



## **CAHIER DES CLAUSES TECHNIQUES PARTICULIERES**

### **POUR**

### **Fourniture et mise en service d'un système de sécurité réseau-Pare-feu A Bordeaux Sciences Agro**

#### **Article premier : Dispositions générales**

##### *Pouvoir Adjudicateur :*

Le Pouvoir adjudicateur est l'École Nationale Supérieure des Sciences Agronomiques de Bordeaux, établissement public à caractère administratif d'enseignement supérieur et de recherches sous tutelle du Ministère de l'Agriculture, sise 1, Cours du Général de Gaulle, à GRADIGNAN (33170), valablement représentée aux présentes par Madame Sabine BRUN-RAGEUL, en sa qualité de Directrice.

##### *Objet du marché*

Les stipulations du présent Cahier des Clauses Techniques Particulières (C.C.T.P.) concernent :

#### **Fourniture et mise en service d'un système de sécurité réseau-Pare-feu A Bordeaux Sciences Agro**

Lieu de livraison et d'exécution :

Bordeaux Sciences Agro 1, cours du Général de Gaulle CS 40201 33175 Gradignan.

Décomposition de la prestation

Compte tenu de sa spécificité, le présent marché n'est pas alloti.

Le présent Cahier des Clauses Techniques Particulières [C.C.T.P] vise à définir la nature, la qualité et les conditions de mise en œuvre des prestations à fournir au titre du marché.

L'entreprise dispose des éléments suivants pour établir son offre :

Le présent Cahier des Clauses Techniques Particulières objet du présent document ..  
Le Règlement de consultation

Le candidat devra, dans l'exécution des prestations qui lui incombent, se conformer aux clauses, conditions et prescriptions des documents techniques, normes françaises et normes techniquement équivalentes et généralement à la réglementation en vigueur pour ce type de fournitures. L'entreprise ne saurait se prévaloir de l'absence de référence à un texte réglementaire pour prétendre s'y soustraire. Si au cours des travaux de nouveaux règlements ou normes entraient en vigueur, l'adjudicataire du présent lot est tenu d'en référer par écrit au Maître d'ouvrage.

### **Qualification de l'entreprise**

Le candidat fournit tout acte administratif, notamment extrait K-BIS, assurance responsabilité civile et décennale, et toutes références adéquates sur les 3 dernières années en relation avec ce type de prestation.

### **Mémoire Technique**

Le candidat devra joindre lors de la remise de son offre **un mémoire technique** permettant d'appréhender ses capacités, sa méthodologie et la valeur technique de son offre y compris la politique de Responsabilité sociale et environnementale conduite par son entreprise.

Le mémoire technique comprendra, notamment et cela à minima :

Les moyens humains affectés à la prestation ou aux travaux,  
Les moyens matériels affectés à la prestation ou aux travaux  
Les dispositions prises par l'entreprise pour respecter les exigences du CCTP,  
La méthodologie de mise en œuvre et la gestion des déchets de chantiers.

### **Lieu de livraison**

**Bordeaux Sciences Agro  
1, cours du Général de Gaulle  
33175 Gradignan**

### **Description des équipements**

Les fiches techniques détaillées ainsi que tous les documents techniques concernant les matériels seront fournis avec l'offre de l'entrepreneur.  
Ces documents pourront être présentés dans un document relié.

## **Article 2 : Présentation de l'architecture réseau**

Bordeaux Sciences Agro est équipé d'un réseau Ethernet (LAN) divisé en plusieurs sous-réseaux (VLAN) privés et publics. Il dispose d'une interconnexion sur le réseau de campus par deux liens fibre distincts à 10 Gbps.

Le LAN de l'établissement est un réseau Ethernet TCP/IP. Plusieurs VLAN sont propagés. L'ensemble des actifs réseaux relèvent de plusieurs générations et sont amenés à être modernisés. Le cœur de réseau est composé de 4 switches fibre optique répartis dans deux salles pour assurer le PCA.

Depuis plusieurs années, le filtrage et la sécurité entre les réseaux sont assurés par deux pare-feu (actif/passif) applicatifs de niveau 7.

## **Article 3. Description du projet**

### **3.1. Besoins**

Afin d'offrir la même qualité de service à ses usagers, Bordeaux Sciences Agro souhaite déployer un système de pare-feu matériel de dernière génération.

Les nouveaux équipements viendront en remplacement des équipements existants.

