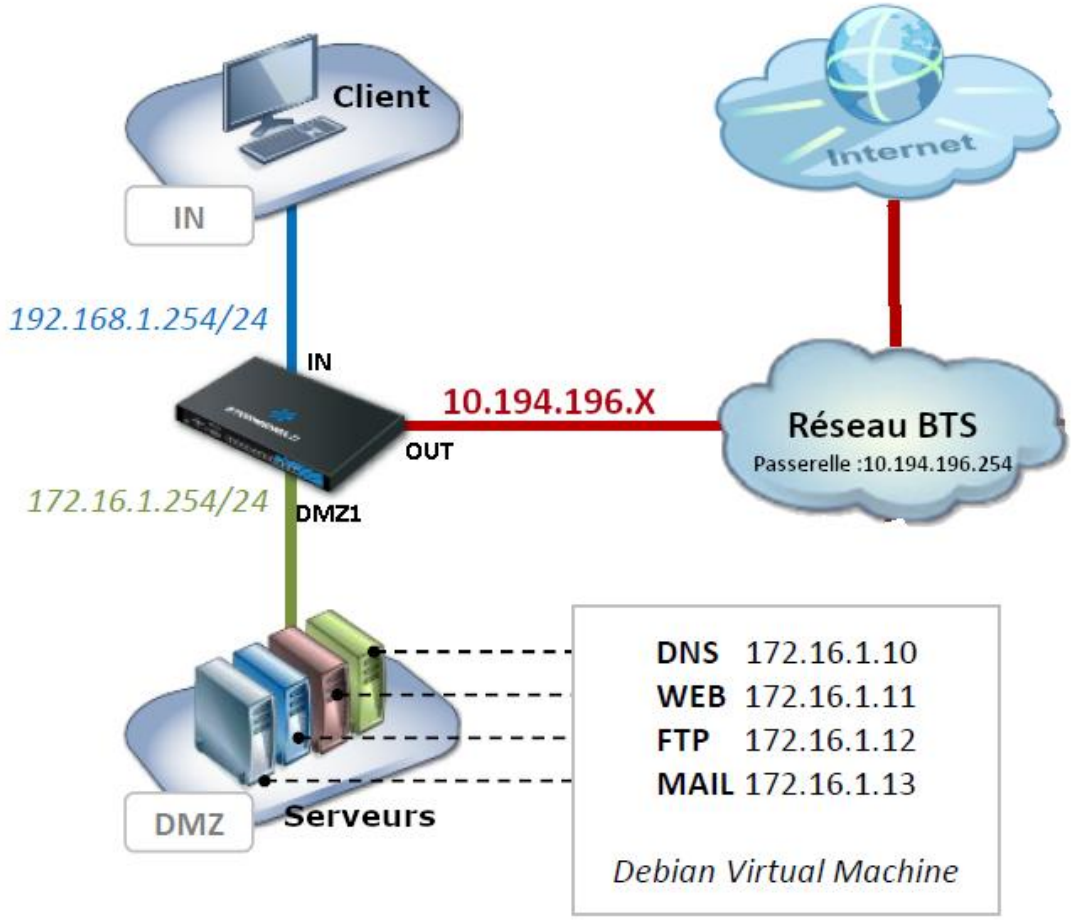
Activité 1
Prise en main du pare feu Stormshield

L'objectif de cette activité est de mettre en place la configuration de base pour un firewall EVA Stormshield.

1 – Présentation de l'infrastructure virtuelle



Notre structure composée de trois machines virtuelles représente l'architecture réseau d'une entreprise :

- **Un sous réseau 192.168.1.0/24** représente le réseau interne de l'entreprise. Il sera simulé par la VM (Machine Virtuelle) **Client**. Ce sous réseau sera connecté sur l'interface "IN" du pare-feu Stormshield.

- **Un sous réseau "DMZ1" 172.161.0/24** sur lequel on trouve un serveur DNS (172.16.1.10), un serveur WEB (172.16.1.11), un serveur FTP (172.16.1.12) et un serveur mail (172.16.1.13). Il sera simulé par la VM **Serveur**. Ce sous réseau sera connecté sur l'interface "DMZ1" du pare-feu Stormshield.

- Le pare feu Stormshield est installé sur une VM nommée **Pare-feu**. **L'interface "OUT" du pare-feu** sera connectée au même réseau que l'hôte sur le réseau 10.194.196.0/24 (Réseau Freebox).

Au total on aura besoin de trois machines virtuelles pour simuler ce réseau. Elles seront installées sur votre machine et vous utiliserez Virtual Box pour simuler les VM.

