BANQUE CENTRALE DE LA REPUBLIQUE DE GUINEE
(BCRG)

TERMES DE REFERENCE POUR LA FOURNITURE, LA CONFIGURATION ET LE DÉPLOIEMENT D'ÉQUIPEMENTS DE SÉCURITÉ FORTINET A LA BANQUE CENTRALE DE LA REPUBLIQUE DE GUINEE

MAI 2026

12, boulevard du Commerce, 6e avenue de la République C/Kaloum - BP 692 - Conakry - République de Guinée
Tél : (+224) 664 67 77 77 - Fax : (+224) 669 08 88 88 - mail : secretariat.gouv@bcrg-guinee.org
www.bcrg-guinee.org

1. Présentation de l'institution

La Banque Centrale de la République de Guinée (BCRG) est l'institution chargée de définir et de mettre en œuvre la politique monétaire nationale, d'assurer la stabilité du système financier et de superviser les établissements de crédit et les systèmes de paiement.
Dans le cadre de la modernisation continue de son système d'information et du renforcement de sa posture de cybersécurité, la BCRG engage un projet visant à moderniser son infrastructure de sécurité réseau afin de protéger les services bancaires critiques et les flux d'informations sensibles.

2. Contexte

La sécurité des infrastructures informatiques constitue un enjeu stratégique pour la BCRG compte tenu de la sensibilité des données manipulées et de la criticité des services bancaires fournis.
L'infrastructure actuelle repose notamment sur des équipements sécurité qui arrivent progressivement en fin de cycle de vie, ce qui entraîne :

- des limitations en termes de performance et de fonctionnalités de sécurité avancées ;
- des difficultés de maintenance et de support constructeur ;
- une complexité accrue dans la gestion et l'administration des équipements.

Par ailleurs, la multiplication des menaces informatiques et l'évolution constante des techniques d'attaque nécessitent l'adoption de solutions de sécurité modernes capables d'assurer :

- une inspection avancée du trafic réseau ;
- une protection renforcée des applications critiques ;
- une gestion centralisée des politiques de sécurité ;
- une haute disponibilité des infrastructures de sécurité.

Dans ce contexte, la BCRG souhaite moderniser son infrastructure de sécurité en déployant des équipements Fortinet de nouvelle génération et en renforçant la protection de ses applications web.

3. Objet du cahier des charges

Le présent cahier des charges a pour objet de définir les conditions techniques et administratives relatives à la sélection d'un prestataire chargé de :

- la fourniture d'équipements de sécurité FortiGate 120G ;
- la fourniture d'un système de gestion centralisée FortiManager 400G ;
- le renouvellement des licences de sécurité des équipements FortiWeb (400E et 100E) ;
- l'installation, la configuration et la mise en service de l'ensemble des équipements.

Le projet est structuré en un lot unique couvrant l'ensemble des prestations.

4. Objectifs du projet

Le projet vise à :

- Remplacer les équipements de sécurité arrivant en fin de vie par des FortiGate 120G ;
- Mettre en place une architecture haute disponibilité (HA) au siège (datacenter primaire et backup à chaud) ;
- Mettre en place une architecture haute disponibilité (HA) au site de secours à froid
- Sécuriser les connexions entre le siège et les agences régionales ;
- Déployer une solution de gestion centralisée via FortiManager ;

- Assurer la protection continue des applications web critiques via FortiWeb ;
- Maintenir la continuité de service durant la migration vers la nouvelle infrastructure.

5. Périmètre du projet

5.1 sites concernés

Le projet concerne les sites suivants :

- Siège de la BCRG (Datacenter primaire, salle backup à chaud)
- Site de Backup à froid (Kindia)
- Cinq (05) agences régionales
  - Boké ;
  - Mamou ;
  - Labé ;
  - Kankan ;
  - N'zérékoré.

5.2 Équipements concernés

N°	Équipement	Quantité	Site	Description
1	FortiGate 120G	2	Datacenter primaire – siège (Conakry)	FortiGate 120G Hardware + 3-Year Unified Threat Protection (UTP) Bundle with FortiCare Premium
2	FortiGate 120G	2	Salle de secours à chaud - siège (Conakry)	FortiGate 120G Hardware + 3-Year Unified Threat Protection (UTP) Bundle with FortiCare Premium
3	FortiGate 120G	2	Datacenter secondaire (Kindia)	FortiGate 120G Hardware + 3-Year Unified Threat Protection (UTP) Bundle with FortiCare Premium
4	FortiGate 120G	5	Boké, Labé, Mamou, Kankan et N'zérékoré	FortiGate 120G Hardware + 3-Year Unified Threat Protection (UTP) Bundle with FortiCare Premium
5	FortiManager 400G	1	Datacenter primaire – siège (Conakry)	FortiManager Hardware Appliance + 25-Device Management License with FortiCare Premium Support
6	FortiWeb 100E	1	Datacenter secondaire (Kindia)	FortiWeb 100E 1-Year Standard Security Bundle with FortiCare Support
7	FortiWeb 400E	1	Datacenter primaire – siège (Conakry)	FortiWeb-400E 1 Year Advanced Security Bundle with FortiCare Support

