CAHIER DES CLAUSES TECHNIQUES PARTICULIÈRES

(C.C.T.P.)

ESIGELEC
Ecole d'Enseignement Supérieur
Technopole du Madrillet
Avenue GALILEE
BP 10024
76801 Sainte Etienne du Rouvray

Cahier des Clauses Techniques Particulières : 19S0005

ACQUISITION ET MAINTENANCE D'UNE SOLUTION FIREWALL EN HAUTE DISPONIBILITE

Procédure adaptée en application de l'(des) article 27 du Décret n°2016-360 du 25 mars 2016 relatif aux marchés publics.

PRESENTATION ET BESOIN

L'ESIGELEC, établissement d'enseignement supérieur, école d'ingénieurs généraliste, veut renouveler son boitier firewall UTM.

La nouvelle solution s'inscrit dans un contexte global de garantie du service informatique, l'évaluation technique des solutions se fera sur des critères de performance, de disponibilité, de fonctionnalité et de possibilités d'évolution .

CAHIER DES CLAUSES TECHNIQUES

Contexte

Ce document décrit les différentes fournitures dans le cadre du remplacement de la solution de firewall UTM actuellement en place à la l'Esigelec.

La sécurité de l'ensemble est actuellement assurée par 2 Boitier XTM 545 Watchguard pour laquelle nous avons les administrer en total autonomie.

Deux sorties internet :

- 100 Mbits/s
- 10 Gbits/s

Objet du marché

La présente consultation a pour objet la fourniture d'une solution de sécurité intégrant

- La fourniture de matériel
- Les licences associées
- Le support, les modifications de paramétrage et la maintenance sur 3 ans
- Une journée d'intervention

Descriptif technique de la solution :

Vue d'ensemble :

Le nombre d'utilisateurs total sera d'environ 2200. Chaque utilisateur sera en mesure d'utiliser au moins 2 équipements en simultanément.

Les produits mis en place devront être maintenus et mis à jour sur une période minimum de 3 ans (En option sur 5 ans).

Fonctionnalités attendues de la solution proposée :

- 8 ports physiques 1gb Ethernet cuivre et 4 ports 10 Gb SFP minimum par boitier
- Equipement compatible avec la mise en armoires au format 19 pouces
- La réponse devra détailler les licences, la mise en place et la formation nécessaire.
- La réponse financière devra lister de façon détaillée l'ensemble des matériels et prestations.
- Les outils d'analyse et paramétrage avancés qui peuvent être externes aux boitiers et soumis à licences devront être chiffrés séparément.

Administration :

- Offrir la possibilité de définir la configuration des boitiers en mode offline, pour la pousser ensuite sur les appareils.
- Permettre la configuration, en mode graphique et en mode ligne de commande .
- Permettre l'ordonnancement automatique des règles de sécurité pour une meilleure efficacité de protection et d'en simplifier l'administration.

Proxy :

- Permettre la mise en œuvre de Proxys transparents (sans nécessiter la configuration de ce proxy sur les postes clients).
- Permettre le filtrage niveau 7, et un contrôle de contenu sur les flux suivants :
    - HTTP
    - HTTPS
    - POP3
    - SMTP
    - FTP
    - DNS
    - SIP
    - H323

- Interdire les relais de messagerie. Permettre la spécification des domaines de messagerie entrants et sortants. Permettre d'effectuer des filtres sur les émetteurs et expéditeurs.
- Permettre la mise en œuvre d'un serveur de quarantaine Antispam, accessible aux utilisateurs en mode Web dans la solution de base
- Le Proxy SMTP doit permettre des actions basées sur le nom et le type des fichiers contenus dans un fichier d'archive compressé, par exemple bloquer un .exe dans une archive zip.

Fonctionnalités :

- La solution doit être un boîtier de gestion unifiée, permettant le filtrage des flux au niveau 7 en appliquant à minima les traitements suivants : Antivirus, Antispam, Filtrage de contenu, IPS/IDS, contrôle d'application. Ces fonctionnalités doivent pouvoir fonctionner sur la base de règles mentionnant des utilisateurs ou des groupes d'utilisateurs, s'appuyant sur l'Active directory.

