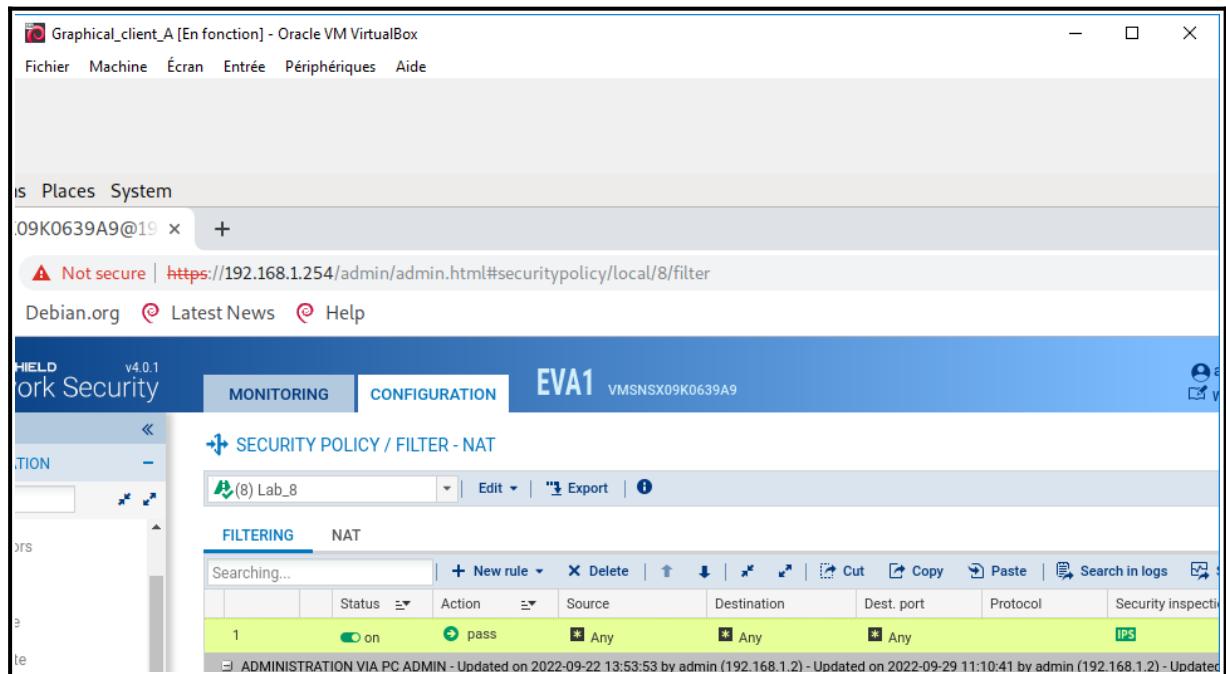




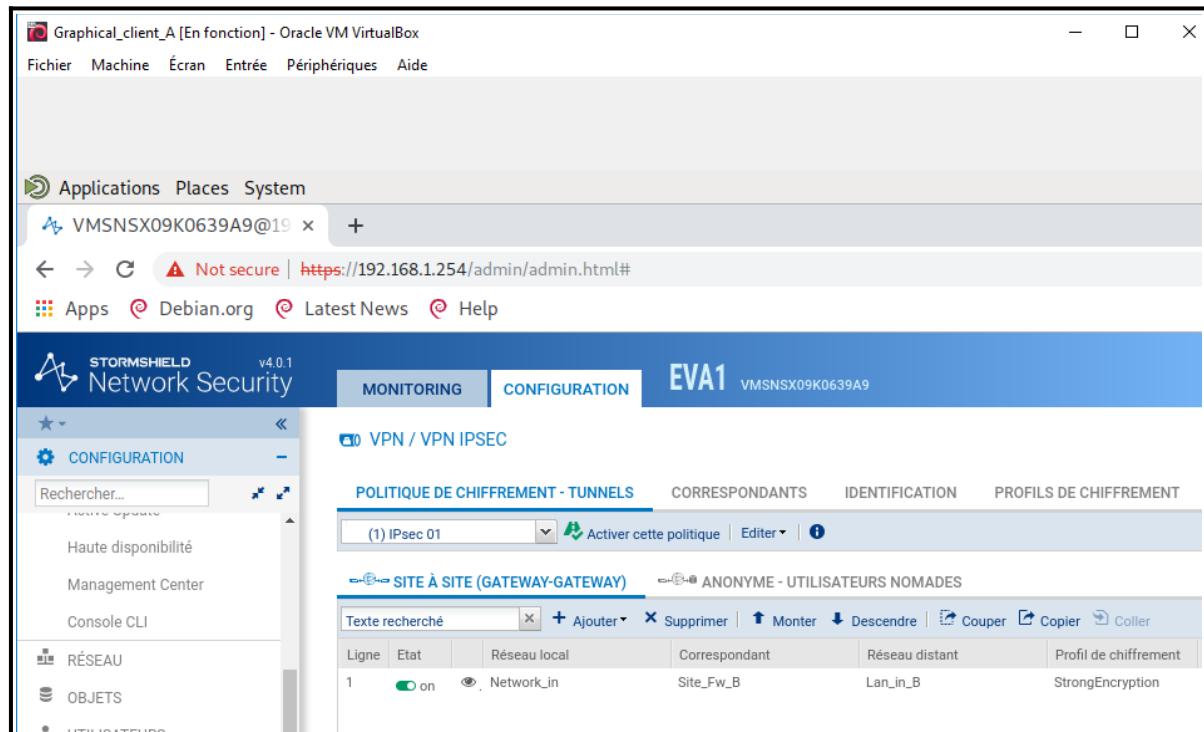
STORMSHIELD

LAB 8 :
VPN IPsec

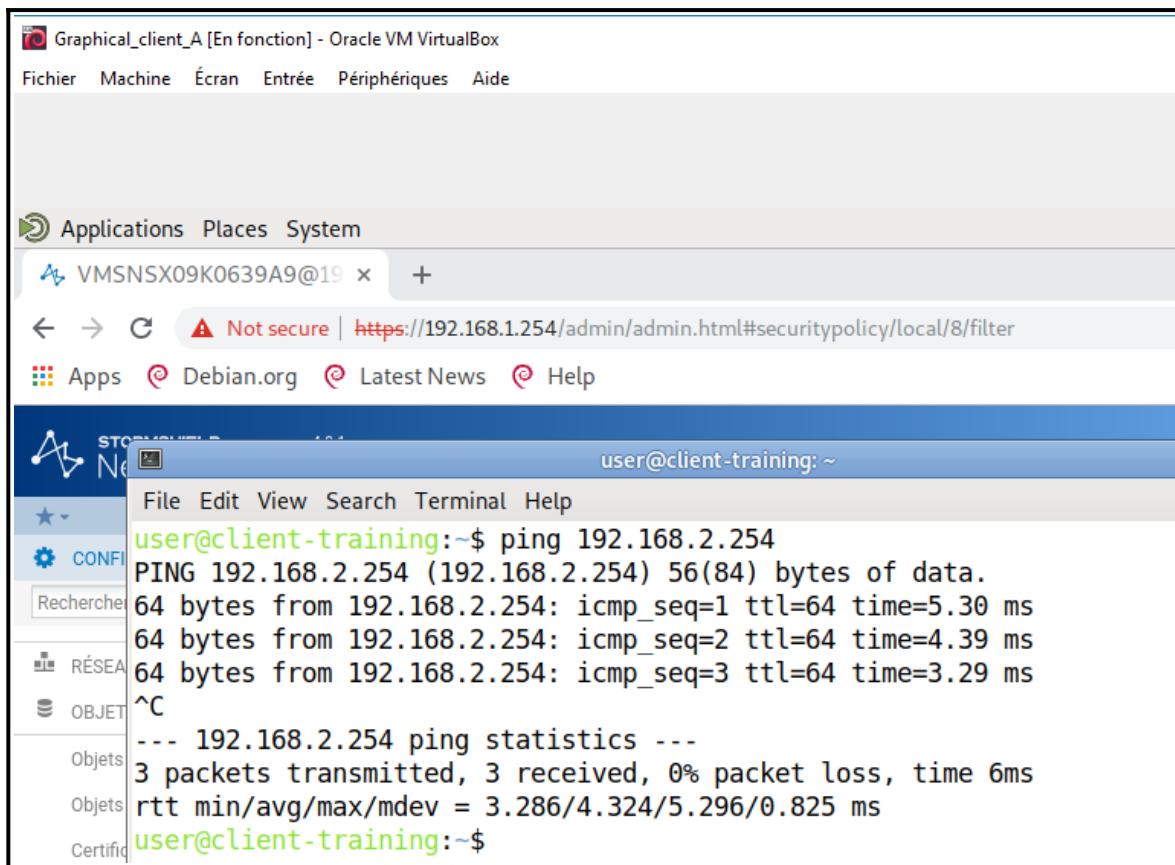
Réseau A :



1ère étape : Ajout de la règle de filtrage pass any any.



2ème étape : Configuration d'un tunnel Ipsec afin de relier le réseau A au réseau B.



Graphical_client_A [En fonction] - Oracle VM VirtualBox

Fichier Machine Écran Entrée Périphériques Aide

Applications Places System

VMSNSX09K0639A9@19 x +

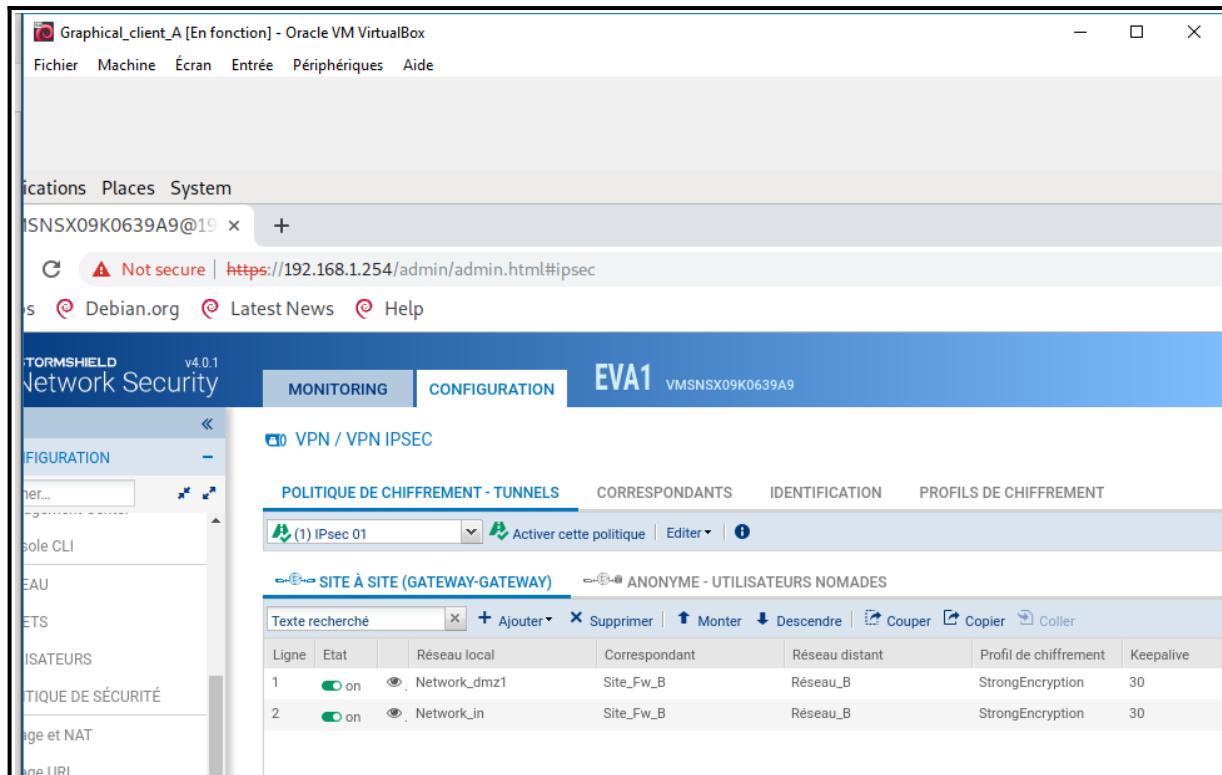
Not secure | <https://192.168.1.254/admin/admin.html#securitypolicy/local/8/filter>

Apps Debian.org Latest News Help

user@client-training: ~

```
File Edit View Search Terminal Help
user@client-training:~$ ping 192.168.2.254
PING 192.168.2.254 (192.168.2.254) 56(84) bytes of data.
64 bytes from 192.168.2.254: icmp_seq=1 ttl=64 time=5.30 ms
64 bytes from 192.168.2.254: icmp_seq=2 ttl=64 time=4.39 ms
64 bytes from 192.168.2.254: icmp_seq=3 ttl=64 time=3.29 ms
^C
--- 192.168.2.254 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 6ms
rtt min/avg/max/mdev = 3.286/4.324/5.296/0.825 ms
user@client-training:~$
```

3ème étape : Test de ping du réseau A au firewall de B.



