



المصرف المغربي للإستثمار و التجارة الخارجية  
Banque Maghrébine d'Investissement et de Commerce Extérieur

**Appel d'offre N°2/2025**  
**Pour la Fourniture et l'Installation d'Equipements**  
**de Sécurité Informatique**  
**(Firewalls Edge, Firewalls Data Center)**

Juin 2025

## **A- Cahier des Clauses Administratives Particulières**

Je soussigné (Nom, prénom et fonction) .....

Représentant la société (Nom, adresse complète et n° de téléphone)  
.....

Déclare avoir pris connaissance et accepté les clauses suivantes :

### **ARTICLE 1 - OBJET DE L'APPEL D'OFFRES**

Le présent Appel d'offres a pour objet la fourniture et la mise en place des équipements de sécurité au profit de la Banque Maghrébine d'Investissement et de Commerce Extérieur **BMICE**, conformément aux dispositions du présent Appel d'offres.

Les équipements à fournir sont :

- 2 Firewalls Edge
- 2 Firewalls Datacenter

### **Le présent Appel d'offres se compose d'un seul lot.**

L'offre du soumissionnaire ne doit pas contenir plus d'une variante sous peine de rejet de l'offre.

On entend par "équipements" l'ensemble de matériels à acquérir.

Ces équipements qui doivent être conformes aux spécifications techniques décrites dans le présent cahier des charges Administratives et Techniques, seront installés dans les locaux de la Banque Maghrébine d'Investissement et de Commerce Extérieur (Siège social à Tunis).

### **ARTICLE 2 : PIECES CONSTITUTIVES DU PRESENT APPEL D'OFFRES**

Les pièces constitutives de l'Appel d'offres sont par ordre d'importance

- La soumission qui constitue l'acte d'engagement.
- Le bordereau des prix.
- L'Appel d'offres lancé par la BMICE

### **ARTICLE 3- LANGUE DE L'OFFRE**

L'offre préparée par le soumissionnaire ainsi que toutes les correspondances, les plans et dessins, les caractéristiques techniques et tout document concernant l'offre, échangé entre le soumissionnaire et l'acquéreur seront obligatoirement rédigés en langue française.

Certaines fiches techniques pourront, toutefois, être présentées en langue anglaise.

#### **ARTICLE 4- DEMANDES D'ÉCLAIRCISSEMENTS**

Toute question qui pourrait se présenter concernant l'interprétation du document du présent Appel d'offres, y compris les spécifications techniques ou toute autre demande d'information complémentaire nécessaire à la clarification du contenu de ce document, devra être demandée par écrit à la Banque Maghrébine d'Investissement et de Commerce Extérieur **BMICE**.

Les réponses fournies par écrit prendront la forme d'additifs aux documents du marché résultant de l'Appel d'offres et seront communiquées **à l'ensemble des candidats** ayant déjà retiré le cahier de charges et ce avant la date limite de clôture des soumissions. Les explications ou instructions fournies oralement n'ont aucune valeur contractuelle.

#### **ARTICLE 5 – CONDITIONS DE PRESENTATION DE L'OFFRE**

Les soumissionnaires, par le fait même de soumissionner, reconnaissent être en mesure de réaliser les prestations prévues au bordereau des prix.

L'offre technique et l'offre financière sont placées dans deux enveloppes séparées et fermées. Ces deux enveloppes, les documents administratifs accompagnant les offres et les cahiers des charges seront placés dans une troisième enveloppe extérieure fermée sur laquelle est indiquée :

#### **« Acquisition des Equipements de sécurité Informatique Pour la BMICE >>**

Avec la mention « **A NE PAS OUVRIR** » ainsi que l'adresse suivante : Banque Maghrébine d'Investissement et de Commerce Extérieur **BMICE – Immeuble Lilia Rue de la Bourse, Les Berges du Lac 2 Tunis 1053 TUNISIE**.

Les offres, pour être valables, devront être entièrement rédigées à l'encre et particulièrement pour la soumission, le bordereau des prix et la décomposition des prix qui devront être paraphés à toutes les pages, signés et portant le cachet du mandataire à la dernière page.

#### **ARTICLE 6 : DOCUMENTS DE L'APPEL D'OFFRES & PIECES A FOURNIR :**

1. ENVELOPPE EXTERIEURE : DOCUMENTS ADMINISTRATIFS ET CAHIERS DES CHARGES :

N°	DOCUMENTS APPELLATION	OPERATION A REALISER	AUTHENTIFICATION
A.1	Attestation de situation Fiscale	Dernière attestation en date de la Direction Générale des impôts, valable à la date limite de remise des plis.	Copie
A.2	Un extrait du RNE qui date de moins de 3 mois	Originale	
A.3	Attestation d'affiliation à la caisse nationale de sécurité sociale.		Copie
A.4	Déclaration sur l'honneur de non-faillite	Remplir le modèle fourni en annexe 4	Date, signature et cachet du soumissionnaire à la fin du document.
A.5	Déclaration sur l'honneur comportant la confirmation du soumissionnaire de n'avoir pas fait par lui-même ou par personne interposée, des promesses, des dons ou des présents en vue d'influer sur les différentes procédures de conclusion du marché et des étapes de sa réalisation.	Remplir le modèle fourni en annexe 5	Date, signature et cachet du soumissionnaire à la fin du document.
A.6	Copie Originale du présent cahier des charges Administratives et Techniques		Paraphe sur chaque page, Signature & cachet du soumissionnaire sur la dernière page.

