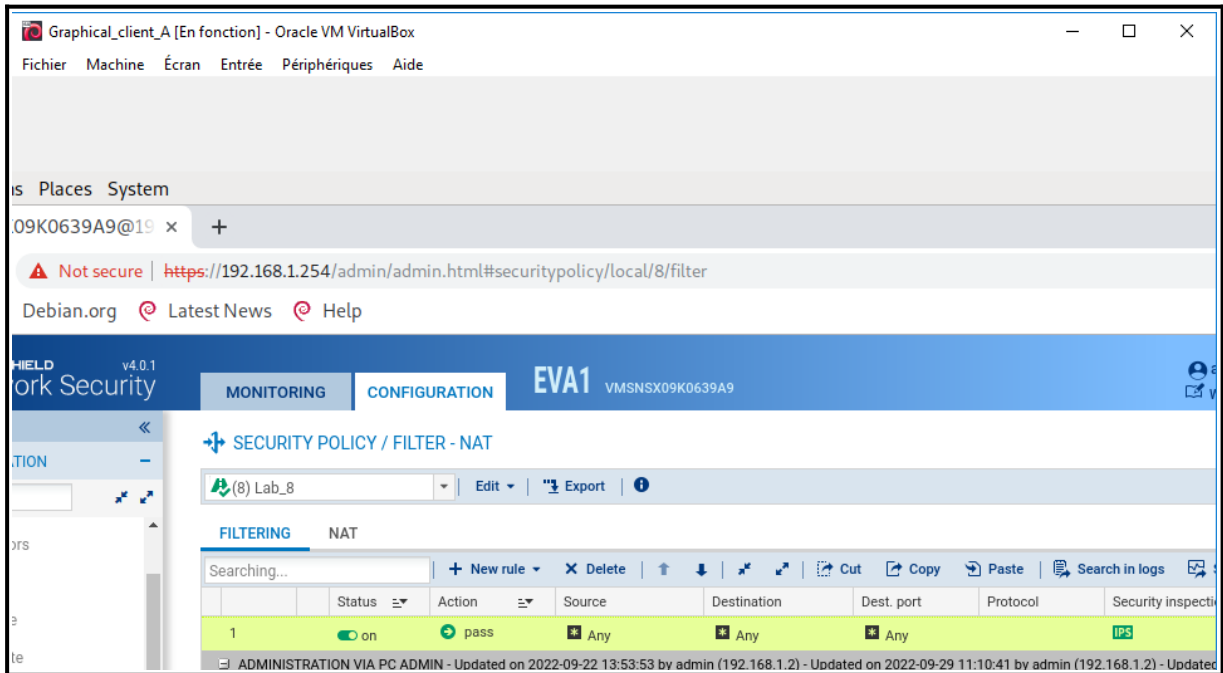




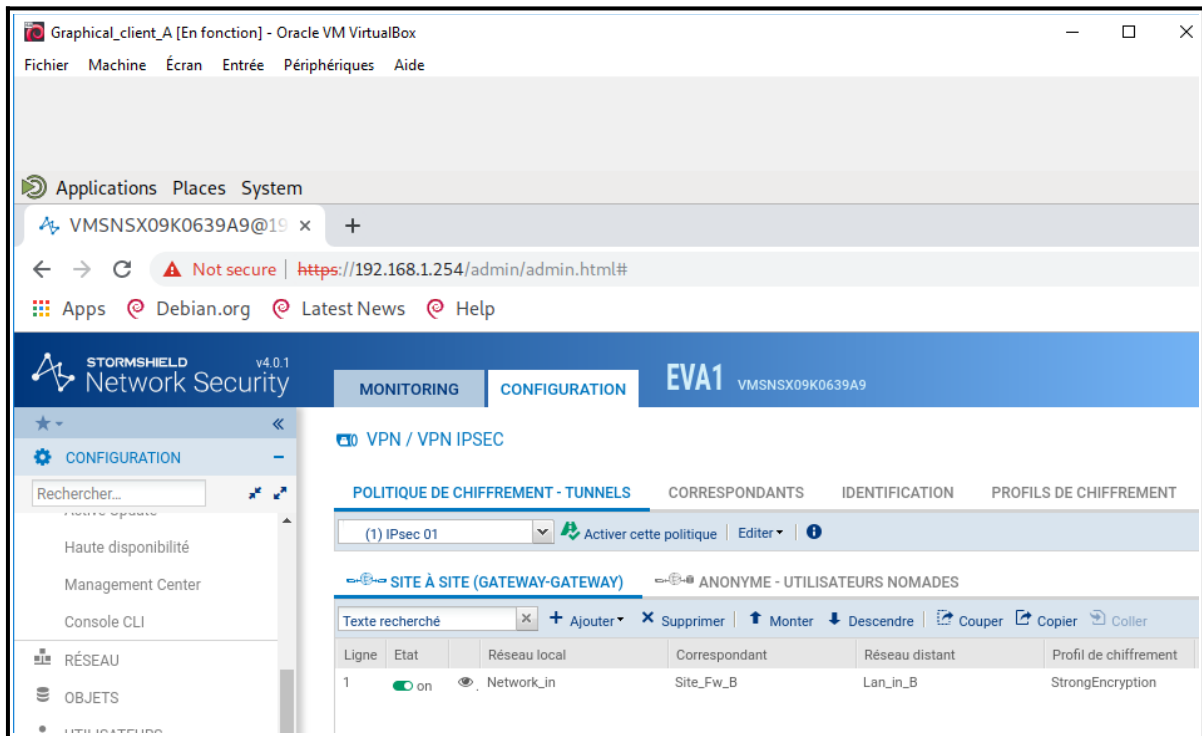
**STORMSHIELD**

# **LAB 8 : VPN IPsec**

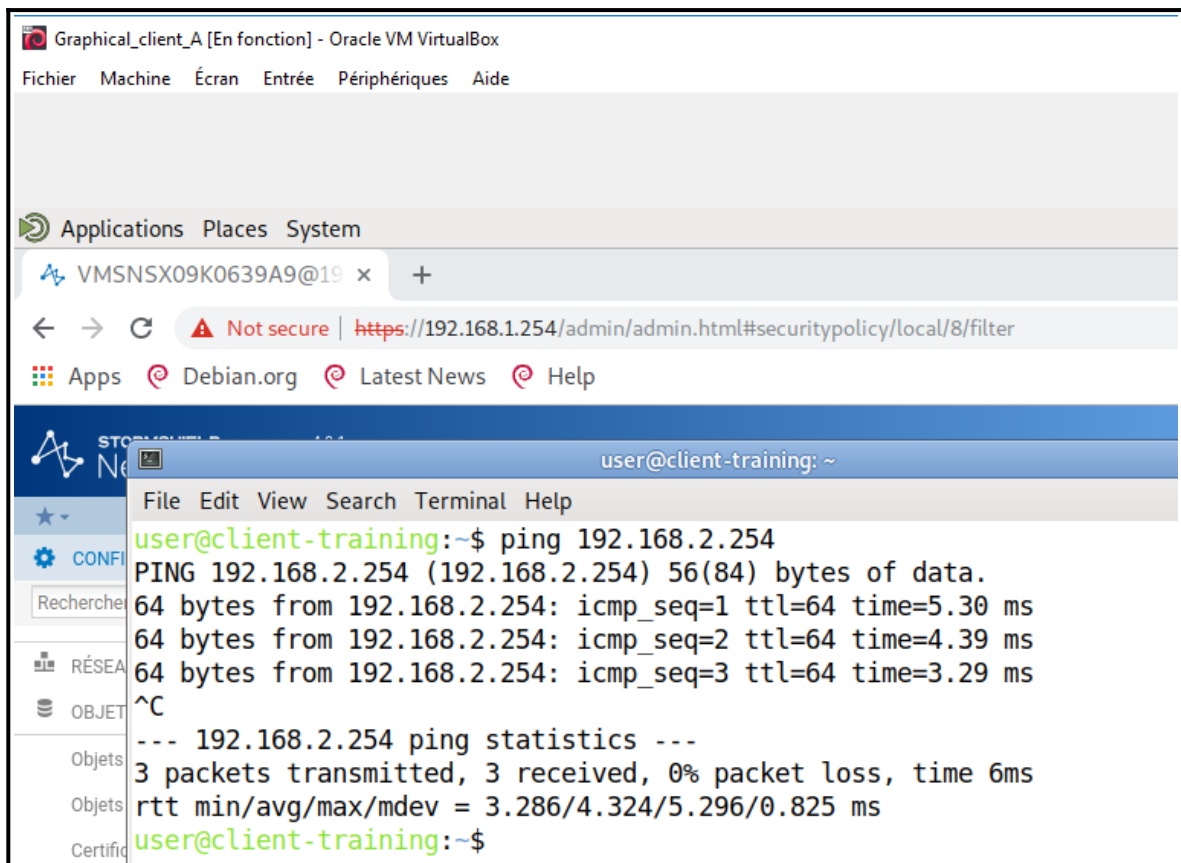
### Réseau A :