Graphical_client_A [En fonction] - Oracle VM VirtualBox

Fichier Machine Écran Entrée Périphériques Aide

Applications Places System

VMSNSX09K0639A9@19 x +

Not secure | <https://192.168.1.254/admin/admin.html#ipsec>

Debian.org Latest News Help

TORMSHIELD Network Security v4.0.1

MONITORING CONFIGURATION EVA1 VMSNSX09K0639A9

VPN / VPN IPSEC

POLITIQUE DE CHIFFREMENT - TUNNELS

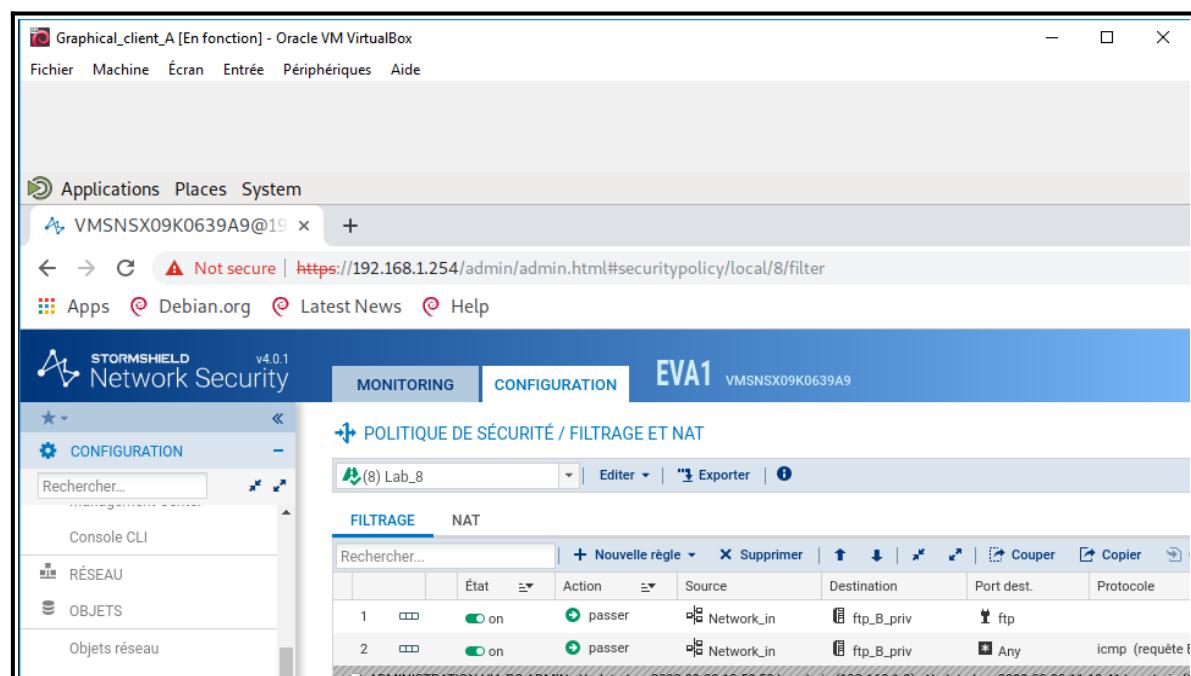
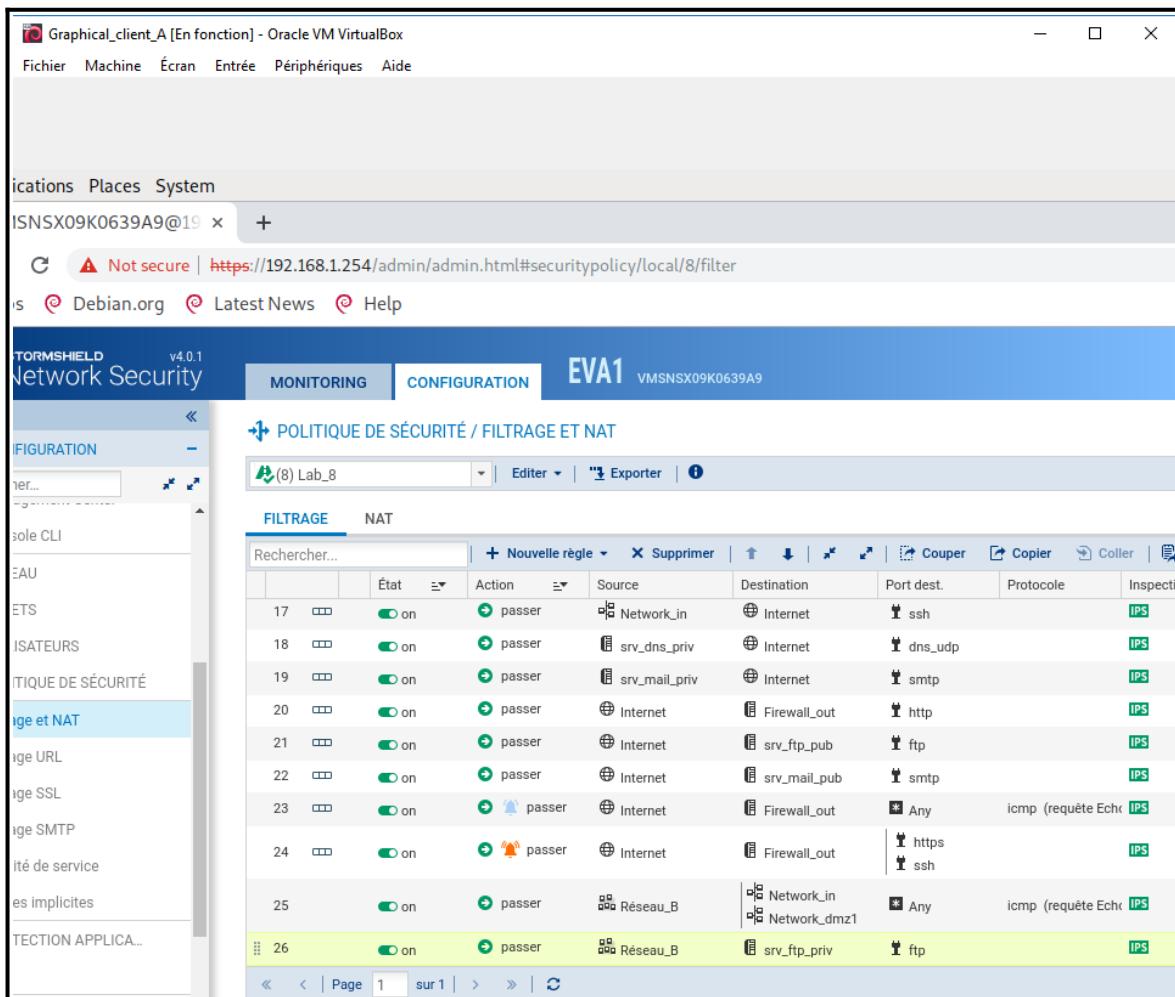
Ligne	Etat	Réseau local	Correspondant	Réseau distant	Profil de chiffrement	Keepalive
1	on	Network_dmz1	Site_Fw_B	Réseau_B	StrongEncryption	30
2	on	Network_in	Site_Fw_B	Réseau_B	StrongEncryption	30

SITE À SITE (GATEWAY-GATEWAY)