<b>A.7</b>	Fiche d 'identification du soumissionnaire.	Remplir le modèle fourni en annexe 1	Date, Signature et cachet du soumissionnaire à la fin du document.
<b>A.8</b>	Cautionnement provisoire <b>valable 45 jours</b> agréé par établissement bancaire agréé par l'administration. <b>(Annexe 10)</b>	Date, signature et tampon du soumissionnaire à la fin du document	
<b>A.9</b>	Attestation prouvant la qualité du signataire de l'offre.	Au cas où des procurations seraient nécessaires, elles seront établies conformément aux lois et réglementation en vigueur	Authentification légale
<b>A.10</b>	Certificat ISO 9001 Ver 2015		
<b>A.11</b>	Caractéristiques Commerciales	Remplir le modèle fourni en annexe 8	Minimum 03 références Justificatifs à fournir (PV de réception et/ou contrat)
<b>A.12</b>	Autorisation de constructeur		Le soumissionnaire doit fournir une autorisation de constructeur pour la participation

**Important :**

- La non- fourniture du Caution entrainera l'annulation de l'offre.
- La non-fourniture de A1, A2, A3, A4, A5, A6, A7, A8, A9, A10, A11 et A12 après relance de la BMICE restée sans effet entrainera l'annulation de l'offre correspondant.

## 2. L'ENVELOPPE INTERIEURE « T » OFFRE TECHNIQUE :

N°	Documents	Authentification
T.1	Les Fichiers des spécifications techniques du constructeur	Copie en couleur, avec caché du soumissionnaire
T.2	Composition et expérience de l'équipe intervenante (Annexe 9)	Il est obligatoire de fournir : - Copie du diplôme pour chaque membre de l'équipe. - CV signé pour chaque membre de l'équipe. - Certifications pour chaque membre de l'équipe.

### **Important :**

- La non-fourniture des justificatifs de T1 et T2 après relance de la BMICE restée sans effet entraînera aussi l'annulation de l'offre correspondant.

## 3. L'ENVELOPPE INTERIEURE « F » OFFRE FINANCIERE :

N°	DOCUMENTS	OPERATION A REALISER	AUTHENTIFICATION
F1	La soumission Remplir le modèle fourni en annexe 2	Original du document remis par la BMICE dûment complété par le soumissionnaire	Datée et portant signature et cachet du soumissionnaire à la fin du document.
F2	Le bordereau des prix (Remplir le modèle fourni en annexe)	Original du document remis par la BMICE dûment complété par le soumissionnaire	Paraphe, signature & cachet du soumissionnaire

### **Important :**

- La non-fourniture de l'un de F1 entraînera l'annulation de l'offre.
- La non-fourniture de F2 après relance entraînera l'annulation de l'offre.

### **ARTICLE 7 : CAUTIONNEMENT PROVISOIRE**

Le montant du cautionnement provisoire est fixé à un montant forfaitaire de **Trois Mille (3000 DT) DINARS**, il peut être remplacé par une caution personnelle et solidaire qui devra être constituée conformément au modèle fourni en annexe, par une banque agréée. Il devra être valable pendant Quarante cinq JOURS (45 jours) à compter du jour suivant la date limite de réception des offres.

Toute offre ne comportant pas le cautionnement provisoire est éliminée.

### **ARTICLE 8 : CAUTIONNEMENT DEFINITIVE**

Le montant du cautionnement définitif est fixé à 3% du montant du marché initial augmenté le cas échéant du montant des avenants.

- La fourniture de ce cautionnement qui doit être établie conformément au modèle en annexe se fera dans les (20) jours au plus tard de la date de la notification de l'attribution du marché ou de la commande.
- Le versement du cautionnement définitif pourra être remplacé par une caution bancaire délivrée par une banque agréée et qui s'engage à verser immédiatement au maître d'ouvrage et à la première demande le montant de cette caution.

### **ARTICLE 9 - DÉLAIS DE VALIDITÉ DES OFFRES**

Les offres doivent être valables pendant une durée minimale de 90 jours à compter du jour suivant la date limite de réception des offres.

Toute offre dont la validité est inférieure à cette période sera écartée par l'acquéreur comme non conforme aux conditions du présent Appel d'Offres.

Pendant toute la période de validité de son offre, le soumissionnaire s'engage expressément et sans réserve, à renoncer au droit de retirer son offre et de ne pas y apporter ni additif ni correction, à moins que l'acquéreur ne le lui demande par écrit.

### **ARTICLE 10- DATE LIMITE DE RÉCEPTION DES OFFRES**

La date limite de réception des offres est fixée au **30/06/2025** (Le cachet du bureau d'ordre de La Banque Maghrébine d'Investissement et de Commerce Extérieur **BMICE** faisant foi).

L'acquéreur se réserve le droit de prolonger le délai de réception des offres. Dans ce cas, toutes les obligations des soumissionnaires seront maintenues au nouveau délai.

**Toute offre parvenue après expiration du délai de réception des offres fixé par l'acquéreur, sera automatiquement rejetée.**

## **ARTICLE 11- OUVERTURE DES PLIS**

La Commission de Marchés se réunit pour ouvrir les enveloppes contenant les offres techniques et financières en une séance unique.

La séance d'ouverture des plis est non publique.

La Commission de Marchés vérifie la présence des documents administratifs et élimine les offres parvenues hors délais.

La Commission de Marchés désigne les membres de la Commission d'Evaluation Technico-Financière.

## **ARTICLE 12- NATURE DES PRIX**

Les prix indiqués en hors Taxes sont fermes et non révisables pendant toute la durée d'exécution du marché et incluent tous les frais y nécessaires.

## **ARTICLE 13- GARANTIE**

Le soumissionnaire garantit que tous les équipements proposés seront fournis à l'état neuf, n'ayant pour cela jamais fonctionné depuis leur fabrication dans les usines du constructeur.

**La période de garantie est fixée à 36 mois au minimum.**

Le délai de garantie commence à courir à partir de la date de mise en marche des équipements.

