Royaume du Maroc

Ministère du Tourisme, de l'Artisanat
et de l'Economie Sociale et Solidaire
Département de l'Artisanat et de l'Economie Sociale et Solidaire
****
Direction des Ressources et des Systèmes d'Information

المملكة المغربية

وزارة السياحة والصناعة التقليدية
والاقتصاد الاجتماعي والتضامني
قطاع الصناعة التقليدية والاقتصاد الاجتماعي والتضامني
****
مديرية الموارد وأنظمة المعلومات

CAHIER DES PRESCRIPTIONS SPECIALES

APPEL D'OFFRES OUVERT

N° 6/IN/2022

RELATIF

A

Achat de matériel informatique pour la sécurité informatique (Pare-feu et Passerelle de messagerie sécurisée) pour le compte du Département de l'Artisanat et de l'Economie Sociale et Solidaire en lot unique

PASSÉ AVEC : ..... (Nom du Fournisseur)

Sommaire

Préambule du cahier des prescriptions spéciales

Appel d'offres ouvert sur offre de prix passé en application des dispositions de l'alinéa 2 du paragraphe 1 de l'article 16, du paragraphe 1 de l'article 17 et de l'alinéa 3 du paragraphe 3 de l'article 17 du Décret n° 2-12-349 du 8 joumada I 1434 (20 mars 2013) relatif aux marchés publics.

ENTRE

Le Ministère du Tourisme, de l'Artisanat, et de l'Economie Sociale et Solidaire - Département de l'Artisanat et de l'Economie Sociale et Solidaire -, représenté par le Directeur des Ressources et des Systèmes d'information ou son représentant, désigné ci-après par le terme "Maître d'Ouvrage"

D'UNE PART

ET

1. **Cas d'une personne morale**

M. .....
Qualité .....
Agissant au nom et pour le compte de.....

En vertu des pouvoirs qui lui sont conférés.

Au capital social..... **Patente n°** .....
Registre de commerce de .....**Sous le n°**.....
Affilié à la CNSS sous n° .....
Faisant élection de domicile au .....
Identifient Fiscal.....

Compte bancaire n° (RIB sur 24 positions).....
Ouvert auprès de .....

Désigné ci-après par le terme « Prestataire ».

D'autre part

Il a été arrêté et convenu ce qui suit

2. **Cas de personne physique**

M. ..... Agissant en son nom et pour son propre compte

Registre de commerce de .....Sous le n°.....

Patente n° .....Affilié à la CNSS sous n° .....
Faisant élection de domicile au .....
Compte bancaire n° (RIB sur 24 positions)..... .....

Ouvert auprès de .....
Désigné ci-après par le terme « Prestataire ».

D'autre part

Il a été arrêté et convenu ce qui suit

Cas d'un groupement.

Les membres du groupement soussignés constitués aux termes de la convention.....(*les références de la convention*).....

3-1- Membre :

M. .....
Qualité .....
Agissant au nom et pour le compte de.....

En vertu des pouvoirs qui lui sont conférés.

Au capital social..... Patente n° .....
Registre de commerce de .....Sous le n°.....
Affilié à la CNSS sous n° .....
Faisant élection de domicile au .....

Compte bancaire n° (RIB sur 24 positions).....
Ouvert auprès de .....

3-2- Membre :

M. .....
(Servir les renseignements le concernant)

- .....

- .....

3-n- Membre :

M. .....
(Servir les renseignements le concernant)

- .....

Nous nous obligeons (conjointement ou solidairement, selon la nature du groupement) ayant :

M..... (**Prénom, Nom et Qualité**) en tant que mandataire du groupement et coordonnateur de l'exécution des prestations, ayant un **compte bancaire commun sous n° (RIB sur 24 positions)**.....
Ouvert auprès.....

Désigné ci-après par le terme « Prestataire ».

D'autre part

Il a été arrêté et convenu ce qui suit

CHAPITRE I : CLAUSES ADMINISTRATIVES ET FINANCIERE

ARTICLE I-1 : OBJET DE L'APPEL D'OFFRES

Le présent appel d'offres a pour objet : Achat de matériel informatique pour la sécurité informatique (Pare-feu et Passerelle de messagerie sécurisée) pour le compte du Département de l'Artisanat et de l'Economie Sociale et Solidaire en lot unique.

ARTICLE I-2 : CONSISTANCE DES PRESTATIONS

Les prestations à exécuter au titre du présent appel d'offres consistent à : L'Achat, les travaux de pose, l'installation et la configuration des matériels livrés:

- PRIX 1 : PARE-FEU NOUVELLE GENERATION : **deux (02)** Appliances physiques en redondance en Actif/Passif (voir Prix 1- chapitre II : clauses techniques).
- PRIX 2 : PASSERELLE EMAIL SECURISEE: **deux (02)** Appliances physiques en redondance en Actif/Passif (voir Prix 2- chapitre II : clauses techniques)

La consistance des prestations objet du présent appel d'offres est indiquée au niveau du **chapitre II - Clauses Techniques.**

ARTICLE I-3 : OBLIGATIONS DU TITULAIRE

Pendant toute la durée du marché, le titulaire devra désigner son représentant auprès du Département de l'Artisanat et de l'Economie Sociale et Solidaire investi des pouvoirs et des prérogatives nécessaires pour assurer le bon déroulement des prestations.

Pour mener à bien les prestations, objet du marché, le titulaire s'engage à mettre à la disposition du maître d'ouvrage un chef de projet et une équipe projet composée d'au moins de deux ressources techniques qualifiées dans le domaine d'intervention du présent appel d'offres.

Avant le commencement des prestations, le titulaire doit présenter à l'agrément du maître d'ouvrage :

1- Le CV de chaque membre de l'équipe ;

2- La copie du diplôme de chaque membre de l'équipe ;

Le titulaire est tenu de garder les mêmes membres proposés pour l'exécution des prestations. Si pour des raisons indépendantes de la volonté du Titulaire, il s'avère nécessaire de remplacer un des membres du personnel, le titulaire présentera à l'agrément du Maître d'Ouvrage, une personne de qualification égale ou supérieure à celle dont le remplacement est demandé.

Le maître d'ouvrage se réserve le droit de demander le changement de toute personne pour des raisons de compétence ou de comportement.

ARTICLE I-4 : DOCUMENTS CONSTITUTIFS DU MARCHE

Les documents et pièces incorporés au marché sont énumérés ci-après :

1. L'acte d'engagement ;
2. Le présent Cahier des prescriptions spéciales
3. Le bordereau de prix- détail estimatif ;

4. Le Cahier des Clauses Administratives Générales applicables aux marchés de travaux (CCAG-T approuvé par le Décret n° 2-14-394 du 06 chaabane 1437 (13 mai 2016).
   En cas de contradiction ou de différence entre les documents constitutifs du marché, ceux-ci prévalent dans l'ordre où ils sont énumérés ci-dessus.

