



Programme du module

- → Présentation de la plateforme de Lab
- → Lab Mise en place de la plateforme de Lab



Les labs seront effectués en virtuel sous VirtualBox. La plateforme des labs est présentée ci-dessus, elle est constituée de 2 sites (Agence A et Agence B) reliés entre eux via un réseau externe « 192.36.253.0/24 ».

Chaque site possède :

- un firewall virtuel SNS\_EVA1\_V4.3
- une machine Debian\_Server\_dmz1 qui embarque 4 serveurs (DNS, WEB, FTP et MAIL), connectée au réseau privé DMZ « 172.16.X.0/24 »
- une machine graphique Debian\_Client\_in, connectée au réseau privé IN « 192.168.X.0/24 ».

NOTE : Sur tous les firewalls, le mot de passe de l'utilisateur « admin » est « admin ».





La configuration réseau des machines virtuelles est décrite sur la figure ci-dessus. Elle permet d'accéder à l'interface Web du firewall SNS d'un site depuis la machine graphique Debian\_Client\_in. Elle permet également aux firewalls de se connecter à Internet via l'interface « NatNetwork ».

**NOTE** : Le réseau VirtualBox « NatNetwork » doit être créé et configuré avant de démarrer les machines virtuelles.

Les réseaux « Internal\_Networks » sont déployés par import de l'OVA.

**PRÉREQUIS** : L'infrastructure virtuelle complète décrite ci-dessus nécessite un espace disque minimum de 11,5 Go (les VM fournies ont des disques à allocation dynamique) et une mémoire RAM de 4,2 Go

- 1024 Mo de RAM par firewall,
- 96 Mo de RAM par Debian\_Server\_dmz1,
- 1024 Mo de RAM par Debian\_Client\_in, nous vous recommandons de multiplier cette valeur par 2, 3 ou 4 si la RAM disponible sur votre hôte physique le permet.





## Installation et préparation de la plateforme virtuelle

- 1. Installez Virtualbox (nos labs sont compatibles avec les versions 5.2 ou ultérieure, les captures d'écran ci-après ont été faites sur la version 6.1.34).
- Créez l'interface « NatNetwork » depuis VirtualBox dans le menu Fichier ⇒ Paramètres ⇒ Réseau ⇒ onglet Réseau NAT, configurez la avec le réseau WAN « 192.36.253.0/24 » et désactivez l'option « supporte le DHCP ».



- Importez le package « CSNx-v4.3-FW-DEBIANS.ova » contenant un firewall et les deux Debian, depuis le menu VirtualBox « Fichier ⇒ Importer un appareil virtuel » ⇒ cochez la case « Réinitialisez l'adresse MAC de chaque carte réseau ». Le Firewall est en configuration usine.
- Pour un fonctionnement correct de la machine Debian\_Client\_in, dans le menu Configuration ⇒ Système ⇒ Carte mère, cochez la case « Activer les IO-APIC », si elle ne l'est pas.

File Machine Help	New Settings Discard Start		
✓ OVA_virtual_lab	😳 Debian_Client_in_A - Setting	5	?
SNS_EVA1_V4.3_A Powered Off Debian_Client_in_A Powered Off Debian_Server_dmz1_A Powered Off	General System   System Mother   Display E   Storage Audio   Network Serial Ports   VISB Poil   Shared Folders Extender   User Interface Storage	thoard Processor Acceleration ase Memory: 4MB Boot Order: 4MB Boot Order: 4MB Boot Order: 4MB Boot Order: 4MB Boot Order: 4MB Floppy 0 Optical Network Chipset: PIIX3 Chipset: PIIX3 Enable I/O APIC Enable EFI (special OSes only) Hardware Clock in UTC Time	1024 MB €





5. Vérifiez ou configurez les interfaces réseau des VM selon le schéma de la diapositive n°3. Ces machines sont sur le site de l'agence A.



