## A faire pour la compagnie A et la compagnie B.

1. Avec VirtualBox, faire un instantané de chaque VM avant de commencer les labs en les ayant au préalable arrêtés.

**Indications :**

* sous VirtualBox, cliquez droit sur les VMs en fonction, menu « Fermer » puis « Extinction par ACPI ».
* Pour chaque VM en surbrillance, cliquez sur le bouton « Instantanés » puis « Prendre », en donnant un nom à l’instantané come par exemple « Lab initial ».

1. Les pare-feu Stormshield sont en configuration usine. Connectez-vous à l’interface d’administration web.

**Indications :**

* Après avoir redémarré les VM, relancez le script sur les machines graphiques Debian pour les configurer avec le choix « sns »,
* Dans le navigateur Chromium de la VM graphique Debian, entrez l’URL <https://10.0.0254/admin>.

1. Sur les pare-feux, modifiez les préférences pour ne jamais être déconnecté en cas d'inactivité sur l’interface d'administration.

**Indications** :

* Cliquez sur le nom d’utilisateur, puis sur **Préférences** (icone avec une clé et un tournevis), sélectionnez ensuite dans la ligne **Déconnexion en cas d'inactivité** la valeur **Toujours rester connecté**.

1. Paramétrez la langue (traces et clavier) et le fuseau horaire de votre firewall et vérifiez que votre firewall est à l’heure après le redémarrage.

**Indications** :

* Langue et fuseau horaire : cliquez sur le menu **Système => Configuration** dans le menu de gauche. Commencez ici par configurer le fuseau horaire, ce qui nécessite un redémarrage du firewall. Par la suite, vous pouvez vérifier la date, l'heure (et la synchroniser avec celle de votre machine ), ainsi que la langue des messages générés par le firewall dans l’onglet **configuration générale**.

1. Activez le service SSH avec l'authentification par mot de passe.

**Indications** :

* Le SSH s'active depuis le menu **Système => Configuration =>** onglet **Administration du firewall** en cochant **Activer l’accès par SSH** et **Autoriser l’utilisation de mot de passe**.

1. Vérifiez la validité de votre licence et des éventuelles options disponibles, configurez la mise à jour automatique de votre licence avec une vérification hebdomadaire.

**Indications** :

* Les détails de la licence sont visualisables via le menu **Système => Licence** du menu de gauche. Dans les propriétés avancées, activez l’installation automatique de la licence.

1. Faites une sauvegarde de la configuration en local.

**Indications** :

* La sauvegarde de la configuration se fait dans le menu **Système => Maintenance =>** onglet **Sauvegarder**.

1. Modifiez le mot de passe de l’utilisateur « admin » (il faut choisir un mot de passe d’au moins 8 caractères).

**Indications** :

* La modification du mot de passe se fait dans le menu **Système => Administrateurs =>** onglet **Compte ADMIN**.

1. Vérifiez que le stockage local des logs est activé sur le disque dur de la VM.

**Indications** :

* L’activation du stockage local des logs peut être vérifiée dans le menu **Configuration => Notifications – Logs – Syslog – IPFIX**.

## NOTES :

Lors des labs, si vous levez une alarme « Attaque possible des ressources (connexion) », c’est que vous avez atteint le nombre de connexions maximum autorisé par la licence de la VM pédagogique. Dans ce cas, toutes les nouvelles connexions sont bloquées, patientez quelques minutes, le temps que la table des connexions se purge, pour revenir à un comportement normal.