SOCIETE REDAL

APPEL D'OFFRE N°103/2020/C

Acquisition Et Mise En Œuvre De Solutions Informatiques

CAHIER DES PRESCRIPTIONS SPECIALES

(CPS)

PIECE N° 3

SOMMAIRE

1. OBJECTIF DE L'APPEL D'OFFRES

REDAL vise à travers le présent appel d'offres d'acquérir et mettre en œuvre des solutions informatiques lui permettant d'améliorer le niveau de sécurité et de disponibilité de ses plateformes informatiques.

Cet appel d'offres est fractionné en 3 lots à savoir :

- **Lot 1 :** Acquisition et intégration du module de corrélation des logs de sécurité au niveau de la solution existante.
- **Lot 2 :** Acquisition et mise en œuvre d'une solution de haute disponibilité pour le WAF existant
- **Lot 3 :** Acquisition d'une solution de gestion des accès distants et d'une solution PAM

NB : Chaque concurrent peut soumissionner pour un lot ou plusieurs lots.

2. EXIGENCES GENERALES DES SOLUTIONS CIBLES

Dans le cadre de cet appel d'offres, le(s) soumissionnaire (s) devra fournir tous les prérequis nécessaires pour la mise en œuvre optimale et complète des solutions cibles (Hardware, software et licences). Les solutions proposées par le(s) soumissionnaire(s) doivent pouvoir répondre aux exigences suivantes :

- **Compatibilité** : Le prestataire doit justifier dans son offre technique la compatibilité de sa solution avec l'infrastructure existante au niveau des Datacenter de REDAL.

- **Fiabilité :** Les solutions proposées doivent offrir un niveau de résilience et de robustesse très élevé garantissant la fiabilité globale des systèmes mis en place.

- **Performance :** Toute la configuration proposée doit être optimale et évolutive permettant d'assurer un niveau maximal de performance.

- **La Sécurité :** Les solutions proposées doivent disposer d'un très haut niveau de sécurité et de mécanismes de protection avancés.

- **Facilité d'administration**: Toutes les briques des solutions proposées doivent être dotées d'un outil d'administration et de gestion à base d'interface utilisateur simple à utiliser.

- **Évolutivité et flexibilité :** Les solutions proposées doivent être évolutive en termes de capacité et de performance.

- **Impact sur les systèmes de production :** La mise en place des solutions proposées ne doivent pas impacter le niveau de performance et de disponibilité des systèmes de production de la REDAL.

La solution proposée pour répondre aux spécifications techniques décrites dans ce cahier des charges doit être fournie sous sa dernière version disponible au moment de la livraison, ainsi que toutes les licences garantissant le bon fonctionnement de la solution objet de cet appel d'offres.

3. CONSISTANCE DES PRESTATIONS

Les solutions attendues doivent être installées et mises en œuvre par le(s) soumissionnaire(s) à travers des prestations de haute qualité permettant de tirer le maximum des solutions proposées et un transfert de compétences aux équipes informatiques de la REDAL.

L'implémentation des différentes composantes des plateformes proposées devra être assurée par des équipes certifiées par les éditeurs sur les solutions proposées.

Toutes les opérations d'installations et configurations doivent être incluses dans le prix du marché.

Les opérations doivent comprendre ce qui suit :

- Le soumissionnaire est invité à effectuer une visite des lieux de chaque site, pour :

  Apprécier à juste valeur l'architecture technique des plateformes en exploitation et devant fonctionner en interaction avec les solutions techniques à mettre en place dans le cadre du présent appel d'offres et évaluer la consistance de la mission à réaliser.

  Une attestation de visite des lieux dûment signée est à fournir obligatoirement au dépôt de la soumission ;
- Le soumissionnaire doit fournir une attestation d'engagement signée par le constructeur, indiquant l'aptitude du soumissionnaire à livrer, installer et mettre en service les produits fournis ;
- Le soumissionnaire devra prévoir une présentation de son offre technique dans les locaux de la REDAL avant le jugement technique des offres ;
- Détermination d'architecture, prérequis nécessaire et plan de mise en œuvre de toutes les briques de la mise en œuvre de(s) solution(s) cible selon les besoins de REDAL et en tenant compte de l'existant et l'avancement des projets en cours.
- Lors de la phase d'installation : installer, paramétrer et configurer la solution selon l'architecture validée par l'équipe projet de REDAL.
- Le titulaire s'engage à assurer la mise en œuvre des fonctionnalités attendues de la solution cible en tenant compte du site d'hébergement des infrastructures (deux sites au total). Il doit également prendre à sa charge tout autre outil jugé nécessaire inclue l'installation, la configuration pour garantir le bon fonctionnement de la solution proposée.
- Assistance pendant après la mise en production en vue d'ajuster la configuration pour une utilisation optimale.
- Implication forte de l'équipe Projet de la REDAL tout au long de la durée de mise en œuvre, afin d'assurer un transfert de compétences et une maîtrise totale des technologies de l'infrastructure à mettre en place.
- Fournir et développer les procédures nécessaires pour sauvegarder et restaurer les environnements.
- Fournir un document de recette avec les procédures de test de bon fonctionnement par solution et par lot.

4. LOT 1 : Acquisition et intégration du module de corrélation des logs de sécurité au niveau de la solution existante

4.1 Objectif

Pour accompagner l'évolution de son système d'information et faire face aux risques pesant sur la sécurité de ses systèmes, REDAL souhaite acquérir et mettre en œuvre un système de corrélation des logs pour analyser en temps réel les événements de sécurité centralisés au niveau du loggeur existant.

4.2 Description de l'existant

REDAL dispose d'une plateforme de centralisation des logs de sécurité basée sur la solution ci-dessous

- Nom de la solution : ArcSight de Micro Focus
- Module Actif : Logger
- Version : 6.7.0.8242.0
- Capacité sous licence : 600 EPS

4.3 Description du module à acquérir

Le module de corrélation des logs à fournir dans le cadre de ce lot doit permettre à la REDAL de:

- Corréler en temps réel les événements de sécurité en s'appuyant sur le flux des logs centralisés au niveau du logger,
- Mettre en place de règles de corrélation permettant d'alerter sur un incident en cours et permettant d'identifier les causes d'un événement a posteriori.
- Détecter des attaques (simples et complexes) en maintenant une surveillance continue du SI (tentative d'exfiltration de données, communication avec un serveur, etc.).
- Contrôler la conformité à des contraintes réglementaires et la politique de sécurité en détectant des anomalies ou des non-conformités.
- Répondre aux incidents et permettre des analyses de type forensics (investigation numérique) exploitant au maximum les traces (logs) récoltées.
- Détecter les comportements anormaux d'utilisateurs, des serveurs, des applicatifs et du réseau.
- Élaborer des tableaux de bord de sécurité opérationnelle à destination des responsables techniques moyennant la définition, en amont, d'indicateurs à suivre et l'envoi de rapports programmés.
- Rejouer les anciens événements pour mener des enquêtes post-incident.
- Supporter la corrélation des logs de tous les équipements utilisés au niveau de REDAL
- Le module de corrélation proposé doit supporter les types de corrélation suivante : Rule-Based Correlation, Vulnerability Based Correlation,Statistical Based, Historical Based, Heuristic Based.
- Générer des tableaux de bord selon le profil utilisateur
- Le module de corrélation devra permettre d'initier automatiquement un Workflow qui permettra d'ouvrir et d'attribuer des tickets sur une solution externe tout en conservant une piste d'audit complète pour le processus de traitement de l'incident.
- Le module à fournir doit être en mesure de suivre l'activité des utilisateurs et lier un individu à une action. Les analystes doivent être en mesure de générer des rapports détaillant les ressources auxquelles un utilisateur pour une période de temps définie.
- La solution doit être capable de situer une adresse IP sur carte (pays, ville, etc).
- Le Dashboard doit afficher le statut de la solution (CPU, Disque, processus, etc).
- La solution doit permettre de créer des vues pour chaque utilisateur selon les équipements qui lui sont attribués
- Traiter de manière évolutive de tout cas d'utilisation de SIEM auquel REDAL pourrait être confrontée, quelle que soit sa complexité.

Dimensionnement

La solution doit supporter au minumum 300 EPS et devra être extensible en fonction des besoins futurs de REDAL.

NB : Le soumissionnaire doit détailler dans son offre le mode de licensing proposé

Architecture globale de la solution cible

- Le module de corrélation des logs doit être mis en œuvre sur une architecture hautement sécurisée. A ce titre le prestataire est tenu de préciser dans son offre l'architecture est les prérequis techniques nécessaires à la mise en œuvre dudit module.

