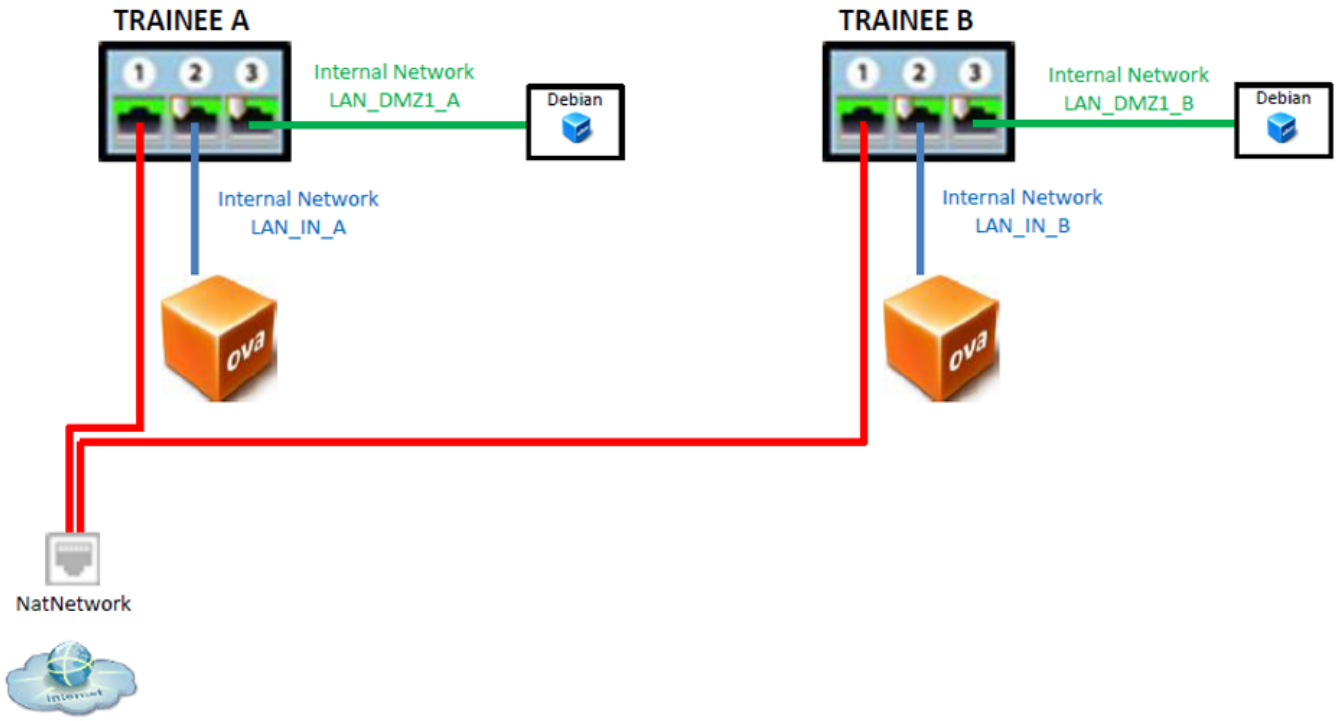
Stormshield : Activité Mise en place du lab

Présentation

Vous allez importer les archives sous VirtualBox et configurer les VMs pour obtenir l'infrastructures suivante :



Dans les informations fournies ci-après, il suffira de modifier le « x » suivant la lettre de l'agence à gérer :

- A⇒1,
- B⇒2,
- C⇒3...

Chaque agence est composée :

- d'un réseau externe **OUT** « 192.36.253.x0/24 » auquel les firewalls de toutes les agences sont connectés relié à l'interface OUT du pare-feu SNS ;
- d'un réseau interne **IN** Agence x « 192.168.x.0/24 » relié à l'interface **IN** du pare-feu SNS avec un poste utilisateur : machine virtuelle cliente linux fournie ou autre VM ;
- d'un réseau **DMZ** « 172.16.x.0/24 » avec des services (DNS, WEB, FTP, MAIL) intégrés dans la machine virtuelle Debian serveur fournie dans le kit Stormshield CSNA.

