

MARCHE 2020/15
CAHIER DES CLAUSES TECHNIQUES PARTICULIERES
(C.C.T.P.)

PARE-FEUX POUR L'UNIVERSITE d'ANGERS

Le présent CCTP comporte 4 feuillets numérotés de 1 à 7

Pour le Président et par délégation,
Le Directeur Général des Services

Olivier HUISMAN

Sommaire

ARTICLE 1 – DEFINITION DU MARCHE.....	3
ARTICLE 2 – CONTEXTE.....	3
ARTICLE 3 – CARACTERISTIQUES TECHNIQUES.....	4
3.1 - Généralités.....	4
3.2 – Fonctionnalités obligatoires des pare-feux.....	4
ARTICLE 4 – QUALITE DE SERVICE.....	5
4.1 - Généralités.....	5
4.2 - Pare-feux	5
ARTICLE 5 – MEMOIRE TECHNIQUE.....	6
5.1 - Généralités.....	6
5.2 – Pare-feux.....	6
5.3 – Installation / transfert de compétences.....	7
5.4 – Formations.....	7

ARTICLE 1 – DEFINITION DU MARCHÉ

Le présent marché a pour objet :

- La fourniture et la garantie de 2 matériels informatiques de type pare-feux ;
- La maintenance de ces matériels ;
- La fourniture des logiciels permettant leur fonctionnement ;
- La maintenance et la garantie d'évolution de ces logiciels ;
- L'installation, le transfert de compétences et la formation sur ces matériels ;
- Un bordereau de prix unitaire complètera l'offre pour les matériels et licences complémentaires.

ARTICLE 2 – CONTEXTE

Le réseau commuté haut débit de l'université d'Angers, mis en place à partir de 1999, est actuellement constitué des éléments suivants :

- Deux routeurs 10 Gigabits Extreme Networks avec un accès à Renater à 10 Gb/s ;
- Des commutateurs Extreme Networks avec des ports fibres et cuivres Gigabit et 10-Gigabit en cœur de réseau ;
- 250 commutateurs Ethernet Extreme Networks ;
- 700 bornes wifi ;

Actuellement 21000 équipements sont raccordés au réseau de l'université d'Angers, ordinateurs, GTB/GTC, équipements de laboratoires, téléphones, ordinateurs portables en wifi.

Le schéma de sécurité informatique de l'université d'Angers s'est traduit par la mise en place, en 2015, de deux pare-feux, Fortinet 1500D, en actif/passif, ayant chacun 6 interfaces 10 Gb/s et 10 interfaces 1 Gb/s.

Ces équipements sont connectés sur des commutateurs de marque Extreme Networks.

Les fonctionnalités actuellement utilisées sur ces pare-feux sont :

- VDom : 10
- Advanced Routing
- IPV6
- Application control
- IDS/IPS
- Load Balancing
- Antivirus

Ce marché vise à remplacer ces deux équipements qui sont en limite de performances, principalement, en termes de CPU et mémoire.

ARTICLE 3 – CARACTERISTIQUES TECHNIQUES

3.1 - Généralités

Les articles qui suivent définissent les fonctionnalités souhaitées sur les différents matériels. Ils précisent également les configurations physiques demandées par rapport aux tableaux de prix en annexes à l'acte d'engagement.

3.2 – Fonctionnalités obligatoires des 2 pare-feux

1. Le réseau de l'université comprend 71 réseaux, IPV4 et IPV6, dont 40 sont traités par le pare-feu. D'autre part, les flux d'accès à internet de tous les postes informatiques de l'université ne chemineront pas ces pare-feux.
2. Le système de pare-feu sera installé pour permettre ou interdire les différents trafics entre ces réseaux (L3 à L7). Pour chaque sous-réseau IP connecté, le pare-feu devra pouvoir être déclaré comme passerelle de sortie (« gateway ») ou non.
3. La fonctionnalité de relai DNS ou forwarder DNS doit être proposée.
4. Les différentes interfaces du pare-feu sur le réseau devront utiliser le protocole 802.1q pour permettre le trafic des différents réseaux virtuels.
5. Si le trafic est autorisé, la communication entre 2 réseaux devra pouvoir avoir les modes suivants :
 - a. Mode transparent
 - b. Mode routé en IPV4 et IPV6, avec en ipv4 la possibilité de traduction d'adresses NAT ou PAT ;
6. Dans tous les cas, le pare-feu devra être transparent vis-à-vis de tous les champs de QoS de niveau 2, 802.1p, ou 3, comme les champs tos et diffserv.
7. Les règles de pare-feu devront offrir toutes les possibilités de niveau 3 et 4. Elles proposeront également des fonctionnalités de niveau 7 par repérage des différentes applications utilisées.
8. D'autre part, des fonctionnalités de détection d'intrusion (IDS) et de protection contre les intrusions (IPS) devront également être fournies.
9. Au niveau physique, le système se composera de deux matériels identiques redondants en mode haute disponibilité actif-actif ou actif-passif.
10. Les deux matériels seront reliés par une paire dédiée de fibre optique monomode (longueur > 10 km) connectée sur des ports HA (« high availability ») spécifiques. Les GBIC, SFP, SFP+ associés pour les ports HA doivent être fournis.
11. Chaque matériel devra avoir au moins 6 ports 10 Gigabit Ethernet installés, hors port HA. Les interfaces 10 Gigabit Ethernet devront pouvoir être agrégées avec le protocole