- La solution doit être exécutée sur un OS et base de données sécurisée. La configuration du stockage doit offrir une configuration RAID 0,1,5 et 10 en cas de proposition de solution sous forme de boitier.

- La solution devra disposer d'une console de management centralisée permettant de gérer et visualiser l'état des différentes composante de l'architecture cible (existante et à acquérir)

- Pour des raisons d'homogénéité, le module à acquérir doit être du même éditeur que le loggeur existant

4.4 Attestations

- Attestation Éditeur engageant le support éditeur/constructeur dans le processus de la mise en place de la solution proposée,
- Le prestataire doit fournir une attestation de support éditeur de **1 année**.

4.5 Présentation de l'offre

Présentation générale de l'offre

L'offre technique doit inclure obligatoirement les informations ci-dessous :

- La description détaillée des solutions techniques proposées ainsi que les éléments d'appréciation de ces solutions. Il y a lieu notamment de fournir :
  - Les schémas d'architecture technique à mettre en place au niveau de la REDAL.
  - La description des moyens prévus pour assurer la haute disponibilité de la solution.
  - La description de toutes les fonctionnalités de la solution proposée.
  - La description détaillée fonctionnelle et technique des procédures et stratégies à mettre en œuvre.
  - La description de l'évolutivité de la solution proposée
  - La description de la méthodologie et organisation de la mise en œuvre du projet
  - La description de l'intégration avec l'existant
  - La description des livrables du projet
  - Les CVs de l'équipe projet
  - Les pré-requis et recommandations hardware et software d'installation de la solution

- Un planning détaillé de réalisation du projet : Livraison des licences, Installation, Paramétrage et configuration, Intégration avec les plateformes existante, Elaboration des procédures et Mise en œuvre des solutions proposées, Formation et Transfert de compétences ;
- Un support éditeur de minimum **1 année** doit être fourni avec les licences ;
- La politique de tarification sur une période de 5 ans comprenant en détail un engagement sur le coût des add-on des toutes les composantes logicielles proposées : liste à fournir ;
- Une proposition de contrat de maintenance conforme au niveau de service décrit dans le présent Lot du CPS ;
- Le tableau de conformité technique dûment complété tel que décrit ci-dessous renseignant ainsi sur la conformité totale, partielle, ou la non-conformité de l'offre par rapport aux exigences demandées dans le cadre du présent Lot du CPS.

Tableau de conformité

Chaque soumissionnaire à ce lot est tenu de remplir le tableau de conformité ci-après. Ce tableau représente ce même cahier des charges mis sous format de tableau où la première colonne représente les clauses et les spécifications de ce cahier des charges et les deux autres colonnes sont réservées au soumissionnaire pour apporter ses remarques ou ses réponses en termes de conformité ou non-conformité.

Exigence CPT	**CONFORMITE** (T: Totale, P: partielle, N : Non conforme)	**OBSERVATION** (Si applicable)
L'offre technique contient la description détaillée des solutions techniques proposées		
Les schémas d'architecture technique à mettre en place		

Les spécifications techniques de chaque plateforme technique et de chaque variante logicielle proposée au niveau de la plateforme.		
Le planning détaillé de réalisation du projet :		
mise en œuvre des solutions proposées, formation et transfert de compétences		
L'offre contient tous les équipements qui ne seraient pas mentionnés dans le bordereau des spécifications techniques et qui seraient nécessaires au bon fonctionnement du logiciel livré et/ou à intégrer ainsi qu'à la mise en œuvre de la solution ciblée		
Présentation détaillée des moyens du soumissionnaire : -Moyens humains et logistiques -Attestations de prestations similaires -Certificats et/ou attestations de partenariat délivré par les éditeurs/constructeurs		
La solution proposée permet de :		
Corréler en temps réel les événements de sécurité en s'appuyant sur le flux des logs centralisé au niveau du logger,		
Mettre en place de règles de corrélation permettant d'alerter sur un incident en cours et permettant d'identifier les causes d'un événement a posteriori.		
Détecter des attaques (simples et complexes) en maintenant une surveillance continue du SI (tentative d'exfiltration de données, communication avec un serveur, etc.).		
Contrôler la conformité à des contraintes réglementaires et la politique de sécurité en détectant des anomalies ou des non-conformités.		
Répondre aux incidents et permettre des analyses de type forensics (investigation numérique) exploitant au maximum les traces (logs) récoltées.		
Détecter les comportements anormaux d'utilisateurs, des serveurs, des applicatifs et du réseau.		
Élaborer des tableaux de bord de sécurité opérationnelle à destination des responsables techniques moyennant la définition, en amont, d'indicateurs à suivre et l'envoi de rapport programmé.		2
Rejouer les anciens événements pour mener des enquêtes post-incident.		
Supporter la corrélation des logs de tous les équipements utilisés au niveau de REDAL		
La solution supporte au minimum ***300*** EPS extensible en fonction des besoins futurs de REDAL.		Préciser le nombre d'EPS proposée
Le module de corrélation proposé doit supporter les types de corrélation suivante : Rule-Based Correlation , Vulnerability Based Correlation,Statistical Based, Historical Based, Heuristic Based.		
Générer des tableaux de bord selon le profil utilisateur		

Le module de corrélation devra permettre d'initier automatiquement un Workflow qui permettra d'ouvrir et d'attribuer des tickes sur une solution externe tout en conservant une piste d'audit complète pour le processus de traitement de l'incident.		
Le module à fournir doit être en mesure de suivre l'activité des utilisateurs et lier un individu à une action. Les analystes doivent être en mesure de générer des rapports détaillant les ressources auxquelles un utilisateur pour une période de temps définie.		
La solution doit être capable de situer une adresse IP sur carte (pays, ville, etc).		
Le Dashboard doit afficher le statut de la solution (CPU, Disque, processus, etc).		
La solution doit permettre de créer des vues pour chaque utilisateur selon les équipements qui lui sont attribués xTraiter de manière évolutive de tout cas d'utilisation de SIEM auquel REDAL pourrait être confrontée, quelle que soit sa complexité		
L'offre inclut toutes les licences nécessaires à l'activation de toutes les fonctionnalités exigées sur le présent cahier des charges		
L'offre inclut **1 année** de support éditeur avec possibilité d'extension.		
L'offre inclut toutes les prestations de mise en œuvre du module de corrélation		
La mise en œuvre de l'ensemble de la solution sera achevée sur une période maximale de **3 mois** à compter de la date d'adjudication du marché.		

5. LOT 2 : Acquisition et mise en œuvre d'une solution de haute disponibilité pour le WAF existant

5.1 Objectif

L'objectif du présent Appel d'offres est la fourniture, l'installation et le paramétrage d'un WAF (Web Application Firewall) pour assurer le partage de charge et la haute disponibilité du WAF existant à la REDAL.

Les prestations d'installation et de paramétrage de la solution devront être réalisées conformément aux règles de l'art.

5.2 Description de l'existant

Informations pouvant être fournies lors de la visite des lieux

5.3 Description De La Solution Cible

Le prestataire devra fournir :

- Une solution WAF hardware de la technologie F5 Networks de la gamme i2600
- Les licences d'upgrade pour les modules Advanced WAF pour le WAF existant et pour le nouveau boitier.

- Licences nécessaires pour la gestion de partage de charge sur la plateforme WAF cible ainsi que les licences IP intelligence

➢ **SUPPORT**

- Le support doit être d'un minimum de 3 ans
- Le support devra être proposé de base en 5 jours sur 7 et 8h-18h.
- Le support doit être délivré en Français si disponible sinon en Anglais y compris pour le support constructeur / éditeur.

