Spécifications techniques d'une solution de sécurité

Caractéristiques minimales	Quantité
Firewall	**01**
• Solution firewall permettant la création de règles de sécurité granulaires à base d'adresse IP, nom d'utilisateur ou type d'équipement (PC, téléphone ou tablette)	
• Translation d'adresses NAT et PAT	
• Déploiement en mode Routage (Niveau 3), mode transparent (Niveau 2) ou en mode Proxy	
• Routage Statique et Dynamique RIP, OSPF et BGP	
• Virtualisation : Possibilité de créer plusieurs Firewalls virtuels dans le même équipement physique.	
• VLAN Tagging (802.1Q)	
• Proxy Cache	
• Optimisation des Flux WAN	
• Qualité de service QoS , réservation de bande passante	
• Load Balancing sur les liens ISP	
• Clustering Actif/Passif ou Actif/Actif	
• Gestion des réseaux wifi (Contrôleur Wifi) pour une future installation d'un réseau wifi	
VPN	
• Support du VPN IPSec site a site	
• Chiffrement DES, 3DES et AES / Hachage SHA-1/MD5	
• Protocoles IKEv1 et IKEv2	
• Clients VPN IPSec et SSL VPN pour les utilisateurs nomades	
• Chiffrement DES, 3DES et AES / Hachage SHA-1/MD5	
• Protocoles IKEv1 et IKEv2	
IPS et contrôle applicatif	
• Protection contre les intrusions	
• Gestion des anomalies des protocoles	
• Signatures personnalisables	
• Mise à jour automatique des bases d'attaques	
• Inspection SSL/TLS sur les trafics HTTPS et SSH	
• Identification et Control dynamique des applications (Control d'accès par Application)	

• Base de réputation des IP pour la détection des Botnet	
Antivirus	
• Antispyware et prévention des vers sur les protocoles HTTP/HTTPS, SMTP/SMTPS, POP3/POP3S, IMAP/IMAPS, FTP, CIFS, MAPI et Messagerie Instantanée	
• Intégration avec des solutions d'analyses avancées contre les menaces (ATP Advanced Threat Protection)	
• Mises à jour en temps réel et périodiques	
• Mise en quarantaine des fichiers	
Filtrage URL	
• Filtrage URL à base par catégorie	
• Filtrage des protocoles HTTP/HTTPS et sur les requêtes DNS	
• Liste d'exclusion d'URL (WhiteList ou BlackList)	
• Filtrage des en-têtes MIME	
Authentification des utilisateurs	
• Base de données LDAP en local	
• Intégration avec Active Directory (AD) ou serveurs Radius/Tacacs+/LDAP externes	
Prévention contre les fuites de données	
• Identification et monitoring des données confidentielles en transit	
• Base de données de modèles	
• Moteur d'expressions régulières pour personnaliser les filtres	
• Actions configurables (neutralisation/log)	
• Surveillance de la messagerie instantanée, des flux HTTP/HTTPS et autres protocoles	
• Prise en charge des types de fichiers courants	
• Prise en charge des caractères internationaux	
• Marquage des fichiers par une signature digitale afin de détecter la fuite de ces fichiers même si le nom ou l'extension ont été changés	
Administration et Reporting	
• Gestion via une interface Web (HTTP/HTTPS) ou CLI (Console/SSH/Telnet)	
• Interface Web multilingue supportant le français	

• Log des évènements en local et/ou vers un serveur SysLog externe	**01**
• Tableaux de bord en temps réel ou historique	
• Outils de Monitoring et Reporting intégrés	
• Différents profils d'administration	
• Compatible SNMP	
• Notification des administrateurs par email des virus et attaques détectés	

Performances matérielles :

Désignation	caractéristiques minimales
Interfaces	10 x GbE RJ45 + 8 x GbE SFP
Trancievers à inclure	2x SFP (SX 1 GE)
Performance FW	16 Gbps
Performance VPN	14 Gbps
Performance SSL VPN	400 Mbps
Performance IPS	4.7 Gbps
Performance AV	3.4 Gbps
Connexion simultanées	20 000
Client IPSec VPN	10 000
Client SSL VPN	500
VPN Site à Site	2 000
Firewalls Virtuel	10
Alimentation Redondante	oui

Indication importante :

- Il y a lieu d'inclure les frais d'installation et de configuration de la solution ;
- L'ensemble des équipements objet de la consultation doivent être garantie pour une période d'une année au minimum ;
- Le Certificat SSL doit être inclus dans l'offre
- En cas de panne ou défectuosité, il sera remplacé l'équipement en question ;