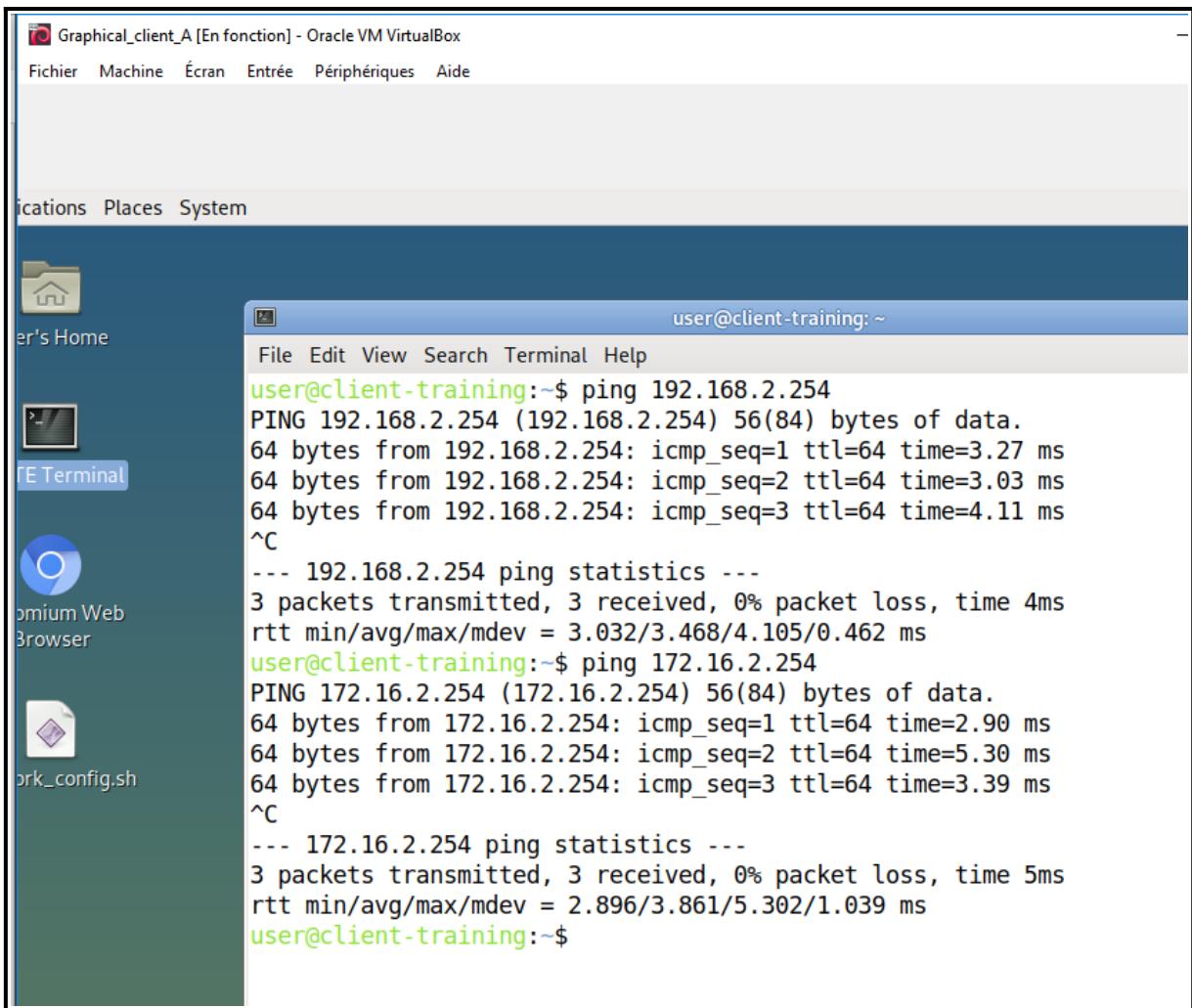
ANONYME - UTILISATEURS NOMADES

Texte recherché	Ajouter	Supprimer	Monter	Descendre	Couper	Copier	Coller

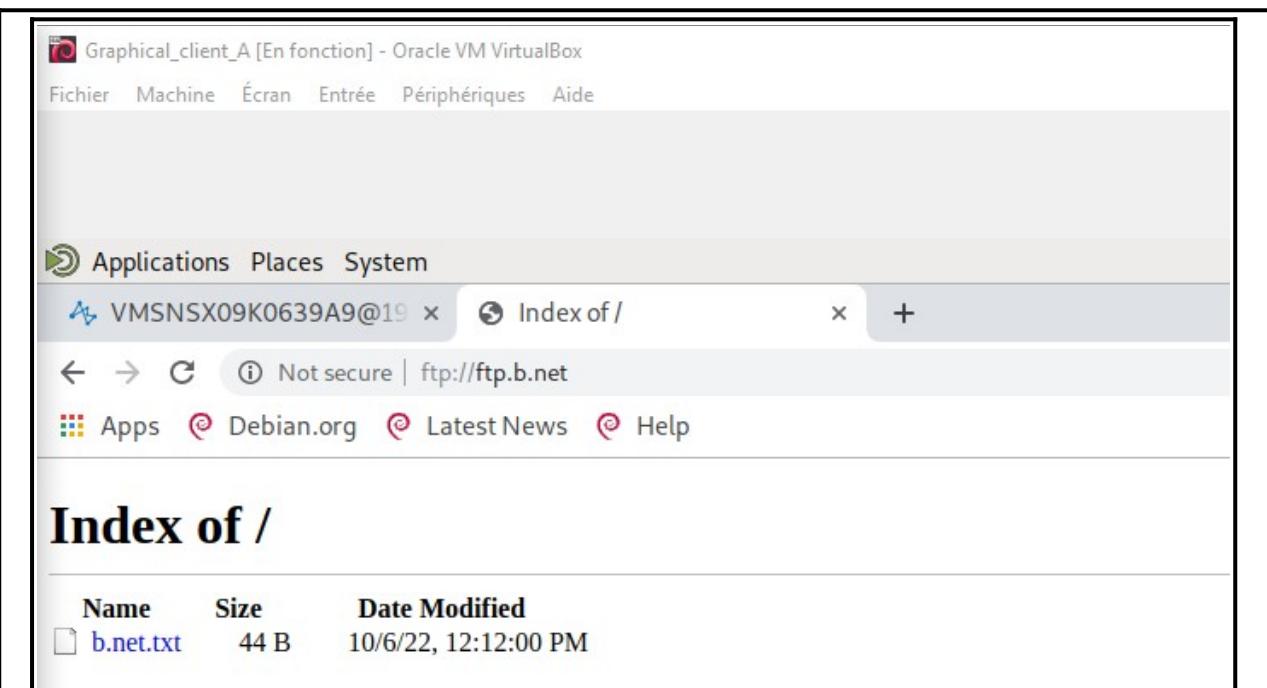
4ème étape : Après avoir créer un objet regroupant le réseau IN et DMZ de B, nous adaptions les extrémités de trafic avec l'option keep-alive à 30.



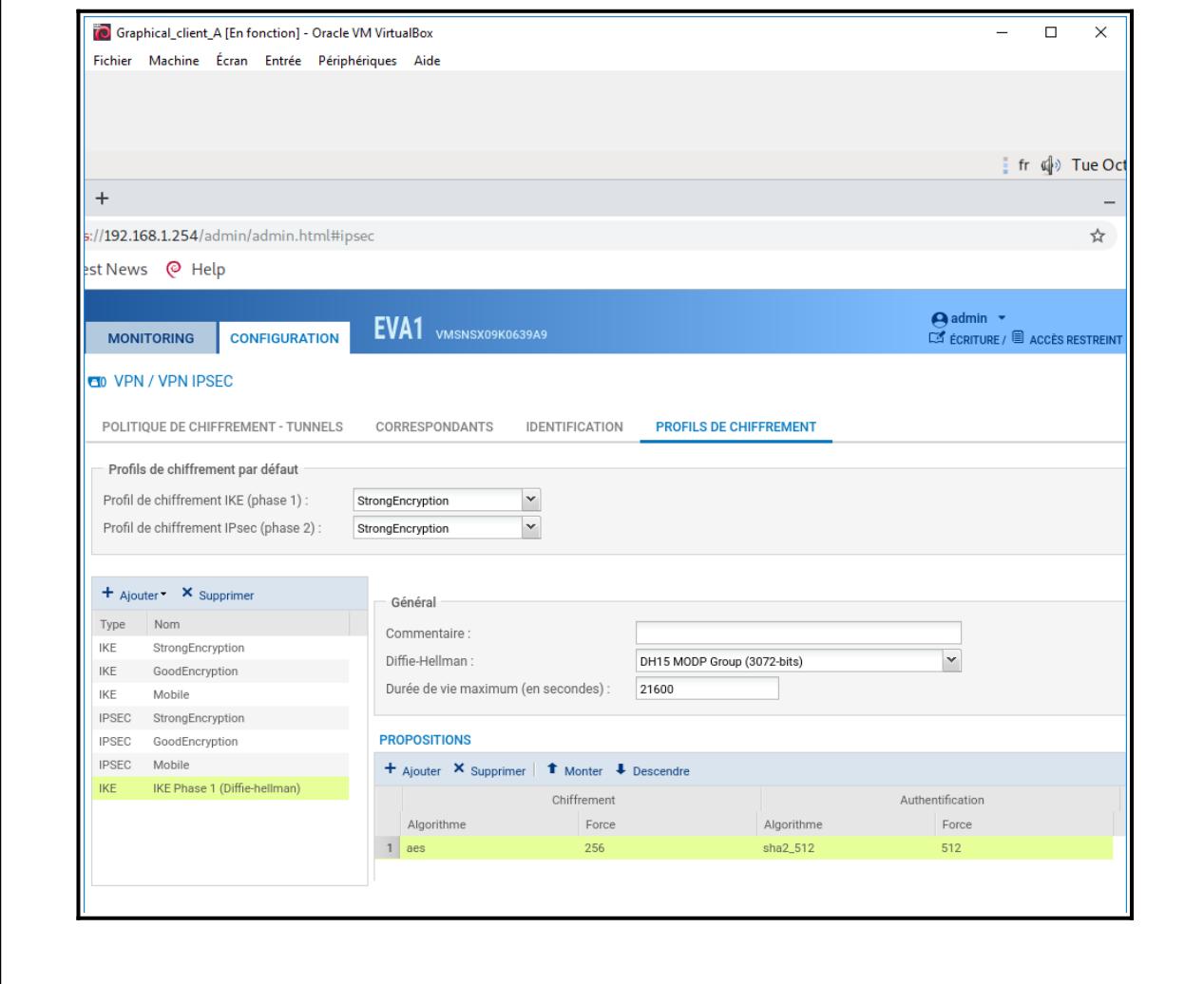
5ème étape : Ajout des règles de filtrages autorisant les réseaux du site B à ping le réseau A ainsi que les serveurs FTP et WEB.



6ème étape : Les règles étant mises en place du côté de B aussi, A peut donc également ping dans le réseau de B.



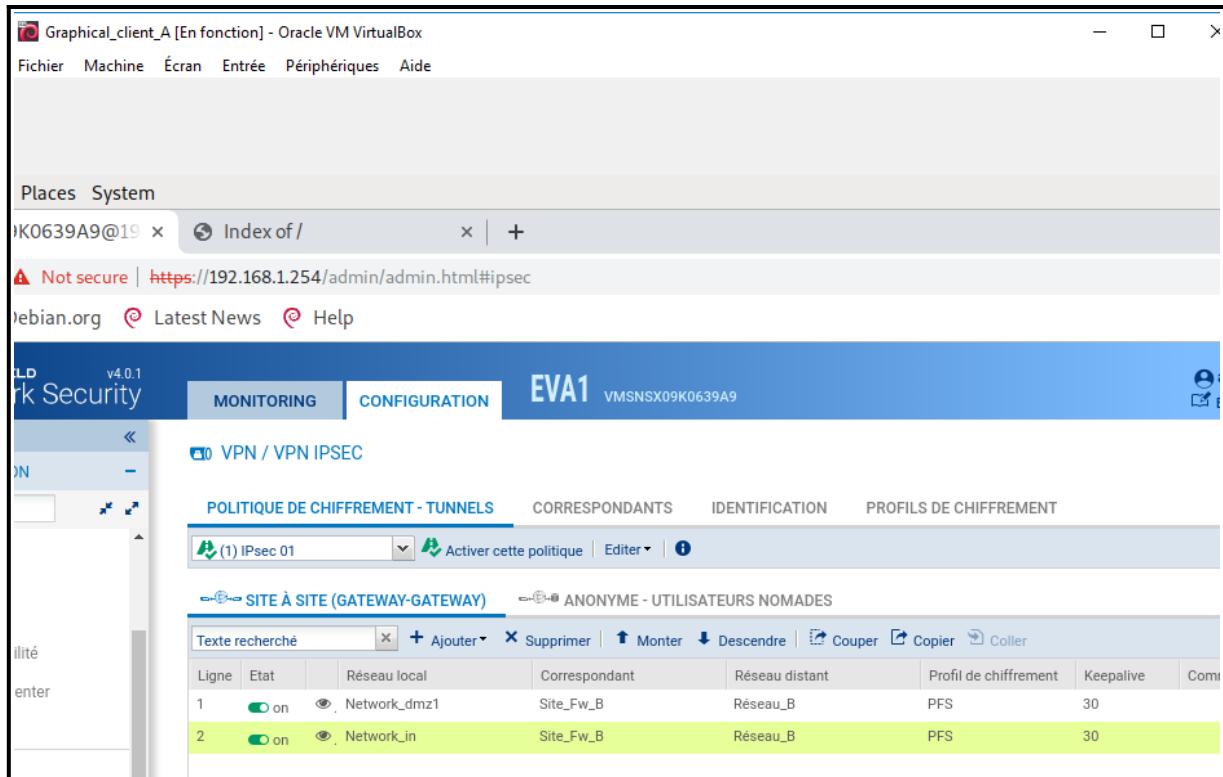
7ème étape : Test d'accès au serveur FTP de B depuis le réseau A.