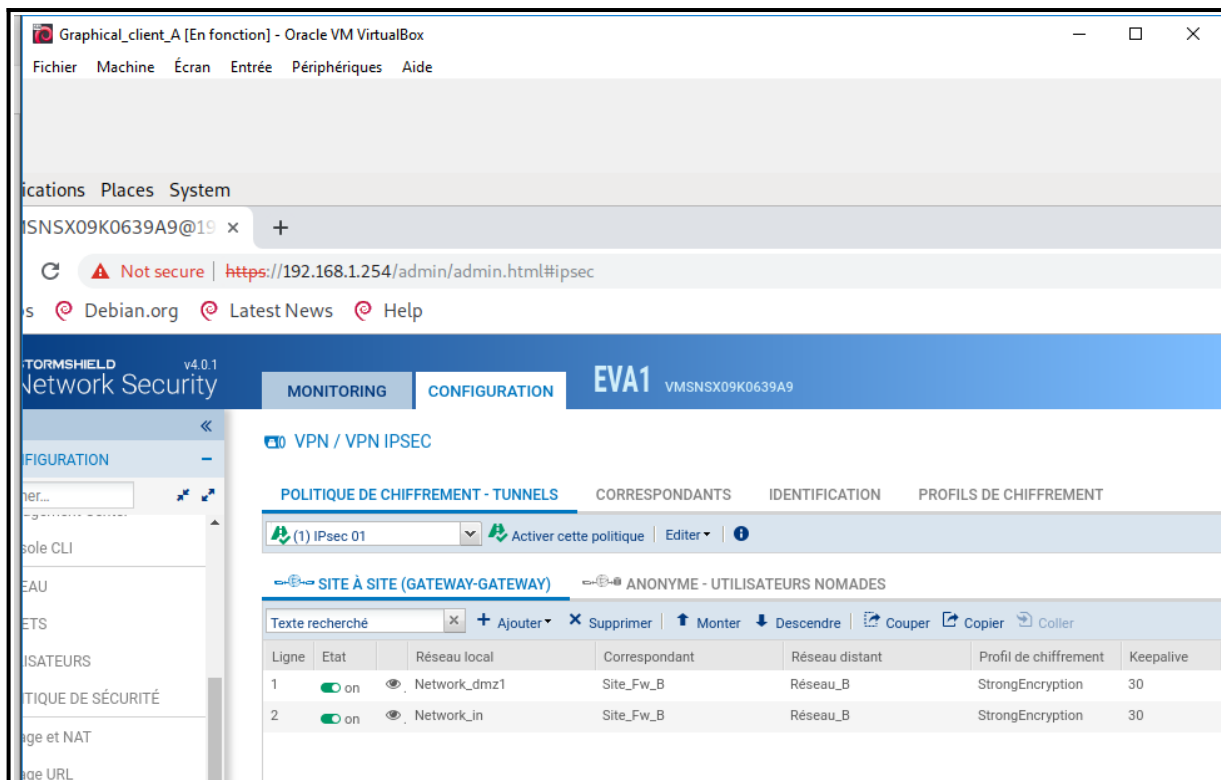
**1ère étape** : Ajout de la règle de filtrage pass any any.



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



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



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

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>

Debian.org Latest News Help

STORMSHIELD Network Security v4.0.1

MONITORING CONFIGURATION EVA1 VMSNSX09K0639A9

POLITIQUE DE SÉCURITÉ / FILTRAGE ET NAT

(8) Lab\_8

FILTRAGE NAT

	État	Action	Source	Destination	Port dest.	Protocole	Inspection
17	on	passer	Network_in	Internet	ssh		IPS
18	on	passer	srv_dns_priv	Internet	dns_udp		IPS
19	on	passer	srv_mail_priv	Internet	smtp		IPS
20	on	passer	Internet	Firewall_out	http		IPS
21	on	passer	Internet	srv_ftp_pub	ftp		IPS
22	on	passer	Internet	srv_mail_pub	smtp		IPS
23	on	passer	Internet	Firewall_out	Any	icmp (requête Echo)	IPS
24	on	passer	Internet	Firewall_out	https, ssh		IPS
25	on	passer	Réseau_B	Network_in, Network_dmz1	Any	icmp (requête Echo)	IPS
26	on	passer	Réseau_B	srv_ftp_priv	ftp		IPS

Page 1 sur 1

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

STORMSHIELD Network Security v4.0.1

MONITORING CONFIGURATION EVA1 VMSNSX09K0639A9

POLITIQUE DE SÉCURITÉ / FILTRAGE ET NAT

(8) Lab\_8

FILTRAGE NAT

	État	Action	Source	Destination	Port dest.	Protocole
1	on	passer	Network_in	ftp_B_priv	ftp	
2	on	passer	Network_in	ftp_B_priv	Any	icmp (requête Echo)