5.4 Attestations

- Attestation Éditeur engageant le support éditeur/constructeur dans le processus de la mise en place de la solution proposée,
- Le prestataire doit fournir une attestation de support et garantie constructeur des équipements proposés dans ce projet,

5.5 Présentation de l'offre

Présentation générale de l'offre

L'offre technique doit inclure obligatoirement les informations ci-dessous :

- La description détaillée des solutions techniques proposées ainsi que les éléments d'appréciation de ces solutions. Il y a lieu notamment de fournir :
    - Les schémas d'architecture technique à mettre en place au niveau de chaque site de la REDAL.
    - La description des moyens prévus pour assurer la haute disponibilité de la solution.
    - La description de toutes les fonctionnalités de la solution proposée.
    - La description détaillée fonctionnelle et technique des procédures et stratégies à mettre en œuvre.
    - La description de l'évolutivité de la solution proposée
    - La description de la méthodologie et organisation de la mise en œuvre du projet
    - La description de l'intégration avec l'existant
    - La description des livrables du projet
    - Les Cvs de l'équipe projet
    - Les pré-requis et recommandations hardware et software d'installation de la solution
- Un planning détaillé de réalisation du projet : Livraison des licences, Installation, Paramétrage et configuration, Intégration avec les plateformes existante, Elaboration des procédures et Mise en œuvre des solutions proposées, Formation et Transfert de compétences ;
- Un support éditeur de minimum **(03)** ans doit être fourni avec les licences ;
- La politique de tarification sur une période de 5 ans comprenant en détail un engagement sur le coût des add-on des toutes les composantes logicielles proposées : liste à fournir ;
- Une proposition de contrat de maintenance conforme au niveau de service décrit dans le présent Lot du CPS ;
- Le tableau de conformité technique dûment complété tel que décrit ci-dessous renseignant ainsi sur la conformité totale, partielle, ou la non-conformité de l'offre par rapport aux exigences demandées dans le cadre du présent Lot du CPS.

➢ **Tableau de conformité**

Chaque soumissionnaire est tenu de remplir le tableau de conformité ci-après. Ce tableau représente ce même cahier des charges mis sous format de tableau où la première colonne représente les clauses et les spécifications de ce cahier des charges et les deux autres colonnes sont réservées au soumissionnaire pour apporter ses remarques ou ses réponses en termes de conformité ou non-conformité.

Caractéristique	CONFORMITE (T : Totale P : Partielle N : Non conforme)	Commentaire
L'offre technique contient la description détaillée des solutions techniques proposées		
Les schémas d'architecture technique à mettre en place		
Le planning détaillé de réalisation du projet :		
L'offre inclut les prestations de mise en œuvre des solutions proposées, la formation et transfert de compétences		
L'offre contient tous les équipements qui ne seraient pas mentionnés dans le bordereau des spécifications techniques et qui seraient nécessaires au bon fonctionnement du logiciel livré et/ou à intégrer ainsi qu'à la mise en œuvre de la solution ciblée		
Présentation détaillée des moyens du soumissionnaire : -Moyens humains et logistiques -Attestations de prestations similaires -Certificats et/ou attestations de partenariat délivré par les éditeurs/constructeurs		
Spécifications et dimensionnement de la plateforme		
Marque	A préciser	
La solution doit être sous forme physique (Appliance)		
Quantité	1	
Leader ou challenger durant les 2 dernières années dans le rapport Magic Quadrant pour Web Application Firewalls		
La solution doit avoir la certification ICSA WAF		
RAM : 16 GB		
Disque dur : 500 GB		
Alimentation : Redondante		
Dimension : Boitier Rackable		
OS : 64 bits		
Type de Licence : Pas de restriction par application		
Ports 1G : 4 ports 1G RJ45		
Ports Fibre 10 G : 2 emplacements		
Débit : 10Gb/S		
Nombre minimal de Requêtes niveau 7 par seconde : 350.000		
Nombre minimal de Connections niveau 4 par seconde : 120.000		

Nombre minimal de Requêtes http par Seconde : 550.000		
Nombre minimal de Connections concurrentes : 13.000.000		
Débit minimal du trafic chiffré : 5Gb/s		
Nombre minimal de Transactions par seconde : 2500, Clé de chiffrement de 2K		
Débit minimal du trafic compressé : 2,5 Gb/s		
Capable de gérer le trafic IPv4 et IPv6.		
Fonctionnalités de protection		
Protection contre les attaques Top10 OWASP		
Protection contre le mécanisme d'évasion		
La solution doit supporter un langage de scripting pour acheminer, réacheminer, rediriger, inspecter, modifier, retarder, rejeter ou rejeter, consigner ou toute autre action que n'est pas configurable via la GUI		
Protection Antivirale via ICAP		
Protection contre le DoS et DDoS applicatif comme (HASH DoS, Slowloris, floods, Keep dead, XML bomb, …)		
Protection contre les attaques automatisées et détection de botNET		
Blocage par zone géographique		
Utilisation du moteur d'apprentissage automatique		
Support de l'approche sécurité positive et/ou négative dans une règle de sécurité.		
Fournir des templates ou assistant de configuration pour les applications standards (Oracle, Microsoft OWA, …)		
Protection FTP et SMTP		
Conformité des schémas XML		
Validation de l'utilisation des méthodes SOAP		
Protection des Parsers XML		
Vérification de motifs d'attaques dans les messages XML		
Utilisation d'un résultat d'un outil d'audit de vulnérabilité		
La solution devrait soutenir la fonctionnalité multi-tenancy, c-à-d avoir plusieurs capacités de routage: il devrait soutenir l'affectation des applications Web protégées à conteneurs de réseau virtuel avec des tables de routage indépendants et ACLS réseau.		
Les politiques de sécurité doivent tenir compte de : • Extension des pages • URLs : • Paramètres de l'application • Session and Logins • Header • IP Adresses • Attack Signatures • Gestion XML, Jason, Google Web Toolkit (GWT) et les jeux de caractères		

• Contenu des pages • Gestion du Cross Site Request Forgery • Géolocalisation		
La solution doit permettre la mise à jour de la base de signature d'une manière automatique et manuelle		
Chiffrement à la volée des informations sur les formulaires web		
Fournir des techniques de détection de robot web avancées comme : détection d'activité suspecte clavier et Souris, surf rapide ou séquences irrégulières d'évènements, …		
Fournir une protection avancée par cookie		
Détection et prévention du Web Scraping		
La solution doit disposer de mécanisme de corrélation basé sur la source, la destination, le type d'attaque qui permet de regrouper les événements sous forme d'incidents.		
La solution doit fournir un service cloud permettant le fonctionnement du WAF avec Microsoft Azure and Amazon AWS afin de protéger des applications héberger en Cloud.		
La solution devrait intégrer en option les technologies de navigateur blindés pour empêcher Man-In-TheBrowser (MITB) attaques et d'étendre la couverture de sécurité à la fin de client.		
La solution doit permettre de terminer les sessions SSL/TLS, afin d'augmenter les performances d'accélération SSL et d'inspecter les données pour effectuer une décision au niveau de l'application		
La solution doit intégrer un ASIC ou carte ou processeur dédié pour l'accélération SSL/TLS et les chiffrements symétriques et asymétriques afin d'éviter l'utilisation de ressources CPU et RAM et dans ce cas ne pas impacter les performances de répartition de charge		
La solution doit avoir un mécanisme qui permet de réduire le nombre de connexions TCP gérées par les serveurs Web afin de libérer les ressources physiques (notamment la consommation CPU des serveurs WEB).		
L'offre inclut la licence Advanced WAF pour toute la plateforme cible		
L'offre inclut les prérequis de fonctionnement en haute disponibilité de l'architecture cible		
La solution doit être en mesure de compresser les flux HTTP et les flux HTTPS. Les protocoles de compression doivent être des protocoles standards et utilisés par la majorité des navigateurs		
La solution doit offrir la possibilité de mise en cache des		

objets HTTP qui permettra de réduire de manière importante le nombre de requêtes sur les serveurs http		
La solution doit offrir des mécanismes avancés de cashing		
Il faut avoir la possibilité de configurer la solution pour loguer, en temps réel, toutes les requêtes et/ou réponses qui traversent l'équipement		
La solution doit offrir des options avancées de debugging et de prise de traces tels que : • Liste l'état des interfaces physiques • Liste les connexions actives • « tcpdump » pour capture de traffic • « ssldump » pour capture de traffic SSL • « curl », « telnet », « netcat », « dig », etc. tests de service Web, TCP ou UDP • Un mécanisme de port mirroring pour les interfaces.		
Les équipements doivent avoir la possibilité de stocker trois versions de configuration et d'OS dans la mémoire		
L'offre inclut les licences IP intelligence		
L'offre inclut tous les prérequis et les prestations de mise en œuvre de l'architecture demandée notamment, la mise en œuvre de la haute disponibilité, du partage de charge , l'intégration et l'activation des fonctionnalités Advanced WAF		
L'offre inclut **<u>03 ans</u>** de support constructeur pour l'ensemble des composantes de la plateforme		
Evolutivité de la plateforme		
La solution doit être évolutive en performance sans changement de boitier (augmentation du nombre de requête et connexion par seconde)		
Pour besoins futurs, la solution doit supporter sans changement de boitier des fonctionnalités avancée de protection et optimisation des applications WEB : • Fonctionnalités anti-fraud **(**Détection de Malware**,** Chiffrement au niveau applicatif, …) • Fonctionnalités de Load Balancing des applications entre serveur et entre Datacenter • Solution Anti DDos • Solution de sécurité d'accès • Solution de pour fournir le service DNS et sécurité DNS		
Délai de mise en œuvre du projet		
La mise en œuvre de la solution devra être achevée sur une période maximale de 3 mois à compter de la date d'adjudication du marché.		

