• Utilisateur et/ou adresses IP</li> <li>• Port utilisé</li> <li>• Contenu associé : fichier, menace ou autre.</li> </ul> </li> <li>- La base de données de contrôle des applications doit contenir plus de 3 000 applications connues ;</li> <li>- La solution doit pouvoir créer une règle de filtrage avec plusieurs catégories ;</li> </ul>
	<p><b>Identification, authentification des utilisateurs et protection des identités</b></p> <ul style="list-style-type: none"> <li>- Prise en charge des services d'authentification suivants pour l'identification et authentifications des utilisateurs : <ul style="list-style-type: none"> <li>• Active Directory</li> <li>• Kerberos</li> <li>• LDAP</li> <li>• Radius</li> <li>• Base Locale</li> <li>• SAML</li> <li>• Authentification via SSO Kerberos sans agent</li> <li>• Authentification par Certificat client</li> </ul> </li> </ul>



Item	Spécifications techniques
	<ul style="list-style-type: none"> <li>• Portail captif</li> <li>- Identification des utilisateurs indépendamment : <ul style="list-style-type: none"> <li>• Du terminal (ordinateur, un téléphone intelligent ou une tablette)</li> <li>• Du système d'exploitation utilisé,</li> <li>• Des adresses IP et de la zone (LAN, VPN, hors du périmètre du réseau)</li> </ul> </li> </ul>
	<p><b>Fonctions Réseau :</b></p> <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> <li>- Support de la fonctionnalité <b>SD-WAN</b> pour le routage avancé des flux sur plusieurs liaisons à base d'application afin d'augmenter la disponibilité et la performance WAN en se basant sur les paramètres de performance (Latence, Perte de packets et jitter) que ce soit lors de la navigation Internet et pour la communication inter-sites (<b>fonctionnalité et licence à fournir</b>)</li> </ul>
	<p><b>Fonction VPN :</b></p> <ul style="list-style-type: none"> <li>- VPN IPsec site-site, client-site et hub &amp; Spoke. (<b>Fonctionnalité et licence à fournir</b>)</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>
	<p><b>Gestion de la bande passante :</b></p> <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>
	<p><b>Administration et gestion des journaux :</b></p> <ul style="list-style-type: none"> <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> <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> </ul>



5  
H2

Item	Spécifications techniques
	<ul style="list-style-type: none"> <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>
	<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>
1.2	<b>PRESTATION DE SERVICE</b> Le prestataire doit proposer dans son offre toutes les prestations nécessaires à la mise en œuvre de la solution de sécurité : <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>- Intégration de la solution dans le réseau de la CMC ;</li> <li>- L'interconnexion du NGFW avec les Switch Datacenter ;</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 d'un an avec un délai de prise en charge de <b>2 heures</b> après déclaration de l'incident et un délai de <b>4 heures</b> de résolution ou de contournement du problème ;</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

Item	Désignation	Unité	CMC ERRACHIDIA
1	Solution de Firewall Nouvelle Génération NGFW de type Appliance		
1.1	Firewall	U	1
1.2	PRESTATION DE SERVICE	ens	1

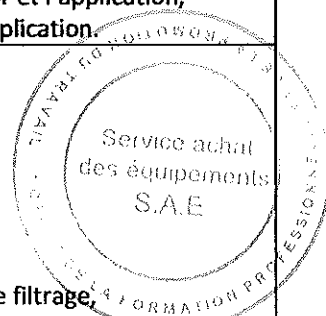
LOT 10 : Solution de Firewall Nouvelle Génération NGFW pour la CMC GUELMIM

Item	Spécifications techniques
1 .	<b>Solution de Firewall Nouvelle Génération NGFW de type Appliance</b>
1.1	<b>Leader dans Gartner dans la technologie Network Firewall pour les trois années minimum 2019, 2020 et 2021</b>
	<p><b>Fonctions Firewall</b></p> <ul style="list-style-type: none"> <li>- Doit intégrer un système d'exploitation propriétaire sécurisé,</li> <li>- Filtrage de paquets et être doté de la fonction de filtrage dynamique,</li> <li>- Filtrage basé sur les applications niveau 7 en plus des ports/Protocol et par plages de ports UDP ou TCP</li> <li>- Filtrage et inspection en IPv4 et IPv6,</li> <li>- Failover de connexion Internet,</li> <li>- Prise en compte de paramètre Horaire dans les règles de filtrage,</li> <li>- Doit fournir, via sa console d'administration, des statistiques sur le nombre d'accès aux règles de sécurité,</li> <li>- Doit inclure la possibilité de fonctionner en mode transparent ou routé (natté),</li> <li>- 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,</li> <li>- La création de la politique de sécurité basée sur : <ul style="list-style-type: none"> <li>• Geolocation par pays</li> <li>• Zones</li> <li>• Groupes de Zones</li> <li>• Applications, Groupes d'applications</li> <li>• Catégories d'Applications</li> <li>• Technologies d'Applications</li> <li>• Filtres d'Applications</li> <li>• Utilisateurs et Groupes</li> <li>• Adresses IP, Groupes d'adresses IP, Sous-réseaux IP, Groupes de sous-réseaux IP</li> <li>• Services, Groupes de Services</li> </ul> </li> <li>- 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) : <ul style="list-style-type: none"> <li>• <b>IPS (prévention des intrusions)</b> 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 : <ul style="list-style-type: none"> <li>- Détection par signatures ;</li> <li>- Détection par anomalies ;</li> <li>- Capable de faire des analyses comportementales de tout type de trafic ;</li> <li>- Possibilité de créer des signatures personnalisées ;</li> <li>- Mise à jour automatique des signatures IPS ;</li> <li>- Création et affectation des politiques IPS par type de zone ou interface ;</li> <li>- 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) ... ;</li> <li>- Gestion de profils IPS avec association à certains trafics dans la politique de filtrage (IP source, IP destination, service, protocole, réseau...) ;</li> </ul> </li> <li>• <b>Filtrage URL</b>, pour assurer le contrôle de l'accès interne aux contenus Web indésirables, non productifs, voire illégaux,</li> <li>• <b>Control Applicatif</b>, afin d'identifier, reconnaître et contrôler les applications dans les flux,</li> </ul> </li> </ul>

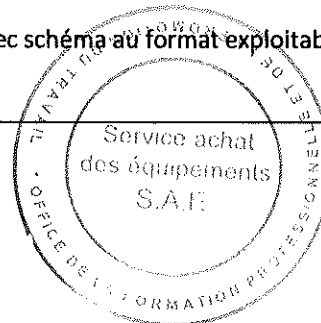
Item	Spécifications techniques
	<p><b>Spécifications matérielles et performance :</b></p> <ul style="list-style-type: none"> <li>- Format : Appliance Rackable, 19"</li> <li>- Débit de Prevention des menaces (Firewall niveau 7 avec Contrôle applicatif + IPS + Anti Malware + Sandboxing+ Antispyware + filtrage URL, filtrage de contenu et Journalisation) : 2.5 Gbps Minimum</li> <li>- Nombre de sessions inspectées simultanées : 1 Million Minimum</li> <li>- Nombre de nouvelles sessions par seconde : 50 000 Minimum</li> <li>- Stockage Disque dur dédiée de type SSD de 200 GB Minimum</li> <li>- Les ports (en dehors des ports de management et de la haute disponibilité) <ul style="list-style-type: none"> <li>• Minimum 8 ports 10/100/1000 BaseT</li> <li>• Minimum 4 ports 1G/10G SFP/SFP+ dont 4 avec Transceiver SFP+</li> </ul> </li> <li>- Les ports de management et Clustering : <ul style="list-style-type: none"> <li>• Minimum 1 port 10/100/1000 BaseT pour le management</li> <li>• Minimum 1 port console RJ-45</li> <li>• Minimum 1 port USB</li> <li>• Minimum 1 ports 10/100/1000 BaseT pour le HA</li> </ul> </li> <li>- 2 Alimentations électriques Redondantes Minimum (AC),</li> </ul>
	<p><b>Support de la haute disponibilité :</b></p> <ul style="list-style-type: none"> <li>- Actif/Actif avec synchronisation d'état de session,</li> <li>- Actif/Passif,</li> </ul>
	<p><b>Contrôle applicatif :</b></p> <ul style="list-style-type: none"> <li>- Identification des applications en se basant sur : <ul style="list-style-type: none"> <li>• Signatures</li> <li>• Décodage du protocole (respecte la spécification du protocole)</li> <li>• Déchiffrement du trafic encapsulé</li> </ul> </li> <li>- Identification et contrôle des applications partageant la même connexion</li> <li>- Contrôle de la fonction de transfert de fichiers d'une application</li> <li>- Visibilité du trafic applicatif inconnu à travers l'identification de sa nature : <ul style="list-style-type: none"> <li>• Volume du trafic</li> <li>• Utilisateur et/ou adresses IP</li> <li>• Port utilisé</li> <li>• Contenu associé : fichier, menace ou autre.</li> </ul> </li> <li>- La base de données de contrôle des applications doit contenir plus de 3 000 applications connues ;</li> <li>- La solution doit pouvoir créer une règle de filtrage avec plusieurs catégories ;</li> </ul>
	<p><b>Identification, authentification des utilisateurs et protection des identités</b></p> <ul style="list-style-type: none"> <li>- Prise en charge des services d'authentification suivants pour l'identification et authentifications des utilisateurs : <ul style="list-style-type: none"> <li>• Active Directory</li> <li>• Kerberos</li> <li>• LDAP</li> <li>• Radius</li> <li>• Base Locale</li> <li>• SAML</li> <li>• Authentification via SSO Kerberos sans agent</li> <li>• Authentification par Certificat client</li> </ul> </li> </ul>



Item	Spécifications techniques
	<ul style="list-style-type: none"> <li>• Portail captif</li> <li>- Identification des utilisateurs indépendamment : <ul style="list-style-type: none"> <li>• Du terminal (ordinateur, un téléphone intelligent ou une tablette)</li> <li>• Du système d'exploitation utilisé,</li> <li>• Des adresses IP et de la zone (LAN, VPN, hors du périmètre du réseau)</li> </ul> </li> </ul>
	<p><b>Fonctions Réseau :</b></p> <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> <li>- Support de la fonctionnalité <b>SD-WAN</b> pour le routage avancé des flux sur plusieurs liaisons à base d'application afin d'augmenter la disponibilité et la performance WAN en se basant sur les paramètres de performance (Latence, Perte de packets et jitter) que ce soit lors de la navigation Internet et pour la communication inter-sites (<b>fonctionnalité et licence à fournir</b>)</li> </ul>
	<p><b>Fonction VPN :</b></p> <ul style="list-style-type: none"> <li>- VPN IPsec site-site, client-site et hub &amp; Spoke. (<b>Fonctionnalité et licence à fournir</b>)</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>
	<p><b>Gestion de la bande passante :</b></p> <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>
	<p><b>Administration et gestion des journaux :</b></p> <ul style="list-style-type: none"> <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> <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> </ul>



Item	Spécifications techniques
	<ul style="list-style-type: none"> <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>
	<p><b>Filtrage URL et Filtrage de contenu</b></p> <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>
1.2	<p><b>PRESTATION DE SERVICE</b></p> <p>Le prestataire doit proposer dans son offre toutes les prestations nécessaires à la mise en œuvre de la solution de sécurité :</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>- Intégration de la solution dans le réseau de la CMC ;</li> <li>- L'interconnexion du NGFW avec les Switch Datacenter ;</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 d'un an 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 ;</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>



Handwritten signature/initials.

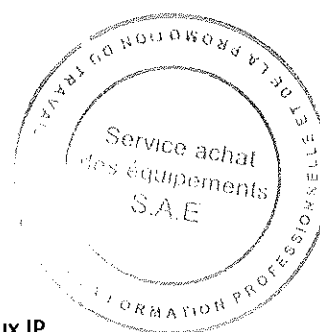


Tableau de répartition

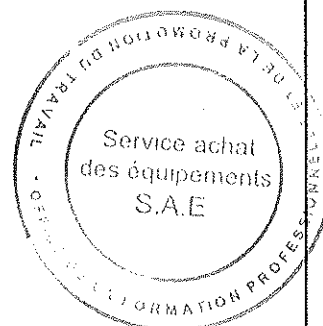
Item	Désignation	Unité	CMC GUELMIM
1	Solution de Firewall Nouvelle Génération NGFW de type Appliance		
1.1	Firewall	U	1
1.2	PRESTATION DE SERVICE	ens	1

**LOT 11 : Solution de Firewall Nouvelle Génération NGFW pour la CMC DAKHLA**

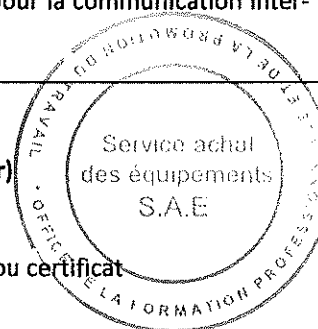
Item	Spécifications techniques
1 .	<b>Solution de Firewall Nouvelle Génération NGFW de type Appliance</b>
1.1	<b>Leader dans Gartner dans la technologie Network Firewall pour les trois années minimum 2019, 2020 et 2021</b>
	<p><b>Fonctions Firewall</b></p> <ul style="list-style-type: none"> <li>- Doit intégrer un système d'exploitation propriétaire sécurisé,</li> <li>- Filtrage de paquets et être doté de la fonction de filtrage dynamique,</li> <li>- Filtrage basé sur les applications niveau 7 en plus des ports/Protocol et par plages de ports UDP ou TCP</li> <li>- Filtrage et inspection en IPv4 et IPv6,</li> <li>- Failover de connexion Internet,</li> <li>- Prise en compte de paramètre Horaire dans les règles de filtrage,</li> <li>- Doit fournir, via sa console d'administration, des statistiques sur le nombre d'accès aux règles de sécurité,</li> <li>- Doit inclure la possibilité de fonctionner en mode transparent ou routé (natté),</li> <li>- 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,</li> <li>- La création de la politique de sécurité basée sur : <ul style="list-style-type: none"> <li>• Geolocation par pays</li> <li>• Zones</li> <li>• Groupes de Zones</li> <li>• Applications, Groupes d'applications</li> <li>• Catégories d'Applications</li> <li>• Technologies d'Applications</li> <li>• Filtres d'Applications</li> <li>• Utilisateurs et Groupes</li> <li>• Adresses IP, Groupes d'adresses IP, Sous-réseaux IP, Groupes de sous-réseaux IP</li> <li>• Services, Groupes de Services</li> </ul> </li> <li>- 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) : <ul style="list-style-type: none"> <li>• <b>IPS (prévention des intrusions)</b> 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 : <ul style="list-style-type: none"> <li>- Détection par signatures ;</li> <li>- Détection par anomalies ;</li> <li>- Capable de faire des analyses comportementales de tout type de trafic ;</li> </ul> </li> </ul> </li> </ul>



Item	Spécifications techniques
	<ul style="list-style-type: none"> <li>- Possibilité de créer des signatures personnalisées ;</li> <li>- Mise à jour automatique des signatures IPS ;</li> <li>- Création et affectation des politiques IPS par type de zone ou interface ;</li> <li>- 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) ... ;</li> <li>- Gestion de profils IPS avec association à certains trafics dans la politique de filtrage (IP source, IP destination, service, protocole, réseau...) ;</li> <li>• <b>Filtrage URL</b>, pour assurer le contrôle de l'accès interne aux contenus Web indésirables, non productifs, voire illégaux,</li> <li>• <b>Control Applicatif</b>, afin d'identifier, reconnaître et contrôler les applications dans les flux,</li> </ul>
	<p><b>Spécifications matérielles et performance :</b></p> <ul style="list-style-type: none"> <li>- Format : Appliance Rackable, 19"</li> <li>- Débit de Prevention des menaces (Firewall niveau 7 avec Contrôle applicatif + IPS + Anti Malware + Sandboxing+ Antispyware + filtrage URL, filtrage de contenu et Journalisation) : 2.5 Gbps Minimum</li> <li>- Nombre de sessions inspectées simultanées : <b>1 Million Minimum</b></li> <li>- Nombre de nouvelles sessions par seconde : <b>50 000 Minimum</b></li> <li>- Stockage Disque dur dédiée de type SSD de <b>200 GB Minimum</b></li> <li>- Les ports (en dehors des ports de management et de la haute disponibilité) <ul style="list-style-type: none"> <li>• Minimum 8 ports 10/100/1000 BaseT</li> <li>• Minimum 4 ports 1G/10G SFP/SFP+ dont 4 avec Transceiver SFP+</li> </ul> </li> <li>- Les ports de management et Clustering : <ul style="list-style-type: none"> <li>• Minimum 1 port 10/100/1000 BaseT pour le management</li> <li>• Minimum 1 port console RJ-45</li> <li>• Minimum 1 port USB</li> <li>• Minimum 1 ports 10/100/1000 BaseT pour le HA</li> </ul> </li> <li>- 2 Alimentations électriques Redondantes Minimum (AC),</li> </ul>
	<p><b>Support de la haute disponibilité :</b></p> <ul style="list-style-type: none"> <li>- Actif/Actif avec synchronisation d'état de session,</li> <li>- Actif/Passif,</li> </ul>
	<p><b>Contrôle applicatif :</b></p> <ul style="list-style-type: none"> <li>- Identification des applications en se basant sur : <ul style="list-style-type: none"> <li>• Signatures</li> <li>• Décodage du protocole (respecte la spécification du protocole)</li> <li>• Déchiffrement du trafic encapsulé</li> </ul> </li> <li>- Identification et contrôle des applications partageant la même connexion</li> <li>- Contrôle de la fonction de transfert de fichiers d'une application</li> <li>- Visibilité du trafic applicatif inconnu à travers l'identification de sa nature : <ul style="list-style-type: none"> <li>• Volume du trafic</li> <li>• Utilisateur et/ou adresses IP</li> <li>• Port utilisé</li> <li>• Contenu associé : fichier, menace ou autre.</li> </ul> </li> <li>- La base de données de contrôle des applications doit contenir plus de <b>3 000 applications connues</b> ;</li> <li>- La solution doit pouvoir créer une règle de filtrage avec plusieurs catégories ;</li> </ul>
	<p><b>Identification, authentification des utilisateurs et protection des identités</b></p>

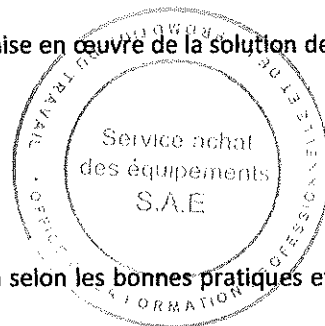


Item	Spécifications techniques
	<ul style="list-style-type: none"> <li>- Prise en charge des services d'authentification suivants pour l'identification et authentifications des utilisateurs : <ul style="list-style-type: none"> <li>• Active Directory</li> <li>• Kerberos</li> <li>• LDAP</li> <li>• Radius</li> <li>• Base Locale</li> <li>• SAML</li> <li>• Authentification via SSO Kerberos sans agent</li> <li>• Authentification par Certificat client</li> <li>• Portail captif</li> </ul> </li> <li>- Identification des utilisateurs indépendamment : <ul style="list-style-type: none"> <li>• Du terminal (ordinateur, un téléphone intelligent ou une tablette)</li> <li>• Du système d'exploitation utilisé,</li> <li>• Des adresses IP et de la zone (LAN, VPN, hors du périmètre du réseau)</li> </ul> </li> </ul>
	<p><b>Fonctions Réseau :</b></p> <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> <li>- Support de la fonctionnalité <b>SD-WAN</b> pour le routage avancé des flux sur plusieurs liaisons à base d'application afin d'augmenter la disponibilité et la performance WAN en se basant sur les paramètres de performance (Latence, Perte de packets et jitter) que ce soit lors de la navigation Internet et pour la communication inter-sites (<b>fonctionnalité et licence à fournir</b>)</li> </ul>
	<p><b>Fonction VPN :</b></p> <ul style="list-style-type: none"> <li>- VPN IPsec site-site, client-site et hub &amp; Spoke. (<b>Fonctionnalité et licence à fournir</b>)</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>
	<p><b>Gestion de la bande passante :</b></p> <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>
	<p><b>Administration et gestion des journaux :</b></p> <ul style="list-style-type: none"> <li>- Administration via une interface web intuitive et sécurisée en HTTPS,</li> <li>- Administration en ligne de commande SSH et Telnet,</li> </ul>



Handwritten marks: a checkmark and the signature 'H.A.'