ARTICLE I-5 : REFERENCE AUX TEXTES GENEREAUX APPLICABLES AU MARCHE

Les parties contractantes du marché sont soumises aux dispositions des textes suivants :

- La loi n 112.13 du 29 rabii II 1436 (19 fevrier 2015) relative au nantissement des marchés publics.
- Dahir n°1-56-211 du 11 décembre 1956 relatif aux garanties pécuniaires des soumissionnaires et adjudicataires de marchés publics.
- Dahir n°1-00-91 du 15 février 2000 portant promulgation de la loi n °17-97 sur la protection de la propriété intellectuelle.
- Le Décret n° 2.12.349 du 8 Joumada I 1434 (20 Mars 2013) relatif aux marchés publics.
- Décret n° 2-14-394 du 06 chaabane 1437 (13 mai 2016) approuvant le cahier des clauses administratives générales applicables aux marchés de travaux.
- 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 ;
- Décret 2-07-1235 du 05 kaada 1429 (04 novembre 2008) relatif au contrôle des dépenses de l'Etat ;
- Le décret n ° 2-16-344 du 17 Chaoual 1437 (22 Juillet 2016) fixant les délais de paiement et les intérêts moratoires relatifs aux commandes publiques.
- Décret n°2-14-272 du 14 rejeb 1435(14 mai 2014) relatif aux avances en matière de marchés publics.
- Arrêté du Ministère de l'Economie et des finances n° 1982-21 du 14 décembre 2021 relatif à la dématérialisation des procédures de passation des marchés publics et des garanties pécuniaires.
- Circulaire n° 72/CAB du 26 novembre 1992 d'application du Dahir n°1-56-211 du 11 décembre 1956 relatif aux garanties pécuniaires des soumissionnaires et adjudicataires de marchés publics.

Tous les textes réglementaires ayant trait aux marchés de l'Etat rendus applicables à la date de l'ouverture des plis.

Le titulaire ne pourra en aucun cas, invoquer à son profit l'ignorance des dispositions de ces documents.

ARTICLE I-6 : VALIDITE ET DATE DE NOTIFICATION DE L'APPROBATION DU MARCHE

Le marché ne sera valable et définitif qu'après son approbation par l'autorité compétente.
L'approbation du marché est notifiée à l'attributaire dans un délai maximum de soixante-quinze jours (75) à compter de la date fixée par d'ouverture des plis. Si la notification de l'approbation n'est pas intervenue dans ce délai, l'attributaire est libéré de son engagement vis à vis du maître d'ouvrage. Dans ce cas, main levée lui est donnée, à sa demande, de son cautionnement provisoire.

Lorsque le maître d'ouvrage décide de demander à l'attributaire de proroger la validité de son offre, il doit, avant l'expiration du délai susvisé, lui proposer par lettre recommandée, par fax conformé ou par tout autre moyen de communication donnant date certaine, de maintenir son offre pour une

période supplémentaire ne dépassant pas trente (30) jours, l'attributaire doit faire connaître sa réponse avant la date limite fixée par le Maitre d'Ouvrage. En cas de refus de l'attributaire, mainlevée lui est donnée de son cautionnement provisoire.

ARTICLE I-7 : PIECES MISES A LA DISPOSITION DU TITULAIRE

Aussitôt après la notification de l'approbation du marché, le maître d'ouvrage remet au titulaire, contre décharge, les documents constitutifs du marché en l'occurrence les pièces expressément désignées à l'article N° I-4 du présent CPS à l'exception du cahier des clauses administratives générales applicables aux marchés de travaux (CCAG-Travaux).

Le maître d'ouvrage ne peut délivrer ces documents qu'après constitution du cautionnement définitif.

ARTICLE I-8 : ELECTION DU DOMICILE DU TITULAIRE

En application des dispositions de l'article 20 du CCAG-Travaux, toutes les notifications du maître d'ouvrage sont valablement faites au domicile élu ou au siège social du titulaire mentionné dans l'acte d'engagement et rappelé dans le préambule du marché.

En cas de changement de domicile, le fournisseur est tenu d'en aviser le maitre d'ouvrage dans un délai de 15 jours suivant ce changement.

ARTICLE I-9 : NANTISSEMENT

Dans l'éventualité d'une affectation en nantissement, il sera fait application des dispositions du dahir n° 1-15-O5 du 29 rabii 11 1436 (19 février 2015) portant promulgation de la loi n° 112-13 relative au nantissement des marchés publics, étant précisé que :

1) la liquidation des sommes dues par : Ministère du Tourisme, de l'Artisanat, et de l'Economie Sociale et Solidaire -Département de l'Artisanat et de l'Economie Sociale et Solidaire- en exécution du présent marché sera opérée par les soins de la Direction des Ressources et des Systèmes d'Information ;

2) Au cours d'exécution du marché, les documents cités à l'article 8 de la loi n°112-13 peuvent être requis du maître d'ouvrage par le titulaire de marché ou le bénéficiaire des nantissements ou subrogations et sont établis sous sa responsabilité.

3) Lesdits documents sont transmis directement à la partie bénéficiaire du nantissement avec communication d'une copie au titulaire du marché dont les conditions prévues par l'article 8 de la loi n°112-13

4) les paiements prévus au présent marché seront effectués par le Trésorier Ministériel du Tourisme, seul qualifié pour recevoir les significations des créanciers du titulaire du présent marché.

5) Le maître d'ouvrage délivre sans frais, au titulaire, sur sa demande et contre récépissé, un exemplaire spécial du marché portant la mention " exemplaire unique" ou copie conforme du marché et destiné à former titre conformément aux dispositions du dahir du 19 février 2015 relatif au nantissement des marchés publics.

Les frais de timbre et d'enregistrement de l'original du marché ainsi que de « l'exemplaire unique » remis au titulaire sont à la charge de ce dernier.

ARTICLE I-10 : SOUS-TRAITANCE

Si le titulaire du marché envisage de sous-traiter une partie du marché, il choisit librement ses sous-traitants sous réserve qu'il notifie au maître d'ouvrage la nature des prestations ainsi que l'identité, la raison ou la dénomination sociale et l'adresse des sous-traitants et une copie conforme du contrat de la sous-traitance.

La sous-traitance ne peut en aucun cas dépasser cinquante pour cent (50%) du montant du marché ni porter sur le corps d'état principale.

Les sous-traitants doivent satisfaire aux conditions requises des concurrents conformément aux dispositions de l'article 24 du décret n° 2-12-349 précité.

Les prestations qui constituent le corps d'état principal et qui ne peuvent pas faire l'objet de la sous-traitance sont : PARE-FEU NOUVELLE GENERATION.

