



CENTRE HOSPITALIER UNIVERSITAIRE DE BESANCON

DIRECTION DU SYSTEME D'INFORMATION ET DE LA CONVERGENCE NUMERIQUE
2 PLACE SAINT-JACQUES
25030 - BESANÇON CEDEX

Cahier des Clauses Administratives Particulières (C.C.T.P.)

AO N° 2025- 50

**Date et heure limites de réception des offres :
lundi 20 octobre 2025 à 12:00**

**Fournitures de produits, prestations et services pour la
sécurisation du réseau informatique
Pour le CHU de Besançon**

Ce document comporte 10 pages numérotées de 1 à 10

AVERTISSEMENT

Ce document contient des informations confidentielles.

Il doit être utilisé uniquement dans le cadre de l'appel d'offre dont il fait l'objet.

Les informations qu'il contient, ainsi que toute autre information complémentaire qui pourrait être fournie par le CHU de Besançon, ne peuvent être transmises à des tiers, ou utilisées à d'autres fins, sans accord explicite du CHU de Besançon.

Toute reproduction, numérique ou physique, de ce document est interdite.

Par conséquent, en prenant possession de ce document, le candidat s'engage à :

- **Ne pas divulguer les informations de ce document à des personnes non expressément autorisées à recevoir ces informations.**
- **N'utiliser ce document que dans le cadre de la réponse à cet appel d'offre**
- **A prendre toutes les mesures permettant d'éviter toute utilisation détournée ou frauduleuse des informations contenues dans ce document**
- **A procéder à la destruction de ce document à l'issue de cet appel d'offre s'il n'est pas retenu, ou à la fin du marché consécutif à cet appel d'offre, dans le cas où il serait retenu**

En cas de non-respect des dispositions précitées, la responsabilité de la société est engagée et le CHU. de Besançon se réserve le droit d'engager des poursuites à l'encontre de la société.

1. Objet de l'appel d'offre

Le présent appel d'offre porte sur la sécurisation du réseau du système d'information du CHU de Besançon (par la suite désigné par CHU)

2. Environnement du CHU de BESANCON

2.1. Généralités

Le CHU est actuellement réparti sur plusieurs sites reliés par fibres optiques. Le CHU compte environ 5000 postes de travail.

Le CHU possède trois salles informatiques.

Les différents points réseau sont reliés en fibres optique, avec un cœur de réseau en 100Gb/s.

2.2. Architecture technique existante

Accès Internet

Le CHU possède 2 accès Internet chez 2 opérateurs distincts, avec plusieurs adresses IP publiques, en répartition de charge via un load-balancer (cluster de 2 FortiADC de Fortinet). Le CHU gère les domaines chu-besancon.fr et chru-besancon.fr

RADIUS

Le logiciel IDENTIKEY Authentication Server Standard Edition de OneSpan assure la fonction authentification RADIUS pour les accès Télétravail, avec aussi des tokens mobiles et physiques Onespan.

Firewall

Le CHU est doté de deux firewalls :

- ⇒ Un cluster de firewall Fortinet pour la protection des zones internes. Les logs du firewall sont remontés sur un Fortianalyzer installé sous forme de VM.
- ⇒ Un cluster de firewall PaloAlto pour la protection des zones extérieures, dont Internet et les DMZ. Ce cluster effectue un filtrage web et applicatif pour les accès web, sur la base d'une authentification AD. Il assure aussi une fonction de VPN SSL (GlobalProtect). Les logs du firewall sont remontés sur un Panorama installé sous forme de VM.

Le CHU gère également un firewall Palo-Alto situé sur un site distant, relié au CHU en IPSEC, via le Panorama ci-dessus.

Antispam

Un cluster de 2 Fortimail de Fortinet, installés sous forme de VM, assure la fonction antispam.

WAF

Un cluster de 2 Fortiweb de Fortinet, installés sous forme de VM, assure la fonction de firewall d'applications (WAF) pour les services exposés sur Internet.

Portail VPN-SSL

Un cluster de 2 Ivanti Connect Secure assure la fonction de portail VPN-SSL. Ce portail permet, après une authentification forte à base de token OneSpan, un accès pour la télémaintenance des fournisseurs. Le candidat inclura donc ceux-ci au BPU.

Bastion

Le produit PRA de BeyondTrust assure les fonctions de Bastion sur le réseau CHU : les flux et opérations d'administrations sont assurés par ce Bastion. Il est utilisé par les agents du CHU, et par les fournisseurs (à terme, il remplacera complètement le VPN-SSL Ivanti).

IPSEC

Le CHU utilise plusieurs routeurs CISCO ASA pour des connexions IPSEC avec des sites distants et différents fournisseurs.

MicroSOC

L'infrastructure (postes de travail et serveurs) du CHU est surveillée à distance par un microSOC se basant sur Cortex XDR de PaloAlto.