Item	Spécifications techniques
	<ul style="list-style-type: none"> <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> <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>
	<p><b>Filtrage URL et Filtrage de contenu</b></p> <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>
1.2	<p><b>PRESTATION DE SERVICE</b></p> <p>Le prestataire doit proposer dans son offre toutes les prestations nécessaires à la mise en œuvre de la solution de sécurité :</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>- Intégration de la solution dans le réseau de la CMC ;</li> <li>- L'interconnexion du NGFW avec les Switch Datacenter ;</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 d'un an 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 ;</li> <li>- Livrables :</li> </ul>



✓  
A2

Item	Spécifications techniques
	<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>

Tableau de répartition

Item	Désignation	Unité	CMC DAKHLA
1	Solution de Firewall Nouvelle Génération NGFW de type Appliance		
1.1	Firewall	U	1
1.2	PRESTATION DE SERVICE	ens	1

LE SOUSMISSIONNAIRE	LE MAITRE D'OUVRAGE DELEGUE
Lu et accepté	<p><b>Abdellf AOURAGH</b></p> <p>Directeur de l'Approvisionnement et de la Logistique</p>



Handwritten signature and initials.

## **Annexe :**

**Spécifications techniques des fournitures proposées par le concurrent par lot :**



**LOT 1: Solution de Firewall Nouvelle Génération NGFW de type Appliance pour la CMC Nador**

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

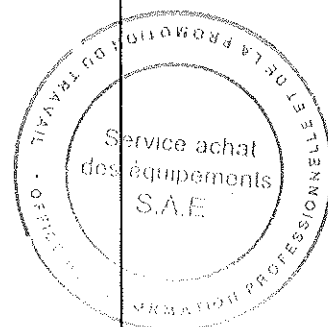
*Tout article ne répondant pas aux spécifications demandées sera déclaré non-conforme.*

*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.*

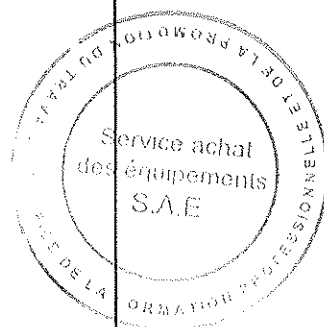
*Les valeurs des dimensions, longueurs, capacités,... Doivent être renseignées d'une manière précise dans la colonne « Proposition du soumissionnaire ».*

Item	Spécifications techniques	Proposition du soumissionnaire	Appréciation de l'administration
<b>1 .</b>	<b>Solution de Firewall Nouvelle Génération NGFW de type Appliance</b>		
<b>1.1</b>	<b>Leader dans Gartner dans la technologie Network Firewall pour les trois années minimum 2019, 2020 et 2021</b>		
	<b>Fonctions Firewall</b> <ul style="list-style-type: none"> <li>- Doit intégrer un système d'exploitation propriétaire sécurisé,</li> <li>- Filtrage de paquets et être doté de la fonction de filtrage dynamique,</li> <li>- Filtrage basé sur les applications niveau 7 en plus des ports/Protocol et par plages de ports UDP ou TCP</li> <li>- Filtrage et inspection en IPv4 et IPv6,</li> <li>- Failover de connexion Internet,</li> <li>- Prise en compte de paramètre Horaire dans les règles de filtrage,</li> <li>- Doit fournir, via sa console d'administration, des statistiques sur le nombre d'accès aux règles de sécurité,</li> <li>- Doit inclure la possibilité de fonctionner en mode transparent ou routé (natté),</li> <li>- 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,</li> <li>- La création de la politique de sécurité basée sur : <ul style="list-style-type: none"> <li>• Geolocation par pays</li> <li>• Zones</li> <li>• Groupes de Zones</li> <li>• Applications, Groupes d'applications</li> <li>• Catégories d'Applications</li> <li>• Technologies d'Applications</li> <li>• Filtres d'Applications</li> <li>• Utilisateurs et Groupes</li> <li>• Adresses IP, Groupes d'adresses IP, Sous-réseaux IP, Groupes de sous-réseaux IP</li> <li>• Services, Groupes de Services</li> </ul> </li> <li>- 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) :</li> </ul>	<b>Marque :</b> <b>Référence :</b> <b>Caractéristiques proposées</b>	



HP

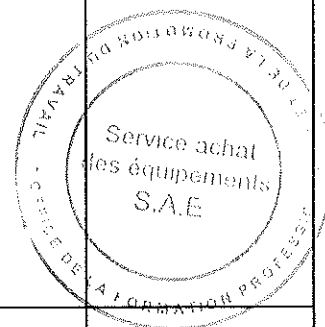
Item	Spécifications techniques	Proposition du soumissionnaire	Appréciation de l'administration
	<ul style="list-style-type: none"> <li>• <b>IPS (prévention des intrusions)</b> pour se protéger contre les menaces réseau telles que vers, chevaux de Troie et autres programmes malveillants. Le système de prévention des intrusions (IPS) doit aussi apporter une protection contre les menaces réseaux existantes et émergentes. Ce module IPS doit avoir deux mécanismes : <ul style="list-style-type: none"> <li>- Détection par signatures ;</li> <li>- Détection par anomalies ;</li> <li>- Capable de faire des analyses comportementales de tout type de trafic ;</li> <li>- Possibilité de créer des signatures personnalisées ;</li> <li>- Mise à jour automatique des signatures IPS ;</li> <li>- Création et affectation des politiques IPS par type de zone ou interface ;</li> <li>- 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) ... ;</li> <li>- Gestion de profils IPS avec association à certains trafics dans la politique de filtrage (IP source, IP destination, service, protocole, réseau...) ;</li> </ul> </li> <li>• <b>Filtrage URL</b>, pour assurer le contrôle de l'accès interne aux contenus Web indésirables, non productifs, voire illégaux,</li> <li>• <b>Control Applicatif</b>, afin d'identifier, reconnaître et contrôler les applications dans les flux,</li> </ul>		
	<p><b>Spécifications matérielles et performance :</b></p> <ul style="list-style-type: none"> <li>- Format : Appliance Rackable, 19"</li> <li>- Débit de Prévention des menaces (Firewall niveau 7 avec Contrôle applicatif + IPS + Anti Malware + Sandboxing+ Antispyware + filtrage URL, filtrage de contenu et Journalisation) : <b>2.5 Gbps Minimum</b></li> <li>- Nombre de sessions inspectées simultanées : <b>1 Million Minimum</b></li> <li>- Nombre de nouvelles sessions par seconde : <b>50 000 Minimum</b></li> <li>- Stockage Disque dur dédiée de type SSD de <b>200 GB Minimum</b></li> <li>- Les ports (en dehors des ports de management et de la haute disponibilité) <ul style="list-style-type: none"> <li>• Minimum 8 ports 10/100/1000 BaseT</li> <li>• Minimum 4 ports 1G/10G SFP/SFP+ dont <b>4 avec Transceiver SFP+</b></li> </ul> </li> <li>- Les ports de management et Clustering : <ul style="list-style-type: none"> <li>• Minimum 1 port 10/100/1000 BaseT pour le management</li> <li>• Minimum 1 port console RJ-45</li> <li>• Minimum 1 port USB</li> <li>• Minimum 1 ports 10/100/1000 BaseT pour le HA</li> </ul> </li> </ul> <p><b>2 Alimentations électriques Redondantes Minimum (AC),</b></p>		
	<p><b>Support de la haute disponibilité :</b></p> <ul style="list-style-type: none"> <li>- Actif/Actif avec synchronisation d'état de session,</li> <li>- Actif/Passif,</li> </ul>		



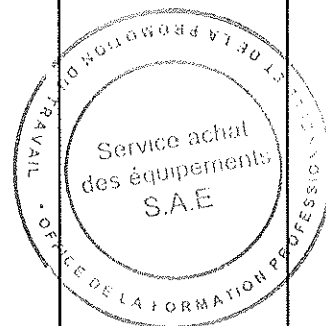
*Handwritten marks: a checkmark and the signature 'H2'.*



Item	Spécifications techniques	Proposition du soumissionnaire	Appréciation de l'administration
	<p><b>Contrôle applicatif :</b></p> <ul style="list-style-type: none"> <li>- Identification des applications en se basant sur : <ul style="list-style-type: none"> <li>• Signatures</li> <li>• Décodage du protocole (respecte la spécification du protocole)</li> <li>• Déchiffrement du trafic encapsulé</li> </ul> </li> <li>- Identification et contrôle des applications partageant la même connexion</li> <li>- Contrôle de la fonction de transfert de fichiers d'une application</li> <li>- Visibilité du trafic applicatif inconnu à travers l'identification de sa nature : <ul style="list-style-type: none"> <li>• Volume du trafic</li> <li>• Utilisateur et/ou adresses IP</li> <li>• Port utilisé</li> <li>• Contenu associé : fichier, menace ou autre.</li> </ul> </li> <li>- La base de données de contrôle des applications doit contenir plus de 3 000 applications connues ;</li> </ul> <p>La solution doit pouvoir créer une règle de filtrage avec plusieurs catégories ;</p>		
	<p><b>Identification, authentification des utilisateurs et protection des identités</b></p> <ul style="list-style-type: none"> <li>- Prise en charge des services d'authentification suivants pour l'identification et authentifications des utilisateurs : <ul style="list-style-type: none"> <li>• Active Directory</li> <li>• Kerberos</li> <li>• LDAP</li> <li>• Radius</li> <li>• Base Locale</li> <li>• SAML</li> <li>• Authentification via SSO Kerberos sans agent</li> <li>• Authentification par Certificat client</li> <li>• Portail captif</li> </ul> </li> <li>- Identification des utilisateurs indépendamment : <ul style="list-style-type: none"> <li>• Du terminal (ordinateur, un téléphone intelligent ou une tablette)</li> <li>• Du système d'exploitation utilisé,</li> <li>• Des adresses IP et de la zone (LAN, VPN, hors du périmètre du réseau)</li> </ul> </li> </ul>		
	<p><b>Fonctions Réseau :</b></p> <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> </ul>		

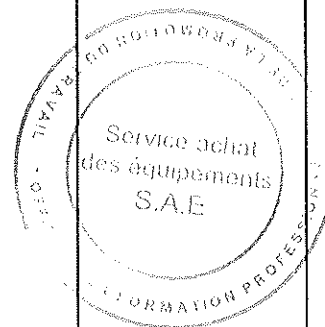


Item	Spécifications techniques	Proposition du soumissionnaire	Appréciation de l'administration
	<ul style="list-style-type: none"> <li>- Nat dynamique, Nat Statique, Nat par port, Nat64</li> <li>- Support de Multicast</li> <li>- Support de la fonctionnalité <b>SD-WAN</b> pour le routage avancé des flux sur plusieurs liaisons à base d'application afin d'augmenter la disponibilité et la performance WAN en se basant sur les paramètres de performance (Latence, Perte de packets et jitter) que ce soit lors de la navigation Internet et pour la communication inter-sites (<b>fonctionnalité et licence à fournir</b>)</li> <li>-</li> </ul>		
	<b>Fonction VPN :</b> <ul style="list-style-type: none"> <li>- VPN IPSec site-site, client-site et hub &amp; Spoke. (<b>Fonctionnalité et licence à fournir</b>)</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> <li>-</li> </ul>		
	<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> </ul> Limitation de la bande passante par source, destination, application ou catégorie d'application.		
	<b>Administration et gestion des journaux :</b> <ul style="list-style-type: none"> <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> <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> </ul>		



7  
A\*

Item	Spécifications techniques	Proposition du soumissionnaire	Appréciation de l'administration
	<ul style="list-style-type: none"> <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>		
	<p><b>Filtrage URL et Filtrage de contenu</b></p> <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>		
<b>1.2</b>	<p><b>PRESTATION DE SERVICE</b></p> <p>Le prestataire doit proposer dans son offre toutes les prestations nécessaires à la mise en œuvre de la solution de sécurité :</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>- Intégration de la solution dans le réseau de la CMC ;</li> <li>- L'interconnexion du NGFW avec les Switch Datacenter ;</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 d'un an avec un délai de prise en charge de <b>2 heures</b> après déclaration de l'incident et un délai de <b>4 heures</b> de résolution ou de contournement du problème ;</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> </ul> </li> </ul> <p>Manuel d'exploitation ;</p>		



Handwritten marks: a checkmark and the letters 'HE'.

**BORDEREAU DES PRIX – DETAIL ESTIMATIF**

**LOT 1 : Solution de Firewall Nouvelle Génération NGFW de type Appliance pour la CMC Nador**

Items N°	Désignations	Unité	(1) QTE	(2) Prix unitaire HT/HDD/HTV A	(3) Prix total HT/HDD/HTV A (3) = (1) x (2)	(4) Droits de Douanes sur (3)	(5) Prix total Hors TVA (5) = (3)+(4)	(6) TVA Appliqué e sur (5)	(7) Montant TTC (7) = (5)+(6)
1	Solution de Firewall Nouvelle Génération NGFW de type Appliance								
1.1	Firewall	U	1						
1.2	PRESTATION DE SERVICE	ens	1						
<b>MONTANT TOTAL =</b>									

Important : 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 à ce sujet.

Fait à ..... le .....

Signature et cachet du concurrent



✓

Hr

**LOT 2 : Solution de Firewall Nouvelle Génération NGFW pour la CMC LAAYOUNE**

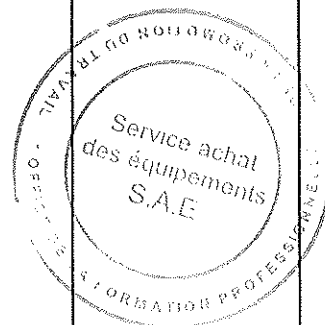
*N.B : les soumissionnaires sont invités à remplir la case 'Proposition du soumissionnaire' en précisant les caractéristiques du matériel. La réponse du soumissionnaire doit être justifiée par des notes explicatives, des fiches techniques (marquer les justifications), ou tout autre moyen pouvant justifier la proposition du soumissionnaire.*

*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.*

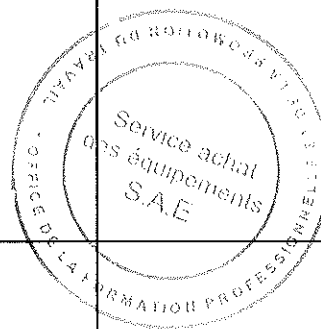
*Le concurrent est tenu à renseigner pour chaque item, la marque, la référence et les caractéristiques des fournitures proposées et ce, dans le cadre de la colonne 'Proposition du soumissionnaire' et la ligne correspondante à l'item.*

Item	Spécifications techniques	Proposition du soumissionnaire	Appréciation de l'administration
<b>1 .</b>	<b>Solution de Firewall Nouvelle Génération NGFW de type Appliance</b>		
<b>1.1</b>	<b>Leader dans Gartner dans la technologie Network Firewall pour les trois années minimum 2019, 2020 et 2021</b>		
	<b>Fonctions Firewall</b> <ul style="list-style-type: none"> <li>- Doit intégrer un système d'exploitation propriétaire sécurisé,</li> <li>- Filtrage de paquets et être doté de la fonction de filtrage dynamique,</li> <li>- Filtrage basé sur les applications niveau 7 en plus des ports/Protocol et par plages de ports UDP ou TCP</li> <li>- Filtrage et inspection en IPv4 et IPv6,</li> <li>- Faillover de connexion Internet,</li> <li>- Prise en compte de paramètre Horaire dans les règles de filtrage,</li> <li>- Doit fournir, via sa console d'administration, des statistiques sur le nombre d'accès aux règles de sécurité,</li> <li>- Doit inclure la possibilité de fonctionner en mode transparent ou routé (natté),</li> <li>- 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,</li> <li>- La création de la politique de sécurité basée sur : <ul style="list-style-type: none"> <li>• Geolocation par pays</li> <li>• Zones</li> <li>• Groupes de Zones</li> <li>• Applications, Groupes d'applications</li> <li>• Catégories d'Applications</li> <li>• Technologies d'Applications</li> <li>• Filtres d'Applications</li> <li>• Utilisateurs et Groupes</li> <li>• Adresses IP, Groupes d'adresses IP, Sous-réseaux IP, Groupes de sous-réseaux IP</li> <li>• Services, Groupes de Services</li> </ul> </li> <li>- 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) : <ul style="list-style-type: none"> <li>• <b>IPS (prévention des intrusions)</b> pour se protéger contre les menaces réseau telles que vers, chevaux de Troie et autres</li> </ul> </li> </ul>	<b>Marque :</b> <b>Référence :</b> <b>Caractéristiques proposées</b>	