Le titulaire du marché est tenu, lorsqu'il envisage de sous-traiter une partie du marché, de la confier à des titulaires installés au Maroc et notamment à des petites et moyennes entreprises Coopératives, Unions des coopératives et l'auto- entrepreneur, conformément à l'article 158 de décret n° 2-12-349 Précité

Le titulaire du marché demeure personnellement responsable de toutes les obligations résultant du marché tant envers le maître d'ouvrage que vis-à-vis des ouvriers et des tiers. Le maître d'ouvrage ne se reconnait aucun lien juridique avec les sous-traitants.

ARTICLE I-11 : DELAI D'EXECUTION

Le titulaire devra réaliser les prestations désignées en objet dans **un délai de six (06) mois.**

Le délai de la livraison et de la mise en place court à partir de la date prévue par l'ordre de service prescrivant le commencement de l'exécution des prestations objet du marché.

ARTICLE I-12 : NATURE DES PRIX

Conformément à l'article 11 du Décret n°2-12-349, le présent marché est à prix unitaires.

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

ARTICLE I-13 : CARACTERE DES PRIX

Conformément à l'article 12 du Décret n°2-12-349, le présent marché est passé à prix ferme. 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 du règlement.

ARTICLE I-14 : CAUTIONNEMENT PROVISOIRE ET CAUTIONNEMENT DEFINITIF

Le montant du cautionnement provisoire est fixé à **quinze mille dirhams (15.000,00 dhs).**

Le montant du cautionnement définitif est fixé à trois pour cent (3%) du montant initial marché.

Si le titulaire du marché ne réalise pas le cautionnement définitif dans un délai de 20 jours à compter de la date de la notification de l'approbation du présent marché, le montant du cautionnement provisoire fixé ci-dessus reste acquis à l'Etat.

ARTICLE I-15 : RETENUE DE GARANTIE

Une retenue de garantie sera prélevée sur les acomptes. Elle est égale à dix pour cent (10 %) du montant de chaque acompte.

Elle cessera d'accroître lorsqu'elle atteindra sept pour cent (7%) du montant initial du marché augmenté le cas échéant, du montant des avenants.

ARTICLE I-16 : ASSURANCES - RESPONSABILITE

Avant le commencement de la livraison du matériel cité en objet, le titulaire doit adresser au Maître d'ouvrage, une attestation délivrée par un établissement agréé à cet effet, conformément à l'article N° 25 du CCAG-T, justifiant la souscription d'une ou plusieurs polices d'assurances pour couvrir les risques inhérents à l'exécution du marché et précisant leurs dates de validité.

ARTICLE I-17 : PROPRIETE INDUSTRIELLE OU COMMERCIALE

Le titulaire du marché garantit formellement le maître d'ouvrage contre toutes les revendications des tiers concernant les brevets d'invention relatifs aux procédés et moyens utilisés, marques de fabrique, de commerce et de service, conformément à l'article N° 26 du CCAG-T

Il appartient au titulaire du marché le cas échéant, d'obtenir les cessions, licence d'exploitation ou d'autorisation nécessaires et de supporter la charge des frais et redevances y afférentes.

ARTICLE I-18 : CONDITIONS DE LIVRAISON

La livraison et la mise en place de matériel sont à la charge du titulaire.

Toute livraison doit s'effectuer pendant les jours ouvrables et en dehors des jours fériés et dans tous les cas selon un programme préétabli par le titulaire du marché et accepté par le maître d'ouvrage.

La livraison se déroulera sur les lieux du siège du Département de l'Artisanat et de l'Economie Sociale et Solidaire à Rabat. Elle est effectuée en présence des représentants dûment habilité du maître d'ouvrage et du titulaire du marché.

Lorsque des contrôles préliminaires laissent apparaître des discordances entre le matériel indiqué dans le marché et celle effectivement livré, la livraison est refusée par le maître d'ouvrage et le titulaire est saisi immédiatement, par écrit, pour procéder au remplacement du matériel non-conforme dans un délai de 10 jours.

Le retard engendré par le remplacement du matériel jugé non conforme par le maître d'ouvrage sera imputable au titulaire du marché et la non réception de ce qui est non conforme par le maître d'ouvrage ne justifie pas, par lui-même, l'octroi d'une prolongation du délai contractuel.

Après remplacement du matériel refusé, le maître d'ouvrage procède à nouveau aux mêmes opérations de vérification et de contrôle.

ARTICLE I-19 : MODALITES DE REGLEMENT

Pour l'établissement du décompte le titulaire du marché est tenu de fournir au maître d'ouvrage une facture appuyée par les bons de livraisons et établie en cinq exemplaires, indiquant les quantités livrées, le montant total à payer ainsi que tous les éléments nécessaires à la détermination de ce montant.
Le règlement sera effectué après réception provisoire conformément à l'article I-20 cité ci-dessous.
Sur la base d'un seul décompte en application du prix du bordereau des prix – détail estimatif aux quantités réellement livrées, déduction faite de la retenue de garantie et l'application des pénalités de retard, le cas échéant.
Sur ordre du maître d'ouvrage, les sommes dues au titulaire du marché seront versées à son Compte bancaire indiqué dans son acte d'engagement et rappelé dans le préambule du marché.

ARTICLE I-20 : RECEPTIONS PROVISOIRE

Le maître d'ouvrage s'assure, en présence du titulaire ou de son représentant, de la conformité du matériel livré et de sa mise en place aux spécifications techniques du marché.
La livraison du matériel, est soumise à des vérifications avec les caractéristiques techniques indiquées au Chapitre II du Clauses Techniques.
A l'issue de ces opérations, le maître d'ouvrage prononcera la réception provisoire.
La réception provisoire est sanctionnée par un procès-verbal signé par les membres de la commission de réception désignée à cet effet et le représentant du titulaire du marché

ARTICLE I-21 : DELAI DE GARANTIE

Conformément à l'article 75 du CCAG-T, le délai de garantie est fixé à **trois (03) ans** à compter de la date de la réception provisoire. La garantie couvrira le support constructeur, l'assistance, pièces, main-d'œuvre et intervention sur site.

Pendant le délai de garantie, le titulaire du marché sera tenu, de procéder aux rectifications qui lui seraient demandées en cas de mauvaise qualité, anomalies, mise à jour ou défectuosités constatées, sans pour autant que ces prestations supplémentaires puissent donner lieu au paiement.

ARTICLE I-22 : RECEPTIONS DEFINITIVE

Conformément aux stipulations de l'article 76 du CCAG-T et après expiration du délai de garantie, il sera procédé à la réception définitive.

La libération du cautionnement définitif et de la retenue de garantie ne peut intervenir qu'après réception définitive.

La réception définitive est sanctionnée par un procès-verbal signé par les membres de la commission de réception désignée à cet effet et le représentant du titulaire du marché.

