**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 |

**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**

1. **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) :

-----------------------------------------------------------------------------------------------------------------

1. **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 aux 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

**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** |
| --- | --- | --- | --- |
| **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** |  |  |
|  | **Fonctions Firewall**   * Doit intégrer un système d’exploitation propriétaire sécurisé, * Filtrage de paquets et être doté de la fonction de filtrage dynamique, * Filtrage basé sur les applications niveau 7 en plus des ports/Protocol et par plages de ports UDP ou TCP * Filtrage et inspection en IPv4 et IPv6, * Failover de connexion Internet, * Prise en compte de paramètre Horaire dans les règles de filtrage, * Doit fournir, via sa console d’administration, des statistiques sur le nombre d'accès aux règles de sécurité, * Doit inclure la possibilité de fonctionner en mode transparent ou routé (natté), * Doit fournir la possibilité de définir des instances firewall virtuels sur la même Appliance, et capable d’activer les fonctionnalités de protection IPS, Sandboxing, Control Applicatif, filtrage d’URL, Anti-bot, Anti-virus/Antimalware, * La création de la politique de sécurité basée sur :   + Geolocation par pays   + Zones   + Groupes de Zones   + Applications, Groupes d’applications   + Catégories d’Applications   + Technologies d’Applications   + Filtres d’Applications   + Utilisateurs et Groupes   + Adresses IP, Groupes d’adresses IP, Sous-réseaux IP, Groupes de sous-réseaux IP   + Services, Groupes de Services * La solution doit être de type Next Generation Firewall avec capacité de prévention contre les menaces avancées, combinée avec des fonctionnalités de base suivantes (**licences incluses)** : * **IPS (prévention des intrusions)** pour se protéger contre les menaces réseau telles que vers, chevaux de Troie et autres programmes malveillants. Le système de prévention des intrusions (IPS) doit aussi apporter une protection contre les menaces réseaux existantes et émergentes. Ce module IPS doit avoir deux mécanismes : * Détection par signatures ; * Détection par anomalies ; * Capable de faire des analyses comportementales de tout type de trafic ; * Possibilité de créer des signatures personnalisées ; * Mise à jour automatique des signatures IPS ; * Création et affectation des politiques IPS par type de zone ou interface ; * Pour chaque événement d’attaque, il sera possible de laisser passer ou bloquer, de faire une mise en quarantaine automatique (IP totalement bloquée pendant un temps donné) … ; * Gestion de profils IPS avec association à certains trafics dans la politique de filtrage (IP source, IP destination, service, protocole, réseau…) ; * **Filtrage URL**,pour assurer le contrôle de l’accès interne aux contenus Web indésirables, non productifs, voire illégaux, * **Control Applicatif,** afin d’identifier, reconnaître et contrôler les applications dans les flux, | **Marque :**  **Référence :**  **Caractéristiques proposées** |  |
|  | **Spécifications matérielles et performance :**   * Format : Appliance Rackable, 19’’ * 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 * Nombre de sessions inspectées simultanées : **1 Million** Minimum * Nombre de nouvelles sessions par seconde : **50 000** Minimum * Stockage Disque dur dédiée de type SSD de **200** GB Minimum * Les ports (en dehors des ports de management et de la haute disponibilité)   + Minimum 8 ports 10/100/1000 BaseT   + Minimum 4 ports 1G/10G SFP/SFP+ dont **4** avec **Transceiver SFP+** * Les ports de management et Clustering :   + Minimum 1 port 10/100/1000 BaseT pour le management   + Minimum 1 port console RJ-45   + Minimum 1 port USB   + Minimum 1 ports 10/100/1000 BaseT pour le HA   2 Alimentations électriques Redondantes Minimum (AC), |  |  |
|  | **Support de la haute disponibilité** :   * Actif/Actif avec synchronisation d’état de session, * Actif/Passif, |  |  |
|  | **Contrôle applicatif :**   * Identification des applications en se basant sur :   + Signatures   + Décodage du protocole (respecte la spécification du protocole)   + Déchiffrement du trafic encapsulé * Identification et contrôle des applications partageant la même connexion * Contrôle de la fonction de transfert de fichiers d’une application * Visibilité du trafic applicatif inconnu à travers l’identification de sa nature :   + Volume du trafic   + Utilisateur et/ou adresses IP   + Port utilisé   + Contenu associé : fichier, menace ou autre. * La base de données de contrôle des applications doit contenir plus de **3 000** applications connues ;   La solution doit pouvoir créer une règle de filtrage avec plusieurs catégories ; |  |  |
|  | **Identification, authentification des utilisateurs et protection des identités**   * Prise en charge des services d'authentification suivants pour l'identification et authentifications des utilisateurs :   + Active Directory   + Kerberos   + LDAP   + Radius   + Base Locale   + SAML   + Authentification via SSO Kerberos sans agent   + Authentification par Certificat client   + Portail captif * Identification des utilisateurs indépendamment :   + Du terminal (ordinateur, un téléphone intelligent ou une tablette)   + Du système d’exploitation utilisé,   + Des adresses IP et de la zone (LAN, VPN, hors du périmètre du réseau) |  |  |
|  | **Fonctions Réseau :**   * Support mode Routage, mode transparent, TAP ou SPAN, * Support IPv4 et IPv6 * Routage IPv4 : Statique et Dynamique, RIPv2, OSPFv3 et BGP au minimum * Agrégation des liens 802.3ad, LACP * Support des VLAN 802.1q * Support des modes de translations NAT et PAT * Nat dynamique, Nat Statique, Nat par port, Nat64 * Support de Multicast * 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)** |  |  |
|  | **Fonction VPN :**   * VPN IPSec site-site, client-site et hub & Spoke. **(Fonctionnalité et licence à fournir)** * Support du VPN SSL mode portail et mode tunnel (avec ou sans agent) * Support du Tunnel GRE * Support de IKEv1 et IKEv2 avec authentification à base de clé pré-partagée (PSK) ou certificat * Standard de Chiffrement : 3DES, AES 256 au minimum * Algorithme de contrôle d’intégrité : MD5, SHA-256, SHA-384, SHA-512, |  |  |
|  | **Gestion de la bande passante :**   * Réservation et Priorisation des flux en fonction de la source, la destination, l’utilisateur et l’application,   Limitation de la bande passante par source, destination, application ou catégorie d’application. |  |  |
|  | **Administration et gestion des journaux :**   * Administration via une interface web intuitive et sécurisée en HTTPS, * Administration en ligne de commande SSH et Telnet, * Interface d’administration graphique multi-langues : Français et Anglais au minimum, * Support de l’administration par rôle, * Permettre l’export et l’importation de la configuration, * Suivie et visibilité en temps réel sur les flux transitant par le firewall avec possibilité de filtrage, * Outil de filtrage et recherche multicritère dans les journaux pour faciliter l’identification des incidents de sécurité. * Prise en charge de balises (tags) pour l’organisation des règles et des objets. * Différente vue pour les journaux : Flux, Menaces, Filtrage de contenu, Authentification, Systèmes * Vue synthétique des applications, menaces et URL, * Export des journaux vers des systèmes externes en Syslog et Intégration avec des solutions SIEM * Support de SNMPv3 * Journalisation locale dans le disque du NGFW sans dégradation des performances. * La solution doit inclure une autorité de certification x.509 interne qui peut générer des certificats pour les passerelles et les utilisateurs pour permettre une authentification facile sur les VPN, * La solution doit inclure la possibilité d'utiliser des autorités de certification externes, * La visionneuse de journaux doit avoir la possibilité de créer un filtre en utilisant les noms d'objets prédéfinis (hôtes, réseau, groupes, utilisateurs...), |  |  |
|  | **Filtrage URL** **et Filtrage de contenu**   * Filtrage HTTP, HTTPS, HTTP2 ; * Filtrage URL à base de catégories ; * Inspection des flux chiffrés TLS 1.3 ; * Validation des certificats des serveurs (CRL, Algorithm, Cipher…) ; * Filtrage URL à base de l’adresse IP ; * Filtrage des liens de phishing dans les e-mails, des sites de phishing ; * Filtrage des commandes et contrôles basés sur HTTP et les pages contenant des kits d’exploits ; * Filtrage des données en fonction du type de fichier, propriété de fichier, Metadata, mot clés… * Mise à jour de la base des URL. |  |  |
| **1.2** | **PRESTATION DE SERVICE**  Le prestataire doit proposer dans son offre toutes les prestations nécessaires à la mise en œuvre de la solution de sécurité :   * Ingénierie et définition de l’architecture finale ; * Analyse du plan d’adressage IP, de routage et de découpage VLAN ; * Intégration de la solution dans le réseau de la CMC ; * L’interconnexion du NGFW avec les Switch Datacenter ; * L’installation et la configuration des fonctions du pare feu nouvelle génération selon les bonnes pratiques et les standards de la sécurité ; * La définition de la matrice des flux ; * Le prestataire doit réaliser tout essai jugé nécessaire pour s’assurer de la conformité et du bon fonctionnement de la plateforme de sécurité ; * Transfert de compétence ; * Garantie et maintenance (couvre l’assistance (sur site ou à distance), l’intervention sur site, les pièces de rechanges et la main d’œuvre) pour une durée 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 ; * Livrables :   + Document d’architecture finale et de configuration de la solution (avec schéma au format exploitable et un fichier de configuration) ;   Manuel d’exploitation ; |  |  |

**BORDEREAU DES PRIX – DETAIL ESTIMATIF**

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

| **Items N°** | **Désignations** | **Unité** | **(1)**  **QTE** | **(2)**  **Prix unitaire**  **HT/HDD/HTVA** | **(3)**  **Prix total HT/HDD/HTVA**  **(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**