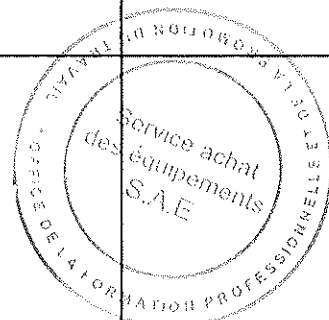
✓  
H2

Item	Spécifications techniques	Proposition du soumissionnaire	Appréciation de l'administration
	<p>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 :</p> <ul style="list-style-type: none"> <li>- Détection par signatures ;</li> <li>- Détection par anomalies ;</li> <li>- Capable de faire des analyses comportementales de tout type de trafic ;</li> <li>- Possibilité de créer des signatures personnalisées ;</li> <li>- Mise à jour automatique des signatures IPS ;</li> <li>- Création et affectation des politiques IPS par type de zone ou interface ;</li> <li>- 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) ... ;</li> <li>- Gestion de profils IPS avec association à certains trafics dans la politique de filtrage (IP source, IP destination, service, protocole, réseau...) ;</li> <li>• <b>Filtrage URL</b>, pour assurer le contrôle de l'accès interne aux contenus Web indésirables, non productifs, voire illégaux,</li> <li>• <b>Control Applicatif</b>, afin d'identifier, reconnaître et contrôler les applications dans les flux,</li> </ul>		
	<p><b>Spécifications matérielles et performance :</b></p> <ul style="list-style-type: none"> <li>- Format : Appliance Rackable, 19"</li> <li>- Débit de Prevention des menaces (Firewall niveau 7 avec Contrôle applicatif + IPS + Anti Malware + Sandboxing+ Antispyware + filtrage URL, filtrage de contenu et Journalisation) : <b>2.5 Gbps Minimum</b></li> <li>- Nombre de sessions inspectées simultanées : <b>1 Million Minimum</b></li> <li>- Nombre de nouvelles sessions par seconde : <b>50 000 Minimum</b></li> <li>- Stockage Disque dur dédiée de type SSD de <b>200 GB Minimum</b></li> <li>- Les ports (en dehors des ports de management et de la haute disponibilité) <ul style="list-style-type: none"> <li>• Minimum 8 ports 10/100/1000 BaseT</li> <li>• Minimum 4 ports 1G/10G SFP/SFP+ dont 4 avec Transceiver SFP+</li> </ul> </li> <li>- Les ports de management et Clustering : <ul style="list-style-type: none"> <li>• Minimum 1 port 10/100/1000 BaseT pour le management</li> <li>• Minimum 1 port console RJ-45</li> <li>• Minimum 1 port USB</li> <li>• Minimum 1 ports 10/100/1000 BaseT pour le HA</li> </ul> </li> </ul> <p>2 Alimentations électriques Redondantes Minimum (AC),</p>		
	<p><b>Support de la haute disponibilité :</b></p> <ul style="list-style-type: none"> <li>- Actif/Actif avec synchronisation d'état de session,</li> <li>- Actif/Passif,</li> </ul>		
	<p><b>Contrôle applicatif :</b></p>		

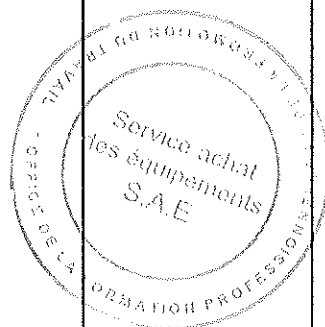


V  
H2

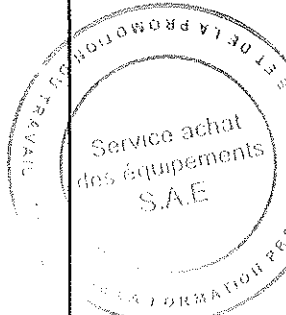
Item	Spécifications techniques	Proposition du soumissionnaire	Appréciation de l'administration
	<ul style="list-style-type: none"> <li>- Identification des applications en se basant sur : <ul style="list-style-type: none"> <li>• Signatures</li> <li>• Décodage du protocole (respecte la spécification du protocole)</li> <li>• Déchiffrement du trafic encapsulé</li> </ul> </li> <li>- Identification et contrôle des applications partageant la même connexion</li> <li>- Contrôle de la fonction de transfert de fichiers d'une application</li> <li>- Visibilité du trafic applicatif inconnu à travers l'identification de sa nature : <ul style="list-style-type: none"> <li>• Volume du trafic</li> <li>• Utilisateur et/ou adresses IP</li> <li>• Port utilisé</li> <li>• Contenu associé : fichier, menace ou autre.</li> </ul> </li> <li>- La base de données de contrôle des applications doit contenir plus de 3 000 applications connues ;</li> </ul> <p>La solution doit pouvoir créer une règle de filtrage avec plusieurs catégories ;</p>		
	<p><b>Identification, authentification des utilisateurs et protection des identités</b></p> <ul style="list-style-type: none"> <li>- Prise en charge des services d'authentification suivants pour l'identification et authentifications des utilisateurs : <ul style="list-style-type: none"> <li>• Active Directory</li> <li>• Kerberos</li> <li>• LDAP</li> <li>• Radius</li> <li>• Base Locale</li> <li>• SAML</li> <li>• Authentification via SSO Kerberos sans agent</li> <li>• Authentification par Certificat client</li> <li>• Portail captif</li> </ul> </li> <li>- Identification des utilisateurs indépendamment : <ul style="list-style-type: none"> <li>• Du terminal (ordinateur, un téléphone intelligent ou une tablette)</li> <li>• Du système d'exploitation utilisé,</li> <li>• Des adresses IP et de la zone (LAN, VPN, hors du périmètre du réseau)</li> </ul> </li> </ul>		
	<p><b>Fonctions Réseau :</b></p> <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>		



Item	Spécifications techniques	Proposition du soumissionnaire	Appréciation de l'administration
	<ul style="list-style-type: none"> <li>- Support de la fonctionnalité <b>SD-WAN</b> pour le routage avancé des flux sur plusieurs liaisons à base d'application afin d'augmenter la disponibilité et la performance WAN en se basant sur les paramètres de performance (Latence, Perte de packets et jitter) que ce soit lors de la navigation Internet et pour la communication inter-sites (<b>fonctionnalité et licence à fournir</b>)</li> </ul>		
	<p><b>Fonction VPN :</b></p> <ul style="list-style-type: none"> <li>- VPN IPsec site-site, client-site et hub &amp; Spoke. (<b>Fonctionnalité et licence à fournir</b>)</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>		
	<p><b>Gestion de la bande passante :</b></p> <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> </ul> <p>Limitation de la bande passante par source, destination, application ou catégorie d'application.</p>		
	<p><b>Administration et gestion des journaux :</b></p> <ul style="list-style-type: none"> <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> <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> </ul>		





Item	Spécifications techniques	Proposition du soumissionnaire	Appréciation de l'administration
	<ul style="list-style-type: none"> <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>		
	<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>		
1.2	<b>PRESTATION DE SERVICE</b> Le prestataire doit proposer dans son offre toutes les prestations nécessaires à la mise en œuvre de la solution de sécurité : <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>- Intégration de la solution dans le réseau de la CMC ;</li> <li>- L'interconnexion du NGFW avec les Switch Datacenter ;</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 d'un an 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 ;</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> </ul> </li> </ul> Manuel d'exploitation ;		

5  
H2

**BORDEREAU DES PRIX – DETAIL ESTIMATIF**

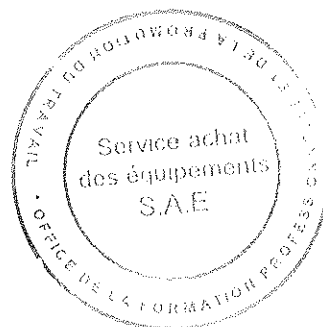
**LOT 2 : Solution de Firewall Nouvelle Génération NGFW de type Appliance pour la CMC LAAYOUNE**

Items N°	Désignations	Unité	(1) QTE	(2) Prix unitaire HT/HDD/HTV A	(3) Prix total HT/HDD/HTV A (3) = (1) x (2)	(4) Droits de Douanes sur (3)	(5) Prix total Hors TVA (5) = (3) + (4)	(6) TVA Appliquée sur (5)	(7) Montant TTC (7) = (5) + (6)
1	Solution de Firewall Nouvelle Génération NGFW de type Appliance								
1.1	Firewall	U	1						
1.2	PRESTATION DE SERVICE	ens	1						
<b>MONTANT TOTAL =</b>									

Important : 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 à ce sujet.

Fait à ..... le .....

Signature et cachet du concurrent



**LOT 3 : Solution de Firewall Nouvelle Génération NGFW pour la CMC TANGER**

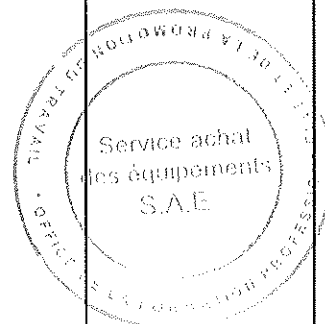
*N.B : les soumissionnaires sont invités à remplir la case 'Proposition du soumissionnaire' en précisant les caractéristiques du matériel. La réponse du soumissionnaire doit être justifiée par des notes explicatives, des fiches techniques (marquer les justifications), ou tout autre moyen pouvant justifier la proposition du soumissionnaire.*

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

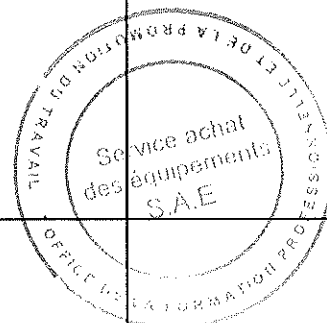
*Les colonnes 'Désignations et caractéristiques techniques' et 'Appréciation de l'administration' ne doivent pas être renseignées ou modifiées.*

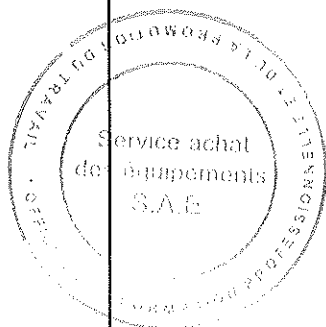
*Le concurrent est tenu à renseigner pour chaque item, la marque, la référence et les caractéristiques des fournitures proposées et ce, dans le cadre de la colonne 'Proposition du soumissionnaire' et la ligne correspondante à l'item.*

Item	Spécifications techniques	Proposition du soumissionnaire	Appréciation de l'administration
<b>1 .</b>	<b>Solution de Firewall Nouvelle Génération NGFW de type Appliance</b>		
<b>1.1</b>	<b>Leader dans Gartner dans la technologie Network Firewall pour les trois années minimum 2019, 2020 et 2021</b>		
	<b>Fonctions Firewall</b> <ul style="list-style-type: none"> <li>- Doit intégrer un système d'exploitation propriétaire sécurisé,</li> <li>- Filtrage de paquets et être doté de la fonction de filtrage dynamique,</li> <li>- Filtrage basé sur les applications niveau 7 en plus des ports/Protocol et par plages de ports UDP ou TCP</li> <li>- Filtrage et inspection en IPv4 et IPv6,</li> <li>- Failover de connexion Internet,</li> <li>- Prise en compte de paramètre Horaire dans les règles de filtrage,</li> <li>- Doit fournir, via sa console d'administration, des statistiques sur le nombre d'accès aux règles de sécurité,</li> <li>- Doit inclure la possibilité de fonctionner en mode transparent ou routé (natté),</li> <li>- 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,</li> <li>- La création de la politique de sécurité basée sur : <ul style="list-style-type: none"> <li>• Geolocation par pays</li> <li>• Zones</li> <li>• Groupes de Zones</li> <li>• Applications, Groupes d'applications</li> <li>• Catégories d'Applications</li> <li>• Technologies d'Applications</li> <li>• Filtres d'Applications</li> <li>• Utilisateurs et Groupes</li> <li>• Adresses IP, Groupes d'adresses IP, Sous-réseaux IP, Groupes de sous-réseaux IP</li> <li>• Services, Groupes de Services</li> </ul> </li> <li>- 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) : <ul style="list-style-type: none"> <li>• <b>IPS (prévention des intrusions)</b> 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</li> </ul> </li> </ul>	<b>Marque :</b> <b>Référence :</b> <b>Caractéristiques proposées</b>	



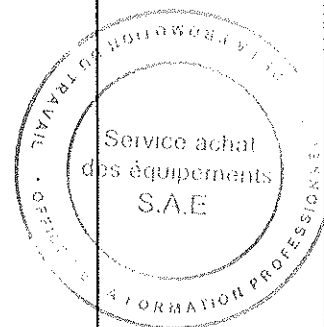
Item	Spécifications techniques	Proposition du soumissionnaire	Appréciation de l'administration
	<p>menaces réseaux existantes et émergentes. Ce module IPS doit avoir deux mécanismes :</p> <ul style="list-style-type: none"> <li>- Détection par signatures ;</li> <li>- Détection par anomalies ;</li> <li>- Capable de faire des analyses comportementales de tout type de trafic ;</li> <li>- Possibilité de créer des signatures personnalisées ;</li> <li>- Mise à jour automatique des signatures IPS ;</li> <li>- Création et affectation des politiques IPS par type de zone ou interface ;</li> <li>- 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) ... ;</li> <li>- Gestion de profils IPS avec association à certains trafics dans la politique de filtrage (IP source, IP destination, service, protocole, réseau...) ;</li> <li>• <b>Filtrage URL</b>, pour assurer le contrôle de l'accès interne aux contenus Web indésirables, non productifs, voire illégaux,</li> <li>• <b>Control Applicatif</b>, afin d'identifier, reconnaître et contrôler les applications dans les flux,</li> </ul>		
	<p><b>Spécifications matérielles et performance :</b></p> <ul style="list-style-type: none"> <li>- Format : Appliance Rackable, 19"</li> <li>- Débit de Prevention des menaces (Firewall niveau 7 avec Contrôle applicatif + IPS + Anti Malware + Sandboxing+ Antispyware + filtrage URL, filtrage de contenu et Journalisation) : <b>2.5 Gbps Minimum</b></li> <li>- Nombre de sessions inspectées simultanées : <b>1 Million Minimum</b></li> <li>- Nombre de nouvelles sessions par seconde : <b>50 000 Minimum</b></li> <li>- Stockage Disque dur dédiée de type SSD de <b>200 GB Minimum</b></li> <li>- Les ports (en dehors des ports de management et de la haute disponibilité) <ul style="list-style-type: none"> <li>• Minimum 8 ports 10/100/1000 BaseT</li> <li>• Minimum 4 ports 1G/10G SFP/SFP+ dont <b>4 avec Transceiver SFP+</b></li> </ul> </li> <li>- Les ports de management et Clustering : <ul style="list-style-type: none"> <li>• Minimum 1 port 10/100/1000 BaseT pour le management</li> <li>• Minimum 1 port console RJ-45</li> <li>• Minimum 1 port USB</li> <li>• Minimum 1 ports 10/100/1000 BaseT pour le HA</li> </ul> </li> </ul> <p><b>2 Alimentations électriques Redondantes Minimum (AC),</b></p>		
	<p><b>Support de la haute disponibilité :</b></p> <ul style="list-style-type: none"> <li>- Actif/Actif avec synchronisation d'état de session,</li> <li>- Actif/Passif,</li> </ul>		
	<p><b>Contrôle applicatif :</b></p> <ul style="list-style-type: none"> <li>- Identification des applications en se basant sur : <ul style="list-style-type: none"> <li>• Signatures</li> </ul> </li> </ul>		



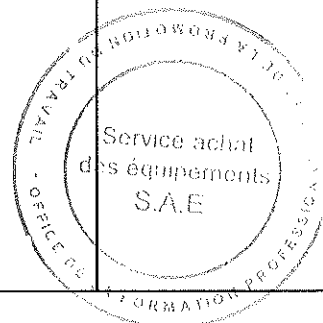
Item	Spécifications techniques	Proposition du soumissionnaire	Appréciation de l'administration
	<ul style="list-style-type: none"> <li>• Décodage du protocole (respecte la spécification du protocole)</li> <li>• Déchiffrement du trafic encapsulé</li> <li>- Identification et contrôle des applications partageant la même connexion</li> <li>- Contrôle de la fonction de transfert de fichiers d'une application</li> <li>- Visibilité du trafic applicatif inconnu à travers l'identification de sa nature : <ul style="list-style-type: none"> <li>• Volume du trafic</li> <li>• Utilisateur et/ou adresses IP</li> <li>• Port utilisé</li> <li>• Contenu associé : fichier, menace ou autre.</li> </ul> </li> <li>- La base de données de contrôle des applications doit contenir plus de <b>3 000</b> applications connues ;</li> </ul> <p>La solution doit pouvoir créer une règle de filtrage avec plusieurs catégories ;</p>		
	<p><b>Identification, authentification des utilisateurs et protection des identités</b></p> <ul style="list-style-type: none"> <li>- Prise en charge des services d'authentification suivants pour l'identification et authentifications des utilisateurs : <ul style="list-style-type: none"> <li>• Active Directory</li> <li>• Kerberos</li> <li>• LDAP</li> <li>• Radius</li> <li>• Base Locale</li> <li>• SAML</li> <li>• Authentification via SSO Kerberos sans agent</li> <li>• Authentification par Certificat client</li> <li>• Portail captif</li> </ul> </li> <li>- Identification des utilisateurs indépendamment : <ul style="list-style-type: none"> <li>• Du terminal (ordinateur, un téléphone intelligent ou une tablette)</li> <li>• Du système d'exploitation utilisé,</li> <li>• Des adresses IP et de la zone (LAN, VPN, hors du périmètre du réseau)</li> </ul> </li> </ul>		
	<p><b>Fonctions Réseau :</b></p> <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> <li>- Support de la fonctionnalité <b>SD-WAN</b> pour le routage avancé des flux sur plusieurs liaisons à base d'application afin d'augmenter la disponibilité et la performance WAN en se basant sur les paramètres de performance (Latence, Perte de packets et jitter) que ce soit lors de</li> </ul>		

5  
H2

Item	Spécifications techniques	Proposition du soumissionnaire	Appréciation de l'administration
	la navigation Internet et pour la communication inter-sites (fonctionnalité et licence à fournir) -		
	<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> <li>-</li> </ul>		
	<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> </ul> Limitation de la bande passante par source, destination, application ou catégorie d'application.		
	<b>Administration et gestion des journaux :</b> <ul style="list-style-type: none"> <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> <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> </ul>		



Item	Spécifications techniques	Proposition du soumissionnaire	Appréciation de l'administration
	<ul style="list-style-type: none"> <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>		
	<p><b>Filtrage URL et Filtrage de contenu</b></p> <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>		
1.2	<p><b>PRESTATION DE SERVICE</b></p> <p>Le prestataire doit proposer dans son offre toutes les prestations nécessaires à la mise en œuvre de la solution de sécurité :</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>- Intégration de la solution dans le réseau de la CMC ;</li> <li>- L'interconnexion du NGFW avec les Switch Datacenter ;</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 d'un an 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 ;</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> </ul> </li> </ul> <p>Manuel d'exploitation ;</p>		



**BORDEREAU DES PRIX – DETAIL ESTIMATIF**

**LOT 3 : Solution de Firewall Nouvelle Génération NGFW de type Appliance pour la CMC TANGER**

Items N°	Désignations	Unité	(1) QTE	(2) Prix unitaire HT/HDD/HTV A	(3) Prix total HT/HDD/HTV A (3) = (1) x (2)	(4) Droits de Douanes sur (3)	(5) Prix total Hors TVA (5) = (3) + (4)	(6) TVA Appliquée sur (5)	(7) Montant TTC (7) = (5) + (6)
1	Solution de Firewall Nouvelle Génération NGFW de type Appliance								
1.1	Firewall	U	1						
1.2	PRESTATION DE SERVICE	ens	1						
<b>MONTANT TOTAL =</b>									

Important : 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 à ce sujet.