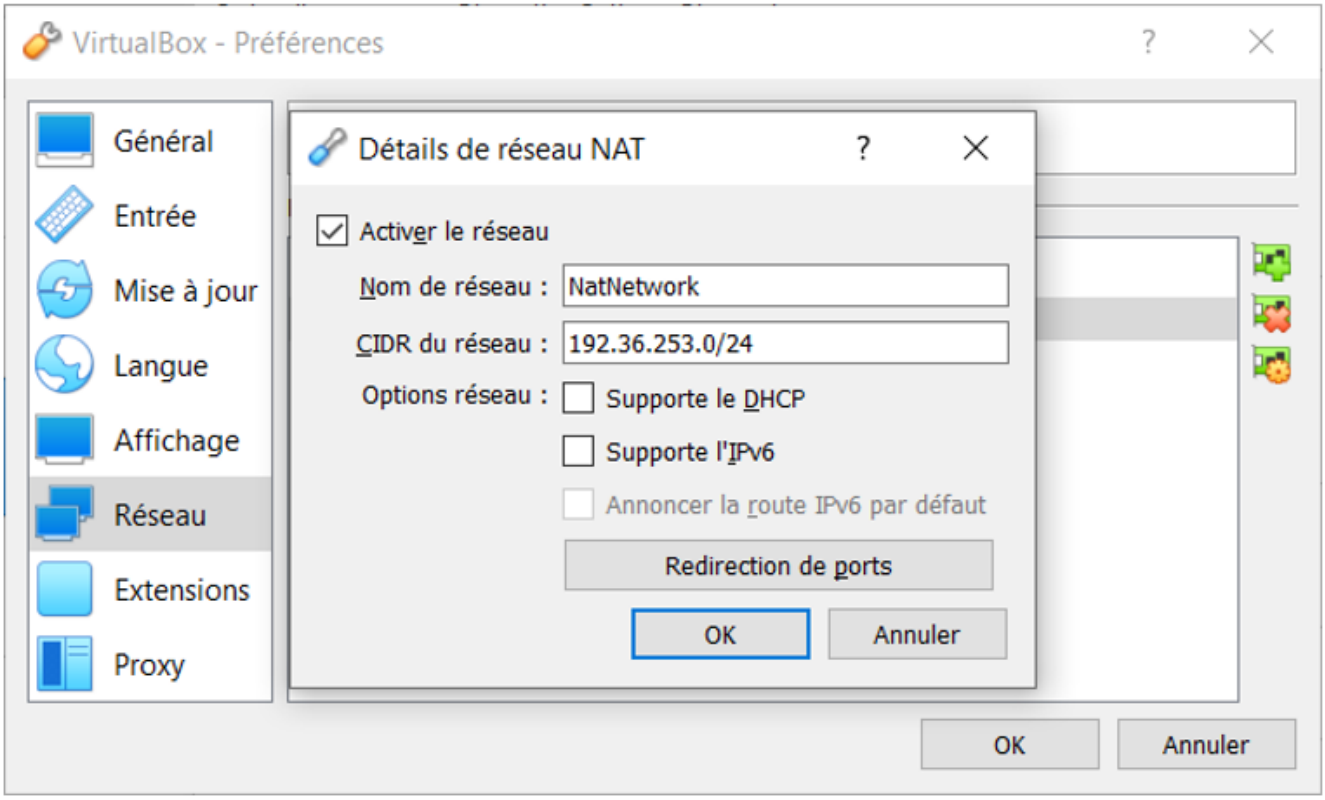
Configuration IP des interfaces du SNS Stormshield :

Interface	Adresse réseau	Adresse IP
m0 OUT	Réseau d'interconnexion « 192.36.253.x0 /24 »	192.36.253.x0 /24
em1 IN	Réseau interne Agence X « 192.168.x.0/24 »	192.168.x.254 /24
em2 DMZ1	Réseau DMZ « 172.16.x.0/24 »	172.16.x.254 /24

Importation des VM dans VirtualBox

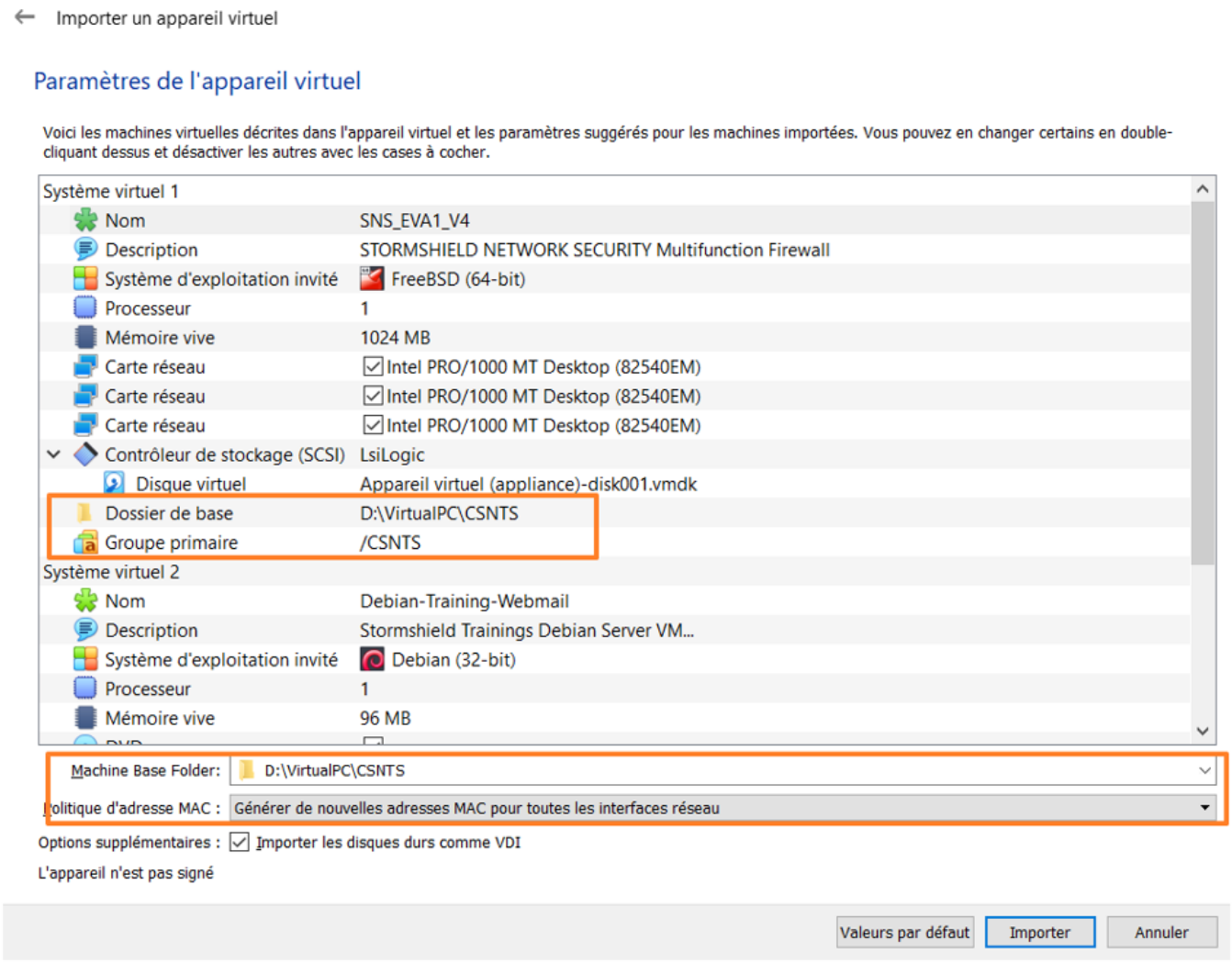
Tout d'abord il est nécessaire de créer dans VirtrualBox l'interface NatNetwork :