6. LOT 3 : Acquisition et mise en œuvre d'une solution de PAM et de gestion des accès à distance.

6.1 Objectif

L'objectif de ce lot est la fourniture et l'installation d'une solution de sécurité permettant à REDAL de maitriser les risques liés aux accès à ses SI, il s'agit des types d'accès suivants:

- **Accès à distance :** la solution cible doit permettre d'éviter les risques liés à l'utilisation des comptes VPN, elle doit permettre une granularité dans la gestion des accès en décidant d'ouvrir certaines applications à certaines utilisateurs et elle doit permettre également de vérifier / valider la conformité des postes de travail avant de lui autoriser l'accès à un SI internes tout en permettant la génération de mots de passe à usage unique (OTP).

- **Accès à hauts privilèges :** la solution cible doit permettre la traçabilité et le contrôle des comptes à hauts privilèges permettant ainsi aux administrateurs techniques de connaitre en temps réel les activités opérés sur les différents équipements. La solution cible doit disposer d'une fonctionnalité coffre-fort pour mieux protéger les mots de passe des comptes

La solution cible doit permettre une intégration facile avec l'infrastructure existante.

6.2 Consistance Des Prestations

Le soumissionnaire aura à sa charge la réalisation de tous les travaux spécifiés dans ce cahier des charges. Il doit assurer une prestation de qualité et veiller au respect des règles de l'art en termes d'ingénierie et de mise en place en termes de performance, fiabilité et sécurité.

Les prestations de services doivent inclure, notamment :

- ✓ Etude et analyse de l'existant
- ✓ Définition de l'architecture détaillée de déploiement
- ✓ Ingénierie de mise en œuvre
- ✓ Plan de déploiement
- ✓ Plan de retour en arrière
- ✓ Tests et Recette
- ✓ Déploiement et mise en production

- La formation sur l'administration de la solution

La prestation doit prévoir au minimum la fourniture des livrables suivants :

- Dossier d'ingénierie
- Dossier d'installation
- Dossier d'exploitation

6.3 Description De La Solution Cible

Architecture cible :

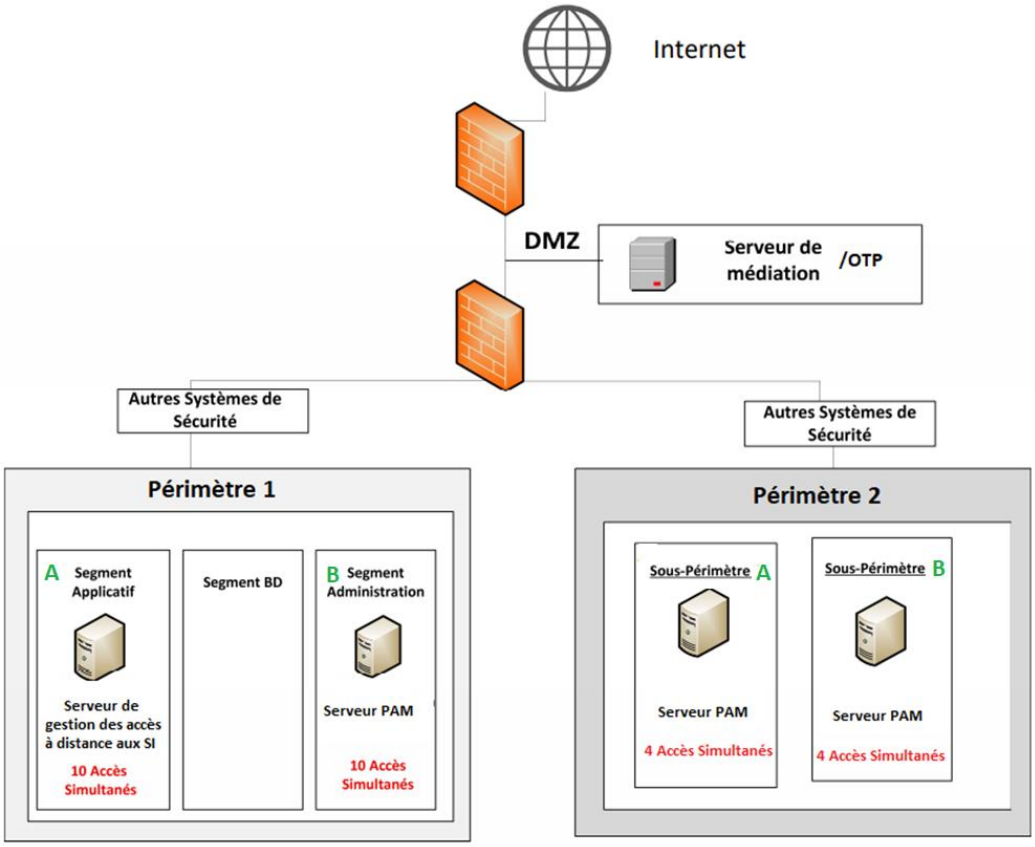
- La solution cible doit permettre la gestion des comptes à hauts privilèges de trois sous-périmètres physiquement séparés et doit tenir compte du besoin de réduction de la surface d'attaque.

- La gestion des accès à distance doit gérer les accès aux SI d'un seul périmètre. Le soumissionnaire peut proposer une ou deux solutions pour couvrir la totalité du besoin fonctionnel exprimé dans ce lot (Gestion des accès à distance et Gestion des accès à hauts privilèges)

- L'architecture proposée doit être basée sur une architecture hautement disponible et à double barrières.

Dimensionnement

Le schéma ci-dessous est fourni à titre d'ébauche pour illustrer le besoin de séparation des briques de l'infrastructure. Ce schéma illustre également le dimensionnement de la solution cible en nombre d'accès simultanés.



Le soumissionnaire peut proposer une offre de licence en mode utilisateur nommé. Le nombre de licence minimum à prévoir pour ce mode est équivalent à :

- 50 utilisateurs nommés pour la solution de gestion d'accès à distance (périmètre 1-A)
- 20 Utilisateurs nommés PAM périmètre 1-B
- 08 Utilisateurs nommés PAM périmètre 2-A
- 08 Utilisateurs nommés PAM périmètre 2-B

Spécifications techniques

- **Gestion des comptes à hauts privilèges**

La Gestion des comptes à hauts privilèges devra :

a. Se baser sur des boitiers physiques / Appliances virtuels
b. Etre dimensionnée pour gérer sans latence et sans impact sur les performances **des** sessions simultanées.
c. Etre dimensionnée pour assurer une rétention de **12** mois. La solution devra aussi permettre d'exporter les différents enregistrements, et d'étendre le stockage sur un support externe.
d. Il est préférable que la solution ne soit pas limitée en nombre d'équipements gérés. Toutefois le soumissionnaire peut proposer des licences pour la gestion de 200 équipements

La solution doit être évolutive en termes de nombre d'équipements supervisés et doit disposer des fonctionnalités suivantes :

- Etre parmi les meilleures solutions sur le marché
- Certifié par un organisme tels que l'ANSSI
- Fonctionner en mode agentless (sans agent) et supporter les modes de déploiement en mode transparent, en mode routeur ou en mode proxy explicite.
- Assurer la traçabilité des protocoles SSH, X11, Telnet et TN3270, RDP, VNC, Citrix ICA, HTTP/HTTPS et afficher l'ensemble des connexions actives par protocole.
- Permettre la traçabilité et le contrôle des transferts de fichiers utilisant les différents protocoles, notamment sur RDP, SCP et SFTP.
- Gérer les protocoles RDP 5, 6 et 7 ainsi que le mode Terminal Server Gateway ou Remote Desktop Gateway
- Permettre de surveiller l'écran, le flux clavier ou la souris d'un poste de travail, quel que soit les réglages des couleurs, la résolution, le protocole du réseau ou du système d'exploitation utilisé
- Permettre à un administrateur de superviser et surveiller en temps réel les sessions établies des utilisateurs, et d'y mettre fin si nécessaire
- Sauvegarder les différents logs en local des actions réalisées par les intervenants, notamment en réalisant un enregistrement vidéo de toutes les sessions dans un format sécurisé, non altérable et juridiquement acceptable.
- Exporter une session en format de capture de paquets (PCAP).
- Enregistrer toutes les actions faites sur la console d'administration, sans possibilité de modification.