Fait à ..... le .....

Signature et cachet du concurrent





**LOT 4 : Solution de Firewall Nouvelle Génération NGFW pour la CMC RABAT**

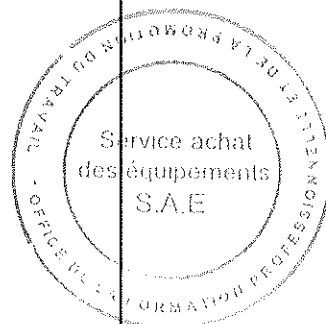
*N.B : les soumissionnaires sont invités à remplir la case 'Proposition du soumissionnaire' en précisant les caractéristiques du matériel. La réponse du soumissionnaire doit être justifiée par des notes explicatives, des fiches techniques (marquer les justifications), ou tout autre moyen pouvant justifier la proposition du soumissionnaire.*

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

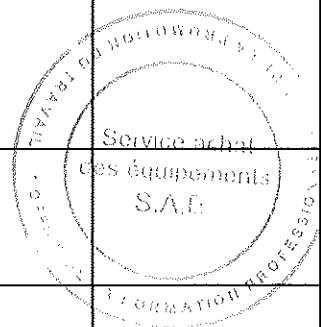
*Les colonnes 'Désignations et caractéristiques techniques' et 'Appréciation de l'administration' ne doivent pas être renseignées ou modifiées.*

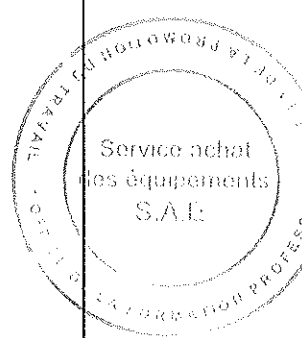
*Le concurrent est tenu à renseigner pour chaque item, la marque, la référence et les caractéristiques des fournitures proposées et ce, dans le cadre de la colonne 'Proposition du soumissionnaire' et la ligne correspondante à l'item.*

Item	Spécifications techniques	Proposition du soumissionnaire	Appréciation de l'administration
<b>1 .</b>	<b>Solution de Firewall Nouvelle Génération NGFW de type Appliance</b>		
<b>1.1</b>	<b>Leader dans Gartner dans la technologie Network Firewall pour les trois années minimum 2019, 2020 et 2021</b>		
	<b>Fonctions Firewall</b> <ul style="list-style-type: none"> <li>- Doit intégrer un système d'exploitation propriétaire sécurisé,</li> <li>- Filtrage de paquets et être doté de la fonction de filtrage dynamique,</li> <li>- Filtrage basé sur les applications niveau 7 en plus des ports/Protocol et par plages de ports UDP ou TCP</li> <li>- Filtrage et inspection en IPv4 et IPv6,</li> <li>- Failover de connexion Internet,</li> <li>- Prise en compte de paramètre Horaire dans les règles de filtrage,</li> <li>- Doit fournir, via sa console d'administration, des statistiques sur le nombre d'accès aux règles de sécurité,</li> <li>- Doit inclure la possibilité de fonctionner en mode transparent ou routé (natté),</li> <li>- 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,</li> <li>- La création de la politique de sécurité basée sur : <ul style="list-style-type: none"> <li>• Geolocation par pays</li> <li>• Zones</li> <li>• Groupes de Zones</li> <li>• Applications, Groupes d'applications</li> <li>• Catégories d'Applications</li> <li>• Technologies d'Applications</li> <li>• Filtres d'Applications</li> <li>• Utilisateurs et Groupes</li> <li>• Adresses IP, Groupes d'adresses IP, Sous-réseaux IP, Groupes de sous-réseaux IP</li> <li>• Services, Groupes de Services</li> </ul> </li> <li>- 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) : <ul style="list-style-type: none"> <li>• <b>IPS (prévention des intrusions)</b> 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</li> </ul> </li> </ul>	<b>Marque :</b> <b>Référence :</b> <b>Caractéristiques proposées</b>	

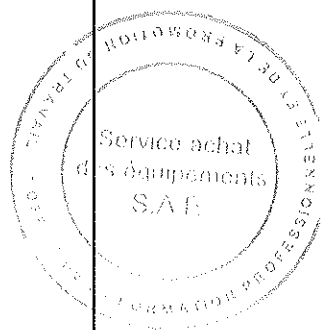


Item	Spécifications techniques	Proposition du soumissionnaire	Appréciation de l'administration
	<p>menaces réseaux existantes et émergentes. Ce module IPS doit avoir deux mécanismes :</p> <ul style="list-style-type: none"> <li>- Détection par signatures ;</li> <li>- Détection par anomalies ;</li> <li>- Capable de faire des analyses comportementales de tout type de trafic ;</li> <li>- Possibilité de créer des signatures personnalisées ;</li> <li>- Mise à jour automatique des signatures IPS ;</li> <li>- Création et affectation des politiques IPS par type de zone ou interface ;</li> <li>- 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) ... ;</li> <li>- Gestion de profils IPS avec association à certains trafics dans la politique de filtrage (IP source, IP destination, service, protocole, réseau...) ;</li> <li>• <b>Filtrage URL</b>, pour assurer le contrôle de l'accès interne aux contenus Web indésirables, non productifs, voire illégaux,</li> <li>• <b>Control Applicatif</b>, afin d'identifier, reconnaître et contrôler les applications dans les flux,</li> </ul>		
	<p><b>Spécifications matérielles et performance :</b></p> <ul style="list-style-type: none"> <li>- Format : Appliance Rackable, 19"</li> <li>- Débit de Prevention des menaces (Firewall niveau 7 avec Contrôle applicatif + IPS + Anti Malware + Sandboxing+ Antispyware + filtrage URL, filtrage de contenu et Journalisation) : <b>2.5 Gbps Minimum</b></li> <li>- Nombre de sessions inspectées simultanées : <b>1 Million Minimum</b></li> <li>- Nombre de nouvelles sessions par seconde : <b>50 000 Minimum</b></li> <li>- Stockage Disque dur dédiée de type SSD de <b>200 GB Minimum</b></li> <li>- Les ports (en dehors des ports de management et de la haute disponibilité) <ul style="list-style-type: none"> <li>• Minimum 8 ports 10/100/1000 BaseT</li> <li>• Minimum 4 ports 1G/10G SFP/SFP+ dont 4 avec Transceiver SFP+</li> </ul> </li> <li>- Les ports de management et Clustering : <ul style="list-style-type: none"> <li>• Minimum 1 port 10/100/1000 BaseT pour le management</li> <li>• Minimum 1 port console RJ-45</li> <li>• Minimum 1 port USB</li> <li>• Minimum 1 ports 10/100/1000 BaseT pour le HA</li> </ul> </li> </ul> <p>2 Alimentations électriques Redondantes Minimum (AC),</p>		
	<p><b>Support de la haute disponibilité :</b></p> <ul style="list-style-type: none"> <li>- Actif/Actif avec synchronisation d'état de session,</li> <li>- Actif/Passif,</li> </ul>		
	<p><b>Contrôle applicatif :</b></p> <ul style="list-style-type: none"> <li>- Identification des applications en se basant sur : <ul style="list-style-type: none"> <li>• Signatures</li> </ul> </li> </ul>		



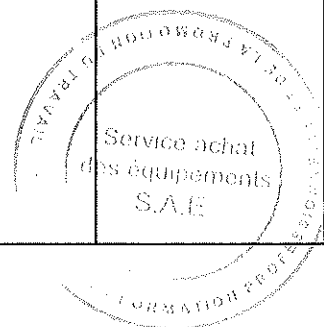
Item	Spécifications techniques	Proposition du soumissionnaire	Appréciation de l'administration
	<ul style="list-style-type: none"> <li>Décodage du protocole (respecte la spécification du protocole)</li> <li>Déchiffrement du trafic encapsulé</li> <li>- Identification et contrôle des applications partageant la même connexion</li> <li>- Contrôle de la fonction de transfert de fichiers d'une application</li> <li>- Visibilité du trafic applicatif inconnu à travers l'identification de sa nature : <ul style="list-style-type: none"> <li>Volume du trafic</li> <li>Utilisateur et/ou adresses IP</li> <li>Port utilisé</li> <li>Contenu associé : fichier, menace ou autre.</li> </ul> </li> <li>- La base de données de contrôle des applications doit contenir plus de 3 000 applications connues ;</li> </ul> <p>La solution doit pouvoir créer une règle de filtrage avec plusieurs catégories ;</p>		
	<p><b>Identification, authentification des utilisateurs et protection des identités</b></p> <ul style="list-style-type: none"> <li>- Prise en charge des services d'authentification suivants pour l'identification et authentifications des utilisateurs : <ul style="list-style-type: none"> <li>Active Directory</li> <li>Kerberos</li> <li>LDAP</li> <li>Radius</li> <li>Base Locale</li> <li>SAML</li> <li>Authentification via SSO Kerberos sans agent</li> <li>Authentification par Certificat client</li> <li>Portail captif</li> </ul> </li> <li>- Identification des utilisateurs indépendamment : <ul style="list-style-type: none"> <li>Du terminal (ordinateur, un téléphone intelligent ou une tablette)</li> <li>Du système d'exploitation utilisé,</li> <li>Des adresses IP et de la zone (LAN, VPN, hors du périmètre du réseau)</li> </ul> </li> </ul>		
	<p><b>Fonctions Réseau :</b></p> <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> <li>- Support de la fonctionnalité <b>SD-WAN</b> pour le routage avancé des flux sur plusieurs liaisons à base d'application afin d'augmenter la</li> </ul>		

Item	Spécifications techniques	Proposition du soumissionnaire	Appréciation de l'administration
	<p>disponibilité et la performance WAN en se basant sur les paramètres de performance (Latence, Perte de packets et jitter) que ce soit lors de la navigation Internet et pour la communication inter-sites (fonctionnalité et licence à fournir)</p> <p>-</p>		
	<p><b>Fonction VPN :</b></p> <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> <li>-</li> </ul>		
	<p><b>Gestion de la bande passante :</b></p> <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> </ul> <p>Limitation de la bande passante par source, destination, application ou catégorie d'application.</p>		
	<p><b>Administration et gestion des journaux :</b></p> <ul style="list-style-type: none"> <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> <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> </ul>		



✓  
H2

Item	Spécifications techniques	Proposition du soumissionnaire	Appréciation de l'administration
	<ul style="list-style-type: none"> <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>		
	<p><b>Filtrage URL et Filtrage de contenu</b></p> <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>		
<b>1.2</b>	<p><b>PRESTATION DE SERVICE</b></p> <p>Le prestataire doit proposer dans son offre toutes les prestations nécessaires à la mise en œuvre de la solution de sécurité :</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>- Intégration de la solution dans le réseau de la CMC ;</li> <li>- L'interconnexion du NGFW avec les Switch Datacenter ;</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 d'un an avec un délai de prise en charge de <b>2 heures</b> après déclaration de l'incident et un délai de <b>4 heures</b> de résolution ou de contournement du problème ;</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> </ul> </li> </ul> <p>Manuel d'exploitation ;</p>		



## BORDEREAU DES PRIX – DETAIL ESTIMATIF

LOT 4 : Solution de Firewall Nouvelle Génération NGFW de type Appliance pour la CMC  
RABAT

Items N°	Désignations	Unité	(1) QTE	(2) Prix unitaire HT/HDD/HTV A	(3) Prix total HT/HDD/HTV A (3) = (1) x (2)	(4) Droits de Douanes sur (3)	(5) Prix total Hors TVA (5) = (3)+(4)	(6) TVA Appliquée sur (5)	(7) Montant TTC (7) = (5)+(6)
1	Solution de Firewall Nouvelle Génération NGFW de type Appliance								
1.1	Firewall	U	1						
1.2	PRESTATION DE SERVICE	ens	1						
MONTANT TOTAL =									

Important : 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 à ce sujet.

Fait à ..... le .....

Signature et cachet du concurrent



Handwritten marks: a checkmark and the number 112.

**LOT 5 : Solution de Firewall Nouvelle Génération NGFW pour la CMC BENI MELLAL**

*N.B : les soumissionnaires sont invités à remplir la case 'Proposition du soumissionnaire' en précisant les caractéristiques du matériel. La réponse du soumissionnaire doit être justifiée par des notes explicatives, des fiches techniques (marquer les justifications), ou tout autre moyen pouvant justifier la proposition du soumissionnaire.*

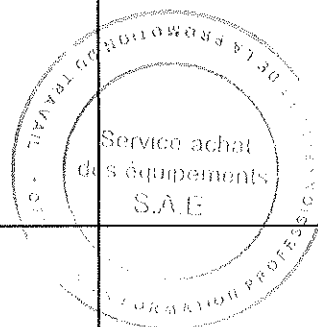
*Tout article ne répondant pas aux spécifications demandées sera déclaré non-conforme.*

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

*Le concurrent est tenu à 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.*

Item	Spécifications techniques	Proposition du soumissionnaire	Appréciation de l'administration
1 .	<b>Solution de Firewall Nouvelle Génération NGFW de type Appliance</b>		
1.1-	<b>Leader dans Gartner dans la technologie Network Firewall pour les trois années minimum 2019, 2020 et 2021</b>		
	<b>Fonctions Firewall</b> <ul style="list-style-type: none"> <li>- Doit intégrer un système d'exploitation propriétaire sécurisé,</li> <li>- Filtrage de paquets et être doté de la fonction de filtrage dynamique,</li> <li>- Filtrage basé sur les applications niveau 7 en plus des ports/Protocol et par plages de ports UDP ou TCP</li> <li>- Filtrage et inspection en IPv4 et IPv6,</li> <li>- Failover de connexion Internet,</li> <li>- Prise en compte de paramètre Horaire dans les règles de filtrage,</li> <li>- Doit fournir, via sa console d'administration, des statistiques sur le nombre d'accès aux règles de sécurité,</li> <li>- Doit inclure la possibilité de fonctionner en mode transparent ou routé (natté),</li> <li>- 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,</li> <li>- La création de la politique de sécurité basée sur : <ul style="list-style-type: none"> <li>• Geolocation par pays</li> <li>• Zones</li> <li>• Groupes de Zones</li> <li>• Applications, Groupes d'applications</li> <li>• Catégories d'Applications</li> <li>• Technologies d'Applications</li> <li>• Filtres d'Applications</li> <li>• Utilisateurs et Groupes</li> <li>• Adresses IP, Groupes d'adresses IP, Sous-réseaux IP, Groupes de sous-réseaux IP</li> <li>• Services, Groupes de Services</li> </ul> </li> <li>- 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) : <ul style="list-style-type: none"> <li>• <b>IPS (prévention des intrusions)</b> pour se protéger contre les menaces réseau telles que vers, chevaux de Troie et autres programmes malveillants. Le système de prévention des</li> </ul> </li> </ul>	<b>Marque :</b> <b>Référence :</b> <b>Caractéristiques proposées</b>	

Item	Spécifications techniques	Proposition du soumissionnaire	Appréciation de l'administration
	<p>intrusions (IPS) doit aussi apporter une protection contre les menaces réseaux existantes et émergentes. Ce module IPS doit avoir deux mécanismes :</p> <ul style="list-style-type: none"> <li>- Détection par signatures ;</li> <li>- Détection par anomalies ;</li> <li>- Capable de faire des analyses comportementales de tout type de trafic ;</li> <li>- Possibilité de créer des signatures personnalisées ;</li> <li>- Mise à jour automatique des signatures IPS ;</li> <li>- Création et affectation des politiques IPS par type de zone ou interface ;</li> <li>- 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) ... ;</li> <li>- Gestion de profils IPS avec association à certains trafics dans la politique de filtrage (IP source, IP destination, service, protocole, réseau...) ;</li> <li>• <b>Filtrage URL</b>, pour assurer le contrôle de l'accès interne aux contenus Web indésirables, non productifs, voire illégaux,</li> <li>• <b>Control Applicatif</b>, afin d'identifier, reconnaître et contrôler les applications dans les flux,</li> </ul>		
	<p><b>Spécifications matérielles et performance :</b></p> <ul style="list-style-type: none"> <li>- Format : Appliance Rackable, 19"</li> <li>- Débit de Prevention des menaces (Firewall niveau 7 avec Contrôle applicatif + IPS + Anti Malware + Sandboxing+ Antispyware + filtrage URL, filtrage de contenu et Journalisation) : <b>2.5 Gbps Minimum</b></li> <li>- Nombre de sessions inspectées simultanées : <b>1 Million Minimum</b></li> <li>- Nombre de nouvelles sessions par seconde : <b>50 000 Minimum</b></li> <li>- Stockage Disque dur dédiée de type SSD de <b>200 GB Minimum</b></li> <li>- Les ports (en dehors des ports de management et de la haute disponibilité) <ul style="list-style-type: none"> <li>• Minimum 8 ports 10/100/1000 BaseT</li> <li>• Minimum 4 ports 1G/10G SFP/SFP+ dont <b>4 avec Transceiver SFP+</b></li> </ul> </li> <li>- Les ports de management et Clustering : <ul style="list-style-type: none"> <li>• Minimum 1 port 10/100/1000 BaseT pour le management</li> <li>• Minimum 1 port console RJ-45</li> <li>• Minimum 1 port USB</li> <li>• Minimum 1 ports 10/100/1000 BaseT pour le HA</li> </ul> </li> </ul> <p><b>2 Alimentations électriques Redondantes Minimum (AC),</b></p>		
	<p><b>Support de la haute disponibilité :</b></p> <ul style="list-style-type: none"> <li>- Actif/Actif avec synchronisation d'état de session,</li> <li>- Actif/Passif,</li> </ul>		
	<p><b>Contrôle applicatif :</b></p> <ul style="list-style-type: none"> <li>- Identification des applications en se basant sur :</li> </ul>		