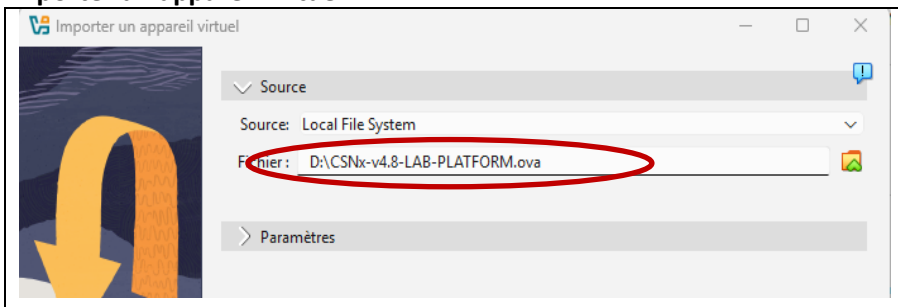
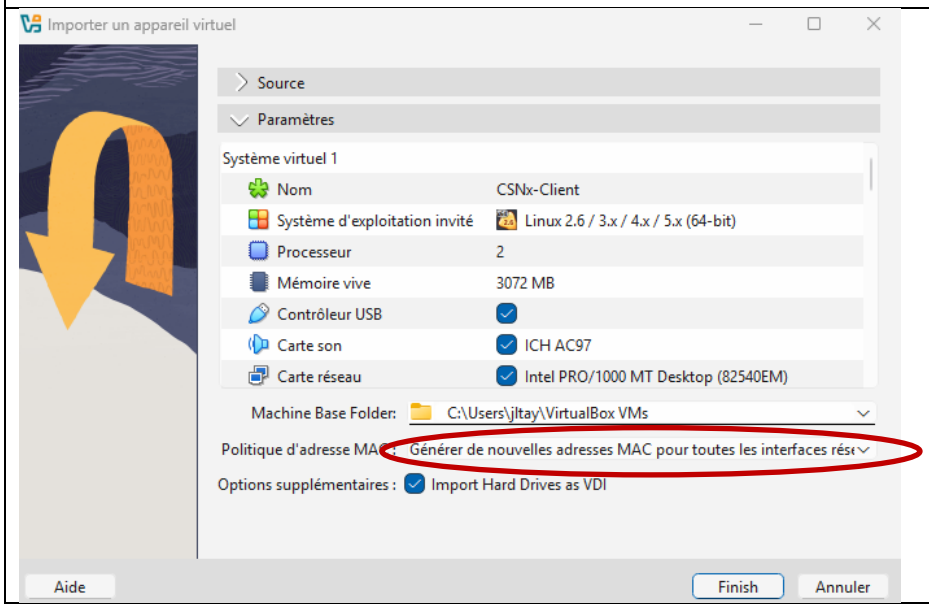
Installation et préparation de la plateforme virtuelle

☞ 1 – Installez VirtualBox s'il n'est pas installé sur votre ordinateur.

☞ 2 – Démarrer VirtualBox.

☞ 3 – Sous VirtualBox, rendez-vous dans le menu Fichier ⇒ Paramètres et cliquez sur le bouton **Expert** afin de débloquer les options avancées.

☞ 4 – Sous VirtualBox, importez le fichier **CSNx-v4.8-LAB-PLATFORM.ova** : menu Fichier, puis en sélectionnant **Importer un appareil virtuel**.

	Indiquez l'emplacement de ce fichier. Puis cliquez sur **Paramètres.**
	Sélectionner l'option **Générer de nouvelles adresses MAC pour toutes les interfaces réseau**. Cliquez sur **Finish**

VirtualBox va installer trois machines virtuelles :

- Client : **CSNx-client.ova**

- Pare-feu : **CSNx-SNS-Firewall.ova.** Le Firewall EVA importé est en configuration usine.

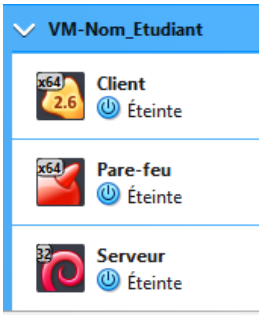
- Les serveurs : **CSNx-Server.ova**

☞ 5 – Renommez le groupe "VM_VotreNOM". Renommez les VM suivant l'exemple ci-dessus.