**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** |
| --- | --- | --- | --- |
| **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** |  |  |
|  | **Fonctions Firewall**   * Doit intégrer un système d’exploitation propriétaire sécurisé, * Filtrage de paquets et être doté de la fonction de filtrage dynamique, * Filtrage basé sur les applications niveau 7 en plus des ports/Protocol et par plages de ports UDP ou TCP * Filtrage et inspection en IPv4 et IPv6, * Failover de connexion Internet, * Prise en compte de paramètre Horaire dans les règles de filtrage, * Doit fournir, via sa console d’administration, des statistiques sur le nombre d'accès aux règles de sécurité, * Doit inclure la possibilité de fonctionner en mode transparent ou routé (natté), * Doit fournir la possibilité de définir des instances firewall virtuels sur la même Appliance, et capable d’activer les fonctionnalités de protection IPS, Sandboxing, Control Applicatif, filtrage d’URL, Anti-bot, Anti-virus/Antimalware, * La création de la politique de sécurité basée sur :   + Geolocation par pays   + Zones   + Groupes de Zones   + Applications, Groupes d’applications   + Catégories d’Applications   + Technologies d’Applications   + Filtres d’Applications   + Utilisateurs et Groupes   + Adresses IP, Groupes d’adresses IP, Sous-réseaux IP, Groupes de sous-réseaux IP   + Services, Groupes de Services * La solution doit être de type Next Generation Firewall avec capacité de prévention contre les menaces avancées, combinée avec des fonctionnalités de base suivantes (**licences incluses)** : * **IPS (prévention des intrusions)** pour se protéger contre les menaces réseau telles que vers, chevaux de Troie et autres programmes malveillants. Le système de prévention des intrusions (IPS) doit aussi apporter une protection contre les menaces réseaux existantes et émergentes. Ce module IPS doit avoir deux mécanismes : * Détection par signatures ; * Détection par anomalies ; * Capable de faire des analyses comportementales de tout type de trafic ; * Possibilité de créer des signatures personnalisées ; * Mise à jour automatique des signatures IPS ; * Création et affectation des politiques IPS par type de zone ou interface ; * Pour chaque événement d’attaque, il sera possible de laisser passer ou bloquer, de faire une mise en quarantaine automatique (IP totalement bloquée pendant un temps donné) … ; * Gestion de profils IPS avec association à certains trafics dans la politique de filtrage (IP source, IP destination, service, protocole, réseau…) ; * **Filtrage URL**,pour assurer le contrôle de l’accès interne aux contenus Web indésirables, non productifs, voire illégaux, * **Control Applicatif,** afin d’identifier, reconnaître et contrôler les applications dans les flux, | **Marque :**  **Référence :**  **Caractéristiques proposées** |  |
|  | **Spécifications matérielles et performance :**   * Format : Appliance Rackable, 19’’ * 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 * Nombre de sessions inspectées simultanées : **1 Million** Minimum * Nombre de nouvelles sessions par seconde : **50 000** Minimum * Stockage Disque dur dédiée de type SSD de **200** GB Minimum * Les ports (en dehors des ports de management et de la haute disponibilité)   + Minimum 8 ports 10/100/1000 BaseT   + Minimum 4 ports 1G/10G SFP/SFP+ dont **4** avec **Transceiver SFP+** * Les ports de management et Clustering :   + Minimum 1 port 10/100/1000 BaseT pour le management   + Minimum 1 port console RJ-45   + Minimum 1 port USB   + Minimum 1 ports 10/100/1000 BaseT pour le HA   2 Alimentations électriques Redondantes Minimum (AC), |  |  |
|  | **Support de la haute disponibilité** :   * Actif/Actif avec synchronisation d’état de session, * Actif/Passif, |  |  |
|  | **Contrôle applicatif :**   * Identification des applications en se basant sur :   + Signatures   + Décodage du protocole (respecte la spécification du protocole)   + Déchiffrement du trafic encapsulé * Identification et contrôle des applications partageant la même connexion * Contrôle de la fonction de transfert de fichiers d’une application * Visibilité du trafic applicatif inconnu à travers l’identification de sa nature :   + Volume du trafic   + Utilisateur et/ou adresses IP   + Port utilisé   + Contenu associé : fichier, menace ou autre. * La base de données de contrôle des applications doit contenir plus de **3 000** applications connues ;   La solution doit pouvoir créer une règle de filtrage avec plusieurs catégories ; |  |  |
|  | **Identification, authentification des utilisateurs et protection des identités**   * Prise en charge des services d'authentification suivants pour l'identification et authentifications des utilisateurs :   + Active Directory   + Kerberos   + LDAP   + Radius   + Base Locale   + SAML   + Authentification via SSO Kerberos sans agent   + Authentification par Certificat client   + Portail captif * Identification des utilisateurs indépendamment :   + Du terminal (ordinateur, un téléphone intelligent ou une tablette)   + Du système d’exploitation utilisé,   + Des adresses IP et de la zone (LAN, VPN, hors du périmètre du réseau) |  |  |
|  | **Fonctions Réseau :**   * Support mode Routage, mode transparent, TAP ou SPAN, * Support IPv4 et IPv6 * Routage IPv4 : Statique et Dynamique, RIPv2, OSPFv3 et BGP au minimum * Agrégation des liens 802.3ad, LACP * Support des VLAN 802.1q * Support des modes de translations NAT et PAT * Nat dynamique, Nat Statique, Nat par port, Nat64 * Support de Multicast * 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)** |  |  |
|  | **Fonction VPN :**   * VPN IPSec site-site, client-site et hub & Spoke. **(Fonctionnalité et licence à fournir)** * Support du VPN SSL mode portail et mode tunnel (avec ou sans agent) * Support du Tunnel GRE * Support de IKEv1 et IKEv2 avec authentification à base de clé pré-partagée (PSK) ou certificat * Standard de Chiffrement : 3DES, AES 256 au minimum * Algorithme de contrôle d’intégrité : MD5, SHA-256, SHA-384, SHA-512, |  |  |
|  | **Gestion de la bande passante :**   * Réservation et Priorisation des flux en fonction de la source, la destination, l’utilisateur et l’application,   Limitation de la bande passante par source, destination, application ou catégorie d’application. |  |  |
|  | **Administration et gestion des journaux :**   * Administration via une interface web intuitive et sécurisée en HTTPS, * Administration en ligne de commande SSH et Telnet, * Interface d’administration graphique multi-langues : Français et Anglais au minimum, * Support de l’administration par rôle, * Permettre l’export et l’importation de la configuration, * Suivie et visibilité en temps réel sur les flux transitant par le firewall avec possibilité de filtrage, * Outil de filtrage et recherche multicritère dans les journaux pour faciliter l’identification des incidents de sécurité. * Prise en charge de balises (tags) pour l’organisation des règles et des objets. * Différente vue pour les journaux : Flux, Menaces, Filtrage de contenu, Authentification, Systèmes * Vue synthétique des applications, menaces et URL, * Export des journaux vers des systèmes externes en Syslog et Intégration avec des solutions SIEM * Support de SNMPv3 * Journalisation locale dans le disque du NGFW sans dégradation des performances. * La solution doit inclure une autorité de certification x.509 interne qui peut générer des certificats pour les passerelles et les utilisateurs pour permettre une authentification facile sur les VPN, * La solution doit inclure la possibilité d'utiliser des autorités de certification externes, * La visionneuse de journaux doit avoir la possibilité de créer un filtre en utilisant les noms d'objets prédéfinis (hôtes, réseau, groupes, utilisateurs...), |  |  |
|  | **Filtrage URL** **et Filtrage de contenu**   * Filtrage HTTP, HTTPS, HTTP2 ; * Filtrage URL à base de catégories ; * Inspection des flux chiffrés TLS 1.3 ; * Validation des certificats des serveurs (CRL, Algorithm, Cipher…) ; * Filtrage URL à base de l’adresse IP ; * Filtrage des liens de phishing dans les e-mails, des sites de phishing ; * Filtrage des commandes et contrôles basés sur HTTP et les pages contenant des kits d’exploits ; * Filtrage des données en fonction du type de fichier, propriété de fichier, Metadata, mot clés… * Mise à jour de la base des URL. |  |  |
| **1.2** | **PRESTATION DE SERVICE**  Le prestataire doit proposer dans son offre toutes les prestations nécessaires à la mise en œuvre de la solution de sécurité :   * Ingénierie et définition de l’architecture finale ; * Analyse du plan d’adressage IP, de routage et de découpage VLAN ; * Intégration de la solution dans le réseau de la CMC ; * L’interconnexion du NGFW avec les Switch Datacenter ; * L’installation et la configuration des fonctions du pare feu nouvelle génération selon les bonnes pratiques et les standards de la sécurité ; * La définition de la matrice des flux ; * Le prestataire doit réaliser tout essai jugé nécessaire pour s’assurer de la conformité et du bon fonctionnement de la plateforme de sécurité ; * Transfert de compétence ; * Garantie et maintenance (couvre l’assistance (sur site ou à distance), l’intervention sur site, les pièces de rechanges et la main d’œuvre) pour une durée 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 ; * Livrables :   + Document d’architecture finale et de configuration de la solution (avec schéma au format exploitable et un fichier de configuration) ;   Manuel d’exploitation ; |  |  |

**BORDEREAU DES PRIX – DETAIL ESTIMATIF**

**LOT 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/HTVA** | **(3)**  **Prix total HT/HDD/HTVA**  **(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**

**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** |
| --- | --- | --- | --- |
| **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** |  |  |
|  | **Fonctions Firewall**   * Doit intégrer un système d’exploitation propriétaire sécurisé, * Filtrage de paquets et être doté de la fonction de filtrage dynamique, * Filtrage basé sur les applications niveau 7 en plus des ports/Protocol et par plages de ports UDP ou TCP * Filtrage et inspection en IPv4 et IPv6, * Failover de connexion Internet, * Prise en compte de paramètre Horaire dans les règles de filtrage, * Doit fournir, via sa console d’administration, des statistiques sur le nombre d'accès aux règles de sécurité, * Doit inclure la possibilité de fonctionner en mode transparent ou routé (natté), * Doit fournir la possibilité de définir des instances firewall virtuels sur la même Appliance, et capable d’activer les fonctionnalités de protection IPS, Sandboxing, Control Applicatif, filtrage d’URL, Anti-bot, Anti-virus/Antimalware, * La création de la politique de sécurité basée sur :   + Geolocation par pays   + Zones   + Groupes de Zones   + Applications, Groupes d’applications   + Catégories d’Applications   + Technologies d’Applications   + Filtres d’Applications   + Utilisateurs et Groupes   + Adresses IP, Groupes d’adresses IP, Sous-réseaux IP, Groupes de sous-réseaux IP   + Services, Groupes de Services * La solution doit être de type Next Generation Firewall avec capacité de prévention contre les menaces avancées, combinée avec des fonctionnalités de base suivantes (**licences incluses)** : * **IPS (prévention des intrusions)** pour se protéger contre les menaces réseau telles que vers, chevaux de Troie et autres programmes malveillants. Le système de prévention des intrusions (IPS) doit aussi apporter une protection contre les menaces réseaux existantes et émergentes. Ce module IPS doit avoir deux mécanismes : * Détection par signatures ; * Détection par anomalies ; * Capable de faire des analyses comportementales de tout type de trafic ; * Possibilité de créer des signatures personnalisées ; * Mise à jour automatique des signatures IPS ; * Création et affectation des politiques IPS par type de zone ou interface ; * Pour chaque événement d’attaque, il sera possible de laisser passer ou bloquer, de faire une mise en quarantaine automatique (IP totalement bloquée pendant un temps donné) … ; * Gestion de profils IPS avec association à certains trafics dans la politique de filtrage (IP source, IP destination, service, protocole, réseau…) ; * **Filtrage URL**,pour assurer le contrôle de l’accès interne aux contenus Web indésirables, non productifs, voire illégaux, * **Control Applicatif,** afin d’identifier, reconnaître et contrôler les applications dans les flux, | **Marque :**  **Référence :**  **Caractéristiques proposées** |  |
|  | **Spécifications matérielles et performance :**   * Format : Appliance Rackable, 19’’ * 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 * Nombre de sessions inspectées simultanées : **1 Million** Minimum * Nombre de nouvelles sessions par seconde : **50 000** Minimum * Stockage Disque dur dédiée de type SSD de **200** GB Minimum * Les ports (en dehors des ports de management et de la haute disponibilité)   + Minimum 8 ports 10/100/1000 BaseT   + Minimum 4 ports 1G/10G SFP/SFP+ dont **4** avec **Transceiver SFP+** * Les ports de management et Clustering :   + Minimum 1 port 10/100/1000 BaseT pour le management   + Minimum 1 port console RJ-45   + Minimum 1 port USB   + Minimum 1 ports 10/100/1000 BaseT pour le HA   2 Alimentations électriques Redondantes Minimum (AC), |  |  |
|  | **Support de la haute disponibilité** :   * Actif/Actif avec synchronisation d’état de session, * Actif/Passif, |  |  |
|  | **Contrôle applicatif :**   * Identification des applications en se basant sur :   + Signatures   + Décodage du protocole (respecte la spécification du protocole)   + Déchiffrement du trafic encapsulé * Identification et contrôle des applications partageant la même connexion * Contrôle de la fonction de transfert de fichiers d’une application * Visibilité du trafic applicatif inconnu à travers l’identification de sa nature :   + Volume du trafic   + Utilisateur et/ou adresses IP   + Port utilisé   + Contenu associé : fichier, menace ou autre. * La base de données de contrôle des applications doit contenir plus de **3 000** applications connues ;   La solution doit pouvoir créer une règle de filtrage avec plusieurs catégories ; |  |  |
|  | **Identification, authentification des utilisateurs et protection des identités**   * Prise en charge des services d'authentification suivants pour l'identification et authentifications des utilisateurs :   + Active Directory   + Kerberos   + LDAP   + Radius   + Base Locale   + SAML   + Authentification via SSO Kerberos sans agent   + Authentification par Certificat client   + Portail captif * Identification des utilisateurs indépendamment :   + Du terminal (ordinateur, un téléphone intelligent ou une tablette)   + Du système d’exploitation utilisé,   + Des adresses IP et de la zone (LAN, VPN, hors du périmètre du réseau) |  |  |
|  | **Fonctions Réseau :**   * Support mode Routage, mode transparent, TAP ou SPAN, * Support IPv4 et IPv6 * Routage IPv4 : Statique et Dynamique, RIPv2, OSPFv3 et BGP au minimum * Agrégation des liens 802.3ad, LACP * Support des VLAN 802.1q * Support des modes de translations NAT et PAT * Nat dynamique, Nat Statique, Nat par port, Nat64 * Support de Multicast * 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)** |  |  |
|  | **Fonction VPN :**   * VPN IPSec site-site, client-site et hub & Spoke. **(Fonctionnalité et licence à fournir)** * Support du VPN SSL mode portail et mode tunnel (avec ou sans agent) * Support du Tunnel GRE * Support de IKEv1 et IKEv2 avec authentification à base de clé pré-partagée (PSK) ou certificat * Standard de Chiffrement : 3DES, AES 256 au minimum * Algorithme de contrôle d’intégrité : MD5, SHA-256, SHA-384, SHA-512, |  |  |
|  | **Gestion de la bande passante :**   * Réservation et Priorisation des flux en fonction de la source, la destination, l’utilisateur et l’application,   Limitation de la bande passante par source, destination, application ou catégorie d’application. |  |  |
|  | **Administration et gestion des journaux :**   * Administration via une interface web intuitive et sécurisée en HTTPS, * Administration en ligne de commande SSH et Telnet, * Interface d’administration graphique multi-langues : Français et Anglais au minimum, * Support de l’administration par rôle, * Permettre l’export et l’importation de la configuration, * Suivie et visibilité en temps réel sur les flux transitant par le firewall avec possibilité de filtrage, * Outil de filtrage et recherche multicritère dans les journaux pour faciliter l’identification des incidents de sécurité. * Prise en charge de balises (tags) pour l’organisation des règles et des objets. * Différente vue pour les journaux : Flux, Menaces, Filtrage de contenu, Authentification, Systèmes * Vue synthétique des applications, menaces et URL, * Export des journaux vers des systèmes externes en Syslog et Intégration avec des solutions SIEM * Support de SNMPv3 * Journalisation locale dans le disque du NGFW sans dégradation des performances. * La solution doit inclure une autorité de certification x.509 interne qui peut générer des certificats pour les passerelles et les utilisateurs pour permettre une authentification facile sur les VPN, * La solution doit inclure la possibilité d'utiliser des autorités de certification externes, * La visionneuse de journaux doit avoir la possibilité de créer un filtre en utilisant les noms d'objets prédéfinis (hôtes, réseau, groupes, utilisateurs...), |  |  |
|  | **Filtrage URL** **et Filtrage de contenu**   * Filtrage HTTP, HTTPS, HTTP2 ; * Filtrage URL à base de catégories ; * Inspection des flux chiffrés TLS 1.3 ; * Validation des certificats des serveurs (CRL, Algorithm, Cipher…) ; * Filtrage URL à base de l’adresse IP ; * Filtrage des liens de phishing dans les e-mails, des sites de phishing ; * Filtrage des commandes et contrôles basés sur HTTP et les pages contenant des kits d’exploits ; * Filtrage des données en fonction du type de fichier, propriété de fichier, Metadata, mot clés… * Mise à jour de la base des URL. |  |  |
| **1.2** | **PRESTATION DE SERVICE**  Le prestataire doit proposer dans son offre toutes les prestations nécessaires à la mise en œuvre de la solution de sécurité :   * Ingénierie et définition de l’architecture finale ; * Analyse du plan d’adressage IP, de routage et de découpage VLAN ; * Intégration de la solution dans le réseau de la CMC ; * L’interconnexion du NGFW avec les Switch Datacenter ; * L’installation et la configuration des fonctions du pare feu nouvelle génération selon les bonnes pratiques et les standards de la sécurité ; * La définition de la matrice des flux ; * Le prestataire doit réaliser tout essai jugé nécessaire pour s’assurer de la conformité et du bon fonctionnement de la plateforme de sécurité ; * Transfert de compétence ; * Garantie et maintenance (couvre l’assistance (sur site ou à distance), l’intervention sur site, les pièces de rechanges et la main d’œuvre) pour une durée 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 ; * Livrables :   + Document d’architecture finale et de configuration de la solution (avec schéma au format exploitable et un fichier de configuration) ;   Manuel d’exploitation ; |  |  |