La réception définitive est sanctionnée par un procès-verbal signé par les membres de la commission de réception désignée à cet effet et le représentant du titulaire du marché.

ARTICLE I-23 : PENALITES POUR RETARD

A défaut d'avoir terminé la livraison de matériel objet du marché dans les délais prescrits, il sera appliqué au titulaire du marché une pénalité par jour calendaire de retard de 1 ‰ (un pour mille) du montant initial du marché modifié ou complété éventuellement par les avenants.

Cette pénalité sera appliquée de plein droit et sans mise en demeure sur toutes les sommes dues au titulaire dudit marché.

Toutefois, le montant cumulé de ces pénalités est plafonné à 08% du montant initial du marché modifié ou complété éventuellement par des avenants.

ARTICLE I-24 : RETENUE A LA SOURCE APPLICABLE AUX TITULAIRES ETRANGERS NON RESIDENTS AU MAROC

Une retenue à la source au titre de l'impôt sur les sociétés ou de l'impôt sur le revenu, le cas échéant, fixée au taux de dix pour cent (10 %), sera prélevée sur le montant hors taxe sur la valeur ajoutée de la licence livrée au Maroc dans le cadre dudit marché.

ARTICLE I-25 : DROITS DE TIMBRE

Conformément à l'article 7 du CCAG-T applicable aux marchés de travaux, le titulaire du marché doit acquitter les droits auxquels peuvent donner lieu le timbre, tels que ces droits résultent des lois et règlements en vigueur.

ARTICLE I-26 : LUTTE CONTRE LA FRAUDE ET LA CORRUPTION

Le fournisseur ne doit pas recourir par lui-même ou par personne interposée à des actes de corruption, à des manœuvres frauduleuses, et à des pratiques collusoires, à quelque titre que ce soit, dans les différentes procédures de passation, de gestion et d'exécution du marché.
Le fournisseur ne doit pas faire, par lui-même ou par personne interposée, des promesses, des dons ou des présents en vue d'influer sur les différentes procédures de conclusion d'un marché et lors des étapes de son exécution.

Les dispositions du présent article s'appliquent à l'ensemble des intervenants dans la réalisation du présent marché.

ARTICLE I-27: RESILIATION DU MARCHE

La résiliation du marché peut être prononcée conformément aux dispositions prévues par l'article 159 du décret n° 2-12-349 du (20 Mars 2013) relatif aux marchés publics et celles prévues par le CCAG applicable aux marchés de travaux.

ARTICLE I-28 : REGLEMENT DES DIFFERENDS ET LITIGES

Si, en cours d'exécution du marché, des différends et litiges surviennent avec le titulaire, les parties s'engagent à régler ceux-ci dans le cadre du CCAG - Travaux.
Les litiges éventuels entre le maître d'ouvrage et titulaire sont soumis aux tribunaux compétents.

ARTICLE I-29 : CONFIDENTIALITE

Le Titulaire et son personnel sont tenus au secret professionnel, pendant toute la durée du marché et après son achèvement, sur les renseignements et documents recueillis ou portés à leur connaissance à l'occasion de l'exécution du marché. Sans autorisation préalable du Maître d'Ouvrage, ils ne peuvent communiquer à des tiers la teneur de ces renseignements et documents. De plus, ils ne peuvent faire un usage préjudiciable au Maître d'Ouvrage des renseignements qui leur sont fournis pour accomplir leur mission.

ARTICLE I-30: CAS DE FORCE MAJEURE

Conformément aux prescriptions de l'article 47 du CCAG-Travaux, notamment son paragraphe 2, les seuils des intempéries qui sont réputés constituer un événement de force majeur sont définis comme suit :

- La neige : 50 cm ;
- La pluie : 140 mm ;
- Le vent : 120 Km/h ;
- Le séisme : 5,5 degré sur l'échelle de Richter.
- L'état d'urgence sanitaire

ARTICLE I-31 : AVANCES

Conformément au décret n° 2-14-272 du 14 Rajab 1435 (14 Mai 2014) relatif aux avances en matière des marchés publics, le titulaire du marché a droit à une avance qui sera calculée par application de l'article 5 du décret susmentionné. L'avance est octroyée au titulaire du marché, lorsque le montant initial du marché est supérieur ou égal à cinq cent mille (500.000) dirhams toutes taxes comprises (TTC)

Cette avance sera octroyée au titulaire après la notification de l'ordre de service de commencer les prestations objet du marché contre remise d'une caution personnelle est solidaire du même montant, ne comportant aucune réserve et demeure affectée aux garanties pécuniaires exigées du titulaire du marché.

Le montant de l'avance n'est pas révisable. Il ne peut être modifié même à l'occasion d'avenants ayant pour effet d'augmenter ou de diminuer le montant du marché.

Le marché fait l'objet d'un seul règlement, l'avance est récupérée en une seule fois par précompte sur le règlement unique

CHAPITRE II : CLAUSES TECHNIQUES

Le présent appel d'offre consiste l'Achat, les travaux de pose, l'installation et la configuration des matériels livrés de Prix 1 (**Pare-feu nouvelle génération)** et Prix 2 **(passerelle email sécurisée).**

PRIX 1 : PARE-FEU NOUVELLE GENERATION

Le Pare-feu devra permettre d'atteindre les objectifs suivants :

- Assurer le niveau de protection le plus élevé possible des réseaux, systèmes et données du Département, en prévenant les attaques connues et les attaques les plus évoluées.
- Remise à niveau de l'architecture de sécurité réseaux à travers une segmentation en différente zone de sécurité et en utilisant la capacité de créer des instances virtuelles de Pare-feu. **Une instance Pare-feu pour Internet** et une **deuxième pour les ressources dorsales (Services Datacenter).**
- Permettre une segmentation en différentes zones de sécurité en fonction des niveaux de risques, besoins métiers et services à protéger.
- Fournir la visibilité et le contrôle des flux entrants et sortant du Département.
- Fournir les moyens pour détecter et prévenir les attaques sur les différents stades.
- Assurer la disponibilité via des mécanismes de haute disponibilité et l'intégrité à travers un contrôle d'accès efficace au système d'information du Département.
- Permettre la conformité à la politique de sécurité du Département et des standards/référentiels en vigueur notamment les contrôles tels que définis par la **DGSSI.**
- Permettre d'implémenter une architecture Zero Trust entreprise.
- Permettre de se conformer aux standards et frameworks de sécurité NIST, CIS et ISO.

