TP N°2 : Cas Concret

Le dirigeant d'une industrie **Textile** souhaite renouveler son installation de sécurité multisite tout en la dotant de concepts supplémentaires. Elle se dote pour cela d'une série de VM FortiGate L'installation actuelle sur chaque site comprends :

1. Un Firewall virtualisé permettant de segmenter l'architecture telle que :
    a. Un réseau Bureautique en 10.X.X.0/24 en tant que réseau LAN,
    b. Un réseau SRV en 10.X*2.X*2.0/25 servant à l'hébergement des serveurs
    c. Une liaison WAN fournie par l'opérateur,
    d. Une liaison ADMIN a paramétrer par vos soins.
2. Une communication LAN vers WAN est nécessaire pour assurer le bon fonctionnement bureautique,
3. Des tunnels VPN IPsec vers certains autres sites pour relier les Bureaux entre eux (avec votre binôme de paillasse),

Il souhaiterait ainsi mettre en place les ajouts suivants :

1. Ajout d'un administrateur Read-Only appelé « Prestataire » dont le mot de passe sera à renseigner, ainsi que l'ajout d'un compte par Administrateur en super Admin,
2. La modification du Hostname et du fuseau horaire dans les paramètres système de la VM comme suis :
    a. Mise en place du bon fuseau horaire,
    b. Changement du Hostname par le nom de l'administrateurs gérant le cluster,
3. Un filtrage Web, DNS & Applicatif adapté à ses besoins (appliqué dans le sens réseau Bureau vers WAN) avec la politique suivante :
    a. Allow des catégories liées à la production et aux besoins de l'entreprise,
    b. Block des catégories non adaptées au travail et potentiellement répréhensibles,
    c. Monitoring du reste,
4. Mise en place d'un traitement Antivirus sur chaque règle pour tous les protocoles disponibles sauf les protocoles mails,
5. Ajouter un Web Rating Override pour allouer l'url www.ihaveabadreputation.com en tant que « General Business » → « Information Technology »,
6. Mises en place de mécanismes IPS cohérents monitorant les menaces de degré moyen et bloquant les plus critiques,
7. Implémentation des DNS choisis par l'entreprise 208.67.222.222 & 208.67.220.220,
8. Les fonctionnalités considérées comme étant inutiles seront masquées pour une meilleure exploitation future du Pare-feu,
9. (Bonus) Mise en place de politique de traffic shaping pour limiter la bande passante liée à YouTube à 1Mo par IP.
10. (Bonus) une page de blocage URL indiquant le type de blocage et le numéro du groupe concerné serait un plus.
11. (Bonus) la mise en place du télétravail avec votre voisin.

Une convention de nommage des objets et règles du Pare-Feu sera adoptée et respectée tout au long de la configuration.

Toute optimisation de la configuration compte tenu des besoins et de la situation de l'entreprise seront appréciées. Un rapport est attendu présentant la réalisation et les choix de configuration ainsi qu'un backup de la configuration ainsi qu'un cahier de recette fournissant les preuves de fonctionnement.