La configuration des boîtiers existants devra être reprise, et la politique de sécurité devra être modifiée pour se conformer au mieux à un audit qui a été réalisé en 2023 et dont les conclusions seront remises au titulaire du marché dès qu'il aura été désigné.

### **3.2. Objectifs**

Le présent marché porte sur le déploiement d'un système de pare-feu comprenant la fourniture, l'installation et les prestations nécessaires à la mise en œuvre d'une solution de sécurité réseau « clés en main » basée sur les normes standards du marché en remplacement de la solution actuelle.

Le présent marché comporte un seul lot.

Ce marché comprend :

- La fourniture des équipements réseau permettant le filtrage et la sécurisation de la circulation des flux réseau.
- La fourniture des équipements nécessaires à l'intégration de ces équipements dans le réseau existant.
- La dépose et le recyclage des équipements existants.
- L'installation et la configuration de ces matériels et l'intégration au réseau existant.
- La fourniture d'une prestation de maintenance des équipements 5j/7 heures ouvrées délai d'intervention J+1, pendant 3 à 5 ans sur site (le candidat fera les deux propositions).

Ces travaux sont à exécuter en site occupé. Des dispositions sont à prévoir pour éviter la dispersion de poussières. La gestion des coupures de service devra faire l'objet d'une attention particulière et être décrite dans le détail de la réponse.

### **3.3. Résultats attendus**

#### **ARCHITECTURE FONCTIONNELLE**

##### **Caractéristiques techniques :**

Les solutions de sécurité demandées, devront assurer le filtrage des flux de niveau 7. Afin d'assurer notamment une migration la plus douce possible, l'objectif est de pouvoir remplacer dans les règles de firewalls la référence aux « ports » par une référence à « l'application ». La détection applicative au niveau 7 doit nativement être réalisée par identification du payload au travers d'une base de signatures et non sur la base d'un port TCP ou UDP. Pour pallier, au cas où des flux applicatifs seraient inconnus par l'équipement, il devra être possible de créer ses propres signatures de détection d'application, ou de demander à l'éditeur de la solution de les créer. À cette fin, un mode d'emploi et un transfert de compétence spécifique devra être fourni par le titulaire, expliquant précisément la manière de créer ses propres signatures personnalisées, en minimisant le risque de faux-positif ou d'évasion d'application.

Les mises à jour des bases de signature applicatives documentées doivent être automatiques (constructeur) ou manuelles en cas de besoin. Ces mises à jour devront pouvoir être effectuées :

- Soit « online » directement avec possibilité de passer par un proxy
- Soit « offline » sans raccordement direct à internet du pare-feu, par update manuel des fichiers récupérés sur le site du constructeur

Les performances demandées sont définies sur une base de mix applicatifs niveau 7 et devront à minima respecter 8 Gbps et 3 Gbps avec Threat Prevention actif (anti-virus, IDS/IPS, anti-malware, détection des attaques inconnues, filtrage URL, DDOS, DLP...).

Les équipements devront fournir a minima 2 interfaces physiques 10 Gbit/s SFP+

Les équipements devront proposer obligatoirement au moins un port de gestion « out-of-band ». Ce port devra être dédié et non routable par l'intermédiaire des autres interfaces physiques.

Les processus d'administration des pare-feu devront utiliser des ressources dédiées, afin de séparer le traitement des flux d'administration, du traitement des flux de production. La méthode interne de cette séparation des traitements sera explicitée par le candidat.

Les pare-feu devront pouvoir être gérés directement, sans console tierce. Cette gestion devra s'effectuer en Web via https, ainsi qu'en SSH pour les accès en ligne de commandes.

L'ensemble de la configuration devra être lisible au format texte. Il devra être possible de la modifier hors ligne, puis de l'importer dans l'équipement.

Les équipements objets du marché relèvent des technologies Gigabit Ethernet/10GbE, et doivent impérativement être conformes aux normes en vigueur (normes IEEE 802.3, 802.3ab, 802.3ae2002, 802.3u, 802.3z, 802.1D, 802.1Q, 802.1X selon les types de ports mis en œuvre).

Le titulaire fournit les descriptifs techniques des équipements concernés. Ces descriptifs mentionnent le(s) type(s) de connecteurs disponibles pour les interfaces fibre optique (LC, SFP+, etc.).

Comme mentionné, les capacités de traitement correspondent à la somme des flux analysés par l'équipement à un instant donné, soit la somme des flux traversant l'ensemble des interfaces de l'équipement à un instant donné avec les fonctionnalités de filtrage et de prévention d'intrusion décrites ci-dessous activées. Les capacités de traitement seront également fournies avec tous les modules activés,

tels qu'anti-virus, anti-spyware, détection d'intrusions, DLP...

