Compte rendu du TP - Architecture sécurisée:

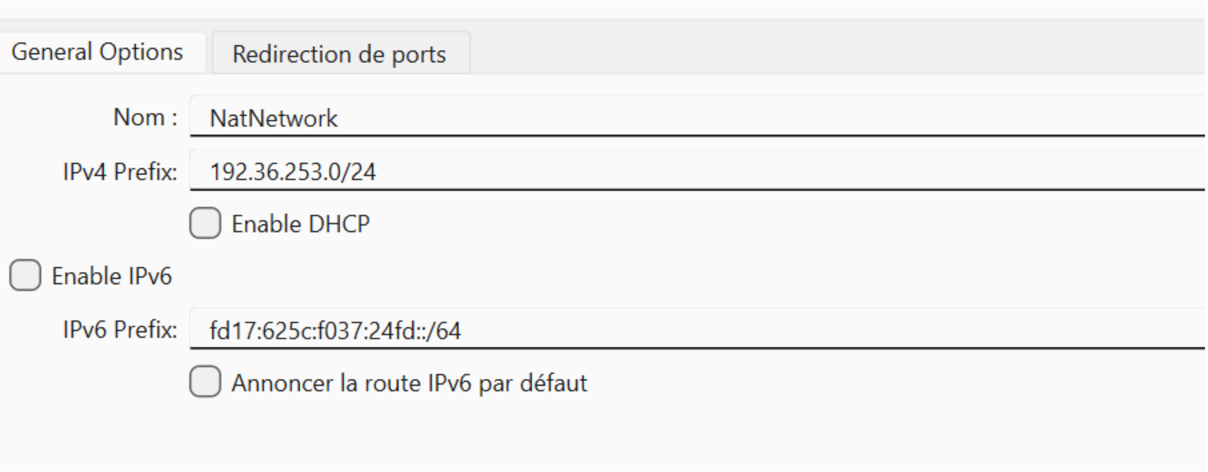
TP VIRTUAL LABS

UNIVERSITÉ SORBONNE PARIS NORD

AWA SALIF DOUMBIA

Installation et préparation de la plateforme virtuelle :

1-Créer le réseau NATNetwork (WAN)



Nom : NatNetwork

IPv4 Prefix: 192.36.253.0/24

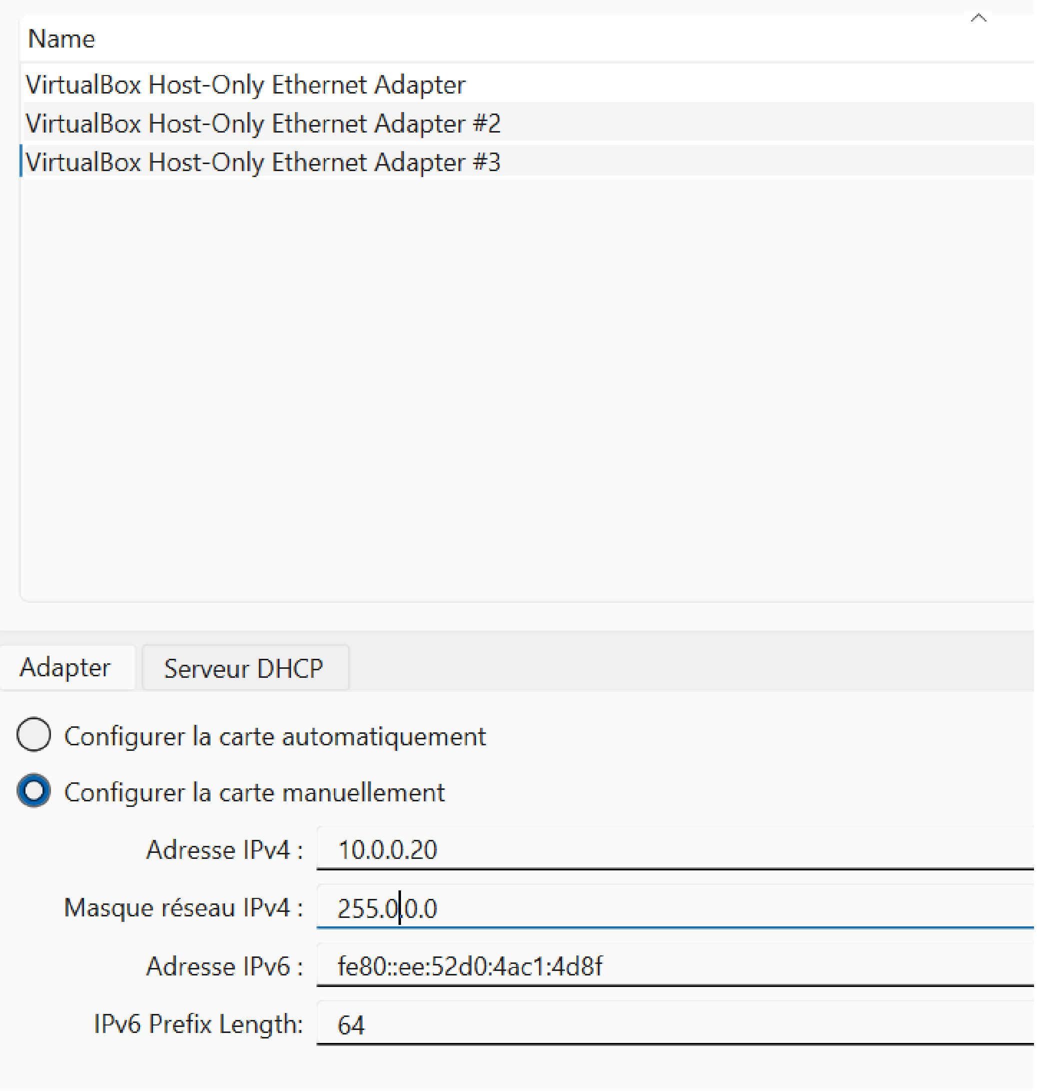
□ Enable DHCP

□ Enable IPv6

IPv6 Prefix: fd17:625c:f037:24fd::/64

□ Annoncer la route IPv6 par défaut

2-Créer les interfaces "Host-only" (si tu n'utilises pas la VM graphique Stormshield)



Name
VirtualBox Host-Only Ethernet Adapter
VirtualBox Host-Only Ethernet Adapter #2
VirtualBox Host-Only Ethernet Adapter #3

○ Configurer la carte automatiquement

● Configurer la carte manuellement

Adresse IPv4 : 10.0.0.20

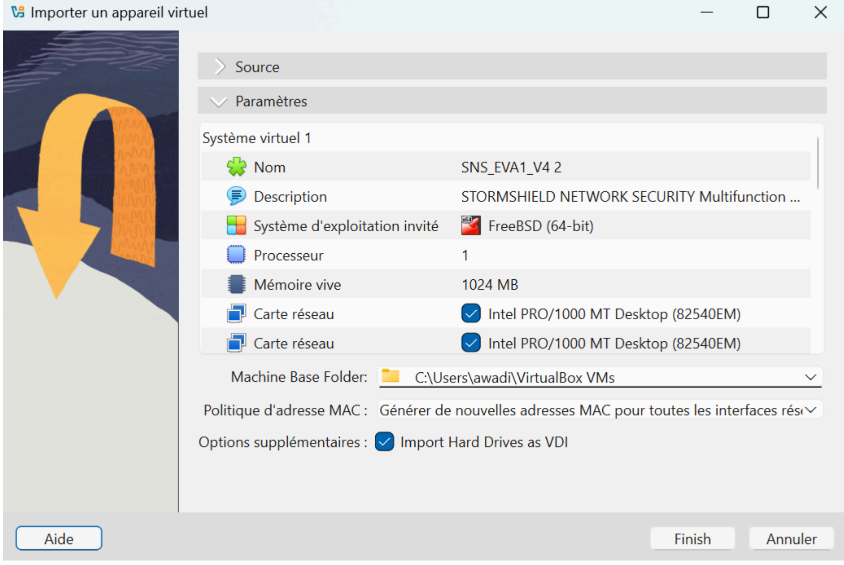
Masque réseau IPv4 : 255.0.0.0

Adresse IPv6 : fe80::ee:52d0:4ac1:4d8f

IPv6 Prefix Length: 64

N

3-Importer les VMs:



Importer un appareil virtuel

Système virtuel 1

Nom	SNS_EVA1_V4 2
Description	STORMSHIELD NETWORK SECURITY Multifunction ...
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)

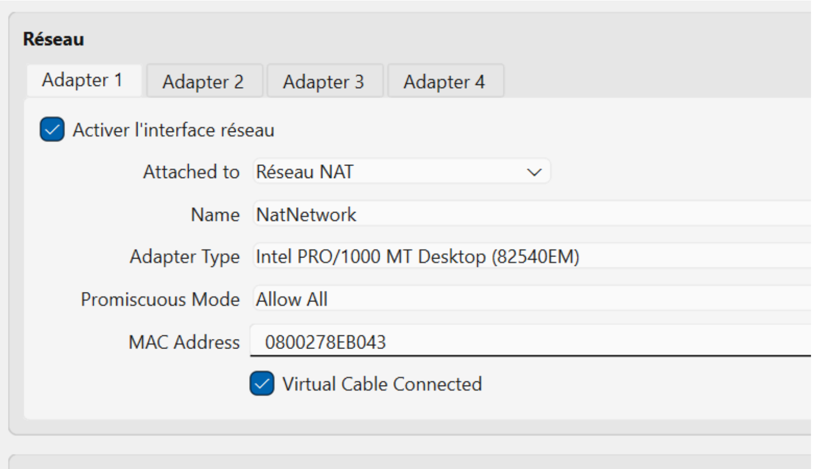
Machine Base Folder: C:\Users\awadi\VirtualBox VMs

Politique d'adresse MAC : Générer de nouvelles adresses MAC pour toutes les interfaces rés

Options supplémentaires : ☑ Import Hard Drives as VDI

4- Configuration réseau des VMs:

SNS:



Réseau

☑ Activer l'interface réseau

Attached to: Réseau NAT

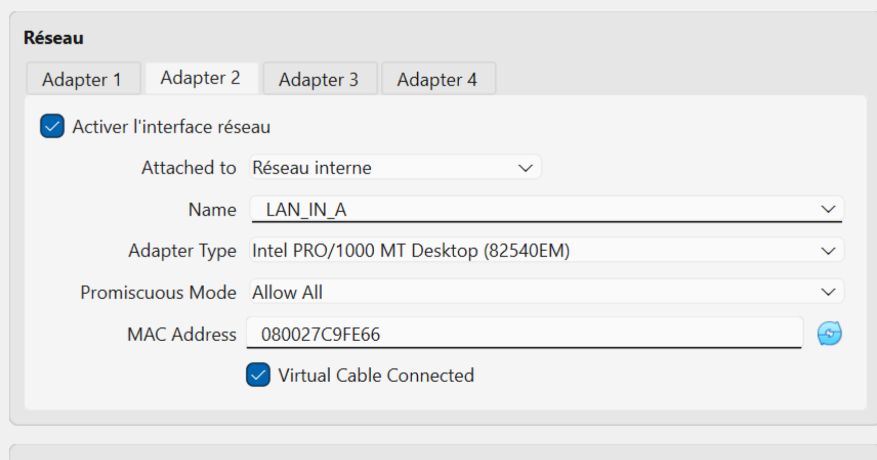
Name: NatNetwork

Adapter Type: Intel PRO/1000 MT Desktop (82540EM)