**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.

```
Graphical_client_A [En fonction] - Oracle VM VirtualBox
Fichier  Machine  Écran  Entrée  Périphériques  Aide

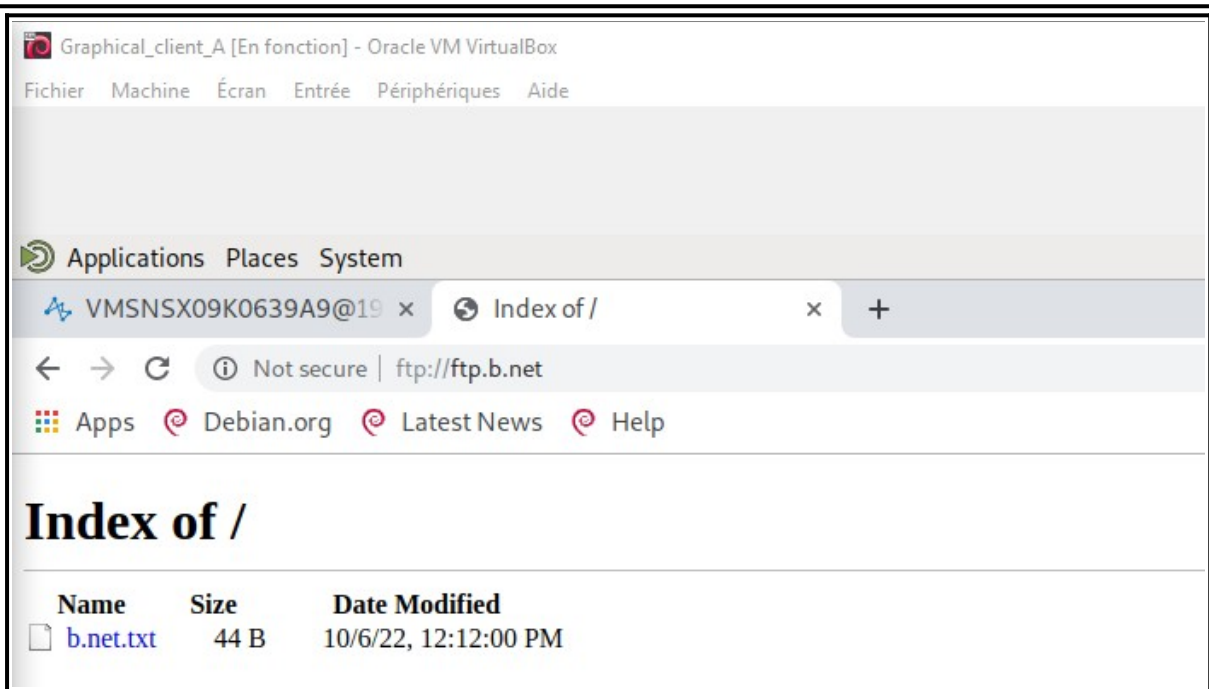
Applications  Places  System

er's Home
Terminal
mium Web Browser
ork_config.sh

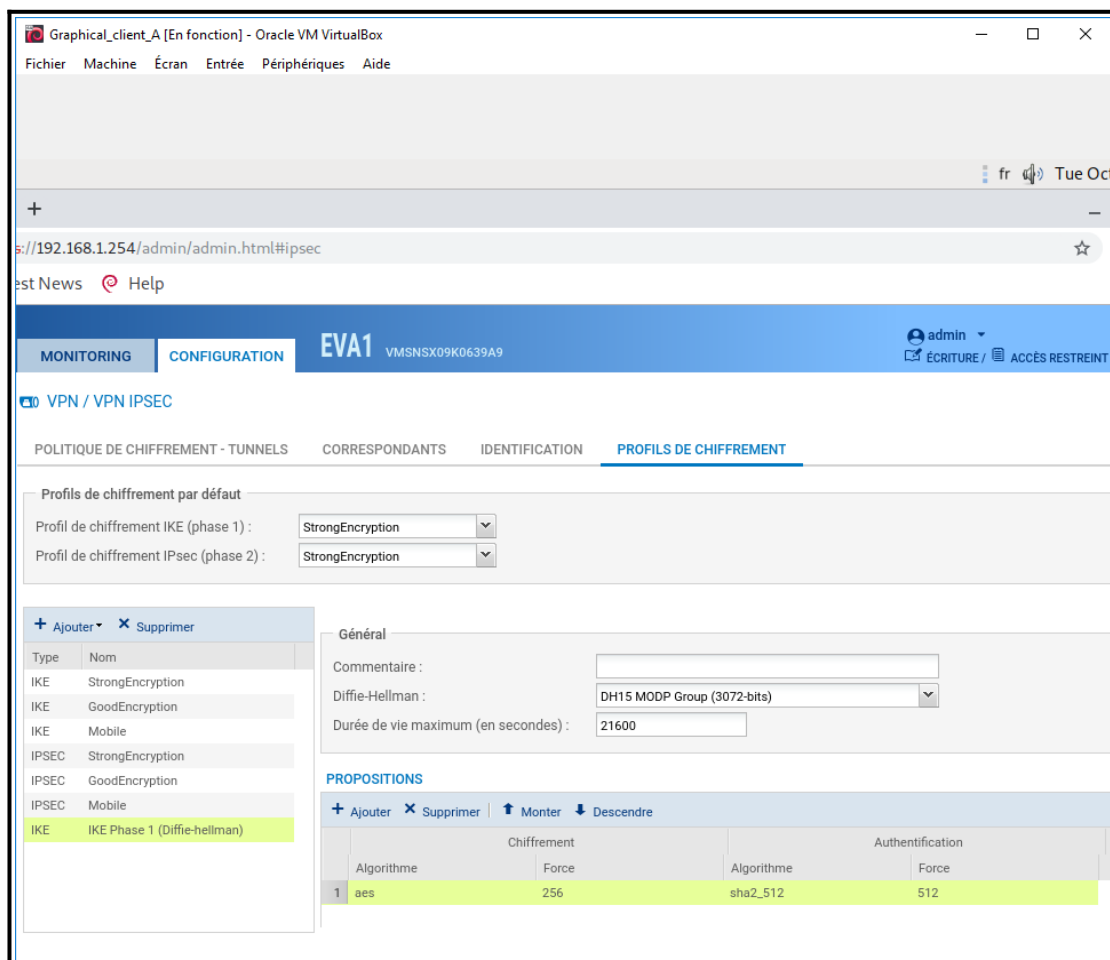
user@client-training: ~
File Edit View Search Terminal Help

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=3.27 ms
64 bytes from 192.168.2.254: icmp_seq=2 ttl=64 time=3.03 ms
64 bytes from 192.168.2.254: icmp_seq=3 ttl=64 time=4.11 ms
^C
--- 192.168.2.254 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 4ms
rtt min/avg/max/mdev = 3.032/3.468/4.105/0.462 ms
user@client-training:~$ ping 172.16.2.254
PING 172.16.2.254 (172.16.2.254) 56(84) bytes of data.
64 bytes from 172.16.2.254: icmp_seq=1 ttl=64 time=2.90 ms
64 bytes from 172.16.2.254: icmp_seq=2 ttl=64 time=5.30 ms
64 bytes from 172.16.2.254: icmp_seq=3 ttl=64 time=3.39 ms
^C
--- 172.16.2.254 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 5ms
rtt min/avg/max/mdev = 2.896/3.861/5.302/1.039 ms
user@client-training:~$
```

**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.



Graphical\_client\_A [En fonction] - Oracle VM VirtualBox

Fichier Machine Écran Entrée Périphériques Aide

fr Tue Oc

+/192.168.1.254/admin/admin.html#ipsec

st News Help

MONITORING CONFIGURATION EVA1 VMSNSX09K0639A9 admin ÉCRITURE / ACCÈS RESTREINT

VPN / VPN IPSEC

POLITIQUE DE CHIFFREMENT - TUNNELS CORRESPONDANTS IDENTIFICATION PROFILS DE CHIFFREMENT

Profils de chiffrement par défaut

Profil de chiffrement IKE (phase 1) : StrongEncryption

Profil de chiffrement IPsec (phase 2) : StrongEncryption

+ Ajouter × Supprimer

Type	Nom
IKE	StrongEncryption
IKE	GoodEncryption
IKE	Mobile
IPSEC	StrongEncryption
IPSEC	GoodEncryption
IPSEC	Mobile
IKE	IKE Phase 1 (Diffie-hellman)
IPSEC	PFS

Général

Commentaire :