## **ARTICLE 14- LIVRAISON ET INSTALLATION DES EQUIPEMENTS ET PRESTATIONS**

- **14.1** Le délai de livraison des équipements et des logiciels ne doit pas dépasser **soixante (60) Jours** à partir du jour suivant la date de notification du marché.
- **14.2 Le Titulaire** s'engage à fournir tous les moyens nécessaires pour la configuration et les tests de mise en marche des équipements livrés en présence d'une équipe technique désignée par l'acheteur.
- **14.3** Les équipements non conformes seront refusés et le fournisseur doit les remplacer dans les **15 jours** qui suivent son information par lettre recommandée.
- **14.4 Le Titulaire** doit installer tous les équipements dans un délai maximum de dix (10) jours à compter de la date de livraison.
- **14.5 Le titulaire** doit fournir tous les moyens nécessaires pour la configuration et les tests de mise en marche des équipements livrés en présence d'une équipe technique désignée par la BMICE.
- **14.6** A l'issue de cette installation, les équipements doivent être fonctionnels et exploitables par les services utilisateurs de la BMICE conformément aux spécifications techniques détaillées dans l'appel d'offres.
- **14.7** L'installation de la mise en service des équipements doivent être réalisés obligatoirement sans perturber la bonne marche de la BMICE.

- **14.8** En cas de force majeure, tel que défini par le droit Tunisien, ces délais pourront être prolongés par demande écrite du fournisseur qui doit justifier que l'évènement qu'il invoque, présente les caractéristiques de forces majeures. C'est-à-dire qu'il était imprévisible, lors de la remise de l'offre.

## **ARTICLE 15: Transfert de compétence**

Dans le cadre de la présente prestation, le prestataire s'engage à assurer un transfert de compétences structuré et documenté aux équipes techniques de la Banque, afin de garantir leur autonomie dans la gestion opérationnelle et sécuritaire de la solution firewalls.

Ce transfert de compétences est une exigence contractuelle essentielle, compte tenu des enjeux critiques de continuité d'activité, de conformité réglementaire et de maîtrise des risques cyber dans le secteur bancaire.

### **15.1** Contenu du transfert

Le transfert de compétences devra obligatoirement couvrir, de manière théorique et pratique:

- L'architecture fonctionnelle et sécuritaire des firewalls fournis ;
- La gestion des politiques de sécurité : filtrage réseau, applicatif, utilisateurs (pare-feu, proxy, IPS/IDS, etc.) ;
- La gestion des VPN (site-to-site, utilisateur distant) et leur durcissement ;
- La configuration des systèmes de haute disponibilité et de bascule automatique (failover/HA) ;
- Les procédures de journalisation, d'analyse de logs et de génération de rapports d'audit ;
- La gestion des mises à jour, correctifs et licences dans un contexte de conformité continue ;
- La configuration d'alertes de sécurité et l'intégration éventuelle avec les systèmes SOC/SIEM existants.

### **15.2** Modalités de réalisation

Le prestataire devra fournir :

- Un plan de transfert de compétences en annexe de son offre, précisant les objectifs pédagogiques, le programme détaillé, la durée, les profils des formateurs, et les livrables ; incluant entre autres :
  - Les thématiques abordées pour chaque type de firewalls
  - La durée estimée de chaque session
  - Le profil et l'expérience des formateurs
  - Les livrables remis (supports, guides, procédures)
- Une formation sur site ou à distance, d'une durée minimale de 3 jours, à destination d'au moins 3 administrateurs réseau/sécurité désignés par la Banque ;
- Des supports de formation personnalisés (en français) incluant les captures d'écran, scénarios de configuration, fiches de procédures et manuels d'exploitation ;
- Un accompagnement post-installation de 5 jours ouvrés, incluant un support technique renforcé lors des premières semaines d'exploitation en production.
- Des supports pédagogiques personnalisés incluant :

- Fiches de configuration (Edge vs Datacenter)
- Procédures de sauvegarde/restauration
- Bonnes pratiques de sécurité et durcissement

### **15.3 Attestation et évaluation**

À l'issue du transfert, une attestation de transfert de compétences devra être signée par les deux parties. Un rapport d'évaluation des acquis pourra être exigé.

### **ARTICLE 16 : PENALITE DE RETARD**

En cas de retard dument constaté dans le délai global, le soumissionnaire est passible, sans qu'il soit nécessaire d'effectuer une mise en demeure préalable, d'une Pénalité P du montant total du marché hors taxes par jour de retard (dimanche et jours de fête non compris) ; les pénalités sont plafonnées à 5% (cinq pour cent) du montant du marché hors taxes et calculées selon la formule suivante :

$P = V/1000 \times R$  Où :

- P = Montant des pénalités
- V = Montant total du marché hors taxes.
- R = Nombre de jours de retard.

Dans le cas où les pénalités dépasseraient le plafond de cinq pour cent (5%) du montant total du présent marché hors taxes, la BMICE pourra prendre toutes les dispositions nécessaires et réglementaires pour terminer l'étude objet du présent marché par tout moyen qu'il jugera nécessaire aux frais et risques du titulaire du marché défaillant.

### **ARTICLE 17 : EVALUATION DES OFFRES**

L'évaluation des offres portera sur les offres techniques et les offres financières, le soumissionnaire qui sera retenu sera celui qui aura présenté l'offre financière la moins disante et répondant strictement aux spécifications demandées.

L'évaluation des offres sera réalisée par la BMICE seule, postérieurement après la séance de l'ouverture des offres.

### **ARTICLE 18- DOCUMENTATION**

Le titulaire doit fournir au minimum un jeu de documentation technique exhaustif pour chaque type de produit, matériel ou logiciel qui sera installé.

### **ARTICLE 19- RECEPTION**

Les réceptions des équipements seront effectuées de la manière suivante :

- **19.1- Réception provisoire :**

Une réception provisoire sera prononcée après :

1/ La livraison des équipements sur le site de l'acquéreur tel qu'indiqué ci-dessus.

2/ L'installation de tous les équipements.

3/ la configuration et les tests de mise en marche des équipements

- **19.2- Réception définitive :**

Une réception définitive sera prononcée après 30 jours de la réception provisoire.

**La réception provisoire et la réception définitive doivent être sanctionnées par un procès-verbal, dûment signé par les deux parties contractantes.**

### **ARTICLE 20- MODALITES DE PAIEMENT**

- 60% Suite à la signature réception provisoire
- 40% Suite à la signature de réception définitive libérables contre une caution bancaire établie par une institution bancaire reconnue et ce dès la signature de la réception provisoire.

