Appel d'Offres N° 02/2024

Acquisition des Equipements de sécurité informatique

Pour la BMICE

A- Cahier des Clauses Administratives

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 LA CONSULTATION

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 de la présente consultation.

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 Appel d'Offres, seront installés dans les locaux de la Banque (Siège social à Tunis).

ARTICLE 2 : PIECES CONSTITUTIVES DE LA CONSULTATION

Les pièces constitutives du présent Appel d'Offres sont par ordre d'importance

- La soumission qui constitue l'acte d'engagement.
- Le bordereau des prix.
- Le présent Appel d'Offres lancée 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 de la consultation, 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 du présent 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 Du PRESENT *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	Le registre de commerce	Original ou copie certifiée conforme à l'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 de la consultation.		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 tunisien 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 réglementation en vigueur	Authentification légale
A.10	Certificat ISO 9001 Ver 2015		
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

Important :

- La nom 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/ou 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	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 - CV - Certifications

Important :

- La non-fourniture des justificatifs de T1 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 des documents F1 entraînera l'annulation de l'offre.
- La non-fourniture de F2 après relance entraînera l'annulation de l'offre.

ARTICLE 8 : CAUTIONNEMENT PROVISOIRE

Le montant du cautionnement provisoire est fixé à un montant forfaitaire de **Mille (1000 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 9 : 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 à **La BMICE** et à la première demande le montant de cette caution.

ARTICLE 10 - DÉLAIS DE VALIDITÉ DES OFFRES

Les offres doivent être valables pendant une durée minimale de 60 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 **La BMICE** 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 La BMICE ne le lui demande par écrit.

ARTICLE 11- DATE LIMITE DE RÉCEPTION DES OFFRES

La date limite de réception des offres est fixée au **18/11/2024 à 16H00** (Le cachet du bureau d'ordre de La Banque Maghrébine d'Investissement et de Commerce Extérieur **BMICE** faisant foi).

La BMICE 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 La BMICE sera automatiquement rejetée.

ARTICLE 12- OUVERTURE DES PLIS ET EVALUATION DES OFFRES

La commission des 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 des marchés vérifie la présence des documents administratifs et élimine les offres parvenues hors délais.

La commission des marchés désigne les membres de la commission d'évaluation des offres techniques et financières.

La Commission d'évaluation technique classifie les offres financières par ordre croissant, et évalue l'offre technique du soumissionnaire ayant présenté l'offre financière le moins disant. Elle annonce que l'offre de ce soumissionnaire est retenue une fois que son offre technique est conforme aux clauses techniques du cahier des charges. Sinon, la commission d'évaluation passe à l'évaluation de l'offre technique du soumissionnaire suivant.

Remarque :

Outre les clauses de ce cahier de charges, les décisions et procédures de la BMICE en matière de passation de marché ou d'acquisition de biens et services sont applicables.

ARTICLE 13- 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 14- 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 livraison des équipements.

ARTICLE 15– LIVRAISON ET INSTALLATION

Le délai de livraison des équipements et des logiciels ne doit pas dépasser **90 Jours** à partir du jour suivant la date de notification du marché.

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 **La BMICE**.

Les équipements non conformes seront refusés et le fournisseur doit les remplacer dans les **30 jours** qui suivent son information par lettre recommandée ou par notification par mail sur son adresse électronique indiqué dans son offre.

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'elle jugera nécessaire aux frais et risques du titulaire du marché défaillant.

ARTICLE 17- 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 18- RECEPTION

Les réceptions des équipements seront effectuées de la manière suivante :

18.1- Réception provisoire :

Une réception provisoire sera prononcée après :

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

2/ L'installation de tous les équipements.

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

18.2- 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 19- MODALITES DE PAIEMENT

- 50% Suite à la signature du PV de réception des équipements
- 40% Suite à la signature du PV de réception provisoire
- 10% Suite à la signature du PV 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 20: 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.
- La non-fourniture des pièces constituants l'offre technique
- La non-fourniture des pièces administratives après demande de l'acquéreur.
- La 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 la consultation 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 particulières CCTP sera éliminée.

ARTICLE 21 : PROCÉDURE DE PASSATION DU MARCHÉ

21.1 – 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.

21.2 – 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 La BMICE.

21.3 – 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.

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

ARTICLE 22 : 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 23- RESILIATION

En plus des dispositions de ce cahier des charges le marché peut être résilié par décision de La BMICE 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 La BMICE.

ARTICLE 24- 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 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.