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

Durée de vie (en secondes) : 3600

PROPOSITIONS D'AUTHENTIFICATION

+ Ajouter × Supprimer

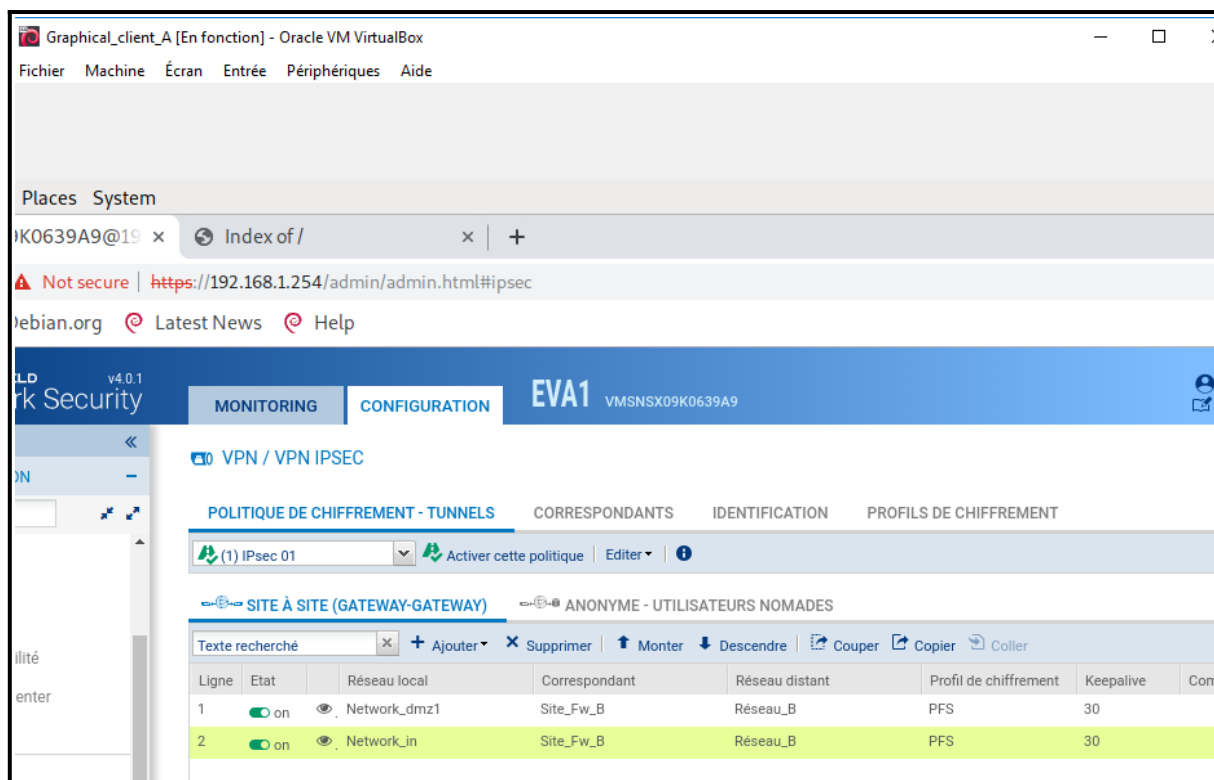
	Algorithme	Force
1	hmac_sha512	512

PROPOSITIONS DE CHIFFREMENT

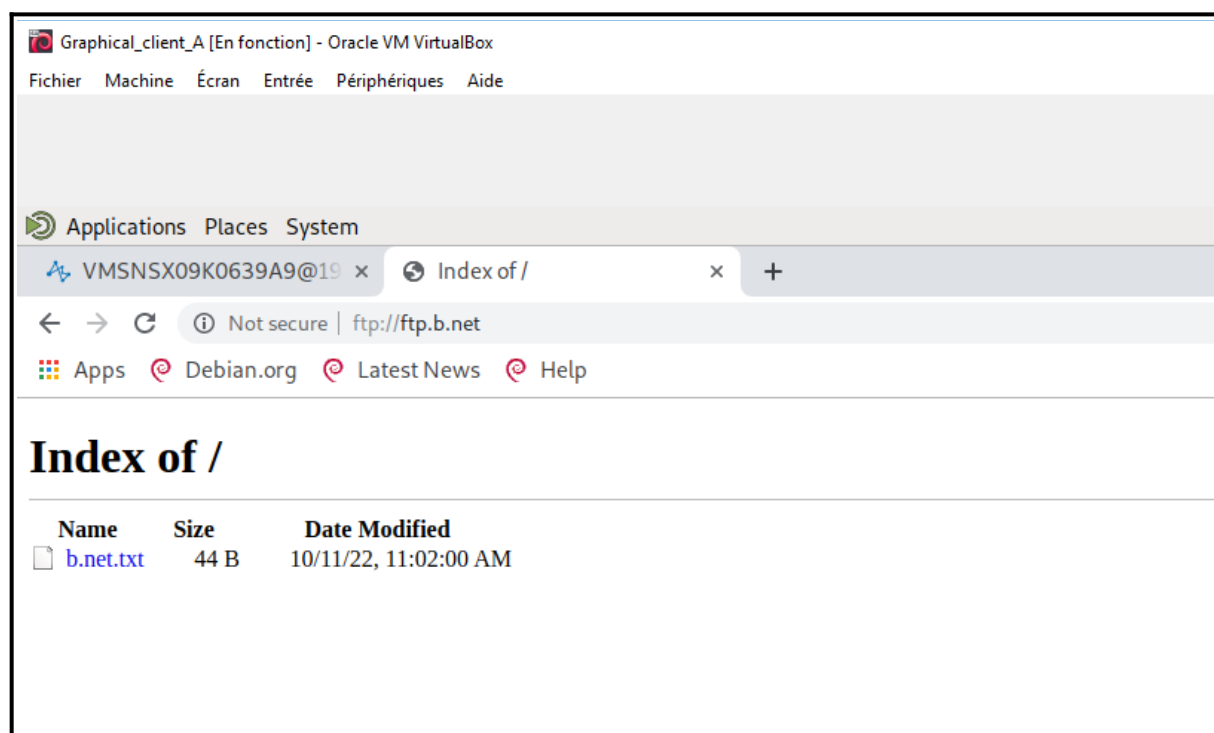
+ Ajouter × Supprimer

	Algorithme	Force
1	aes	256

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

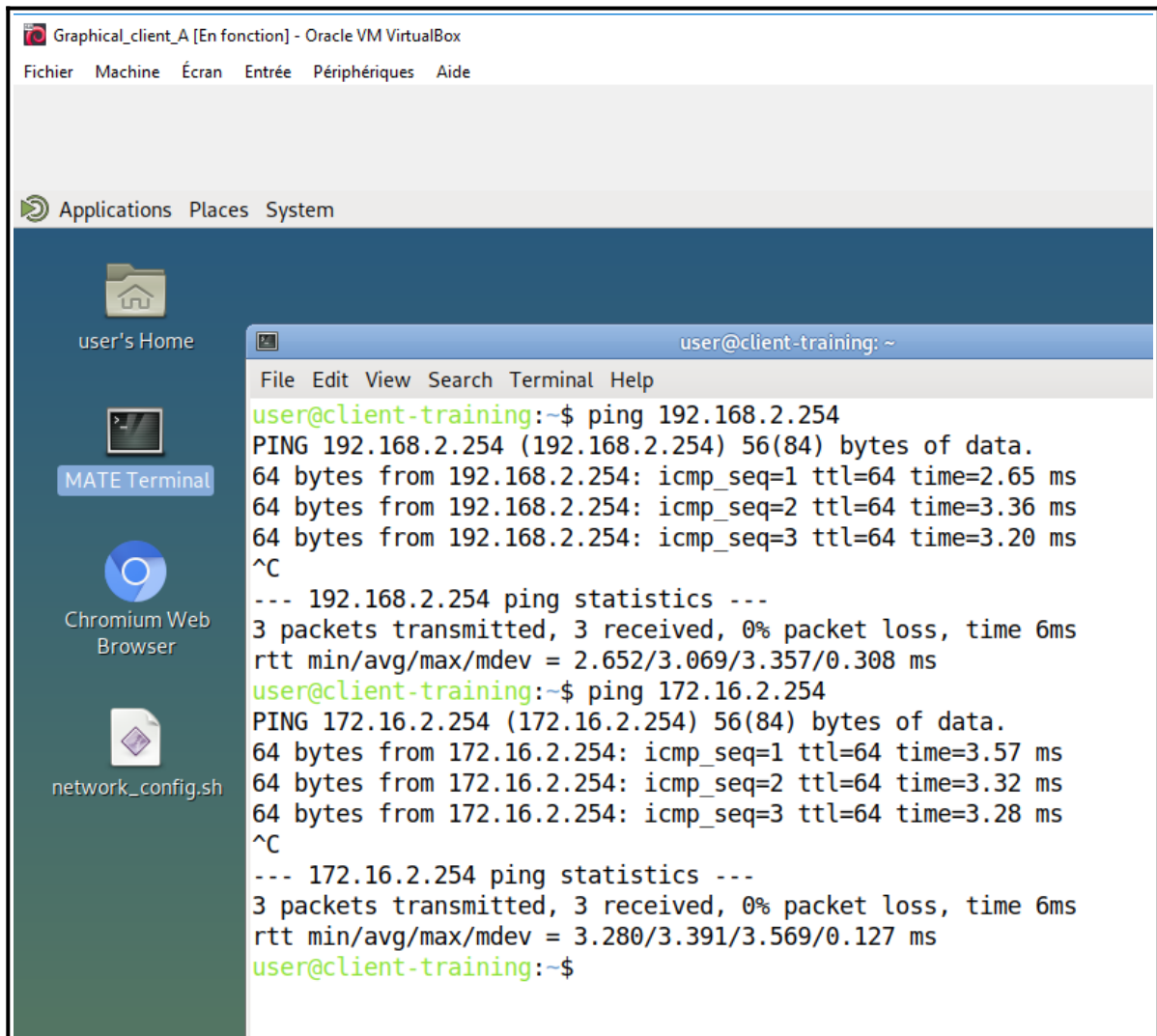


**9ème :** Nous appliquons donc les nouveaux profils de chiffrement créer précédemment sur notre VPN.



**10ème étape :** Nouveau test d'accès au serveur FTP de 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 +

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

Apps Debian.org Latest News Help

**STORMSHIELD** v4.0.1  
**Network Security**

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 +

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

s Debian.org Latest News Help

**STORMSHIELD** v4.0.1  
**Network Security**

MONITORING CONFIGURATION EVA1 VMSNSX09K0639A9

CONFIGURATION

Rechercher...