La caution de garantie dans ce cas sera libérée suite à la signature de la réception définitive.

### **ARTICLE 21- CRITÈRES D'ÉLIMINATION**

- Toute offre technique ou financière non-conforme aux conditions des cahiers des charges ou comporte des réserves demeurées non levées est éliminée.
- Le non-fourniture des pièces constituant l'offre technique
- Le non-fourniture des pièces administratives après demande de l'acquéreur.
- Le non-fourniture des documents constituant l'offre financière.
- Toute information qui s'avère erronée constitue un motif de rejet de l'offre.
- Toutes réponses aux conditions de l'Appel d'offres doivent être accompagnées des pièces justificatives qui constituent en leur absence un motif de rejet de l'offre, et ce après demande de l'acquéreur.
- Toute offre technique non conforme à une ou à la totalité des spécifications techniques du cahier des clauses techniques sera éliminée.

### **ARTICLE 22-PROCÉDURE DE PASSATION DU MARCHÉ**

- **22.1** – Le soumissionnaire provisoirement retenu en recevra notification à son adresse officielle mentionnée à l'annexe. Il devra dans les 10 jours qui suivent, remplir toutes les formalités relatives à la passation du marché.
- **22.2** – Dans le cas où le soumissionnaire n'aurait pas rempli ces obligations, le choix de celui-ci pour exécuter les travaux pourra être annulé sans aucun recours et le cautionnement provisoire sera encaissé par l'acquéreur.
- **22.3** – Une fois que le marché approuvé, l'adjudicataire provisoire en reçoit notification. Il doit verser son cautionnement définitif trois pour cent (3%) du montant de l'offre retenue

dans les vingt (20) jours suivants. Il doit aussi s'acquitter les frais auxquels peuvent donner lieu les droits d'enregistrement du marché dans un délai n'excédant pas quarante-cinq (45) jours à partir de la date de notification.

- **22.4** –Toutes les offres qui ne répondent pas aux conditions énumérées ci-dessus seront rejetées.

### **ARTICLE 23- CAS DE FORCE MAJEURE**

Les cas de force majeure doivent être signalés par écrit, par l'entreprise au plus tard dans les dix (10) jours qui suivent l'évènement. Passé ce délai, l'entreprise n'est plus admise à réclamer.

### **ARTICLE 24- RESILIATION**

En plus des dispositions de ce cahier des charges le marché peut être résilié par décision du L'acquéreur dans les cas suivants :

- Décès ou faillite du titulaire.
- Incapacité nette et permanente du titulaire du marché.
- Le titulaire déclare ne pas pouvoir exécuter ses engagements sans qu'il puisse invoquer un cas de force majeure, entre autres en modifiant la constitution des équipes proposées dans son offre, sans autorisation préalable de l'acquéreur.

### **ARTICLE 25- REGLEMENT DES LITIGES**

Les litiges qui pourraient découler de l'interprétation ou de l'exécution des clauses du présent cahier des charges, seront, à défaut de solution amiable entre les deux parties, soumis au tribunal de Tunis 1 compétent en la matière.

Fait à ..... le .....

**Signature et cachet du soumissionnaire**

## B- Cahier de Clause Technique

### I. Introduction

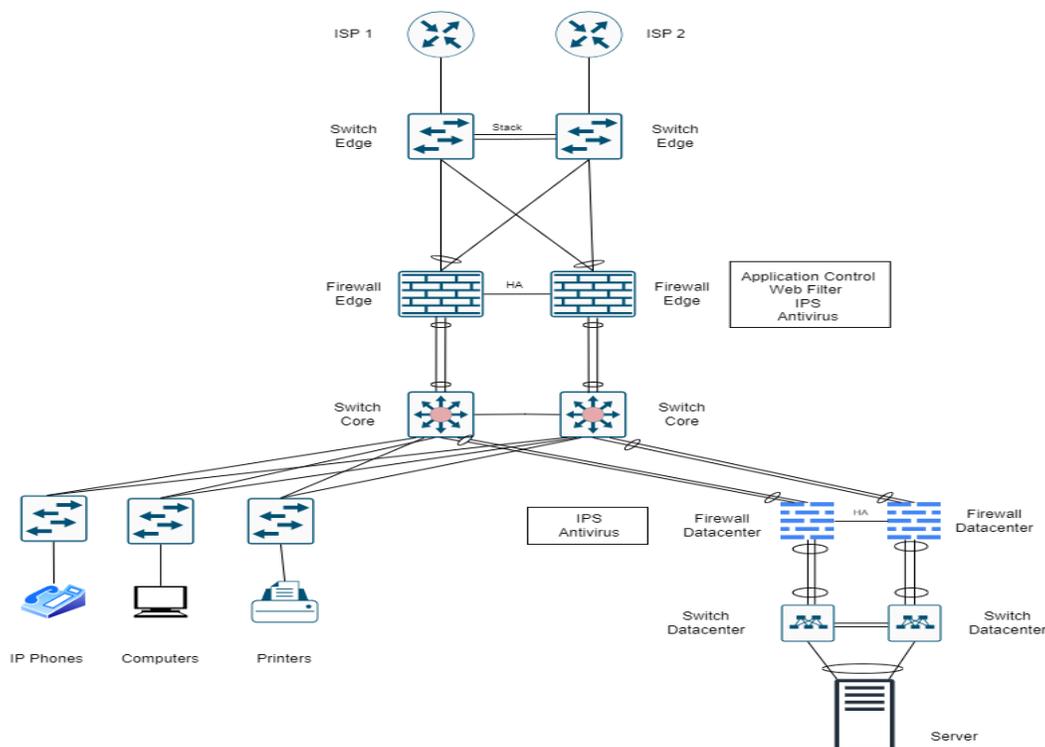
La BMICE vise à mettre à niveau l'infrastructure réseau en mettant en œuvre deux Firewalls Edge pour remplacer le firewalls existant et en mettant en place un cluster de Firewalls Data Center.