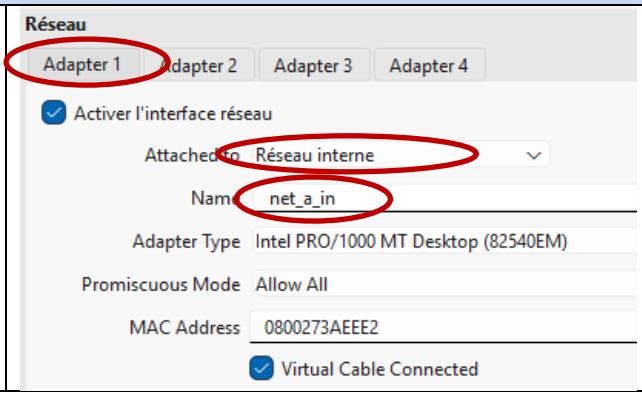
CSNx-client → Client

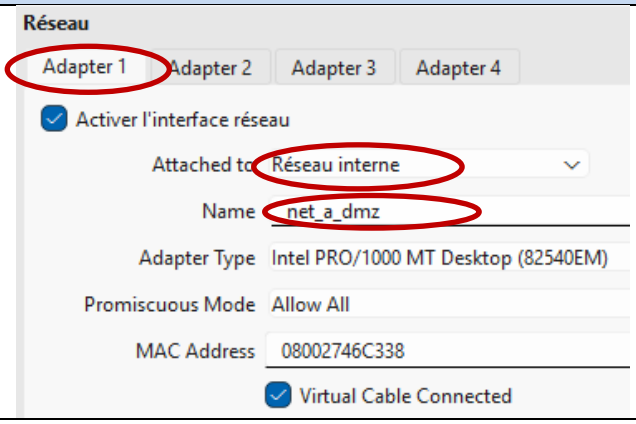
CSNx-SNS-Firewall → Pare-feu
(il faut faire la question 6 avant la modif)

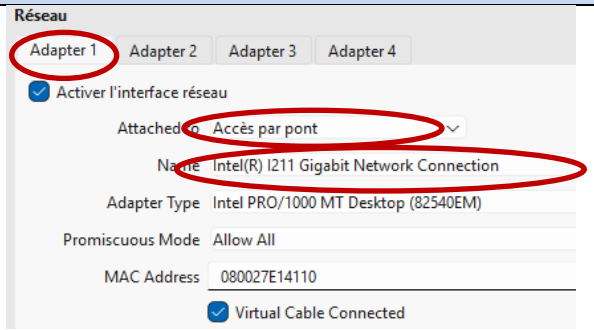
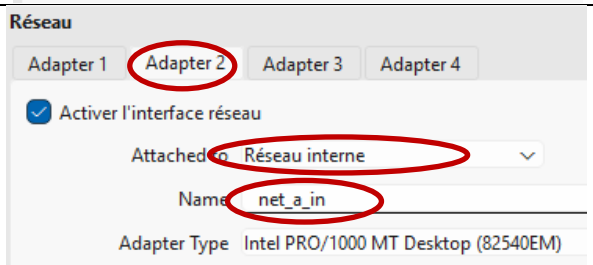
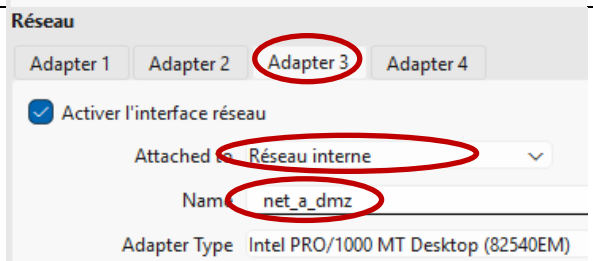
CSNx-Server → Serveur



☞ 6 – Vérifiez que les interfaces réseau des machines virtuelles sont correctement paramétrées.

Interface réseau VM Client	
Mode accès (Attached) : **Réseau interne** Adaptater 1 ⇒ **LAN_IN_A** Les adaptateurs 2, 3 et 4 ne seront pas utilisés. Adaptateur = carte réseau installée sur la VM	

Interface réseau VM Serveur	
Mode accès (Attached) : **Réseau interne** Adaptater 1 ⇒ **LAN_DMZ1_A** Les adaptateurs 2, 3 et 4 ne seront pas utilisés. Adaptateur = carte réseau installée sur la VM	