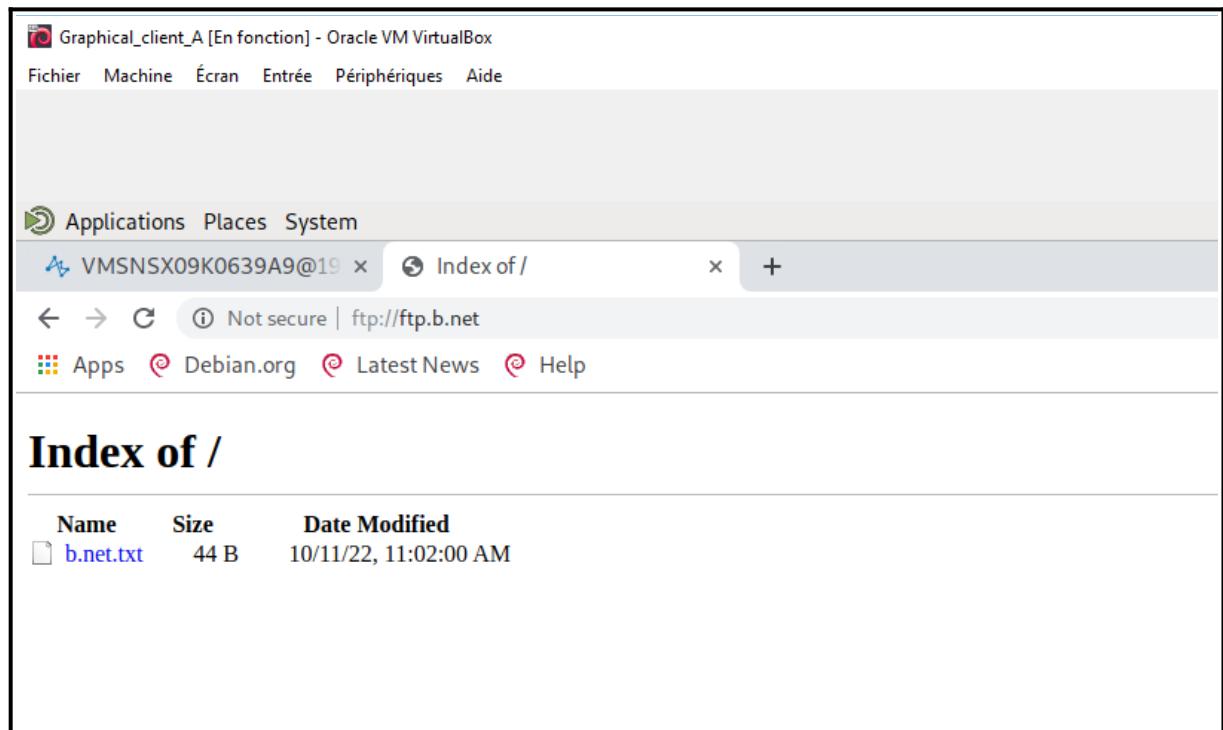
The screenshot shows the EVA1 configuration interface for a VPN/IPsec profile. The 'PROFILS DE CHIFFREMENT' tab is active. The 'Général' section includes fields for 'Commentaire', 'Perfect Forward Secrecy (PFS)', and 'Durée de vie (en secondes)'. The 'PROPOSITIONS D'AUTHENTIFICATION' section lists an algorithm: 'hmac_sha512' with a key length of '512'. On the left, a list of available profiles shows 'PFS' selected.

The screenshot shows the 'PROPOSITIONS DE CHIFFREMENT' configuration interface. The 'aes' profile is selected, showing its properties: 'Algorithme' (aes), 'Force' (256), and 'Taille de clé' (512).

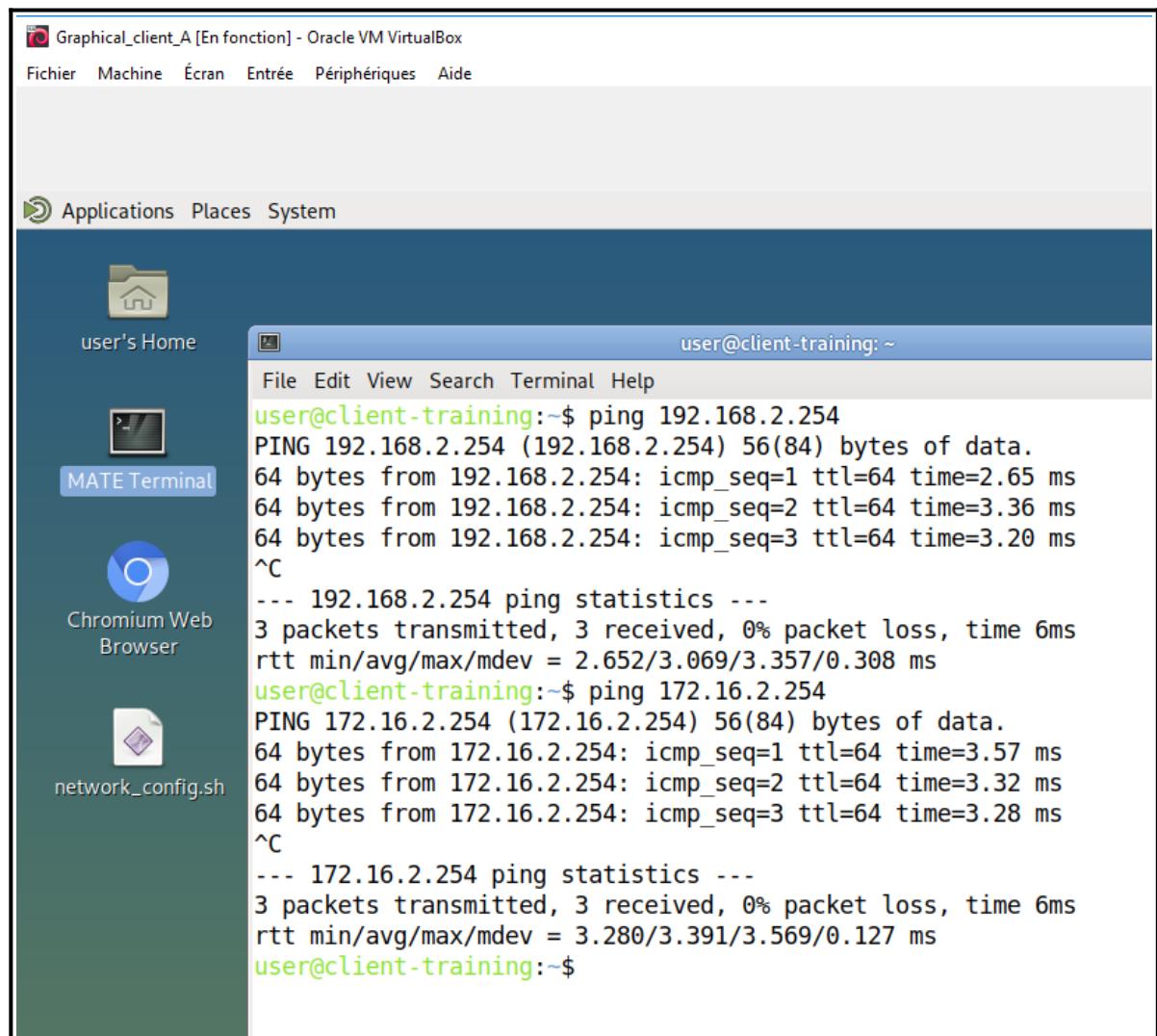
8ème étape : Créez les profils de chiffrement ci-dessus.



9ème : Nous appliquons donc les nouveaux profils de chiffrement créer précédemment sur notre VPN.



10ème étape : Nouveau test d'accès au serveur FTP de B depuis le réseau A.



11ème étape : Nouveaux tests de ping du réseau A vers le réseau B.

Graphical_client_A [En fonction] - Oracle VM VirtualBox

Fichier Machine Écran Entrée Périphériques Aide

Applications Places System

VMSNSX09K0639A9@19 x +

← → C Not secure | <https://192.168.1.254/admin/admin.html#vtigre/ipsec>

Apps Debian.org Latest News Help

STORMSHIELD Network Security v4.0.1

MONITORING CONFIGURATION EVA1 VMSNSX09K0639A9

CONFIGURATION

Rechercher...

Haute disponibilité Management Center Console CLI

RÉSEAU / INTERFACES VIRTUELLES

INTERFACES IPSEC (VTI) INTERFACES GRE LOOPBACK

Rechercher	+ Ajouter	X Supprimer	Vérifier l'utilisation	
État	Nom	Adresse IPv4	Masque IPv4	Commentaire
Activé	VTI_to_B	192.168.120.0	255.255.255.254	

Graphical_client_A [En fonction] - Oracle VM VirtualBox

Fichier Machine Écran Entrée Périphériques Aide

Applications Places System

VMSNSX09K0639A9@19 x +

C Not secure | <https://192.168.1.254/admin/admin.html#networkrouting/routing>

Apps Debian.org Latest News Help

STORMSHIELD Network Security v4.0.1

MONITORING CONFIGURATION EVA1 VMSNSX09K0639A9

CONFIGURATION

Rechercher...