L'équipement filtrant devra permettre de définir, sur chacune de ses interfaces physiques, des VLAN (norme 802.1q) et être en mesure d'appliquer une politique de filtrage inter-VLAN.

Pour la couche 3, les caractéristiques suivantes sont demandées :

- Plusieurs interfaces physiques de l'équipement filtrant doivent pouvoir être associées à un même VLAN.
- L'équipement peut être compatible avec les protocoles 802.1p, 802.1w et 802.1ad

#### Configuration et administration

Il est demandé que la solution réside dans un boîtier actif unique. Un boîtier passif est exigé. Le titulaire précise les certifications ou qualifications du matériel proposé, notamment par l'ANSSI.

Les équipements proposés doivent être administrables à distance et leur configuration doit pouvoir être sauvegardée et rechargée vers un serveur (protocole à préciser).

La proposition technique du titulaire décrit l'interface d'administration distante.

Les traces doivent pouvoir être exportées sur un serveur dédié par le protocole syslog.

#### **Le(s) logiciel(s) d'administration**

Ses fonctionnalités doivent être les suivantes :

- Mise à jour des versions d'OS/Firmware
- Mise à jour des configurations
- Analyse des journaux d'événements, éventuellement avec une solution supplémentaire que le candidat précisera
- Bascule manuelle/automatique sur l'équipement de secours

L'accès des administrateurs à la plate-forme doit être soumis à authentification ; il doit être possible de limiter l'accès d'un administrateur à tout ou partie du parc géré par le logiciel et de définir des parties seulement en consultation. Il sera précisé si l'interface est en français.

Le logiciel doit signaler si un autre administrateur est en train de faire des modifications. Le logiciel doit permettre de générer des rapports, manuels ou automatiques, concernant les flux qui le traversent :

- Bande passante consommée par port/application, et par utilisateur/IP
- Vulnérabilités, virus
- Évolution des flux par rapport à une journée de référence.

#### BASCULE ET FONCTIONNALITÉS

##### **Redondance :**

Le candidat doit renseigner les points suivants :

- La redondance des alimentations électriques (de base ou optionnelle)
- La synchronisation entre les équipements en cluster dans chacun des modes supportés, indiquer 5 CCTP-DSI-PF

notamment si cette synchronisation inclut la synchronisation des configurations, paramétrages et suivi des sessions.

- Le temps de bascule actif/passif et l'impact sur les sessions actives (bascule transparente, temps de coupure, ...).
- Le traitement séquentiel ou en parallèle des différentes fonctions (routage, firewalling, analyse Niveau 7, antivirus, IDS-IPS).
- L'encombrement du matériel (poids, dimensions) et s'il est rackable en baie standard 19"
- Les dispositifs internes de redondance des équipements (ventilateurs, disques, ...)

### **Fonctionnalités (cf. 3.3.1)**

Les fonctionnalités suivantes devront être présentes sur la solution :

- Identification, analyse et contrôle des flux applicatifs (IPv4 et IPv6 de niveau 7) basée sur l'identité des applications et pas uniquement sur les ports et les protocoles (Firewall de Nouvelle Génération). En conséquence, le filtrage doit pouvoir être mis en place sur la base des critères suivants :
  - Applications connues et/ou inconnues
  - Adresse IP (machine ou réseau) source et/ou destination
  - Protocole de niveau 3 (IP, ICMP, IPSEC, ...)
  - Protocole de niveau 4 (TCP, UDP)
- Le candidat précise les mécanismes de QoS et de limitation de bande passante.

Le candidat précise, à titre indicatif, si la solution permet du filtrage basé sur des catégories d'URL. Le candidat explicite, pour chacune des fonctionnalités ci-dessus, si elle est disponible pour les protocoles IPv6 et avec quel niveau de performance.

### **Fonctions de filtrage profilées.**

Filtrages en fonction de l'utilisateur : nous souhaitons pouvoir effectuer des filtrages en fonction de l'authentification individuelle de l'utilisateur (ou de son appartenance à des groupes d'utilisateurs (enseignant, étudiant...) auprès d'annuaires de type OpenLDAP et/ou Radius. Le candidat précisera les modalités de mise en œuvre et notamment si plusieurs bases d'authentification peuvent être utilisées simultanément.