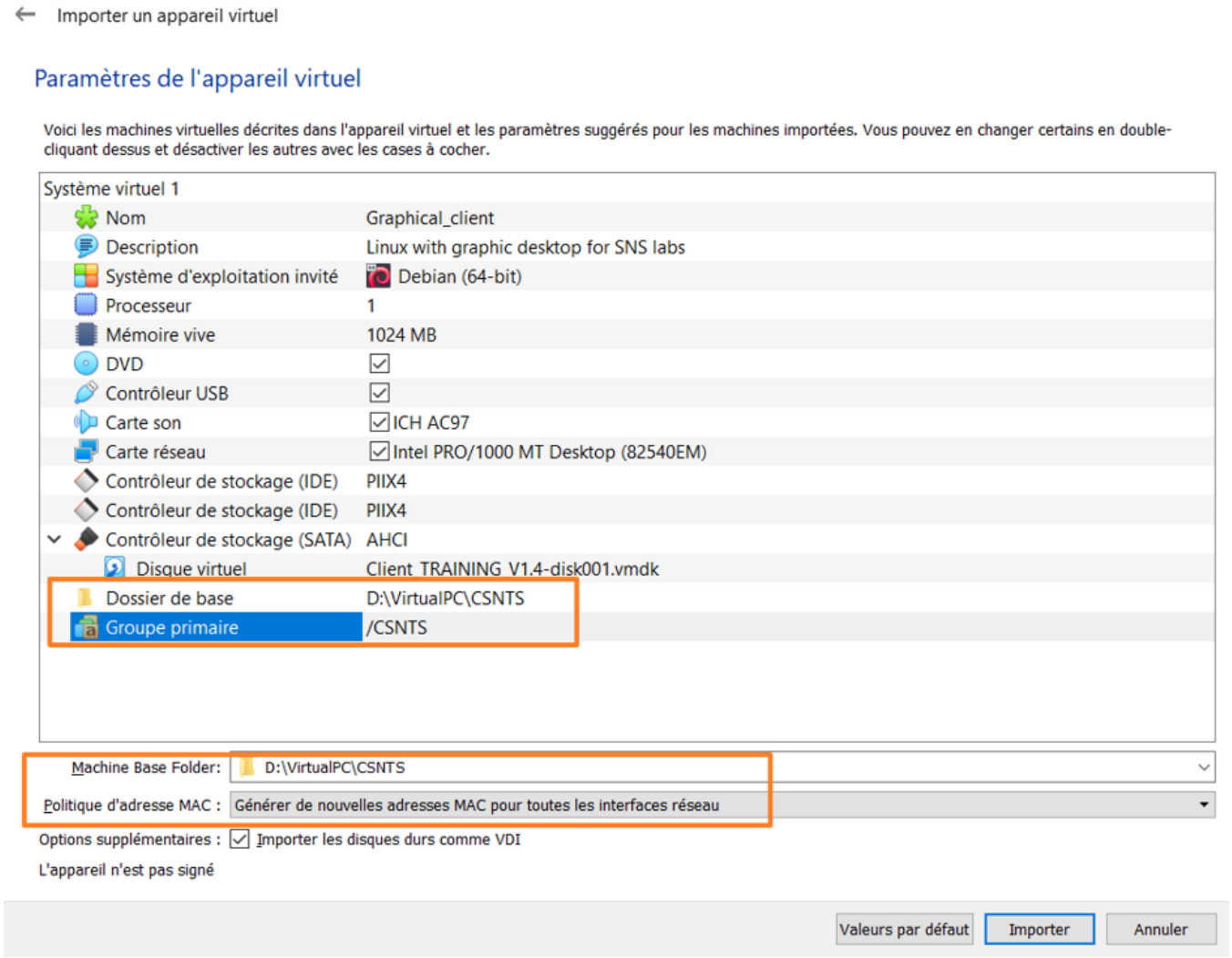
- menu > Paramètres > Réseau
- @réseau : 192.36.253.0/24
- Pas de DHCP