✓  
H2

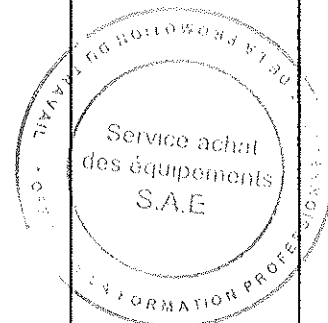


Item	Spécifications techniques	Proposition du soumissionnaire	Appréciation de l'administration
	<ul style="list-style-type: none"> <li>• Signatures</li> <li>• Décodage du protocole (respecte la spécification du protocole)</li> <li>• Déchiffrement du trafic encapsulé</li> <li>- Identification et contrôle des applications partageant la même connexion</li> <li>- Contrôle de la fonction de transfert de fichiers d'une application</li> <li>- Visibilité du trafic applicatif inconnu à travers l'identification de sa nature : <ul style="list-style-type: none"> <li>• Volume du trafic</li> <li>• Utilisateur et/ou adresses IP</li> <li>• Port utilisé</li> <li>• Contenu associé : fichier, menace ou autre.</li> </ul> </li> <li>- La base de données de contrôle des applications doit contenir plus de 3 000 applications connues ;</li> </ul> <p>La solution doit pouvoir créer une règle de filtrage avec plusieurs catégories ;</p>		
	<p><b>Identification, authentification des utilisateurs et protection des identités</b></p> <ul style="list-style-type: none"> <li>- Prise en charge des services d'authentification suivants pour l'identification et authentifications des utilisateurs : <ul style="list-style-type: none"> <li>• Active Directory</li> <li>• Kerberos</li> <li>• LDAP</li> <li>• Radius</li> <li>• Base Locale</li> <li>• SAML</li> <li>• Authentification via SSO Kerberos sans agent</li> <li>• Authentification par Certificat client</li> <li>• Portail captif</li> </ul> </li> <li>- Identification des utilisateurs indépendamment : <ul style="list-style-type: none"> <li>• Du terminal (ordinateur, un téléphone intelligent ou une tablette)</li> <li>• Du système d'exploitation utilisé,</li> <li>• Des adresses IP et de la zone (LAN, VPN, hors du périmètre du réseau)</li> </ul> </li> </ul>		
	<p><b>Fonctions Réseau :</b></p> <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>		

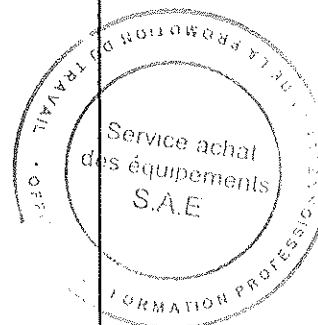


5  
H2

Item	Spécifications techniques	Proposition du soumissionnaire	Appréciation de l'administration
	<ul style="list-style-type: none"> <li>- Support de la fonctionnalité <b>SD-WAN</b> pour le routage avancé des flux sur plusieurs liaisons à base d'application afin d'augmenter la disponibilité et la performance WAN en se basant sur les paramètres de performance (Latence, Perte de packets et jitter) que ce soit lors de la navigation Internet et pour la communication inter-sites (<b>fonctionnalité et licence à fournir</b>)</li> <li>-</li> </ul>		
	<b>Fonction VPN :</b> <ul style="list-style-type: none"> <li>- VPN IPSec site-site, client-site et hub &amp; Spoke. (<b>Fonctionnalité et licence à fournir</b>)</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> <li>-</li> </ul>		
	<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> </ul> Limitation de la bande passante par source, destination, application ou catégorie d'application.		
	<b>Administration et gestion des journaux :</b> <ul style="list-style-type: none"> <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> <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> </ul>		



Item	Spécifications techniques	Proposition du soumissionnaire	Appréciation de l'administration
	<ul style="list-style-type: none"> <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>		
	<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>		
1.2	<b>PRESTATION DE SERVICE</b> Le prestataire doit proposer dans son offre toutes les prestations nécessaires à la mise en œuvre de la solution de sécurité : <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>- Intégration de la solution dans le réseau de la CMC ;</li> <li>- L'interconnexion du NGFW avec les Switch Datacenter ;</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 d'un an 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 ;</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> </ul> </li> </ul> <b>Manuel d'exploitation ;</b>		



Handwritten marks: a checkmark and the signature 'HSE'.

**BORDEREAU DES PRIX – DETAIL ESTIMATIF**

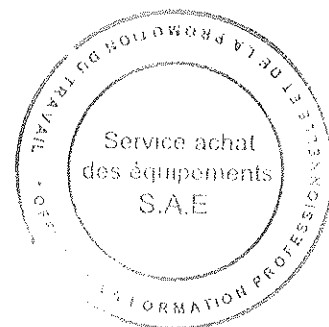
**LOT 5 : Solution de Firewall Nouvelle Génération NGFW de type Appliance pour la CMC BENI MELLAL**

Items N°	Désignations	Unité	(1) QTE	(2) Prix unitaire HT/HDD/HTV A	(3) Prix total HT/HDD/HTV A (3) = (1) x (2)	(4) Droits de Douanes sur (3)	(5) Prix total Hors TVA (5) = (3) + (4)	(6) TVA Appliquée sur (5)	(7) Montant TTC (7) = (5) + (6)
1	Solution de Firewall Nouvelle Génération NGFW de type Appliance								
1.1	Firewall	U	1						
1.2	PRESTATION DE SERVICE	ens	1						
<b>MONTANT TOTAL =</b>									

Important : 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 à ce sujet.

Fait à ..... le .....

Signature et cachet du concurrent



5

A2

**LOT 6 : Solution de Firewall Nouvelle Génération NGFW pour la CMC MARRAKECH**

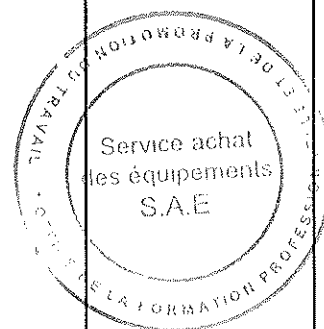
N.B : les soumissionnaires sont invités à remplir la case 'Proposition du soumissionnaire' en précisant les caractéristiques du matériel. La réponse du soumissionnaire doit être justifiée par des notes explicatives, des fiches techniques (marquer les justifications), ou tout autre moyen pouvant justifier la proposition du soumissionnaire.

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

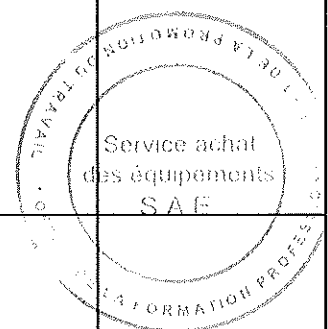
Les colonnes 'Désignations et caractéristiques techniques' et 'Appréciation de l'administration' ne doivent pas être renseignées ou modifiées.

Le concurrent est tenu à 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.

Item	Spécifications techniques	Proposition du soumissionnaire	Appréciation de l'administration
<b>1 .</b>	<b>Solution de Firewall Nouvelle Génération NGFW de type Appliance</b>		
<b>1.1</b>	<b>Leader dans Gartner dans la technologie Network Firewall pour les trois années minimum 2019, 2020 et 2021</b>		
	<b>Fonctions Firewall</b> <ul style="list-style-type: none"> <li>- Doit intégrer un système d'exploitation propriétaire sécurisé,</li> <li>- Filtrage de paquets et être doté de la fonction de filtrage dynamique,</li> <li>- Filtrage basé sur les applications niveau 7 en plus des ports/Protocol et par plages de ports UDP ou TCP</li> <li>- Filtrage et inspection en IPv4 et IPv6,</li> <li>- Failover de connexion Internet,</li> <li>- Prise en compte de paramètre Horaire dans les règles de filtrage,</li> <li>- Doit fournir, via sa console d'administration, des statistiques sur le nombre d'accès aux règles de sécurité,</li> <li>- Doit inclure la possibilité de fonctionner en mode transparent ou routé (natté),</li> <li>- 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,</li> <li>- La création de la politique de sécurité basée sur : <ul style="list-style-type: none"> <li>• Geolocation par pays</li> <li>• Zones</li> <li>• Groupes de Zones</li> <li>• Applications, Groupes d'applications</li> <li>• Catégories d'Applications</li> <li>• Technologies d'Applications</li> <li>• Filtres d'Applications</li> <li>• Utilisateurs et Groupes</li> <li>• Adresses IP, Groupes d'adresses IP, Sous-réseaux IP, Groupes de sous-réseaux IP</li> <li>• Services, Groupes de Services</li> </ul> </li> <li>- 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) : <ul style="list-style-type: none"> <li>• <b>IPS (prévention des intrusions)</b> 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</li> </ul> </li> </ul>	<b>Marque :</b> <b>Référence :</b> <b>Caractéristiques proposées</b>	

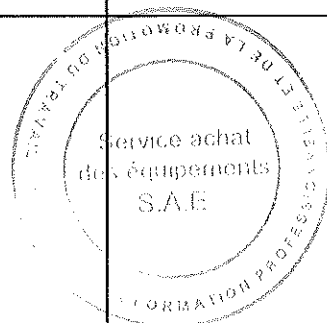


Item	Spécifications techniques	Proposition du soumissionnaire	Appréciation de l'administration
	<p>menaces réseaux existantes et émergentes. Ce module IPS doit avoir deux mécanismes :</p> <ul style="list-style-type: none"> <li>- Détection par signatures ;</li> <li>- Détection par anomalies ;</li> <li>- Capable de faire des analyses comportementales de tout type de trafic ;</li> <li>- Possibilité de créer des signatures personnalisées ;</li> <li>- Mise à jour automatique des signatures IPS ;</li> <li>- Création et affectation des politiques IPS par type de zone ou interface ;</li> <li>- 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) ... ;</li> <li>- Gestion de profils IPS avec association à certains trafics dans la politique de filtrage (IP source, IP destination, service, protocole, réseau...) ;</li> <li>• <b>Filtrage URL</b>, pour assurer le contrôle de l'accès interne aux contenus Web indésirables, non productifs, voire illégaux,</li> <li>• <b>Control Applicatif</b>, afin d'identifier, reconnaître et contrôler les applications dans les flux,</li> </ul>		
	<p><b>Spécifications matérielles et performance :</b></p> <ul style="list-style-type: none"> <li>- Format : Appliance Rackable, 19"</li> <li>- Débit de Prevention des menaces (Firewall niveau 7 avec Contrôle applicatif + IPS + Anti Malware + Sandboxing+ Antispyware + filtrage URL, filtrage de contenu et Journalisation) : 2.5 Gbps Minimum</li> <li>- Nombre de sessions inspectées simultanées : 1 Million Minimum</li> <li>- Nombre de nouvelles sessions par seconde : 50 000 Minimum</li> <li>- Stockage Disque dur dédiée de type SSD de 200 GB Minimum</li> <li>- Les ports (en dehors des ports de management et de la haute disponibilité) <ul style="list-style-type: none"> <li>• Minimum 8 ports 10/100/1000 BaseT</li> <li>• Minimum 4 ports 1G/10G SFP/SFP+ dont 4 avec Transceiver SFP+</li> </ul> </li> <li>- Les ports de management et Clustering : <ul style="list-style-type: none"> <li>• Minimum 1 port 10/100/1000 BaseT pour le management</li> <li>• Minimum 1 port console RJ-45</li> <li>• Minimum 1 port USB</li> <li>• Minimum 1 ports 10/100/1000 BaseT pour le HA</li> </ul> </li> </ul> <p>2 Alimentations électriques Redondantes Minimum (AC),</p>		
	<p><b>Support de la haute disponibilité :</b></p> <ul style="list-style-type: none"> <li>- Actif/Actif avec synchronisation d'état de session,</li> <li>- Actif/Passif,</li> </ul>		
	<p><b>Contrôle applicatif :</b></p> <ul style="list-style-type: none"> <li>- Identification des applications en se basant sur : <ul style="list-style-type: none"> <li>• Signatures</li> </ul> </li> </ul>		

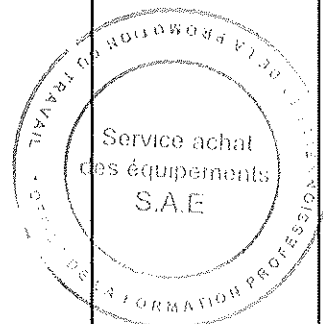


F  
A2

Item	Spécifications techniques	Proposition du soumissionnaire	Appréciation de l'administration
	<ul style="list-style-type: none"> <li>• Décodage du protocole (respecte la spécification du protocole)</li> <li>• Déchiffrement du trafic encapsulé</li> <li>- Identification et contrôle des applications partageant la même connexion</li> <li>- Contrôle de la fonction de transfert de fichiers d'une application</li> <li>- Visibilité du trafic applicatif inconnu à travers l'identification de sa nature :               <ul style="list-style-type: none"> <li>• Volume du trafic</li> <li>• Utilisateur et/ou adresses IP</li> <li>• Port utilisé</li> <li>• Contenu associé : fichier, menace ou autre.</li> </ul> </li> <li>- La base de données de contrôle des applications doit contenir plus de 3 000 applications connues ;</li> </ul> <p>La solution doit pouvoir créer une règle de filtrage avec plusieurs catégories ;</p>		
	<p><b>Identification, authentification des utilisateurs et protection des identités</b></p> <ul style="list-style-type: none"> <li>- Prise en charge des services d'authentification suivants pour l'identification et authentifications des utilisateurs :               <ul style="list-style-type: none"> <li>• Active Directory</li> <li>• Kerberos</li> <li>• LDAP</li> <li>• Radius</li> <li>• Base Locale</li> <li>• SAML</li> <li>• Authentification via SSO Kerberos sans agent</li> <li>• Authentification par Certificat client</li> <li>• Portail captif</li> </ul> </li> <li>- Identification des utilisateurs indépendamment :               <ul style="list-style-type: none"> <li>• Du terminal (ordinateur, un téléphone intelligent ou une tablette)</li> <li>• Du système d'exploitation utilisé,</li> <li>• Des adresses IP et de la zone (LAN, VPN, hors du périmètre du réseau)</li> </ul> </li> </ul>		
	<p><b>Fonctions Réseau :</b></p> <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> <li>- Support de la fonctionnalité <b>SD-WAN</b> pour le routage avancé des flux sur plusieurs liaisons à base d'application afin d'augmenter la disponibilité et la performance WAN en se basant sur les paramètres de performance (Latence, Perte de packets et jitter) que ce soit lors de</li> </ul>		



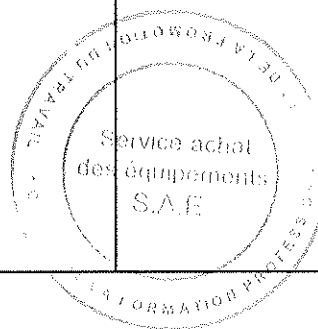
Item	Spécifications techniques	Proposition du soumissionnaire	Appréciation de l'administration
	la navigation Internet et pour la communication inter-sites (fonctionnalité et licence à fournir)		
	<b>Fonction VPN :</b> <ul style="list-style-type: none"> <li>- VPN IPSec site-site, client-site et hub &amp; 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>		
	<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> </ul> Limitation de la bande passante par source, destination, application ou catégorie d'application.		
	<b>Administration et gestion des journaux :</b> <ul style="list-style-type: none"> <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> <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> </ul>		



7  
A2



Item	Spécifications techniques	Proposition du soumissionnaire	Appréciation de l'administration
	<ul style="list-style-type: none"> <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>		
	<p><b>Filtrage URL et Filtrage de contenu</b></p> <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>		
<b>1.2</b>	<p><b>PRESTATION DE SERVICE</b></p> <p>Le prestataire doit proposer dans son offre toutes les prestations nécessaires à la mise en œuvre de la solution de sécurité :</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>- Intégration de la solution dans le réseau de la CMC ;</li> <li>- L'interconnexion du NGFW avec les Switch Datacenter ;</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 d'un an avec un délai de prise en charge de <b>2 heures</b> après déclaration de l'incident et un délai de <b>4 heures</b> de résolution ou de contournement du problème ;</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> </ul> </li> </ul> <p>Manuel d'exploitation ;</p>		



**BORDEREAU DES PRIX – DETAIL ESTIMATIF**

**LOT 6 : Solution de Firewall Nouvelle Génération NGFW de type Appliance pour la CMC MARRAKECH**

Items N°	Désignations	Unité	(1) QTE	(2) Prix unitaire HT/HDD/HTV A	(3) Prix total HT/HDD/HTV A (3) = (1) x (2)	(4) Droits de Douanes sur (3)	(5) Prix total Hors TVA (5) = (3) + (4)	(6) TVA Appliquée sur (5)	(7) Montant TTC (7) = (5) + (6)
1	Solution de Firewall Nouvelle Génération NGFW de type Appliance								
1.1	Firewall	U	1						
1.2	PRESTATION DE SERVICE	ens	1						
<b>MONTANT TOTAL =</b>									

Important : 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 à ce sujet.

Fait à ..... le .....

Signature et cachet du concurrent



## LOT 7 : Solution de Firewall Nouvelle Génération NGFW pour la CMC CASABLANCA

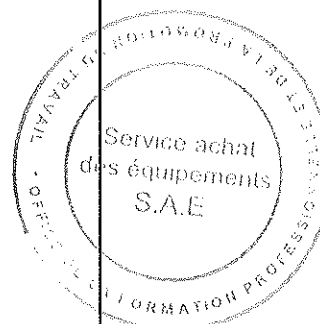
N.B : les soumissionnaires sont invités à remplir la case 'Proposition du soumissionnaire' en précisant les caractéristiques du matériel. La réponse du soumissionnaire doit être justifiée par des notes explicatives, des fiches techniques (marquer les justifications), ou tout autre moyen pouvant justifier la proposition du soumissionnaire.

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.

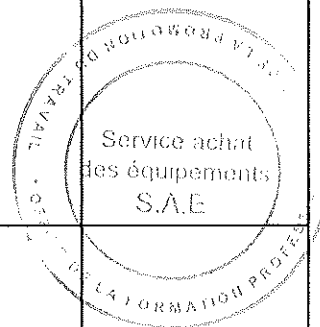
Le concurrent est tenu à renseigner pour chaque item, la marque, la référence et les caractéristiques des fournitures proposées et ce, dans le cadre de la colonne 'Proposition du soumissionnaire' et la ligne correspondante à l'item.