6. Spécifications techniques

6.1 FortiGate 120G

6.1.1 Performances minimales

Les équipements proposés devront respecter au minimum les caractéristiques suivantes :

- Débit Firewall ≥ 120 Gbps
- Débit IPS ≥ 5 Gbps
- Débit VPN SSL/IPsec ≥ 10 Gbps
- Sessions simultanées ≥ 20 millions

- Support multi-WAN et SD-WAN
- Interfaces réseau minimum 16 ports 10/25/40 Gbps

6.1.2 Fonctionnalités requises

Les équipements devront intégrer au minimum les fonctionnalités suivantes :

- Pare-feu nouvelle génération (NGFW)
- Système de prévention d'intrusion (IPS/IDS)
- Antivirus et anti-malware
- Filtrage web avancé
- Contrôle applicatif
- Inspection SSL/TLS
- VPN IPsec site-à-site (Siège – Agences)
- SSL VPN pour accès distant sécurisé
- Segmentation réseau (VLAN)
- Secure SD-WAN
- Haute disponibilité (Active / Passive)
- Journalisation centralisée
- Support des protocoles de routage (BGP, OSPF)
- Support NAT et VLAN

6.2 FortiManager 400G

6.2.1 Caractéristiques matérielles minimales

N°	Élément	Caractéristiques
1	Type d'équipement	Appliance de gestion centralisée
2	Format	Rackable 2U
3	Mémoire	>= 32 Go RAM
4	Capacité de stockage	Jusqu'à 32 To

6.2.2 Fonctionnalités

La solution devra permettre :

- la gestion centralisée de tous les FortiGate du siège et des agences ;
- la gestion centralisée des politiques de sécurité ;
- la mise à jour centralisée des firmwares ;
- la centralisation des journaux et événements ;
- la gestion des accès basée sur les rôles (RBAC) ;
- l'automatisation des déploiements (Zero Touch Provisioning) ;
- la gestion des sauvegardes et restaurations de configuration ;
- le support des architectures SD-WAN et Security Fabric ;
- le support des domaines administratifs (ADOM).

6.2.3 Interfaces réseau

- 4 ports Gigabit Ethernet RJ45
- 2 ports SFP
- 1 port console RJ45
- 2 ports USB pour maintenance et sauvegarde

6.3 Licences FortiWeb

Le prestataire devra assurer :

- le renouvellement des licences existantes pour une durée de 3 ans ;
- la mise à jour automatique des signatures de sécurité ;
- la protection contre les attaques web (OWASP Top 10, injection SQL, attaques XSS, DDoS applicatif) ;
- le maintien du support technique constructeur.

Un certificat officiel de renouvellement des licences devra être fourni.

7. Prestations attendues

Le prestataire devra assurer les prestations suivantes.

7.1 Installation et configuration

- installation physique des équipements ;
- raccordement réseau ;
- configuration initiale des équipements ;
- configuration des VLAN ;
- configuration des politiques de sécurité ;
- configuration des règles NAT ;
- configuration des VPN IPsec siège-agences ;
- mise en place de la haute disponibilité (HA) au siège ;
- intégration avec FortiManager ;
- activation et renouvellement des licences FortiWeb.

7.2 Migration des configurations des pares-feux existants vers FortiGate

Le prestataire devra :

- réaliser un audit complet des règles ASA existantes ;
- traduire et migrer les règles vers la plateforme FortiGate ;
- effectuer des tests fonctionnels avant mise en production ;
- valider la migration avec les équipes réseau et sécurité de la BCRG.

7.3 Tests et recette

Le prestataire devra effectuer :

- tests de connectivité réseau ;
- tests des tunnels VPN ;
- tests de filtrage de sécurité ;
- tests de haute disponibilité ;
- validation finale avant mise en production.

Un rapport de recette et de mise en production devra être fourni.

8. Transfert de compétences

Le prestataire devra assurer :

- le transfert de compétences pour l'exploitation quotidienne ;
- la remise d'une documentation technique complète.