Configuration générale

Passerelle par défaut (routeur): gw\_default

**RÉSEAU / ROUTAGE**

ROUTES STATIQUES IPV4 ROUTAGE DYNAMIQUE ROUTES DE RETOUR IPV4

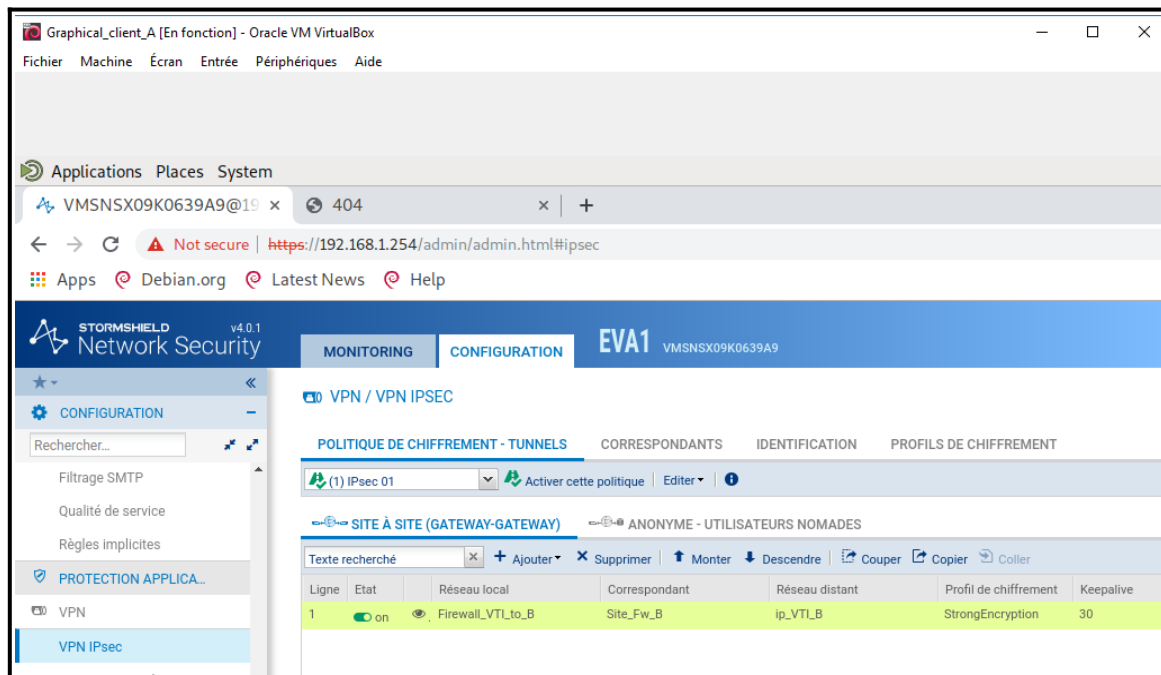
Configuration générale

Passerelle par défaut (routeur): gw\_default

**ROUTES STATIQUES**

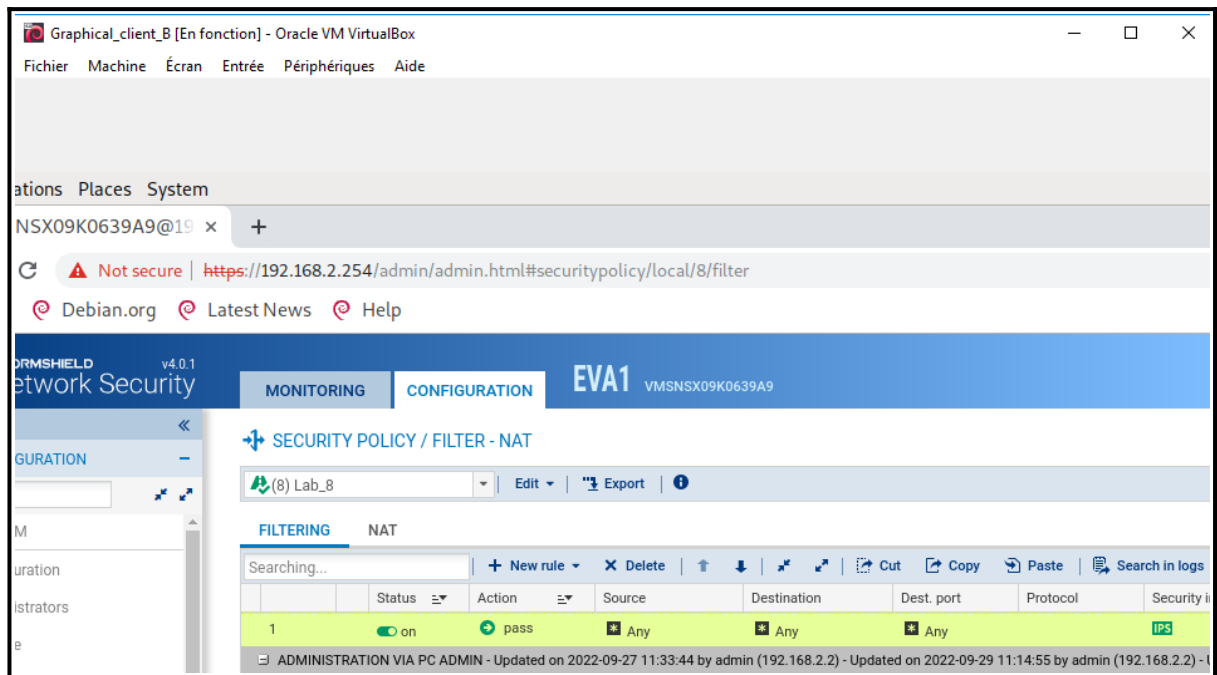