Item	Spécifications techniques	Proposition du soumissionnaire	Appréciation de l'administration
<b>1 .</b>	<b>Solution de Firewall Nouvelle Génération NGFW de type Appliance</b>		
<b>1.1</b>	<b>Leader dans Gartner dans la technologie Network Firewall pour les trois années minimum 2019, 2020 et 2021</b>		
	<b>Fonctions Firewall</b> <ul style="list-style-type: none"> <li>- Doit intégrer un système d'exploitation propriétaire sécurisé,</li> <li>- Filtrage de paquets et être doté de la fonction de filtrage dynamique,</li> <li>- Filtrage basé sur les applications niveau 7 en plus des ports/Protocol et par plages de ports UDP ou TCP</li> <li>- Filtrage et inspection en IPv4 et IPv6,</li> <li>- Failover de connexion Internet,</li> <li>- Prise en compte de paramètre Horaire dans les règles de filtrage,</li> <li>- Doit fournir, via sa console d'administration, des statistiques sur le nombre d'accès aux règles de sécurité,</li> <li>- Doit inclure la possibilité de fonctionner en mode transparent ou routé (natté),</li> <li>- 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,</li> <li>- La création de la politique de sécurité basée sur : <ul style="list-style-type: none"> <li>• Geolocation par pays</li> <li>• Zones</li> <li>• Groupes de Zones</li> <li>• Applications, Groupes d'applications</li> <li>• Catégories d'Applications</li> <li>• Technologies d'Applications</li> <li>• Filtres d'Applications</li> <li>• Utilisateurs et Groupes</li> <li>• Adresses IP, Groupes d'adresses IP, Sous-réseaux IP, Groupes de sous-réseaux IP</li> <li>• Services, Groupes de Services</li> </ul> </li> <li>- 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) : <ul style="list-style-type: none"> <li>• <b>IPS (prévention des intrusions)</b> pour se protéger contre les menaces réseau telles que vers, chevaux de Troie et autres programmes malveillants. Le système de prévention des</li> </ul> </li> </ul>	<b>Marque :</b> <b>Référence :</b> <b>Caractéristiques proposées</b>	



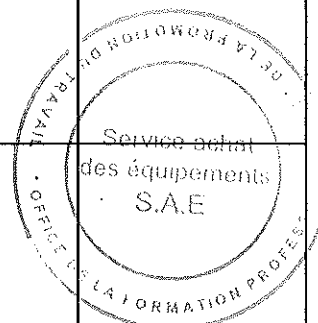
Handwritten marks: a checkmark and the letters 'Hx'.

Item	Spécifications techniques	Proposition du soumissionnaire	Appréciation de l'administration
	<p>intrusions (IPS) doit aussi apporter une protection contre les menaces réseaux existantes et émergentes. Ce module IPS doit avoir deux mécanismes :</p> <ul style="list-style-type: none"> <li>- Détection par signatures ;</li> <li>- Détection par anomalies ;</li> <li>- Capable de faire des analyses comportementales de tout type de trafic ;</li> <li>- Possibilité de créer des signatures personnalisées ;</li> <li>- Mise à jour automatique des signatures IPS ;</li> <li>- Création et affectation des politiques IPS par type de zone ou interface ;</li> <li>- 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) ... ;</li> <li>- Gestion de profils IPS avec association à certains trafics dans la politique de filtrage (IP source, IP destination, service, protocole, réseau...) ;</li> <li>• <b>Filtrage URL</b>, pour assurer le contrôle de l'accès interne aux contenus Web indésirables, non productifs, voire illégaux,</li> <li>• <b>Control Applicatif</b>, afin d'identifier, reconnaître et contrôler les applications dans les flux,</li> </ul>		
	<p><b>Spécifications matérielles et performance :</b></p> <ul style="list-style-type: none"> <li>- Format : Appliance Rackable, 19"</li> <li>- Débit de Prevention des menaces (Firewall niveau 7 avec Contrôle applicatif + IPS + Anti Malware + Sandboxing+ Antispyware + filtrage URL, filtrage de contenu et Journalisation) : <b>2.5 Gbps Minimum</b></li> <li>- Nombre de sessions inspectées simultanées : <b>1 Million Minimum</b></li> <li>- Nombre de nouvelles sessions par seconde : <b>50 000 Minimum</b></li> <li>- Stockage Disque dur dédiée de type SSD de <b>200 GB Minimum</b></li> <li>- Les ports (en dehors des ports de management et de la haute disponibilité) <ul style="list-style-type: none"> <li>• Minimum 8 ports 10/100/1000 BaseT</li> <li>• Minimum 4 ports 1G/10G SFP/SFP+ dont 4 avec Transceiver SFP+</li> </ul> </li> <li>- Les ports de management et Clustering : <ul style="list-style-type: none"> <li>• Minimum 1 port 10/100/1000 BaseT pour le management</li> <li>• Minimum 1 port console RJ-45</li> <li>• Minimum 1 port USB</li> <li>• Minimum 1 ports 10/100/1000 BaseT pour le HA</li> </ul> </li> <li>2 Alimentations électriques Redondantes Minimum (AC),</li> </ul>		
	<p><b>Support de la haute disponibilité :</b></p> <ul style="list-style-type: none"> <li>- Actif/Actif avec synchronisation d'état de session,</li> <li>- Actif/Passif,</li> <li>-</li> </ul>		
	<p><b>Contrôle applicatif :</b></p>		

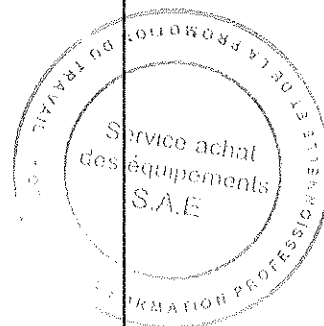


✓  
Hte

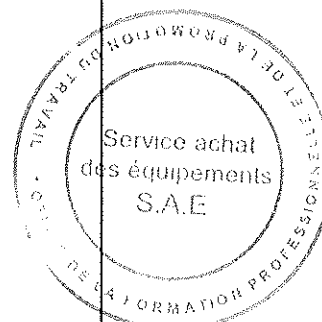
Item	Spécifications techniques	Proposition du soumissionnaire	Appréciation de l'administration
	<ul style="list-style-type: none"> <li>- Identification des applications en se basant sur : <ul style="list-style-type: none"> <li>• Signatures</li> <li>• Décodage du protocole (respecte la spécification du protocole)</li> <li>• Déchiffrement du trafic encapsulé</li> </ul> </li> <li>- Identification et contrôle des applications partageant la même connexion</li> <li>- Contrôle de la fonction de transfert de fichiers d'une application</li> <li>- Visibilité du trafic applicatif inconnu à travers l'identification de sa nature : <ul style="list-style-type: none"> <li>• Volume du trafic</li> <li>• Utilisateur et/ou adresses IP</li> <li>• Port utilisé</li> <li>• Contenu associé : fichier, menace ou autre.</li> </ul> </li> <li>- La base de données de contrôle des applications doit contenir plus de <b>3 000</b> applications connues ;</li> </ul> <p>La solution doit pouvoir créer une règle de filtrage avec plusieurs catégories ;</p>		
	<p><b>Identification, authentification des utilisateurs et protection des identités</b></p> <ul style="list-style-type: none"> <li>- Prise en charge des services d'authentification suivants pour l'identification et authentifications des utilisateurs : <ul style="list-style-type: none"> <li>• Active Directory</li> <li>• Kerberos</li> <li>• LDAP</li> <li>• Radius</li> <li>• Base Locale</li> <li>• SAML</li> <li>• Authentification via SSO Kerberos sans agent</li> <li>• Authentification par Certificat client</li> <li>• Portail captif</li> </ul> </li> <li>- Identification des utilisateurs indépendamment : <ul style="list-style-type: none"> <li>• Du terminal (ordinateur, un téléphone intelligent ou une tablette)</li> <li>• Du système d'exploitation utilisé,</li> <li>• Des adresses IP et de la zone (LAN, VPN, hors du périmètre du réseau)</li> </ul> </li> </ul>		
	<p><b>Fonctions Réseau :</b></p> <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>		



Item	Spécifications techniques	Proposition du soumissionnaire	Appréciation de l'administration
	<ul style="list-style-type: none"> <li>- Support de la fonctionnalité <b>SD-WAN</b> pour le routage avancé des flux sur plusieurs liaisons à base d'application afin d'augmenter la disponibilité et la performance WAN en se basant sur les paramètres de performance (Latence, Perte de packets et jitter) que ce soit lors de la navigation Internet et pour la communication inter-sites (<b>fonctionnalité et licence à fournir</b>)</li> </ul>		
	<p><b>Fonction VPN :</b></p> <ul style="list-style-type: none"> <li>- VPN IPSec site-site, client-site et hub &amp; Spoke. (<b>Fonctionnalité et licence à fournir</b>)</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>		
	<p><b>Gestion de la bande passante :</b></p> <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> </ul> <p>Limitation de la bande passante par source, destination, application ou catégorie d'application.</p>		
	<p><b>Administration et gestion des journaux :</b></p> <ul style="list-style-type: none"> <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> <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> </ul>		



Item	Spécifications techniques	Proposition du soumissionnaire	Appréciation de l'administration
	<ul style="list-style-type: none"> <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>		
	<p><b>Filtrage URL et Filtrage de contenu</b></p> <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>		
1.2	<p><b>PRESTATION DE SERVICE</b></p> <p>Le prestataire doit proposer dans son offre toutes les prestations nécessaires à la mise en œuvre de la solution de sécurité :</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>- Intégration de la solution dans le réseau de la CMC ;</li> <li>- L'interconnexion du NGFW avec les Switch Datacenter ;</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 d'un an 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 ;</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> </ul> </li> </ul> <p>Manuel d'exploitation ;</p>		



**BORDEREAU DES PRIX – DETAIL ESTIMATIF**

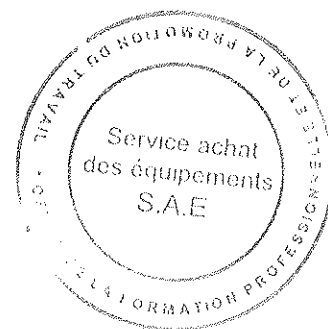
**LOT 7 : Solution de Firewall Nouvelle Génération NGFW pour la CMC CASABLANCA**

Items N°	Désignations	Unité	(1) QTE	(2) Prix unitaire HT/HDD/HTV A	(3) Prix total HT/HDD/HTV A (3) = (1) x (2)	(4) Droits de Douanes sur (3)	(5) Prix total Hors TVA (5) = (3)+(4)	(6) TVA Appliqué e sur (5)	(7) Montant TTC (7) = (5)+(6)
1	Solution de Firewall Nouvelle Génération NGFW de type Appliance								
1.1	Firewall	U	1						
1.2	PRESTATION DE SERVICE	ens	1						
<b>MONTANT TOTAL =</b>									

**Important : 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 à ce sujet.**

Fait à ..... le .....

**Signature et cachet du concurrent**



✓



**LOT 8 : Solution de Firewall Nouvelle Génération NGFW pour la CMC FES**

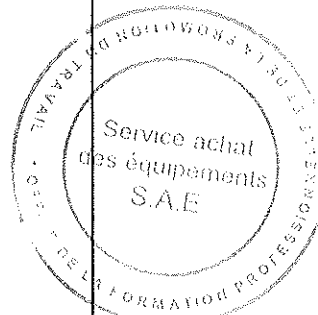
N.B : les soumissionnaires sont invités à remplir la case 'Proposition du soumissionnaire' en précisant les caractéristiques du matériel. La réponse du soumissionnaire doit être justifiée par des notes explicatives, des fiches techniques (marquer les justifications), ou tout autre moyen pouvant justifier la proposition du soumissionnaire.

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 à 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.

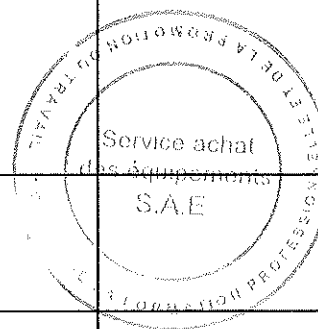
Item	Spécifications techniques	Proposition du soumissionnaire	Appréciation de l'administration
<b>1 .</b>	<b>Solution de Firewall Nouvelle Génération NGFW de type Appliance</b>		
<b>1.1</b>	<b>Leader dans Gartner dans la technologie Network Firewall pour les trois années minimum 2019, 2020 et 2021</b>		
	<b>Fonctions Firewall</b> <ul style="list-style-type: none"> <li>- Doit intégrer un système d'exploitation propriétaire sécurisé,</li> <li>- Filtrage de paquets et être doté de la fonction de filtrage dynamique,</li> <li>- Filtrage basé sur les applications niveau 7 en plus des ports/Protocol et par plages de ports UDP ou TCP</li> <li>- Filtrage et inspection en IPv4 et IPv6,</li> <li>- Failover de connexion Internet,</li> <li>- Prise en compte de paramètre Horaire dans les règles de filtrage,</li> <li>- Doit fournir, via sa console d'administration, des statistiques sur le nombre d'accès aux règles de sécurité,</li> <li>- Doit inclure la possibilité de fonctionner en mode transparent ou routé (natté),</li> <li>- 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,</li> <li>- La création de la politique de sécurité basée sur : <ul style="list-style-type: none"> <li>• Geolocation par pays</li> <li>• Zones</li> <li>• Groupes de Zones</li> <li>• Applications, Groupes d'applications</li> <li>• Catégories d'Applications</li> <li>• Technologies d'Applications</li> <li>• Filtres d'Applications</li> <li>• Utilisateurs et Groupes</li> <li>• Adresses IP, Groupes d'adresses IP, Sous-réseaux IP, Groupes de sous-réseaux IP</li> <li>• Services, Groupes de Services</li> </ul> </li> <li>- 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) : <ul style="list-style-type: none"> <li>• <b>IPS (prévention des intrusions)</b> 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</li> </ul> </li> </ul>	<b>Marque :</b> <b>Référence :</b> <b>Caractéristiques proposées</b>	

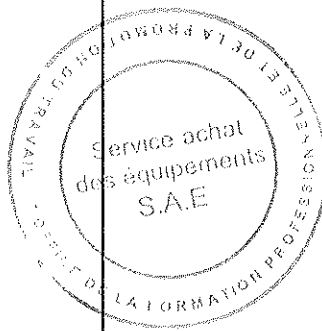


5

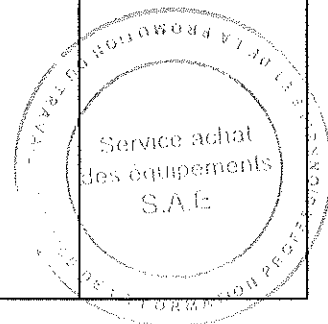
H2

Item	Spécifications techniques	Proposition du soumissionnaire	Appréciation de l'administration
	<p>menaces réseaux existantes et émergentes. Ce module IPS doit avoir deux mécanismes :</p> <ul style="list-style-type: none"> <li>- Détection par signatures ;</li> <li>- Détection par anomalies ;</li> <li>- Capable de faire des analyses comportementales de tout type de trafic ;</li> <li>- Possibilité de créer des signatures personnalisées ;</li> <li>- Mise à jour automatique des signatures IPS ;</li> <li>- Création et affectation des politiques IPS par type de zone ou interface ;</li> <li>- 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) ... ;</li> <li>- Gestion de profils IPS avec association à certains trafics dans la politique de filtrage (IP source, IP destination, service, protocole, réseau...) ;</li> </ul> <ul style="list-style-type: none"> <li>• <b>Filtrage URL</b>, pour assurer le contrôle de l'accès interne aux contenus Web indésirables, non productifs, voire illégaux,</li> <li>• <b>Control Applicatif</b>, afin d'identifier, reconnaître et contrôler les applications dans les flux,</li> </ul>		
	<p><b>Spécifications matérielles et performance :</b></p> <ul style="list-style-type: none"> <li>- Format : Appliance Rackable, 19"</li> <li>- Débit de Prevention des menaces (Firewall niveau 7 avec Contrôle applicatif + IPS + Anti Malware + Sandboxing+ Antispyware + filtrage URL, filtrage de contenu et Journalisation) : <b>2.5 Gbps Minimum</b></li> <li>- Nombre de sessions inspectées simultanées : <b>1 Million Minimum</b></li> <li>- Nombre de nouvelles sessions par seconde : <b>50 000 Minimum</b></li> <li>- Stockage Disque dur dédiée de type SSD de <b>200 GB Minimum</b></li> <li>- Les ports (en dehors des ports de management et de la haute disponibilité) <ul style="list-style-type: none"> <li>• Minimum 8 ports 10/100/1000 BaseT</li> <li>• Minimum 4 ports 1G/10G SFP/SFP+ dont 4 avec Transceiver SFP+</li> </ul> </li> <li>- Les ports de management et Clustering : <ul style="list-style-type: none"> <li>• Minimum 1 port 10/100/1000 BaseT pour le management</li> <li>• Minimum 1 port console RJ-45</li> <li>• Minimum 1 port USB</li> <li>• Minimum 1 ports 10/100/1000 BaseT pour le HA</li> </ul> </li> </ul> <p>2 Alimentations électriques Redondantes Minimum (AC),</p>		
	<p><b>Support de la haute disponibilité :</b></p> <ul style="list-style-type: none"> <li>- Actif/Actif avec synchronisation d'état de session,</li> <li>- Actif/Passif,</li> </ul>		
	<p><b>Contrôle applicatif :</b></p> <ul style="list-style-type: none"> <li>- Identification des applications en se basant sur : <ul style="list-style-type: none"> <li>• Signatures</li> </ul> </li> </ul>		



Item	Spécifications techniques	Proposition du soumissionnaire	Appréciation de l'administration
	<ul style="list-style-type: none"> <li>Décodage du protocole (respecte la spécification du protocole)</li> <li>Déchiffrement du trafic encapsulé</li> <li>Identification et contrôle des applications partageant la même connexion</li> <li>Contrôle de la fonction de transfert de fichiers d'une application</li> <li>Visibilité du trafic applicatif inconnu à travers l'identification de sa nature : <ul style="list-style-type: none"> <li>Volume du trafic</li> <li>Utilisateur et/ou adresses IP</li> <li>Port utilisé</li> <li>Contenu associé : fichier, menace ou autre.</li> </ul> </li> <li>La base de données de contrôle des applications doit contenir plus de 3 000 applications connues ;</li> </ul> <p>La solution doit pouvoir créer une règle de filtrage avec plusieurs catégories ;</p>		
	<p><b>Identification, authentification des utilisateurs et protection des identités</b></p> <ul style="list-style-type: none"> <li>Prise en charge des services d'authentification suivants pour l'identification et authentifications des utilisateurs : <ul style="list-style-type: none"> <li>Active Directory</li> <li>Kerberos</li> <li>LDAP</li> <li>Radius</li> <li>Base Locale</li> <li>SAML</li> <li>Authentification via SSO Kerberos sans agent</li> <li>Authentification par Certificat client</li> <li>Portail captif</li> </ul> </li> <li>Identification des utilisateurs indépendamment : <ul style="list-style-type: none"> <li>Du terminal (ordinateur, un téléphone intelligent ou une tablette)</li> <li>Du système d'exploitation utilisé,</li> <li>Des adresses IP et de la zone (LAN, VPN, hors du périmètre du réseau)</li> </ul> </li> </ul>		
	<p><b>Fonctions Réseau :</b></p> <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> <li>Support de la fonctionnalité <b>SD-WAN</b> pour le routage avancé des flux sur plusieurs liaisons à base d'application afin d'augmenter la disponibilité et la performance WAN en se basant sur les paramètres de performance (Latence, Perte de packets et jitter) que ce soit lors de</li> </ul>		

