

UNIVERSITE DE TOURS

60, rue du Plat d'Etain – BP 12050
37020 TOURS Cedex 1



Cahier des Charges

Renouvellement de licences compatibles avec le routeur SMTP central de l'Université de Tours

1 L'Université de Tours

L'Université est composée de 3 900 personnels (domaine @univ-tours.fr) et 34 000 étudiants (domaine @etu.univ-tours.fr). D'autres domaines sont en vigueur mais sont des alias des deux autres. Le trafic mensuel (entrant et sortant) est de l'ordre de 7 millions de mails, en pointe le trafic peut atteindre 10 000 mails par heure jusqu'à 10 mails par seconde.

2 Objet du marché et transition

Au 31 mai 2026, l'université de Tours devra avoir renouvelé les licences et la maintenance matérielle et logicielle de son dispositif de routage SMTP. Ce dispositif physique est composé de 2 boîtiers Cisco Secure Email Gateway C395 achetés en mai 2023.

Les boîtiers sont connectés dans notre datacentre, ils constituent le cœur de notre système de messagerie. Le dispositif gère l'ensemble des flux SMTP internes mais aussi des flux entrants et sortants. Son rôle principal est d'assurer la sécurité de ces flux et de lutter contre toutes les tentatives d'intrusion via le service de messagerie. Il assure le rôle de chef d'orchestre des flux de messagerie.

La livraison des licences devra obligatoirement être effective, au plus tard, à la date du 31 mai 2026 et devra reprendre toutes les fonctionnalités en vigueur sans rupture de service décrites dans le présent document et actuellement disponible sur les boîtiers. (cf article 4)

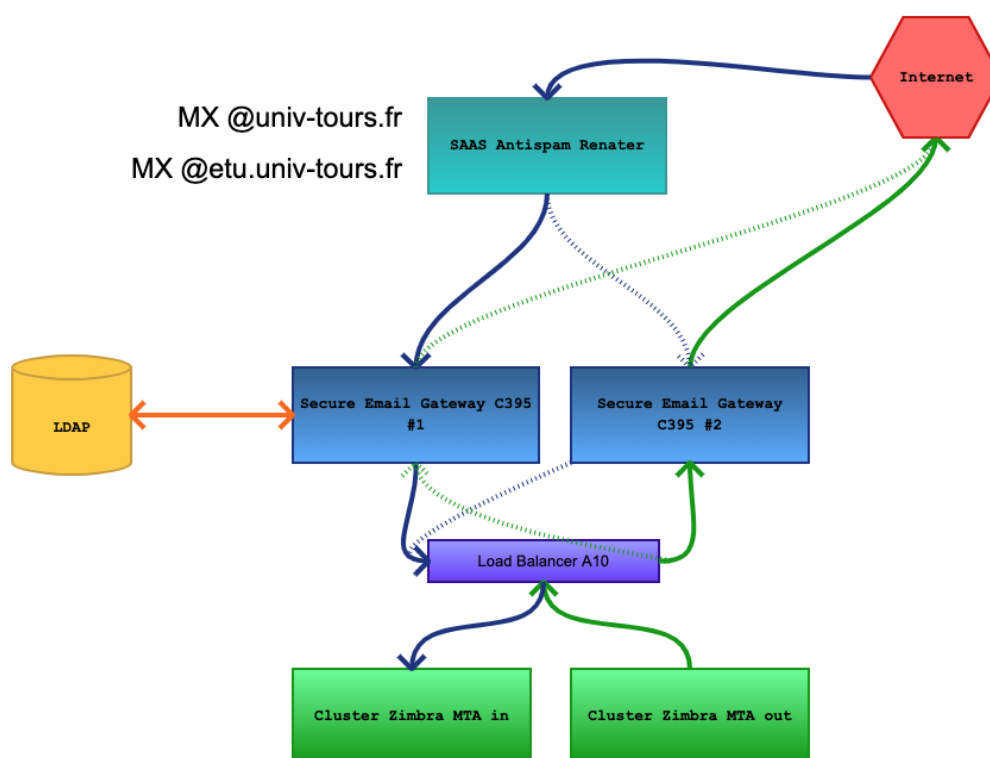
L'objet du marché concerne l'achat de licences compatibles avec le matériel possédé par l'Université de Tours, la maintenance et les services associés pour une durée de 3 ans, à savoir :

- La fourniture, la livraison et la mise en production des nouvelles licences, compatibles avec notre matériel,
- la garantie et la maintenance matérielle et logicielle,
- l'assistance de niveau 2, l'assistance niveau 1 (utilisateur) est prise en charge par l'Université.
- les journées d'intégration nécessaires à la mise en place des prestations.
- 2 jours par an de service pour la maintenance en conditions opérationnelle du service sur la durée du marché (3 ans), soit 6 jours au total.