- Permettre de stocker en interne et de manière sécurisée les éventuels authentifiants utilisés pour l'accès aux serveurs et machines distantes, et permettre aux utilisateurs de se connecter aux systèmes cibles sans connaissance des authentifiants utilisés.
- Permettre de consulter intuitivement les enregistrements vidéo des activités des utilisateurs, à travers un lecteur ou un outil qui permet :
    - De sélectionner directement les événements relatifs aux cliques de la souris ou de la saisie de certaines touches du clavier, ou l'ouverture de certaines fenêtres.
    - D'accélérer les vidéos
    - De prendre des captures de certaines manipulations effectuées lors d'une session.
- Sécuriser la consultation des enregistrements par un utilisateur par une autorisation supplémentaire ou une authentification spécifique
- Permettre de rechercher rapidement toutes les entrées de texte réalisées par les utilisateurs sur les protocoles en mode texte mais aussi les protocoles en mode graphique et ce sur différentes traces en même temps.
- Déconnecter automatiquement un utilisateur, générer des alertes sous formes de traps SNMP ou de messages syslog, et d'envoyer des emails lors :
    - De la saisie ou de l'affichage d'un texte prédéfini et configurable,
    - Du lancement d'une application spécifique
    - De la détection des numéros de cartes de crédit basée sur l'algorithme de Luhn.
- Permettre une notification par email ou par traps SNMP sur un certain nombre d'indicateurs comme des événements liés au trafic (Connexion refusée, Violation du protocole, identification de l'utilisateur a échoué …) et aux erreurs systèmes.
- Intégrer un système de workflow pour autoriser l'accès d'administration à des machines identifiées
- Fournir des tableaux de bord qui représentent un monitoring du système (CPU, RAM et Disque) et sur les différents protocoles supportés (HTTP, RDP, SSH, ICA, VNC et Telnet)
- Disposer de fonction de redémarrage, d'arrêt du système et de ses services depuis l'interface graphique pour limiter l'accès en mode console.
- Fournir depuis l'interface graphique des outils :
    - De Troubleshooting sur l'ensemble des protocoles supportés
    - D'exécution des commandes d'analyse réseau (exemple : Ping, Traceroute)
    - D'affichage des fichiers des fichiers journaux et des logs des protocoles (SSH, VNC et RDP, HTTP)
- Permettre la génération de rapports personnalisables, et des rapports de conformité.
- Générer des rapports manuellement ou automatiquement selon une fréquence journalière, hebdomadaire ou mensuelle avec possibilité de les envoyer par email, au format pdf.
- Effectuer des sauvegardes et des restaurations de la configuration du ou des données qui peuvent être utilisées en cas d'incidents.
- Permettre la remontée d'événements vers le SIEM existant (Format ArcSight CEF) en syslog
- Consommer en moyenne 1 Mo par minute pour les sessions graphiques et 1 Mo par heure pour les sessions texte.

➢ **Coffre-fort des Mots de Passe & Gestion des Mots de Passe**

- Les mots de passe doivent être inscrits sur une appliance matérielle renforcée.

- La base de données de mots de passe doit utiliser au moins 3 modules cryptographiques certifiés par le Programme de validation d'algorithmes cryptographiques (CAVP) pour sa fonctionnalité de cryptage.
- Le processus de demande de mot de passe doit s'appliquer uniquement aux mots de passe uniques.
- Les demandes de mot de passe doivent être rendues possibles en utilisant une infrastructure minimale. Pas plus d'une appliance doit être requise pour que la solution de mise en coffre-fort des mots de passe soit pleinement fonctionnelle pour les demandes d'accès des utilisateurs privilégiés et la gestion des mots de passe des systèmes cibles.
- La solution PAM doit pouvoir stocker les mots de passe pour ses propres comptes d'administration interne et les rendre disponibles à l'aide d'un modèle de demande/ de libération vérifiable et sans limitation.
- Les critères de gestion des mots de passe doivent être configurables pour répondre à la politique organisationnelle de la fréquence de changement des mots de passe/ le contrôle de l'approbation d'utilisation/ les changements après utilisation.
- Le prestataire est tenu de fournir une matrice de la capacité des solutions à gérer les fonctions de gestion des comptes privilégiés pour différents types d'appareils: par exemple, les comptes privilégiés de base de données, les comptes de dispositifs réseau, les comptes privilégiés des systèmes d'exploitation et les fonctionnalités disponibles pour chaque type de dispositif.

➢ **La gestion des accès à distance :**

La gestion des accès à distance devra permettre de :

- Définir finement les accès aux applications (web ou client-serveur) ou des ressources (serveurs ou partages de fichier) en fonction de l'utilisateur et de ses conditions de connexion, que les applications et ressources soient dans un ou plusieurs datacenters,

- Prendre en compte une grande variété de scénarios d'accès, depuis des postes maitrisés, ou des postes non maitrisés (BYOD, BYOPC, prestataires tiers).

- Disposer d'un portail d'accès centralisant toutes les ressources et applications mises à disposition d'un utilisateur.

- Les ressources et applications sont accessibles à travers le portail web, avec ou sans agent sur le poste pour répondre également aux enjeux de BYOD ou de postes non maîtrisés.

- Baser sur une architecture à double barrières

- Permettre une grande précision sur les ouvertures d'accès spécifiques sur les applications au lieu d'ouvrir des accès larges à des réseaux.

- Baser sur architecture offrant des accès multisites, permettant d'accéder depuis un portail unique à des applications et des ressources réparties sur plusieurs Datacenter, on-premise et dans le cloud

- Permettre la définition de profils d'accès

- Permettre une authentification, renforcée par des mécanismes d'OTP (One Time Password)

- Permettre le contrôle de conformité du poste pouvant vérifier l'identité et la santé du terminal d'accès ainsi que des critères d'accès comme le lieu ou l'heure de connexion.

- Certifier CSPN par l'ANSSI et éprouver par le Gartner

Le soumissionnaire devra établir un tableau de conformité reprenant les éléments ci-dessus et spécifier la conformité ou non de la solution qu'il propose par rapport à chaque ligne et proposer en plus une explication de certains éléments supplémentaires offerts par sa solution. Les solutions ne remplissant pas au minimum les exigences ci-dessus seront considérées comme non conformes.

Le prestataire devra livrer une solution clé en main et devra réaliser toutes les opérations nécessaires à sa mise en production, à l'exception des opérations à réaliser sur l'infrastructure de REDAL, que le prestataire devra détailler dans son offre technique.

Le soumissionnaire est tenu de préciser dans son offre la politique de licences, de maintenance et de support techniques des logiciels/appliances proposés.

6.4 Présentation de l'offre

Présentation générale de l'offre

L'offre technique doit inclure obligatoirement les informations ci-dessous :

- La description détaillée des solutions techniques proposées ainsi que les éléments d'appréciation de ces solutions. Il y a lieu notamment de fournir :
    - Les schémas d'architecture technique à mettre en place au niveau de chaque site de la REDAL.
    - La description des moyens prévus pour assurer la haute disponibilité de la solution.
    - La description de toutes les fonctionnalités de la solution proposée.
    - La description détaillée fonctionnelle et technique des procédures et stratégies à mettre en œuvre.
    - La description de l'évolutivité de la solution proposée
    - La description de la méthodologie et organisation de la mise en œuvre du projet
    - La description de l'intégration avec l'existant
    - La description des livrables du projet
    - Les Cvs de l'équipe projet
    - Les pré-requis et recommandations hardware et software d'installation de la solution

- Un planning détaillé de réalisation du projet : Livraison des licences, Installation, Paramétrage et configuration, Intégration avec les plateformes existante, Elaboration des procédures et Mise en œuvre des solutions proposées, Formation et Transfert de compétences ;
- Un support éditeur de minimum **(03)** ans doit être fourni avec les licences ;
- La politique de tarification sur une période de 5 ans comprenant en détail un engagement sur le coût des add-on des toutes les composantes logicielles proposées : liste à fournir ;
- Une proposition de contrat de maintenance conforme au niveau de service décrit dans le présent Lot du CPS ;

- Le tableau de conformité technique dûment complété tel que décrit ci-dessous renseignant ainsi sur la conformité totale, partielle, ou la non-conformité de l'offre par rapport aux exigences demandées dans le cadre du présent Lot du CPS.