3. Description du besoin

3.1. Généralités

On entend par « sécurisation du réseau », la mise en place de tout élément, logiciel ou matériel, positionné sur le réseau et contribuant à la sécurisation du système d'informations, vis-à-vis des réseaux extérieurs (dont les sites partenaires et Internet) et de certains réseaux internes du CHU (dont le réseau des serveurs).

L'objectif de cette sécurisation doit ainsi permettre de bloquer :

- ⇒ Les tentatives d'intrusion,
- ⇒ La propagation de logiciel malveillant,
- ⇒ Le vol de données confidentielles,
- ⇒ L'utilisation à son insu des ressources informatiques du CHU,
- ⇒ Les accès non autorisés aux réseaux internes du CHU, dont les serveurs du CHU, dans un souci de confidentialité et de sécurité
- ⇒ Plus généralement toute tentative pour nuire aux intérêts du CHU et de ses patients.

Cette sécurisation s'appuie sur des outils de suivi, d'administration, d'exploitation... Par conséquent, tout outil permettant de mieux contrôler la sécurité du réseau relève aussi de cet appel d'offre.

L'objet du marché est de fournir et mettre en place ces éléments (logiciels/matériels) de sécurité, de maintenir ces éléments et ceux déjà en place au CHU, et de pouvoir assurer des prestations sur cette infrastructure de sécurité, afin de renforcer sa sécurité face aux nouvelles menaces et pour répondre aux recommandations des instances.

Le CHU pourra s'appuyer aussi sur ce marché pour acquérir de nouveaux outils, encore inconnus aujourd'hui mais toujours relatifs à la « sécurisation du réseau ».

L'utilisation de ce marché se bornera à « la sécurisation du réseau », comme définit plus haut. En

particulier, ce marché ne traite pas de la sécurisation des annuaires type Active Directory, de l'authentification des utilisateurs aux applications métiers, ou de la protection des données du CHU.

Le candidat retenu pourra aussi conseiller et recommander des évolutions ou extensions de cette architecture.

3.2. Exemples de projets à réaliser

Le CHU pourra utiliser ce marché pour mettre tout type de solution permettant de sécuriser son réseau et de contrôler cette sécurité, comme par exemple des outils relatifs à :

1. La centralisation des événements et le monitoring centralisé, type SIEM
2. La reconnaissance d'équipements IOT type biomédicaux, ou autres
3. La gestion/suivi centralisé des politiques de firewall ou autres équipements de sécurité, orchestration de politiques de sécurité

Le candidat devra proposer des produits relatifs à ces 3 type de problématiques : il inclura à sa proposition une description technique de ces outils, ainsi qu'une tarification au **BPU**.

Le candidat fournira la tarification de la maintenance sur les produits fournis

3.3. BPU

Pour répondre aux besoins du CHU, le candidat devra compléter le **BPU** (Bordereau de Prix Unitaires), avec tous les produits/prestations pouvant être commandés sur ce marché.

Dans le bordereau de prix du RPA, le candidat indiquera :

- Onglet « Prestations » :
 - o Un tarif journalier pour chacun des profils en heures ouvrées (entre 8h00 et 17h00, présence effective de 8h00 sur site, frais de transport, restauration, hébergements inclus et un tarif horaire en heures non ouvrées (entre 17h00 et 8h00)/week-end/jours fériés frais de transport, restauration, hébergements inclus.

Dans le bordereau de prix du RPA, le candidat renseignera :

- Onglet « Catalogue de prix chap 3.2 et 3.3 » :
 - o Les prix de son catalogue de produits remisés permettant de répondre aux besoins exprimés au chapitre 3.2 du présent CCTP (3 types de problématique), y compris la maintenance éditeur/constructeur (cf. article 4 du présent CCTP)
 - o Tout autre produit utile pour la sécurisation du réseau, le contrôle et le suivi de cette sécurisation
- Onglet « Catalogue de prix chap 5 » :
 - o Les prix de son catalogue de produits remisés permettant la maintien et l'évolution des produits utilisés par le CHU tel que défini au chapitre 5 du présent CCTP, y compris les tokens et la maintenance éditeur/constructeur (cf. article 4 du présent CCTP)
- Onglet « Support 1^{er} niveau » :
 - o Le prix de son support 1^{er} niveau annuel qu'il offre lui-même sur ces produits, comme défini aux § 3 & 4

4. Support et télémaintenance

Le fournisseur devra intégrer dans le **BPU** la maintenance éditeur/constructeur sur les produits proposés et ceux déjà en place au CHU.

Cette maintenance devra inclure toutes les mises à jour (correctives, évolutives, ou de sécurité) sans surcoût. En particulier, le fournisseur s'engage à prévenir au plus vite le CHU de toute mise à jour majeure relative à la sécurité.