Promiscuous Mode: Allow All

MAC Address: 0800278EB043

☑ Virtual Cable Connected



Réseau

☑ Activer l'interface réseau

Attached to: Réseau interne

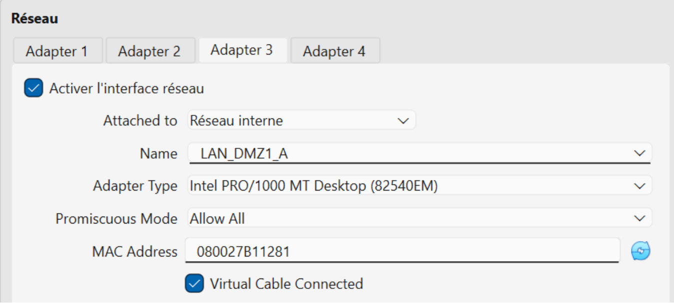
Name: LAN_IN_A

Adapter Type: Intel PRO/1000 MT Desktop (82540EM)

Promiscuous Mode: Allow All

MAC Address: 080027C9FE66

☑ Virtual Cable Connected



☑ Activer l'interface réseau

Attached to: Réseau interne

Name: LAN_DMZ1_A

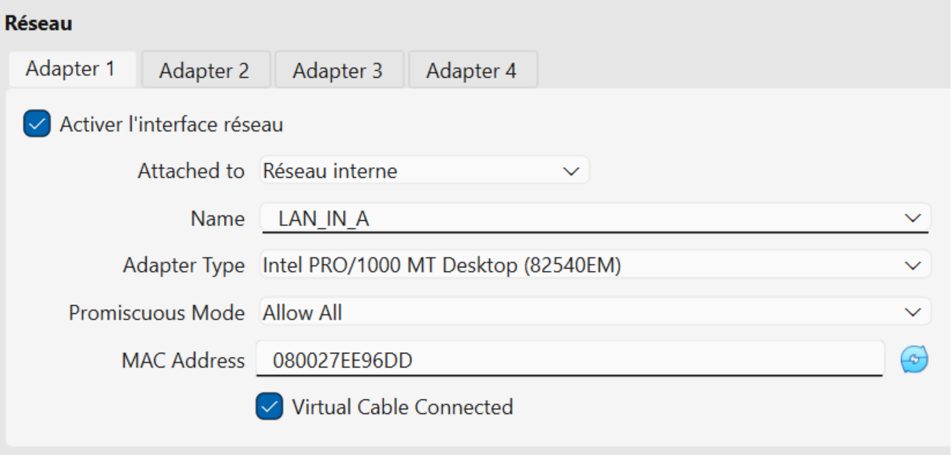
Adapter Type: Intel PRO/1000 MT Desktop (82540EM)

Promiscuous Mode: Allow All

MAC Address: 080027B11281

☑ Virtual Cable Connected

Graphical Client:



☑ Activer l'interface réseau

Attached to: Réseau interne

Name: LAN_IN_A

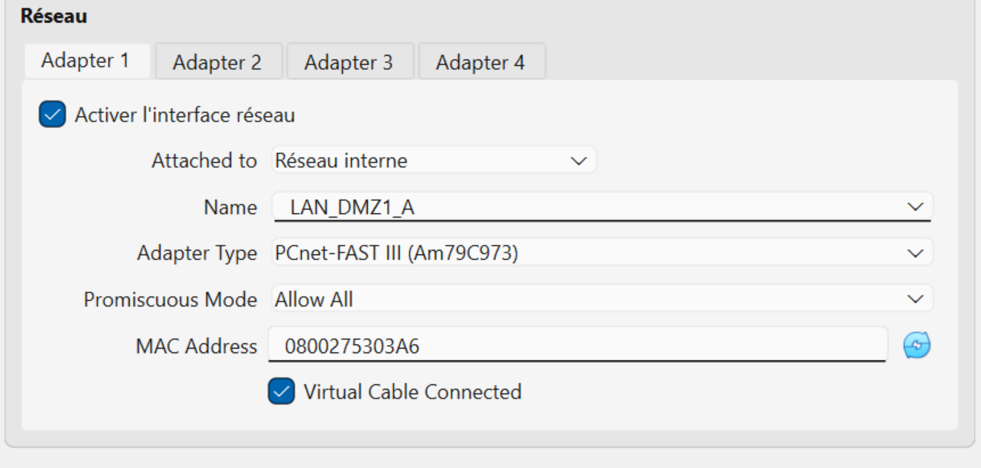
Adapter Type: Intel PRO/1000 MT Desktop (82540EM)

Promiscuous Mode: Allow All

MAC Address: 080027EE96DD

☑ Virtual Cable Connected

Debian training:



☑ Activer l'interface réseau

Attached to: Réseau interne

Name: LAN_DMZ1_A

Adapter Type: PCnet-FAST III (Am79C973)

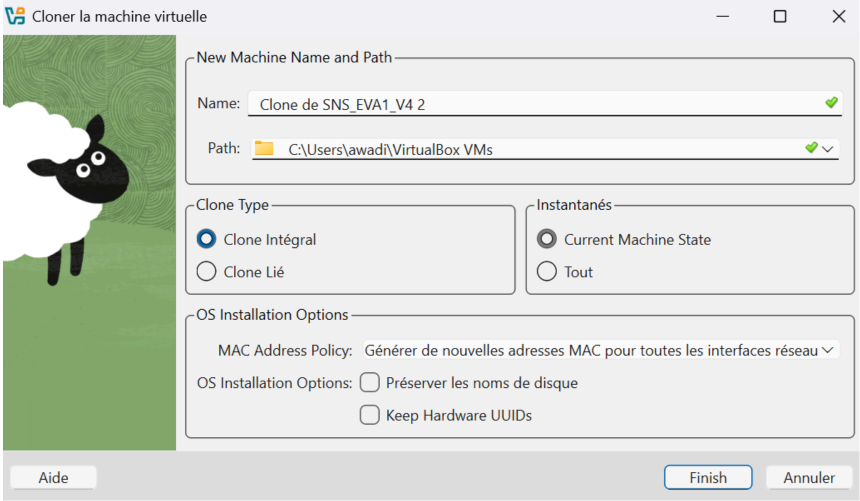
Promiscuous Mode: Allow All

MAC Address: 0800275303A6

☑ Virtual Cable Connected

5-Clonage:

SNS



Cloner la machine virtuelle

New Machine Name and Path

Name: Clone de SNS_EVA1_V4 2

Path: C:\Users\awadi\VirtualBox VMs

Clone Type

● Clone Intégral

○ Clone Lié

Instantanés

● Current Machine State

○ Tout

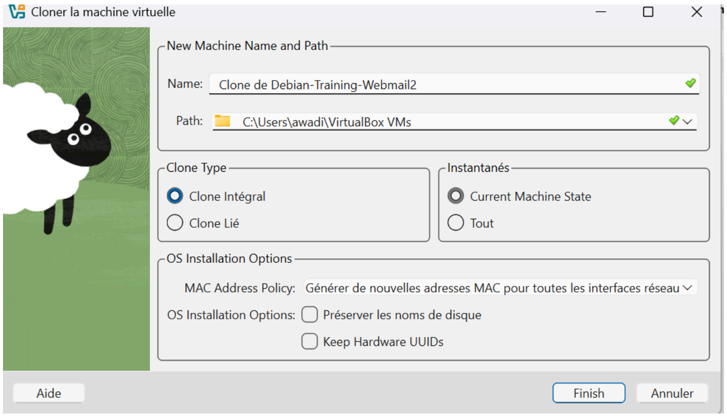
OS Installation Options

MAC Address Policy: Générer de nouvelles adresses MAC pour toutes les interfaces réseau

OS Installation Options: □ Préserver les noms de disque

□ Keep Hardware UUIDs

6-Client graphique et Debian training (Même procédure):



Cloner la machine virtuelle

New Machine Name and Path

Name: Clone de Debian-Training-Webmail2

Path: C:\Users\awadi\VirtualBox VMs

Clone Type

● Clone Intégral

○ Clone Lié

Instantanés

● Current Machine State

○ Tout

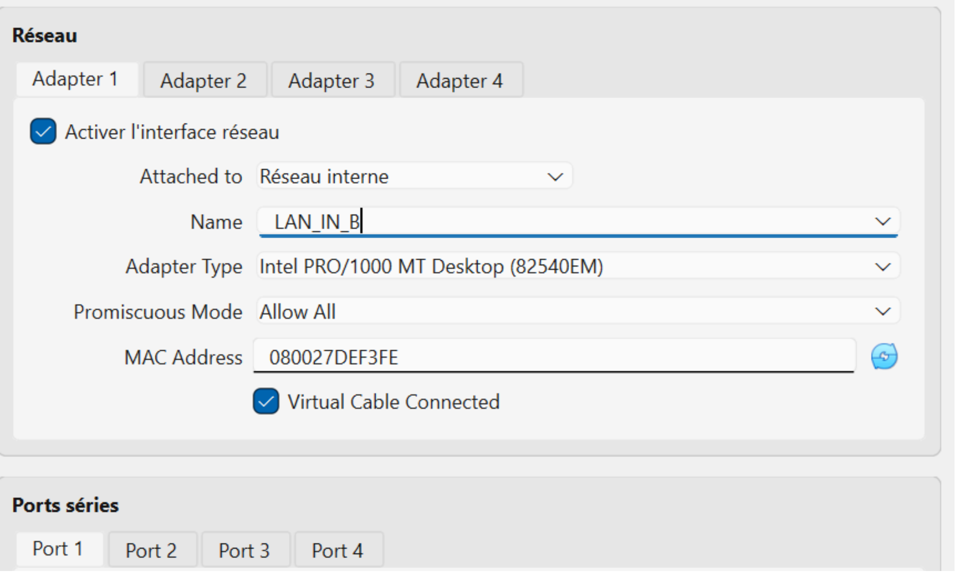
OS Installation Options

MAC Address Policy: Générer de nouvelles adresses MAC pour toutes les interfaces réseau

OS Installation Options: □ Préserver les noms de disque

□ Keep Hardware UUIDs

7-Renommer:



Réseau

☑ Activer l'interface réseau

Attached to: Réseau interne

Name: LAN_IN_B

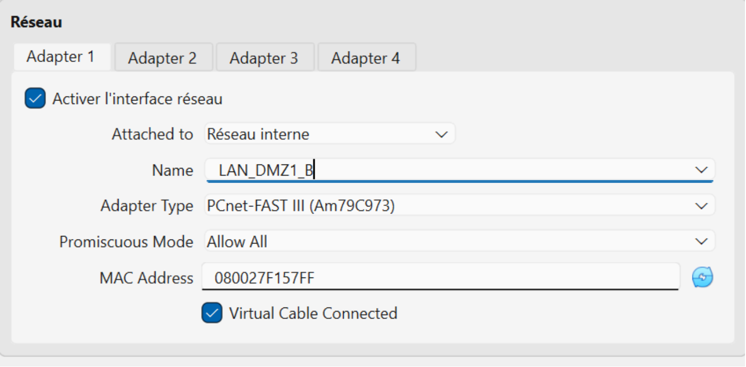
Adapter Type: Intel PRO/1000 MT Desktop (82540EM)