faces virtuelles

age

age multicast

dynamique

Passerelle par défaut (routeur): gw_default

RÉSEAU / ROUTAGE

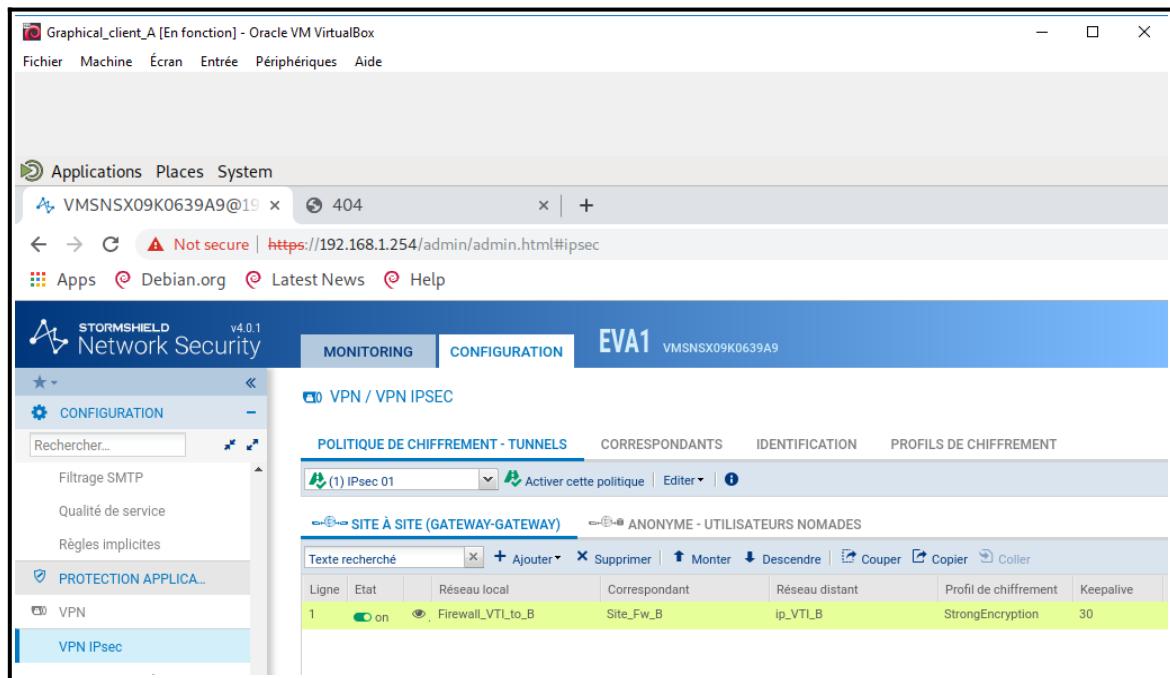
ROUTES STATIQUES IPV4 ROUTAGE DYNAMIQUE ROUTES DE RETOUR IPV4

Configuration générale

Passerelle par défaut (routeur): gw_default

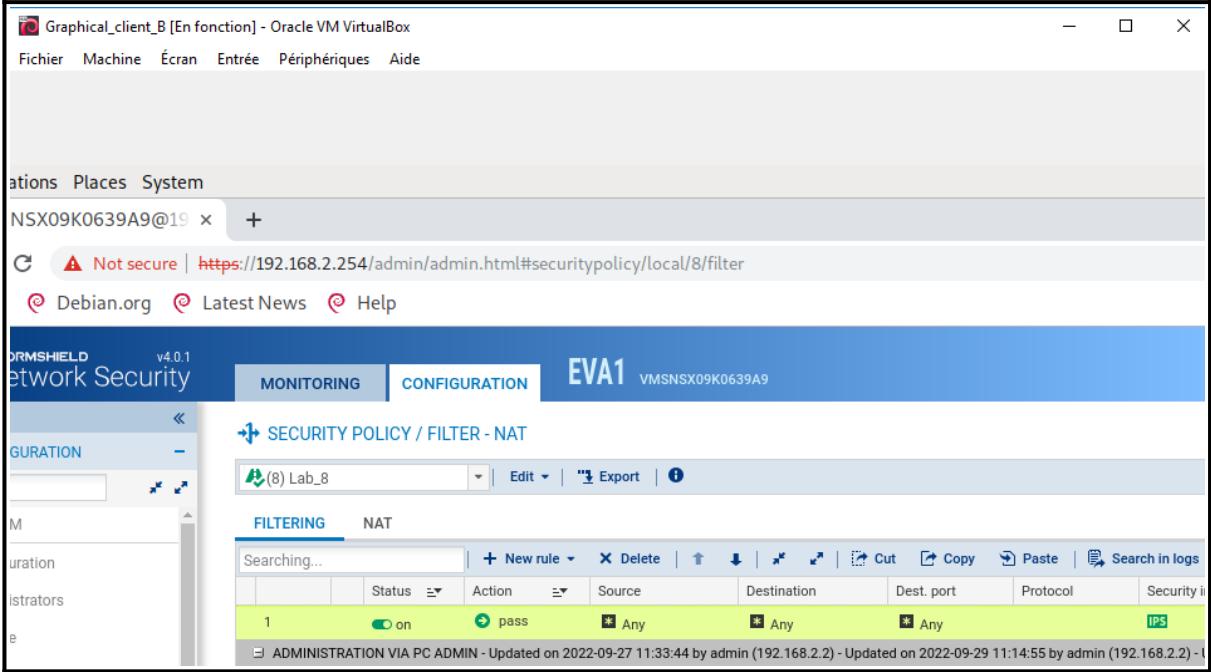
ROUTES STATIQUES

Rechercher...	+ Ajouter	X Supprimer		
État	Réseau de destination (objet ma...)	Interface	Plan d'adressage	Passerelle
on	Lan_in_B	VTI_to_B	192.168.2.0/24	ip_VTI_B



12ème étape : Réalisation de l’interconnexion des réseaux, en configurant des tunnels basés sur des VTI.

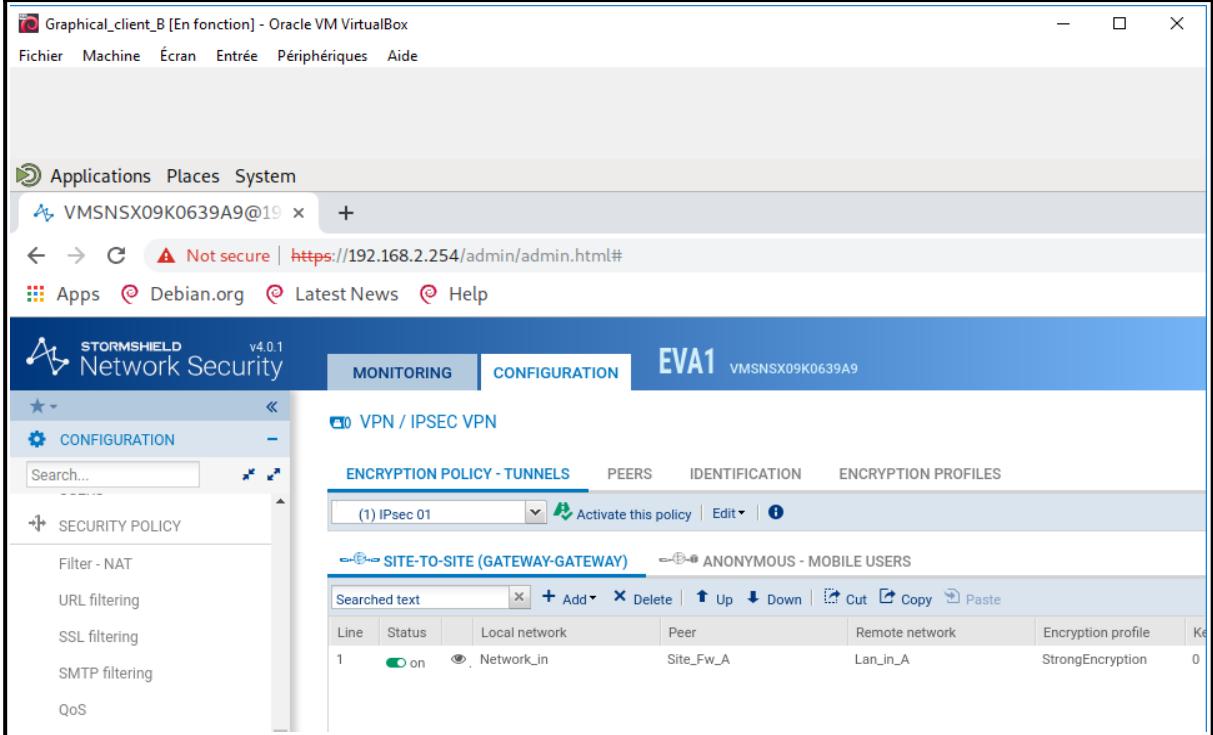
Réseau B :



The screenshot shows the Stormshield Network Security interface. The main title is "SECURITY POLICY / FILTER - NAT". The table below shows a single rule:

Line	Status	Action	Source	Destination	Dest. port	Protocol	Security
1	on	pass	* Any	* Any	* Any	IPS	

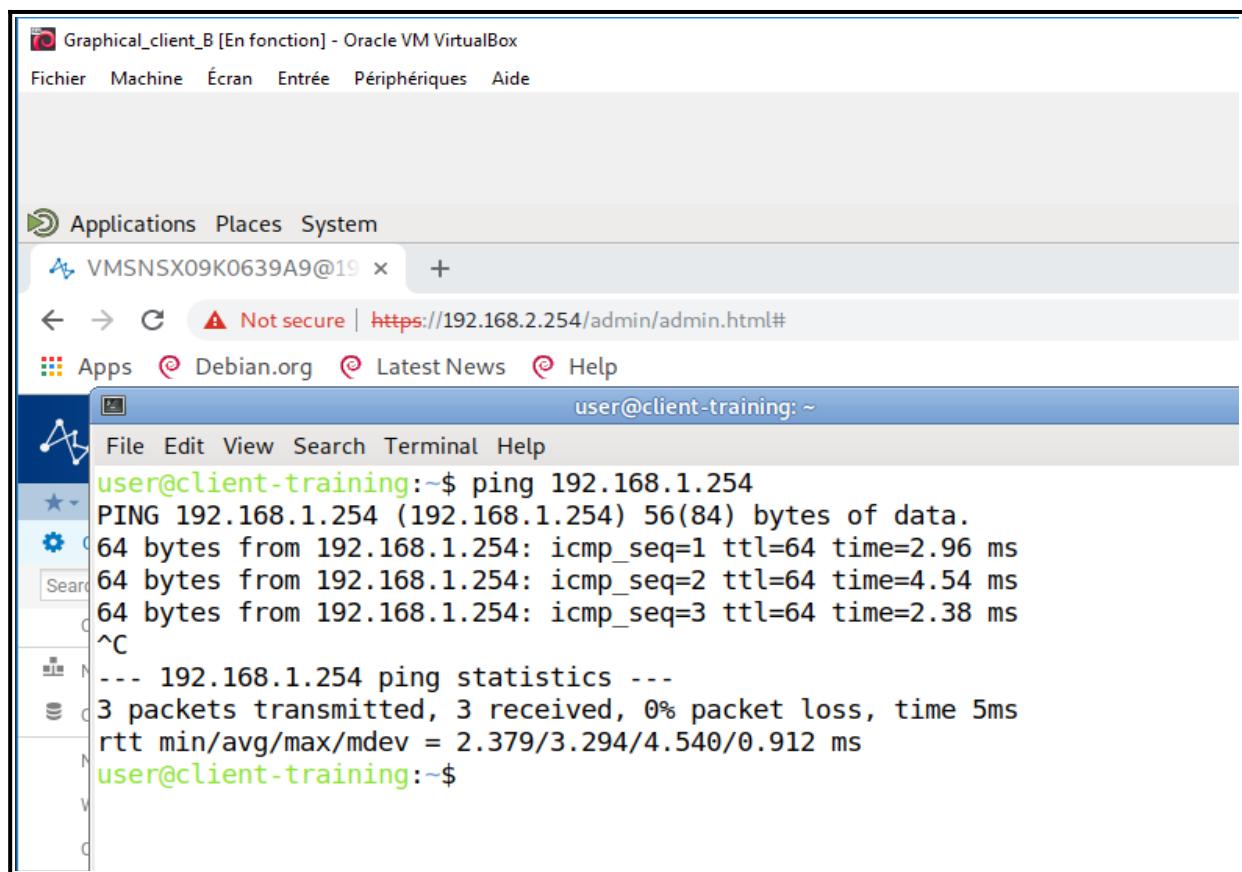
1ère étape : Ajout de la règle de filtrage pass any any.



The screenshot shows the Stormshield Network Security interface. The main title is "VPN / IPSEC VPN". The table below shows the tunnel configuration:

Line	Status	Local network	Peer	Remote network	Encryption profile	Key
1	on	Network_in	Site_Fw_A	Lan_in_A	StrongEncryption	0

2ème étape : Configuration d'un tunnel Ipsec afin de relier le réseau A au réseau B.