Il proposera en outre, un support supplémentaire de premier niveau autre que celui de l'éditeur/constructeur et devra compléter le Bordereau des Prix Unitaires (**BPU**). Ce support sera directement géré par le fournisseur.

Par conséquent, en cas d'incident, le CHU contactera directement le fournisseur, qui prendra en charge cet incident et sa résolution, en se retournant éventuellement vers le constructeur ou l'éditeur.

Ce support se fera en langue française et sera accessible par téléphone (aux heures ouvrées, et non ouvrées pour les incidents bloquants), et par le web.

Le candidat décrira l'organisation en place pour assurer ce support, et en particulier précisera:

- ⇒ La procédure pour déclarer un incident : numéro de hotline et adresse du site web, les informations à fournir, les jours et les heures d'ouverture, les délais de rappel, d'intervention et de résolution,
- ⇒ Les moyens mis en œuvre pour être averti des nouvelles versions et recevoir les correctifs et mises à jour.

En cas d'anomalie bloquante :

Le fournisseur devra intervenir à distance (par téléphone ou par télémaintenance, voir § suivant « Télémaintenance ») dans l'heure, à partir de l'ouverture d'un incident. Il mettra alors tout en œuvre pour apporter un diagnostic, et résoudre ou contourner le problème. En cas d'intervention sur site, les frais seront à la charge du fournisseur.

Télémaintenance

En cas d'accès au réseau du CHU pour un besoin de télémaintenance, le fournisseur devra utiliser le Bastion du CHU. Pour cela, il devra:

- ⇒ Fournir son ou ses adresses IP sources publiques
- ⇒ Désigner un administrateur au sein de sa société, qui devra gérer les autres utilisateurs (les accès au Bastion du CHU sont nominatifs), à travers un portail d'auto-enregistrement mis à sa disposition.
- ⇒ Se conformer aux règles d'accès au Bastion du CHU (en particulier enregistrement vidéo des sessions)

Tout autre moyen de télémaintenance (comme par exemple Teamviewer, Bastion autre que celui du CHU...) est proscrit.

5. Eléments existant à maintenir

Ce paragraphe décrit la maintenance des équipements existant à prendre en compte dans cet appel d'offre, le candidat remplira le **BPU** en conséquence. En plus de ces maintenances, le candidat proposera son propre support sur ces produits comme décrit au §3 : support téléphonique en français en 24x7.

5.1. Équipements Fortinet

Appliance	Nb appliances/ VM	Début maintenance 1ère année
Fortigate 2500E , en cluster <i>Threat Protection Bundle (24x7 FortiCare plus Application Control, IPS, AV and Botnet IP/Domain Services)</i>	2	23/01/2026
Fortianalyzer VM <i>Support 24x7 FortiCare Contract (for 1-26 GB)</i>	1	23/01/2026
Fortimai VM01 , en cluster <i>24x7 FortiCare and FortiGuard Enterprise ATP Bundle Contract</i>	2	23/01/2026
Fortweb VM02 , en cluster <i>Advanced Bundle - Standard Bundle plus Credential Stuffing Defense Service and Threat Analytics</i>	2	23/01/2026
FortiADC-220F , en cluster <i>FortiCare Premium Supported</i>	2	23/01/2026

La maintenance inclura:

- ⇒ Un support téléphone 24x7 sur tous ces équipements
- ⇒ Les mises à jours : firmware, signatures (IPS, Antivirus...)
- ⇒ Au minimum le remplacement de l'appliance à J+1 en cas de panne: le candidat précisera les modalités de ce remplacement (dans quel cas de figure, quelle période, quel délai, intervention sur place ou non....)
- ⇒ Le candidat pourra proposer une intervention sur place pour réparation

5.2. Équipements PaloAlto

Appliance	Nb appliances/ VM	Début maintenance 1ère année
PAN-PA-5410 en cluster - Core Security Subscription Bundle (Advanced Threat Prevention, Advanced URL Filtering, Advanced Wildfire, DNS Security and SD-WAN), 3 years - PA-5410, Prisma Access Agent subscription, for one (1) device in an HA pair, 3 years - Partner enabled premium support 3-year term, PA-5410	2	Octobre 2028
Panorama 25 devices <i>premium support</i>	1	04/11/2026

Appliance	Nb appliances/ VM	Début maintenance 1ère année
PAN-PA-440 <i>Advanced Threat prevention, premium support</i>	1	04/11/2026

La maintenance inclura:

- ⇒ Un support téléphone 24x7 sur tous ces équipements
- ⇒ Les mises à jours : firmware, signatures (IPS, Antivirus...)
- ⇒ Au minimum le remplacement de l'appliance à J+1 en cas de panne: le candidat précisera les modalités de ce remplacement (dans quel cas de figure, quelle période, quel délai, intervention sur place ou non....)
- ⇒ Le candidat pourra proposer une intervention sur place pour réparation