Rechercher... + Ajouter X Supprimer

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

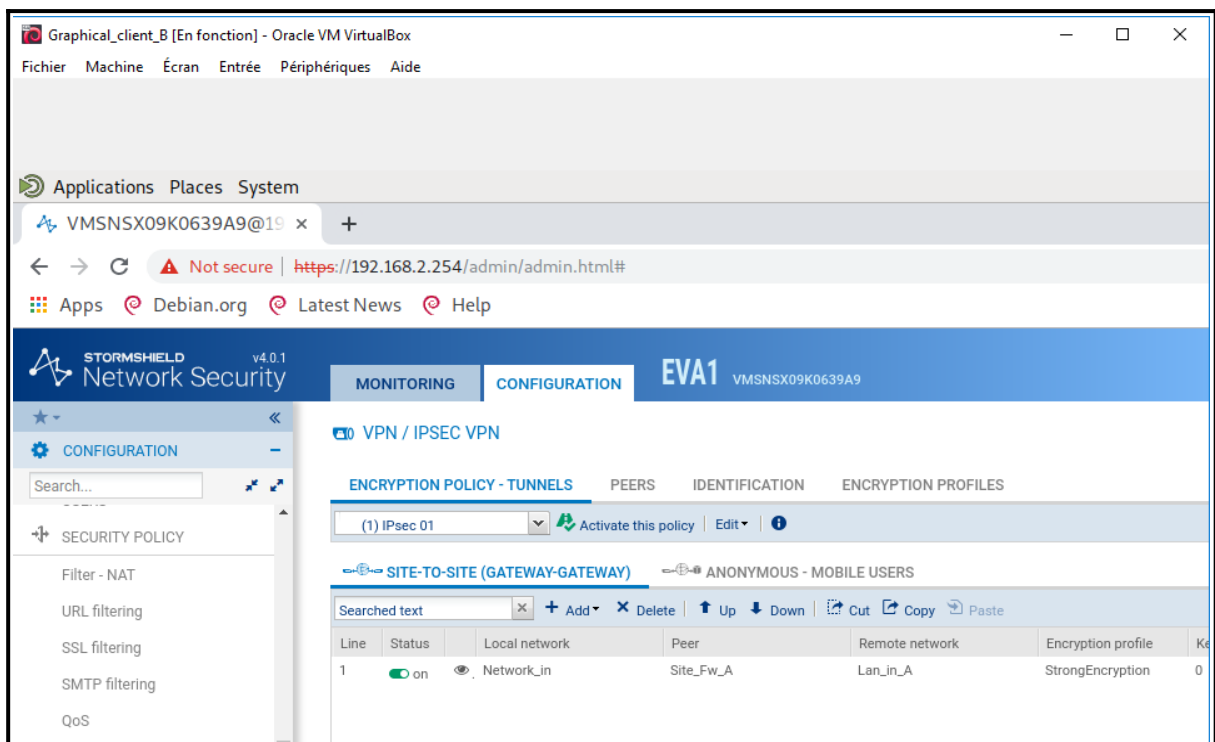


**12ème étape :** Réalisation de l'interconnexion des réseaux, en configurant des tunnels basés sur des VTI.

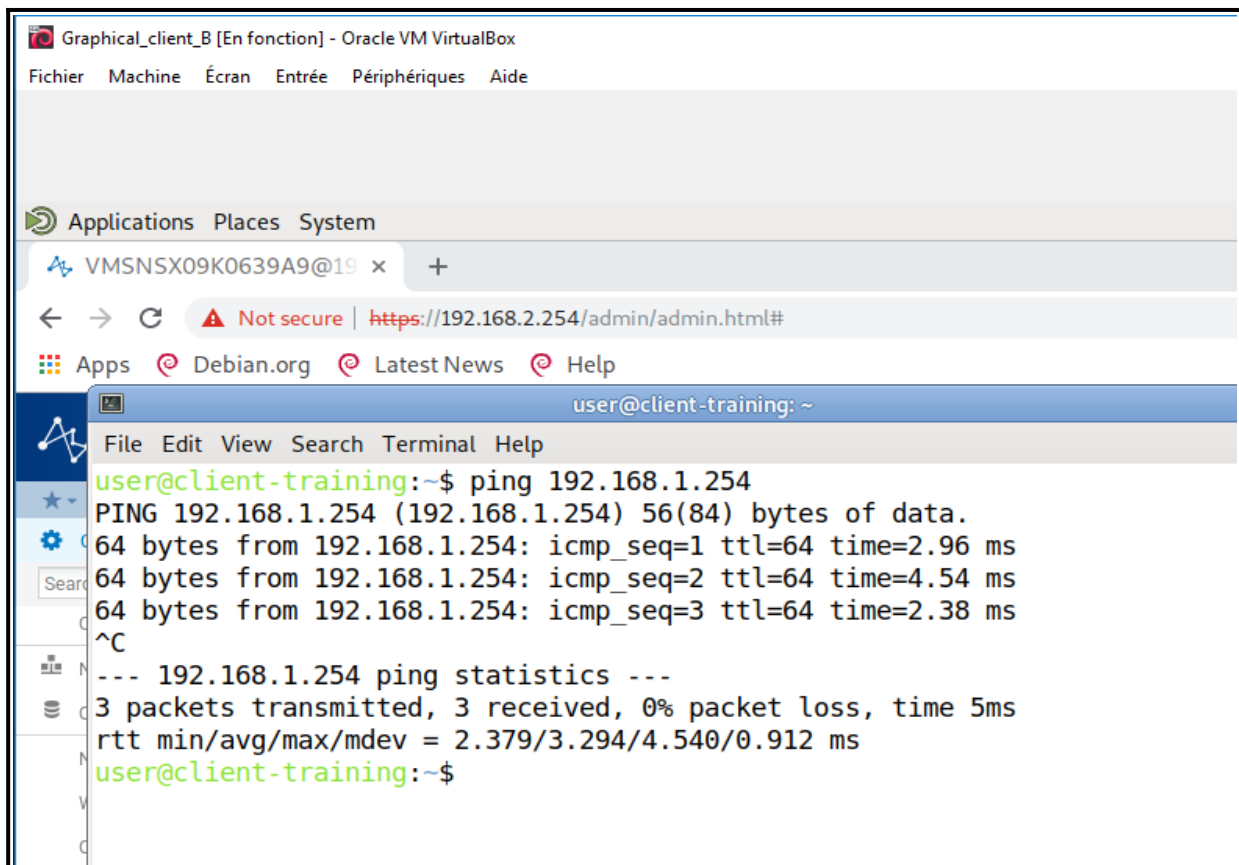
## Réseau B :