9. Formation

Le soumissionnaire devra prévoir dans son offre l'inscription de deux (02) ingénieurs réseaux de la BCRG à une formation officielle Fortinet Certified Professional – Network Security (FCP). À cet effet, il devra proposer trois variantes de modalités de formation, à savoir :

- Une formation en présentiel dans les locaux de la BCRG, assurée par un formateur certifié ;
- Une formation en ligne (à distance), si cette modalité est disponible dans le programme officiel ;
- Une formation en présentiel dans un centre de formation agréé Fortinet.

Cette formation devra permettre aux ingénieurs concernés d'acquérir une autonomie complète dans l'exploitation, la configuration et l'administration de la solution Fortinet.

9. Livrables

Les livrables attendus comprennent :

- équipements fournis, installés et configurés ;
- architecture réseau mise à jour ;
- fichiers de configuration de chaque équipement ;
- documentation technique complète ;
- procédures de sauvegarde et restauration ;

- procédures d'exploitation ;
- rapport final de mise en production.

10. Maintenance et support

Le prestataire devra assurer :

- un support technique **24h/24 et 7j/7** ;
- une assistance pendant toute la durée de garantie ;
- un délai d'intervention critique inférieur ou égal à **4 heures** ;
- les mises à jour de sécurité ;
- un contrat de maintenance et support constructeur pour **une durée de 3 ans**.

11. Profil et qualification du prestataire

Le soumissionnaire devra présenter un profil technique et organisationnel solide, garantissant la réussite du projet de FOURNITURE, CONFIGURATION ET DÉPLOIEMENT D'ÉQUIPEMENTS DE SÉCURITÉ FORTINET de la Banque Centrale de la République de Guinée (BCRG).

11.1. Expérience et références

Le soumissionnaire devra :

- Justifier d'une expérience minimale de cinq (5) ans dans la conception et la mise en œuvre de projets similaires, notamment dans les domaines des réseaux LAN, Datacenter et sécurité informatique.
- Démontrer une expérience significative dans le déploiement et l'intégration de solutions Fortinet.
- Présenter des références vérifiables dans des projets multi-sites ou dans des environnements critiques.
- Fournir des attestations ou certificats de bonne exécution pour des projets comparables.
- Disposer idéalement de références dans le secteur bancaire, financier ou dans des institutions critiques, où la continuité de service est un enjeu majeur.

11.2. Certifications constructeurs

Le soumissionnaire devra disposer de certifications constructeurs valides démontrant sa capacité à intervenir sur les équipements concernés par le projet, notamment :

- Cisco : CCNP, CCIE ou équivalent ;
- Fortinet : NSE4, NS6, ou certification supérieure ;

Ces certifications devront être fournies sous forme de copies des certificats en cours de validité.

11.3. Compétences et composition de l'équipe projet

Le soumissionnaire devra mettre à disposition une équipe projet qualifiée, composée d'ingénieurs spécialisés en réseaux et en sécurité informatique.

L'équipe devra notamment inclure :

- Ingénieurs réseaux certifiés (CCNP, CCIE ou équivalent) ;
- Ingénieurs sécurité certifiés (Fortinet NSE4 ou supérieur, Palo Alto PCNSE ou équivalent) ;

La composition de l'équipe proposée devra être cohérente avec l'ampleur du projet, les livrables attendus et le planning de mise en œuvre.

11.4. Connaissance des environnements critiques et du secteur bancaire

Le soumissionnaire devra démontrer une bonne compréhension des exigences et contraintes propres aux environnements critiques, en particulier dans le secteur bancaire, notamment :

- les exigences de haute disponibilité et de continuité de service ;
- les impératifs de confidentialité, d'intégrité et de conformité réglementaire ;
- la gestion des risques liés aux infrastructures critiques.

12. Présentation des offres
Les offres doivent être rédigées en langue française en trois (3) exemplaires, dont un original et deux (2) copies, et doivent être présentées comme suit :

12.1. Une enveloppe A: Offre technique.

Elle comprendra un dossier administratif et un dossier technique.

Le dossier administratif est composé de :

- l'attestation d'immatriculation au Registre du Commerce et du Crédit Mobilier ;
- la copie du quitus fiscal ;
- la copie du quitus social ;
- ;
- la justification des pouvoirs accordés aux soumissionnaires au cas où il agit pour le compte d'une société ou d'un groupe d'entreprises.

Le dossier technique est composé :

- de l'offre technique conforme aux spécifications techniques des présents TDR;
- de l'expérience d'au moins trois (3) ans dans la fourniture, la configuration et le déploiement d'équipements de sécurité Fortinet;
- du délai de réalisation des prestations.