Tableau De Conformité

Exigence CPT	**CONFORMITE** (T: Totale, P: partielle, N : Non conforme)	**OBSERVATION** (Si applicable)
L'offre technique contient la description détaillée des solutions techniques proposées		
Les schémas d'architecture technique à mettre en place		
Les spécifications techniques de chaque plateforme technique et de chaque variante logicielle proposée au niveau de la plateforme.		
Le planning détaillé de réalisation du projet :		
mise en œuvre des solutions proposées, formation et transfert de compétences		
L'offre contient tous les équipements qui ne seraient pas mentionnés dans le bordereau des spécifications techniques et qui seraient nécessaires au bon fonctionnement du logiciel livré et/ou à intégrer ainsi qu'à la mise en œuvre de la solution ciblée		
Présentation détaillée des moyens du soumissionnaire : -Moyens humains et logistiques -Attestations de prestations similaires -Certificats et/ou attestations de partenariat délivré par les éditeurs/constructeurs		
Gérer les comptes à hauts privilèges :		
Architecture et dimensionnement		
Solution basée sur des boitiers physiques / Appliances virtuels		Préciser le type proposé
Dimensionnée pour gérer sans latence et sans impact les performances des sessions simultanées.		
Dimensionnée pour assurer une rétention de **12** mois informations de traçabilité.		
La solution permet d'exporter les différents enregistrements, et d'étendre le stockage sur un support externe.		
Couverture fonctionnelle		
La solution est évolutive en termes de licence notamment en nombre d'équipements		

La solution est Certifieés CSPN par l'ANSSI et éprouvée par le Gartner		
La solution peut Fonctionner en mode agentless (sans agent) et supporte les modes de déploiement en mode transparent, en mode routeur ou en mode proxy explicite.		
La solution assure la traçabilité des protocoles SSH, X11, Telnet et TN3270, RDP, VNC, Citrix ICA, HTTP/HTTPS et afficher l'ensemble des connexions actives par protocole.		
La solution permet la traçabilité et le contrôle des transferts de fichiers utilisant les différents protocoles, notamment sur RDP, SCP et SFTP.		
La solution permet de gérer les protocoles RDP 5, 6 et 7 ainsi que le mode Terminal Server Gateway ou Remote Desktop Gateway		
La solution permet de surveiller l'écran, le flux clavier ou la souris d'un poste de travail, quel que soit les réglages des couleurs, la résolution, le protocole du réseau ou du système d'exploitation utilisé		
La solution permet à un administrateur de superviser et surveiller en temps réel les sessions établies des utilisateurs, et d'y mettre fin si nécessaire La solution permet de sauvegarder les différents logs en local des actions réalisées par les intervenants, notamment en réalisant - un enregistrement vidéo de toutes les sessions dans un format sécurisé, non altérable et juridiquement acceptable. - Exporter une session en format de capture de paquets (PCAP).		
La solution permet d'enregistrer toutes les actions faites sur la console d'administration, sans possibilité de modification.		
La solution permet de stocker en interne et de manière sécurisée les éventuels authentifiants utilisés pour l'accès aux serveurs et machines distantes, et permettre aux utilisateurs de se connecter aux systèmes cibles sans connaissance des authentifiants utilisés.		

La solution permet de consulter intuitivement les enregistrements vidéo des activités des utilisateurs, à travers un lecteur ou un outil qui permet : o De sélectionner directement les événements relatifs aux cliques de la souris ou de la saisie de certaines touches du clavier, ou l'ouverture de certaines fenêtres. o D'accélérer les vidéos o De prendre des captures de certaines manipulations effectuées lors d'une session.		
La solution permet de sécuriser la consultation des enregistrements par un utilisateur par une autorisation supplémentaire ou une authentification spécifique		
La solution permet de rechercher rapidement toutes les entrées de texte réalisées par les utilisateurs sur les protocoles en mode texte mais aussi les protocoles en mode graphique et ce sur différentes traces en même temps.		
La solution permet de déconnecter automatiquement un utilisateur, générer des alertes sous formes de traps SNMP ou de messages syslog, et d'envoyer des emails lors : o De la saisie ou de l'affichage d'un texte prédéfini et configurable, o Du lancement d'une application spécifique o De la détection des numéros de cartes de crédit basée sur l'algorithme de Luhn. - Permettre une notification par email ou par traps		
La solution permet de définir finement les accès aux applications (web ou client-serveur) ou des ressources (serveurs ou partages de fichier) en fonction de l'utilisateur et de ses conditions de connexion, que les applications et ressources soient dans un ou plusieurs datacenters,		
- SNMP sur un certain nombre d'indicateurs comme des événements liés au trafic (Connexion refusée, Violation du protocole, identification de l'utilisateur a échoué …) et aux erreurs systèmes.		
- La solution intégre un système de workflow pour autoriser l'accès d'administration à des machines identifiées		

- La solution permet de fournir des tableaux de bord qui représentent un monitoring du système (CPU, RAM et Disque) et sur les différents protocoles supportés (HTTP, RDP, SSH, ICA, VNC et Telnet)		
- La solution disposer de fonction de redémarrage, d'arrêt du système et de ses services depuis l'interface graphique pour limiter l'accès en mode console.		
- La solution fournit depuis l'interface graphique des outils : o De Troubleshooting sur l'ensemble des protocoles supportés o D'exécution des commandes d'analyse réseau (exemple : Ping, Traceroute) o D'affichage des fichiers des fichiers journaux et des logs des protocoles (SSH, VNC et RDP, HTTP)		
- La solution permet la génération de rapports personnalisables, et des rapports de conformité.		
- La solution permet d'effectuer des sauvegardes et des restaurations de la configuration du ou des données qui peuvent être utilisées en cas d'incidents.		
- Permettre la remontée d'événements vers le SIEM existant (Format ArcSight CEF) en syslog		
Coffre-fort des Mots de Passe & Gestion des Mots de passe		
Les mots de passe sont inscrits sur une Appliance matérielle renforcée.		
La base de données de mots de passe doit utiliser au moins 3 modules cryptographiques certifiés par le Programme de validation d'algorithmes cryptographiques (CAVP) pour sa fonctionnalité de cryptage.		
Le processus de demande de mot de passe s'applique uniquement aux mots de passe uniques.		
Les demandes de mot de passe doivent être rendues possibles en utilisant une infrastructure minimale. Pas plus d'une appliance doit être requise pour que la solution de mise en coffre-fort des mots de passe soit pleinement fonctionnelle pour les demandes d'accès des utilisateurs privilégiés et la gestion des mots de passe des systèmes cibles.		
La solution PAM doit pouvoir stocker les mots de passe pour ses propres comptes d'administration interne et les rendre disponibles à l'aide d'un modèle de		

demande/ de libération vérifiable.		
Les critères de gestion des mots de passe doivent être configurables pour répondre à la politique organisationnelle de la fréquence de changement des mots de passe/ le contrôle de l'approbation d'utilisation/ les changements après utilisation.		
Veuillez fournir une matrice de la capacité des solutions à gérer les fonctions de gestion des comptes privilégiés pour différents types d'appareils: par exemple, les comptes privilégiés de base de données, les comptes de dispositifs réseau, les comptes privilégiés des systèmes d'exploitation et les fonctionnalités disponibles pour chaque type de dispositif.		
- Permettre la définition de profils d'accès		
- Permettre une authentification, renforcée par des mécanismes d'OTP (One Time Password)		
- Permettre le contrôle de conformité du poste pouvant vérifier l'identité et la santé du terminal d'accès ainsi que des critères d'accès comme le lieu ou l'heure de connexion.		
<u>Gestion des accès à distance :</u> La gestion des accès à distance devra :		
Permettre de définir finement les accès aux applications (web ou client-serveur) ou des ressources (serveurs ou partages de fichier) en fonction de l'utilisateur et de ses conditions de connexion, que les applications et ressources soient dans un ou plusieurs datacenters,		
Prendre en compte une grande variété de scénarios d'accès, depuis des postes maitrisés, ou des postes non maitrisés (BYOD, BYOPC, prestataires tiers).		
Disposer d'un portail d'accès centralisant toutes les ressources et applications mises à disposition d'un utilisateur.		
Permettre l'accès aux ressources et applications à travers le portail web, avec ou sans agent sur le poste pour répondre également aux enjeux de BYOD ou de postes non maîtrisés.		
Baser sur une architecture à double barrières		

Permettre une grande précision sur les ouvertures d'accès spécifiques sur les applications au lieu d'ouvrir des accès larges à des réseaux.		
Baser sur architecture offrant des accès multisites, permettant d'accéder depuis un portail unique à des applications et des ressources réparties sur plusieurs Datacenter, on-premise et dans le cloud		
Permettre la définition de profils d'accès		
Permettre une authentification, renforcée par des mécanismes d'OTP (Onrese Time Password)		
Permettre le contrôle de conformité du poste pouvant vérifier l'identité et la santé du terminal d'accès ainsi que des critères d'accès comme le lieu ou l'heure de connexion.		
Certifier CSPN par l'ANSSI et éprouver par le Gartner		
L'offre inclut **03 ans** de support pour la totalité du périmètre fonctionnel		
L'offre de prestation inclut la mise en œuvre de l'architecture et des fonctionnalités demandées		