**BORDEREAU DES PRIX – DETAIL ESTIMATIF**

**LOT 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/HTVA** | **(3)**  **Prix total HT/HDD/HTVA**  **(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**

**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** |
| --- | --- | --- | --- |
| **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** |  |  |
|  | **Fonctions Firewall**   * Doit intégrer un système d’exploitation propriétaire sécurisé, * Filtrage de paquets et être doté de la fonction de filtrage dynamique, * Filtrage basé sur les applications niveau 7 en plus des ports/Protocol et par plages de ports UDP ou TCP * Filtrage et inspection en IPv4 et IPv6, * Failover de connexion Internet, * Prise en compte de paramètre Horaire dans les règles de filtrage, * Doit fournir, via sa console d’administration, des statistiques sur le nombre d'accès aux règles de sécurité, * Doit inclure la possibilité de fonctionner en mode transparent ou routé (natté), * Doit fournir la possibilité de définir des instances firewall virtuels sur la même Appliance, et capable d’activer les fonctionnalités de protection IPS, Sandboxing, Control Applicatif, filtrage d’URL, Anti-bot, Anti-virus/Antimalware, * La création de la politique de sécurité basée sur :   + Geolocation par pays   + Zones   + Groupes de Zones   + Applications, Groupes d’applications   + Catégories d’Applications   + Technologies d’Applications   + Filtres d’Applications   + Utilisateurs et Groupes   + Adresses IP, Groupes d’adresses IP, Sous-réseaux IP, Groupes de sous-réseaux IP   + Services, Groupes de Services * La solution doit être de type Next Generation Firewall avec capacité de prévention contre les menaces avancées, combinée avec des fonctionnalités de base suivantes (**licences incluses)** : * **IPS (prévention des intrusions)** pour se protéger contre les menaces réseau telles que vers, chevaux de Troie et autres programmes malveillants. Le système de prévention des intrusions (IPS) doit aussi apporter une protection contre les menaces réseaux existantes et émergentes. Ce module IPS doit avoir deux mécanismes : * Détection par signatures ; * Détection par anomalies ; * Capable de faire des analyses comportementales de tout type de trafic ; * Possibilité de créer des signatures personnalisées ; * Mise à jour automatique des signatures IPS ; * Création et affectation des politiques IPS par type de zone ou interface ; * Pour chaque événement d’attaque, il sera possible de laisser passer ou bloquer, de faire une mise en quarantaine automatique (IP totalement bloquée pendant un temps donné) … ; * Gestion de profils IPS avec association à certains trafics dans la politique de filtrage (IP source, IP destination, service, protocole, réseau…) ; * **Filtrage URL**,pour assurer le contrôle de l’accès interne aux contenus Web indésirables, non productifs, voire illégaux, * **Control Applicatif,** afin d’identifier, reconnaître et contrôler les applications dans les flux, | **Marque :**  **Référence :**  **Caractéristiques proposées** |  |
|  | **Spécifications matérielles et performance :**   * Format : Appliance Rackable, 19’’ * 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 * Nombre de sessions inspectées simultanées : **1 Million** Minimum * Nombre de nouvelles sessions par seconde : **50 000** Minimum * Stockage Disque dur dédiée de type SSD de **200** GB Minimum * Les ports (en dehors des ports de management et de la haute disponibilité)   + Minimum 8 ports 10/100/1000 BaseT   + Minimum 4 ports 1G/10G SFP/SFP+ dont **4** avec **Transceiver SFP+** * Les ports de management et Clustering :   + Minimum 1 port 10/100/1000 BaseT pour le management   + Minimum 1 port console RJ-45   + Minimum 1 port USB   + Minimum 1 ports 10/100/1000 BaseT pour le HA   2 Alimentations électriques Redondantes Minimum (AC), |  |  |
|  | **Support de la haute disponibilité** :   * Actif/Actif avec synchronisation d’état de session, * Actif/Passif, |  |  |
|  | **Contrôle applicatif :**   * Identification des applications en se basant sur :   + Signatures   + Décodage du protocole (respecte la spécification du protocole)   + Déchiffrement du trafic encapsulé * Identification et contrôle des applications partageant la même connexion * Contrôle de la fonction de transfert de fichiers d’une application * Visibilité du trafic applicatif inconnu à travers l’identification de sa nature :   + Volume du trafic   + Utilisateur et/ou adresses IP   + Port utilisé   + Contenu associé : fichier, menace ou autre. * La base de données de contrôle des applications doit contenir plus de **3 000** applications connues ;   La solution doit pouvoir créer une règle de filtrage avec plusieurs catégories ; |  |  |
|  | **Identification, authentification des utilisateurs et protection des identités**   * Prise en charge des services d'authentification suivants pour l'identification et authentifications des utilisateurs :   + Active Directory   + Kerberos   + LDAP   + Radius   + Base Locale   + SAML   + Authentification via SSO Kerberos sans agent   + Authentification par Certificat client   + Portail captif * Identification des utilisateurs indépendamment :   + Du terminal (ordinateur, un téléphone intelligent ou une tablette)   + Du système d’exploitation utilisé,   + Des adresses IP et de la zone (LAN, VPN, hors du périmètre du réseau) |  |  |
|  | **Fonctions Réseau :**   * Support mode Routage, mode transparent, TAP ou SPAN, * Support IPv4 et IPv6 * Routage IPv4 : Statique et Dynamique, RIPv2, OSPFv3 et BGP au minimum * Agrégation des liens 802.3ad, LACP * Support des VLAN 802.1q * Support des modes de translations NAT et PAT * Nat dynamique, Nat Statique, Nat par port, Nat64 * Support de Multicast * 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)** |  |  |
|  | **Fonction VPN :**   * VPN IPSec site-site, client-site et hub & Spoke. **(Fonctionnalité et licence à fournir)** * Support du VPN SSL mode portail et mode tunnel (avec ou sans agent) * Support du Tunnel GRE * Support de IKEv1 et IKEv2 avec authentification à base de clé pré-partagée (PSK) ou certificat * Standard de Chiffrement : 3DES, AES 256 au minimum * Algorithme de contrôle d’intégrité : MD5, SHA-256, SHA-384, SHA-512, |  |  |
|  | **Gestion de la bande passante :**   * Réservation et Priorisation des flux en fonction de la source, la destination, l’utilisateur et l’application,   Limitation de la bande passante par source, destination, application ou catégorie d’application. |  |  |
|  | **Administration et gestion des journaux :**   * Administration via une interface web intuitive et sécurisée en HTTPS, * Administration en ligne de commande SSH et Telnet, * Interface d’administration graphique multi-langues : Français et Anglais au minimum, * Support de l’administration par rôle, * Permettre l’export et l’importation de la configuration, * Suivie et visibilité en temps réel sur les flux transitant par le firewall avec possibilité de filtrage, * Outil de filtrage et recherche multicritère dans les journaux pour faciliter l’identification des incidents de sécurité. * Prise en charge de balises (tags) pour l’organisation des règles et des objets. * Différente vue pour les journaux : Flux, Menaces, Filtrage de contenu, Authentification, Systèmes * Vue synthétique des applications, menaces et URL, * Export des journaux vers des systèmes externes en Syslog et Intégration avec des solutions SIEM * Support de SNMPv3 * Journalisation locale dans le disque du NGFW sans dégradation des performances. * La solution doit inclure une autorité de certification x.509 interne qui peut générer des certificats pour les passerelles et les utilisateurs pour permettre une authentification facile sur les VPN, * La solution doit inclure la possibilité d'utiliser des autorités de certification externes, * La visionneuse de journaux doit avoir la possibilité de créer un filtre en utilisant les noms d'objets prédéfinis (hôtes, réseau, groupes, utilisateurs...), |  |  |
|  | **Filtrage URL** **et Filtrage de contenu**   * Filtrage HTTP, HTTPS, HTTP2 ; * Filtrage URL à base de catégories ; * Inspection des flux chiffrés TLS 1.3 ; * Validation des certificats des serveurs (CRL, Algorithm, Cipher…) ; * Filtrage URL à base de l’adresse IP ; * Filtrage des liens de phishing dans les e-mails, des sites de phishing ; * Filtrage des commandes et contrôles basés sur HTTP et les pages contenant des kits d’exploits ; * Filtrage des données en fonction du type de fichier, propriété de fichier, Metadata, mot clés… * Mise à jour de la base des URL. |  |  |
| **1.2** | **PRESTATION DE SERVICE**  Le prestataire doit proposer dans son offre toutes les prestations nécessaires à la mise en œuvre de la solution de sécurité :   * Ingénierie et définition de l’architecture finale ; * Analyse du plan d’adressage IP, de routage et de découpage VLAN ; * Intégration de la solution dans le réseau de la CMC ; * L’interconnexion du NGFW avec les Switch Datacenter ; * L’installation et la configuration des fonctions du pare feu nouvelle génération selon les bonnes pratiques et les standards de la sécurité ; * La définition de la matrice des flux ; * Le prestataire doit réaliser tout essai jugé nécessaire pour s’assurer de la conformité et du bon fonctionnement de la plateforme de sécurité ; * Transfert de compétence ; * Garantie et maintenance (couvre l’assistance (sur site ou à distance), l’intervention sur site, les pièces de rechanges et la main d’œuvre) pour une durée 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 ; * Livrables :   + Document d’architecture finale et de configuration de la solution (avec schéma au format exploitable et un fichier de configuration) ;   Manuel d’exploitation ; |  |  |

**BORDEREAU DES PRIX – DETAIL ESTIMATIF**

**LOT 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/HTVA** | **(3)**  **Prix total HT/HDD/HTVA**  **(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**