802.3ad, LACP, afin d'offrir des liaisons n*10 Gigabit Ethernet

12. Chaque matériel devra avoir, à minima, une double alimentation électrique.
13. Pour l'administration, il doit être possible : De créer des comptes utilisateurs ; De protéger l'accès à l'administration du pare-feu par un filtre IP.
14. Des outils de logs doivent être disponibles permettant leur déport vers un serveur syslog
15. La configuration doit pouvoir être sauvegardée dans un fichier-texte lisible par un humain.
16. Le chiffrage à indiquer devra correspondre à un ensemble comprenant :
 - a. 2 pare-feux redondants définis matériellement comme ci-dessus ; Maintenance matérielle suivant les conditions définies à l'article 4-2 et pour toute la durée du marché ;
 - b. Les différents logiciels et licences nécessaires permettant l'usage et l'évolution de l'ensemble des fonctionnalités indiquées pendant la durée du marché ;
 - c. Une intervention de 5 journées sur site pour l'installation des matériels et des logiciels et un transfert de compétences ;
 - d. Une formation de 5 journées sur site, sur les matériels et logiciels livrés.

ARTICLE 4 – QUALITE DE SERVICE

4.1 - Généralités

Durant la durée du marché, le titulaire doit fournir une prestation de maintenance de l'ensemble des logiciels fournis et un service de support technique.

La maintenance logicielle comprend la fourniture des **nouvelles versions correctives et évolutives, c'est-à-dire dites mineures ou dites majeures**, de chacun des logiciels.

Le support technique consiste à l'ouverture d'un accès par téléphone et par messagerie électronique Internet, ou par plateforme internet de type helpdesk, afin de répondre aux différents problèmes logiciels rencontrés : difficultés de paramétrage, incidents majeurs, dysfonctionnements, etc. Il doit permettre l'ouverture de tickets d'incident auprès du constructeur.

4.2 - Pare-feux

Une prestation de maintenance matérielle, sous forme de garantie de temps de rétablissement (GTR), est également demandée et devra être assurée pendant la durée du marché et à compter de l'installation sur site des matériels.

Le titulaire s'engage au rétablissement du fonctionnement normal du système de pare-feu dans **un délai de 30 heures ouvrées** après le signalement en heure ouvrable de la panne ou du mauvais

fonctionnement par le Service Systèmes et Réseaux de l'université d'Angers.

Les heures ouvrées s'entendent de 8h à 18h, du lundi au vendredi, hors jours fériés.

Pour garantir le bon fonctionnement des matériels et les délais de rétablissement du service en cas de panne, le titulaire pourra :

- Effectuer des contrôles réguliers sur site et remplacer tout élément dont il a pu constater un défaut, avant que ne survienne la panne, en informant le Service Systèmes et Réseaux des problèmes rencontrés ;
- Appeler le Service Système et Réseaux afin de faire procéder par ce dernier à tout test nécessaire ;
- Tenir à la disposition du Service Système et Réseaux du matériel de remplacement.

Afin de réaliser ces prestations, le titulaire ne pourra avoir accès aux locaux de l'université d'Angers que sous le contrôle du Service Systèmes et Réseaux et après avoir pris préalablement contact avec ce dernier.

Il ne pourra interrompre le service qu'hors heures ouvrées et après avoir obtenu l'accord du Service Systèmes et Réseaux.

ARTICLE 5 – MEMOIRE TECHNIQUE

5.1 - Généralités

Le mémoire technique doit répondre explicitement aux différentes demandes indiquées ci-dessous et **si possible dans le même ordre**.

Le candidat doit d'abord préciser les moyens organisationnels, humains et techniques qui seront mis en oeuvre pour la réalisation des prestations demandées.

Il devra en particulier :

- Préciser la procédure d'ouverture et de suivi d'incidents jusqu'à leur résolution ; **(4 points)**
- Préciser la méthode permettant de fournir les nouvelles versions des logiciels utilisés ; **(2 points)**
- Indiquer clairement son niveau de certification auprès du constructeur ; **(5 points)**
- Préciser une certification de la solution proposée par l'Agence nationale de la sécurité des systèmes d'information, l'ANSSI. **(5 points si précisé, 0 sinon)**

5.2 – Pare-feux

Le candidat doit décrire le mode ou les différents modes de haute disponibilité proposés actif-actif ou actif-passif. **(4 points)**

Il doit indiquer l'ensemble des interfaces disponibles sur les matériels et les protocoles utilisables, notamment 802.1q, 802.3ad. **(3 points)**

D'autre part, le candidat doit **explicitement toutes les fonctionnalités citées à l'article 3-2, dans le même ordre (7 points)**

Le candidat remplira l'annexe 5, tableau de performances et tableau d'évolutivité.

Tableau de performances :

Le candidat qui présentera la solution avec les meilleurs indicateurs de performances aura **(5 points)**.

Tableau d'évolutivité :

Le candidat qui présentera la solution avec les meilleurs indicateurs d'évolutivité aura **(5 points)**

*Nota : A contrario, il est inutile de développer les différentes fonctionnalités de protection contre les pourriels (« anti-spam »), de vpn ssl ou ipsec qui **ne sont pas demandées** à l'article 3-2.*

5.3 – Installation / transfert de compétences

- Le candidat développera le processus d'installation et le transfert de compétences envisagé durant les 5 jours prévus. **(5 points)**

5.4 – Formations

- Le candidat développera le contenu des 5 jours de formation. Elles se dérouleront sur le site de l'université d'Angers. L'objectif est de rendre autonome 2 personnes du service systèmes et réseaux, sur les matériels et logiciels livrés. **(5 points)**

Le candidat pourra fournir toutes les informations techniques complémentaires qu'il estimera utile à la compréhension de son offre.