### **Fonctions anti menace**

La solution devra proposer un traitement du trafic en un seul passage avec toutes les fonctions de sécurité actives.

Il serait souhaitable que les équipements puissent proposer un système d'analyse proactive des règles et de la configuration s'appuyant sur les données collectées par la télémétrie.

Le candidat précisera les capacités de sa solution pour la prévention des menaces en intégrant des mécanismes d'antivirus, d'anti-malware, détection des vulnérabilités, botnet, « command and control », attaques de brutes forces et IPS/IDS sans perte de performance.

Le candidat explicite le mode de mise à jour des bases qui permettent le contrôle applicatif.

Le candidat précisera explicitement si sa solution peut résoudre le problème d'attaque en brute force sur des login/mot de passe d'applicatifs publiés (web, mail, vpn, etc...).

Les équipements devront pouvoir proposer un contrôle d'intégrité paramétrable pour les accès VPN.

Les accès VPN devront prendre en charge les méthodes d'authentification forte (MFA), y compris les certificats, les cartes à puce et l'intégration SAML.

### **Fonctions réseau**

Le candidat précise le nombre maximum de zones de sécurité ainsi que le nombre maximum de VLANs autorisés par équipement.

Il précise aussi les limitations en nombre de politiques de filtrage par équipement.  
Le candidat précise si la solution permet une délégation d'administration.

Le candidat décrira les fonctionnalités autour des fonctions suivantes :

- Protocoles de routages BGP, OSPF, RIP et routage statique. Relayage des protocoles BOOTP et DHCP.
- NAT, IPv6 et Multicast (dont PIM, IGMP, ...)
- Protocole d'administration SNMP, Syslog et protocole de métrologie : Netflow ou équivalent

La solution devra permettre aux utilisateurs de se connecter au réseau via un tunnel VPN. Le candidat devra préciser :

- Le nombre maximum de sessions simultanées (licences/performances),
- La compatibilité des clients VPN SSL et VPN IPSEC avec les OS suivants : Windows, Linux, MacOS X, IOS, Android, en particulier si les clients sont directement disponibles dans le système d'exploitation, ou si l'éditeur propose un client VPN pour ces systèmes d'exploitation.
- Les modes de personnalisation/intégration/déploiement des clients VPN sur les postes de travail,
- La disponibilité d'un portail SSL (ne nécessitant pas l'installation d'un client lourd sur le poste de travail).
- La capacité d'attribuer différents niveaux d'accès aux VLANs aux utilisateurs en fonction de leur appartenance à des groupes (OpenLDAP, le candidat précisera le type de groupe).

### **3.4. Prestation d'installation et de paramétrage**

Le candidat précisera les modalités de la prestation d'installation et de paramétrage. Bordeaux Sciences Agro fournira au candidat retenu un compte-rendu d'audit, qu'il conviendra d'appliquer autant que possible sur la politique de sécurité des boîtiers pare-feu installés. Pour information cet audit comporte 52 mises en conformité, décrites et mises en contexte, de diverses sévérités.

### **3.5. Maintenance et support**

#### **Pérennité des équipements**

La maintenance matérielle (remplacement du matériel en panne par du matériel de fonctionnalités et performances équivalentes) et logicielle (mises à jour mineures, majeures et fonctionnelles) des équipements proposés doivent être possibles pendant au moins les cinq années suivant la date limite de remise des offres.

La proposition technique du titulaire fournit les informations de l'éditeur/constructeur sur le cycle de vie de l'équipement proposé : date de fin de commercialisation prévue, date de fin de support prévue ou, si aucun renseignement n'est disponible, une attestation de l'éditeur/constructeur s'engageant à assurer la maintenance dans les cinq années à venir et à continuer à faire évoluer le logiciel embarqué (mises à jour mineures, majeures et fonctionnelles).

#### **Garantie matérielle**

En cas de panne du matériel, une ouverture d'incident sera signalée auprès du centre de support par un correspondant technique de Bordeaux Sciences Agro.

Après diagnostic de la panne effectué par le centre de support, la pièce défectueuse fera l'objet d'un échange standard, puis un retour atelier.

Les éléments en panne seront remplacés par du matériel identique expédié par le titulaire du marché. Ces éléments deviennent alors la propriété de Bordeaux Sciences Agro.

#### **Garantie logicielle**

Le titulaire s'engage à informer Bordeaux Sciences Agro par courrier électronique de la disponibilité d'une nouvelle version logicielle. Qu'il s'agisse d'une évolution mineure ou majeure.