7. OBLIGATION DU TITULAIRE

Pour l'ensemble des lots le(s) Titulaire(s) est tenu de présenter auprès du maitre d'ouvrage les pièces suivantes :

- Les Curriculums Vitae, détaillés et portant le cachet de l'entreprise, des personnes que le prestataire s'engage à affecter pour la réalisation du présent projet. L'implémentation des différentes composantes de l'infrastructure proposée devra être assurée par une équipe spécialisée et certifiée constructeur. Les membres de l'équipe doivent avoir au minimum les spécialités suivantes :
    - Un Ingénieur ou équivalent **responsable de la gestion du projet** est indispensable, ayant au moins 5 ans d'expérience justifié autant que chef de projet de même grandeur ou plus.
    - Un Ingénieur ou équivalent **certifié sur la solution proposée** dans le cadre de cet appel d'offres, ayant au moins 3 ans d'expérience et un niveau de certification expert.

- Une liste nominative du personnel affecté au projet doit faire l'objet d'un tableau récapitulatif selon le format suivant :

Nom & prénom	Rôle dans le projet	Diplômes	Certificats obtenus	Années d'expériences

Les membres de l'équipe projet proposée par le titulaire ne peuvent être remplacés par de nouveaux membres qu'après accord écrit du Maitre d'Ouvrage. Si pour des raisons, indépendantes de la volonté du Titulaire (justifiables), il s'avère nécessaire de remplacer un des membres de l'équipe projet, le Titulaire fournira immédiatement une personne de qualification égale ou supérieure qui doit recevoir l'approbation du Maître d'ouvrage.

REDAL garde le droit de remplacer à tout moment un membre de l'équipe, si il n'est pas satisfait de sa performance ou de ses compétences, ou découvre qu'il s'est rendu coupable de vulgarisation des données de la REDAL, le Titulaire devra, sur demande du Maître d'ouvrage, fournir dans un délai de cinq jours au maximum, un remplaçant dont les qualifications et l'expérience seront soumises à l'approbation du Maître d'ouvrage.

Le Titulaire ne pourra pas soumettre des demandes de paiements au titre des coûts supplémentaires résultant du retrait ou remplacement du personnel.

Le Maitre d'ouvrage garde le droit de la résiliation du marché à tout moment, si le titulaire ne satisfait pas l'une de ses obligations.

Représentation du Titulaire et Gestion du Projet

- Le Titulaire désignera un représentant auprès du Maître d'ouvrage muni des pouvoirs nécessaires pour assurer tout le suivi du projet.

- Le Titulaire participera à une réunion de démarrage qui sera organisée dès l'entrée en vigueur du marché à la demande du maître d'ouvrage. La réunion aura pour objet la finalisation des diverses composantes du projet (prérequis, étapes, jalons, livrables, intervenants et organisation des prestations), la vérification des interfaces et la coordination des plannings (élaborer le planning d'exécution du présent marché).

- Le Titulaire s'engage à donner suite à toute demande d'information permettant au Maître d'ouvrage d'assurer le contrôle du projet.

- Le Titulaire doit valider préalablement le plan de chaque livrable avec le Maître d'ouvrage.

- Le Titulaire assurera le pilotage et le suivi de la maîtrise d'œuvre du projet et, à ce titre, devra:
  - Gérer l'avancement du projet, en veillant au respect des plannings
  - Assurer le Reporting dans un tableau de bord hebdomadaire
  - Assurer la coordination des équipes.

Le titulaire du projet doit communiquer chaque vendredi au maitre d'ouvrage, le bilan d'avancement des travaux. Il doit présenter toutes les actions qui devront être menées. Ces actions doivent être priorisées selon l'urgence et selon le degré de gain en qualité et en performance.

Des réunions périodiques doivent être prévues pour la présentation de l'état d'avancement des travaux. Dans ce cadre, un tableau détaillé d'avancement devra être tenu à jour par le Titulaire et communiqué au maître d'ouvrage.
Le Titulaire devra mobiliser le personnel nécessaire pour mener le projet dans les délais prévus. Si des retards ou des écarts sont constatés, il devra fournir les ressources nécessaires et de qualité pour les rattraper. Il devra faire appel, chaque fois que nécessaire, à des experts du domaine (même non prévus au début de sa mission) afin de dépasser d'éventuelles difficultés qui viendraient à survenir.
Il devra aussi, dans le cadre de l'exécution du présent marché :

- Mettre en place les outils et les documents méthodologiques liés à l'objet contractuel de la mission ;
- Élaborer les procès-verbaux des réunions tenues au cours du déroulement de sa mission;
- Mobiliser toutes les ressources humaines et matérielles qui lui seront nécessaires à la bonne exécution du marché dans les meilleurs délais.

Le Titulaire s'engage à respecter les exigences de la charte de sécurité des prestataires ainsi que la politique de sécurité du système d'information en vigueur à REDAL.

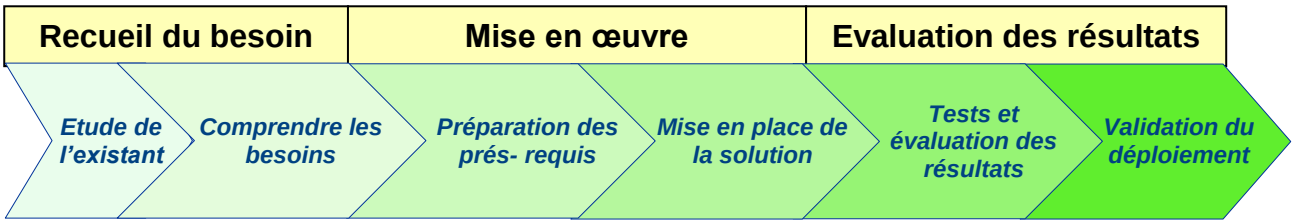
8. ADD-ON

Les soumissionnaires s'engageront obligatoirement sur le prix maximal des add-ons communiqués dans leurs offres pour les 5 années à venir. Ils doivent préciser dans leurs offres en fonction du lot auquel ils soumissionnent le coût des extensions suivantes:

N° du Lot	Add-on exigés
Lot1	Extension des licences de corrélation des logs de 250 EPS supplémentaires.
Lot2	- Acquisition licence Module de partage de charge entre Datacenter et service DNS pour la totalité de la plateforme cible - Acquisition Module de sécurité d'accès des utilisateurs pour la totalité de la plateforme cible - Acquisition Module Anti-DDoS pour la totalité de la plateforme cible
Lot3	- Extension des licences de la solution de gestion des accès à distance pour 50 utilisateurs supplémentaires - Extension des licences de la solution PAM pour 10 utilisateurs supplémentaires

9. PROCESSUS DU PROJET

Le(s) prestataire(s) retenu devra respecter les différentes phases du projet comme décrit ci-dessous, ou sinon proposera une approche qui devra être validée en commun accord avec la REDAL.



9.1 Etude De L'existant

Le prestataire devra effectuer les étapes ci-après en établissant un rapport détaillé:

- Collecter les informations relatives à l'infrastructure existante et effectuer un inventaire ;
- Formuler les recommandations nécessaires pour aligner la plate-forme avec la nouvelle approche de la REDAL.

9.2 Comprendre Les Besoins

- Le prestataire retenu est tenu de fournir un état de l'existant à travers les informations relevées lors de l'étude de l'existant ;
- Evaluer la situation et déterminer les besoins à travers des Workshop à tenir avec les administrateurs ;
- S'aligner avec les objectifs de la nouvelle solution proposée et produire un plan d'actions détaillé du projet.

9.3 Préparation Des Prérequis

Le prestataire devra communiquer sur la base de son étude de l'existant tous les prés-requis nécessaires pour la mise en place de l'architecture cible, cette étape doit être accompagnée d'un dossier d'ingénierie qui tient compte de l'impact sur l'existant. Une fois ce dossier validé, le soumissionnaire en collaboration avec la REDAL passera à l'implémentation de l'ensemble des prés-requis.

9.4 Mise En Place De La Solution

- Le soumissionnaire doit définir un plan d'actions détaillé de mise en place de l'architecture cible qui sera validé en commun accord avec La REDAL ;
- Les solutions à mettre en place ne doivent pas nécessiter des mises à jour logicielles ou des mises à niveau couteuses.