Graphical_client_B [En fonction] - Oracle VM VirtualBox

Fichier Machine Écran Entrée Périphériques Aide

Applications Places System

VMSNSX09K0639A9@19 x +

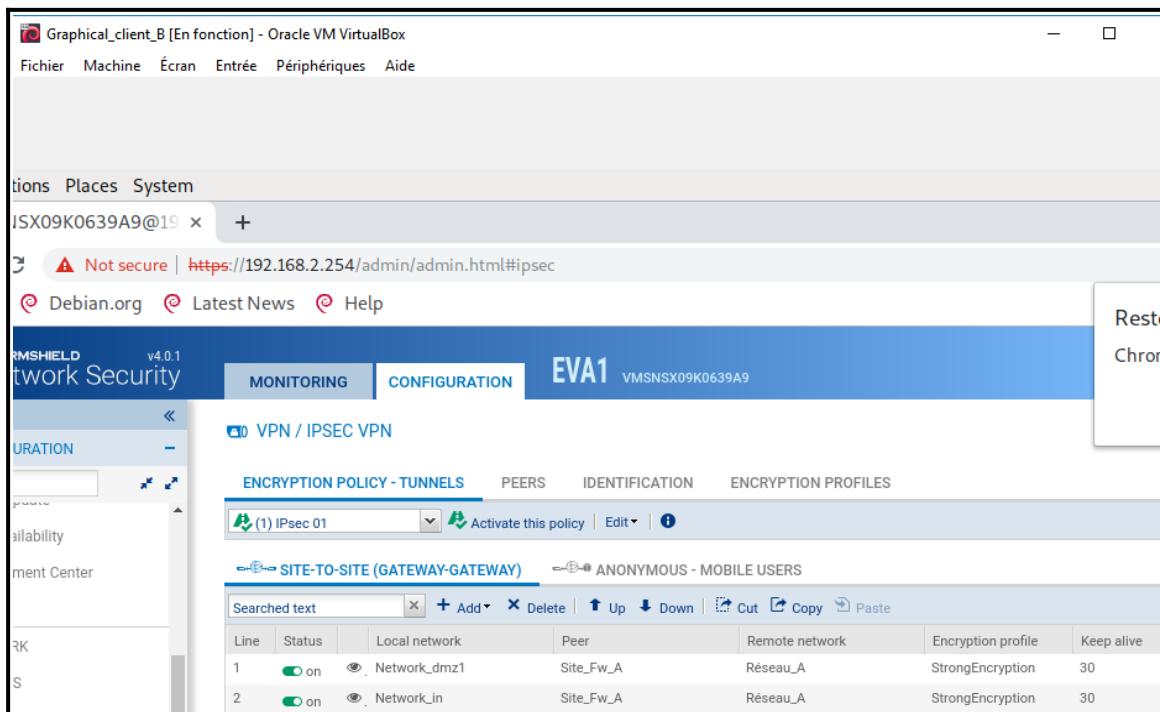
Not secure | <https://192.168.2.254/admin/admin.html#>

Apps Debian.org Latest News Help

user@client-training:~

```
File Edit View Search Terminal Help
user@client-training:~$ ping 192.168.1.254
PING 192.168.1.254 (192.168.1.254) 56(84) bytes of data.
64 bytes from 192.168.1.254: icmp_seq=1 ttl=64 time=2.96 ms
64 bytes from 192.168.1.254: icmp_seq=2 ttl=64 time=4.54 ms
64 bytes from 192.168.1.254: icmp_seq=3 ttl=64 time=2.38 ms
^C
--- 192.168.1.254 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 5ms
rtt min/avg/max/mdev = 2.379/3.294/4.540/0.912 ms
user@client-training:~$
```

3ème étape : Test de ping du réseau B au firewall de A.



Graphical_client_B [En fonction] - Oracle VM VirtualBox

Fichier Machine Écran Entrée Périphériques Aide

Applications Places System

VMSNSX09K0639A9@19 x +

Not secure | <https://192.168.2.254/admin/admin.html#ipsec>

Debian.org Latest News Help

IPMSHIELD v4.0.1

Network Security

MONITORING CONFIGURATION EVA1 VMSNSX09K0639A9

VPN / IPSEC VPN

ENCRIPTION POLICY - TUNNELS PEERS IDENTIFICATION ENCRYPTION PROFILES

(1) IPsec 01 Activate this policy | Edit |

SITE-TO-SITE (GATEWAY-GATEWAY) ANONYMOUS - MOBILE USERS

Searched text + Add x Delete | Up Down | Cut Copy Paste

Line	Status	Local network	Peer	Remote network	Encryption profile	Keep alive
1	on	Network_dmz1	Site_Fw_A	Réseau_A	StrongEncryption	30
2	on	Network_in	Site_Fw_A	Réseau_A	StrongEncryption	30

4ème étape : Après avoir créer un objet regroupant le réseau IN et DMZ de A, nous adaptons les extrémités de trafic avec l'option keep-alive à 30.

SECURITY POLICY / FILTER - NAT

FILTERING NAT

	Status	Action	Source	Destination	Dest. port	Protocol	Security
20	on	pass	Internet	Firewall_out	http	IPS	
21	on	pass	Internet	srv_ftp_pub	ftp	IPS	
22	on	pass	Internet	srv_mail_pub	smtp	IPS	
23	on	pass	Internet	Firewall_out	Any	icmp (Echo requests)	
24	on	pass	Internet	Firewall_out	https	IPS	
25	on	pass	Réseau_A	Network_in	Any	icmp (Echo requests)	
26	on	pass	Réseau_A	srv_ftp_priv	ftp	IPS	

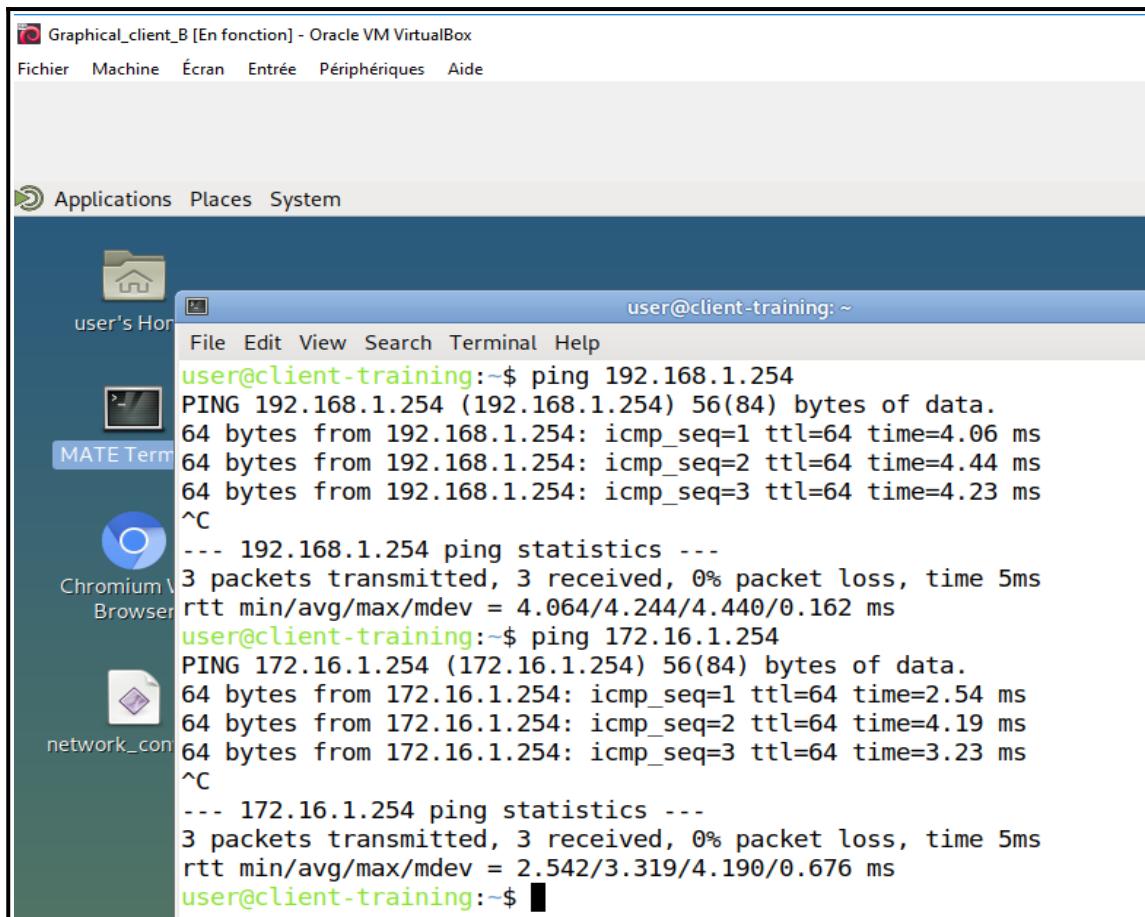
SECURITY POLICY / FILTER - NAT

FILTERING NAT

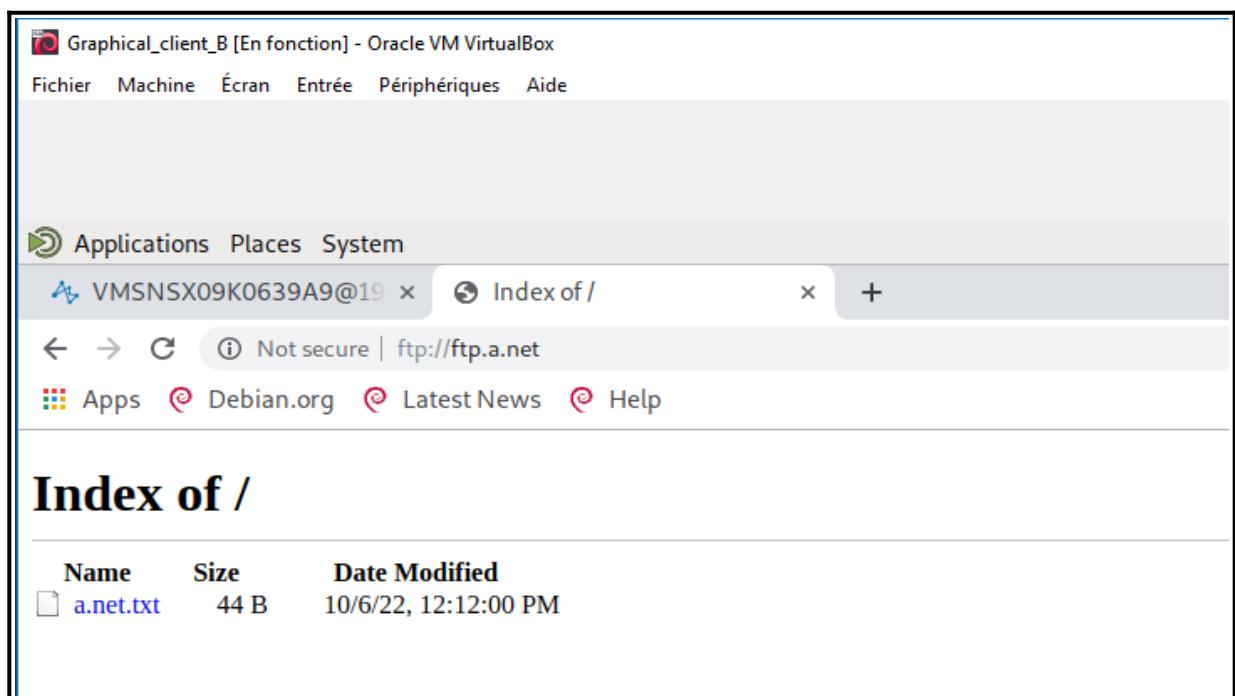
	Status	Action	Source	Destination	Dest. port	Protocol	Security
1	on	pass	Network_in	ftp_A_priv	ftp	IPS	
2	on	pass	Network_in	Any	Any	icmp (Echo requests)	

ADMINISTRATION VIA PC ADMIN - Updated on 2022-09-27 11:33:44 by admin (192.168.2.2) - Updated on 2022-09-29 11:14:55 by admin (192.168.2.2) - Updated on (co)