3 Architecture actuelle de la messagerie

L'architecture de messagerie de l'Université de Tours est basée sur 3 types d'appareils/logiciels

- Un service antispam-antivirus en SaaS opéré par le GIP Renater (en amont de l'arrivée des mails)
- le cluster matériel faisant l'objet du marché, composé de deux Cisco ESA C395 actuellement en version 16.0.3 (gérant flux entrant, traitement smtp interne, flux de soumission clients et flux sortant)
- un cluster zimbra 10 pour la remise finale dans les boîtes. Ce cluster héberge les boîtes du personnel (3900 boîtes) et pour les étudiants (45000 boîtes car il y a inscription avant la sortie des anciens étudiants)



4 Fonctionnalités attendues

Après intégration des licences dans nos boîtiers le prestataire garantira un fonctionnement identique à la solution actuelle exposés dans les articles 4.1 à 4.5.

Dans un second temps, des améliorations pourront être proposées par le prestataire. Ces modifications fonctionnelles feront l'objet d'une validation commune université de Tours – titulaire du marché. Les améliorations se feront après la mise en service à iso-fonctionnalité.

4.1 Cluster de routage SMTP

Le service smtp fonctionne en tolérance de pannes et partage de charge avec

pour objectif la haute disponibilité du service. Le service est porté actuellement par un cluster de 2 nœuds physiques. L'université de Tours utilise plusieurs mécanismes de partage de flux dont un répartiteur de charge externe (A10 Thunder™ 3030S) qui ajuste les algorithmes de basculement en fonction des cas.

La solution technique du titulaire permettra de router l'entièreté des flux de messagerie et d'appliquer l'ensemble des traitements de sécurité avec un délai de traitement de l'ordre de la seconde en temps normal (25 000 mails par heure) et ne pas excéder la minute pour les pics à 50 mails par seconde.

Le dispositif offrira les dernières évolutions « à l'état de l'art » des protocoles utilisés (routage, filtrage, sécurité).

4.2 Administration et intégration

La technologie proposée s'administrera avec une interface web et une interface cli (pour automatisation des procédures) et ce pour l'ensemble du cluster. Le système produira des fichiers de journaux exploitables (lisibles avec un éditeur de texte basique type vi - emacs) et exportables (syslog et graylog) tout en proposant un moteur de recherche graphique permettant de connaître l'état de l'ensemble des traitements effectués sur chacun des messages. Ce moteur de recherche proposera une recherche multicritère sur les métadonnées du message (from, to, subject date, status de filtrage des différents moteurs et status de remise...).

Le système permettra de gérer les files d'attentes des messages (transferts, nettoyage, reprise...).

L'ensemble des personnalisations utilisateur se feront selon des requêtes dans l'annuaire d'établissement (Openldap à la norme Supann). Le système gèrera plusieurs profils utilisateur : administrateur de la plateforme, opérateur des quarantaines, utilisateur (pour débloquer leurs messages en quarantaine).

4.3 Flux gérés

Le dispositif gère quatre types de flux :

- Flux entrant à la suite de l'antispam de RENATER ;
- Flux sortant pour les messages à destination des autres domaines ;
- Flux des clients de messageries :
 - postes internes ;
 - postes itinérants/mobiles via smtpauth ;
- Flux internes :
 - routage inter-domaines,
 - serveurs de messagerie (zimbra, listes de diffusion, enquêtes...),

- serveurs identifiés (outils numériques, monitoring,...).

Chaque flux est géré par des IP/ports paramétrables, ce qui permet un paramétrage fin de ce qui est exposé à l'extérieur de l'Université. Seuls les IP/ports entrants sont visibles de l'extérieur.

Les traitements effectués sont configurables par politique. Les politiques peuvent être différentes en fonction des sources d'émission (IP, domaines, réputation, géolocalisation) mais aussi des expéditeurs ou destinataires selon leur appartenance à des groupes de notre annuaire Openldap.

Les politiques sont capables de faire de la limitation de flux par écrêtage (nb de sessions ou destinataires par unité de temps...).

4.3.1 Traitements attendus sur les flux SMTP entrant

Le cluster permet de compléter le filtrage du flux entrant commencé par Renater. Il intégrera un service de quarantaine.