9.5 Tests Et Evaluation Des Résultats

Le prestataire devra fournir un plan de test relatif au déroulement des opérations de sauvegardes, d'externalisation des sauvegardes. Ce plan sera validé entre les deux parties

Le prestataire devra définir les critères d'évaluation de résultats et métriques permettant de juger et valider la solution.

9.6 Validation Du Déploiement De La Solution

Le prestataire devra déterminer :

- Le Plan de déploiement ;
- Produire le rapport final de la mise en place ;
- Produire la revue finale du projet.

9.7 Livrables

Pour chaque phase, le Titulaire produira des livrables adaptés, dont notamment :

Document	Contenu	Format
Dossier d'ingénierie technique	Etude détaillée de l'architecture cible. Ce document décrira les spécifications de chacun des composants dans l'architecture cible et détaillera les interconnexions entre les différentes composantes.	Word
Dossier de sécurité	Analyse des spécifications détaillées liées à la sécurité du système (contrôle d'accès, authentification, ports à ouvrir, …).	Word
Planning de gestion du projet	Détaille les différentes phases du déploiement, les intervenants, les dates début et fin de chaque opération.	MS Project
Dossier d'installation et de configuration	- Décrit les tâches d'installation et de configuration des différents composants de la solution. - Précise les équipements installés, caractéristiques techniques, schémas, fichiers de configuration.	Word
Dossier d'exploitation	- Décrit les tâches d'exploitation quotidiennes en termes d'arrêt/démarrage des services et des procédures de synchronisation de données entre les deux sites. - Manuels d'utilisation des équipements et des composantes proposées.	Word
Dossier de Supervision et d'exploitation	Décrit l'architecture de supervision, les métriques à définir et les tâches de supervision & d'exploitation	Word
Cahier de recette	Décrit : ▪ Méthodologie de recette. ▪ Fiches de tests.	Word
Plan de restauration de la plateforme	Détaille les différentes étapes ainsi que les procédures de restauration du système à partir des sauvegardes.	Word

Les livrables doivent répondre aux exigences ci-dessous :

- Etre rédigés en langue française ;
- Etre fournis en deux exemplaires sur un support non réinscriptible de type CD ou DVD contre signature d'un bordereau de livraison ;
- Etre dans des formats permettant leur exploitation et leur mise à jour par la REDAL. Ainsi, il doit être possible d'éditer les documents avec les logiciels bureautiques déployés au sein de la REDAL ;
- Faire l'objet de validation de la part de la REDAL dans des délais nécessaires et suffisants qui seront fixés d'un commun accord entre les deux parties.

N.B : Les livrables de chaque phase doivent être validé par l'équipe projet REDAL avant de passer à la phase suivante du projet.

10. FORMATION ET TRANSFERT DE COMPETENCES

Les concurrents doivent proposer des formations en fonction des lots auxquels ils soumissionnent, l'objectif est de former des équipes composées d'administrateurs techniques, pour leur permettre d'acquérir les compétences nécessaires pour gérer et prendre en charge les solutions proposées. Les frais des formations proposées seront à la charge des soumissionnaires.

Les formations doivent être dispensées obligatoirement avant le commencement des travaux d'installation et de configuration sur site.

Les soumissionnaires sont tenus de :

- Présenter les justificatifs des compétences, certificats et références d'un instructeur **Francophone** du constructeur, attestant d'un niveau d'expertise technique sur le logiciel objet de l'appel d'offres et d'une méthodologie pédagogique éprouvée. Des copies de certificats sont à fournir dans l'offre ;
- Justifier dans leurs offres techniques que les sessions de formation seront déroulées dans un centre de formation permettant aux participants de bien assimiler le thème de la formation.
- Lesdits centres doivent être spécialisés dans le métier de la formation aux nouvelles technologies de l'information. Les salles de formation doivent être équipées de matériels pédagogiques et techniques récents, adaptés aux formations dispensées ;
- Un manuel de formation est à fournir à chaque participant bénéficiant de la formation (en langue française de préférence).
- Garantir tout au long de la formation, une alternance de l'aspect théorique avec des ateliers pratiques (50% théorie - 50% pratique), l'objectif étant de permettre aux participants de valider leurs acquis ;
- Délivrer des attestations de suivi des formations dispensées au profit des participants ;
- Délivrer un support de cours qui constitue une véritable référence pour les administrateurs, édité par l'éditeur officiel et utilisable pendant et après la formation ;

Le tableau ci-dessous précise le nombre de personnes à former par lot :

N° du Lot	Nombre de personnes à former
Lot 1 : Acquisition et intégration du module de corrélation des logs de sécurité au niveau de la solution existante.	**04 Personnes**
Lot 2 : Acquisition et mise en œuvre d'une solution de haute disponibilité pour le WAF existant	**02 Personnes**
Lot 3 : Acquisition d'une solution de gestion des accès distants et d'une solution PAM	**04 Personnes**

NB : Les soumissionnaires sont tenus de détailler dans leurs offres les formations proposées ainsi que le niveau de maitrise de la solution par les participants à l'issue de la formation.

11. GARANTIE ET MAINTENANCE

Les Titulaires garantissent que tous les équipements et logiciels livrés en exécution du marché sont neufs. Il garantit en outre que le matériel et logiciels livrés en exécution du marché n'auront aucune défectuosité quant à leur conception, aux matériaux utilisés ou à leur mise en œuvre ou à tout acte ou omission du Titulaire.
Cette garantie s'étend à tous les équipements et logiciels sans aucune exception sur une période de **Douze (12) mois**. Ce délai de garantie commence à courir à partir du lendemain de la date de la réception provisoire prononcée par le Maître d'Ouvrage.

Le(s) éditeur(s) des solutions proposées devra disposer d'une équipe de support locale prête à intervenir sur site en cas d'incident.

Tous les logiciels proposés doivent être souscrits au support officiel de leurs éditeurs avec attestation de l'éditeur à l'appui.

Le titulaire doit fournir au préalable les informations nécessaires du support : Téléphone, Fax et Email.

Le Titulaire doit fournir à la livraison une attestation de garantie finale des éditeurs des différents composants de la solution proposée pour une durée minimale de 1 an.

Pendant cette période de garantie, le Titulaire dispensera au Maître d'ouvrage le service suivant :

- Le rétablissement de la conformité des solutions et des services aux spécifications annoncées dans le présent CPS et dans l'offre du titulaire;
- Intervenir sur appel de l'Administration pour remettre en état de fonctionnement la solution et les services défectueux :

Le TITULAIRE doit prendre en charge la demande d'intervention du maître d'ouvrage objet de ce marché dans un délai maximum d'une (1) heure à partir de la demande (Téléphone, fax ou Email) sur une base de 24hx7j. Le système de production doit être remis dans son état normal dans les quatre heures qui suivent la demande d'intervention.

- Informer par écrit le maître d'ouvrage des mises à jour parues et les installer à la demande de ce dernier.

L'entretien préventif comprend les mises au point nécessaires :

- Mise à jour des solutions proposées;
- Bilan de santé de la solution et les problèmes soulevés
- Vérification du bon fonctionnement et configuration des logiciels d'administration et supervision avec résolution des anomalies soulevées.

L'entretien préventif doit être effectué une fois tous les six(6) mois au frais du titulaire et en présence d'une équipe désignée par le maître d'ouvrage.

Le titulaire doit assurer l'ensemble des outils et matériaux nécessaires à l'entretien préventif ainsi qu'un document précisant l'ensemble des opérations et tests à effectuer.

Pour assurer les services indiqués ci-dessus, le Titulaire s'engage à :

Mettre à la disposition du Maître d'ouvrage une équipe de maintenance composée de personnes qualifiées.

12. CONTRAT DE MAINTENANCE

Le concurrent doit proposer dans son offre un contrat de maintenance par lot qui prendrait effet à la fin de la période de garantie pour résoudre les incidents /difficultés rencontrées par REDAL lors de l'exploitation du logiciel mis en œuvre dans le cadre de cet AO avec un niveau de service équivalent à celui dispensé durant la période de garantie.

En cas de non-respect des délais de résolution des incidents stipulés dans le contrat de maintenance, sauf cas de force majeure, le titulaire sera soumis à une pénalité de retard qui sera calculée selon la formule suivante :

$$P = (V * R) / 364$$

P = le montant de la pénalité ;

V = la valeur de la rémunération annuelle versée au titre de la maintenance ;

R = le nombre de jours de retard.

Cachet et Signature du soumissionnaire