Promiscuous Mode: Allow All

MAC Address: 080027DEF3FE

☑ Virtual Cable Connected

Ports séries



☑ Activer l'interface réseau

Attached to: Réseau interne

Name: LAN_DMZ1_B

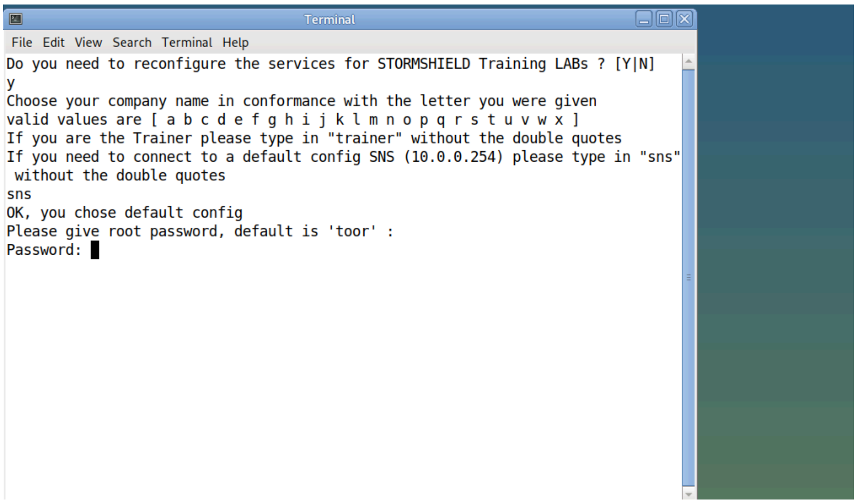
Adapter Type: PCnet-FAST III (Am79C973)

Promiscuous Mode: Allow All

MAC Address: 080027F157FF

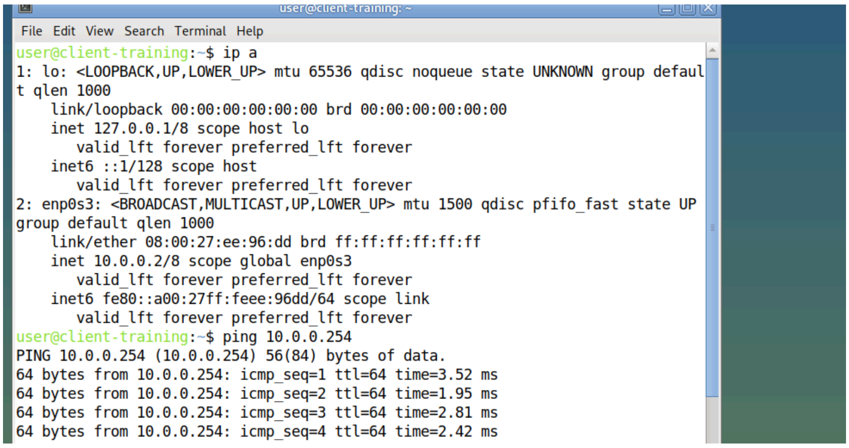
☑ Virtual Cable Connected

8-Démarrez les VM:



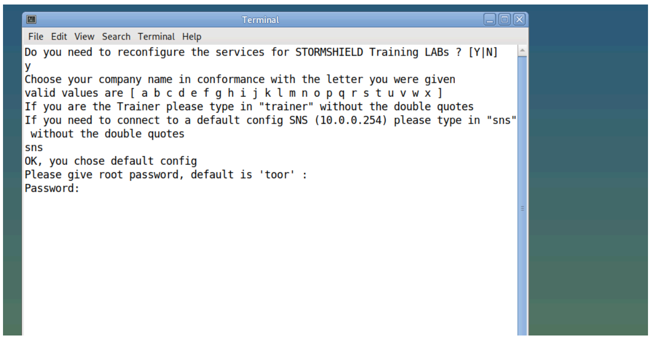
```
Do you need to reconfigure the services for STORMSHIELD Training LABs ? [Y|N]
y
Choose your company name in conformance with the letter you were given
valid values are [ a b c d e f g h i j k l m n o p q r s t u v w x ]
If you are the Trainer please type in "trainer" without the double quotes
If you need to connect to a default config SNS (10.0.0.254) please type in "sns"
 without the double quotes
sns
OK, you chose default config
Please give root password, default is 'toor' :
Password: 
```

9-Vérifier la connectivité entre le client et le firewall:



```
user@client-training:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group defaul
t qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP
group default qlen 1000
    link/ether 08:00:27:ee:96:dd brd ff:ff:ff:ff:ff:ff
    inet 10.0.0.2/8 scope global enp0s3
       valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:feee:96dd/64 scope link
       valid_lft forever preferred_lft forever
user@client-training:~$ ping 10.0.0.254
PING 10.0.0.254 (10.0.0.254) 56(84) bytes of data.
64 bytes from 10.0.0.254: icmp_seq=1 ttl=64 time=3.52 ms
64 bytes from 10.0.0.254: icmp_seq=2 ttl=64 time=1.95 ms
64 bytes from 10.0.0.254: icmp_seq=3 ttl=64 time=2.81 ms
64 bytes from 10.0.0.254: icmp_seq=4 ttl=64 time=2.42 ms
```

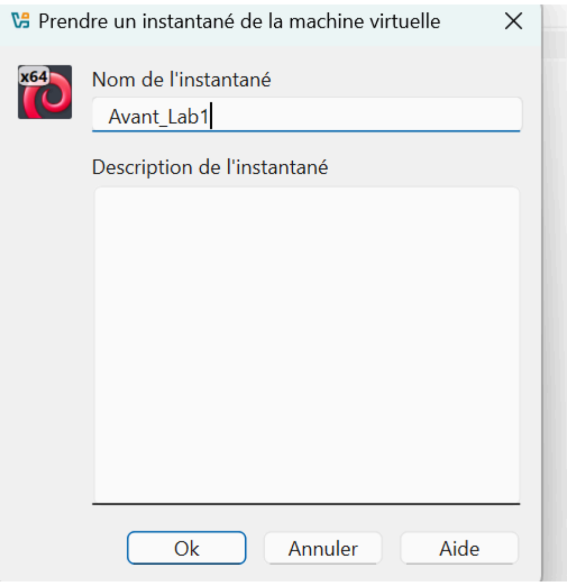
10-Recommencez les points 9 et 10 avec les VM du site B:



```
Do you need to reconfigure the services for STORMSHIELD Training LABs ? [Y|N]
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
sns
OK, you chose default config
Please give root password, default is 'toor' :
Password:
```

LAB1:Configuration du Firewall

1)Création des instantanés (Avant_Labs):

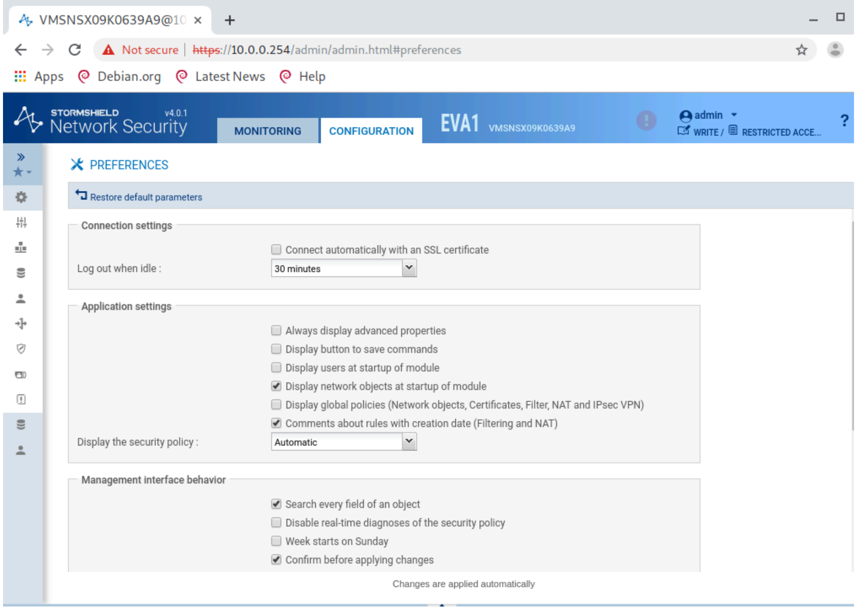


Prendre un instantané de la machine virtuelle

Nom de l'instantané: Avant_Lab1

Description de l'instantané:

3)Modifier les préférences:



https://10.0.0.254/admin/admin.html#preferences

PREFERENCES

Restore default parameters

Connection settings

- ☐ Connect automatically with an SSL certificate
- Log out when idle : 30 minutes

Application settings

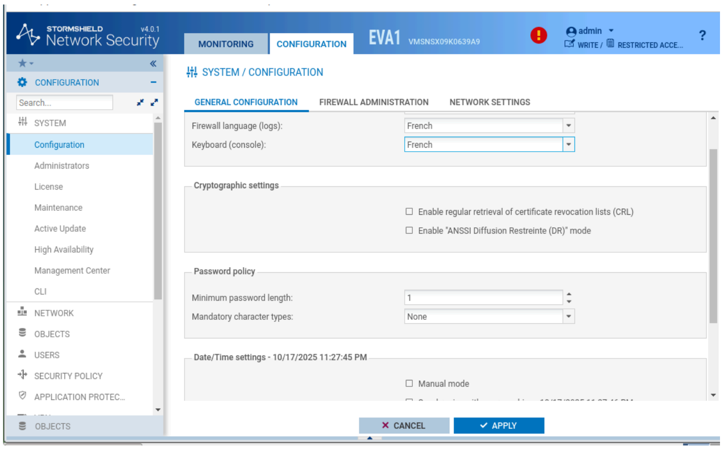
- ☐ Always display advanced properties
- ☐ Display button to save commands
- ☐ Display users at startup of module
- ☑ Display network objects at startup of module
- ☐ Display global policies (Network objects, Certificates, Filter, NAT and IPsec VPN)
- ☑ Comments about rules with creation date (Filtering and NAT)
- Display the security policy : Automatic

Management interface behavior

- ☑ Search every field of an object
- ☐ Disable real-time diagnoses of the security policy
- ☐ Week starts on Sunday
- ☑ Confirm before applying changes

Changes are applied automatically

4)Changer la langue, le clavier et le fuseau horaire:



SYSTEM / CONFIGURATION

GENERAL CONFIGURATION

- Firewall language (logs): French
- Keyboard (console): French

Cryptographic settings

- ☐ Enable regular retrieval of certificate revocation lists (CRL)
- ☐ Enable "ANSSI Diffusion Restreinte (DR)" mode

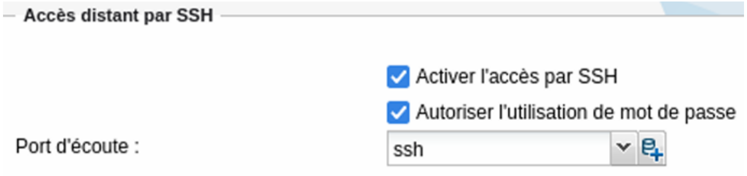
Password policy

- Minimum password length: 1
- Mandatory character types: None

Date/Time settings - 10/17/2025 11:27:45 PM

- ☐ Manual mode

5)Activer ssh:



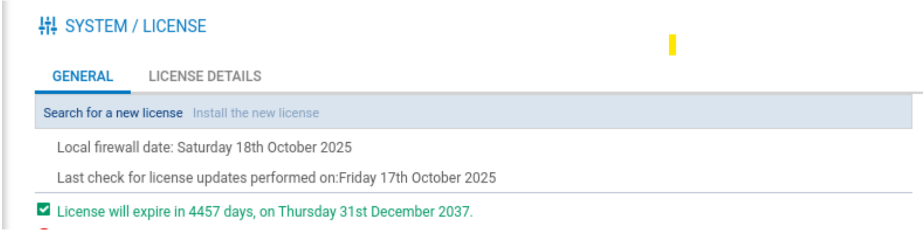
Accès distant par SSH

☑ Activer l'accès par SSH

☑ Autoriser l'utilisation de mot de passe

Port d'écoute : ssh

6)Vérification license:



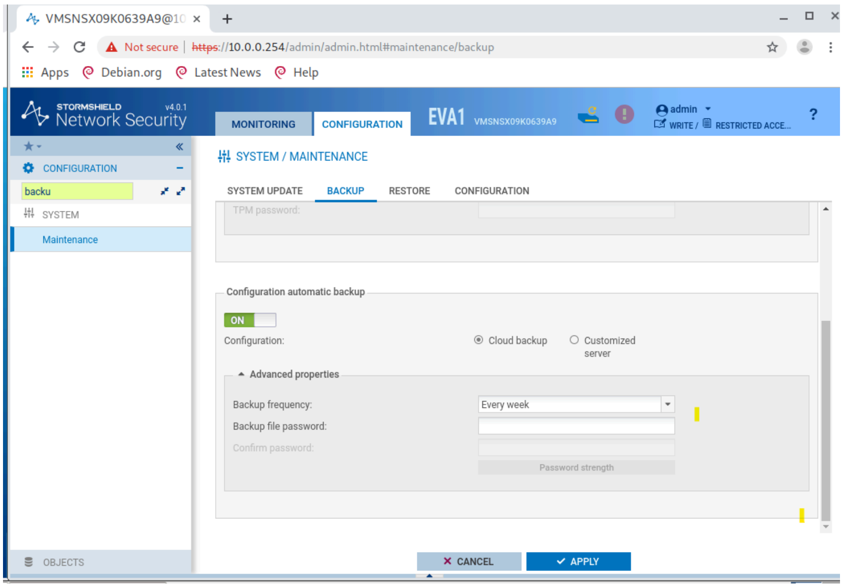
SYSTEM / LICENSE

Local firewall date: Saturday 18th October 2025

Last check for license updates performed on:Friday 17th October 2025

☑ License will expire in 4457 days, on Thursday 31st December 2037.

7)Sauvegarde:



TPM password:

Configuration automatic backup

ON

Configuration: ● Cloud backup ○ Customized server

Advanced properties

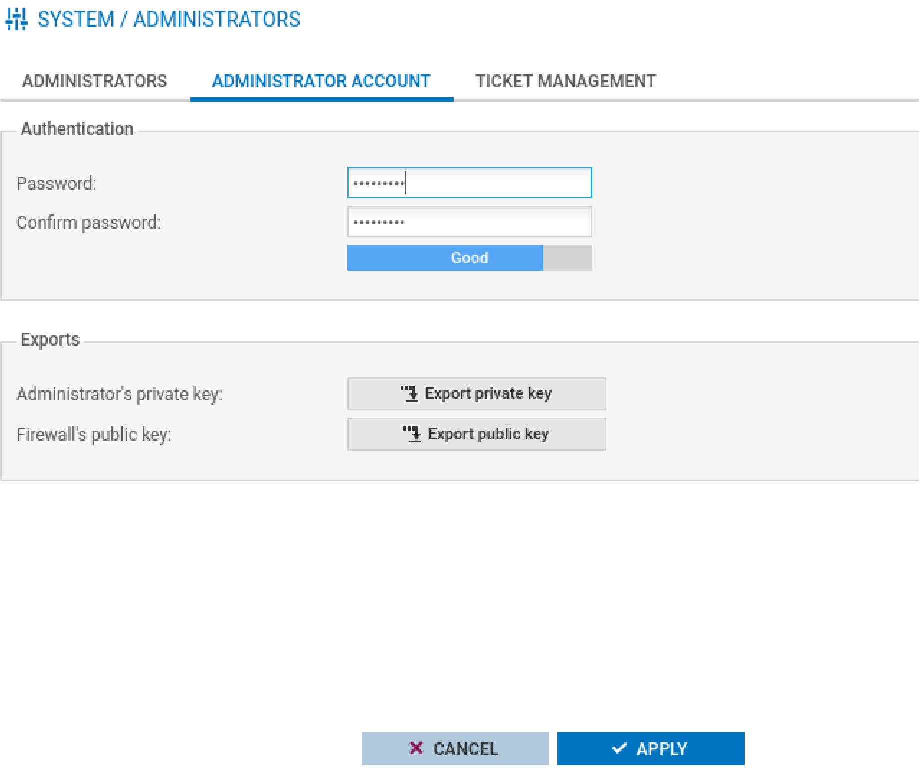
Backup frequency: Every week

Backup file password:

Confirm password:

Password strength

8)Mot de passe (Admin123#):



Authentication

Password: •••••••••

Confirm password: •••••••••

Good

Exports

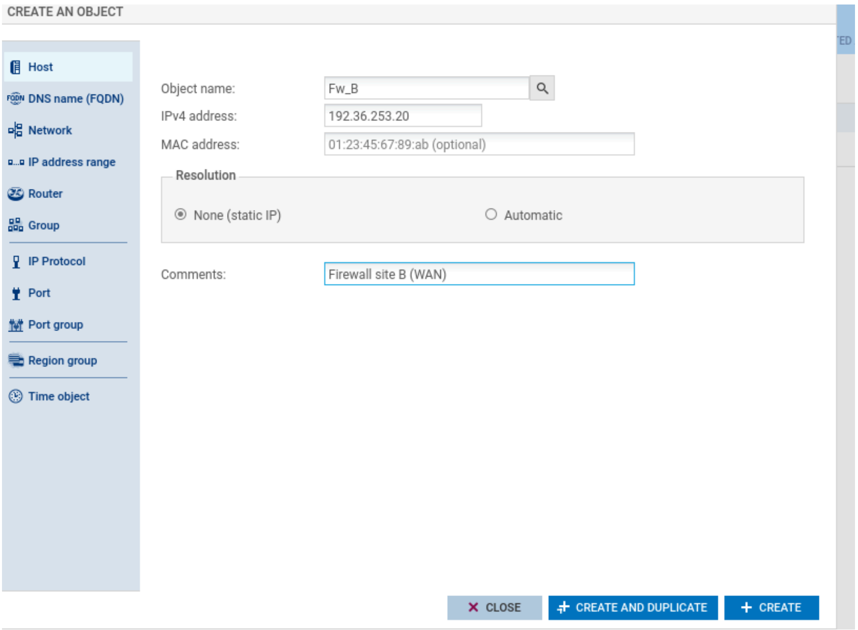
Administrator's private key:

Firewall's public key:

LAB 2:Création des Objets

1)Création des objets :

Firewall



Object name: Fw_B

IPv4 address: 192.36.253.20

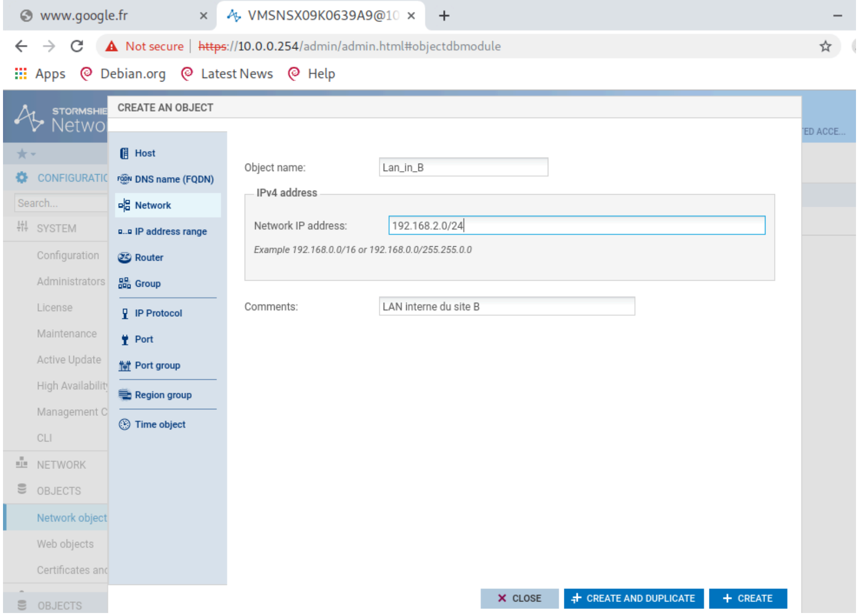
MAC address: 01:23:45:67:89:ab (optional)

Resolution

● None (static IP) ○ Automatic

Comments: Firewall site B (WAN)

réseau distant:



CREATE AN OBJECT

Object name: Lan_in_B

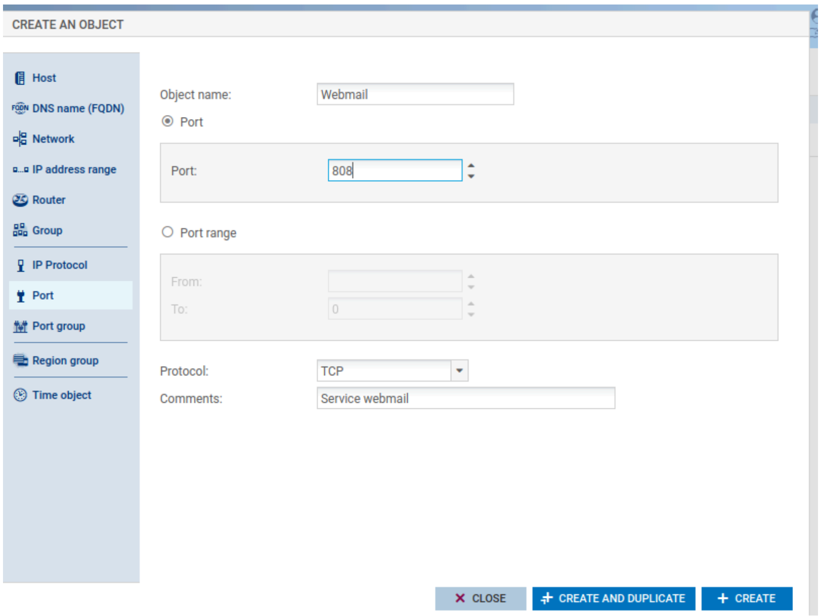
IPv4 address

Network IP address: 192.168.2.0/24

Example 192.168.0.0/16 or 192.168.0.0/255.255.0.0

Comments: LAN interne du site B

2)Ajoutez un nouveau service basé sur TCP fonctionnant sur le port 808, appelé webmail:



CREATE AN OBJECT

Object name: Webmail

● Port

Port: 808

○ Port range

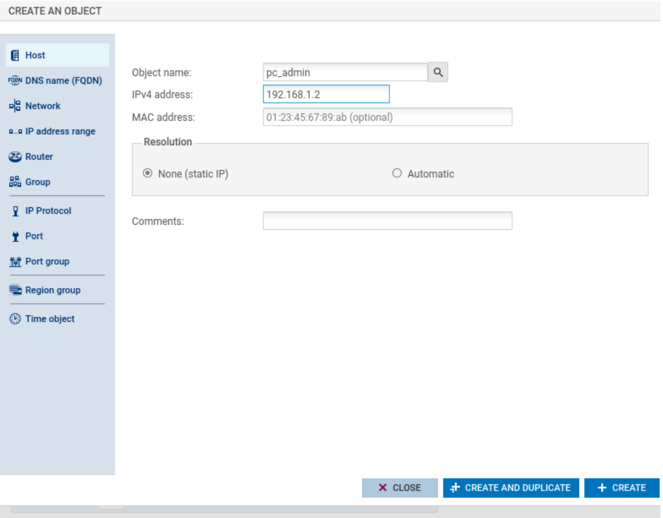
From:

To: 0

Protocol: TCP

Comments: Service webmail

3) Créez un objet « pc_admin»avec l’adresse 192.168.x.2 :



Object name: pc_admin

IPv4 address: 192.168.1.2

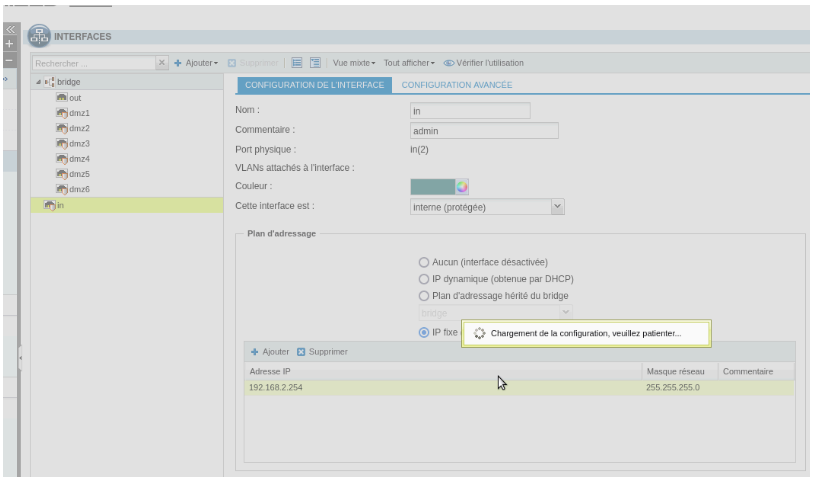
MAC address: 01:23:45:67:89:ab (optional)

Resolution

● None (static IP) ○ Automatic

Comments:

-changement de l'ip sur l'interface in (port 2) :



Nom : in

Commentaire : admin

Port physique : in(2)

VLANs attachés à l'interface :

Couleur :

Cette interface est : interne (protégée)

Plan d'adressage

○ Aucun (interface désactivée)

○ IP dynamique (obtenue par DHCP)

○ Plan d'adressage hérité du bridge

bridge

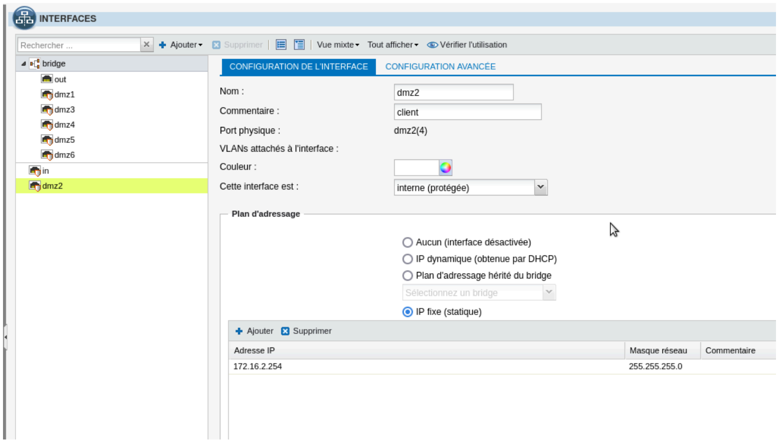
● IP fixe

Chargement de la configuration, veuillez patienter...

Ajouter Supprimer

Adresse IP	Masque réseau	Commentaire
192.168.2.254	255.255.255.0	

-config interface client:



Nom : dmz2

Commentaire : client

Port physique : dmz2(4)

VLANs attachés à l'interface :

Couleur :

Cette interface est : interne (protégée)

Plan d'adressage

○ Aucun (interface désactivée)

○ IP dynamique (obtenue par DHCP)

○ Plan d'adressage hérité du bridge

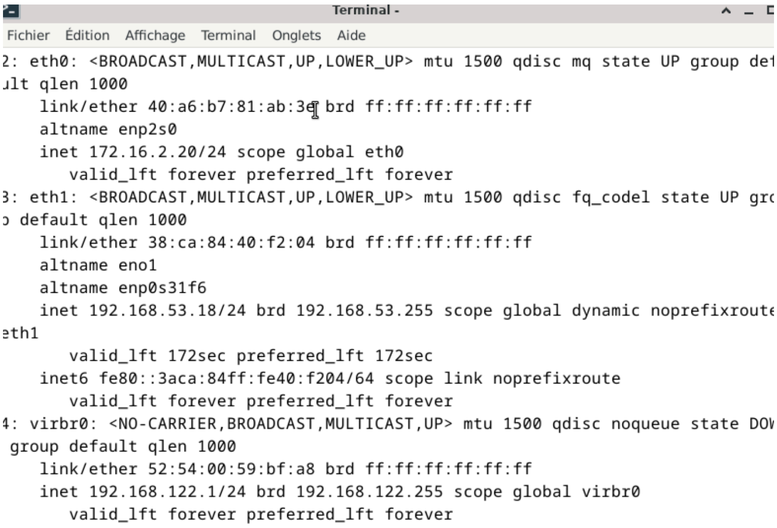
Sélectionnez un bridge

● IP fixe (statique)

Ajouter Supprimer

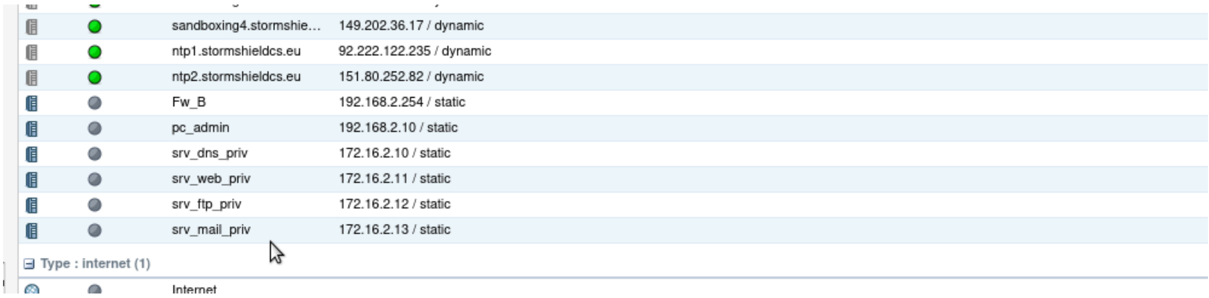
Adresse IP	Masque réseau	Commentaire
172.16.2.254	255.255.255.0	

-Changement de l'adresse IP niveau client



```
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group def
ult qlen 1000
    link/ether 40:a6:b7:81:ab:3e brd ff:ff:ff:ff:ff:ff
    altname enp2s0
    inet 172.16.2.20/24 scope global eth0
       valid_lft forever preferred_lft forever
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP gro
p default qlen 1000
    link/ether 38:ca:84:40:f2:04 brd ff:ff:ff:ff:ff:ff
    altname eno1
    altname enp0s31f6
    inet 192.168.53.18/24 brd 192.168.53.255 scope global dynamic noprefixroute
eth1
       valid_lft 172sec preferred_lft 172sec
    inet6 fe80::3aca:84ff:fe40:f204/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
4: virbr0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOW
 group default qlen 1000
    link/ether 52:54:00:59:bf:a8 brd ff:ff:ff:ff:ff:ff
    inet 192.168.122.1/24 brd 192.168.122.255 scope global virbr0
       valid_lft forever preferred_lft forever
```

-voici les objets créer dans la catégorie objet:machine

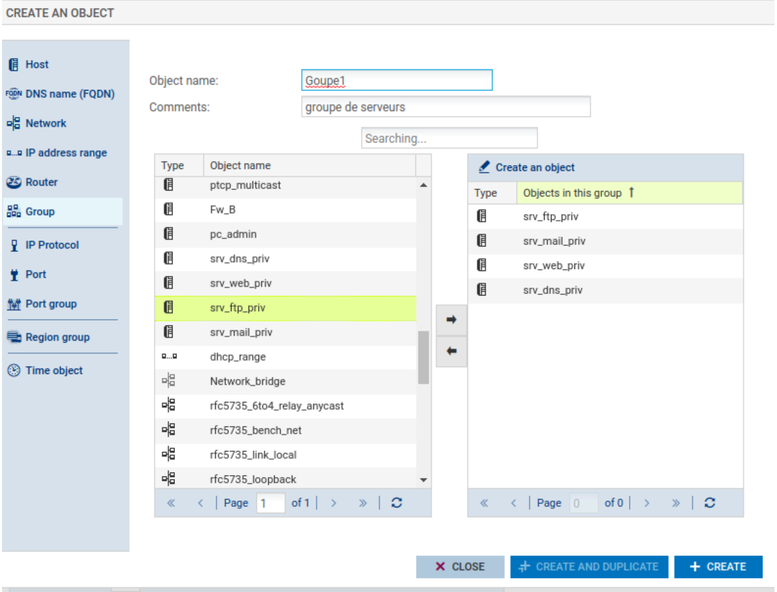


	●	sandboxing4.stormshie…	149.202.36.17 / dynamic
	●	ntp1.stormshieldcs.eu	92.222.122.235 / dynamic
	●	ntp2.stormshieldcs.eu	151.80.252.82 / dynamic
	●	Fw_B	192.168.2.254 / static
	●	pc_admin	192.168.2.10 / static
	●	srv_dns_priv	172.16.2.10 / static
	●	srv_web_priv	172.16.2.11 / static
	●	srv_ftp_priv	172.16.2.12 / static
	●	srv_mail_priv	172.16.2.13 / static

⊟ Type : internet (1)

	●	Internet

4-5-6-7-8) Création du groupe d'objets contenant les 4 serveurs:



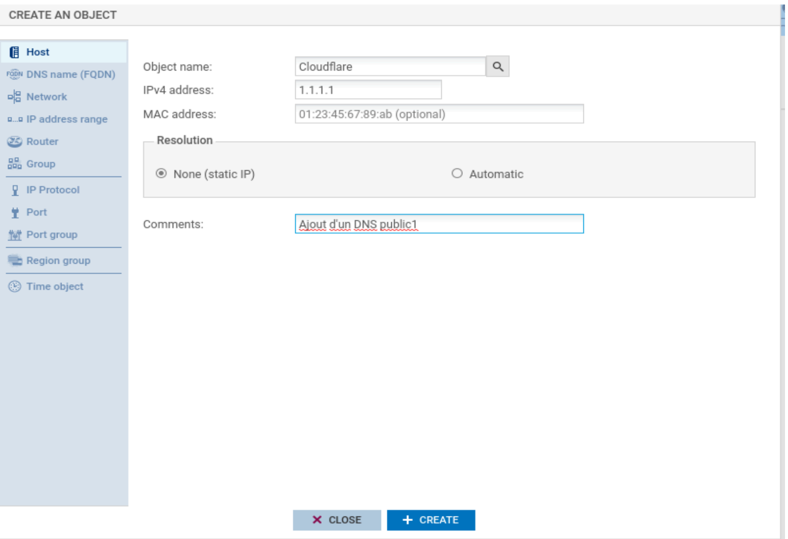
Object name: Goupe1

Comments: groupe de serveurs

Type	Object name
	ptcp_multicast
	Fw_B
	pc_admin
	srv_dns_priv
	srv_web_priv
	srv_ftp_priv
	srv_mail_priv
	dhcp_range
	Network_bridge
	rfc5735_6to4_relay_anycast
	rfc5735_bench_net
	rfc5735_link_local
	rfc5735_loopback