Les principaux objectifs de cette migration sont les suivants :

- **Sécurité renforcée :** Les Firewall Edge protègent le réseau contre les menaces externes, tandis que les Firewall 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 Firewall, 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 Firewall 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

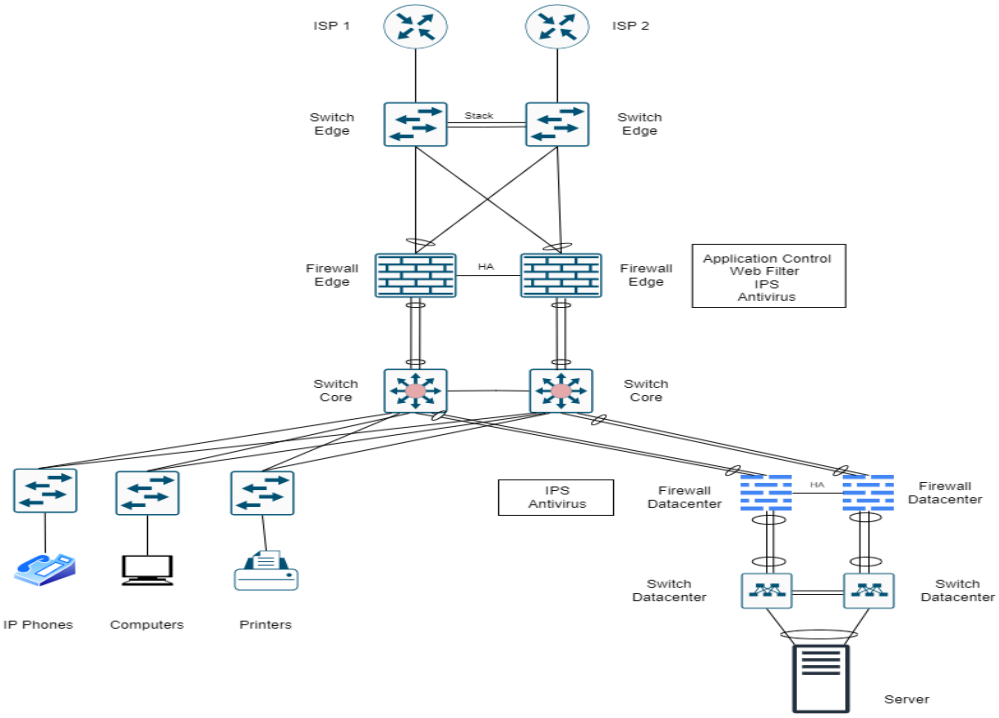

Figure 1: Architecture cible pour La BMICE

III. Exigence Fonctionnelles

1- Firewall Edge:

Les Firewalls Edge doivent être positionnés à la frontière externe du réseau de l'organisation 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 l'organisation, 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 – Firewall Edge

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

Débit en Clair	40 Gbps	
Débit NGFW\NGIPS	2 Gbps	
Débit IPSec	10 Gbps	
Nombre des Tunnels VPN IPSec	20 000	
Nombre de connexions simultanées	5 millions	
Nombre de nouvelles connexions par seconde	150 000	
Caractéristiques générales		
Securité		
Mode de déploiement	- L3 Firewall - L2\Transparent Firewall - IPS - Combinaison des modes L2, L3 sur le même NGFW	
Contrôle Applicatif	Oui (+6000 Applications prédéfinies)	
Filtrage URL basé sur les catégories	Oui (80 catégories au moins)	
Définition des règles de contrôle d'accès	Basé sur IP\User ID\ Application Source\ Version Windows\zone de sécurité	
Intrusion Prevention System	Oui (inclus dans la licence de base)	
Inspection du trafic TLS granulaire	Oui (inclus dans la licence de base)	
Protection Anti-Botnet	Oui (inclus dans la licence de base)	
Capture du trafic par interface (pcap)	Oui	
Protection contre les attaques DoS/DDoS	Oui	
Protection Antimalware \Antivirale	La solution doit fournir une protection sur plusieurs niveaux : - Protection par réputation de fichier - Protection par un moteur antimalware	
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	Tacacs+, radius	
High Availability		
Mode	Actif\Actif, Actif\Standby	

Nombre de node par cluster	Jusqu'à 10 nœuds en mode Actif\Actif	
Clustering	- Possibilité de mettre en cluster des FW de version OS différente - Possibilité de mettre en cluster des FW de gamme différente	
Server load balancing	Partage de charge sur les serveurs avec prise en charge du SNAT	
Lien internet	Partage de charge dynamique sur les liens ISP (5 au minimum)	
Routage		
Routage statique IPv4 et IPv6	Oui	
policy-based routing	Oui	
static multicast routing	Oui	
Protocole de routage dynamique	RIPv2, RIPng, OSPFv2, OSPFv3, BGP, PIM	
Support Dynamic routing (OSPF, BGP)	En mode Actif\Actif et Actif\Standby	
NAT	Source NAT, Dest NAT, Port Forwarding	
SD-WAN		
Type de VPN	- Policy Based VPN - Route based VPN	
Configuration	- 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	
Protocoles	IPSEC et TLS	
Topologies supportées	- 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	
Tunnel VPN	Création automatique des tunnels VPN sur tous les interfaces WAN disponible par un simple drag&drop	
Partage de charge sur les tunnels VPN	Utilisation d'un mécanisme dynamique pour le partage de charge entre tunnel VPN en se basant sur la qualité de chaque tunnel VPN	