Le soumissionnaire devra proposer deux (2) Appliance physique en haute disponibilité (Actif /Passif)

Le Pare-feu devra répondre, **au minimum**, aux spécifications indiquées dans le tableau suivant :

Reconnaissance et Classement:	
Le Pare-feu (NGFW "Next génération Firewall") doit être : - certifié ICSA" International Computer Security Association" Labs pour l'année 2021 au minima pour **la gamme proposée** dans le cadre de cet Appel d'offre. - d'un éditeur/constructeur reconnu qui a figuré Leader du Quadrant Magic du Gartner pour les Trois (3) dernières années consécutives (2019, 2020 et 2021). - testé contre les techniques d'évasion et ayant bloqué 100% des techniques d'évasion testées dans la dernière évaluation technique NSS Labs de 2019.	
1. Dimensionnement	
Type	Appliance physique
Format	19"

Nombre d'interfaces 10/100/1000 Ethernet utiles (hors management et High-Availibility)	12
Nombre d'interfaces 10 Gb/s (SFP+) (hors management et High-Availibility)	**4**
Nombre interface 1GE pour l'administration	1
Nombre interface 1GE pour la haute disponibilité.	2
Débit de protection des menaces NGFW avec les modules de sécurité et protection activés au minimum (IPS" Intrusion Prevention System", Antivirus, Antispyware, Sandboxing, FW "Firewall"L7 avec App Contrôle, Filtrage des fichiers et Journalisation locale,).	2.5 Gbps minimum
Nombre de sessions simultanées	1 million de sessions simultanées.
Stockage des rapports et des journaux sur un disque dur local de type SSD dans le NGFW	Minimum de 200 go.
MTBF " Mean Time Between Failure "	Minimum 12 ans
Nombre de Pare-feu virtuel	5
Alimentation redondante et remplaçable à chaud.	Oui
2. Fonctions Réseaux et Pare-feu	
Le Pare-feu devra prendre en charge la haute disponibilité et clustering Actif/Actif et Actif/Passif	
supporte du protocole 802.3ad - agrégation des liens	
Gestion de flux sortants sur plusieurs liens pour la haute disponibilité des liaisons Internet	
Supporte des VLAN 802.1q	
Supporte serveur DHCP " Dynamic Host Configuration Protocol"	
Supporte Relais DHCP IPv4 et IPv6	
Support service DNS " Domain Name System " Proxy et Résolveur statique avec gestion du cache DNS	
Routage statique	
Routage dynamique	
RIPv2 " Routing Information Protocol "	
Support OSPF v3 " Open Shortest Path First"	
Support BGP " Border Gateway Protocol"	
NAT " Network Address Translation" dynamique	
NAT " Network Address Translation" statique	
NAT " Network Address Translation" par service	
NAT " Network Address Translation" IPv4/IPv6	
Supporte la création/gestion de plusieurs instances de Routeurs Virtuels.	
Le pare-feu (NGFW) doit offrir la visibilité, le contrôle des applications et l'inspection des menaces en mode tap, transparent câble virtuel, couche 2/couche 3, et en mode routage/NAT " Network Address Translation".	
Supporte le mode déploiement en mode câble virtuel transparent avec support des sous-interfaces virtuels pour séparer les zones de sécurité.	
Le pare-feu doit supporter le filtrage et l'inspection des applications et services en IPv4 et IPv6	
Le pare-feu doit supporter la création de la politique de sécurité basée sur une condition ou une combinaison : - Geolocation par pays - Zones - Groupes de Zones - Applications, Groupes d'applications - Catégories d'Applications	

- Technologies d'Applications - Facteur de Risque d'Application - Filtres d'Applications - Utilisateurs et Groupes - Adresses IP, Groupes d'adresses IP, Sous-réseaux IP, Groupes de sous-réseaux IP - Services, Groupes de Services - Conformité du poste de travail
Le Pare-feu doit prendre en charge le blocage des flux en utilisant des listes dynamiques externes (IP, URL, DNS…) Open Sources et autres.
Le Pare-feu doit permettre le déchiffrement et l'inspection des flux chiffrés en TLS " Transport Layer Security" entrants et sortants.
Le Pare-feu doit permettre de bloquer les flux chiffrés avec un standard non reconnu, pour la protection contre les flux dissimulés.
Le Pare-feu doit identifier les applications utilisées indépendamment des ports.
Possibilité de prendre en charge des applications développées en interne avec identification personnalisée manuellement par le client.
Prise en charge des nouvelles applications automatiquement dans les règles de Pare-feu après mise à jour.
3. Filtrage et Prévention des intrusions
Prise en charge de l'analyse par IPS, Antivirus et Antispyware.
Inspection des contenus en temps réel sur l'ensemble des protocoles.
Protection sur la base de signatures, analyse comportementale et protocolaire.
Protection complète pour bloquer les virus, les logiciels espions (spyware), les logiciels malveillants (malware) et vers (network warms) et l'exploitation de vulnérabilités et des techniques d'évasions.
Détection et protection contre les techniques de camouflage (Evasion Techniques)
Protection avancée contre les programmes malveillants pour empêcher les attaques ciblées et les APT" Advanced Persistent Threat" modernes.
Détection et protection contre les attaques Denial of Service (DoS), et les attaques par Brute Force.
Prend en charge la protection de Spoofing.
Prévention de l'exploitation des vulnérabilités applicatives.
Détection et protection contre les Botnets, les Call-Back (CnC) et prévention des attaques avancées via un module dédié Antispyware en plus de la protection IPS "Intrusion Prevention System".
Détection et protection contre les attaques de reconnaissance IPv4 et IPv6
Le Pare-feu doit permettre de créer et personnaliser les signatures IPS.
Le Pare-feu doit permettre d'Exiger une authentification forte ou multi-facteurs (MFA " Multi Factor Authentication ") pour les applications critiques et sensibles via des règles spécifiques.
Protection par réputation basée sur des feeds provenant d'autres sources SIEM " Security Information and Event Management ", Threat Intelligence ou un système de partage de feeds et IoC " Indicators of Compromise".
Le Pare-feu doit permettre de filtrer les données et prévenir la fuite par type/propriété de fichier, Metadata, Tag, Classification…
Mise à jour automatique des signatures.
4. Antivirus/Anti-Spyware
Prise en charge de l'analyse anti malware et anti spyware par application