- Validation des signatures SPF, DKIM et de l'état DMARC ;
- Classes de services en fonction de critères de l'expéditeur (IP, géolocalisation...) ;
- Anti-spam avancé pour le personnel de l'Université :
 - avec traitement différentiel selon la catégorie ;
 - le taux de faux positif devra être de l'ordre de 1 pour 1 million de mails traités ;
 - la politique par défaut est de ne pas délivrer les positifs, la quarantaine sera utilisée pour récupérer les faux positifs éventuels ;
 - Les politiques sont déterminées en fonction de l'appartenance à des groupes LDAP ;
- Traitement antivirus interne à la passerelle ;
- Anti-malware ;
- Filtrage d'URL et autres dispositifs anti-phishing ;
- Anti-relayage ;
- Traitement des vulnérabilités de type « zéro day » ;
- Gestion des quarantaines administrateur et utilisateur ;
- Protection contre les attaques par dictionnaire ;
- Filtrage par dictionnaire sur le contenu des messages ;
- Quarantaine utilisateur pour tous les usagers (authentification LDAP).

4.3.2 Flux sortants

La gestion des flux sortants permet d'éviter le blacklistage de nos messages sortant vers nos partenaires. En conséquence le dispositif redirigera tout ou partie du flux sortant vers une autre adresse IP en fonction des besoins.

Voici les traitements effectués :

- Gestion fine du flux sortant de mail par domaine (écrêtage de flux) ;
- Traitement Anti-spam et antivirus du flux sortant ;

- même capacité que l'antispam entrant avec un réglage indépendant.
- Filtres manuels par contenu ;
- Dispositif anti-Backscatter (*rétrodiffusion*) ;
- Signature DKIM ;
- Marquage SPF.

4.4 Routage interne

Le cluster est le pivot du routage du mail interne : tous les serveurs SMTP délivrent leurs flux à ce dispositif, les principaux fournisseurs sont les serveurs zimbra, le serveur de liste de diffusion, les serveurs d'enquêtes, mais aussi tout serveur destiné à envoyer des e-mails.

Le routage smtp interne vers les domaines internes se fait par référence à un champ de l'annuaire LDAP qui indique le prochain serveur saut SMTP. Il n'y a aucun traitement antispam /antivirus sur le routage interne.

4.5 Soumission des messages et authentification

Le flux de mail des clients lourds est aussi géré par ce dispositif. Les clients utilisent des connexions chiffrées et authentifiées sur notre annuaire LDAP. La machine affecte différentes classes de traitement en fonction de l'adresse IP émettrice (réputation, géolocalisation, historique de traitement...). Ces classes de traitement permettent de définir les outils de sécurité mis en œuvre et de définir les droits à envoyer sous forme de nombre de destinataires par expéditeur défini par unité de temps. Enfin l'annuaire LDAP donne le droit individuel à utiliser ce service de soumission (mécanisme de blocage des comptes).

5 Garantie, Assistance et support

L'offre intégrera un contrat de maintenance matérielle et logicielle (mises à jour mineures et majeures) pour la totalité de la durée du marché (3 ans).

Le soumissionnaire inclura dans l'offre une prestation de support à destination des administrateurs techniques de la DSI de l'université de Tours. Les demandes d'assistance devront se faire en français avec un interlocuteur unique et identifié, expert de la solution. L'ensemble des modalités d'appel à la maintenance ainsi que le mode de contact, les durées d'intervention et le mode de qualification de la sévérité des incidents seront explicités.

Délais d'intervention attendus :

- matériel J+1 5j/7
- support logiciel et assistance : H+8 5j/7

Pendant toute la durée du Marché, le titulaire garantira le bon fonctionnement de la solution. Dans le cas où une rupture de pièces détachées interviendrait, le titulaire du marché s'engage à remplacer le matériel par une solution équivalente jusqu'à la fin de l'engagement contractuel de service.

6 Pérennité de la solution et année d'exploitation supplémentaire

L'offre mentionnera la durée de vie de la solution proposée au-delà du présent marché (matériel, logiciel et maintenance).

7 Conditions de livraison

Les licences seront à livrer et installer sur nos matériels situés à l'adresse suivante :

Université de Tours : DSI-Direction des Systèmes d'Information, 60 rue du plat d'étain, Bâtiment D, 37020 Tours.

8 Réversibilité

Il est rappelé que l'université de Tours est propriétaire de toutes les données et documents produits au sein de la solution et qu'elle devra être autonome pour obtenir une extraction complète des données.