Les principaux objectifs de cette migration sont les suivants :

- **Sécurité renforcée** : Les Firewalls Edge protègent le réseau contre les menaces externes, tandis que les Firewalls Datacenter sécurisent les données et les applications à l'intérieur du réseau, offrant ainsi une défense multicouche.
- **Segmentation du trafic** : L'utilisation des deux types de Firewalls, permet de segmenter le trafic réseau en fonction de son origine et de sa destination et de mieux contrôler et gérer le flux de données.
- **Optimisation des performances** : La distribution des charges de sécurité entre les Firewalls Edge et Datacenter permet d'éviter la surcharge et d'optimiser les performances du réseau.

### II. Architecture proposée :

L'architecture réseau proposée pour la BMICE devrait mettre en œuvre des Firewalls Edge et Datacenter, configurés pour protéger les ressources critiques de l'organisation contre les menaces, tout en permettant un flux de données nécessaire pour les opérations de la BMICE



**Figure 1: Architecture cible pour BMCIE**

### III. Exigence Fonctionnelles

#### 1- Firewalls Edge:

Les Firewalls Edge doivent être positionnés à la frontière externe du réseau de la banque entre le réseau interne et Internet.

Ils doivent être configurés pour permettre un trafic spécifique nécessaire aux activités de la BMICE tout en bloquant tout trafic non autorisé.

#### 2- Firewalls Datacenter:

Les Firewalls Datacenter doivent être situés à l'intérieur du réseau de la banque, généralement entre les segments du réseau ou entre les réseaux de différents niveaux de sécurité.

Ils doivent être configurés pour permettre le trafic nécessaire entre les différents composants du réseau de la BMICE, tout en bloquant tout trafic non autorisé et en surveillant le trafic interne pour détecter les activités suspectes.

### IV. Tableau Technique

#### 1 – Firewalls Edge

Désignations	Caractéristiques techniques minimales Exigées	Spécifications techniques proposées
<b>Quantité</b>	1 (un cluster de 2 Firewalls)	
<b>Identification</b>		
<b>Marque</b>	A spécifier – Doit être différente de celle du Firewalls Datacenter	
<b>Modèle</b>	A spécifier	
<b>Type de solution</b>	NG Firewalls	
<b>Firewalls stateful inspection</b>	Oui	
<b>Interfaces</b>		
<b>Nombre d'interfaces réseau physiques (10/100/1000) RJ45</b>	8 x 1 Gbps Ethernet RJ45	
<b>Nombre d'interfaces réseau physiques SFP</b>	4 x 10 Gbps Ethernet SFP	
<b>Autres Interfaces</b>	2 x Port USB 1 x Port Console	
<b>Performances</b>		

<b>Débit en Clair</b>	10 Gbps	
<b>Débit NGFW\NGIPS</b>	2 Gbps	
<b>Débit IPSec</b>	2 Gbps	
<b>Nombre des Tunnels VPN IPSec</b>	2 000	
<b>Nombre de connexions simultanées</b>	1 millions	
<b>Nombre de nouvelles connexions par seconde</b>	50 000	
<b>Caractéristiques générales</b>		
<b>Securité</b>		
<b>Mode de déploiement</b>	- L3 Firewalls - L2\Transparent Firewalls - IPS - Combinaison des modes L2, L3 sur le même NGFW	
<b>Contrôle Applicatif</b>	Oui (+6000 Applications prédéfinies)	
<b>Filtrage URL basé sur les catégories</b>	Oui (80 catégories au moins)	
<b>Définition des règles de contrôle d'accès</b>	Basé sur IP\User ID\ Application Source\ Version Windows\zone de sécurité	
<b>Intrusion Prevention System</b>	Oui (inclus dans la licence de base)	
<b>Inspection du trafic TLS granulaire</b>	Oui (inclus dans la licence de base)	
<b>Protection Anti-Botnet</b>	Oui (inclus dans la licence de base)	
<b>Capture du trafic par interface (pcap)</b>	Oui	
<b>Protection contre les attaques DoS/DDoS</b>	Oui	
<b>Protection Antimalware \Antivirale</b>	La solution doit fournir une protection sur plusieurs niveaux : - Protection par réputation de fichier - Protection par un moteur antimalware	
<b>Identification \authentification des utilisateurs</b>		
<b>Authentification des utilisateurs</b>	Authentification active des utilisateurs via browser ou client VPN	
<b>Identification des utilisateur</b>	Identification transparente des utilisateurs	
<b>Annuaire Externe supporté</b>	LDAP, Active Directory	
<b>Protocole d'authentification</b>	Tacacs+, radius	
<b>High Availability</b>		

<b>Mode</b>	Actif\Actif, Actif\Standby	
<b>Nombre de node par cluster</b>	Jusqu'à 10 nœuds en mode Actif\Actif	
<b>Clustering</b>	- Possibilité de mettre en cluster des FW de version OS différente - Possibilité de mettre en cluster des FW de gamme différente	
<b>Server load balancing</b>	Partage de charge sur les serveurs avec prise en charge du SNAT	
<b>Lien internet</b>	Partage de charge dynamique sur les liens ISP (5 au minimum)	
<b>Routing</b>		
<b>Routage statique IPv4 et IPv6</b>	Oui	
<b>policy-based routing</b>	Oui	
<b>static multicast routing</b>	Oui	
<b>Protocole de routage dynamique</b>	RIPv2, RIPv6, OSPFv2, OSPFv3, BGP, PIM	
<b>Support Dynamic routing (OSPF, BGP)</b>	En mode Actif\Actif et Actif\Standby	
<b>NAT</b>	Source NAT, Dest NAT, Port Forwarding	
<b>SD-WAN</b>		
<b>Type de VPN</b>	- Policy Based VPN - Route based VPN	
<b>Configuration</b>	- Configuration et dépannage exclusivement à partir de la GUI (no CLI) - Reconfiguration de l'architecture SD-WAN par un simple Drag&Drop sans utilisation de CLI	
<b>Protocoles</b>	IPSEC et TLS	
<b>Topologies supportées</b>	- Hub and spoke, full mesh, partial mesh, Hybrid topologies - Création de tunnel a la demande entre spoke possédant des adresses IP dynamiques et sans utilisation de protocole de routage	
<b>Tunnel VPN</b>	Création automatique des tunnels VPN sur tous les interfaces WAN disponible par un simple drag&drop	