Analyse des fichiers contre les malwares pour les échanges à travers les protocoles http, http2, ftp " File Transfer Protocol", imap " Internet Message Access Protocol", pop3, smtp " Simple Mail Transfer Protocol" et smb" Server Message Block".
Protection par Technologie de Sandboxing, via les signatures et feeds sans avoir besoin d'envoyer les fichiers vers un cloud public.
Offre la possibilité de choisir les types de fichier à analyser dans un Sandbox en cloud.
Détection et blocage des malwares utilisant les Call-Back (CnC).
Protection contre les botnets par signature basée sur le DNS " Domain Name System ".
Fonctionnalités de DNS " Domain Name System " Sinkholing pour détecter les attaques DNS " Domain Name System "et les domaines malveillants et identifier les machines potentielles infectées.
Possibilité de définir des signatures personnalisées pour les spywares.
5. Filtrage URL et Filtrage de contenu
Filtrage et Inspection des flux HTTP, HTTPS, HTTP2
Filtrage URL à base de catégories web
Identification du phishing et spear-phishing par moteur machine learning
Prévention et Protection contre le vol des informations d'authentification active directory (compte/mot de passe) configurable par url et par catégorie web.
Prévention et analyse des Scripts malveillants dans les pages web par moteur machine learning
Inspection des flux chiffrés TLS 1.3 sans dégradation en TLS 1.2 ou inférieur
Validation des certificats des serveurs (CRL, Algorithm, Cipher…) pour les flux HTTPS et SSH " Secure Shell".
Filtrage des liens de phishing dans les e-mails, des sites de phishing,
Filtrage des commandes et contrôles basés sur HTTP et les pages contenant des kits d'exploits.
Filtrage des données en fonction du type de fichier, propriété de fichier, Metadata, mot cléss…
Support de la réécriture du champ d'en-tête HTTP X-Forwarded-For.
Mise à jour de la base des URL en temps réel.
6. Sécurité DNS "Domain Name System "

Protection DNS "Domain Name System " sur la base des catégories DNS.
Protection en ligne contre les domaines malveillants, indépendamment de la base de filtrage url.
Blocage des requêtes DNS malveillantes et identification des machines infectées via le mécanisme Sinkhole avec automatisation des réponses (isolation de la machine via politique dynamique).
Blocage des nouveaux domaines malveillants
Détection des attaques DNS : DGA, DNS Tunneling, DNS Dangling, DNS rebinding…
Alimentation en continu des bases des domaines des cybercriminels identifiés en temps réel.
7. Gestion de la bande passante
Réservation et Priorisation des flux en fonction de la source, la destination, l'utilisateur, ou l'application
Limitation de la bande passante par source, destination, application ou catégorie d'application.
8. Identification et authentification des utilisateurs
Identification des utilisateurs depuis Active Directory
Prendre en charge les services d'authentification suivants pour l'identification des utilisateurs :● Microsoft Exchange/● eDirectory /● Kerberos ● Radius/● Authentification par Certificat client/● Portail captif
Identification des utilisateurs via parsing Syslog, XML API et intégration contrôleur WLAN.
Prend en charge la création d'une stratégie de sécurité basée sur les utilisateurs et les groupes Active Directory en plus de l'adresse IP source/destination.
Intégration avec Active Directory pour authentifier les utilisateurs via Single Sign-On (SSO) Kerberos sans déploiement d'agent.
Les utilisateurs Citrix et services Terminal Server doivent être pris en charge dans la politique et les journaux.
Intégration avec solution d'authentification par OTP " One-Time Password" .
Intégration native avec les solutions d'authentification de MFA " Multi-factor Authentication " : RSA, Okta, PingID et Duo.
9. Fonction VPN " Virtual Private Network "
Support natif du VPN " Virtual Private Network " IPSec site-site et client-site
Support du VPN " Virtual Private Network " , SSL " Secure Sockets Layer "
Support IKEv1 et IKEv2 avec authentification à base de clé pré-partagée (PSK) ou certificat (RSA, ECDSA)
Standard de Chiffrement : 3DES, AES 256 au minimum
Algorithme de contrôle d'intégrité : MD5, SHA-256, SHA-384, SHA-512
Authentification transparente pour les clients VPN " Virtual Private Network " via mécanisme pre-logon (connexion avant ouverture de la session windows) et SSO "Single Sign-On".
Agent VPN pour Windows et Mac.
10. Fonctions d'Administration et gestion des journaux :

Administration via une interface web intuitive et sécurisée en HTTPS intégrée dans le NGFW.
Interface d'administration graphique multi-langues : Français et Anglais au minimum
Administration en ligne de commande SSH et Telnet.
Supporte l'administration par rôle.
Prise en charge et gestion du versioning des configurations après chaque changement.
Possibilité de revenir à une version ancienne en cas de besoin.
Permettre l'export et l'importation de la configuration.
Permettre la comparaison entre deux versions de configuration avec indication des changements entre les versions.
Suivie et visibilité en temps réel sur les flux transitant par le Pare-feu avec possibilité de filtrage par simple clique.
Outil de filtrage et recherche multicritère dans les journaux pour faciliter l'identification des incidents de sécurité.
Outil intégré dans la console de gestion pour l'optimisation des règles ; identification des règles permissive, identification des règles dupliquées et dormantes…
Outil de test et validation des politiques: par utilisateur/groupe, ip source, ip destination, application, service/port, catégorie et type de device source.
Différente vue pour les journaux : Flux, Menaces, Filtrage url, Filtrage de contenu, Authentification, décryptage, Configurations, Systèmes, Alarmes…
Prise en charge des étiquettes (tags) pour l'organisation des règles et des objets.
Prise en charge des étiquettes dynamiques pour l'application des règles de sécurité en fonction des événements et incidents de sécurité.
Identification de l'utilisateur journalisée corrélée en temps réel
Gestion des Rapports prédéfinis et personnalisables : Top Utilisateurs, Top Applications, Top Menaces, Les tendances de menaces…
Intègre un outil graphique de capture de paquet.
Outil intégré de suivi en temps réel des sessions ouvertes avec l'ensemble des détails de la session (session id, ip src, ip dst, utilisateur, application, timestamp, nat ip, port src, port dst, state, catégorie url, règle…)
Permettre de terminer une session en cours depuis l'interface de gestion et suivi des sessions.
Outils de supervision des attaques, réseaux, utilisation d'application…
Export des journaux vers des systèmes externes en Syslog et Intégration avec des solutions SIEM" Security Information and Event Management "

Le Pare-feu doit permettre de générer des notifications et des messages Syslog, Email, Http et SNMP " Simple Network Management Protocol " pour les événements et incidents de sécurité
Le Pare-feu doit inclure une autorité de certification X.509 interne qui peut générer des certificats pour les passerelles et les utilisateurs.
Le Pare-feu doit inclure la possibilité d'utiliser des autorités de certification externes,
Le Pare-feu doit supporter l'intégration avec un HSM " Hardware Security Module " pour le stockage des clés privées.
Le Pare-feu doit interdire l'export des clés privées des AR ou Intermédiaires.
Supporte Netflow
Supporte le SNMPv3 "" Simple Network Management Protocol "
La Gestion des journaux et rapports intégrés au Pare-feu avec stockage des logs dans le disque SSD local, aucune solution pour la gestion des journaux ne doit être imposée.
11. Bonnes pratiques et Conformité aux Standards de sécurité:
Le Pare-feu proposé doit offrir un outil d'audit, revue et recommandation automatisée pour valider les bonnes pratiques des configurations et les contrôles de sécurités selon les standards de sécurité afin de permettre au Département de: • Améliorer la posture de sécurité - S'assurer que les meilleures pratiques des experts, standards et framework NIST, CIS sont respectées. • Aider à déployer et mettre en œuvre les meilleures pratiques facilement grâce à l'assistant de configuration. • Optimiser le retour sur investissement - Tirer le meilleur parti des fonctionnalités NGFW grâce à des configurations fondées sur les meilleures pratiques et éviter les vulnérabilités de configuration (configuration inappropriée).