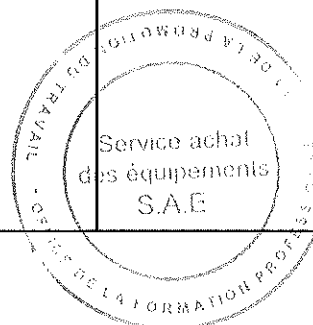
Item	Spécifications techniques	Proposition du soumissionnaire	Appréciation de l'administration
	la navigation Internet et pour la communication inter-sites (fonctionnalité et licence à fournir) -		
	<b>Fonction VPN :</b> <ul style="list-style-type: none"> <li>- VPN IPSec site-site, client-site et hub &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> <li>-</li> </ul>		
	<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> </ul> Limitation de la bande passante par source, destination, application ou catégorie d'application.		
	<b>Administration et gestion des journaux :</b> <ul style="list-style-type: none"> <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> <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> </ul>		



5

Hz

Item	Spécifications techniques	Proposition du soumissionnaire	Appréciation de l'administration
	<ul style="list-style-type: none"> <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>		
	<p><b>Filtrage URL et Filtrage de contenu</b></p> <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>		
1.2	<p><b>PRESTATION DE SERVICE</b></p> <p>Le prestataire doit proposer dans son offre toutes les prestations nécessaires à la mise en œuvre de la solution de sécurité :</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>- Intégration de la solution dans le réseau de la CMC ;</li> <li>- L'interconnexion du NGFW avec les Switch Datacenter ;</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 d'un an 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 ;</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> </ul> </li> </ul> <p>Manuel d'exploitation ;</p>		



**BORDEREAU DES PRIX – DETAIL ESTIMATIF**

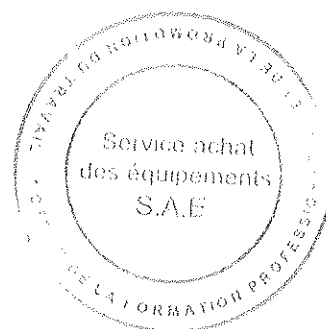
**LOT 8 : Solution de Firewall Nouvelle Génération NGFW pour la CMC FES**

Items N°	Désignations	Unité	(1) QTE	(2) Prix unitaire HT/HDD/HTV A	(3) Prix total HT/HDD/HTV A (3) = (1) x (2)	(4) Droits de Douanes sur (3)	(5) Prix total Hors TVA (5) = (3) + (4)	(6) TVA Appliquée sur (5)	(7) Montant TTC (7) = (5) + (6)
1	Solution de Firewall Nouvelle Génération NGFW de type Appliance								
1.1	Firewall	U	1						
1.2	PRESTATION DE SERVICE	ens	1						
<b>MONTANT TOTAL =</b>									

Important : 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 à ce sujet.

Fait à ..... le .....

Signature et cachet du concurrent



**LOT 9 : Solution de Firewall Nouvelle Génération NGFW pour la CMC ERRACHIDIA**

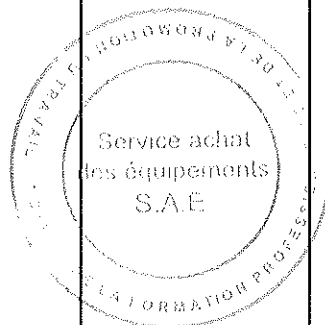
*N.B : les soumissionnaires sont invités à remplir la case 'Proposition du soumissionnaire' en précisant les caractéristiques du matériel. La réponse du soumissionnaire doit être justifiée par des notes explicatives, des fiches techniques (marquer les justifications), ou tout autre moyen pouvant justifier la proposition du soumissionnaire.*

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

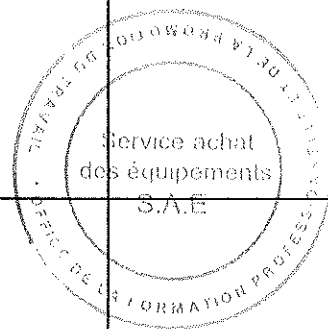
*Les colonnes 'Désignations et caractéristiques techniques' et 'Appréciation de l'administration' ne doivent pas être renseignées ou modifiées.*

*Le concurrent est tenu à 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.*

Item	Spécifications techniques	Proposition du soumissionnaire	Appréciation de l'administration
<b>1 .</b>	<b>Solution de Firewall Nouvelle Génération NGFW de type Appliance</b>		
<b>1.1</b>	<b>Leader dans Gartner dans la technologie Network Firewall pour les trois années minimum 2019, 2020 et 2021</b>		
	<b>Fonctions Firewall</b> <ul style="list-style-type: none"> <li>- Doit intégrer un système d'exploitation propriétaire sécurisé,</li> <li>- Filtrage de paquets et être doté de la fonction de filtrage dynamique,</li> <li>- Filtrage basé sur les applications niveau 7 en plus des ports/Protocol et par plages de ports UDP ou TCP</li> <li>- Filtrage et inspection en IPv4 et IPv6,</li> <li>- Failover de connexion Internet,</li> <li>- Prise en compte de paramètre Horaire dans les règles de filtrage,</li> <li>- Doit fournir, via sa console d'administration, des statistiques sur le nombre d'accès aux règles de sécurité,</li> <li>- Doit inclure la possibilité de fonctionner en mode transparent ou routé (natté),</li> <li>- 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,</li> <li>- La création de la politique de sécurité basée sur : <ul style="list-style-type: none"> <li>• Geolocation par pays</li> <li>• Zones</li> <li>• Groupes de Zones</li> <li>• Applications, Groupes d'applications</li> <li>• Catégories d'Applications</li> <li>• Technologies d'Applications</li> <li>• Filtres d'Applications</li> <li>• Utilisateurs et Groupes</li> <li>• Adresses IP, Groupes d'adresses IP, Sous-réseaux IP, Groupes de sous-réseaux IP</li> <li>• Services, Groupes de Services</li> </ul> </li> <li>- 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) : <ul style="list-style-type: none"> <li>• <b>IPS (prévention des intrusions)</b> 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</li> </ul> </li> </ul>	<b>Marque :</b> <b>Référence :</b> <b>Caractéristiques proposées</b>	



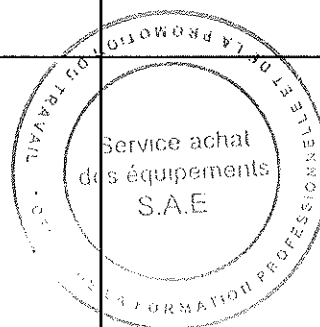
Item	Spécifications techniques	Proposition du soumissionnaire	Appréciation de l'administration
	<p>menaces réseaux existantes et émergentes. Ce module IPS doit avoir deux mécanismes :</p> <ul style="list-style-type: none"> <li>- Détection par signatures ;</li> <li>- Détection par anomalies ;</li> <li>- Capable de faire des analyses comportementales de tout type de trafic ;</li> <li>- Possibilité de créer des signatures personnalisées ;</li> <li>- Mise à jour automatique des signatures IPS ;</li> <li>- Création et affectation des politiques IPS par type de zone ou interface ;</li> <li>- 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) ... ;</li> <li>- Gestion de profils IPS avec association à certains trafics dans la politique de filtrage (IP source, IP destination, service, protocole, réseau...) ;</li> </ul> <ul style="list-style-type: none"> <li>• <b>Filtrage URL</b>, pour assurer le contrôle de l'accès interne aux contenus Web indésirables, non productifs, voire illégaux,</li> <li>• <b>Control Applicatif</b>, afin d'identifier, reconnaître et contrôler les applications dans les flux,</li> </ul>		
	<p><b>Spécifications matérielles et performance :</b></p> <ul style="list-style-type: none"> <li>- Format : Appliance Rackable, 19"</li> <li>- Débit de Prevention des menaces (Firewall niveau 7 avec Contrôle applicatif + IPS + Anti Malware + Sandboxing+ Antispyware + filtrage URL, filtrage de contenu et Journalisation) : <b>2.5 Gbps Minimum</b></li> <li>- Nombre de sessions inspectées simultanées : <b>1 Million Minimum</b></li> <li>- Nombre de nouvelles sessions par seconde : <b>50 000 Minimum</b></li> <li>- Stockage Disque dur dédiée de type SSD de <b>200 GB Minimum</b></li> <li>- Les ports (en dehors des ports de management et de la haute disponibilité) <ul style="list-style-type: none"> <li>• Minimum 8 ports 10/100/1000 BaseT</li> <li>• Minimum 4 ports 1G/10G SFP/SFP+ dont 4 avec Transceiver SFP+</li> </ul> </li> <li>- Les ports de management et Clustering : <ul style="list-style-type: none"> <li>• Minimum 1 port 10/100/1000 BaseT pour le management</li> <li>• Minimum 1 port console RJ-45</li> <li>• Minimum 1 port USB</li> <li>• Minimum 1 ports 10/100/1000 BaseT pour le HA</li> </ul> </li> </ul> <p>2 Alimentations électriques Redondantes Minimum (AC),</p>		
	<p><b>Support de la haute disponibilité :</b></p> <ul style="list-style-type: none"> <li>- Actif/Actif avec synchronisation d'état de session,</li> <li>- Actif/Passif,</li> <li>-</li> </ul>		
	<p><b>Contrôle applicatif :</b></p> <ul style="list-style-type: none"> <li>- Identification des applications en se basant sur :</li> </ul>		



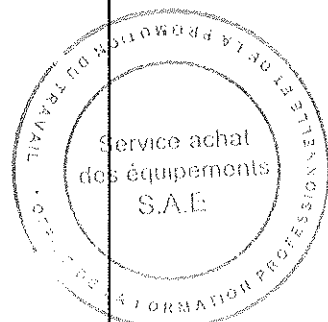
Handwritten marks: a checkmark and the number 42.



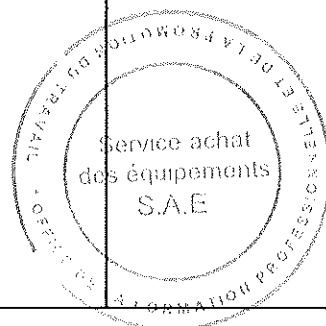
Item	Spécifications techniques	Proposition du soumissionnaire	Appréciation de l'administration
	<ul style="list-style-type: none"> <li>• Signatures</li> <li>• Décodage du protocole (respecte la spécification du protocole)</li> <li>• Déchiffrement du trafic encapsulé</li> <li>- Identification et contrôle des applications partageant la même connexion</li> <li>- Contrôle de la fonction de transfert de fichiers d'une application</li> <li>- Visibilité du trafic applicatif inconnu à travers l'identification de sa nature : <ul style="list-style-type: none"> <li>• Volume du trafic</li> <li>• Utilisateur et/ou adresses IP</li> <li>• Port utilisé</li> <li>• Contenu associé : fichier, menace ou autre.</li> </ul> </li> <li>- La base de données de contrôle des applications doit contenir plus de 3 000 applications connues ;</li> </ul> <p>La solution doit pouvoir créer une règle de filtrage avec plusieurs catégories ;</p>		
	<p><b>Identification, authentification des utilisateurs et protection des identités</b></p> <ul style="list-style-type: none"> <li>- Prise en charge des services d'authentification suivants pour l'identification et authentifications des utilisateurs : <ul style="list-style-type: none"> <li>• Active Directory</li> <li>• Kerberos</li> <li>• LDAP</li> <li>• Radius</li> <li>• Base Locale</li> <li>• SAML</li> <li>• Authentification via SSO Kerberos sans agent</li> <li>• Authentification par Certificat client</li> <li>• Portail captif</li> </ul> </li> <li>- Identification des utilisateurs indépendamment : <ul style="list-style-type: none"> <li>• Du terminal (ordinateur, un téléphone intelligent ou une tablette)</li> <li>• Du système d'exploitation utilisé,</li> <li>• Des adresses IP et de la zone (LAN, VPN, hors du périmètre du réseau)</li> </ul> </li> </ul>		
	<p><b>Fonctions Réseau :</b></p> <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> <li>- Support de la fonctionnalité <b>SD-WAN</b> pour le routage avancé des flux sur plusieurs liaisons à base d'application afin d'augmenter la</li> </ul>		



Item	Spécifications techniques	Proposition du soumissionnaire	Appréciation de l'administration
	disponibilité et la performance WAN en se basant sur les paramètres de performance (Latence, Perte de packets et jitter) que ce soit lors de la navigation Internet et pour la communication inter-sites (fonctionnalité et licence à fournir) -		
	<b>Fonction VPN :</b> - 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, -		
	<b>Gestion de la bande passante :</b> - 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.		
	<b>Administration et gestion des journaux :</b> - 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,		



Item	Spécifications techniques	Proposition du soumissionnaire	Appréciation de l'administration
	<ul style="list-style-type: none"> <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>		
	<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>		
1.2	<b>PRESTATION DE SERVICE</b> Le prestataire doit proposer dans son offre toutes les prestations nécessaires à la mise en œuvre de la solution de sécurité : <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>- Intégration de la solution dans le réseau de la CMC ;</li> <li>- L'interconnexion du NGFW avec les Switch Datacenter ;</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 d'un an 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 ;</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> </ul> </li> </ul> <b>Manuel d'exploitation ;</b>		



**BORDEREAU DES PRIX – DETAIL ESTIMATIF**

**LOT 9 : Solution de Firewall Nouvelle Génération NGFW pour la CMC ERRACHIDIA**

Items N°	Désignations	Unité	(1) QTE	(2) Prix unitaire HT/HDD/HTV A	(3) Prix total HT/HDD/HTV A (3) = (1) x (2)	(4) Droits de Douanes sur (3)	(5) Prix total Hors TVA (5) = (3) + (4)	(6) TVA Appliqué e sur (5)	(7) Montant TTC (7) = (5) + (6)
1	Solution de Firewall Nouvelle Génération NGFW de type Appliance								
1.1	Firewall	U	1						
1.2	PRESTATION DE SERVICE	ens	1						
<b>MONTANT TOTAL =</b>									

**Important : 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 à ce sujet.**

Fait à ..... le .....

**Signature et cachet du concurrent**



**LOT 10 : Solution de Firewall Nouvelle Génération NGFW pour la CMC GUELMIM**

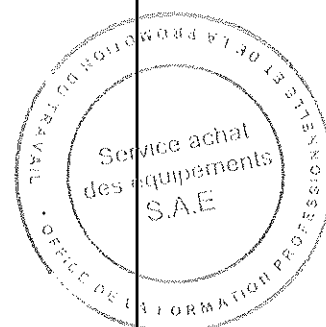
*N.B : les soumissionnaires sont invités à remplir la case 'Proposition du soumissionnaire' en précisant les caractéristiques du matériel. La réponse du soumissionnaire doit être justifiée par des notes explicatives, des fiches techniques (marquer les justifications), ou tout autre moyen pouvant justifier la proposition du soumissionnaire.*

*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.*

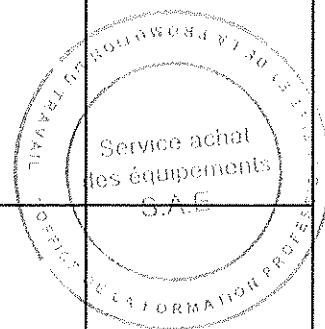
*Le concurrent est tenu à renseigner pour chaque item, la marque, la référence et les caractéristiques des fournitures proposées et ce, dans le cadre de la colonne 'Proposition du soumissionnaire' et la ligne correspondante à l'item.*

Item	Spécifications techniques	Proposition du soumissionnaire	Appréciation de l'administration
<b>1 .</b>	<b>Solution de Firewall Nouvelle Génération NGFW de type Appliance</b>		
<b>1.1</b>	<b>Leader dans Gartner dans la technologie Network Firewall pour les trois années minimum 2019, 2020 et 2021</b>		
	<b>Fonctions Firewall</b> <ul style="list-style-type: none"> <li>- Doit intégrer un système d'exploitation propriétaire sécurisé,</li> <li>- Filtrage de paquets et être doté de la fonction de filtrage dynamique,</li> <li>- Filtrage basé sur les applications niveau 7 en plus des ports/Protocol et par plages de ports UDP ou TCP</li> <li>- Filtrage et inspection en IPv4 et IPv6,</li> <li>- Failover de connexion Internet,</li> <li>- Prise en compte de paramètre Horaire dans les règles de filtrage,</li> <li>- Doit fournir, via sa console d'administration, des statistiques sur le nombre d'accès aux règles de sécurité,</li> <li>- Doit inclure la possibilité de fonctionner en mode transparent ou routé (natté),</li> <li>- 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,</li> <li>- La création de la politique de sécurité basée sur : <ul style="list-style-type: none"> <li>• Geolocation par pays</li> <li>• Zones</li> <li>• Groupes de Zones</li> <li>• Applications, Groupes d'applications</li> <li>• Catégories d'Applications</li> <li>• Technologies d'Applications</li> <li>• Filtres d'Applications</li> <li>• Utilisateurs et Groupes</li> <li>• Adresses IP, Groupes d'adresses IP, Sous-réseaux IP, Groupes de sous-réseaux IP</li> <li>• Services, Groupes de Services</li> </ul> </li> <li>- 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) : <ul style="list-style-type: none"> <li>• <b>IPS (prévention des intrusions)</b> pour se protéger contre les menaces réseau telles que vers, chevaux de Troie et autres programmes malveillants. Le système de prévention des</li> </ul> </li> </ul>	<b>Marque :</b> <b>Référence :</b> <b>Caractéristiques proposées</b>	