<b>Partage de charge sur les tunnels VPN</b>	Utilisation d'un mécanisme dynamique pour le partage de charge entre tunnel VPN en se basant sur la qualité de chaque tunnel VPN	
<b>Routage avancée par application</b>	Routage intelligent des applications sur le meilleur lien ou tunnel VPN en se basant sur un algorithme multi-paramètres prenant en considération la latence, le délai, Jitter, packet Loss, bande passante dans le choix du meilleur lien par application	
<b>QoS</b>	Réservation et limitation de bande passante, priorisation du trafic et support de DSCP	
<b>Monitoring des liens et tunnel VPN</b>	Visibilité complète sur l'utilisation des liens ISP et tunnel VPN incluant : <ul style="list-style-type: none"> <li>- Consommation en temps réel de chaque lien (Upload et Download)</li> <li>- Consommation par application sur chaque lien ISP</li> <li>- Consommation par utilisateur sur chaque lien ISP</li> <li>- Delay, Jittel et Packet Loss de chaque tunnel vpn en temps réel</li> </ul>	
<b>Propriété client VPN</b>	<ul style="list-style-type: none"> <li>- Client VPN pour Microsoft Windows, Android, and Mac OS</li> <li>- Client security checks (OS, AV, FW)</li> <li>- VPN SSL Portal</li> </ul>	
<b>Administration Centralisé</b>		
<b>Type de la solution</b>	Software installable sous Windows ou linux sur serveur physique ou virtuel	
<b>Architecture</b>	Possibilité d'installer le serveur de management et le serveur log sur un seul serveur ou plusieurs pour une meilleur scalabilité	
<b>Capacité de traitement des logs</b>	Capacité illimitée de gestion des logs (selon capacité du serveur host)	
<b>Capacité de stockage des logs</b>	Capacité illimitée de stockage des logs (selon capacité du serveur host)	
<b>Surveillance du parc NGFW\IPS</b>	Monitoring de l'ensemble du parc NGFW\IPS sans limitation sur la version HW\SW et sans création de domaines	
<b>Surveillance d'équipement tiercé</b>	Possibilité de monitorer des solutions tiercé (serveur, routeur ...) via ICMP et SNMP et de traiter leurs logs	

<b>Interaction en log et policy</b>	<ul style="list-style-type: none"> <li>- Consultation des logs à partir d'une règle de sécurité</li> <li>- Création d'une règle de sécurité directement à partir des log</li> </ul>	
<b>Update et Upgrade</b>	<ul style="list-style-type: none"> <li>- Mise a jours des NGFW en cluster sans downtime et sans décomposer le cluster</li> <li>- Possibilité de planifier les updates et les upgrade</li> <li>- La solution doit offrir un mécanisme qui permet un downgrade automatique si un problème est rencontré lors d'un upgrade</li> </ul>	
<b>Gestion des Policy</b>	<ul style="list-style-type: none"> <li>- Sauvegarde automatique des Policy avant chaque application</li> <li>- Restauration intuitive d'une Policy si besoin</li> <li>- Outils de comparaison entre plusieurs versions d'une Policy</li> <li>- Outils de vérification de la base des règles de sécurité en identifiant les anomalies de configuration (ACL, NAT ...), les règles non nécessaires, les règles inaccessible ...</li> </ul>	
<b>Smart Policies</b>	<ul style="list-style-type: none"> <li>- Utilisation des Template pour hiérarchiser les Policy et simplifier leur lecture et gestion</li> <li>- Utilisation de variable (Alias) pour simplifier et réduire la taille des Policy, la valeur de l'alias change selon le NGFW</li> <li>- Utilisation de la notion de sous-Policy pour optimiser l'exécution des ACL et simplifier leurs lectures et gestion</li> </ul>	
<b>Intégration native avec ElasticSearch</b>	<p>La solution de gestion des logs doit offrir une intégration native avec le cluster ElasticSearch. L'administrateur aura le choix de stocker les logs localement ou sur un cluster ElasticSearch avec affichage et filtrage direct sur l'interface d'administration centralisé</p>	

<b>Support et Maintenance</b>		
<b>Type de support</b>	Constructeur	
<b>Durée du support</b>	3 ans	
<b>Audit préventif Annuel</b>	Le contrat de support doit inclure un audit préventif annuel effectué par le <b>Constructeur</b>	
<b>Support 24/24 et 7j/7</b>	Oui	

## 2- Firewalls Datacenter

<b>Caractéristiques minimales exigées</b>	<b>Critères éliminatoires</b>	<b>Spécifications techniques proposées</b>
Quantité	1 (un cluster de 2 Firewalls)	
<b>Identification</b>		
<b>Constructeur</b>	A spécifier – Doit être différente de celle du Firewalls Edge	
<b>Modèle</b>	A spécifier	
<b>Type de solution</b>	Appliance Hardware Dédié	
<b>Type de licence fournie</b>	Licences : <ul style="list-style-type: none"> <li>• IPS,</li> <li>• Application Control</li> <li>• Antimalware</li> </ul>	
<b>Certifications</b>	ICSA Labs et/ou Common Criteria Test Certificate et/OU équivalent...	
<b>Interfaces</b>		
<b>Nombre des interfaces 1GE</b>	16	
<b>Nombre des interfaces 10GE SFP+</b>	8	
<b>Nombre des interfaces GE SFP</b>	6	
<b>Nombre de modules 10GE SFP+ SR fournis et installés</b>	2	
<b>Nombre de modules 1GE SFP SX fournis et installés</b>	2	
<b>Nombre de Virtual Firewalls/Domaines / Contextes</b>	10	