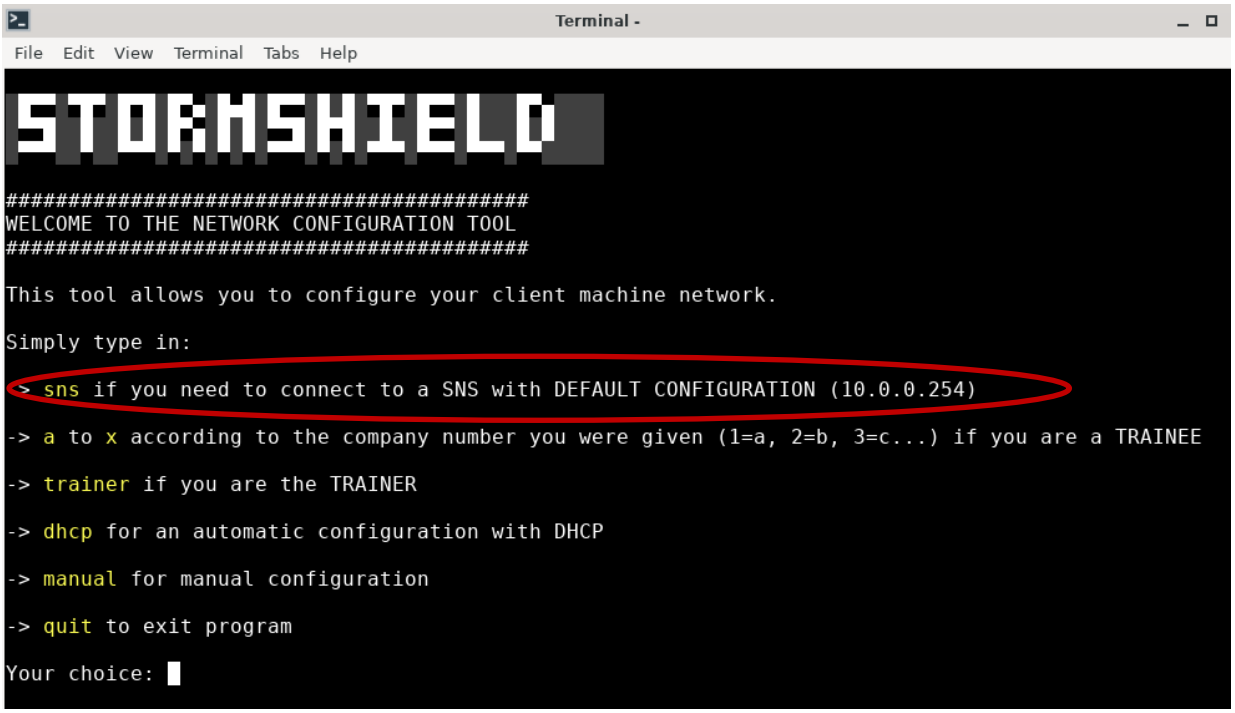
Interfaces réseau VM Pare-feu	
Le pare-feu dispose de trois carte réseaux. Une pour se connecter au réseau de la Freebox, une autre pour se connecter au Client et la dernière pour se connecter au Serveur. Adaptater 1 (interface OUT) ⇒ **Accès par pont** Préciser aussi le nom de la carte réseau connecté au réseau F**reebox** (ipconfig /all – Dans mon cas c'est "I211 Gigabit … ").	
Mode accès (Attached) : **Réseau interne** Adaptater 2 (interface IN) ⇒ **net_a_in**	
Mode accès (Attached) : **Réseau interne** Adaptater 3 (interface IN) ⇒ **net_a_dmz** L'adaptateur 4 ne sera pas utilisé.	

☞ 7 – Démarrez le **Pare-feu**.

La VM "**Pare-feu**" démarre avec un Stormshield EVA1 en config usine. Son adresse IP est 10.0.0.254. Le pare-feu est opérationnel lorsque "login :" s'affiche sur l'écran. Vous n'êtes pas obligé d'attendre la fin du démarrage pour passer à la question suivante.

☞ 8 – Démarrez la VM "**Client**".

Elle vous permettra de vous connecter au pare-feu. Il faut la configurer pour qu'elle soit dans le même réseau que le firewall. Après le démarrage, un script s'affichera sur le bureau de la VM client :



ATTENTION

La disposition du clavier est QWERTY. Pour passer en AZERTY cliquer sur l'option FR.

Remarque

Si vous souhaitez modifier la config ultérieurement, il vous faudra cliquer sur l'icône **Network Configuration** (bureau VM) pour relancer le script.

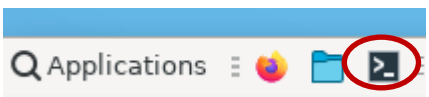
☞ 9 – Démarrer la VM **Serveur**.