Type	Objects in this group ↑
	srv_ftp_priv
	srv_mail_priv
	srv_web_priv
	srv_dns_priv

9) Au cas où les serveurs DNS par défaut (dns1.google.com et dns2.google.com) configurés sur le firewall ne soient pas joignables à votre emplacement, remplacez-les par les serveurs DNS appropriés:



Object name: Cloudflare

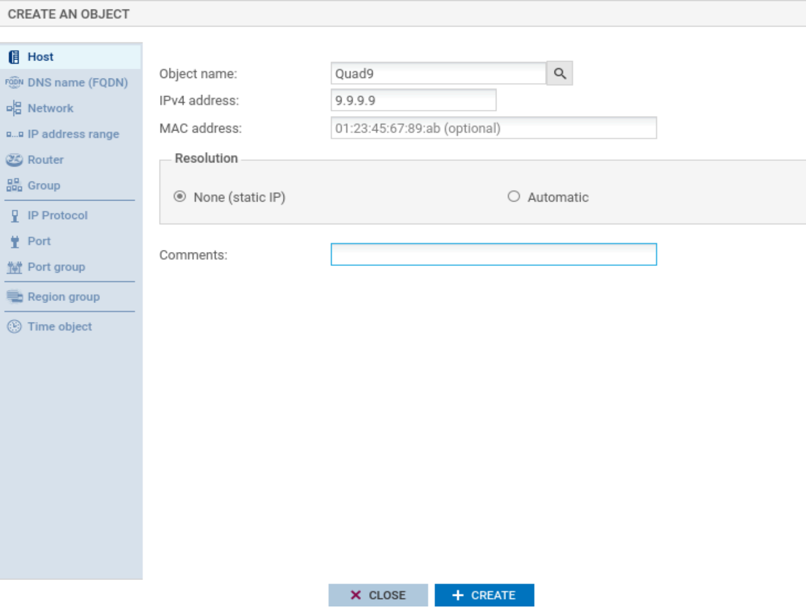
IPv4 address: 1.1.1.1

MAC address: 01:23:45:67:89:ab (optional)

Resolution

● None (static IP) ○ Automatic

Comments: Ajout d'un DNS public1



Object name: Quad9

IPv4 address: 9.9.9.9

MAC address: 01:23:45:67:89:ab (optional)

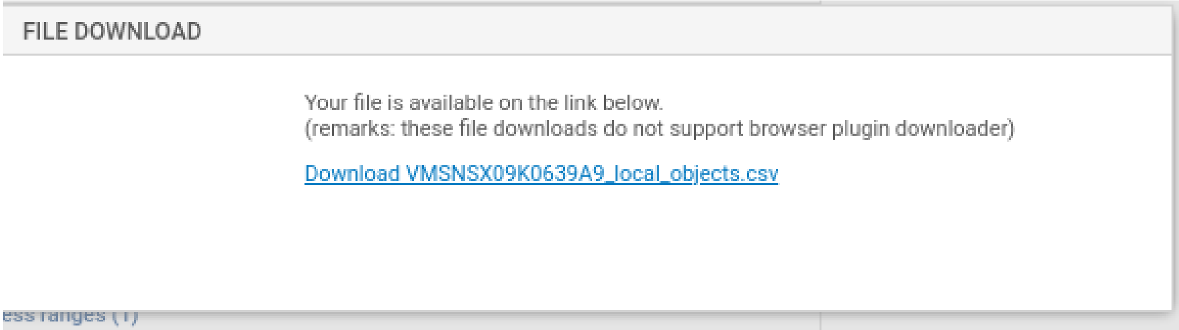
Resolution

● None (static IP) ○ Automatic

Comments:

Bonus

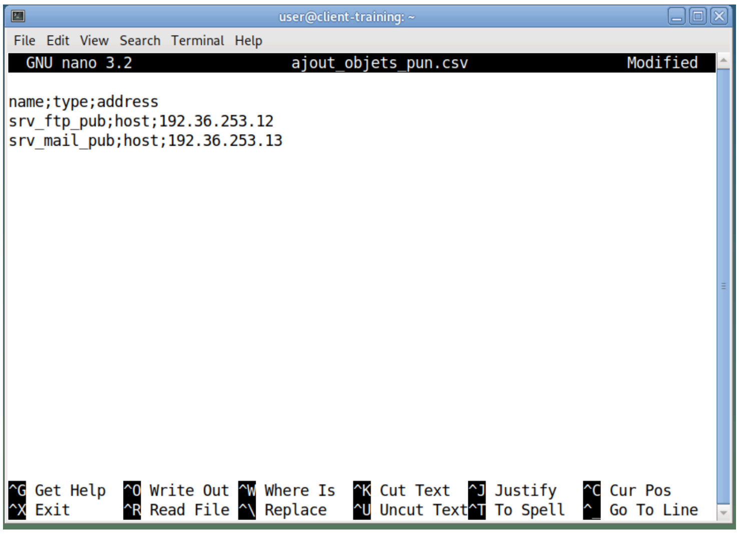
-Exportation (.CSV)



Your file is available on the link below.
(remarks: these file downloads do not support browser plugin downloader)

Download VMSNSX09K0639A9_local_objects.csv

-Création du fichier avec les objets:



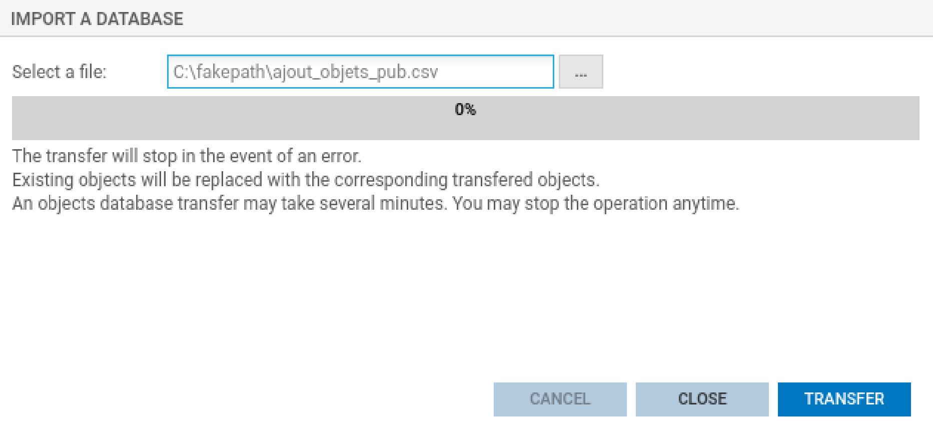
user@client-training: ~
File Edit View Search Terminal Help

```
  GNU nano 3.2                    ajout_objets_pun.csv                    Modified

name;type;address
srv_ftp_pub;host;192.36.253.12
srv_mail_pub;host;192.36.253.13
```

^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify ^C Cur Pos
^X Exit ^R Read File ^\ Replace ^U Uncut Text ^T To Spell ^_ Go To Line

-Importation:



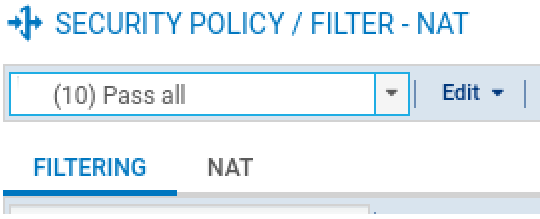
IMPORT A DATABASE

Select a file: C:\fakepath\ajout_objets_pub.csv

0%

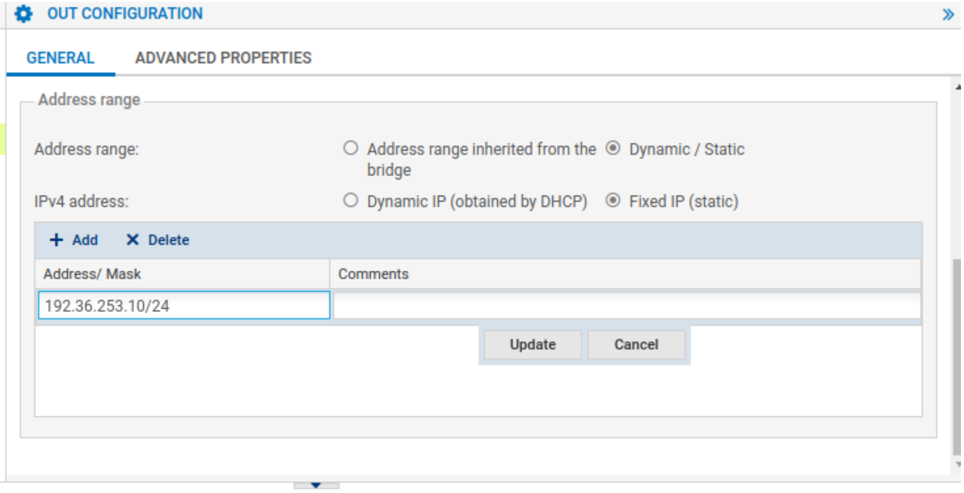
The transfer will stop in the event of an error.
Existing objects will be replaced with the corresponding transfered objects.
An objects database transfer may take several minutes. You may stop the operation anytime.