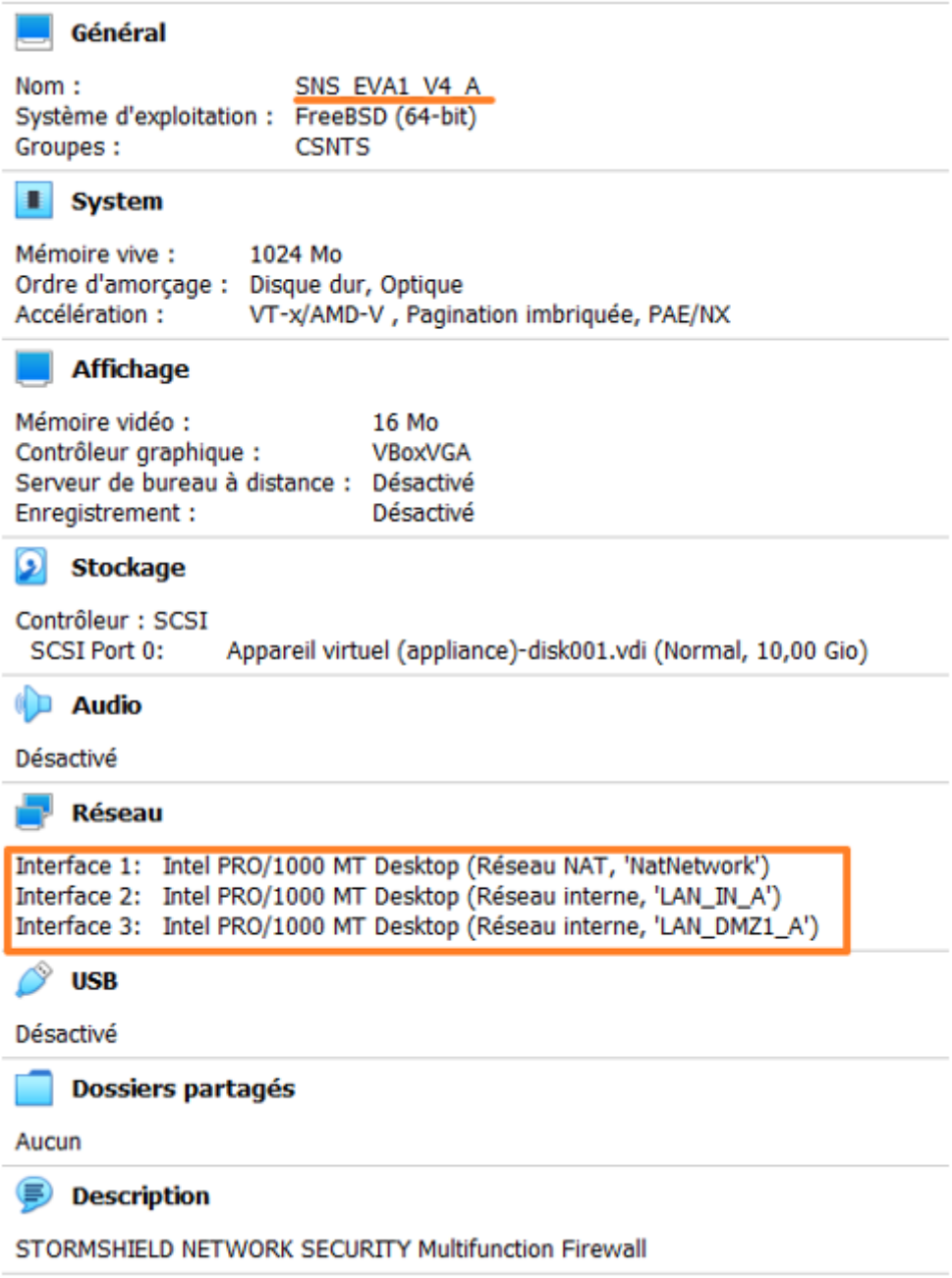
Création de l'agence A

- **Importez** le package **Plateforme-pedagogique-CSNx-v4-FW-DEBIAN.ova** dans VirtualBox en réinitialisant l'adresse MAC de chaque interface → Firewall en configuration usine.
- **Importez** la Debian Graphique à partir du package **Client*TRAINING*V1.4.ova**.