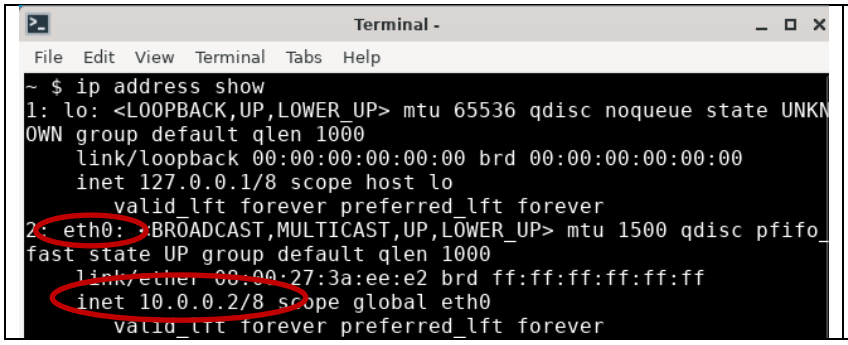
Après le démarrage, sélectionnez la lettre A afin de paramétrer ses adresses IP automatiquement.

- Serveur WEB :172.16.1.11
- Serveur FTP : 172.16.1.12
- Serveur mail : 172.16.1.13

☞ 10 – Revenez sur la VM **client**.

Vérifiez l'adresse IP de votre VM client. Dans le terminal, exécutez la commande "**ip address show**" (format raccourci "**ip a**").





Si vous n'avez pas une adresse IP 10.0.0.2 pour la VM client alors recommencez la configuration de la VM client (voir question 8).

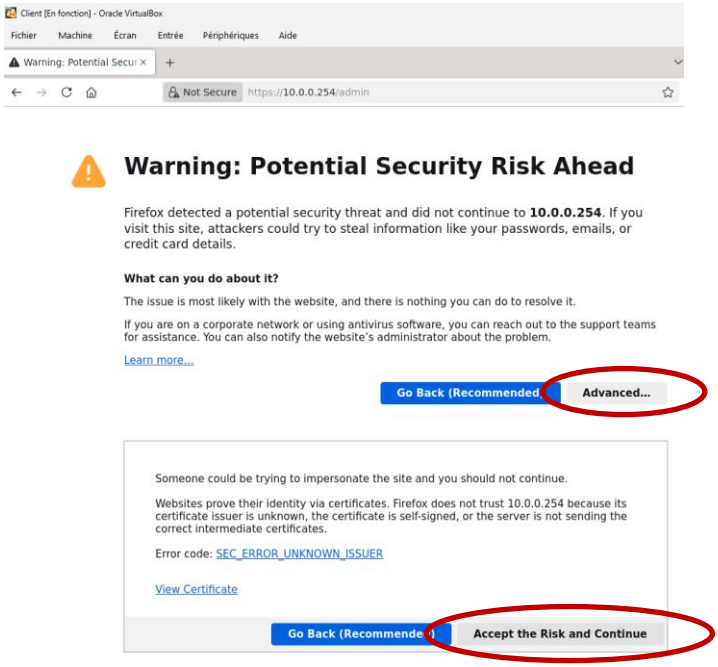
☞ 11 – Depuis la VM **Client**, faites un ping vers la VM **Pare-feu** (10.0.0.254) afin de vérifier la connectivité.

☞ 12 – Si le ping est réussi alors testez une connexion à l'interface graphique d'administration du pare-feu.

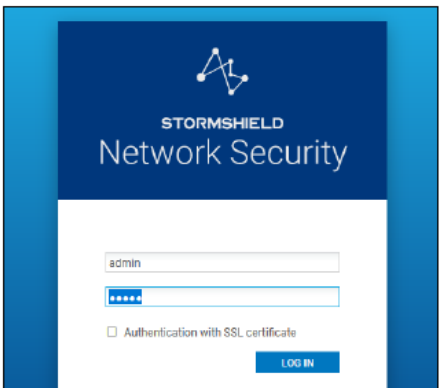
A partir d'un navigateur de la VM **Client**, connectez-vous à l'interface graphique d'administration du firewall :

https://10.0.0.254/admin

Il faudra valider le certificat



https://10.0.0.254/admin



Cliquez sur option et choisir "Français".

En configuration d'usine, il n'existe qu'un seul compte administrateur :

ID : **admin**
Mot de passe : **admin**

Bravo le Stormshield est accessible.

Puisque votre infrastructure est en place,
vous pouvez passer à l'activité 2 : configuration du firewall.

Remarque
Arrêtez les machines proprement, soit à partir de leur interface graphique pour les machines clientes et firewall, soit depuis VirtualBox en fermant les machines et en sélectionnant Envoyer le signal d'extinction.