LAB3:Configuration réseau



1)Configurez les interfaces OUT, DMZ1 et IN de votre firewall comme suit :

-OUT:192.36.253.10/24



OUT CONFIGURATION

GENERAL | ADVANCED PROPERTIES

Address range

Address range: ○ Address range inherited from the bridge ● Dynamic / Static

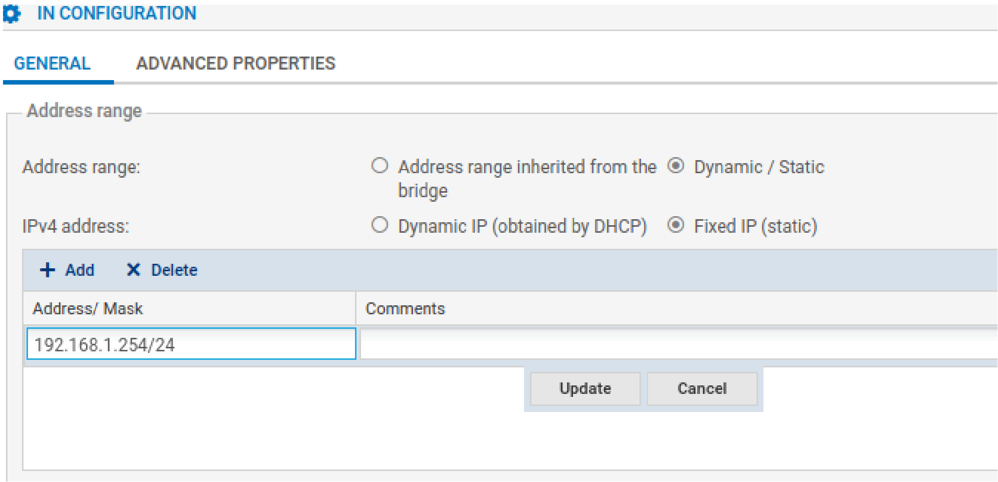
IPv4 address: ○ Dynamic IP (obtained by DHCP) ● Fixed IP (static)

+ Add ✕ Delete

Address/ Mask	Comments
192.36.253.10/24	

Update | Cancel

-IN:192.168.1.254/24



IN CONFIGURATION

GENERAL | ADVANCED PROPERTIES

Address range

Address range: ○ Address range inherited from the bridge ● Dynamic / Static

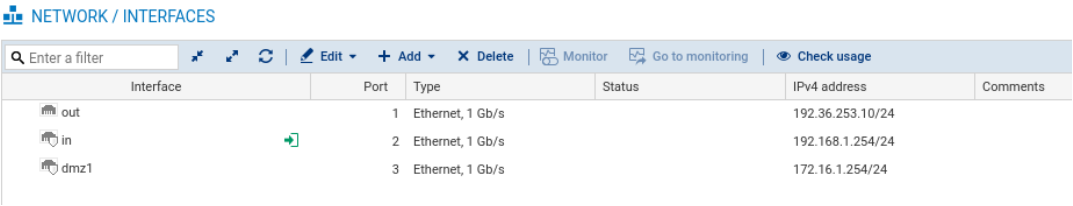
IPv4 address: ○ Dynamic IP (obtained by DHCP) ● Fixed IP (static)

+ Add ✕ Delete

Address/ Mask	Comments
192.168.1.254/24	

Update | Cancel

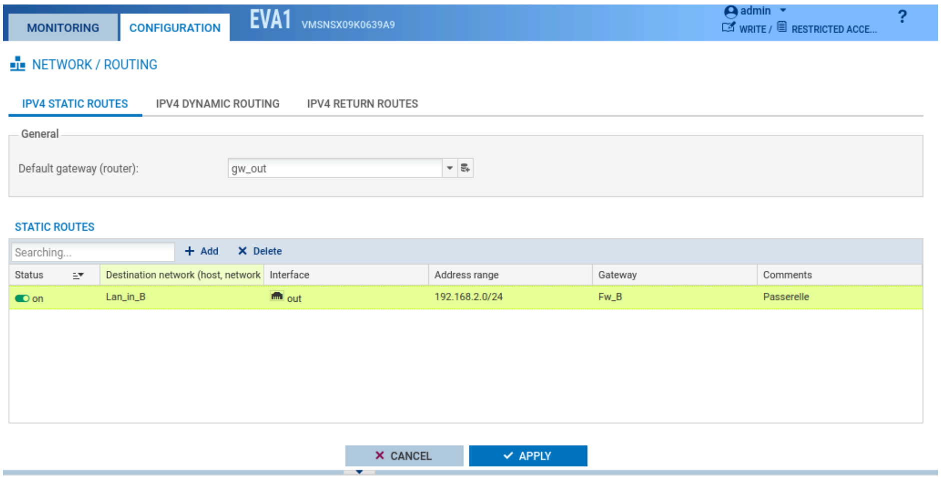
-DMZ:172.16.1.254/24



NETWORK / INTERFACES

Interface	Port	Type	Status	IPv4 address	Comments
out	1	Ethernet, 1 Gb/s		192.36.253.10/24	
in	2	Ethernet, 1 Gb/s		192.168.1.254/24	
dmz1	3	Ethernet, 1 Gb/s		172.16.1.254/24	

2)Configuration de la passerelle par défaut:



General

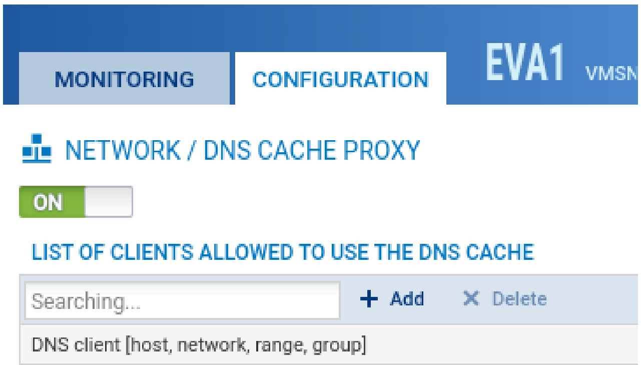
Default gateway (router): gw_out

STATIC ROUTES

Status	Destination network (host, network	Interface	Address range	Gateway	Comments
on	Lan_in_B	out	192.168.2.0/24	Fw_B	Passerelle

3)Configuration du proxy cache DNS:

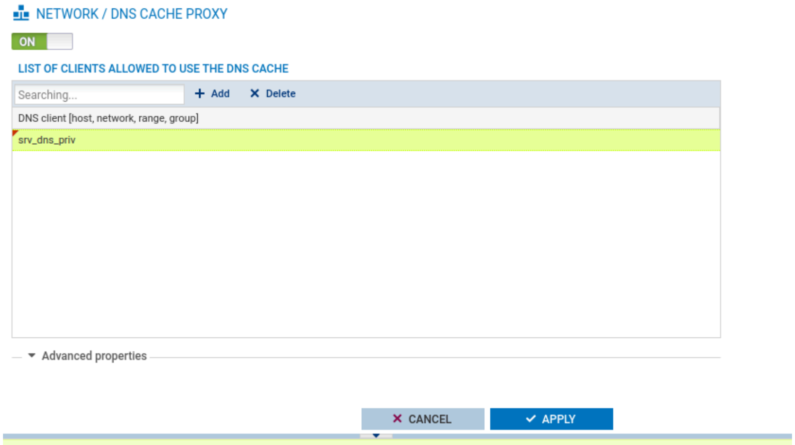
-Activation du cache DNs



LIST OF CLIENTS ALLOWED TO USE THE DNS CACHE

DNS client [host, network, range, group]

-Ajout du serveur DNS interne comme client autorisé:

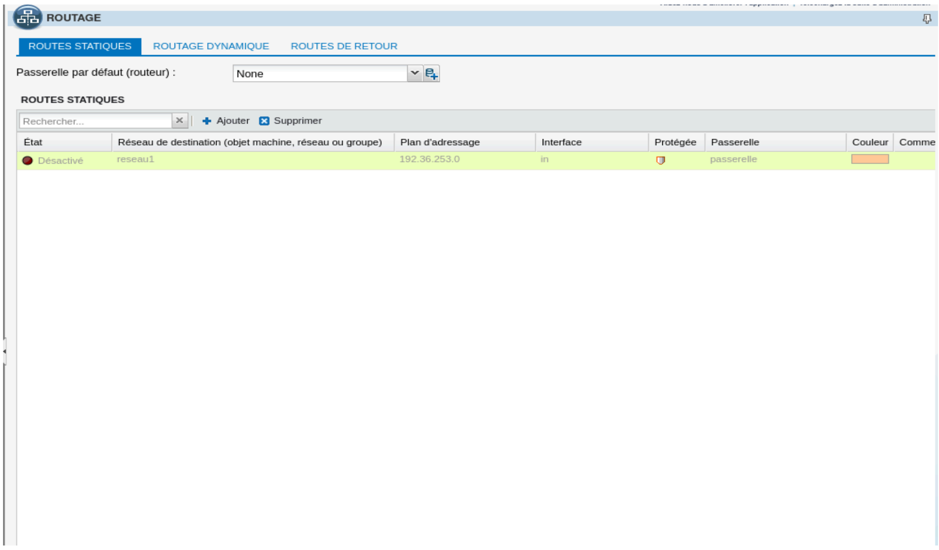


LIST OF CLIENTS ALLOWED TO USE THE DNS CACHE

DNS client [host, network, range, group]
srv_dns_priv

LAB4:Translation d’adresses

-Désactivation de la route statique:



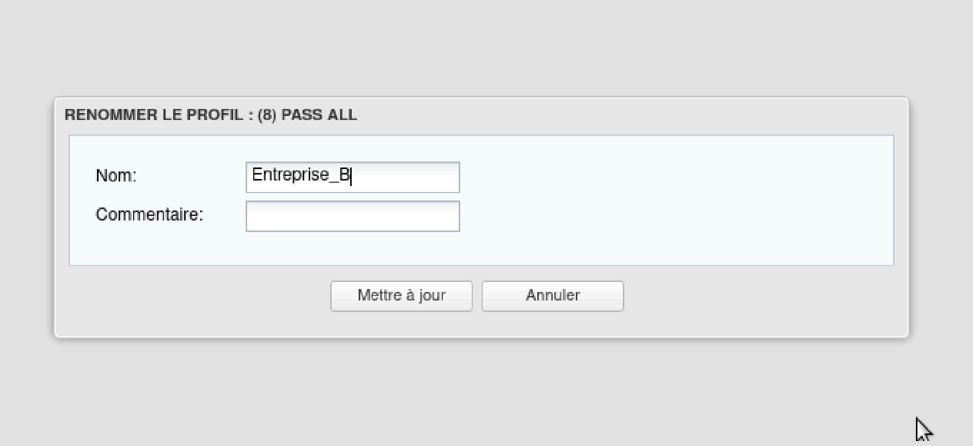
ROUTAGE

ROUTES STATIQUES | ROUTAGE DYNAMIQUE | ROUTES DE RETOUR

Passerelle par défaut (routeur) : None

ROUTES STATIQUES

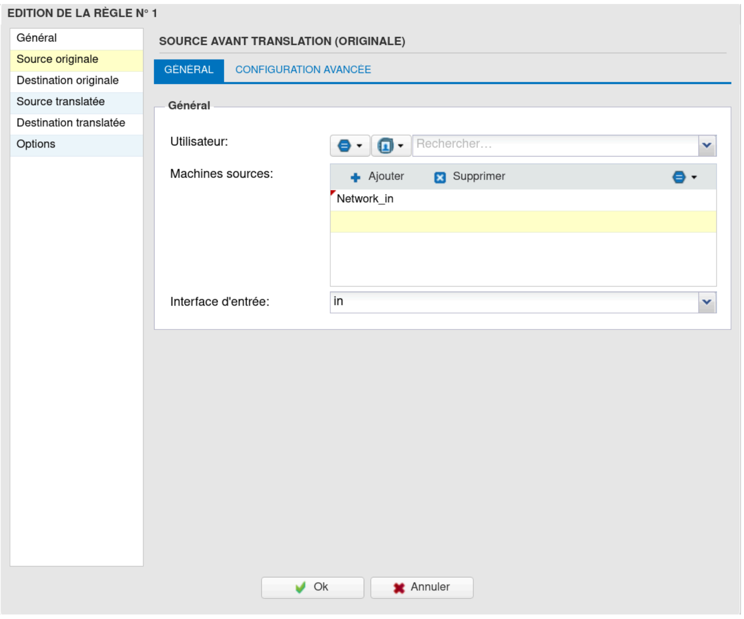
État	Réseau de destination (objet machine, réseau ou groupe)	Plan d'adressage	Interface	Protégée	Passerelle	Couleur	Comme
● Désactivé	reseau1	192.36.253.0	in		passerelle	🟧	



RENOMMER LE PROFIL : (8) PASS ALL

Nom: Entreprise_B

Commentaire:



EDITION DE LA RÈGLE N° 1

SOURCE AVANT TRANSLATION (ORIGINALE)

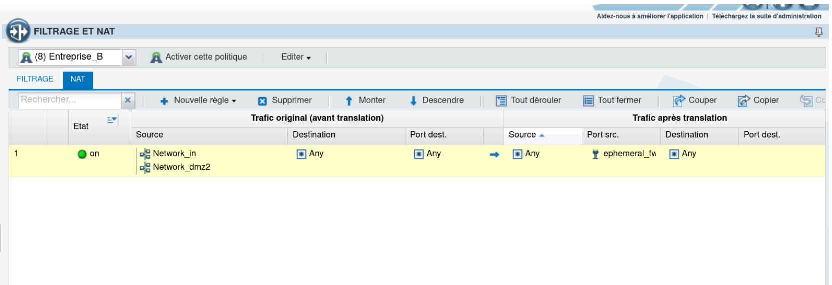
Général

Utilisateur:

Machines sources: Network_in

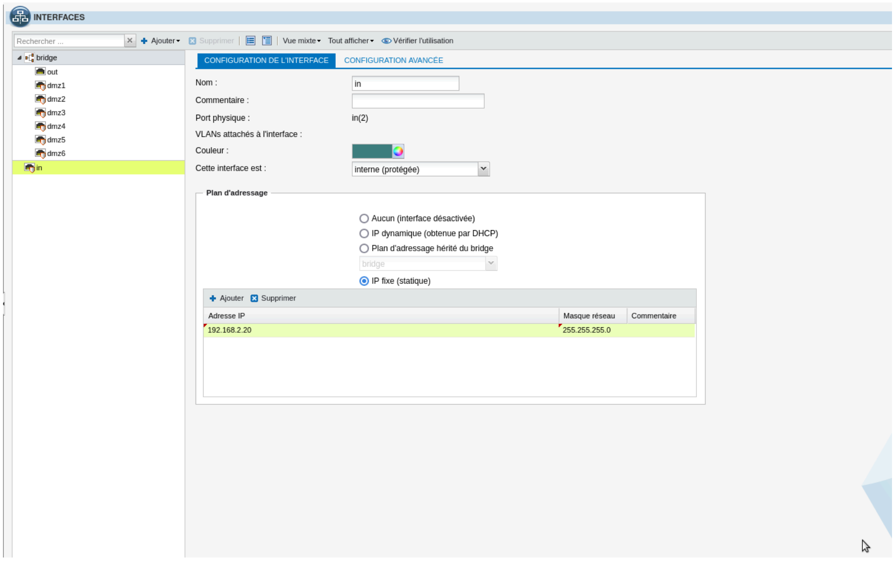
Interface d'entrée: in

-Création de la règle NAT



			Trafic original (avant translation)				Trafic après translation			
		Etat	Source	Destination	Port dest.		Source	Port src.	Destination	Port dest.
1		● on	Network_in Network_dmz2	Any	Any	→	Any	ephemeral_fw	Any	

-Restauration du fichier de configuration de la séance du 24/10/2025



Nom : in

Commentaire :

Port physique : in(2)

VLANs attachés à l'interface :

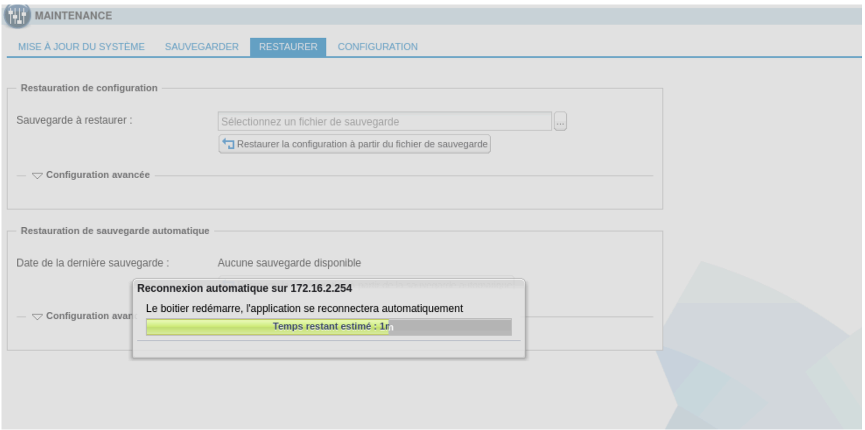
Couleur :

Cette interface est : interne (protégée)

Plan d'adressage

○ Aucun (interface désactivée)
○ IP dynamique (obtenue par DHCP)
○ Plan d'adressage hérité du bridge
bridge
● IP fixe (statique)

Adresse IP	Masque réseau	Commentaire
192.168.2.20	255.255.255.0	



Restauration de configuration

Sauvegarde à restaurer : Sélectionnez un fichier de sauvegarde

Restaurer la configuration à partir du fichier de sauvegarde

Configuration avancée

Restauration de sauvegarde automatique

Date de la dernière sauvegarde : Aucune sauvegarde disponible

Configuration avan

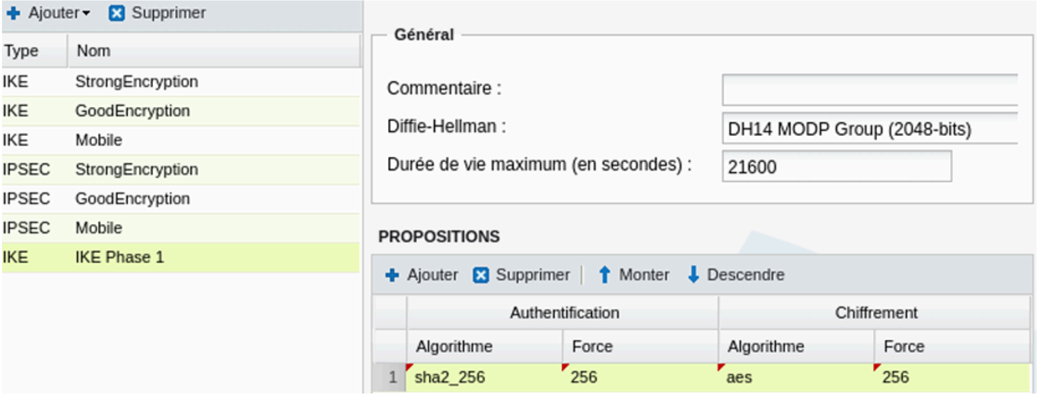
Reconnexion automatique sur 172.16.2.254

Le boitier redémarre, l'application se reconnectera automatiquement

Temps restant estimé : 1n

LAB 8 : VPN IPsec (Site à site)

1)Création des profils de chiffrements:



Type	Nom
IKE	StrongEncryption
IKE	GoodEncryption
IKE	Mobile
IPSEC	StrongEncryption
IPSEC	GoodEncryption
IPSEC	Mobile
IKE	IKE Phase 1

Général

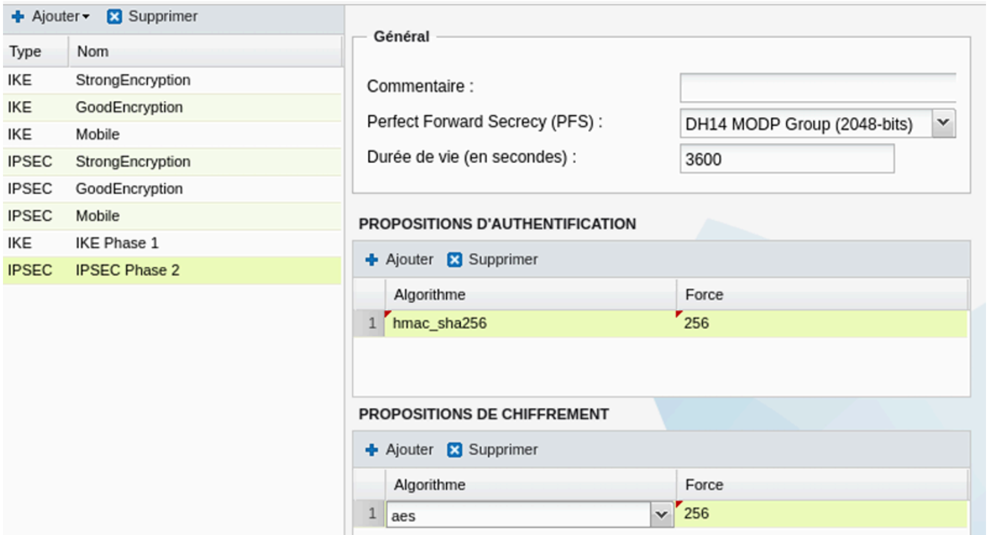
Commentaire :

Diffie-Hellman : DH14 MODP Group (2048-bits)

Durée de vie maximum (en secondes) : 21600

PROPOSITIONS

	Authentification		Chiffrement	
	Algorithme	Force	Algorithme	Force
1	sha2_256	256	aes	256



Type	Nom
IKE	StrongEncryption
IKE	GoodEncryption
IKE	Mobile
IPSEC	StrongEncryption
IPSEC	GoodEncryption
IPSEC	Mobile
IKE	IKE Phase 1
IPSEC	IPSEC Phase 2

Général

Commentaire :

Perfect Forward Secrecy (PFS) : DH14 MODP Group (2048-bits)

Durée de vie (en secondes) : 3600

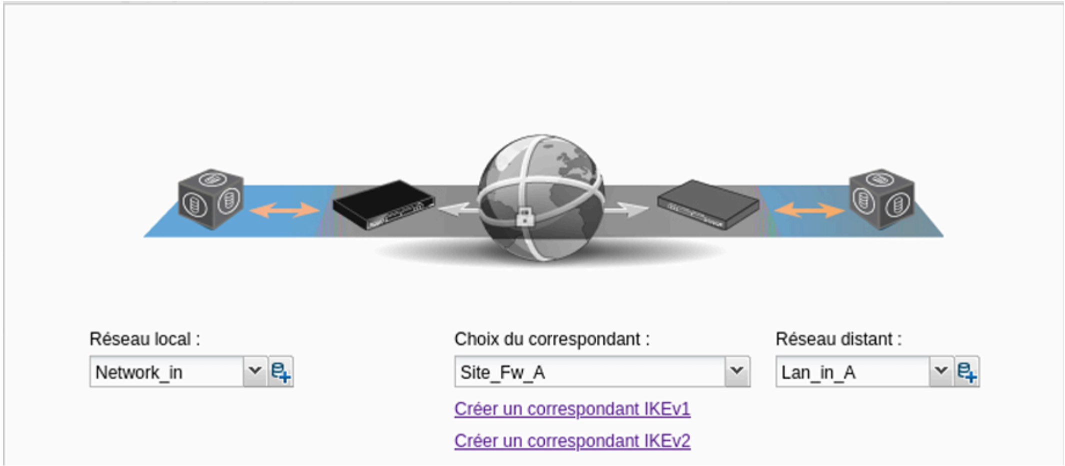
PROPOSITIONS D'AUTHENTIFICATION

	Algorithme	Force
1	hmac_sha256	256

PROPOSITIONS DE CHIFFREMENT

	Algorithme	Force
1	aes	256

2)Configuration du tunnel IPsec avec une authentification par PSK:



Réseau local : Network_in

Choix du correspondant : Site_Fw_A

Réseau distant : Lan_in_A