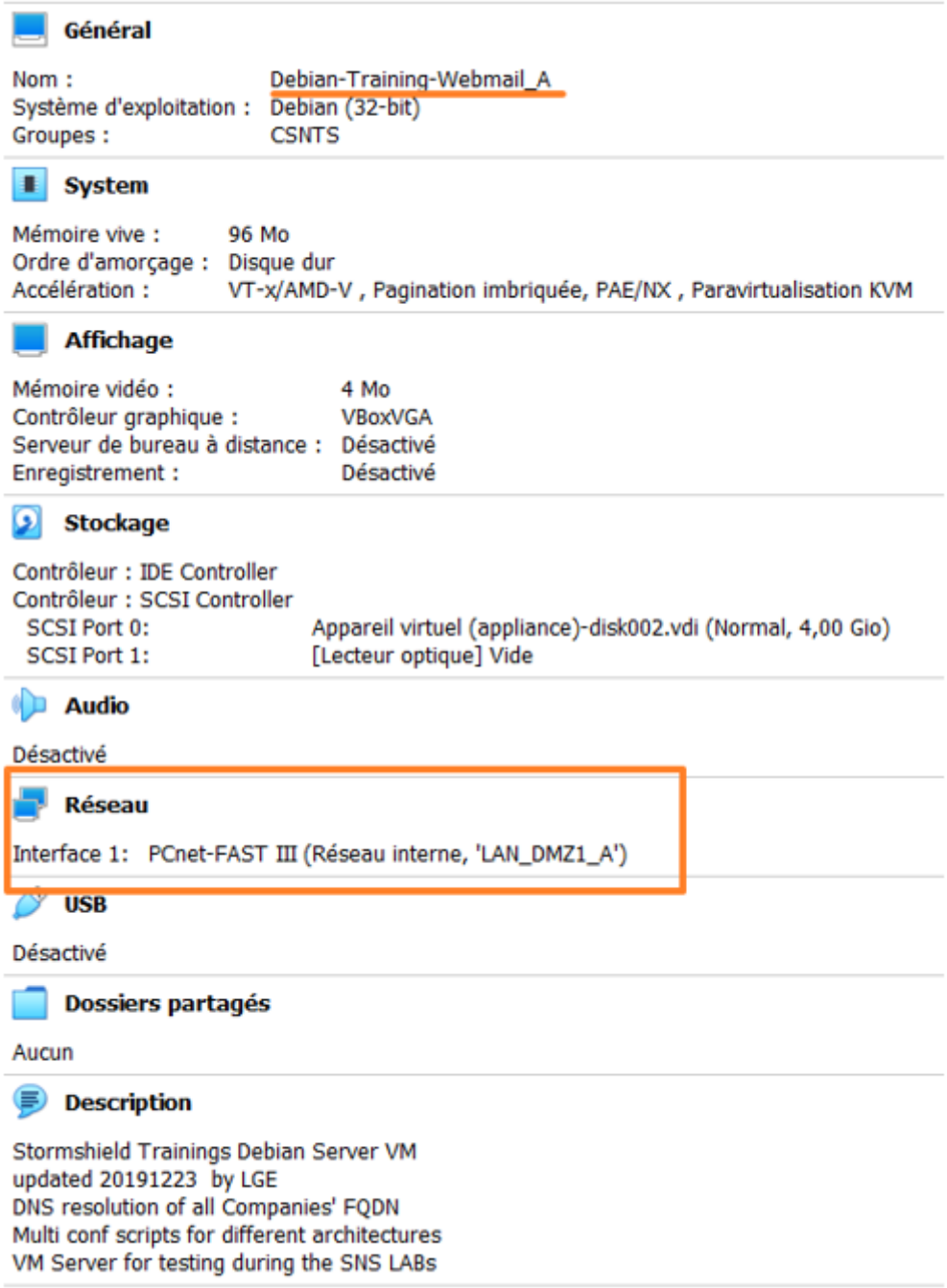

Importer un appareil virtuel
Paramètres de l'appareil virtuel
Voici les machines virtuelles décrites dans l'appareil virtuel et les paramètres suggérés pour les machines importées. Vous pouvez en changer certains en double-cliquant dessus et désactiver les autres avec les cases à cocher.
Système virtuel 1
Nom SNS_EVA1_V4
Description STORMSHIELD NETWORK SECURITY Multifunction Firewall
Système d'exploitation invité FreeBSD (64-bit)
Processeur 1
Mémoire vive 1024 MB
Carte réseau Intel PRO/1000 MT Desktop (82540EM)
Carte réseau Intel PRO/1000 MT Desktop (82540EM)
Carte réseau Intel PRO/1000 MT Desktop (82540EM)
Contrôleur de stockage (SCSI) LsiLogic
Disque virtuel Appareil virtuel (appliance)-disk001.vmdk
Dossier de base D:\VirtualPC\CSNTS
Groupe primaire /CSNTS
Système virtuel 2
Nom Debian-Training-Webmail
Description Stormshield Trainings Debian Server VM...
Système d'exploitation invité Debian (32-bit)
Processeur 1
Mémoire vive 96 MB
Machine Base Folder: D:\VirtualPC\CSNTS
Politique d'adresse MAC : Générer de nouvelles adresses MAC pour toutes les interfaces réseau
Options supplémentaires : Importer les disques durs comme VDI
L'appareil n'est pas signé
Valeurs par défaut
Importer
Annuler



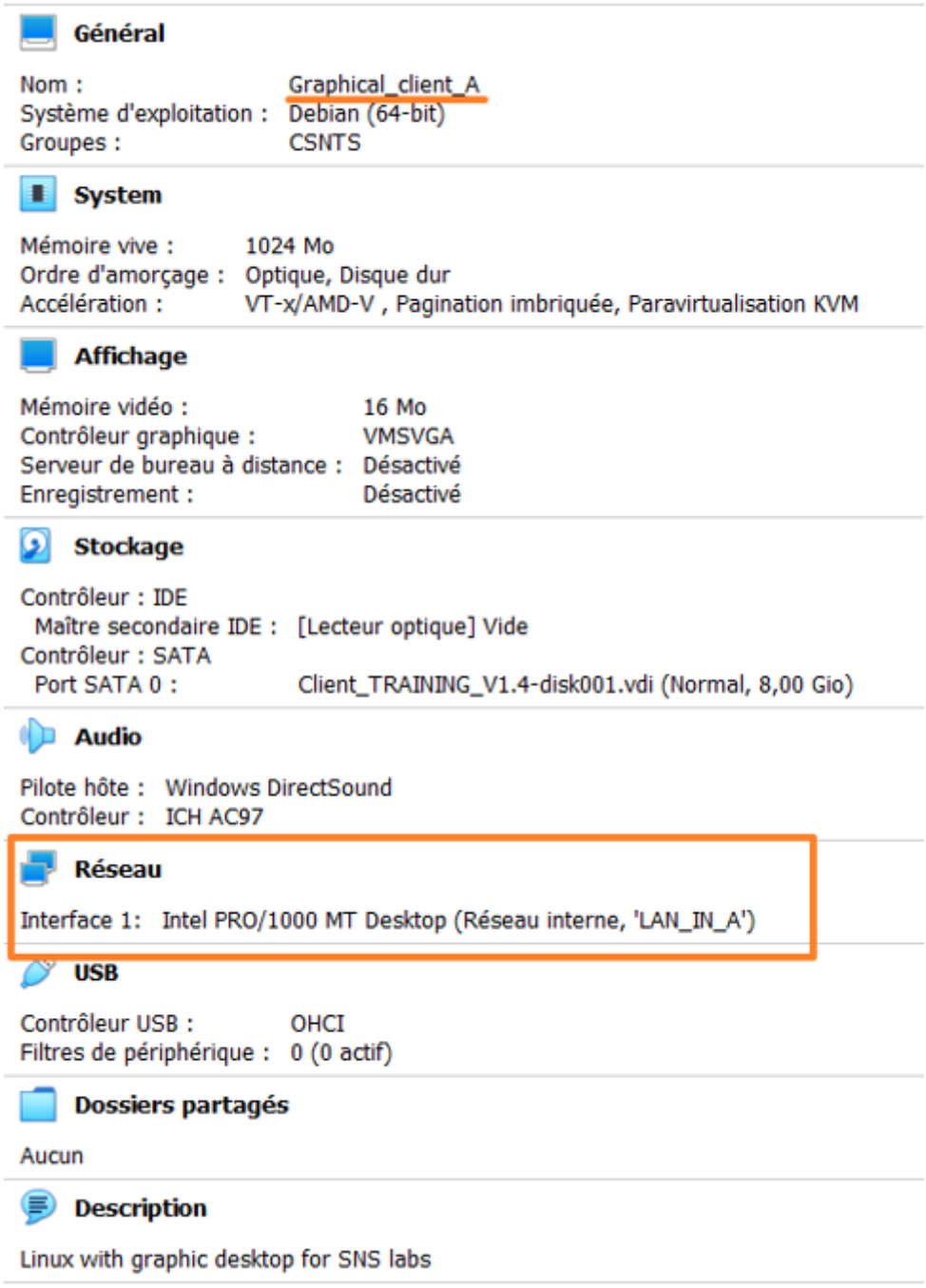
- Renommez les VM en suffixant par A ou B selon le site et vérifier les connexions réseaux.
- Interfaces du SNS :