**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 .** | **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** |  |  |
|  | **Fonctions Firewall**   * Doit intégrer un système d’exploitation propriétaire sécurisé, * Filtrage de paquets et être doté de la fonction de filtrage dynamique, * Filtrage basé sur les applications niveau 7 en plus des ports/Protocol et par plages de ports UDP ou TCP * Filtrage et inspection en IPv4 et IPv6, * Failover de connexion Internet, * Prise en compte de paramètre Horaire dans les règles de filtrage, * Doit fournir, via sa console d’administration, des statistiques sur le nombre d'accès aux règles de sécurité, * Doit inclure la possibilité de fonctionner en mode transparent ou routé (natté), * Doit fournir la possibilité de définir des instances firewall virtuels sur la même Appliance, et capable d’activer les fonctionnalités de protection IPS, Sandboxing, Control Applicatif, filtrage d’URL, Anti-bot, Anti-virus/Antimalware, * La création de la politique de sécurité basée sur :   + Geolocation par pays   + Zones   + Groupes de Zones   + Applications, Groupes d’applications   + Catégories d’Applications   + Technologies d’Applications   + Filtres d’Applications   + Utilisateurs et Groupes   + Adresses IP, Groupes d’adresses IP, Sous-réseaux IP, Groupes de sous-réseaux IP   + Services, Groupes de Services * La solution doit être de type Next Generation Firewall avec capacité de prévention contre les menaces avancées, combinée avec des fonctionnalités de base suivantes (**licences incluses)** : * **IPS (prévention des intrusions)** pour se protéger contre les menaces réseau telles que vers, chevaux de Troie et autres programmes malveillants. Le système de prévention des intrusions (IPS) doit aussi apporter une protection contre les menaces réseaux existantes et émergentes. Ce module IPS doit avoir deux mécanismes : * Détection par signatures ; * Détection par anomalies ; * Capable de faire des analyses comportementales de tout type de trafic ; * Possibilité de créer des signatures personnalisées ; * Mise à jour automatique des signatures IPS ; * Création et affectation des politiques IPS par type de zone ou interface ; * Pour chaque événement d’attaque, il sera possible de laisser passer ou bloquer, de faire une mise en quarantaine automatique (IP totalement bloquée pendant un temps donné) … ; * Gestion de profils IPS avec association à certains trafics dans la politique de filtrage (IP source, IP destination, service, protocole, réseau…) ; * **Filtrage URL**,pour assurer le contrôle de l’accès interne aux contenus Web indésirables, non productifs, voire illégaux, * **Control Applicatif,** afin d’identifier, reconnaître et contrôler les applications dans les flux, | **Marque :**  **Référence :**  **Caractéristiques proposées** |  |
|  | **Spécifications matérielles et performance :**   * Format : Appliance Rackable, 19’’ * 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 * Nombre de sessions inspectées simultanées : **1 Million** Minimum * Nombre de nouvelles sessions par seconde : **50 000** Minimum * Stockage Disque dur dédiée de type SSD de **200** GB Minimum * Les ports (en dehors des ports de management et de la haute disponibilité)   + Minimum 8 ports 10/100/1000 BaseT   + Minimum 4 ports 1G/10G SFP/SFP+ dont **4** avec **Transceiver SFP+** * Les ports de management et Clustering :   + Minimum 1 port 10/100/1000 BaseT pour le management   + Minimum 1 port console RJ-45   + Minimum 1 port USB   + Minimum 1 ports 10/100/1000 BaseT pour le HA   2 Alimentations électriques Redondantes Minimum (AC), |  |  |
|  | **Support de la haute disponibilité** :   * Actif/Actif avec synchronisation d’état de session, * Actif/Passif, |  |  |
|  | **Contrôle applicatif :**   * Identification des applications en se basant sur :   + Signatures   + Décodage du protocole (respecte la spécification du protocole)   + Déchiffrement du trafic encapsulé * Identification et contrôle des applications partageant la même connexion * Contrôle de la fonction de transfert de fichiers d’une application * Visibilité du trafic applicatif inconnu à travers l’identification de sa nature :   + Volume du trafic   + Utilisateur et/ou adresses IP   + Port utilisé   + Contenu associé : fichier, menace ou autre. * La base de données de contrôle des applications doit contenir plus de **3 000** applications connues ;   La solution doit pouvoir créer une règle de filtrage avec plusieurs catégories ; |  |  |
|  | **Identification, authentification des utilisateurs et protection des identités**   * Prise en charge des services d'authentification suivants pour l'identification et authentifications des utilisateurs :   + Active Directory   + Kerberos   + LDAP   + Radius   + Base Locale   + SAML   + Authentification via SSO Kerberos sans agent   + Authentification par Certificat client   + Portail captif * Identification des utilisateurs indépendamment :   + Du terminal (ordinateur, un téléphone intelligent ou une tablette)   + Du système d’exploitation utilisé,   + Des adresses IP et de la zone (LAN, VPN, hors du périmètre du réseau) |  |  |
|  | **Fonctions Réseau :**   * Support mode Routage, mode transparent, TAP ou SPAN, * Support IPv4 et IPv6 * Routage IPv4 : Statique et Dynamique, RIPv2, OSPFv3 et BGP au minimum * Agrégation des liens 802.3ad, LACP * Support des VLAN 802.1q * Support des modes de translations NAT et PAT * Nat dynamique, Nat Statique, Nat par port, Nat64 * Support de Multicast * 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)** |  |  |
|  | **Fonction VPN :**   * VPN IPSec site-site, client-site et hub & Spoke. **(Fonctionnalité et licence à fournir)** * Support du VPN SSL mode portail et mode tunnel (avec ou sans agent) * Support du Tunnel GRE * Support de IKEv1 et IKEv2 avec authentification à base de clé pré-partagée (PSK) ou certificat * Standard de Chiffrement : 3DES, AES 256 au minimum * Algorithme de contrôle d’intégrité : MD5, SHA-256, SHA-384, SHA-512, |  |  |
|  | **Gestion de la bande passante :**   * Réservation et Priorisation des flux en fonction de la source, la destination, l’utilisateur et l’application,   Limitation de la bande passante par source, destination, application ou catégorie d’application. |  |  |
|  | **Administration et gestion des journaux :**   * Administration via une interface web intuitive et sécurisée en HTTPS, * Administration en ligne de commande SSH et Telnet, * Interface d’administration graphique multi-langues : Français et Anglais au minimum, * Support de l’administration par rôle, * Permettre l’export et l’importation de la configuration, * Suivie et visibilité en temps réel sur les flux transitant par le firewall avec possibilité de filtrage, * Outil de filtrage et recherche multicritère dans les journaux pour faciliter l’identification des incidents de sécurité. * Prise en charge de balises (tags) pour l’organisation des règles et des objets. * Différente vue pour les journaux : Flux, Menaces, Filtrage de contenu, Authentification, Systèmes * Vue synthétique des applications, menaces et URL, * Export des journaux vers des systèmes externes en Syslog et Intégration avec des solutions SIEM * Support de SNMPv3 * Journalisation locale dans le disque du NGFW sans dégradation des performances. * La solution doit inclure une autorité de certification x.509 interne qui peut générer des certificats pour les passerelles et les utilisateurs pour permettre une authentification facile sur les VPN, * La solution doit inclure la possibilité d'utiliser des autorités de certification externes, * La visionneuse de journaux doit avoir la possibilité de créer un filtre en utilisant les noms d'objets prédéfinis (hôtes, réseau, groupes, utilisateurs...), |  |  |
|  | **Filtrage URL** **et Filtrage de contenu**   * Filtrage HTTP, HTTPS, HTTP2 ; * Filtrage URL à base de catégories ; * Inspection des flux chiffrés TLS 1.3 ; * Validation des certificats des serveurs (CRL, Algorithm, Cipher…) ; * Filtrage URL à base de l’adresse IP ; * Filtrage des liens de phishing dans les e-mails, des sites de phishing ; * Filtrage des commandes et contrôles basés sur HTTP et les pages contenant des kits d’exploits ; * Filtrage des données en fonction du type de fichier, propriété de fichier, Metadata, mot clés… * Mise à jour de la base des URL. |  |  |
| **1.2** | **PRESTATION DE SERVICE**  Le prestataire doit proposer dans son offre toutes les prestations nécessaires à la mise en œuvre de la solution de sécurité :   * Ingénierie et définition de l’architecture finale ; * Analyse du plan d’adressage IP, de routage et de découpage VLAN ; * Intégration de la solution dans le réseau de la CMC ; * L’interconnexion du NGFW avec les Switch Datacenter ; * L’installation et la configuration des fonctions du pare feu nouvelle génération selon les bonnes pratiques et les standards de la sécurité ; * La définition de la matrice des flux ; * Le prestataire doit réaliser tout essai jugé nécessaire pour s’assurer de la conformité et du bon fonctionnement de la plateforme de sécurité ; * Transfert de compétence ; * Garantie et maintenance (couvre l’assistance (sur site ou à distance), l’intervention sur site, les pièces de rechanges et la main d’œuvre) pour une durée 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 ; * Livrables :   + Document d’architecture finale et de configuration de la solution (avec schéma au format exploitable et un fichier de configuration) ;   Manuel d’exploitation ; |  |  |

**BORDEREAU DES PRIX – DETAIL ESTIMATIF**

**LOT 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/HTVA** | **(3)**  **Prix total HT/HDD/HTVA**  **(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**

**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** |
| --- | --- | --- | --- |
| **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** |  |  |
|  | **Fonctions Firewall**   * Doit intégrer un système d’exploitation propriétaire sécurisé, * Filtrage de paquets et être doté de la fonction de filtrage dynamique, * Filtrage basé sur les applications niveau 7 en plus des ports/Protocol et par plages de ports UDP ou TCP * Filtrage et inspection en IPv4 et IPv6, * Failover de connexion Internet, * Prise en compte de paramètre Horaire dans les règles de filtrage, * Doit fournir, via sa console d’administration, des statistiques sur le nombre d'accès aux règles de sécurité, * Doit inclure la possibilité de fonctionner en mode transparent ou routé (natté), * Doit fournir la possibilité de définir des instances firewall virtuels sur la même Appliance, et capable d’activer les fonctionnalités de protection IPS, Sandboxing, Control Applicatif, filtrage d’URL, Anti-bot, Anti-virus/Antimalware, * La création de la politique de sécurité basée sur :   + Geolocation par pays   + Zones   + Groupes de Zones   + Applications, Groupes d’applications   + Catégories d’Applications   + Technologies d’Applications   + Filtres d’Applications   + Utilisateurs et Groupes   + Adresses IP, Groupes d’adresses IP, Sous-réseaux IP, Groupes de sous-réseaux IP   + Services, Groupes de Services * La solution doit être de type Next Generation Firewall avec capacité de prévention contre les menaces avancées, combinée avec des fonctionnalités de base suivantes (**licences incluses)** : * **IPS (prévention des intrusions)** pour se protéger contre les menaces réseau telles que vers, chevaux de Troie et autres programmes malveillants. Le système de prévention des intrusions (IPS) doit aussi apporter une protection contre les menaces réseaux existantes et émergentes. Ce module IPS doit avoir deux mécanismes : * Détection par signatures ; * Détection par anomalies ; * Capable de faire des analyses comportementales de tout type de trafic ; * Possibilité de créer des signatures personnalisées ; * Mise à jour automatique des signatures IPS ; * Création et affectation des politiques IPS par type de zone ou interface ; * Pour chaque événement d’attaque, il sera possible de laisser passer ou bloquer, de faire une mise en quarantaine automatique (IP totalement bloquée pendant un temps donné) … ; * Gestion de profils IPS avec association à certains trafics dans la politique de filtrage (IP source, IP destination, service, protocole, réseau…) ; * **Filtrage URL**,pour assurer le contrôle de l’accès interne aux contenus Web indésirables, non productifs, voire illégaux, * **Control Applicatif,** afin d’identifier, reconnaître et contrôler les applications dans les flux, | **Marque :**  **Référence :**  **Caractéristiques proposées** |  |
|  | **Spécifications matérielles et performance :**   * Format : Appliance Rackable, 19’’ * 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 * Nombre de sessions inspectées simultanées : **1 Million** Minimum * Nombre de nouvelles sessions par seconde : **50 000** Minimum * Stockage Disque dur dédiée de type SSD de **200** GB Minimum * Les ports (en dehors des ports de management et de la haute disponibilité)   + Minimum 8 ports 10/100/1000 BaseT   + Minimum 4 ports 1G/10G SFP/SFP+ dont **4** avec **Transceiver SFP+** * Les ports de management et Clustering :   + Minimum 1 port 10/100/1000 BaseT pour le management   + Minimum 1 port console RJ-45   + Minimum 1 port USB   + Minimum 1 ports 10/100/1000 BaseT pour le HA   2 Alimentations électriques Redondantes Minimum (AC), |  |  |
|  | **Support de la haute disponibilité** :   * Actif/Actif avec synchronisation d’état de session, * Actif/Passif, |  |  |
|  | **Contrôle applicatif :**   * Identification des applications en se basant sur :   + Signatures   + Décodage du protocole (respecte la spécification du protocole)   + Déchiffrement du trafic encapsulé * Identification et contrôle des applications partageant la même connexion * Contrôle de la fonction de transfert de fichiers d’une application * Visibilité du trafic applicatif inconnu à travers l’identification de sa nature :   + Volume du trafic   + Utilisateur et/ou adresses IP   + Port utilisé   + Contenu associé : fichier, menace ou autre. * La base de données de contrôle des applications doit contenir plus de **3 000** applications connues ;   La solution doit pouvoir créer une règle de filtrage avec plusieurs catégories ; |  |  |
|  | **Identification, authentification des utilisateurs et protection des identités**   * Prise en charge des services d'authentification suivants pour l'identification et authentifications des utilisateurs :   + Active Directory   + Kerberos   + LDAP   + Radius   + Base Locale   + SAML   + Authentification via SSO Kerberos sans agent   + Authentification par Certificat client   + Portail captif * Identification des utilisateurs indépendamment :   + Du terminal (ordinateur, un téléphone intelligent ou une tablette)   + Du système d’exploitation utilisé,   + Des adresses IP et de la zone (LAN, VPN, hors du périmètre du réseau) |  |  |
|  | **Fonctions Réseau :**   * Support mode Routage, mode transparent, TAP ou SPAN, * Support IPv4 et IPv6 * Routage IPv4 : Statique et Dynamique, RIPv2, OSPFv3 et BGP au minimum * Agrégation des liens 802.3ad, LACP * Support des VLAN 802.1q * Support des modes de translations NAT et PAT * Nat dynamique, Nat Statique, Nat par port, Nat64 * Support de Multicast * 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)** |  |  |
|  | **Fonction VPN :**   * VPN IPSec site-site, client-site et hub & Spoke. **(Fonctionnalité et licence à fournir)** * Support du VPN SSL mode portail et mode tunnel (avec ou sans agent) * Support du Tunnel GRE * Support de IKEv1 et IKEv2 avec authentification à base de clé pré-partagée (PSK) ou certificat * Standard de Chiffrement : 3DES, AES 256 au minimum * Algorithme de contrôle d’intégrité : MD5, SHA-256, SHA-384, SHA-512, |  |  |
|  | **Gestion de la bande passante :**   * Réservation et Priorisation des flux en fonction de la source, la destination, l’utilisateur et l’application,   Limitation de la bande passante par source, destination, application ou catégorie d’application. |  |  |
|  | **Administration et gestion des journaux :**   * Administration via une interface web intuitive et sécurisée en HTTPS, * Administration en ligne de commande SSH et Telnet, * Interface d’administration graphique multi-langues : Français et Anglais au minimum, * Support de l’administration par rôle, * Permettre l’export et l’importation de la configuration, * Suivie et visibilité en temps réel sur les flux transitant par le firewall avec possibilité de filtrage, * Outil de filtrage et recherche multicritère dans les journaux pour faciliter l’identification des incidents de sécurité. * Prise en charge de balises (tags) pour l’organisation des règles et des objets. * Différente vue pour les journaux : Flux, Menaces, Filtrage de contenu, Authentification, Systèmes * Vue synthétique des applications, menaces et URL, * Export des journaux vers des systèmes externes en Syslog et Intégration avec des solutions SIEM * Support de SNMPv3 * Journalisation locale dans le disque du NGFW sans dégradation des performances. * La solution doit inclure une autorité de certification x.509 interne qui peut générer des certificats pour les passerelles et les utilisateurs pour permettre une authentification facile sur les VPN, * La solution doit inclure la possibilité d'utiliser des autorités de certification externes, * La visionneuse de journaux doit avoir la possibilité de créer un filtre en utilisant les noms d'objets prédéfinis (hôtes, réseau, groupes, utilisateurs...), |  |  |
|  | **Filtrage URL** **et Filtrage de contenu**   * Filtrage HTTP, HTTPS, HTTP2 ; * Filtrage URL à base de catégories ; * Inspection des flux chiffrés TLS 1.3 ; * Validation des certificats des serveurs (CRL, Algorithm, Cipher…) ; * Filtrage URL à base de l’adresse IP ; * Filtrage des liens de phishing dans les e-mails, des sites de phishing ; * Filtrage des commandes et contrôles basés sur HTTP et les pages contenant des kits d’exploits ; * Filtrage des données en fonction du type de fichier, propriété de fichier, Metadata, mot clés… * Mise à jour de la base des URL. |  |  |
| **1.2** | **PRESTATION DE SERVICE**  Le prestataire doit proposer dans son offre toutes les prestations nécessaires à la mise en œuvre de la solution de sécurité :   * Ingénierie et définition de l’architecture finale ; * Analyse du plan d’adressage IP, de routage et de découpage VLAN ; * Intégration de la solution dans le réseau de la CMC ; * L’interconnexion du NGFW avec les Switch Datacenter ; * L’installation et la configuration des fonctions du pare feu nouvelle génération selon les bonnes pratiques et les standards de la sécurité ; * La définition de la matrice des flux ; * Le prestataire doit réaliser tout essai jugé nécessaire pour s’assurer de la conformité et du bon fonctionnement de la plateforme de sécurité ; * Transfert de compétence ; * Garantie et maintenance (couvre l’assistance (sur site ou à distance), l’intervention sur site, les pièces de rechanges et la main d’œuvre) pour une durée 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 ; * Livrables :   + Document d’architecture finale et de configuration de la solution (avec schéma au format exploitable et un fichier de configuration) ;   Manuel d’exploitation ; |  |  |