- 6. Clonez chaque VM, en cliquant droit sur une VM ⇒ Cloner. Dans l'assistant qui se lance, renommez votre clone (les VM clonées seront sur le site de Trainee B) et cochez la case « Réinitialisez l'adresse MAC de chaque carte réseau ». Sur la page suivante, cochez la case « Clone intégral » et cliquez sur le bouton cloner (au lieu de cloner, il est également possible d'importer à nouveau le package OVA, le renommage des VM s'effectue alors après import).
- 7. Modifiez les interfaces réseau pour les 3 machines clonées, LAN\_IN\_A et LAN\_DMZ1\_A sont renommées respectivement LAN\_IN\_B et LAN\_DMZ1\_B.
- 8. Effectuez un instantané de chaque VM avant de commencer les labs (avec Oracle VirtualBox, faites l'instantané VM éteinte).







9. Démarrez les VM « SNS\_EVA1\_V4\_A » et « Debian\_client\_in\_A ». Sur cette dernière, ouvrez une session (identifiant : user ; mot de passe : user) et double cliquez sur le raccourci bureau «network\_config.sh », puis cliquez sur le bouton « Run in Terminal ». Le firewall SNS étant encore en mode usine, l'option « sns » doit être choisie.

Note : Si l'une des machines ne démarre pas, le passage à 2 CPU peut parfois résoudre ce problème (paramètre System -> Processor.)

Terminal – 🗆	×
File Edit View Search Terminal Help	
Do you need to reconfigure the services for STORMSHIELD Training LABs ? [Y N]	-
<pre>y Choose your company name in conformance with the letter you were given valid values are [ a b c d e f g h i j k l m n o p q r s t u v w x ] If you are the Trainer please type in "trainer" without the double quotes If you need to connect to a default config SNS (10.0.0.254) please type in "sns without the double quotes</pre>	- 0
sns	
OK, you chose default config	
Please give root password, default is 'toor' :	
Password:	+
9. En lançant un terminal, vous pouvez vérifier que l'IP de votre carte réseau es	t

De lançant un terminal, vous pouvez verifier que l'IP de votre carte reseau est correcte avec la commande « ip address show » (format raccourci « ip a »), et lancer un ping vers 10.0.0.254 (la connectivité avec le SNS est bien établie).

us	er@cllent-training:~\$ ip a
1:	lo: <loopback,up,lower up=""> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000</loopback,up,lower>
	link/loopback 00:00:00:00:00 brd 00:00:00:00:00:00
	inet 127.0.0.1/8 scope host lo
	valid lft forever preferred lft forever
2:	enp0s3: <broadcast,multicast,up,lower_up> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000</broadcast,multicast,up,lower_up>
	<u>link/ether 08:00:27:47:27:61 brd ff:f</u> f:ff:ff:ff:ff
	inet 10.0.0.2/8 scope global enp0s3
	valid_lft forever preferred_lft forever

10. Recommencez les points 9 et 10 avec les VM du site B.



Nous vous invitons à imprimer et compléter cette page afin d'avoir les informations des Labs à disposition.

## Informations

Les labs seront effectués à l'aide d'une infrastructure composée de plusieurs sites. Chaque site représente ici une compagnie qui possède trois machines :

- Un poste client Windows permettant de naviguer sur Internet et configurer le SNS
- Un firewall Stormshield Network Security (SNS) virtuel (EVA) ou physique (SN310) •
- Un serveur Debian qui embarque 4 serveurs (DNS, WEB, FTP et MAIL)

Les compagnies sont nommées par une lettre A, B, C, D, etc. et un chiffre, respectivement 1, 2, 3, 4, etc. qui servira dans la définition des adresses IP.

Deux réseaux privés (net-in-x et net-dmz-x, où x représente la lettre du site) sont configurés sur chaque site : IN « 192.168.y.0/24 » et DMZ : « 172.16.y.0/24 » (où y représente le numéro associé à la compagnie).

Les différents sites sont reliés directement à Internet et possèdent des adresses IP publiques dans la plage 192.36.253.10 à 192.36.253.249. Le reste d'Internet est accessible via le firewall du formateur dont l'adresse IP est 192.36.253.254.

## Adresses IP

Je suis compagnie \_\_\_\_\_ (lettre) numéro \_\_\_\_



Serveurs Debian	Firewall Stormshield	
Serveur DNS :	Adresse IP net-DMZ :	
	172.16254	
Serveur web :	Adresse IP publique :	
11	192.36.2530	
Serveur FTP :	Adresse IP net-IN :	
12	192.168 254	
Serveur mail :		
13		



Poste client Adresse IP : 192.168 .\_\_\_\_. 2 Lab