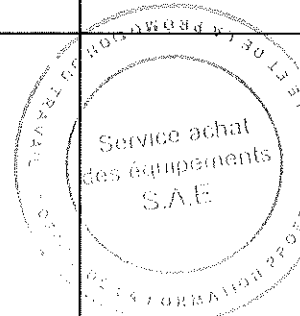
5  
HE

Item	Spécifications techniques	Proposition du soumissionnaire	Appréciation de l'administration
	<p>intrusions (IPS) doit aussi apporter une protection contre les menaces réseaux existantes et émergentes. Ce module IPS doit avoir deux mécanismes :</p> <ul style="list-style-type: none"> <li>- Détection par signatures ;</li> <li>- Détection par anomalies ;</li> <li>- Capable de faire des analyses comportementales de tout type de trafic ;</li> <li>- Possibilité de créer des signatures personnalisées ;</li> <li>- Mise à jour automatique des signatures IPS ;</li> <li>- Création et affectation des politiques IPS par type de zone ou interface ;</li> <li>- 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) ... ;</li> <li>- Gestion de profils IPS avec association à certains trafics dans la politique de filtrage (IP source, IP destination, service, protocole, réseau...) ;</li> </ul> <ul style="list-style-type: none"> <li>• <b>Filtrage URL</b>, pour assurer le contrôle de l'accès interne aux contenus Web indésirables, non productifs, voire illégaux,</li> <li>• <b>Control Applicatif</b>, afin d'identifier, reconnaître et contrôler les applications dans les flux,</li> </ul>		
	<p><b>Spécifications matérielles et performance :</b></p> <ul style="list-style-type: none"> <li>- Format : Appliance Rackable, 19"</li> <li>- Débit de Prevention des menaces (Firewall niveau 7 avec Contrôle applicatif + IPS + Anti Malware + Sandboxing+ Antispyware + filtrage URL, filtrage de contenu et Journalisation) : <b>2.5 Gbps Minimum</b></li> <li>- Nombre de sessions inspectées simultanées : <b>1 Million Minimum</b></li> <li>- Nombre de nouvelles sessions par seconde : <b>50 000 Minimum</b></li> <li>- Stockage Disque dur dédiée de type SSD de <b>200 GB Minimum</b></li> <li>- Les ports (en dehors des ports de management et de la haute disponibilité) <ul style="list-style-type: none"> <li>• Minimum 8 ports 10/100/1000 BaseT</li> <li>• Minimum 4 ports 1G/10G SFP/SFP+ dont 4 avec Transceiver SFP+</li> </ul> </li> <li>- Les ports de management et Clustering : <ul style="list-style-type: none"> <li>• Minimum 1 port 10/100/1000 BaseT pour le management</li> <li>• Minimum 1 port console RJ-45</li> <li>• Minimum 1 port USB</li> <li>• Minimum 1 ports 10/100/1000 BaseT pour le HA</li> </ul> </li> </ul> <p>2 Alimentations électriques Redondantes Minimum (AC),</p>		
	<p><b>Support de la haute disponibilité :</b></p> <ul style="list-style-type: none"> <li>- Actif/Actif avec synchronisation d'état de session,</li> <li>- Actif/Passif,</li> <li>-</li> </ul>		
	<p><b>Contrôle applicatif :</b></p>		

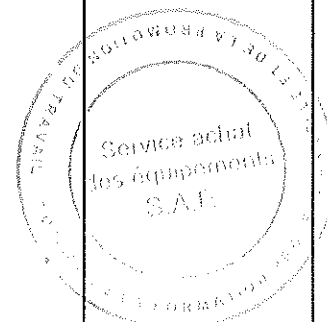


✓

Handwritten signature

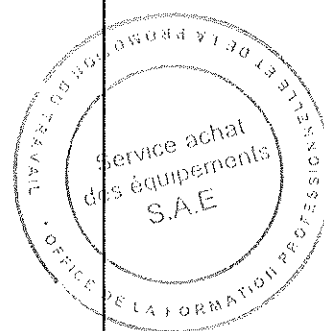
Item	Spécifications techniques	Proposition du soumissionnaire	Appréciation de l'administration
	<ul style="list-style-type: none"> <li>- Identification des applications en se basant sur : <ul style="list-style-type: none"> <li>• Signatures</li> <li>• Décodage du protocole (respecte la spécification du protocole)</li> <li>• Déchiffrement du trafic encapsulé</li> </ul> </li> <li>- Identification et contrôle des applications partageant la même connexion</li> <li>- Contrôle de la fonction de transfert de fichiers d'une application</li> <li>- Visibilité du trafic applicatif inconnu à travers l'identification de sa nature : <ul style="list-style-type: none"> <li>• Volume du trafic</li> <li>• Utilisateur et/ou adresses IP</li> <li>• Port utilisé</li> <li>• Contenu associé : fichier, menace ou autre.</li> </ul> </li> <li>- La base de données de contrôle des applications doit contenir plus de 3 000 applications connues ;</li> </ul> <p>La solution doit pouvoir créer une règle de filtrage avec plusieurs catégories ;</p>		
	<p><b>Identification, authentification des utilisateurs et protection des identités</b></p> <ul style="list-style-type: none"> <li>- Prise en charge des services d'authentification suivants pour l'identification et authentifications des utilisateurs : <ul style="list-style-type: none"> <li>• Active Directory</li> <li>• Kerberos</li> <li>• LDAP</li> <li>• Radius</li> <li>• Base Locale</li> <li>• SAML</li> <li>• Authentification via SSO Kerberos sans agent</li> <li>• Authentification par Certificat client</li> <li>• Portail captif</li> </ul> </li> <li>- Identification des utilisateurs indépendamment : <ul style="list-style-type: none"> <li>• Du terminal (ordinateur, un téléphone intelligent ou une tablette)</li> <li>• Du système d'exploitation utilisé,</li> <li>• Des adresses IP et de la zone (LAN, VPN, hors du périmètre du réseau)</li> </ul> </li> </ul>		
	<p><b>Fonctions Réseau :</b></p> <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>		

Item	Spécifications techniques	Proposition du soumissionnaire	Appréciation de l'administration
	<ul style="list-style-type: none"> <li>- Support de la fonctionnalité <b>SD-WAN</b> pour le routage avancé des flux sur plusieurs liaisons à base d'application afin d'augmenter la disponibilité et la performance WAN en se basant sur les paramètres de performance (Latence, Perte de packets et jitter) que ce soit lors de la navigation Internet et pour la communication inter-sites (<b>fonctionnalité et licence à fournir</b>)</li> </ul>		
	<p><b>Fonction VPN :</b></p> <ul style="list-style-type: none"> <li>- VPN IPSec site-site, client-site et hub &amp; Spoke. (<b>Fonctionnalité et licence à fournir</b>)</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>		
	<p><b>Gestion de la bande passante :</b></p> <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> </ul> <p>Limitation de la bande passante par source, destination, application ou catégorie d'application.</p>		
	<p><b>Administration et gestion des journaux :</b></p> <ul style="list-style-type: none"> <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> <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> </ul>		





Item	Spécifications techniques	Proposition du soumissionnaire	Appréciation de l'administration
	<ul style="list-style-type: none"> <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>		
	<p><b>Filtrage URL et Filtrage de contenu</b></p> <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>		
1.2	<p><b>PRESTATION DE SERVICE</b></p> <p>Le prestataire doit proposer dans son offre toutes les prestations nécessaires à la mise en œuvre de la solution de sécurité :</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>- Intégration de la solution dans le réseau de la CMC ;</li> <li>- L'interconnexion du NGFW avec les Switch Datacenter ;</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 d'un an 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 ;</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> </ul> </li> </ul> <p>Manuel d'exploitation ;</p>		



**BORDEREAU DES PRIX – DETAIL ESTIMATIF**

**LOT 10 : Solution de Firewall Nouvelle Génération NGFW pour la CMC GUELMIM**

Items N°	Désignations	Unité	(1) QTE	(2) Prix unitaire HT/HDD/HTV A	(3) Prix total HT/HDD/HTV A (3) = (1) x (2)	(4) Droits de Douanes sur (3)	(5) Prix total Hors TVA (5) = (3) + (4)	(6) TVA Appliquée sur (5)	(7) Montant TTC (7) = (5) + (6)
1	Solution de Firewall Nouvelle Génération NGFW de type Appliance								
1.1	Firewall	U	1						
1.2	PRESTATION DE SERVICE	ens	1						
<b>MONTANT TOTAL =</b>									

Important : 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 à ce sujet.

Fait à ..... le .....

Signature et cachet du concurrent



**LOT 11 : Solution de Firewall Nouvelle Génération NGFW pour la CMC DAKHLA**

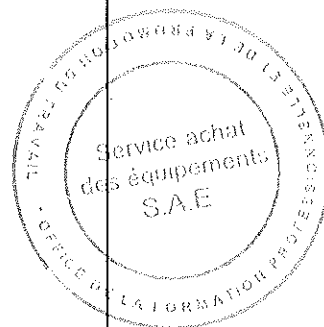
*N.B : les soumissionnaires sont invités à remplir la case 'Proposition du soumissionnaire' en précisant les caractéristiques du matériel. La réponse du soumissionnaire doit être justifiée par des notes explicatives, des fiches techniques (marquer les justifications), ou tout autre moyen pouvant justifier la proposition du soumissionnaire.*

*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.*

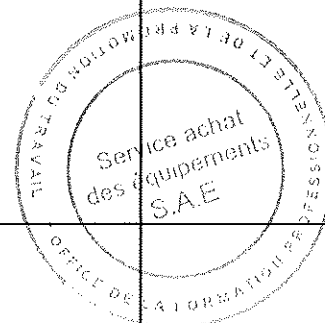
*Le concurrent est tenu à renseigner pour chaque item, la marque, la référence et les caractéristiques des fournitures proposées et ce, dans le cadre de la colonne 'Proposition du soumissionnaire' et la ligne correspondante à l'item.*

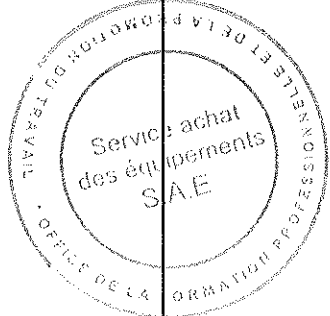
Item	Spécifications techniques	Proposition du soumissionnaire	Appréciation de l'administration
<b>1 .</b>	<b>Solution de Firewall Nouvelle Génération NGFW de type Appliance</b>		
<b>1.1</b>	<b>Leader dans Gartner dans la technologie Network Firewall pour les trois années minimum 2019, 2020 et 2021</b>		
	<b>Fonctions Firewall</b> <ul style="list-style-type: none"> <li>- Doit intégrer un système d'exploitation propriétaire sécurisé,</li> <li>- Filtrage de paquets et être doté de la fonction de filtrage dynamique,</li> <li>- Filtrage basé sur les applications niveau 7 en plus des ports/Protocol et par plages de ports UDP ou TCP</li> <li>- Filtrage et inspection en IPv4 et IPv6,</li> <li>- Failover de connexion Internet,</li> <li>- Prise en compte de paramètre Horaire dans les règles de filtrage,</li> <li>- Doit fournir, via sa console d'administration, des statistiques sur le nombre d'accès aux règles de sécurité,</li> <li>- Doit inclure la possibilité de fonctionner en mode transparent ou routé (natté),</li> <li>- 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,</li> <li>- La création de la politique de sécurité basée sur : <ul style="list-style-type: none"> <li>• Geolocation par pays</li> <li>• Zones</li> <li>• Groupes de Zones</li> <li>• Applications, Groupes d'applications</li> <li>• Catégories d'Applications</li> <li>• Technologies d'Applications</li> <li>• Filtres d'Applications</li> <li>• Utilisateurs et Groupes</li> <li>• Adresses IP, Groupes d'adresses IP, Sous-réseaux IP, Groupes de sous-réseaux IP</li> <li>• Services, Groupes de Services</li> </ul> </li> <li>- 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) : <ul style="list-style-type: none"> <li>• <b>IPS (prévention des intrusions)</b> 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</li> </ul> </li> </ul>	<b>Marque :</b> <b>Référence :</b> <b>Caractéristiques proposées</b>	



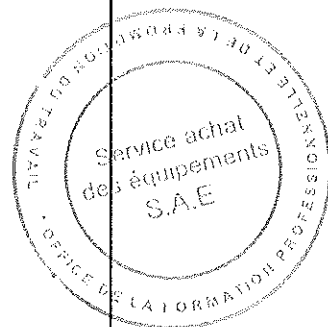
G  
Hz

Item	Spécifications techniques	Proposition du soumissionnaire	Appréciation de l'administration
	<p>menaces réseaux existantes et émergentes. Ce module IPS doit avoir deux mécanismes :</p> <ul style="list-style-type: none"> <li>- Détection par signatures ;</li> <li>- Détection par anomalies ;</li> <li>- Capable de faire des analyses comportementales de tout type de trafic ;</li> <li>- Possibilité de créer des signatures personnalisées ;</li> <li>- Mise à jour automatique des signatures IPS ;</li> <li>- Création et affectation des politiques IPS par type de zone ou interface ;</li> <li>- 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) ... ;</li> <li>- Gestion de profils IPS avec association à certains trafics dans la politique de filtrage (IP source, IP destination, service, protocole, réseau...) ;</li> <li>• <b>Filtrage URL</b>, pour assurer le contrôle de l'accès interne aux contenus Web indésirables, non productifs, voire illégaux,</li> <li>• <b>Control Applicatif</b>, afin d'identifier, reconnaître et contrôler les applications dans les flux,</li> </ul>		
	<p><b>Spécifications matérielles et performance :</b></p> <ul style="list-style-type: none"> <li>- Format : Appliance Rackable, 19"</li> <li>- Débit de Prevention des menaces (Firewall niveau 7 avec Contrôle applicatif + IPS + Anti Malware + Sandboxing+ Antispyware + filtrage URL, filtrage de contenu et Journalisation) : <b>2.5 Gbps Minimum</b></li> <li>- Nombre de sessions inspectées simultanées : <b>1 Million Minimum</b></li> <li>- Nombre de nouvelles sessions par seconde : <b>50 000 Minimum</b></li> <li>- Stockage Disque dur dédiée de type SSD de <b>200 GB Minimum</b></li> <li>- Les ports (en dehors des ports de management et de la haute disponibilité) <ul style="list-style-type: none"> <li>• Minimum 8 ports 10/100/1000 BaseT</li> <li>• Minimum 4 ports 1G/10G SFP/SFP+ dont 4 avec Transceiver SFP+</li> </ul> </li> <li>- Les ports de management et Clustering : <ul style="list-style-type: none"> <li>• Minimum 1 port 10/100/1000 BaseT pour le management</li> <li>• Minimum 1 port console RJ-45</li> <li>• Minimum 1 port USB</li> <li>• Minimum 1 ports 10/100/1000 BaseT pour le HA</li> </ul> </li> </ul> <p>2 Alimentations électriques Redondantes Minimum (AC),</p>		
	<p><b>Support de la haute disponibilité :</b></p> <ul style="list-style-type: none"> <li>- Actif/Actif avec synchronisation d'état de session,</li> <li>- Actif/Passif,</li> </ul>		
	<p><b>Contrôle applicatif :</b></p> <ul style="list-style-type: none"> <li>- Identification des applications en se basant sur :</li> </ul>		



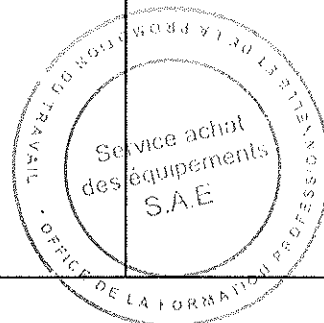
Item	Spécifications techniques	Proposition du soumissionnaire	Appréciation de l'administration
	<ul style="list-style-type: none"> <li>• Signatures</li> <li>• Décodage du protocole (respecte la spécification du protocole)</li> <li>• Déchiffrement du trafic encapsulé</li> <li>- Identification et contrôle des applications partageant la même connexion</li> <li>- Contrôle de la fonction de transfert de fichiers d'une application</li> <li>- Visibilité du trafic applicatif inconnu à travers l'identification de sa nature : <ul style="list-style-type: none"> <li>• Volume du trafic</li> <li>• Utilisateur et/ou adresses IP</li> <li>• Port utilisé</li> <li>• Contenu associé : fichier, menace ou autre.</li> </ul> </li> <li>- La base de données de contrôle des applications doit contenir plus de 3 000 applications connues ;</li> </ul> <p>La solution doit pouvoir créer une règle de filtrage avec plusieurs catégories ;</p>		
	<p><b>Identification, authentification des utilisateurs et protection des identités</b></p> <ul style="list-style-type: none"> <li>- Prise en charge des services d'authentification suivants pour l'identification et authentifications des utilisateurs : <ul style="list-style-type: none"> <li>• Active Directory</li> <li>• Kerberos</li> <li>• LDAP</li> <li>• Radius</li> <li>• Base Locale</li> <li>• SAML</li> <li>• Authentification via SSO Kerberos sans agent</li> <li>• Authentification par Certificat client</li> <li>• Portail captif</li> </ul> </li> <li>- Identification des utilisateurs indépendamment : <ul style="list-style-type: none"> <li>• Du terminal (ordinateur, un téléphone intelligent ou une tablette)</li> <li>• Du système d'exploitation utilisé,</li> <li>• Des adresses IP et de la zone (LAN, VPN, hors du périmètre du réseau)</li> </ul> </li> </ul>		
	<p><b>Fonctions Réseau :</b></p> <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> <li>- Support de la fonctionnalité <b>SD-WAN</b> pour le routage avancé des flux sur plusieurs liaisons à base d'application afin d'augmenter la</li> </ul>		

Item	Spécifications techniques	Proposition du soumissionnaire	Appréciation de l'administration
	<p>disponibilité et la performance WAN en se basant sur les paramètres de performance (Latence, Perte de packets et jitter) que ce soit lors de la navigation Internet et pour la communication inter-sites (fonctionnalité et licence à fournir)</p> <p>-</p>		
	<p><b>Fonction VPN :</b></p> <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> <li>-</li> </ul>		
	<p><b>Gestion de la bande passante :</b></p> <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> </ul> <p>Limitation de la bande passante par source, destination, application ou catégorie d'application.</p>		
	<p><b>Administration et gestion des journaux :</b></p> <ul style="list-style-type: none"> <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> <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> </ul>		



✓  
H5

Item	Spécifications techniques	Proposition du soumissionnaire	Appréciation de l'administration
	<ul style="list-style-type: none"> <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>		
	<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>		
<b>1.2</b>	<b>PRESTATION DE SERVICE</b> Le prestataire doit proposer dans son offre toutes les prestations nécessaires à la mise en œuvre de la solution de sécurité : <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>- Intégration de la solution dans le réseau de la CMC ;</li> <li>- L'interconnexion du NGFW avec les Switch Datacenter ;</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 d'un an avec un délai de prise en charge de <b>2 heures</b> après déclaration de l'incident et un délai de <b>4 heures</b> de résolution ou de contournement du problème ;</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> </ul> </li> </ul> <b>Manuel d'exploitation ;</b>		



## BORDEREAU DES PRIX – DETAIL ESTIMATIF

LOT 11 : Solution de Firewall Nouvelle Génération NGFW pour la CMC DAKHLA

Items N°	Désignations	Unité	(1) QTE	(2) Prix unitaire HT/HDD/HTV A	(3) Prix total HT/HDD/HTV A (3) = (1) x (2)	(4) Droits de Douanes sur (3)	(5) Prix total Hors TVA (5) = (3) + (4)	(6) TVA Appliquée sur (5)	(7) Montant TTC (7) = (5) + (6)
1	Solution de Firewall Nouvelle Génération NGFW de type Appliance								
1.1	Firewall	U	1						
1.2	PRESTATION DE SERVICE	ens	1						
MONTANT TOTAL =									

Important : 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 à ce sujet.

Fait à ..... le .....

Signature et cachet du concurrent