**BORDEREAU DES PRIX – DETAIL ESTIMATIF**

**LOT 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/HTVA** | **(3)**  **Prix total HT/HDD/HTVA**  **(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**

**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** |
| --- | --- | --- | --- |
| **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** |  |  |
|  | **Fonctions Firewall**   * Doit intégrer un système d’exploitation propriétaire sécurisé, * Filtrage de paquets et être doté de la fonction de filtrage dynamique, * Filtrage basé sur les applications niveau 7 en plus des ports/Protocol et par plages de ports UDP ou TCP * Filtrage et inspection en IPv4 et IPv6, * Failover de connexion Internet, * Prise en compte de paramètre Horaire dans les règles de filtrage, * Doit fournir, via sa console d’administration, des statistiques sur le nombre d'accès aux règles de sécurité, * Doit inclure la possibilité de fonctionner en mode transparent ou routé (natté), * Doit fournir la possibilité de définir des instances firewall virtuels sur la même Appliance, et capable d’activer les fonctionnalités de protection IPS, Sandboxing, Control Applicatif, filtrage d’URL, Anti-bot, Anti-virus/Antimalware, * La création de la politique de sécurité basée sur :   + Geolocation par pays   + Zones   + Groupes de Zones   + Applications, Groupes d’applications   + Catégories d’Applications   + Technologies d’Applications   + Filtres d’Applications   + Utilisateurs et Groupes   + Adresses IP, Groupes d’adresses IP, Sous-réseaux IP, Groupes de sous-réseaux IP   + Services, Groupes de Services * La solution doit être de type Next Generation Firewall avec capacité de prévention contre les menaces avancées, combinée avec des fonctionnalités de base suivantes (**licences incluses)** : * **IPS (prévention des intrusions)** pour se protéger contre les menaces réseau telles que vers, chevaux de Troie et autres programmes malveillants. Le système de prévention des intrusions (IPS) doit aussi apporter une protection contre les menaces réseaux existantes et émergentes. Ce module IPS doit avoir deux mécanismes : * Détection par signatures ; * Détection par anomalies ; * Capable de faire des analyses comportementales de tout type de trafic ; * Possibilité de créer des signatures personnalisées ; * Mise à jour automatique des signatures IPS ; * Création et affectation des politiques IPS par type de zone ou interface ; * Pour chaque événement d’attaque, il sera possible de laisser passer ou bloquer, de faire une mise en quarantaine automatique (IP totalement bloquée pendant un temps donné) … ; * Gestion de profils IPS avec association à certains trafics dans la politique de filtrage (IP source, IP destination, service, protocole, réseau…) ; * **Filtrage URL**,pour assurer le contrôle de l’accès interne aux contenus Web indésirables, non productifs, voire illégaux, * **Control Applicatif,** afin d’identifier, reconnaître et contrôler les applications dans les flux, | **Marque :**  **Référence :**  **Caractéristiques proposées** |  |
|  | **Spécifications matérielles et performance :**   * Format : Appliance Rackable, 19’’ * 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 * Nombre de sessions inspectées simultanées : **1 Million** Minimum * Nombre de nouvelles sessions par seconde : **50 000** Minimum * Stockage Disque dur dédiée de type SSD de **200** GB Minimum * Les ports (en dehors des ports de management et de la haute disponibilité)   + Minimum 8 ports 10/100/1000 BaseT   + Minimum 4 ports 1G/10G SFP/SFP+ dont **4** avec **Transceiver SFP+** * Les ports de management et Clustering :   + Minimum 1 port 10/100/1000 BaseT pour le management   + Minimum 1 port console RJ-45   + Minimum 1 port USB   + Minimum 1 ports 10/100/1000 BaseT pour le HA   2 Alimentations électriques Redondantes Minimum (AC), |  |  |
|  | **Support de la haute disponibilité** :   * Actif/Actif avec synchronisation d’état de session, * Actif/Passif, |  |  |
|  | **Contrôle applicatif :**   * Identification des applications en se basant sur :   + Signatures   + Décodage du protocole (respecte la spécification du protocole)   + Déchiffrement du trafic encapsulé * Identification et contrôle des applications partageant la même connexion * Contrôle de la fonction de transfert de fichiers d’une application * Visibilité du trafic applicatif inconnu à travers l’identification de sa nature :   + Volume du trafic   + Utilisateur et/ou adresses IP   + Port utilisé   + Contenu associé : fichier, menace ou autre. * La base de données de contrôle des applications doit contenir plus de **3 000** applications connues ;   La solution doit pouvoir créer une règle de filtrage avec plusieurs catégories ; |  |  |
|  | **Identification, authentification des utilisateurs et protection des identités**   * Prise en charge des services d'authentification suivants pour l'identification et authentifications des utilisateurs :   + Active Directory   + Kerberos   + LDAP   + Radius   + Base Locale   + SAML   + Authentification via SSO Kerberos sans agent   + Authentification par Certificat client   + Portail captif * Identification des utilisateurs indépendamment :   + Du terminal (ordinateur, un téléphone intelligent ou une tablette)   + Du système d’exploitation utilisé,   + Des adresses IP et de la zone (LAN, VPN, hors du périmètre du réseau) |  |  |
|  | **Fonctions Réseau :**   * Support mode Routage, mode transparent, TAP ou SPAN, * Support IPv4 et IPv6 * Routage IPv4 : Statique et Dynamique, RIPv2, OSPFv3 et BGP au minimum * Agrégation des liens 802.3ad, LACP * Support des VLAN 802.1q * Support des modes de translations NAT et PAT * Nat dynamique, Nat Statique, Nat par port, Nat64 * Support de Multicast * 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)** |  |  |
|  | **Fonction VPN :**   * VPN IPSec site-site, client-site et hub & Spoke. **(Fonctionnalité et licence à fournir)** * Support du VPN SSL mode portail et mode tunnel (avec ou sans agent) * Support du Tunnel GRE * Support de IKEv1 et IKEv2 avec authentification à base de clé pré-partagée (PSK) ou certificat * Standard de Chiffrement : 3DES, AES 256 au minimum * Algorithme de contrôle d’intégrité : MD5, SHA-256, SHA-384, SHA-512, |  |  |
|  | **Gestion de la bande passante :**   * Réservation et Priorisation des flux en fonction de la source, la destination, l’utilisateur et l’application,   Limitation de la bande passante par source, destination, application ou catégorie d’application. |  |  |
|  | **Administration et gestion des journaux :**   * Administration via une interface web intuitive et sécurisée en HTTPS, * Administration en ligne de commande SSH et Telnet, * Interface d’administration graphique multi-langues : Français et Anglais au minimum, * Support de l’administration par rôle, * Permettre l’export et l’importation de la configuration, * Suivie et visibilité en temps réel sur les flux transitant par le firewall avec possibilité de filtrage, * Outil de filtrage et recherche multicritère dans les journaux pour faciliter l’identification des incidents de sécurité. * Prise en charge de balises (tags) pour l’organisation des règles et des objets. * Différente vue pour les journaux : Flux, Menaces, Filtrage de contenu, Authentification, Systèmes * Vue synthétique des applications, menaces et URL, * Export des journaux vers des systèmes externes en Syslog et Intégration avec des solutions SIEM * Support de SNMPv3 * Journalisation locale dans le disque du NGFW sans dégradation des performances. * La solution doit inclure une autorité de certification x.509 interne qui peut générer des certificats pour les passerelles et les utilisateurs pour permettre une authentification facile sur les VPN, * La solution doit inclure la possibilité d'utiliser des autorités de certification externes, * La visionneuse de journaux doit avoir la possibilité de créer un filtre en utilisant les noms d'objets prédéfinis (hôtes, réseau, groupes, utilisateurs...), |  |  |
|  | **Filtrage URL** **et Filtrage de contenu**   * Filtrage HTTP, HTTPS, HTTP2 ; * Filtrage URL à base de catégories ; * Inspection des flux chiffrés TLS 1.3 ; * Validation des certificats des serveurs (CRL, Algorithm, Cipher…) ; * Filtrage URL à base de l’adresse IP ; * Filtrage des liens de phishing dans les e-mails, des sites de phishing ; * Filtrage des commandes et contrôles basés sur HTTP et les pages contenant des kits d’exploits ; * Filtrage des données en fonction du type de fichier, propriété de fichier, Metadata, mot clés… * Mise à jour de la base des URL. |  |  |
| **1.2** | **PRESTATION DE SERVICE**  Le prestataire doit proposer dans son offre toutes les prestations nécessaires à la mise en œuvre de la solution de sécurité :   * Ingénierie et définition de l’architecture finale ; * Analyse du plan d’adressage IP, de routage et de découpage VLAN ; * Intégration de la solution dans le réseau de la CMC ; * L’interconnexion du NGFW avec les Switch Datacenter ; * L’installation et la configuration des fonctions du pare feu nouvelle génération selon les bonnes pratiques et les standards de la sécurité ; * La définition de la matrice des flux ; * Le prestataire doit réaliser tout essai jugé nécessaire pour s’assurer de la conformité et du bon fonctionnement de la plateforme de sécurité ; * Transfert de compétence ; * Garantie et maintenance (couvre l’assistance (sur site ou à distance), l’intervention sur site, les pièces de rechanges et la main d’œuvre) pour une durée 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 ; * Livrables :   + Document d’architecture finale et de configuration de la solution (avec schéma au format exploitable et un fichier de configuration) ;   Manuel d’exploitation ; |  |  |

