BMICE | المصرف المغـــاربي للإستثمـــار و التجـــارة الخـــارجية
Banque Maghrébine d'Investissement et de Commerce Extérieur

Appel d'offre N°2/2025

Pour la Fourniture, l'Installation et le support d'Equipements de Sécurité Informatique

(Firewalls Edge, Firewalls Data Center, une Solution de gestion centralisée et une Solution centralisée d'analyse des logs)

La date limite de réception des offres est fixée au 26/09/2025 à 12h

Septembre 2025

A- Cahier des Clauses Administratives Particulières

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

Représentant l a 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 Articles de sécurité au profit de la Banque Maghrébine d'Investissement et de Commerce Extérieur **BMICE**, conformément aux dispositions du présent Appel d'offres.

Les articles à fournir sont :

- 2 Firewalls Edge
- 2 Firewalls Datacenter
- Une solution de gestion centralisée des Firewall
- Une solution centralisée d'analyse des logs

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 "articles" l'ensemble de matériels et logiciels à acquérir.

Ces dits articles 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 :

<< Pour la Fourniture, l'Installation et le support d'Equipements de Sécurité Informatique (Firewalls Edge, Firewalls Data Center, une Solution de gestion centralisée et une Solution centralisée d'analyse des logs) >>

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.

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

Important :

- 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 entraînera 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 relatif au matériel proposé .	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 valides pour chaque membre de l'équipe.
T.3	Présentation du service Support proposé sur 3 ans	Il est obligatoire que le soumissionnaire présente une description détaillée du service support proposé répondant aux attentes de la BMICE, assurant une disponibilité permanente, une réactivité immédiate en cas d'incident critique, ainsi qu'un accompagnement proactif pour garantir la continuité de service et la sécurité de nos équipements et solutions de management.

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 ou F2 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.

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 maitre 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 **26/09/2025 à 12h. (**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 Articles 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 Articles.

ARTICLE 14– LIVRAISON ET INSTALLATION DES ARTICLES ET PRESTATIONS

- **14.1** Le délai de livraison des Articles 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 Articles livrés en présence d'une équipe technique désignée par l'acheteur.
- **14.3** Les Articles 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 Articles 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 Articles livrés en présence d'une équipe technique désignée par la BMICE.
- **14.6** A l'issue de cette installation, les Articles 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 Articles doivent être réalisés obligatoirement sans perturber la bonne marche de la BMICE.
- **14.8** En cas de force majeur, 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), **il à noter qu'un test de basculement devra être réalisé et réussi sans impact avant la clôture du projet**.
- 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 ;

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 :
    - Fiches de configuration (Edge & Datacenter) + **Solutions** de management et Analyse des logs
    - Procédures de sauvegarde/restauration
    - Bonnes pratiques de sécurité et durcissement
- Un accompagnement post-installation de 5 jours ouvrés, incluant un support technique renforcé lors des premières semaines d'exploitation en production.

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 X 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 Articles seront effectuées de la manière suivante :

- **19.1- Réception provisoire :**

Une réception provisoire sera prononcée après :

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

2/ L'installation de tous les Articles.

3/ La configuration et les tests de mise en marche des Articles.

- **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% À la suite de la signature réception provisoire
- 40% À la suite de 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 à la suite de 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 constituants l'offre technique
- Le non-fourniture des pièces administratives après demande de l'acquéreur.
- Le non-fourniture des documents constituants 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 firewall existant et en mettant en place un cluster de Firewalls Data Center. En outre Deux solution de gestion devront être fournies (i) Une solution de gestion centralisée, et (ii) Une solution d'analyse des logs