Le prestataire devra prévoir l'ensemble des accessoires nécessaires à la mise en rack, à la connexion et l'interconnexion des deux appliances proposées et la mise en service des fonctions de haute-disponibilité (**Kits de montage, câbles réseaux, Jarretières optiques, SFP, SFP+**, câbles électriques, etc.).

➢ **Prestations**

Le prestataire est tenu de :

- Effectuer les travaux de pose, d'installation et de configuration des matériels livrés.
- Livrer le manuel d'installation du matériel ;
- Assurer un transfert de compétences pour trois (03) personnes relatives à l'installation et la configuration du Pare-feu proposé.

Le titulaire est tenu de communiquer le compte lié à la gestion de la garantie du matériel livré. Ce compte doit être au nom de Département de l'Artisanat et de l'Economie Sociale et Solidaire et doit

permettre la vérification de l'état de garantie, l'accès à la documentation et aux bases de connaissances ainsi que le téléchargement des mises à jour.

PRIX 2 : PASSERELLE EMAIL SECURISEE

Le soumissionnaire devra proposer deux (2) Appliances physiques en haute disponibilité (Actif /Passif)

La passerelle email sécurisée devra répondre, **au minimum**, aux spécifications indiquées dans le tableau suivant :

Caractéristiques
La passerelle doit permettre l'analyse des messages entrants et sortants pour **500 utilisateurs.**
La passerelle proposée doit intégrer les modules suivants : - Email Pare-feu - Anti-spam - Anti-virus - Classificateur d'imposteurs - Système de réputation dynamique - Analyse des URLs et pièces jointes
La passerelle doit être nommée leader dans The Forrester Wave™ du marché 'Enterprise Email Security' Q2 2021
La passerelle cible doit être d'un constructeur classé parmi les leaders dans le rapport Magic Quadrant de Gartner
Elle doit offrir les fonctionnalités minimales suivantes :
Supporte les protocoles suivants: SMTP " Simple Mail Transfer Protocol ", ESMTP " Extended Simple Mail Transfer Protocol " , SMTPS " Simple Mail Transfer Protocol /Secure ", IMAP "" Internet Message Access Protocol " , IMAPS "" Internet Message Access Protocol /Secure"
Authentification des messages entrant : SPF "Sender Policy Framework, ", DKIM "DomainKeys Identified Mail" et DMARC "Domain-based Message Authentication, Reporting, and Conformance ".
Possibilité de signature message sortant : DKIM
Politiques et fonctionnalités :
Règles personnalisables pour scanner les messages et les pièces jointes entrants et sortants;
Support multi-domaines;
Capacité de routage de domaines vers des serveurs différents et support de routage LDAP "Lightweight Directory Access Protocol";
Stratégies flexibles pour cibler les expéditeurs ou les destinataires par entreprise, par groupe ou par individu;
Gestion des autorisations, filtrage, mise en quarantaine, blocage, notification et reporting;
Comptabilité avec les annuaires pour l'authentification des administrateurs et des utilisateurs (LDAP , Active Directory , Radius)
Offrir une gestion de quarantaine centralisée pour les administrateurs

Envoie des rapports dynamiques et personnalisables aux utilisateurs pour la gestion des emails en quarantaines
Offrir aux utilisateurs la consultation et la gestion de leurs messages en quarantaine via email et interface web
Offrir aux administrateurs la possibilité de prévaloir une autre action que celle choisie par l'utilisateur
Blocage des emails en provenance des domaines non approuvés par le ministère avec autorisation pour un sous ensemble d'utilisateurs;
Gestion avancée des files d'attente
Classification des menaces dans des quarantaines distinctes centralisées (spam, phishing, bulk, adulte…), avec la possibilité de créer d'autre quarantaines.
Filtrage de contenu :
Protection contre les attaques au président (Business Email Compormise - BEC) grâce à un classificateur d'imposteur en utilisant le moteur supernova
Une analyse multicritère des messages afin de détecter les courriers indésirables qui doivent pouvoir être traités de différentes façons, telles que: rejet, mise en quarantaine, modification de l'objet.
Filtrage en temps réel du contenu des e-mails: identifier et prévenir un grand éventail de violations des règles établies pour les e-mails entrants et sortants, notamment le langage offensant, le harcèlement.
Analyse et filtrage de graymail
Application des règles de filtrage en se basant sur les caractéristiques des pièces jointes, des lexiques, et d'autres identifiants (adresse mail interne/externe...).
Fonctions de protection et de sécurité (Filtrage Email , antispam, antivirus et Système de réputation dynamique
Protection contre les attaques de type Directory HarvestAttack
Protection contre toute forme d'attaques de type Deni de Service (DoS) ou mail bombing.
Mécanisme BATV (Bounce Address Tag Validation) pour protéger l'infrastructure de messagerie contre les attaques de type 'Bounce'.
Protection multi-niveaux contre les attaques spam, basée sur de l'intelligence artificielle et sur une analyse de réputation dynamique.
Protection contre les menaces mixtes, virus, chevaux de troie, vers, programmes espions, Url malveillant, logiciels publicitaires, spam, phishing, Vers informatiques (Worm), rançongiciel;
Protection multicouche avec un service de gestion dynamique de la réputation des emails pour bloquer les connexions à partir des adresses IP malveillantes ;
Une détection efficace des menaces, du spam et des attaques ciblées (spear phish, codes malicieux) avec une moyenne de 99,8%
Un taux de faux positifs (un message valide jugé par erreur comme étant un spam) et de faux négatifs (un message spam jugé par erreur comme étant un valide) sont inférieurs à 1/350000.
Un mécanisme d'apprentissage machine 'Machine Learning' capable d'acquérir de nouvelles définitions de spam en temps réel, et ainsi rester à jour et efficace même face aux dernières générations de spams.