- La solution Antivirus embarquée dans le boitier doit permettre d'assainir les flux de données courants (HTTP, HTTPS; FTP, SMTP, POP3) et supporter le scan du contenu des archives (zip, rar, etc...)

- Les systèmes de détections embarqués antispam, antivirus, et filtrage de contenu doivent utiliser des systèmes de réputation basés sur des évènements dans le Cloud afin de rendre ces protections dynamiques et proactives.

- Le système de détection d'intrusion embarqué (IPS) doit fonctionner pour TOUS les protocoles.

- La solution doit comporter un outils de collection de journaux, d'analyse et de rapport inclus dans la solution de base. (Génération de graphiques d'activité, statistiques, collection des logs dans une base de données standard, non propriétaire.)

- Les logs du pare feu doivent être sécurisées (Echanges chiffrés), collectées dans une base de données puis analysées dans un outil de rapports et de statistiques afin de permettre la génération de tableaux de bord personnalisables et planifiables. Possibilité de consulter ces tableaux en mode Web ou génération sous forme de fichiers PDF.

- Permettre la mise en œuvre des boîtiers en cluster, actif / passif et actif / actif

- Boitiers pare feu avec un maximum de robustesse au niveau matériel (Pas de pièces mécaniques, notamment des disques durs)

- La proposition devra décrire la manière de faire évoluer les boitiers pour un accroissement significatif du nombre d'utilisateurs (X2) .

- La solution de base doit permettre la connexion de clients VPN IPSEC et SSL. Le client VPN SSL doit pouvoir être téléchargé simplement depuis le boîtier (LAN et WAN) et être compatible Windows XP, Vista, 7, 8, 10 et Mac OS.

- Le client VPN SSL doit supporter Mac OS X 10.11 (El Capitan)

- Client VPN IPSec et SSL compris dans la solution de base (le nombre devra être précisé dans la réponse)

- La solution proposée ne doit pas être limitée en nombre d'utilisateur, notamment au sujet des fonctions applicatives (Antivirus, antispam etc.)

- Le boitier doit pouvoir fonctionner en mode routeur et en mode transparent.

- Le pare feu doit permettre le contrôle de la bande passante selon des utilisateurs, des groupes, des règles et des protocoles.

- La gestion de plusieurs accès Internet doit être possible dans les modes suivants :
    - Partage de charge
    - Tolérance de panne
    - Aiguillage des flux manuel (Policy Based Routing)
    - Surcharge d'interface

- La solution proposée doit permettre l'authentification sur :
    - La base de données d'utilisateurs et de groupes intégrée
    - Active Directory (Authentification intégrée et transparente depuis le LAN (SSO))
    - Radius
    - LDAP
    - SecureID

- La solution proposée devra permettre l'identification des Malwares avancés (APT) via une solution de Cloud Sandboxing avec des alertes sur les malwares Zero day

- Proposer une solution en option permettant de corréler les menaces avec l'activité des postes de travail.

Maintenance et garantie

Le soumissionnaire devra proposer

- Une GTR de 24 heures.
- Une maintenance et une garantie de 3 ans sur site.
- Une extension de maintenance et de garantie de 2 ans (en option) sur site.

DELAIS et LIVRAISON

ESIGELEC : Avenue Isaac Newton – Technopole du Madrillet 76 801 Saint Etienne du Rouvray.

Les délais de livraison moyens du matériel avec la configuration complète doivent être impérativement indiqués dans la proposition du candidat.

EXECUTION DU MARCHE

Les candidats sont réputés :

- Avoir apprécié exactement la nature des besoins, l'importance et les particularités de ce qui est demandé,

Chaque page parafée

Mention manuscrite « Lu et approuvé » :

Date :

Qualité du signataire :

Signature et cachet de l'entreprise :