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

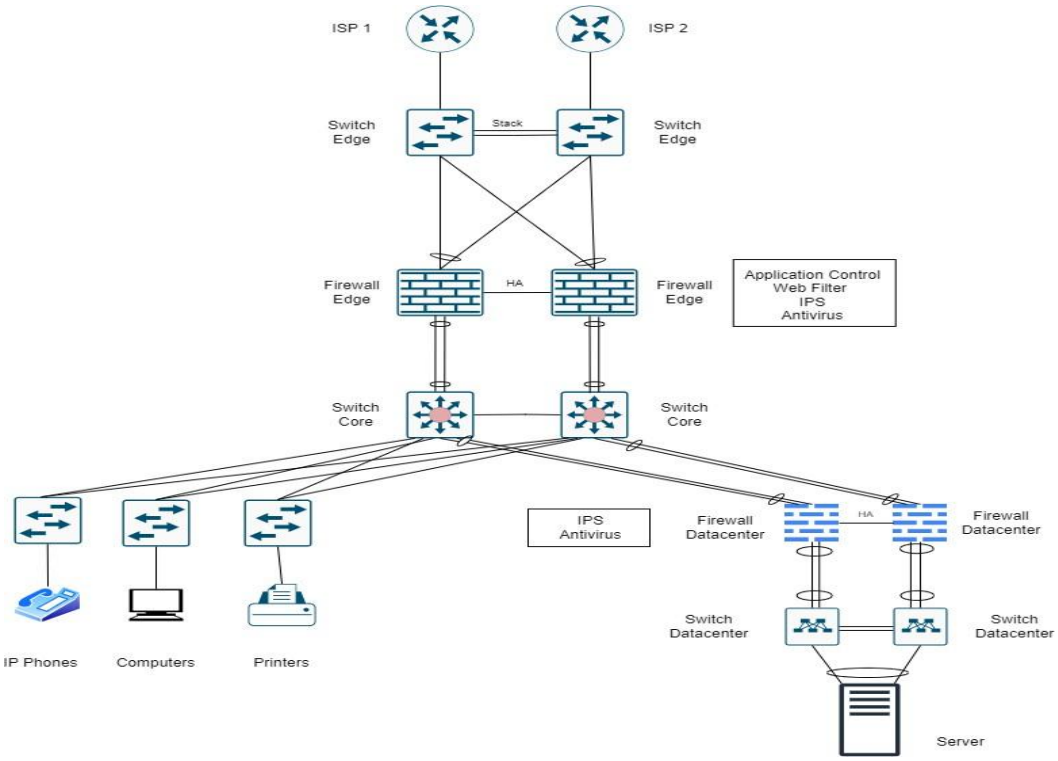

Figure 1: Architecture cible pour BMCIE

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	Spécification Techniques proposées
Quantité	1 (un cluster de 2 Firewalls)	

Identification		
Marque	**Doit être identique à celle des Firewalls Datacenter**	
Modèle	A spécifier	
Type de solution	NG Firewalls	
Firewalls stateful inspection	Oui	

Interfaces		
Nombre d'interfaces réseau physiques GE RJ45	16 x 1 Gbps Ethernet RJ45	
Nombre d'interfaces réseau physiques SFP	8 x 1Gbps Ethernet SFP	
Nombre d'interfaces réseau physiques SFP+	4 x 10 Gbps Ethernet SFP+	
Autres Interfaces	1 x Port USB 1 x Port Console	

Performances		
Débit en Clair	20 Gbps	
Nombre de connexions simultanées	3 millions	
Nombre de nouvelles connexions par seconde	140 000	
Débit IPSec VPN	30 Gbps	
Nombre de Tunnel SSL VPN	16 000	
Nombre des Tunnels VPN IPSec	2 000	
Throughput threat protection	2,8 Gbps	
Throughput IPS	5 Gbps	
Throughput NGFW	3 Gbps	
Contexte virtuel	Minimum 10	

Fonctions de sécurité		
Mode de déploiement	- L3 Firewalls	
	- L2\Transparent Firewalls	
	- IPS	
	- Combinaison des modes L2, L3 sur le même NGFW	
Protection contre les malwares et IPS	Oui, avec licence fournie	
Contrôle des applications et inspection de la couche 7	Oui, avec licence fournie	
Filtrage Web	Oui, avec licence fournie	

Inspection du flux		
Technique d'inspection	Stateful Inspection	
Inspection en mode routé	Oui	
Inspection en mode transparent	Oui	
Filtrage Web basé sur des catégories de sites	Oui (Avec mise à jour automatique et périodique)	
Prévention des attaque DoS basique	Oui	
Détection de Spoofing	Oui	
Des règles de filtrage niveau 2 par Interface physique ou virtuelle	Oui	
Des règles de filtrage niveau 3 par Interface physique ou virtuelle	Oui	
Des règles de filtrage par période de temps	Oui	
Identification des applications traversant le réseau quels que soient le port, le protocole, les techniques de	Oui	

contournement ou le chiffrement (TLS/SSL)		
Utilisation de l'application comme base de politique d'activation et d'autorisation sécurisées (autoriser, refuser, planifier, inspecter, prioriser le trafic, etc.)	Oui	

Identification\authentification des utilisateurs		
Authentification des utilisateurs	Authentification active des utilisateurs via browser ou client VPN	
Identification des utilisateur	Identification transparente des utilisateurs	
Annuaire Externe supporté	LDAP, Active Directory	
Protocole d'authentification	Radius	

High Availability		
Mode	Le cluster de NGFW doit supporter les modes de Clustering, Active-Active, Active-Passive	
Clustering	Oui	
Basculement avec maintien des sessions TCP/UDP	Oui	
Basculement avec maintien des sessions VPN	Oui	

Routage		
Routage statique IPv4 et IPv6	Oui	
policy-based routing	Oui	
static multicast routing	Oui	
Protocole de routage dynamique	OSPF, BGP	
Support Dynamic routing (OSPF, BGP)	En mode Actif\Actif et Actif\Standby	
NAT	Source NAT, Dest NAT, Port Forwarding	

Support et Maintenance		
Type de support	Constructeur	
Durée du support	3 ans	
Support 24/24 et 7j/7	Oui, durant toute la période de la garantie.	