**BORDEREAU DES PRIX – DETAIL ESTIMATIF**

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

| **Items N°** | **Désignations** | **Unité** | **(1)**  **QTE** | **(2)**  **Prix unitaire**  **HT/HDD/HTVA** | **(3)**  **Prix total HT/HDD/HTVA**  **(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**

**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** |
| --- | --- | --- | --- |
| **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** |  |  |
|  | **Fonctions Firewall**   * Doit intégrer un système d’exploitation propriétaire sécurisé, * Filtrage de paquets et être doté de la fonction de filtrage dynamique, * Filtrage basé sur les applications niveau 7 en plus des ports/Protocol et par plages de ports UDP ou TCP * Filtrage et inspection en IPv4 et IPv6, * Failover de connexion Internet, * Prise en compte de paramètre Horaire dans les règles de filtrage, * Doit fournir, via sa console d’administration, des statistiques sur le nombre d'accès aux règles de sécurité, * Doit inclure la possibilité de fonctionner en mode transparent ou routé (natté), * Doit fournir la possibilité de définir des instances firewall virtuels sur la même Appliance, et capable d’activer les fonctionnalités de protection IPS, Sandboxing, Control Applicatif, filtrage d’URL, Anti-bot, Anti-virus/Antimalware, * La création de la politique de sécurité basée sur :   + Geolocation par pays   + Zones   + Groupes de Zones   + Applications, Groupes d’applications   + Catégories d’Applications   + Technologies d’Applications   + Filtres d’Applications   + Utilisateurs et Groupes   + Adresses IP, Groupes d’adresses IP, Sous-réseaux IP, Groupes de sous-réseaux IP   + Services, Groupes de Services * La solution doit être de type Next Generation Firewall avec capacité de prévention contre les menaces avancées, combinée avec des fonctionnalités de base suivantes (**licences incluses)** : * **IPS (prévention des intrusions)** pour se protéger contre les menaces réseau telles que vers, chevaux de Troie et autres programmes malveillants. Le système de prévention des intrusions (IPS) doit aussi apporter une protection contre les menaces réseaux existantes et émergentes. Ce module IPS doit avoir deux mécanismes : * Détection par signatures ; * Détection par anomalies ; * Capable de faire des analyses comportementales de tout type de trafic ; * Possibilité de créer des signatures personnalisées ; * Mise à jour automatique des signatures IPS ; * Création et affectation des politiques IPS par type de zone ou interface ; * Pour chaque événement d’attaque, il sera possible de laisser passer ou bloquer, de faire une mise en quarantaine automatique (IP totalement bloquée pendant un temps donné) … ; * Gestion de profils IPS avec association à certains trafics dans la politique de filtrage (IP source, IP destination, service, protocole, réseau…) ; * **Filtrage URL**,pour assurer le contrôle de l’accès interne aux contenus Web indésirables, non productifs, voire illégaux, * **Control Applicatif,** afin d’identifier, reconnaître et contrôler les applications dans les flux, | **Marque :**  **Référence :**  **Caractéristiques proposées** |  |
|  | **Spécifications matérielles et performance :**   * Format : Appliance Rackable, 19’’ * 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 * Nombre de sessions inspectées simultanées : **1 Million** Minimum * Nombre de nouvelles sessions par seconde : **50 000** Minimum * Stockage Disque dur dédiée de type SSD de **200** GB Minimum * Les ports (en dehors des ports de management et de la haute disponibilité)   + Minimum 8 ports 10/100/1000 BaseT   + Minimum 4 ports 1G/10G SFP/SFP+ dont **4** avec **Transceiver SFP+** * Les ports de management et Clustering :   + Minimum 1 port 10/100/1000 BaseT pour le management   + Minimum 1 port console RJ-45   + Minimum 1 port USB   + Minimum 1 ports 10/100/1000 BaseT pour le HA   2 Alimentations électriques Redondantes Minimum (AC), |  |  |
|  | **Support de la haute disponibilité** :   * Actif/Actif avec synchronisation d’état de session, * Actif/Passif, |  |  |
|  | **Contrôle applicatif :**   * Identification des applications en se basant sur :   + Signatures   + Décodage du protocole (respecte la spécification du protocole)   + Déchiffrement du trafic encapsulé * Identification et contrôle des applications partageant la même connexion * Contrôle de la fonction de transfert de fichiers d’une application * Visibilité du trafic applicatif inconnu à travers l’identification de sa nature :   + Volume du trafic   + Utilisateur et/ou adresses IP   + Port utilisé   + Contenu associé : fichier, menace ou autre. * La base de données de contrôle des applications doit contenir plus de **3 000** applications connues ;   La solution doit pouvoir créer une règle de filtrage avec plusieurs catégories ; |  |  |
|  | **Identification, authentification des utilisateurs et protection des identités**   * Prise en charge des services d'authentification suivants pour l'identification et authentifications des utilisateurs :   + Active Directory   + Kerberos   + LDAP   + Radius   + Base Locale   + SAML   + Authentification via SSO Kerberos sans agent   + Authentification par Certificat client   + Portail captif * Identification des utilisateurs indépendamment :   + Du terminal (ordinateur, un téléphone intelligent ou une tablette)   + Du système d’exploitation utilisé,   + Des adresses IP et de la zone (LAN, VPN, hors du périmètre du réseau) |  |  |
|  | **Fonctions Réseau :**   * Support mode Routage, mode transparent, TAP ou SPAN, * Support IPv4 et IPv6 * Routage IPv4 : Statique et Dynamique, RIPv2, OSPFv3 et BGP au minimum * Agrégation des liens 802.3ad, LACP * Support des VLAN 802.1q * Support des modes de translations NAT et PAT * Nat dynamique, Nat Statique, Nat par port, Nat64 * Support de Multicast * 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)** |  |  |
|  | **Fonction VPN :**   * VPN IPSec site-site, client-site et hub & Spoke. **(Fonctionnalité et licence à fournir)** * Support du VPN SSL mode portail et mode tunnel (avec ou sans agent) * Support du Tunnel GRE * Support de IKEv1 et IKEv2 avec authentification à base de clé pré-partagée (PSK) ou certificat * Standard de Chiffrement : 3DES, AES 256 au minimum * Algorithme de contrôle d’intégrité : MD5, SHA-256, SHA-384, SHA-512, |  |  |
|  | **Gestion de la bande passante :**   * Réservation et Priorisation des flux en fonction de la source, la destination, l’utilisateur et l’application,   Limitation de la bande passante par source, destination, application ou catégorie d’application. |  |  |
|  | **Administration et gestion des journaux :**   * Administration via une interface web intuitive et sécurisée en HTTPS, * Administration en ligne de commande SSH et Telnet, * Interface d’administration graphique multi-langues : Français et Anglais au minimum, * Support de l’administration par rôle, * Permettre l’export et l’importation de la configuration, * Suivie et visibilité en temps réel sur les flux transitant par le firewall avec possibilité de filtrage, * Outil de filtrage et recherche multicritère dans les journaux pour faciliter l’identification des incidents de sécurité. * Prise en charge de balises (tags) pour l’organisation des règles et des objets. * Différente vue pour les journaux : Flux, Menaces, Filtrage de contenu, Authentification, Systèmes * Vue synthétique des applications, menaces et URL, * Export des journaux vers des systèmes externes en Syslog et Intégration avec des solutions SIEM * Support de SNMPv3 * Journalisation locale dans le disque du NGFW sans dégradation des performances. * La solution doit inclure une autorité de certification x.509 interne qui peut générer des certificats pour les passerelles et les utilisateurs pour permettre une authentification facile sur les VPN, * La solution doit inclure la possibilité d'utiliser des autorités de certification externes, * La visionneuse de journaux doit avoir la possibilité de créer un filtre en utilisant les noms d'objets prédéfinis (hôtes, réseau, groupes, utilisateurs...), |  |  |
|  | **Filtrage URL** **et Filtrage de contenu**   * Filtrage HTTP, HTTPS, HTTP2 ; * Filtrage URL à base de catégories ; * Inspection des flux chiffrés TLS 1.3 ; * Validation des certificats des serveurs (CRL, Algorithm, Cipher…) ; * Filtrage URL à base de l’adresse IP ; * Filtrage des liens de phishing dans les e-mails, des sites de phishing ; * Filtrage des commandes et contrôles basés sur HTTP et les pages contenant des kits d’exploits ; * Filtrage des données en fonction du type de fichier, propriété de fichier, Metadata, mot clés… * Mise à jour de la base des URL. |  |  |
| **1.2** | **PRESTATION DE SERVICE**  Le prestataire doit proposer dans son offre toutes les prestations nécessaires à la mise en œuvre de la solution de sécurité :   * Ingénierie et définition de l’architecture finale ; * Analyse du plan d’adressage IP, de routage et de découpage VLAN ; * Intégration de la solution dans le réseau de la CMC ; * L’interconnexion du NGFW avec les Switch Datacenter ; * L’installation et la configuration des fonctions du pare feu nouvelle génération selon les bonnes pratiques et les standards de la sécurité ; * La définition de la matrice des flux ; * Le prestataire doit réaliser tout essai jugé nécessaire pour s’assurer de la conformité et du bon fonctionnement de la plateforme de sécurité ; * Transfert de compétence ; * Garantie et maintenance (couvre l’assistance (sur site ou à distance), l’intervention sur site, les pièces de rechanges et la main d’œuvre) pour une durée 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 ; * Livrables :   + Document d’architecture finale et de configuration de la solution (avec schéma au format exploitable et un fichier de configuration) ;   Manuel d’exploitation ; |  |  |

**BORDEREAU DES PRIX – DETAIL ESTIMATIF**

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

| **Items N°** | **Désignations** | **Unité** | **(1)**  **QTE** | **(2)**  **Prix unitaire**  **HT/HDD/HTVA** | **(3)**  **Prix total HT/HDD/HTVA**  **(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**