12.2. Une enveloppe B : Offre financière comprenant :
- les cadres de décomposition de prix présentés sous la forme d'un détail estimatif ;
- la référence bancaire et les modalités de paiement souhaitées.

12.3. Une enveloppe C : contenant un projet de contrat relatif au marché en version papier et sur clef USB.

Les trois (03) enveloppes seront insérées dans une (01) grande enveloppe portant les mentions suivantes :

[Offre pour la sélection d'un prestataire chargé de la fourniture, de la configuration et du déploiement d'équipements de sécurité Fortinet à la BCRG « - A n'ouvrir qu'en séance d'Ouverture de plis]

Et adressée à :

Monsieur le Directeur des Système d'Information de la Banque Centrale de la République de Guinée.

Boite Postale N° 692 Conakry, 12, Boulevard du Commerce C/Kaloum – République de Guinée.

Le dépôt électronique est possible. Il est adressé à : mory.kaba@bcrg-guinee.org, en veillant à utiliser un code de soumission et à respecter les exigences de confidentialité.

Dans le cas d'une soumission électronique, les prestataires devront transmettre les documents administratifs, l'offre technique et l'offre financière dans des fichiers distincts, clairement identifiés, l'offre financière devant être protégée un code différent de celui de l'offre technique.

Les prestataires devront s'assurer que leur offre est complète, conforme aux exigences du présent cahier des charges et transmise dans les délais impartis. Toute soumission incomplète, non conforme ou transmise hors délai sera rejetée.

13. Reception et validation des offres

La date limite de réception des offres à compter de la date de publication des présents TDR aux soumissionnaires est fixée à (45) quarante-cinq jours.

Toute offre parvenue après la date et l'heure limite indiquée ci-dessus sera considérée comme irrecevable.

Le soumissionnaire reste engagé par son offre pendant une durée de soixante (60) jours.

14. Ouverture des plis et évaluation des offres

L'ouverture des plis et l'examen des offres sont effectués par une Commission de la Banque Centrale mandatée à cet effet, conformément aux procédures budgétaires de la Banque Centrale.

La séance d'ouverture des plis est publique. Celle-ci aura lieu en présence des soumissionnaires ou de leurs représentants.

La grille de notation qui sera appliquée pour évaluer les offres est la suivante:

14.1. Offre technique

N°	Offres techniques	Notes **70**	Scores	Observations
1	**Dossier administratif** a. RCCM b. Quittus fiscal c. Quittus social	**5** 1 2 2		
2	**Capacités techniques** *a.* Conformité technique : *Respect des spécifications techniques - Capacité à assurer haute disponibilité et continuité de service)* *b.* Expérience du prestataire : - *Réalisations antérieures dans le secteur bancaire ou institutions critiques.* - *Références vérifiables (projets similaires).* *- Certifications constructeurs (Cisco, Fortinet).* c. Qualifications des ingénieurs : *Compétences de l'équipe (NSE4, CCNP, etc.).*	**65** 5 20 20		

	d. Méthodologie : - *Clarté et exhaustivité de la méthodologie (audit, design, migration, tests, documentation, transfert de compétences).* *-Gestion des risques et plan de continuité.* *e.* Support et garantie : *SLA, assistance et service après-vente.* *f.* Planning d'éxecution : *-La durée estimée du projet est de 8 à 10 semaines ; -le planning doit inclure la fourniture des équipements ; l'installation et la configuration initiale ; la migration des configurations ; la phase de test et la mise en production.*	10 5 5		

14.2. Offre Financière : 30
Total :100

L'offre financière devra distinguer clairement :

- coût des équipements ;
- coût des licences ;
- coût des prestations de déploiement ;
- coût du support et maintenance.

Seules les offres techniques des soumissionnaires qui auront un score minimum de 60/70 points seront retenues pour l'évaluation financière.

Le présent marché sera attribué au soumissionnaire ayant proposé l'offre économiquement la plus avantageuse.

15. Confidentialité

En recevant les présents Termes de référence (TDR), le soumissionnaire s'engage à ce que les informations écrites ou orales communiquées par la Banque Centrale de la République de Guinée (BCRG):

- soient protégées, gardées strictement confidentielles et soient traitées avec les plus extrêmes précautions et protections ;
- ne soient utilisées qu'aux seules fins de déterminer les possibilités de coopération entre les parties ;
- ne soient divulguées, ni susceptibles d'être divulguées, soit directement ou indirectement à tous tiers ou à toutes personnes pas expressément désignées par la Banque Centrale de la République de Guinée.

LA BANQUE CENTRALE