<b>Performances</b>		
<b>Débit en clair</b>	30 Gbps	
<b>Nombre de sessions concurrentes</b>	2 Millions	
<b>Nombre de nouvelles connexions par seconde</b>	200 000	
<b>Débit Crypté (VPN IPSec)</b>	4 Gbps	
<b>Débit SSL VPN</b>	3 Gbps	
<b>Nombre des Tunnels VPN IPSec global (Client et Gateway)</b>	16 000	
<b>Fonctions de sécurité</b>		
<b>Technologie adoptée</b>	Stateful inspection	
<b>Haute Disponibilité ave Partage de charges</b>	Oui	
<b>Translation d'adresses (NAT) supportée : Par Source (statique et dynamique), Par Destination (@IP et port)</b>	Oui	
<b>Détection de Spoofing</b>	Oui	
<b>Les interfaces du firewalls supporte le vLAN Tagging 802.1q</b>	Oui	
<b>Fonctions UTM</b>		
<b>Throughput IPS</b>	8 Gbps	
<b>Throughput NGFW</b>	5 Gbps	
<b>Throughput application control</b>	5 Gbps	
<b>Reporting</b>		
<b>Génération de rapport d'accès</b>	Oui	
<b>Recherche et filtre dans les logs par source, destination, Protocol, VPN, date...</b>	Oui	
<b>Maintenance support et licences</b>	Tous les licences nécessaires (matériel, ticket support, licence) doivent être fournis pour le firewalls pendant 3 ans	

## V. Tableau de service

<b>Détails des prestations</b>		
<b>Prestation de services</b>	Installation et mise en service des firewalls	
	Configurations des firewalls	
<b>Documentation</b>	High Level Design	
	Low Level Design	
	Diagramme de réseau avec tous les détails des composants	
	Cahier de recette	
<b>Assistance Technique au démarrage de l'exploitation de la plateforme</b>	Un transfert de compétence d'une semaine pour trois personnes	

# Annexes

**ANNEXE 1**  
**IDENTIFICATION DU SOUMISSIONNAIRE**

Soumissionnaire	Valeur
Raison sociale	
Adresse	
Téléphone	
Fax	
E-mail	
Site web	
Directeur Général	
Nom de la personne à contacter	
Date de création	
Capital social	
Effectif 2024	

*Fait à ..... le .....*  
**Signature & cachet du soumissionnaire**

**ANNEXE 2**  
**MODELE DE SOUMISSION**

Je soussigné .....Président Directeur Général agissant au nom et pour le compte de la société .....Inscrite au registre de commerce sous le N° ..... Faisant élection de domicile à .....

Après avoir pris connaissance de toutes les pièces figurantes ou mentionnées au dossier de la consultation N° ..... lancé par la BMICE pour ..... je me sou mets et m'engage à exécuter le marché dans un délai de ....., conformément aux conditions du dossier de la consultation et moyennant le coût que j'ai établi comme suit :

**Montant total HT de l'offre (en chiffres et en lettres) .....**

Le règlement se fera par versement au compte ouvert au nom de ..... à la banque..... sous le N° .....

Les prix du marché sont fermes et non révisables.

Je m'engage, à maintenir valables les conditions de mon offre pendant un délai de Quarante cinq (45) jours à partir de la date limite fixée par la BMICE pour la remise des offres.

J'affirme sous peine de réalisation de plein droit du marché à mes torts exclusifs (ou aux torts exclusifs de la société pour laquelle j'interviens) que je ne tombe pas (ou que la société ne tombe pas) sous le coup d'interdictions légales édictées.

Fait à....., le .....

**A compléter par la mention manuscrite**

**« Lu et Approuvé par le soumissionnaire»**

**Signature(s) manuscrite(s) du soumissionnaire.**

**ANNEXE 3**

**Modèle de bordereau des prix**

Item	Désignation	Unité	Qté	Prix U. HT	Total HT
1	Firewalls Edge	Unité	2		
2	Firewalls Datacenter	Unité	2		
3	Installation et mise en place de la solution				
<b>Total HT.....</b>					

**Montant total HT de l'offre (en chiffres et en lettres) .....**

*Fait à ..... le .....*

**Signature & cachet du soumissionnaire**

**ANNEXE 4**  
**MODELE DECLARATION DE NON FAILLITE**

Je soussigné, (Nom, prénom et fonction) :..... Représentant de la Société, (Nom et adresse de la société) ..... Enregistrée au registre de commerce ..... Sous le n°..... en date du ..... Faisant élection de domicile à, (adresse complète) ..... déclare sur l'honneur de ne pas me trouver en état de faillite ou de liquidation judiciaire.

*Fait à ..... le .....*

**Signature & cachet du soumissionnaire**

## **ANNEXE 5**

### **MODELE DE DECLARATION SUR L'HONNEUR DE NON INFLUENCE**

Je soussigné – nous soussignés [nom(s) et prénoms(s) du ou des signataires]  
..... agissant en qualité de  
..... Représentant du bureau (nom et adresse) .....  
Enregistrée au ..... sous le N°..... Faisant élection de domicile à( adresse  
complète) ..... ci-après dénommé « le soumissionnaire » pour le marché portant sur  
l'étude pour la mise en place d'un nouveau data center à la snit, déclare sur l'honneur de n'avoir pas fait  
et m'engage de ne pas faire par moi-même ou par personne interposée, des promesses, des dons ou des  
présents en vue d'influencer sur les différentes procédures de conclusion du marché et des étapes de sa  
réalisation.

**Fait à ..... le .....**

**Signature & cachet du soumissionnaire**

**ANNEXE N° 6**  
**CAUTIONNEMENT PROVISOIRE**

Je soussigné-nous soussignés **(1)** .....  
Agissant en qualité de **(2)** .....  
**1/Certifie-Certifions que (3)** .....

A constitué entre les mains du Trésorier Général suivant récépissé N°.....en date du..... Le cautionnement fixe de ..... Dinars (..... Dinars) prévu par l'Article (113) de l'arrêté susvisé et que ce cautionnement n'a pas été restitué.

**2/Déclare me (ou déclarons-nous), porter caution personnelle et solidaire (4)** .....domicilié à **(5)** .....au titre du montant du Cautionnement Provisoire pour participer à **(6)** .....publié(e) en date du .....Par **(7)** .....et relatif relative à .....