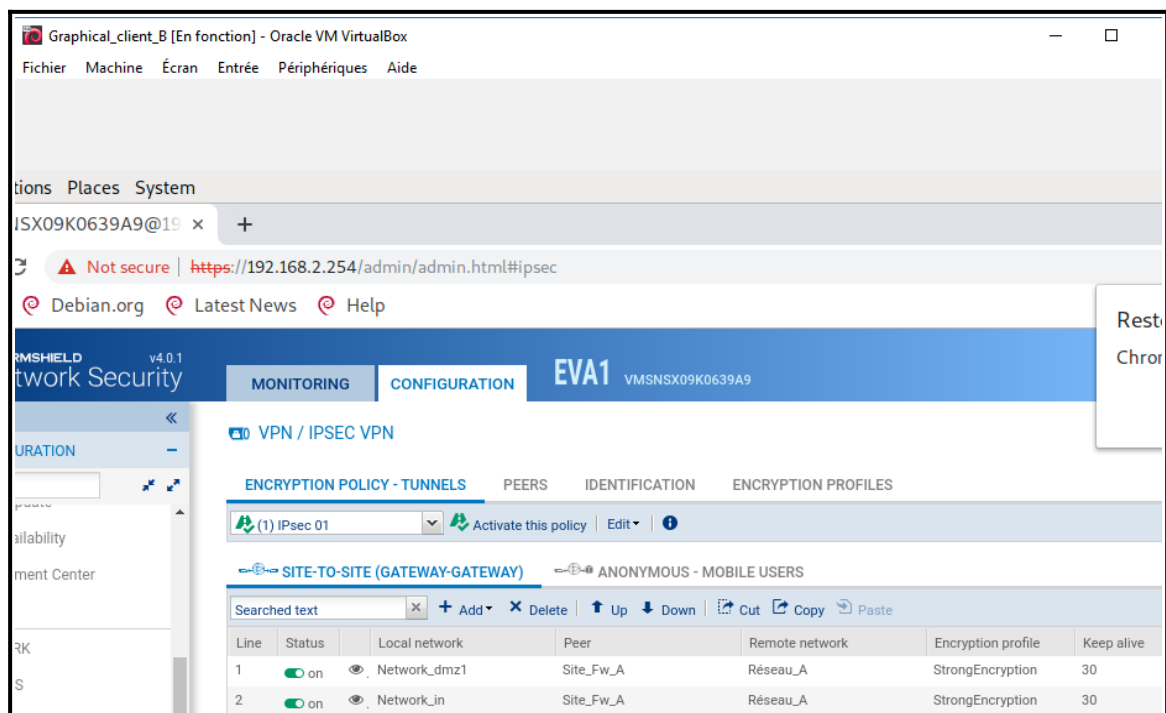
1ère étape : Ajout de la règle de filtrage pass any any.



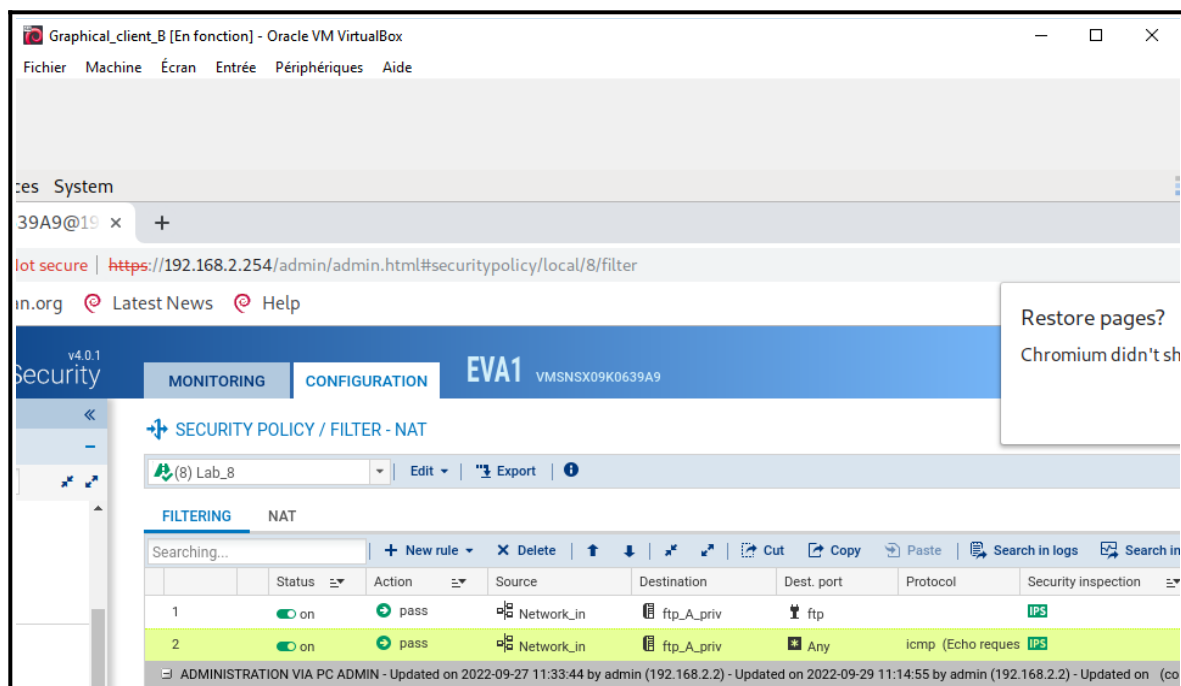
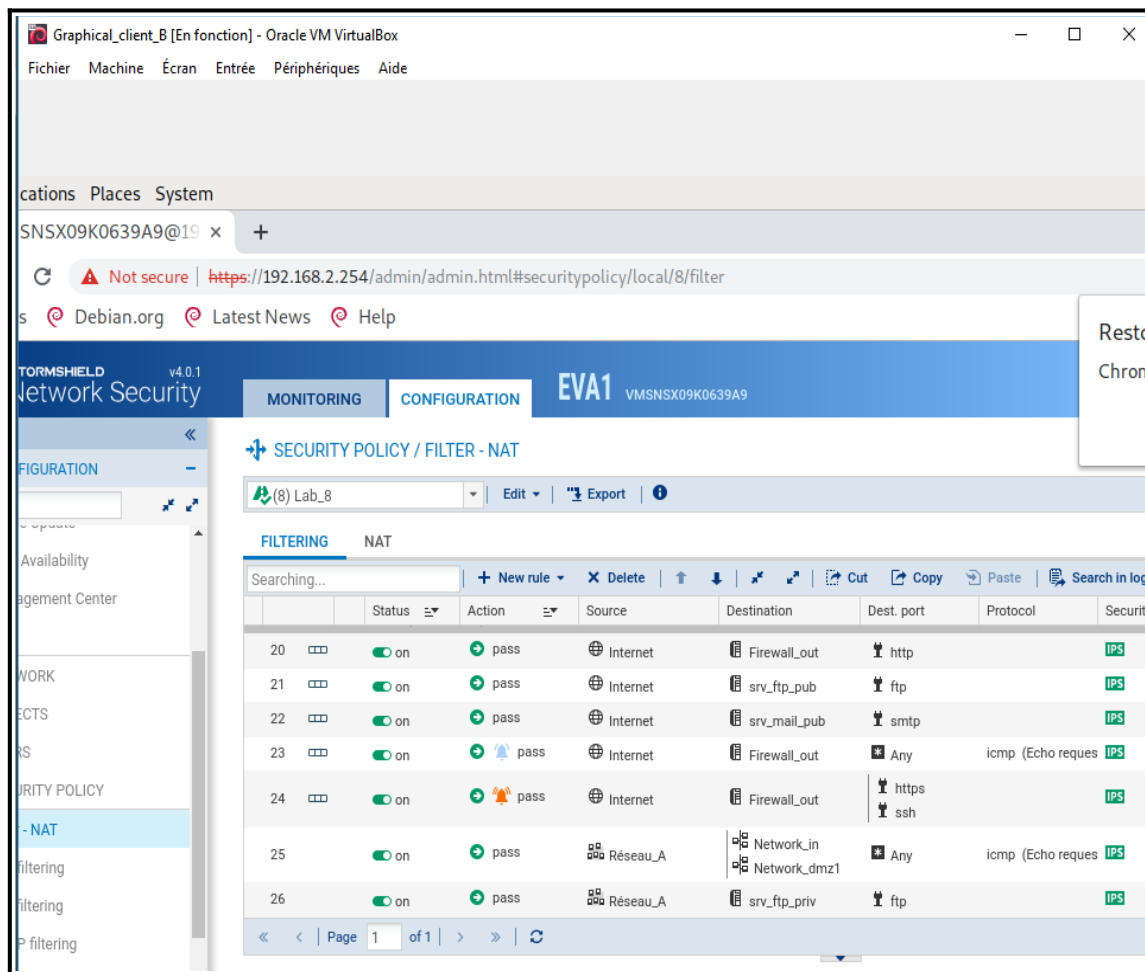
2ème étape : Configuration d'un tunnel Isec afin de relier le réseau A au réseau B.