- Interfaces du serveur Debian :



- Interfaces du client Debian graphique :

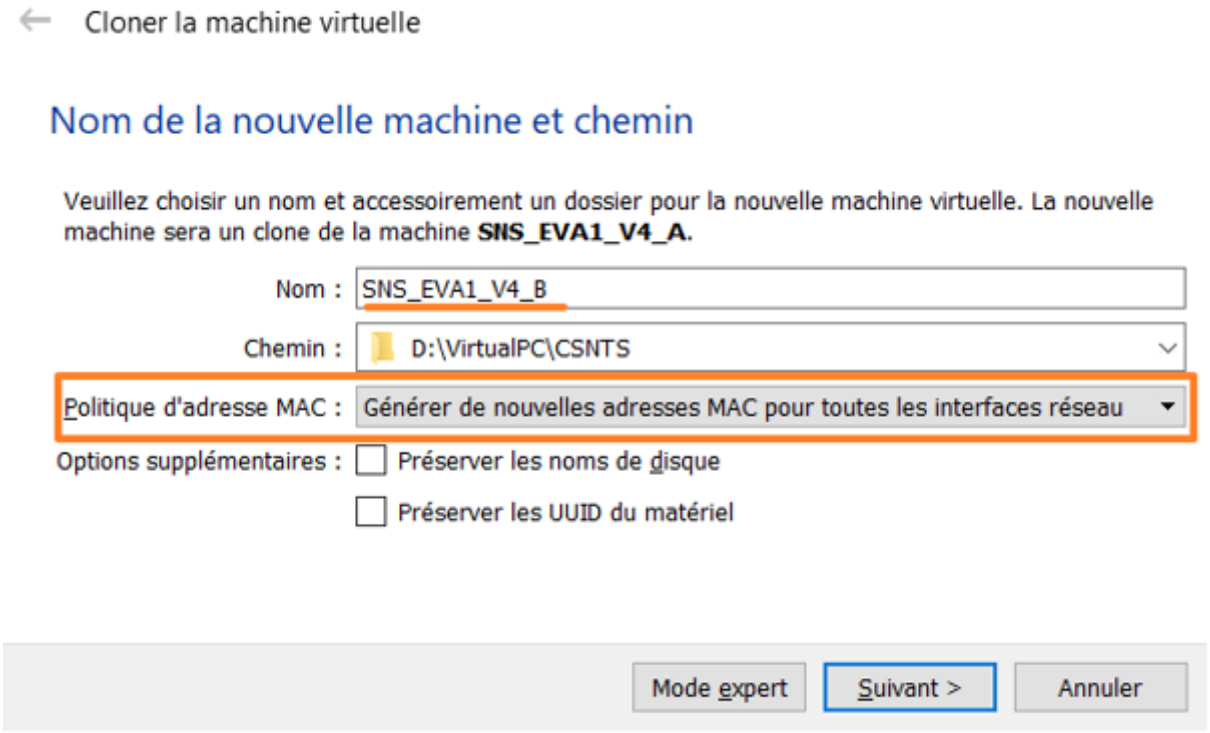


Création des snapshots

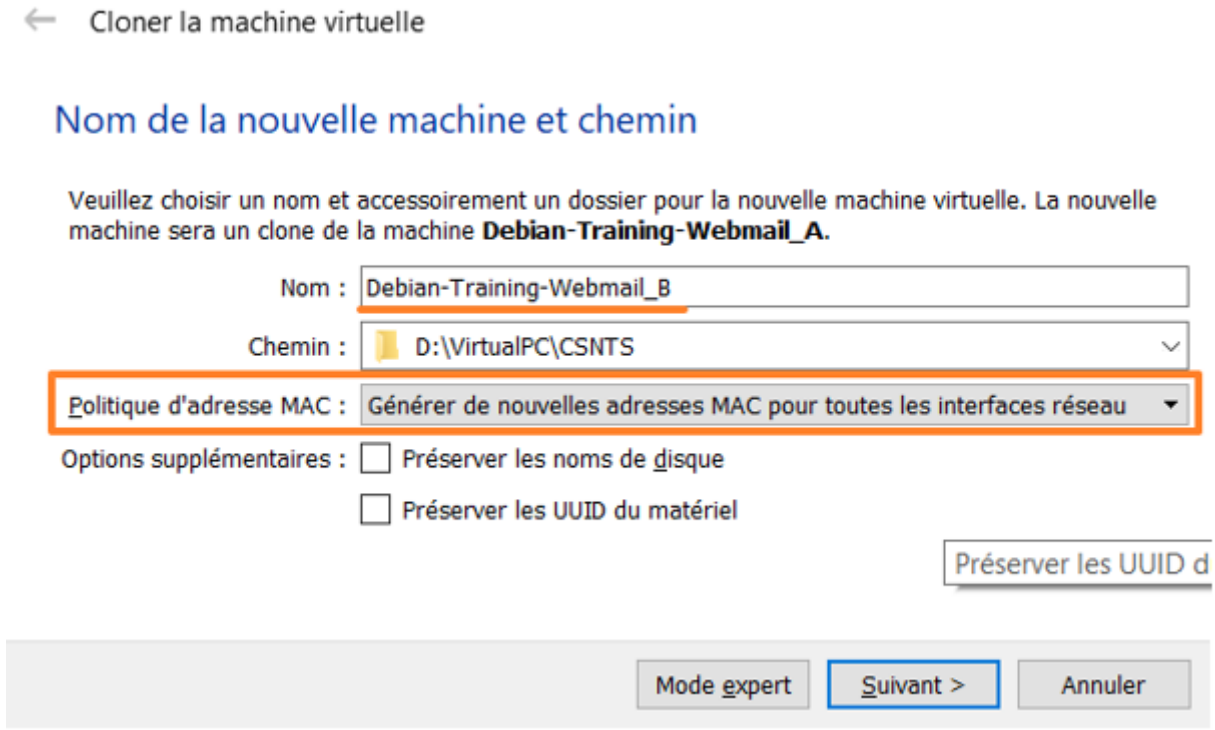
- Créez un snapshot des 3 VM

Test de bon fonctionnement

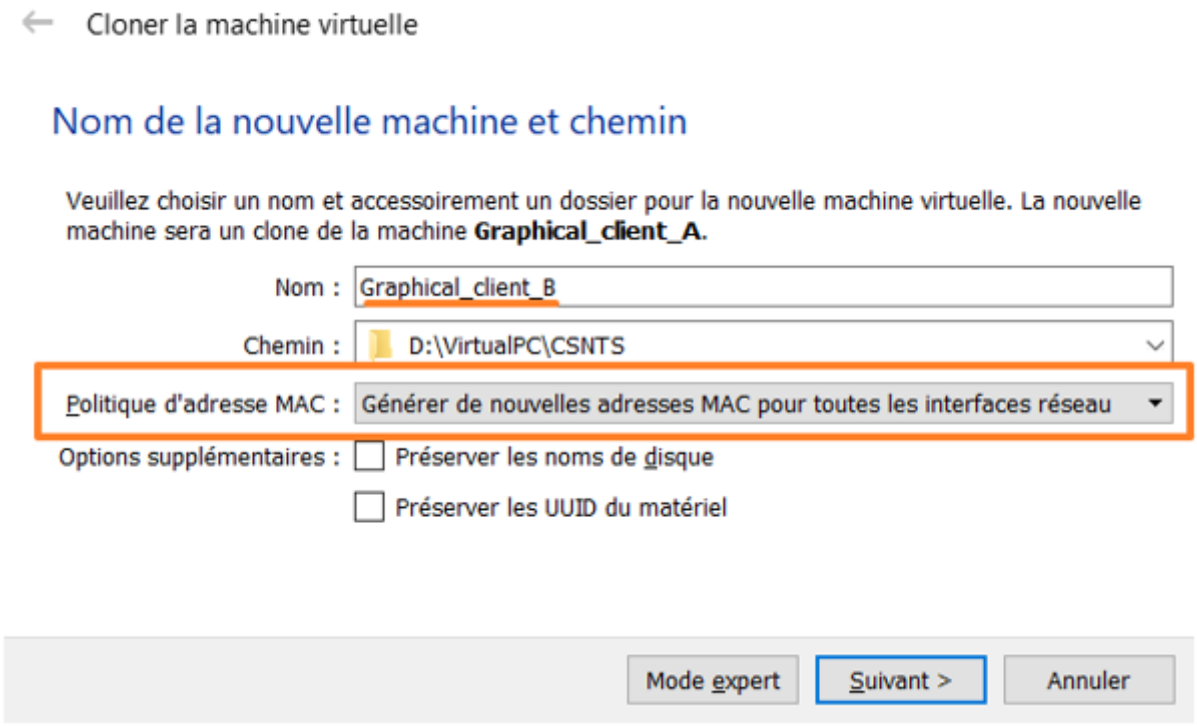
- Lancez le parefeu ***SNSEVA1V4A * Lancez GraphicalclientA ; * Ouvrez une session sur GraphicalclientA avec le compte user mot de passe user ; * Exécutez le script situé sur le bureau et qui se nomme networkconfig.sh : cliquez sur le bouton Run in Terminal et choisir SNS car le firewall est encore en mode usine : * Saisir Y puis sns ; le mot de passe par défaut est toor * Lancez le terminal et vérifier l'@IP (10.0.0.2/8) puis faite un ping vers 10.0.0.254 (SNS) * Depuis la VM GraphicalclientA connectez-vous à l'interface d'administration avec le navigateur à l'URL https://10.0.0.254/admin avec le compte admin et le mot de passe admin. ==== Création de l'agence B ==== * Clonez les 3 VM en clone intégral en cliquant-droit sur les VM : * Renommez les VM en les suffixant par B ; * Réinitialisez les adresses MAC ; * Modifiez les interfaces réseau en les suffixant par B. * Clone du SNS :***