Administration Centralisé		
Type de la solution	Software installable sous Windows ou linux sur serveur physique ou virtuel	

Architecture	Possibilité d'installer les solutions sur des VLAN différents (vlan mgt – Dmz…) pour une meilleure performance et scalabilité et sécurité.	
Surveillance du parc NGFW\IPS	Monitoring de l'ensemble du parc NGFW\IPS sans limitation sur la version HW\SW et sans création de domaines	
Interaction en log et policy	- Consultation des logs à partir d'une règle de sécurité - Création d'une règle de sécurité directement à partir des log	
Update et Upgrade	- Mise a jours des NGFW en cluster sans downtime et sans décomposer le cluster - Possibilité de planifier les updates et les upgrade en HNO (Heures non ouvrables) - La solution doit offrir un mécanisme qui permet un downgrade automatique si un problème est rencontré lors d'un upgrade	
Gestion des Policy	- Sauvegarde automatique des Policy avant chaque application - Restauration intuitive d'une Policy si besoin - Outils de comparaison entre plusieurs versions d'une Policy - 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 …	
Smart Policies	- Utilisation des Template pour hiérarchiser les Policy et simplifier leur lecture et gestion - Utilisation de variable (Alias) pour simplifier et réduire la taille des Policy, la valeur de l'alias change selon le NGFW	
Forward de logs	La solution doit être capable de transférer les logs vers des solutions tierces (exemple ElasticSearch, SIEM, …)	

2- Firewalls Datacenter

Caractéristiques minimales exigées	Critères éliminatoires	Spécifications techniques proposées
Quantité	1 (un cluster de 2 Firewalls)	

Identification		
Constructeur	A spécifier	
Modèle	A spécifier	
Type de solution	Appliance Hardware Dédié	
Type de licence fournie	Licences : • IPS • Application Control • Antimalware	
Certifications	ICSA Labs et/ou Common Criteria Test Certificate et/OU éuquivalent…	

Interfaces		
Nombre des interfaces 1GE RJ45	8	
Nombre des interfaces 10GE SFP+	8	
Nombre des interfaces GE SFP	4	
Nombre de modules 10GE SFP+ SR fournis et installés	2	
Nombre de modules 1GE SFP SX fournis et installés	2	
Autres Interfaces	USB Port Console Port	

Performances		
Débit en clair	25 Gbps	
Nombre de sessions concurrentes	11 Millions	
Nombre de nouvelles connexions par seconde	400 000	
Débit IPSec VPN	26 Gbps	
Débit SSL VPN	3 Gbps	
Nombre des Tunnels VPN IPSec	2000	
Throughput threat protection	6 Gbps	
Throughput IPS	9 Gbps	
Throughput NGFW	7 Gbps	
Nombre de Virtual Firewalls/Domaines / Contextes	10	

Inspection du flux		
Technologie adoptée	Stateful inspection	
Inspection en mode routé	Oui	
Inspection en mode transparent	Oui	
Haute Disponibilité avec Partage de charges	Oui	
Détection de Spoofing	Oui	
Les interfaces du firewalls supporte le vLAN Tagging 802.1q	Oui	
Des règles de filtrage niveau 2 par Interface physique ou virtuelle	Oui	
Des règles de filtrage niveau 3 par Interface physique ou virtuelle	Oui	
Des règles de filtrage par periode de temps	Oui	

High Availability		
Haute Disponibilité	Le cluster de NGFW doit supporter les modes de Clustering, Active-Active, Active-Passive	
Basculement avec maintien des sessions TCP/UDP	Oui	
Basculement avec maintien des sessions VPN	Oui	

Routage		
Routage statique IPv4 et IPv6	Oui	
policy-based routing	Oui	
static multicast routing	Oui	
Protocole de routage dynamique	OSPF, BGP	
Support Dynamic routing (OSPF, BGP)	En mode Actif\Actif et Actif\Standby	
NAT	Source NAT, Dest NAT, Port Forwarding	

Support et Maintenance		
Type de support	Constructeur	
Durée du support	3 ans	
Support 24/24 et 7j/7	Oui	