**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** |
| --- | --- | --- | --- |
| **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** |  |  |
|  | **Fonctions Firewall**   * Doit intégrer un système d’exploitation propriétaire sécurisé, * Filtrage de paquets et être doté de la fonction de filtrage dynamique, * Filtrage basé sur les applications niveau 7 en plus des ports/Protocol et par plages de ports UDP ou TCP * Filtrage et inspection en IPv4 et IPv6, * Failover de connexion Internet, * Prise en compte de paramètre Horaire dans les règles de filtrage, * Doit fournir, via sa console d’administration, des statistiques sur le nombre d'accès aux règles de sécurité, * Doit inclure la possibilité de fonctionner en mode transparent ou routé (natté), * Doit fournir la possibilité de définir des instances firewall virtuels sur la même Appliance, et capable d’activer les fonctionnalités de protection IPS, Sandboxing, Control Applicatif, filtrage d’URL, Anti-bot, Anti-virus/Antimalware, * La création de la politique de sécurité basée sur :   + Geolocation par pays   + Zones   + Groupes de Zones   + Applications, Groupes d’applications   + Catégories d’Applications   + Technologies d’Applications   + Filtres d’Applications   + Utilisateurs et Groupes   + Adresses IP, Groupes d’adresses IP, Sous-réseaux IP, Groupes de sous-réseaux IP   + Services, Groupes de Services * La solution doit être de type Next Generation Firewall avec capacité de prévention contre les menaces avancées, combinée avec des fonctionnalités de base suivantes (**licences incluses)** : * **IPS (prévention des intrusions)** pour se protéger contre les menaces réseau telles que vers, chevaux de Troie et autres programmes malveillants. Le système de prévention des intrusions (IPS) doit aussi apporter une protection contre les menaces réseaux existantes et émergentes. Ce module IPS doit avoir deux mécanismes : * Détection par signatures ; * Détection par anomalies ; * Capable de faire des analyses comportementales de tout type de trafic ; * Possibilité de créer des signatures personnalisées ; * Mise à jour automatique des signatures IPS ; * Création et affectation des politiques IPS par type de zone ou interface ; * Pour chaque événement d’attaque, il sera possible de laisser passer ou bloquer, de faire une mise en quarantaine automatique (IP totalement bloquée pendant un temps donné) … ; * Gestion de profils IPS avec association à certains trafics dans la politique de filtrage (IP source, IP destination, service, protocole, réseau…) ; * **Filtrage URL**,pour assurer le contrôle de l’accès interne aux contenus Web indésirables, non productifs, voire illégaux, * **Control Applicatif,** afin d’identifier, reconnaître et contrôler les applications dans les flux, | **Marque :**  **Référence :**  **Caractéristiques proposées** |  |
|  | **Spécifications matérielles et performance :**   * Format : Appliance Rackable, 19’’ * 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 * Nombre de sessions inspectées simultanées : **1 Million** Minimum * Nombre de nouvelles sessions par seconde : **50 000** Minimum * Stockage Disque dur dédiée de type SSD de **200** GB Minimum * Les ports (en dehors des ports de management et de la haute disponibilité)   + Minimum 8 ports 10/100/1000 BaseT   + Minimum 4 ports 1G/10G SFP/SFP+ dont **4** avec **Transceiver SFP+** * Les ports de management et Clustering :   + Minimum 1 port 10/100/1000 BaseT pour le management   + Minimum 1 port console RJ-45   + Minimum 1 port USB   + Minimum 1 ports 10/100/1000 BaseT pour le HA   2 Alimentations électriques Redondantes Minimum (AC), |  |  |
|  | **Support de la haute disponibilité** :   * Actif/Actif avec synchronisation d’état de session, * Actif/Passif, |  |  |
|  | **Contrôle applicatif :**   * Identification des applications en se basant sur :   + Signatures   + Décodage du protocole (respecte la spécification du protocole)   + Déchiffrement du trafic encapsulé * Identification et contrôle des applications partageant la même connexion * Contrôle de la fonction de transfert de fichiers d’une application * Visibilité du trafic applicatif inconnu à travers l’identification de sa nature :   + Volume du trafic   + Utilisateur et/ou adresses IP   + Port utilisé   + Contenu associé : fichier, menace ou autre. * La base de données de contrôle des applications doit contenir plus de **3 000** applications connues ;   La solution doit pouvoir créer une règle de filtrage avec plusieurs catégories ; |  |  |
|  | **Identification, authentification des utilisateurs et protection des identités**   * Prise en charge des services d'authentification suivants pour l'identification et authentifications des utilisateurs :   + Active Directory   + Kerberos   + LDAP   + Radius   + Base Locale   + SAML   + Authentification via SSO Kerberos sans agent   + Authentification par Certificat client   + Portail captif * Identification des utilisateurs indépendamment :   + Du terminal (ordinateur, un téléphone intelligent ou une tablette)   + Du système d’exploitation utilisé,   + Des adresses IP et de la zone (LAN, VPN, hors du périmètre du réseau) |  |  |
|  | **Fonctions Réseau :**   * Support mode Routage, mode transparent, TAP ou SPAN, * Support IPv4 et IPv6 * Routage IPv4 : Statique et Dynamique, RIPv2, OSPFv3 et BGP au minimum * Agrégation des liens 802.3ad, LACP * Support des VLAN 802.1q * Support des modes de translations NAT et PAT * Nat dynamique, Nat Statique, Nat par port, Nat64 * Support de Multicast * 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)** |  |  |
|  | **Fonction VPN :**   * VPN IPSec site-site, client-site et hub & Spoke. **(Fonctionnalité et licence à fournir)** * Support du VPN SSL mode portail et mode tunnel (avec ou sans agent) * Support du Tunnel GRE * Support de IKEv1 et IKEv2 avec authentification à base de clé pré-partagée (PSK) ou certificat * Standard de Chiffrement : 3DES, AES 256 au minimum * Algorithme de contrôle d’intégrité : MD5, SHA-256, SHA-384, SHA-512, |  |  |
|  | **Gestion de la bande passante :**   * Réservation et Priorisation des flux en fonction de la source, la destination, l’utilisateur et l’application,   Limitation de la bande passante par source, destination, application ou catégorie d’application. |  |  |
|  | **Administration et gestion des journaux :**   * Administration via une interface web intuitive et sécurisée en HTTPS, * Administration en ligne de commande SSH et Telnet, * Interface d’administration graphique multi-langues : Français et Anglais au minimum, * Support de l’administration par rôle, * Permettre l’export et l’importation de la configuration, * Suivie et visibilité en temps réel sur les flux transitant par le firewall avec possibilité de filtrage, * Outil de filtrage et recherche multicritère dans les journaux pour faciliter l’identification des incidents de sécurité. * Prise en charge de balises (tags) pour l’organisation des règles et des objets. * Différente vue pour les journaux : Flux, Menaces, Filtrage de contenu, Authentification, Systèmes * Vue synthétique des applications, menaces et URL, * Export des journaux vers des systèmes externes en Syslog et Intégration avec des solutions SIEM * Support de SNMPv3 * Journalisation locale dans le disque du NGFW sans dégradation des performances. * La solution doit inclure une autorité de certification x.509 interne qui peut générer des certificats pour les passerelles et les utilisateurs pour permettre une authentification facile sur les VPN, * La solution doit inclure la possibilité d'utiliser des autorités de certification externes, * La visionneuse de journaux doit avoir la possibilité de créer un filtre en utilisant les noms d'objets prédéfinis (hôtes, réseau, groupes, utilisateurs...), |  |  |
|  | **Filtrage URL** **et Filtrage de contenu**   * Filtrage HTTP, HTTPS, HTTP2 ; * Filtrage URL à base de catégories ; * Inspection des flux chiffrés TLS 1.3 ; * Validation des certificats des serveurs (CRL, Algorithm, Cipher…) ; * Filtrage URL à base de l’adresse IP ; * Filtrage des liens de phishing dans les e-mails, des sites de phishing ; * Filtrage des commandes et contrôles basés sur HTTP et les pages contenant des kits d’exploits ; * Filtrage des données en fonction du type de fichier, propriété de fichier, Metadata, mot clés… * Mise à jour de la base des URL. |  |  |
| **1.2** | **PRESTATION DE SERVICE**  Le prestataire doit proposer dans son offre toutes les prestations nécessaires à la mise en œuvre de la solution de sécurité :   * Ingénierie et définition de l’architecture finale ; * Analyse du plan d’adressage IP, de routage et de découpage VLAN ; * Intégration de la solution dans le réseau de la CMC ; * L’interconnexion du NGFW avec les Switch Datacenter ; * L’installation et la configuration des fonctions du pare feu nouvelle génération selon les bonnes pratiques et les standards de la sécurité ; * La définition de la matrice des flux ; * Le prestataire doit réaliser tout essai jugé nécessaire pour s’assurer de la conformité et du bon fonctionnement de la plateforme de sécurité ; * Transfert de compétence ; * Garantie et maintenance (couvre l’assistance (sur site ou à distance), l’intervention sur site, les pièces de rechanges et la main d’œuvre) pour une durée 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 ; * Livrables :   + Document d’architecture finale et de configuration de la solution (avec schéma au format exploitable et un fichier de configuration) ;   Manuel d’exploitation ; |  |  |

**BORDEREAU DES PRIX – DETAIL ESTIMATIF**

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

| **Items N°** | **Désignations** | **Unité** | **(1)**  **QTE** | **(2)**  **Prix unitaire**  **HT/HDD/HTVA** | **(3)**  **Prix total HT/HDD/HTVA**  **(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**

**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** |
| --- | --- | --- | --- |
| **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** |  |  |
|  | **Fonctions Firewall**   * Doit intégrer un système d’exploitation propriétaire sécurisé, * Filtrage de paquets et être doté de la fonction de filtrage dynamique, * Filtrage basé sur les applications niveau 7 en plus des ports/Protocol et par plages de ports UDP ou TCP * Filtrage et inspection en IPv4 et IPv6, * Failover de connexion Internet, * Prise en compte de paramètre Horaire dans les règles de filtrage, * Doit fournir, via sa console d’administration, des statistiques sur le nombre d'accès aux règles de sécurité, * Doit inclure la possibilité de fonctionner en mode transparent ou routé (natté), * Doit fournir la possibilité de définir des instances firewall virtuels sur la même Appliance, et capable d’activer les fonctionnalités de protection IPS, Sandboxing, Control Applicatif, filtrage d’URL, Anti-bot, Anti-virus/Antimalware, * La création de la politique de sécurité basée sur :   + Geolocation par pays   + Zones   + Groupes de Zones   + Applications, Groupes d’applications   + Catégories d’Applications   + Technologies d’Applications   + Filtres d’Applications   + Utilisateurs et Groupes   + Adresses IP, Groupes d’adresses IP, Sous-réseaux IP, Groupes de sous-réseaux IP   + Services, Groupes de Services * La solution doit être de type Next Generation Firewall avec capacité de prévention contre les menaces avancées, combinée avec des fonctionnalités de base suivantes (**licences incluses)** : * **IPS (prévention des intrusions)** pour se protéger contre les menaces réseau telles que vers, chevaux de Troie et autres programmes malveillants. Le système de prévention des intrusions (IPS) doit aussi apporter une protection contre les menaces réseaux existantes et émergentes. Ce module IPS doit avoir deux mécanismes : * Détection par signatures ; * Détection par anomalies ; * Capable de faire des analyses comportementales de tout type de trafic ; * Possibilité de créer des signatures personnalisées ; * Mise à jour automatique des signatures IPS ; * Création et affectation des politiques IPS par type de zone ou interface ; * Pour chaque événement d’attaque, il sera possible de laisser passer ou bloquer, de faire une mise en quarantaine automatique (IP totalement bloquée pendant un temps donné) … ; * Gestion de profils IPS avec association à certains trafics dans la politique de filtrage (IP source, IP destination, service, protocole, réseau…) ; * **Filtrage URL**,pour assurer le contrôle de l’accès interne aux contenus Web indésirables, non productifs, voire illégaux, * **Control Applicatif,** afin d’identifier, reconnaître et contrôler les applications dans les flux, | **Marque :**  **Référence :**  **Caractéristiques proposées** |  |
|  | **Spécifications matérielles et performance :**   * Format : Appliance Rackable, 19’’ * 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 * Nombre de sessions inspectées simultanées : **1 Million** Minimum * Nombre de nouvelles sessions par seconde : **50 000** Minimum * Stockage Disque dur dédiée de type SSD de **200** GB Minimum * Les ports (en dehors des ports de management et de la haute disponibilité)   + Minimum 8 ports 10/100/1000 BaseT   + Minimum 4 ports 1G/10G SFP/SFP+ dont **4** avec **Transceiver SFP+** * Les ports de management et Clustering :   + Minimum 1 port 10/100/1000 BaseT pour le management   + Minimum 1 port console RJ-45   + Minimum 1 port USB   + Minimum 1 ports 10/100/1000 BaseT pour le HA   2 Alimentations électriques Redondantes Minimum (AC), |  |  |
|  | **Support de la haute disponibilité** :   * Actif/Actif avec synchronisation d’état de session, * Actif/Passif, |  |  |
|  | **Contrôle applicatif :**   * Identification des applications en se basant sur :   + Signatures   + Décodage du protocole (respecte la spécification du protocole)   + Déchiffrement du trafic encapsulé * Identification et contrôle des applications partageant la même connexion * Contrôle de la fonction de transfert de fichiers d’une application * Visibilité du trafic applicatif inconnu à travers l’identification de sa nature :   + Volume du trafic   + Utilisateur et/ou adresses IP   + Port utilisé   + Contenu associé : fichier, menace ou autre. * La base de données de contrôle des applications doit contenir plus de **3 000** applications connues ;   La solution doit pouvoir créer une règle de filtrage avec plusieurs catégories ; |  |  |
|  | **Identification, authentification des utilisateurs et protection des identités**   * Prise en charge des services d'authentification suivants pour l'identification et authentifications des utilisateurs :   + Active Directory   + Kerberos   + LDAP   + Radius   + Base Locale   + SAML   + Authentification via SSO Kerberos sans agent   + Authentification par Certificat client   + Portail captif * Identification des utilisateurs indépendamment :   + Du terminal (ordinateur, un téléphone intelligent ou une tablette)   + Du système d’exploitation utilisé,   + Des adresses IP et de la zone (LAN, VPN, hors du périmètre du réseau) |  |  |
|  | **Fonctions Réseau :**   * Support mode Routage, mode transparent, TAP ou SPAN, * Support IPv4 et IPv6 * Routage IPv4 : Statique et Dynamique, RIPv2, OSPFv3 et BGP au minimum * Agrégation des liens 802.3ad, LACP * Support des VLAN 802.1q * Support des modes de translations NAT et PAT * Nat dynamique, Nat Statique, Nat par port, Nat64 * Support de Multicast * 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)** |  |  |
|  | **Fonction VPN :**   * VPN IPSec site-site, client-site et hub & Spoke. **(Fonctionnalité et licence à fournir)** * Support du VPN SSL mode portail et mode tunnel (avec ou sans agent) * Support du Tunnel GRE * Support de IKEv1 et IKEv2 avec authentification à base de clé pré-partagée (PSK) ou certificat * Standard de Chiffrement : 3DES, AES 256 au minimum * Algorithme de contrôle d’intégrité : MD5, SHA-256, SHA-384, SHA-512, |  |  |
|  | **Gestion de la bande passante :**   * Réservation et Priorisation des flux en fonction de la source, la destination, l’utilisateur et l’application,   Limitation de la bande passante par source, destination, application ou catégorie d’application. |  |  |
|  | **Administration et gestion des journaux :**   * Administration via une interface web intuitive et sécurisée en HTTPS, * Administration en ligne de commande SSH et Telnet, * Interface d’administration graphique multi-langues : Français et Anglais au minimum, * Support de l’administration par rôle, * Permettre l’export et l’importation de la configuration, * Suivie et visibilité en temps réel sur les flux transitant par le firewall avec possibilité de filtrage, * Outil de filtrage et recherche multicritère dans les journaux pour faciliter l’identification des incidents de sécurité. * Prise en charge de balises (tags) pour l’organisation des règles et des objets. * Différente vue pour les journaux : Flux, Menaces, Filtrage de contenu, Authentification, Systèmes * Vue synthétique des applications, menaces et URL, * Export des journaux vers des systèmes externes en Syslog et Intégration avec des solutions SIEM * Support de SNMPv3 * Journalisation locale dans le disque du NGFW sans dégradation des performances. * La solution doit inclure une autorité de certification x.509 interne qui peut générer des certificats pour les passerelles et les utilisateurs pour permettre une authentification facile sur les VPN, * La solution doit inclure la possibilité d'utiliser des autorités de certification externes, * La visionneuse de journaux doit avoir la possibilité de créer un filtre en utilisant les noms d'objets prédéfinis (hôtes, réseau, groupes, utilisateurs...), |  |  |
|  | **Filtrage URL** **et Filtrage de contenu**   * Filtrage HTTP, HTTPS, HTTP2 ; * Filtrage URL à base de catégories ; * Inspection des flux chiffrés TLS 1.3 ; * Validation des certificats des serveurs (CRL, Algorithm, Cipher…) ; * Filtrage URL à base de l’adresse IP ; * Filtrage des liens de phishing dans les e-mails, des sites de phishing ; * Filtrage des commandes et contrôles basés sur HTTP et les pages contenant des kits d’exploits ; * Filtrage des données en fonction du type de fichier, propriété de fichier, Metadata, mot clés… * Mise à jour de la base des URL. |  |  |
| **1.2** | **PRESTATION DE SERVICE**  Le prestataire doit proposer dans son offre toutes les prestations nécessaires à la mise en œuvre de la solution de sécurité :   * Ingénierie et définition de l’architecture finale ; * Analyse du plan d’adressage IP, de routage et de découpage VLAN ; * Intégration de la solution dans le réseau de la CMC ; * L’interconnexion du NGFW avec les Switch Datacenter ; * L’installation et la configuration des fonctions du pare feu nouvelle génération selon les bonnes pratiques et les standards de la sécurité ; * La définition de la matrice des flux ; * Le prestataire doit réaliser tout essai jugé nécessaire pour s’assurer de la conformité et du bon fonctionnement de la plateforme de sécurité ; * Transfert de compétence ; * Garantie et maintenance (couvre l’assistance (sur site ou à distance), l’intervention sur site, les pièces de rechanges et la main d’œuvre) pour une durée 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 ; * Livrables :   + Document d’architecture finale et de configuration de la solution (avec schéma au format exploitable et un fichier de configuration) ;   Manuel d’exploitation ; |  |  |