* Clone du serveur Debian :



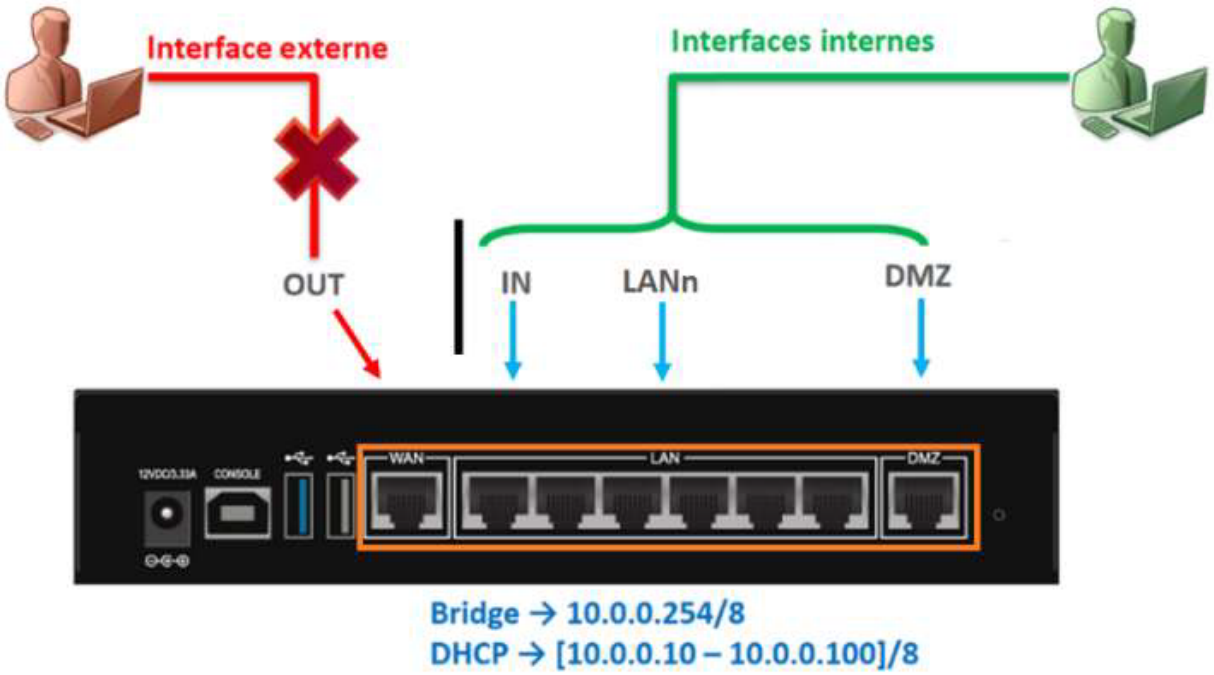
* Clone du client Debian graphique :



=== Création des snapshots === * Créez un snapshot des 3 VM === Test de bon fonctionnement === * Lancez le parefeu **SNS*EVA1V4B* *Lancez GraphicalclientB ; * Ouvrez une session sur GraphicalclientA avec le compte user mot de passe user ; * Exécutez le script situé sur le bureau et qui se nomme networkconfig.sh : cliquez sur le bouton Run in Terminal et choisir SNS car le firewall est encore en mode usine : * Saisir Y puis sns ; le mot de passe par défaut est toor * Lancez le terminal et vérifier l'@IP (10.0.0.2/8) puis faite un ping vers 10.0.0.254 (SNS) * Depuis la VM GraphicalclientB connectez-vous à l'interface d'administration avec le navigateur à l'URL https://10.0.0.254/admin avec le compte admin et le mot de passe admin. ===== Phase 1 Prise en main – configuration initiale ===== La configuration d'usine par défaut du pare-feu SNS (boîtier ou appliance VM laboratoire) est la suivante : * la première interface du pare-feu SNS physique est nommée « OUT », * la seconde « IN » * et le reste des interfaces « DMZx ». L'interface OUT est une interface externe qui est utilisée pour connecter le pare-feu SNS à Internet. Le reste des interfaces sont internes et servent principalement à connecter le pare-feu SNS à des réseaux locaux internes.***

> La distinction **interne/externe** pour les interfaces du SNS permet de se protéger contre les attaques d'usurpation d'adresse IP.

Toutes les interfaces sont incluses dans un **bridge** dont l'adresse est **10.0.0.254/8**. Un **serveur DHCP** est actif sur toutes les interfaces du bridge et il distribue des adresses IP comprises entre **10.0.0.10 et 10.0.0.100**. L'accès à l'interface web de configuration du pare-feu SNS se fait avec l'url : https://10.0.0.254 Par défaut, seul le compte système **admin** (mot de passe par défaut **admin**), disposant de tous les privilèges sur le boîtier, existe et peut se connecter.



===== Retour Accueil Stormshield ===== * Stormshield