Une protection garantie de 100% contre les virus et les infections à travers: - Un moteur anti-virus de détection à base de signatures, tout en offrant le choix au moins entre 2 moteurs anti-virus à base de signatures. - Une protection antivirus 'zero-hour' protégeant contre les nouveaux virus et toute autre forme de code malicieux, immédiatement après leur apparition et jusqu'à la mise à jour des bases de signatures.
Analyse dynamique du contenu des en-têtes et des messages pour identifier les attaques d'usurpation de domaine, d'usurpation de nom
Une liste noire dynamique bloquant les messages entrants en fonction de I'adresse IP, du domaine ou de l'adresse e-mail.
Une liste blanche définie par l'administrateur (expéditeur, relais, nom de domaine)
Interception de spam en utilisant le moteur MLX " Machine Learning Extreme " et en combinant multiples techniques de protection à savoir l'apprentissage machine, la protection multicouche contre les virus, l'analyse de réputation dynamique et la gestion granulaire de politique
Contrôle des envois massifs des message (bulk email) , avec la flexibilité de choisir le type des email massif sans utiliser la configuration de la liste blanche/ noir (whitelisting/blacklisting).
Protection contre les attaques ciblées :
Protection contre les URL compromises incluses dans les messages : Bloquer et mettre en quarantaine les messages avec des URL malveillantes afin qu'ils n'atteignent jamais la boîte de réception, ou que les utilisateurs cliquent dessus et compromettent le système, en se basant sur des rapports connus relatifs à cette même URL (vérification de réputation), La passerelle devra permettre d'analyser un nombre illimité de liens URL / pièce jointes /
La réécriture des URL (TXT, RTF et HTML) qui permet de protéger les utilisateurs, indépendamment du terminal et du réseau auxquels ils sont connectés, et de détecter si un message a été « piégé » après sa remise.
Protection contre les sites de phishing : Fausses pages dropbox, google drive, free mobile, OWA, banques, impôts…
Filtrage des pièges jointes par type (exécutables, documents office, PDF, JS, fichiers compressés,html, etc .) L'analyse des pièces jointes peut se faire à travers la réputation du hachage sans téléchargement du fichier dans le cloud.
Protection contre les nouvelles campagnes Dridex dès le premier fichier évitant le besoin de ré-imager la machine infectée.
Alertes temps réel en cas d'infection.
Monitoring et visibilité des menaces reçues.
Avoir une vue en temps réel pour voir combien et quels types de menaces sont reçues actuellement, ainsi que des détails qui permettent d'identifier les utilisateurs ciblés et de savoir si des messages ont été effectivement livrés.
Mettre en évidence les campagnes d'attaque de grande envergure et des menaces ciblées de ransomware, et voir les attaques ciblant les cadres dirigeants et d'autres collaborateurs présentant un intérêt pour les cybercriminels.
Tableau de bord offrant une visibilité sur toutes les informations concernant la détection, l'analyse, le suivi des clics : identifier les VAP (very attacked person) / C-Level à risque, les personnes très attaquées dans l'organisation et les top cliqueurs , ainsi que la classification des attaques

Permettre à l'administrateur de générer et exporter les rapports des attaques avec les détails suivants : volume, propagation, vulgarisation, aperçu, utilisateurs cibles, infectés et à risque, et typologie des menaces.
Administration/reporting
Mise à jour régulière et automatique de l'ensemble des bases de protection
Une console de gestion Web centralisée et simplifiée.
Authentification avec mot de passe sur le portail Web/ CLI, pour les administrateurs.
Une granularité des droits d'administration, et délégation de l'administration, règles, quarantaine, reporting à des administrateurs locaux.
Tableau de bord permettant à l'administrateur/utilisateur d'examiner efficacement le statut et les performances de la passerelle.
Des journaux d'activité détaillés, en particulier concernant la transmission et le traitement des emails. Ces journaux seront stockés sur la passerelle mais pourront être exportés vers un serveur distant.
Traçage des messages en temps réel;
L'interface d'administration permettra idéalement de prendre connaissance du traitement des messages, de façon graphique.
Alertes par e-mail, et/ou SNMP " Simple Network Management Protocol "
Configuration des rapports automatisés et personnalisés avec des paramètres pertinents comme les intervalles, les utilisateurs, les taux et les politiques.
Génération des rapports de genre (Nombre de Spam détectés, virus détectés, mails analysés etc…) et ce à une durée de rétention spécifique.
Rapports en format csv et html, PDF
Dimensionnement – Appliance physique
La passerelle devra être sous forme d'Appliance physique avec les caractéristiques minimales suivantes : - Alimentation redondante - 2 Interfaces réseau 1GB - 32 GB de RAM - CPU Intel Xeon (4 cores) - Capacité de stockage 2 x 600GB SATA en RAID 1

Le prestataire devra prévoir l'ensemble des accessoires nécessaires à la mise en rack, à la connexion et l'interconnexion des deux appliances proposées et la mise en service des fonctions de haute-disponibilité.

➢ **Prestations**

Le prestataire est tenu de :

- Effectuer les travaux de pose, d'installation et de configuration des matériels livrés.
- Livrer le manuel d'installation du matériel ;
- Assurer un transfert de compétences pour trois (03) personnes relatives à l'installation et la configuration de la Passerelle email proposée.

Le titulaire est tenu de communiquer le compte lié à la gestion de la garantie du matériel livré. Ce compte doit être au nom de Département de l'Artisanat et de l'Economie Sociale et Solidaire et doit permettre la vérification de l'état de garantie, l'accès à la documentation et aux bases de connaissances ainsi que le téléchargement des mises à jour.

CHAPITRE III : BORDEREAU DES PRIX DETAIL ESTIMATIF

BORDEREAU DES PRIX DETAIL ESTIMATIF

N° des Prix	Désignation des prestations	Unité de mesure ou de compte	Qté	Prix Unitaire en Dirhams Hors TVA En Chiffres	Prix Total en Dirhams Hors TVA En Chiffres
1	PARE-FEU NOUVELLE GENERATION	U	1		
2	PASSERELLE EMAIL SECURISEE	U	1		
TOTAL HORS T.V.A :					
TAUX T.V.A 20 % :					
TOTAL T.T.C :					

Fait à ……..le ……...

(signature et cachet du concurrent)

DERNIERE PAGE

APPEL D'OFFRES N° 06/IN/2022

OBJET : Achat de matériel informatique pour la sécurité informatique (Pare-feu et Passerelle de messagerie sécurisée) pour le compte du Département de l'Artisanat et de l'Economie Sociale et Solidaire en lot unique.

Pour un montant de : .....

PRESENTE PAR :

Houda KHALID

Chef de Division
des Systèmes d'Information

A....., LE :...../..../.....

VERIFIE PAR :

LARGUOU Abderrahim

Chef du Service de Comptabilité
et des Achats

A....., LE :...../..../.....

LU ET ACCEPTE PAR :
(Le Prestataire)

A..... LE :...../...../.....

LE MAITRE D'OUVRAGE :

Chef de la Division de la Gestion du Budget
et des Outils Généraux par intérim

Hajar CHEBAB

A..... LE :...../...../.....

VISE PAR :

A..... LE :...../...../.....

APPROUVE PAR :

A....., LE :...../...../.....