Le montant du Cautionnement Provisoire s'élève à ..... Dinars (..... Dinars)

**3/M'engage – nous nous engageons solidairement, à effectuer le versement du montant garanti susvisé et dont le soumissionnaire serait débiteur au titre (6)** .....et ce, à la première demande écrite de l'acheteur public sans une mise en demeure ou une quelconque démarche administrative ou judiciaire Préalable.

Le présent cautionnement est valable pour une durée de **Quarante Cinq Jours (45) jours** à compter du lendemain de la date limite de réception des offres.

**Fait à ..... Le .....**  
**Signature et cachet du soumissionnaire**

(1) - Nom(s) et prénom(s) du (ou des) signataire(s).

(2) - Raison sociale et adresse de l'établissement garant.

(3) - Raison sociale de l'établissement garant.

(4) Nom du soumissionnaire (personne physique) ou raison sociale du soumissionnaire (personne morale).

(5) -Adresse du soumissionnaire.

(6) -Appel d'offres ou consultation.

(7) Acheteur public.

**ANNEXE N° 7**  
**MODÈLE D'ENGAGEMENT D'UNE CAUTION PERSONNELLE ET SOLIDAIRE**

(À produire au lieu et place de la retenue de garantie)

Je soussigné-nous soussignés **(1)** .....

Agissant en qualité de **(2)** .....

**1/Certifie-Certifions que (3)** .....

A constitué entre les mains du Trésorier Général suivant récépissé N°.....en date du ..... Le cautionnement fixe de ..... dinars (..... dinars) prévu par l'Article (113) de l'arrêté susvisé et que ce cautionnement n'a pas été restitué.

**2/Déclare me (ou déclarons-nous), porter caution personnelle et solidaire (4)** .....Domicilié à **(5)** .....au titre du montant de la Retenue de Garantie auquel ce dernier est assujéti en qualité de titulaire du marché N° ..... passé avec **(6)** .....publié(e) en date du .....Par **(7)** .....et relatif-relative à l'acquisition d'équipements informatique pour la BMICE avec des prix fermes et non révisables tel que prévu et spécifié par les documents de la consultation.

Le montant de la Retenu de Garantie s'élève à **Dix (10) %** du montant des acomptes à payer à titre du marché, ce qui correspond à ..... Dinars (en toutes lettres) Et à .....Dinars (en chiffres).

**3/M'engage-nous nous engageons solidairement, à effectuer le versement du montant garanti susvisé et dont le titulaire du marché serait débiteur au titre du marché susvisé, et ce, à la première demande écrite de l'administration sans que j'aie (nous ayons) la possibilité de différer le paiement ou soulever de contestation, pour quelque motif que ce soit et sans une lise en demeure ou une quelconque démarche administrative ou judiciaire préalable.**

**4/ La caution qui remplace la Retenu de Garantie devient caduque après que le titulaire du marché ait accompli toutes ses obligations, et ce à l'expiration du délai de quatre (04) mois après la réception définitive (8).**

Si le titulaire du marché a été avisé par l'acheteur public, avant l'expiration du délai susvisé, par lettre motivée et recommandée ou par tout autre moyen ayant date certaine, qu'il n'a pas honoré tous ces engagements, il est fait opposition à l'expiration de la caution, Dans ce cas la caution ne devient caduque que par main levée délivrée par l'acheteur public.

**Fait à ..... Le .....**

**Signature et cachet du soumissionnaire**

(1) -Nom(s) et prénom(s) du (ou des) signataire(s)

(2) - Raison sociale et adresse de l'établissement

(3) - Raison sociale de l'établissement

(4) - Nom du titulaire du marché

(5) - Adresse du titulaire du marché

(6) - Service qui a passé le marché

(7) - Indication des références d'enregistrement auprès de la recette des finances

(8) - Réception définitive ou de l'expiration du délai de garantie

**ANNEXE N° 8**  
**Caractéristiques Commerciales**

<b>Caractéristique</b>	<b>Référence minimale exigée</b>	<b>Valeur proposée</b>
Ancienneté de l'entreprise	Minimum 07 ans	
Références de vente et de Maintenance des firewalls proposés	Minimum 03 références Justificatifs à fournir (PV de réception définitive et/ou contrat)	
Autorisation de constructeur	Le soumissionnaire doit fournir une autorisation de constructeur pour la participation	
Certification du soumissionnaire	Certificat ISO 9001 Ver 2015	

**ANNEXE N° 9**

**COMPOSITION ET EXPERIENCE DE L'EQUIPE INTERVENANTE**

Caractéristique	Référence minimale exigée	Valeur proposée
<b>Nombre du personnel affecté au projet</b>	03	
<b>(01) Chef de projet</b>	<ul style="list-style-type: none"> <li>- Diplôme d'Ingénieur en informatique ou en télécommunications avec une expérience minimale de 10 ans.</li> <li>- Référence : Réalisation de Trois (03) Projets de mise en place de chaque type de firewalls proposé</li> <li>- Certifié sur les Firewalls proposés</li> </ul> <p><b>Il est obligatoire de fournir :</b></p> <ul style="list-style-type: none"> <li>- Copie du diplôme Certifié Conforme</li> <li>- CV signé par l'intéressé</li> <li>- Copie des certifications Certifiées Conformes</li> </ul>	
<b>(01) Ingénieur et (01) Techniciens</b>	<ul style="list-style-type: none"> <li>- Diplôme d'Ingénieur (Bac + 05) en informatique ou en télécommunications avec une expérience minimale de 3 ans.</li> <li>-Diplôme de technicien en informatique ou réseau télécom avec une expérience minimale de 3 ans.</li> <li>Certification :</li> <li>- Certifié au moins sur un des firewalls proposés</li> </ul> <p><b>Il est obligatoire de fournir :</b></p> <ul style="list-style-type: none"> <li>- Copie du diplôme</li> <li>- CV</li> <li>- Copie des certifications</li> </ul>	