Routage avancée par application	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	
QoS	Réservation et limitation de bande passante, priorisation du trafic et support de DSCP	
Monitoring des liens et tunnel VPN	Visibilité complète sur l'utilisation des liens ISP et tunnel VPN incluant : - Consommation en temps réel de chaque lien (Upload et Download) - Consommation par application sur chaque lien ISP - Consommation par utilisateur sur chaque lien ISP - Delay, Jittel et Packet Loss de chaque tunnel vpn en temps réel	
Propriété client VPN	- Client VPN pour Microsoft Windows, Android, and Mac OS - Client security checks (OS, AV, FW) - VPN SSL Portal	
Administration Centralisé		
Type de la solution	Software installable sous Windows ou linux sur serveur physique ou virtuel	
Architecture	Possibilité d'installer le serveur de management et le serveur log sur un seul serveur ou plusieurs pour une meilleur scalabilité	
Capacité de traitement des logs	Capacité illimitée de gestion des logs (selon capacité du serveur host)	
Capacité de stockage des logs	Capacité illimitée de stockage des logs (selon capacité du serveur host)	
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	
Surveillance d'équipement tiercé	Possibilité de monitorer des solutions tiercé (serveur, routeur …) via ICMP et SNMP et de traiter leurs logs	
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 - 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 - Utilisation de la notion de sous-Policy pour optimiser l'exécution des ACL et simplifier leurs lectures et gestion	
Intégration native avec ElasticSearch	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	
Support et Maintenance		
Type de support	Constructeur	
Durée du support	3 ans	
Audit préventif Annuel	Le contrat de support doit inclure un audit préventif annuel effectué par le **Constructeur**	
Support 24/24 et 7j/7	Oui	

2- Firewall Datacenter

Caractéristiques minimales exigées	Critères éliminatoires	Spécifications techniques proposées
Quantité	1 (un cluster de 2 Firewalls)	
Identification		
Constructeur	A spécifier – Doit être différente de celle du Firewall Edge	
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	
Interfaces		
Nombre des interfaces 1GE	16	
Nombre des interfaces 10GE SFP+	8	
Nombre des interfaces GE SFP	6	
Nombre de modules 10GE SFP+ SR fournis et installés	2	
Nombre de modules 1GE SFP SX fournis et installés	2	
Nombre de Virtual Firewalls/Domaines / Contextes	10	
Performances		
Débit en clair	70 Gbps	
Nombre de sessions concurrentes	7.5 millions	
Nombre de nouvelles connexions par seconde	500 000	
Débit Crypté (VPN IPSec)	50 Gbps	
Débit SSL VPN	3.5 Gbps	
Nombre des Tunnels VPN IPSec global (Client et Gateway)	50 000	
Fonctions de sécurité		

Technologie adoptée	Stateful inspection	
Haute Disponibilité ave Partage de charges	Oui	
Translation d'adresses (NAT) supportée : Par Source (statique et dynamique), Par Destination (@IP et port)	Oui	
Détection de Spoofing	Oui	
Les interfaces du firewall supporte le vLAN Tagging 802.1q	Oui	
Fonctions VPN		
Site-to-Site	Oui	
Client-to-Site	Oui	
Algorithme de Cryptage	DES/3DES/AES	
Méthode d'authentification	Pre-sharedkey/ Certificat	
Fonctions UTM		
Throughput IPS	12 Gbps	
Throughput NGFW	10 Gbps	
Throughput application control	20 Gbps	
Reporting		
Génération de rapport d'accès	Oui	
Recherche et filtre dans les logs par source, destination, Protocol, VPN, date...	Oui	
Maintenance support et licences	Tous les licences nécessaires (matériel, ticket support, licence) doivent être fournis pour le firewall pendants 3 ans	

V. Tableau de service

Détails des prestations		
Prestation de services	Installation et mise en service des firewalls	
	Configurations des firewalls	
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 de deux journées 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 de Tunis 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, en Tunisie.

Fait à Tunis, 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	Firewall Edge	Unité	2		
2	Firewall Datacenter	Unité	2		
3	Installation et mise en place de la solution				
	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 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)** ……

Agréé par le Ministre des Finances en application de l'Article (113) de la loi de l'arrêté n°1039 du 13 Mars 2014 portant réglementations des marchés publics **(3)** ……
A constitué entre les mains du Trésorier Général de Tunisie 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 été agréé par le Ministre des Finances en application de l'Article (113) de l'arrêté n°1039 du 13 mars 2014 portantes réglementations des marchés publics (3**) ……**
A constitué entre les mains du Trésorier Général de Tunisie 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'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/En application des dispositions de l'article (53) du Décret n°2002-3158 du 17 décembre 2002 portant réglementations des marchés publics tel que modifié et complété par les textes subséquents y compris le décret n°2011-623 du 23/05/2011, 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 N° 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 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
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 de chaque type de firewall proposé - Certifié sur les Firewalls proposés **Il est obligatoire de fournir :** **- Copie du diplôme** **- CV** **- Copie des certifications**	
(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 au moins sur un des firewalls proposés **Il est obligatoire de fournir :** **- Copie du diplôme** **- CV** **- Copie des certifications**	