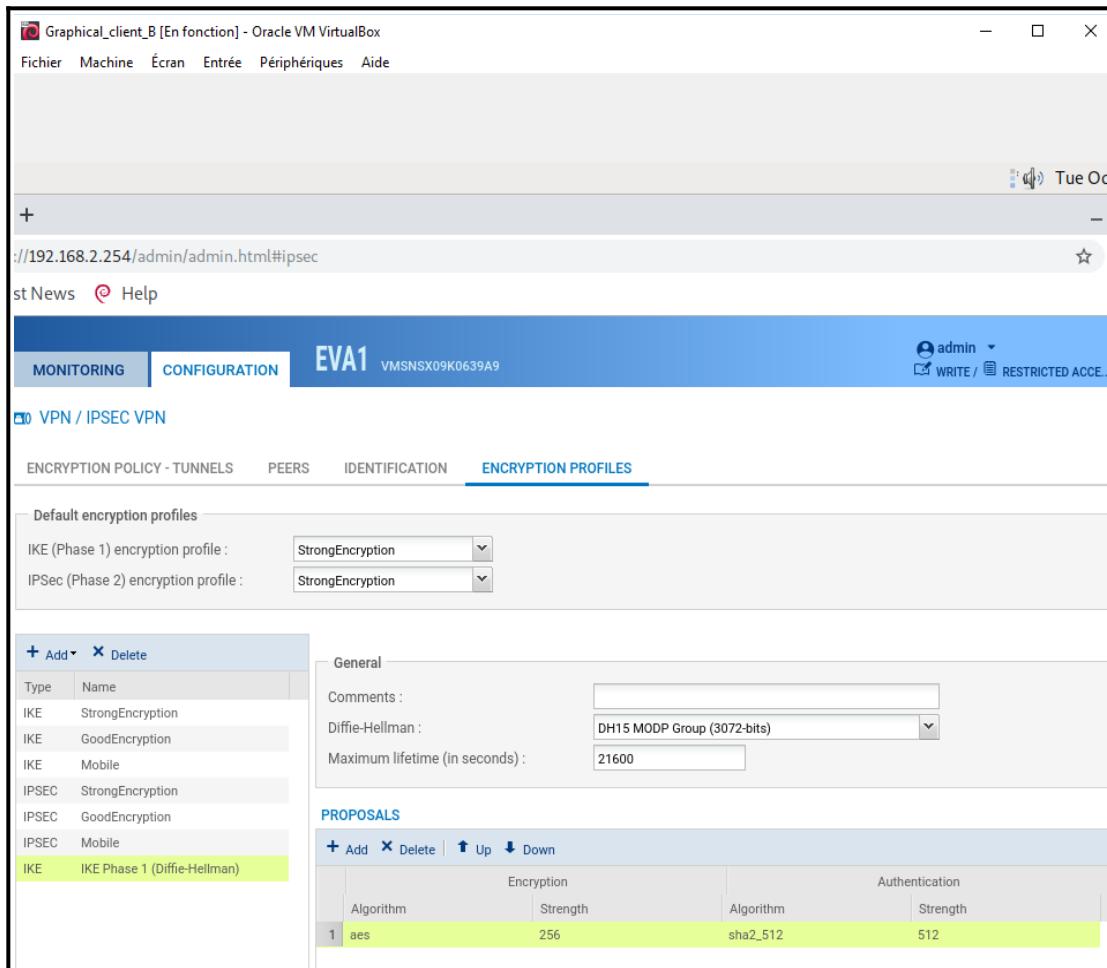
5ème étape : Ajout des règles de filtrages autorisant les réseaux du site A à ping le réseau B ainsi que les serveurs FTP et WEB.



6ème étape : Les règles étant mises en place du côté de A aussi, B peut donc également ping dans le réseau de A.



7ème étape : Test d'accès au serveur FTP de B depuis le réseau A.



Graphical_client_B [En fonction] - Oracle VM VirtualBox

Fichier Machine Écran Entrée Périphériques Aide

+ -

:/192.168.2.254/admin/admin.html#ipsec

st News Help

MONITORING CONFIGURATION EVA1 VMSNSX09K0639A9 admin WRITE / RESTRICTED ACCE...

VPN / IPSEC VPN

ENCRYPTION POLICY - TUNNELS PEERS IDENTIFICATION ENCRYPTION PROFILES

Default encryption profiles

IKE (Phase 1) encryption profile : StrongEncryption

IPSec (Phase 2) encryption profile : StrongEncryption

+ Add × Delete

Type	Name
IKE	StrongEncryption
IKE	GoodEncryption
IKE	Mobile
IPSEC	StrongEncryption
IPSEC	GoodEncryption
IPSEC	Mobile
IKE	IKE Phase 1 (Diffie-Hellman)
IPSEC	IPSEC Phase 2 (PFS)

General

Comments :

Perfect Forward Secrecy (PFS) : DH15 MODP Group (3072-bits)