5.3. Logiciel OneSpan

Logiciel	Nb de licences	Début maintenance 1ère année
IDENTIKEY Authentication Server Standard Edition Maintenance	1060	09/05/2026
IDENTIKEY Authentication Server Standard Edition OAS Standard Edition	50	09/05/2026
ONESPAN – Mobile Authenticator ES Maintenance & Support	640	09/05/2026

La maintenance inclura:

- ⇒ Un support téléphone en heures ouvrées au minimum
- ⇒ Les mises à jours logicielles

Le CHU doit aussi être en mesure d'acquérir de nouveaux tokens VASCO (DP260 ou équivalent, mobile), le candidat inclura donc ceux-ci au **BPU**.

5.4. Logiciel BeyondTrust Privileged Remote Access

Logiciel	Nb de licences	Début maintenance 1ère année
Privileged Remote Access Per Asset Subscription	1500	01/07/2027
BeyondTrust Appliance B Series-VM-Subscription	2	01/07/2027
BeyondTrust Advanced Web Access Subscription	1	01/07/2027

La maintenance inclura:

- ⇒ Un support téléphone 24x7
- ⇒ Les mises à jours

5.5. Équipements Ivanti

Appliance & licences	Nb appliances	Début maintenance 1ère année
Ivanti Virtual Appliance 4000 Base System Subscription Gold Direct	2	09/02/2026
Ivanti Connect Secure VPN Concurrent User Subscription Gold Assurance	2 x 25	09/02/2026

Le support est actuellement assuré en heures ouvrées uniquement.
La maintenance inclura les mises à jours

5.6. Cisco

Equipement	Nb	Début maintenance 1ère année
Cisco ASA 5516-X en cluster JMX2207G327 / JMX2207G324	2	19/05/2026
Cisco ASA 5506 JMX1909Z0DC JMX2134Y2JE JMX2213G09K	3	19/05/2026

La maintenance inclura:

- ⇒ Un support téléphone en jours et heure ouvrés sur tous ces équipements
- ⇒ Les mises à jours : firmware...
- ⇒ Au minimum le remplacement de l'appliance à J+1 en cas de panne: le candidat précisera les modalités de ce remplacement (dans quel cas de figure, quelle période, quel délai, intervention sur place ou non....)
- ⇒ Le candidat pourra proposer une intervention sur place pour réparation

6. Prestations horaires ouvrés et non ouvrés

Les prestations commandées par le CHU se feront sur la base d'un descriptif technique du besoin. Ces prestations porteront sur le périmètre de cet appel d'offre. Le CHU donnera alors au fournisseur tous les éléments nécessaires pour mener à bien la prestation attendue.

Il est entendu par prestation : l'installation (matérielle ou logicielle), la configuration, l'optimisation, l'audit, le conseil, etc... d'une infrastructure dans le périmètre visé par cet appel d'offre.

Deux horaires sont distingués : **ouverts** : du lundi au vendredi entre 8h00 et 17h00 et **non ouverts** : du lundi au vendredi entre 17h00 et 8h00 et les week-ends et jours fériés

Pour les prestations facturées à la journée (horaires ouverts) : les journées de prestation devront être effectuées pendant les heures d'ouverture du service (entre 8h00 et 17h00). Celles-ci devront inclure les frais de transport, de restauration et d'hébergement des prestataires.

Les journées de prestation comprennent huit heures de présence effective au CHU. Si le nombre d'heures de présence journalière n'est pas atteint, le CHU se réserve le droit de payer la journée au prorata du nombre d'heures de présence effective.

Pour les prestations facturées à l'heure (non ouvrées), elles devront inclure les frais de transport, de restauration et d'hébergement des prestataires.

7. Compétences requises

La « sécurité réseau » doit être une activité principale et reconnue du candidat : il doit être partenaire d'au moins une dizaine d'acteurs (éditeurs/constructeurs) majeurs.

Le candidat décrira donc son activité dans ce secteur de la « sécurité réseau » : chiffre d'affaires, nombre de personnes, partenaires, organisation...

Le candidat détaillera dans sa réponse technique toutes les technologies sur lesquelles il a de réelles compétences (on entend par technologie, un domaine lié à la sécurité, comme par exemple le firewall ou les IDS/IPS...) et en particulier sur le besoin exprimé ci-dessus.

Pour chacune de ces technologies, il précisera :

- ⇒ Les produits qu'il propose
- ⇒ Ses certifications chez l'éditeur/constructeur et son positionnement dans l'échelle de certification de cet éditeur ou constructeur
- ⇒ Le nombre de personnes susceptibles d'intervenir sur la technologie et leur niveau de certification.
- ⇒ S'il assure un support sur ces produits
- ⇒ Des références récentes sur des projets menés avec succès