Le titulaire fournit à Bordeaux Sciences Agro un accès en ligne sur le site du constructeur et, le cas échéant, de l'éditeur, permettant le téléchargement de ces mises à jour et de la documentation associée.

En cas d'impossibilité de téléchargement, le titulaire s'engage à fournir les nouvelles révisions ou versions logicielles accompagnées des microcodes correspondants, aux conditions du constructeur.

Le titulaire s'engage à corriger ou à faire corriger les erreurs reproductibles constatées par Bordeaux Sciences Agro et à transmettre les demandes de corrections fonctionnelles auprès du constructeur/éditeur.

## **Maintenance**

Un contrat de maintenance sera proposé. Il devra couvrir l'ensemble des matériels, logiciels et configurations décrits dans la solution du titulaire.

Ce contrat sera établi selon les modalités suivantes :

Durée 5 ans

Intervention jours de semaine aux heures ouvrées (8h00 à 18h00)

Système de gestion : garantie de rétablissement du service J+1

Matériel : échange J+1 en heures ouvrées

Logiciels : diagnostic J+1 en heures ouvrées

Accès à une « hotline » aux heures ouvrées

Le soumissionnaire précisera l'organisation et la localisation des équipes de maintenance.

Le soumissionnaire fournira un exemplaire du contrat de maintenance.

## **4. Planning**

### **4.1. Calendrier**

Le fournisseur devra s'engager sur le calendrier d'installation. Il devra définir une durée de chaque phase du projet, installation des boîtiers, configuration, et durée d'indisponibilité du service.

Le planning prévisionnel, susceptible de modification en fonction des contraintes sanitaires, prévoit un déploiement au plus tard au mois d'octobre 2025. Cette date pourra être repoussée en fonction des aléas et des contraintes liées.

### **4.2. Pénalités de retard délai d'exécution et de support**

Après validation du planning, en cas de dépassement des délais contractuels (délais d'exécution, délai d'intervention pour exercice du support), Bordeaux Sciences Agro pourra appliquer des pénalités de retard, calculées par application de la formule suivante :

<formule à fournir par Alex ?>

## **5. Prix**

Le prix est soumis au taux de TVA applicable pour ce type de prestation

## **Article 6. Visite et livrable**



### **6.1. Visite**

Une visite des locaux est obligatoire. Un certificat de visite sera dressé à l'issue de cette visite. Le candidat prendra contact auprès de la DSI de Bordeaux Sciences Agro au 05 57 35 07 95 (Aurélie Bedeau)

### **6.2. Livrables**

Le candidat fournira dans sa réponse un dossier de spécifications techniques ainsi que le détail des temps et moyens humains mobilisés pour chaque tâche. Ce dossier sera accompagné d'un contrat de maintenance-type.

## **Article 7. Dispositions générales**

### **Prestations générales**

Le marché est passé pour un service clé en main. Le titulaire est réputé avoir pris connaissance des contraintes techniques de tous ordres imposés par l'environnement architectural de Bordeaux Sciences Agro et d'en avoir tenu compte dans l'établissement de sa proposition.

#### **Au titre de la livraison**

Le titulaire aura à sa charge la livraison des marchandises faisant l'objet de la commande directe ainsi que celles connexes à la commande.

#### **Au titre de la fourniture**

Le titulaire prend en charge les éventuelles adaptations, de toutes natures, des marchandises à la topographie des locaux, dans la mesure où ces adaptations sont acceptées par Bordeaux Sciences Agro et rendues nécessaires à l'exécution des prestations.

#### **Au titre des installations**

Le titulaire prend en charge les prestations liées à l'installation (montage, mise en place) des marchandises.

#### **Au titre des essais et contrôles**

Le titulaire aura à sa charge les essais et le contrôle liés à la qualité et à la sécurité des installations.

#### **Au titre de la documentation**

Le titulaire fournit pour chaque type de biens, une documentation relative aux opérations de montage et de démontage ainsi qu'à leur utilisation.

#### **Normes et règlements applicables**

Les prestations du titulaire doivent être conformes aux clauses de l'ensemble des lois, décrets, arrêtés, règlements, circulaires, normes et tous les textes européens, nationaux ou locaux applicables aux prestations de la présente opération, et en particulier aux dispositions nationales et européennes régissant la fourniture de biens meubles.

Le fait de ne pas énumérer de manière exhaustive ces normes et règlements ne peut être pris pour arguments d'ignorance par le titulaire, celui-ci étant réputé les connaître, du seul fait de soumissionner.