Lifetime (in seconds) : 3600

AUTHENTICATION PROPOSALS

+ Add × Delete

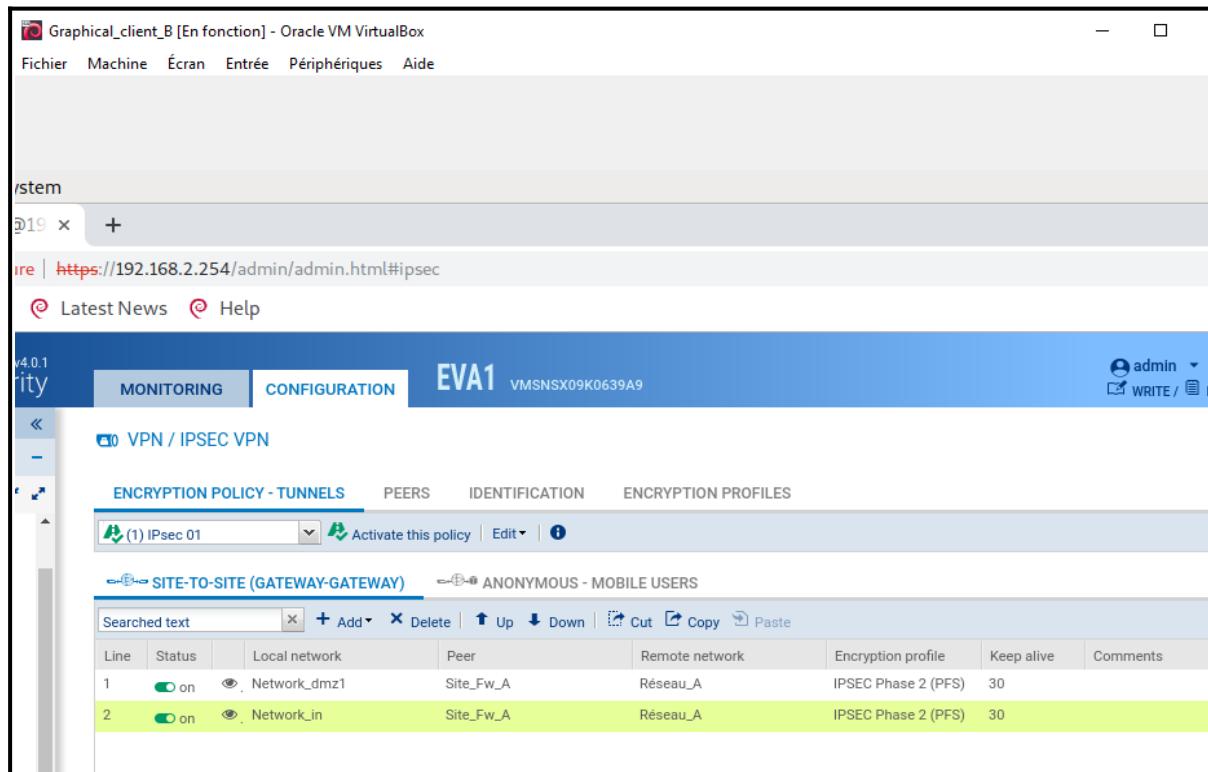
Algorithm	Strength
1 hmac_sha512	512

ENCRYPTION PROPOSALS

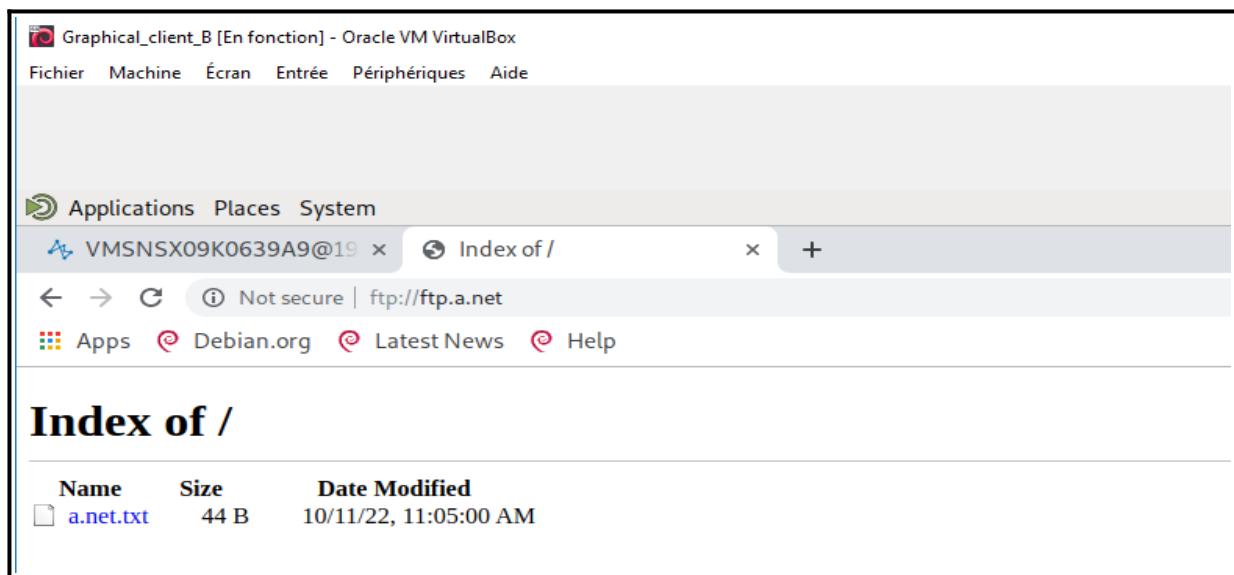
+ Add × Delete

Algorithm	Strength
1 aes	256

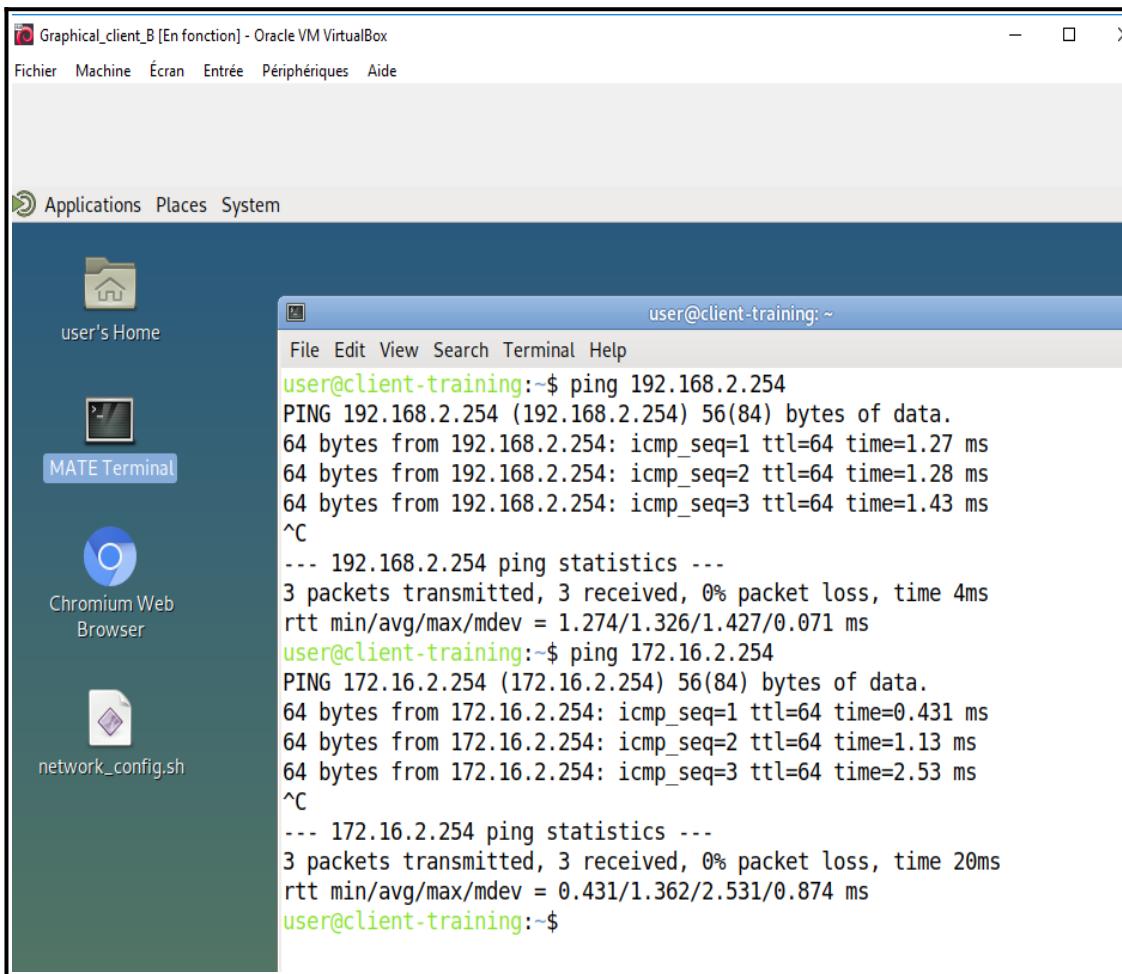
8ème étape : Création des profils de chiffrement ci-dessus.



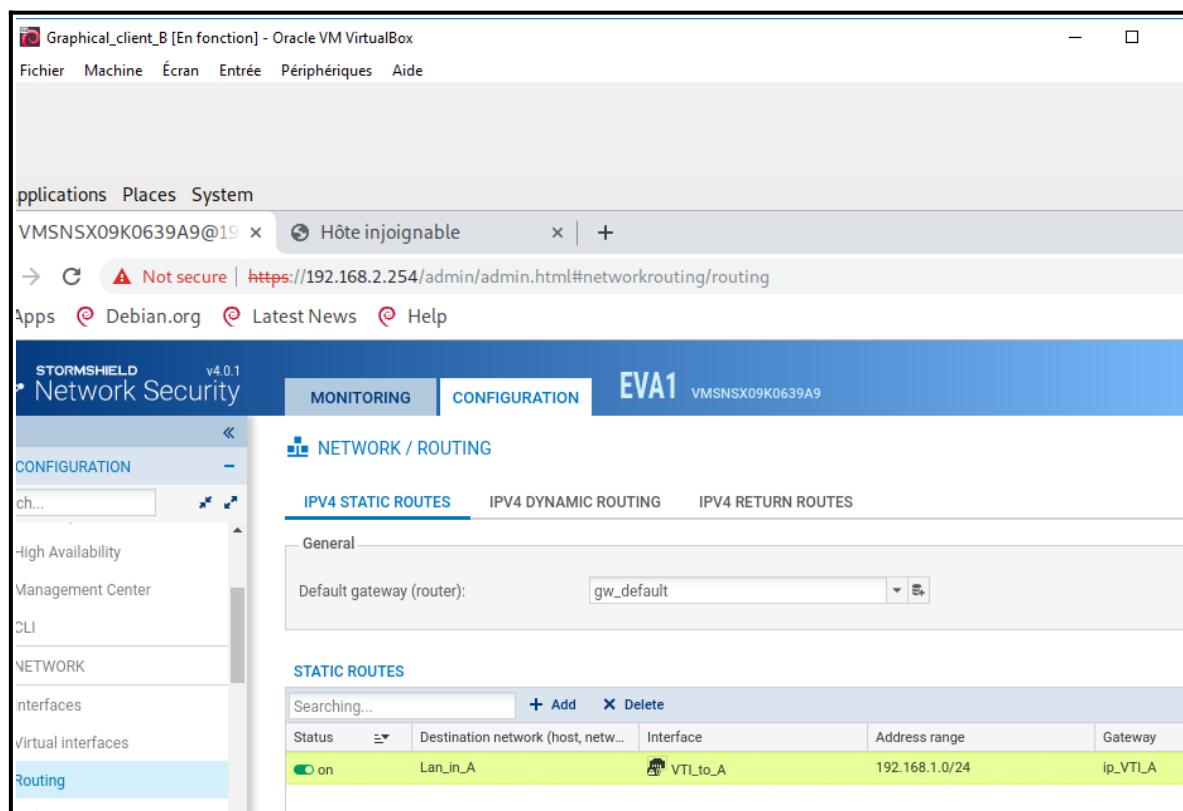
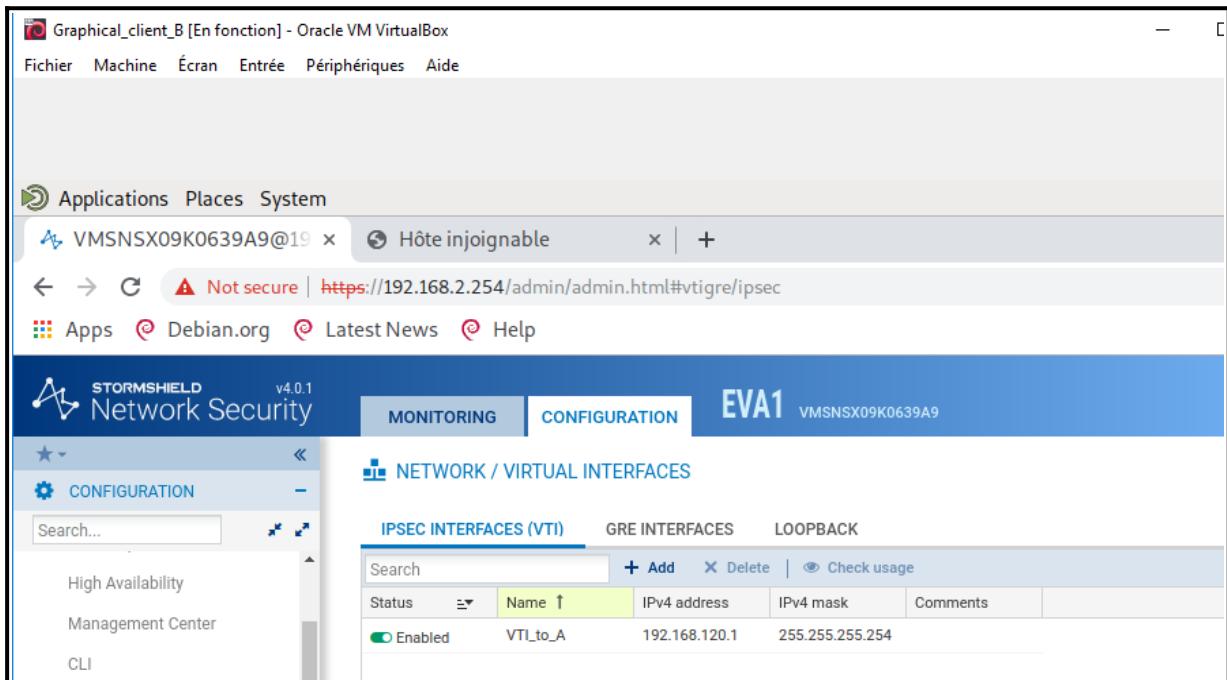
9ème : Nous appliquons donc les nouveaux profils de chiffrement créer précédemment sur notre VPN.

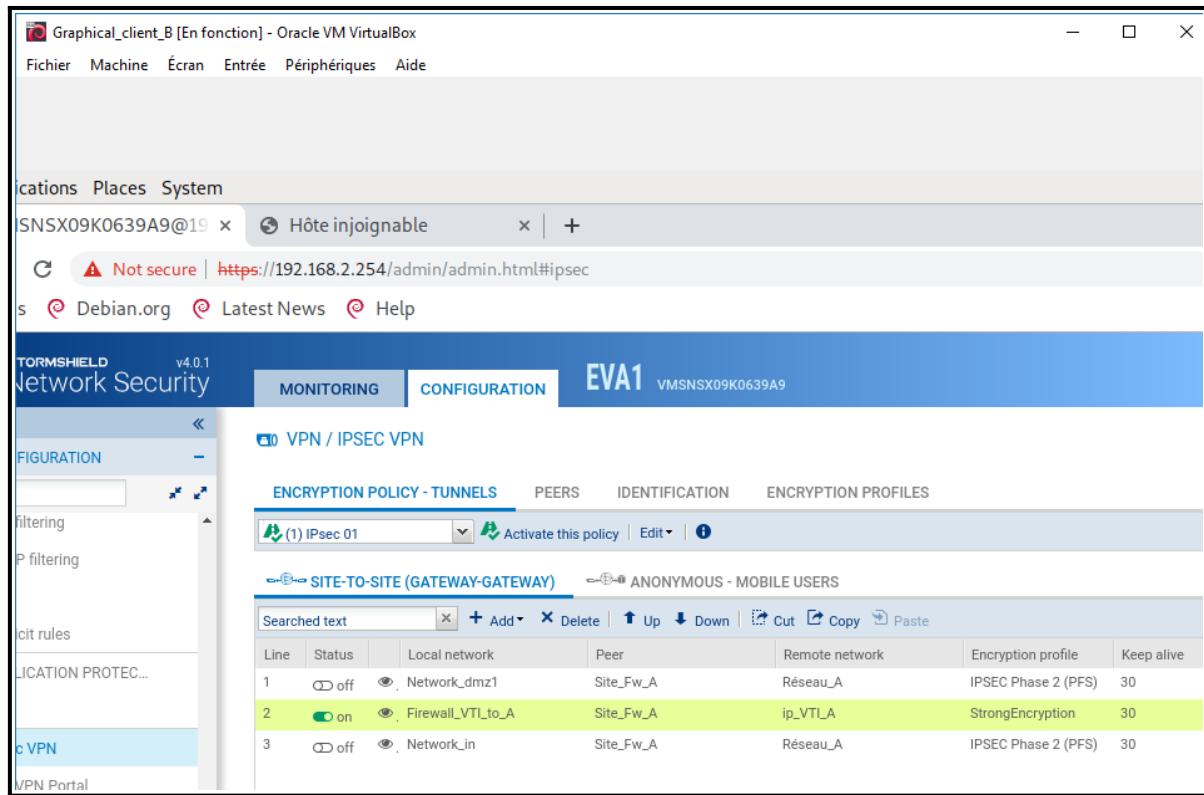


10ème étape : Nouveau test d'accès au serveur FTP de A depuis le réseau B.



11ème étape : Nouveaux tests de ping du réseau A vers le réseau B.





12ème étape : Réalisation de l'interconnexion des réseaux, en configurant des tunnels basés sur des VTI.