3- Solution de gestion centralisée

Solution d'administration centralisée		
Solution de gestion centralisée et de reporting	Oui, compatible avec les Cluster Firewalls Edge et Datacenter sans problème de compatibilité ni de synchronisation	
Type solution	Solution matérielle, logicielle ou Appliance virtuelle dédiée	
Politiques de sécurité	Déploiement centralisé : Application de politiques globales et locales (IPv4/IPv6)	
Gestion des configurations	Sauvegarde et versioning : Sauvegarde automatique, restauration et comparaison de configurations	
	Détection des écarts : Identification des différences entre configurations appliquées et standards définis	
Mises à jour	Gestion des firmwares : Déploiement et gestion centralisée des mises à jour logicielles	
Administration	Multi-utilisateurs Support multi-administrateurs avec rôles et permissions granulaires (RBAC)	
	Journalisation Historique complet des actions d'administration	
	Authentification Support LDAP, RADIUS, SAML, 2FA/FortiToken ou équivalent	
Sécurité et conformité	Traçabilité Audit complet des changements (qui, quoi, quand)	
	Normes Alignement avec ISO 27001, PCI-DSS, RGPD (selon contexte client)	
Capacité de traitement des logs	1 Go / jour (scalable selon les besoins futurs)	
Gestion centralisée des stratégies de sécurité et des objets	oui	
Suivi et visualisation en temps réel avec graphiques	Oui	
Support haute disponibilité et redondance (HA) – (en cas d'extension future.)	Oui	
Rétention et archivage des logs	Oui	

Support et Maintenance		
Type de support	Constructeur	
Durée du support	3 ans	
Support 24/24 et 7j/7	Oui	

4- Solution d'analyse centralisée des logs

Solution d'analyse centralisée des logs		
Administration et gestion centralisée des logs	Collecte, corrélation et gestion centralisée des logs de sécurité provenant des firewalls Edge et Datacenter, et autres Articles réseau compatibles.	
Type solution	Solution matérielle, logicielle ou Appliance virtuelle dédiée	
Capacité de traitement des logs	1 Go / jour (scalable selon les besoins futurs)	
Analyse et corrélation en temps réel	Oui	
Tableaux de bord et reporting avancé	Oui, avec graphiques Possibilité de générer des rapports programmés et personnalisés	
Détection d'anomalies et menaces	Oui, avec corrélation d'événements et alertes	
Exportation/Importation des logs vers un serveur Syslog	Support Syslog, CSV, PDF Possibilité d'intégration avec un outil SIEM	
Collecte des logs	**Sources supportées** Pare-feux, équipements réseau, endpoints, VPN, proxys et autres systèmes de sécurité **Volume** Capacité à gérer un minimum de 1Go de logs/jour **Protocoles** Support des protocoles standards (Syslog, SNMP, etc.)	
Support haute disponibilité et redondance (HA) – (en cas d'extension future.)	Oui	
Recherche et forensic	Oui, avec moteur de recherche avancé sur les logs	
Intégration avec la solution de gestion centralisée	Oui, pour une gestion unifiée sécurité + logs	

Support et Maintenance		
Type de support	Constructeur	
Durée du support	3 ans	
Support 24/24 et 7j/7	Oui	

V. Tableau de service

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

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 soumets 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	Solution de gestion centralisée	Unité	1		
4	Solution d'analyse centralisée des logs	Unité	1		
5	Installation et mise en place des articles	Unité	1		
6	Support sur 36 mois à payer annuellement (sur Trois ans	Unité	1		
	Total HT.....				

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 liquidationjudiciaire.

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] ... . agissantenqualitéde ..... Représentant du bureau (nom et adresse) ..... Enregistrée au ..... sous le N°..... Faisant élection de domicile à(adresse complète) ci-après dénommé«lesoumissionnaire»pourlemarchéportantsur
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 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 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 assujetti en qualité de titulaire du marché N° ..... passé avec **(6)** .....publié(e) en date du .....Par **(7)** .....et relatif-relative à l'acquisition d'Articles 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 publique, 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 8

Caractéristiques Commerciales

Caractéristique	Référence minimale exigée	Valeur proposée
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 9

COMPOSITION ET EXPERIENCE DE L'EQUIPE INTERVENANTE

Caractéristique	Référence minimale exigée	Valeur proposée
Nombre du personnel affecté au projet	03	
(01) Chef de projet	- Diplôme d'Ingénieur en informatique ou en télécommunications avec une expérience minimale de 10 ans. - Référence : Réalisation de Trois (03) Projets de mise en place des firewalls proposés - Certifié sur les Firewalls proposés **Il est obligatoire de fournir :** - **Copie du diplôme Certifié Conforme** - **CV signé par l'intéressé** - **Copie des certifications Certifiées Conformes**	
(01) Ingénieur et (01) Techniciens	- Diplôme d'Ingénieur (Bac + 05) en informatique ou en télécommunications avec une expérience minimale de 3 ans. - Diplôme de technicien en informatique ou réseau télécom avec une expérience minimale de 3 ans. Certification : - Certifié les firewalls proposés Il est obligatoire de fournir : - Copie du diplôme - CV - Copie des certifications	