**BORDEREAU DES PRIX – DETAIL ESTIMATIF**

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

| **Items N°** | **Désignations** | **Unité** | **(1)**  **QTE** | **(2)**  **Prix unitaire**  **HT/HDD/HTVA** | **(3)**  **Prix total HT/HDD/HTVA**  **(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**

**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** |
| --- | --- | --- | --- |
| **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** |  |  |
|  | **Fonctions Firewall**   * Doit intégrer un système d’exploitation propriétaire sécurisé, * Filtrage de paquets et être doté de la fonction de filtrage dynamique, * Filtrage basé sur les applications niveau 7 en plus des ports/Protocol et par plages de ports UDP ou TCP * Filtrage et inspection en IPv4 et IPv6, * Failover de connexion Internet, * Prise en compte de paramètre Horaire dans les règles de filtrage, * Doit fournir, via sa console d’administration, des statistiques sur le nombre d'accès aux règles de sécurité, * Doit inclure la possibilité de fonctionner en mode transparent ou routé (natté), * Doit fournir la possibilité de définir des instances firewall virtuels sur la même Appliance, et capable d’activer les fonctionnalités de protection IPS, Sandboxing, Control Applicatif, filtrage d’URL, Anti-bot, Anti-virus/Antimalware, * La création de la politique de sécurité basée sur :   + Geolocation par pays   + Zones   + Groupes de Zones   + Applications, Groupes d’applications   + Catégories d’Applications   + Technologies d’Applications   + Filtres d’Applications   + Utilisateurs et Groupes   + Adresses IP, Groupes d’adresses IP, Sous-réseaux IP, Groupes de sous-réseaux IP   + Services, Groupes de Services * La solution doit être de type Next Generation Firewall avec capacité de prévention contre les menaces avancées, combinée avec des fonctionnalités de base suivantes (**licences incluses)** : * **IPS (prévention des intrusions)** pour se protéger contre les menaces réseau telles que vers, chevaux de Troie et autres programmes malveillants. Le système de prévention des intrusions (IPS) doit aussi apporter une protection contre les menaces réseaux existantes et émergentes. Ce module IPS doit avoir deux mécanismes : * Détection par signatures ; * Détection par anomalies ; * Capable de faire des analyses comportementales de tout type de trafic ; * Possibilité de créer des signatures personnalisées ; * Mise à jour automatique des signatures IPS ; * Création et affectation des politiques IPS par type de zone ou interface ; * Pour chaque événement d’attaque, il sera possible de laisser passer ou bloquer, de faire une mise en quarantaine automatique (IP totalement bloquée pendant un temps donné) … ; * Gestion de profils IPS avec association à certains trafics dans la politique de filtrage (IP source, IP destination, service, protocole, réseau…) ; * **Filtrage URL**,pour assurer le contrôle de l’accès interne aux contenus Web indésirables, non productifs, voire illégaux, * **Control Applicatif,** afin d’identifier, reconnaître et contrôler les applications dans les flux, | **Marque :**  **Référence :**  **Caractéristiques proposées** |  |
|  | **Spécifications matérielles et performance :**   * Format : Appliance Rackable, 19’’ * 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 * Nombre de sessions inspectées simultanées : **1 Million** Minimum * Nombre de nouvelles sessions par seconde : **50 000** Minimum * Stockage Disque dur dédiée de type SSD de **200** GB Minimum * Les ports (en dehors des ports de management et de la haute disponibilité)   + Minimum 8 ports 10/100/1000 BaseT   + Minimum 4 ports 1G/10G SFP/SFP+ dont **4** avec **Transceiver SFP+** * Les ports de management et Clustering :   + Minimum 1 port 10/100/1000 BaseT pour le management   + Minimum 1 port console RJ-45   + Minimum 1 port USB   + Minimum 1 ports 10/100/1000 BaseT pour le HA   2 Alimentations électriques Redondantes Minimum (AC), |  |  |
|  | **Support de la haute disponibilité** :   * Actif/Actif avec synchronisation d’état de session, * Actif/Passif, |  |  |
|  | **Contrôle applicatif :**   * Identification des applications en se basant sur :   + Signatures   + Décodage du protocole (respecte la spécification du protocole)   + Déchiffrement du trafic encapsulé * Identification et contrôle des applications partageant la même connexion * Contrôle de la fonction de transfert de fichiers d’une application * Visibilité du trafic applicatif inconnu à travers l’identification de sa nature :   + Volume du trafic   + Utilisateur et/ou adresses IP   + Port utilisé   + Contenu associé : fichier, menace ou autre. * La base de données de contrôle des applications doit contenir plus de **3 000** applications connues ;   La solution doit pouvoir créer une règle de filtrage avec plusieurs catégories ; |  |  |
|  | **Identification, authentification des utilisateurs et protection des identités**   * Prise en charge des services d'authentification suivants pour l'identification et authentifications des utilisateurs :   + Active Directory   + Kerberos   + LDAP   + Radius   + Base Locale   + SAML   + Authentification via SSO Kerberos sans agent   + Authentification par Certificat client   + Portail captif * Identification des utilisateurs indépendamment :   + Du terminal (ordinateur, un téléphone intelligent ou une tablette)   + Du système d’exploitation utilisé,   + Des adresses IP et de la zone (LAN, VPN, hors du périmètre du réseau) |  |  |
|  | **Fonctions Réseau :**   * Support mode Routage, mode transparent, TAP ou SPAN, * Support IPv4 et IPv6 * Routage IPv4 : Statique et Dynamique, RIPv2, OSPFv3 et BGP au minimum * Agrégation des liens 802.3ad, LACP * Support des VLAN 802.1q * Support des modes de translations NAT et PAT * Nat dynamique, Nat Statique, Nat par port, Nat64 * Support de Multicast * 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)** |  |  |
|  | **Fonction VPN :**   * VPN IPSec site-site, client-site et hub & Spoke. **(Fonctionnalité et licence à fournir)** * Support du VPN SSL mode portail et mode tunnel (avec ou sans agent) * Support du Tunnel GRE * Support de IKEv1 et IKEv2 avec authentification à base de clé pré-partagée (PSK) ou certificat * Standard de Chiffrement : 3DES, AES 256 au minimum * Algorithme de contrôle d’intégrité : MD5, SHA-256, SHA-384, SHA-512, |  |  |
|  | **Gestion de la bande passante :**   * Réservation et Priorisation des flux en fonction de la source, la destination, l’utilisateur et l’application,   Limitation de la bande passante par source, destination, application ou catégorie d’application. |  |  |
|  | **Administration et gestion des journaux :**   * Administration via une interface web intuitive et sécurisée en HTTPS, * Administration en ligne de commande SSH et Telnet, * Interface d’administration graphique multi-langues : Français et Anglais au minimum, * Support de l’administration par rôle, * Permettre l’export et l’importation de la configuration, * Suivie et visibilité en temps réel sur les flux transitant par le firewall avec possibilité de filtrage, * Outil de filtrage et recherche multicritère dans les journaux pour faciliter l’identification des incidents de sécurité. * Prise en charge de balises (tags) pour l’organisation des règles et des objets. * Différente vue pour les journaux : Flux, Menaces, Filtrage de contenu, Authentification, Systèmes * Vue synthétique des applications, menaces et URL, * Export des journaux vers des systèmes externes en Syslog et Intégration avec des solutions SIEM * Support de SNMPv3 * Journalisation locale dans le disque du NGFW sans dégradation des performances. * La solution doit inclure une autorité de certification x.509 interne qui peut générer des certificats pour les passerelles et les utilisateurs pour permettre une authentification facile sur les VPN, * La solution doit inclure la possibilité d'utiliser des autorités de certification externes, * La visionneuse de journaux doit avoir la possibilité de créer un filtre en utilisant les noms d'objets prédéfinis (hôtes, réseau, groupes, utilisateurs...), |  |  |
|  | **Filtrage URL** **et Filtrage de contenu**   * Filtrage HTTP, HTTPS, HTTP2 ; * Filtrage URL à base de catégories ; * Inspection des flux chiffrés TLS 1.3 ; * Validation des certificats des serveurs (CRL, Algorithm, Cipher…) ; * Filtrage URL à base de l’adresse IP ; * Filtrage des liens de phishing dans les e-mails, des sites de phishing ; * Filtrage des commandes et contrôles basés sur HTTP et les pages contenant des kits d’exploits ; * Filtrage des données en fonction du type de fichier, propriété de fichier, Metadata, mot clés… * Mise à jour de la base des URL. |  |  |
| **1.2** | **PRESTATION DE SERVICE**  Le prestataire doit proposer dans son offre toutes les prestations nécessaires à la mise en œuvre de la solution de sécurité :   * Ingénierie et définition de l’architecture finale ; * Analyse du plan d’adressage IP, de routage et de découpage VLAN ; * Intégration de la solution dans le réseau de la CMC ; * L’interconnexion du NGFW avec les Switch Datacenter ; * L’installation et la configuration des fonctions du pare feu nouvelle génération selon les bonnes pratiques et les standards de la sécurité ; * La définition de la matrice des flux ; * Le prestataire doit réaliser tout essai jugé nécessaire pour s’assurer de la conformité et du bon fonctionnement de la plateforme de sécurité ; * Transfert de compétence ; * Garantie et maintenance (couvre l’assistance (sur site ou à distance), l’intervention sur site, les pièces de rechanges et la main d’œuvre) pour une durée 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 ; * Livrables :   + Document d’architecture finale et de configuration de la solution (avec schéma au format exploitable et un fichier de configuration) ;   Manuel d’exploitation ; |  |  |

**BORDEREAU DES PRIX – DETAIL ESTIMATIF**

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

| **Items N°** | **Désignations** | **Unité** | **(1)**  **QTE** | **(2)**  **Prix unitaire**  **HT/HDD/HTVA** | **(3)**  **Prix total HT/HDD/HTVA**  **(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**