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



**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.



**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.

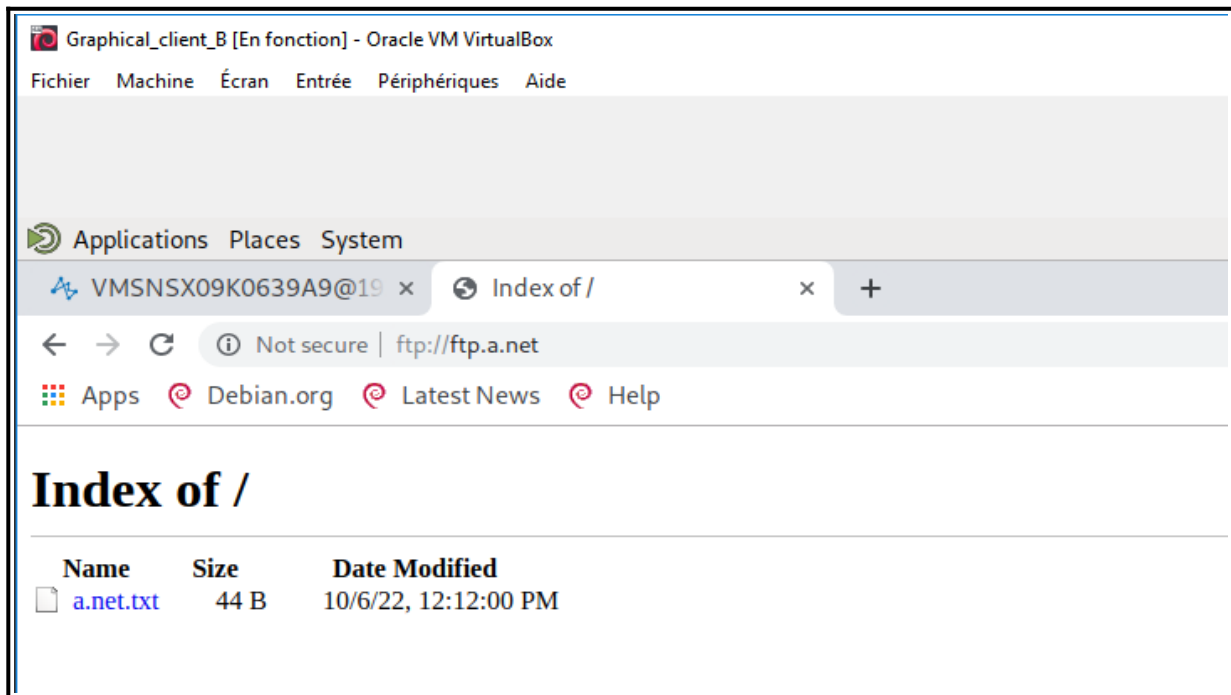
```
Graphical_client_B [En fonction] - Oracle VM VirtualBox
Fichier  Machine  Écran  Entrée  Périphériques  Aide

Applications  Places  System

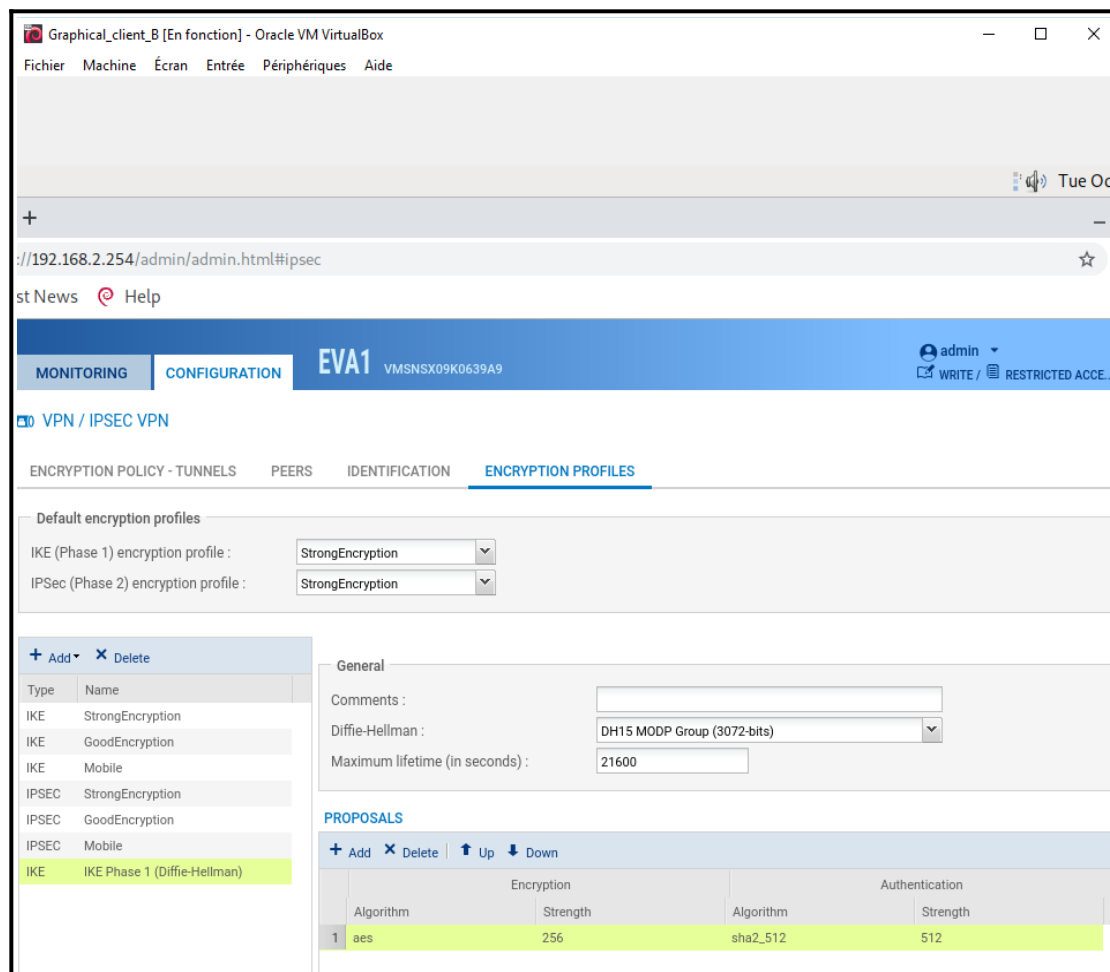
user's Home
MATE Terminal
Chromium Web Browser
network_configuration

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=4.06 ms
64 bytes from 192.168.1.254: icmp_seq=2 ttl=64 time=4.44 ms
64 bytes from 192.168.1.254: icmp_seq=3 ttl=64 time=4.23 ms
^C
--- 192.168.1.254 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 5ms
rtt min/avg/max/mdev = 4.064/4.244/4.440/0.162 ms
user@client-training:~$ ping 172.16.1.254
PING 172.16.1.254 (172.16.1.254) 56(84) bytes of data.
64 bytes from 172.16.1.254: icmp_seq=1 ttl=64 time=2.54 ms
64 bytes from 172.16.1.254: icmp_seq=2 ttl=64 time=4.19 ms
64 bytes from 172.16.1.254: icmp_seq=3 ttl=64 time=3.23 ms
^C
--- 172.16.1.254 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 5ms
rtt min/avg/max/mdev = 2.542/3.319/4.190/0.676 ms
user@client-training:~$
```

**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

Tue Oct

+/

://192.168.2.254/admin/admin.html#ipsec

st News Help

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

VPN / IPSEC VPN

ENCRIPTION POLICY - TUNNELS PEERS IDENTIFICATION **ENCRIPTION 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

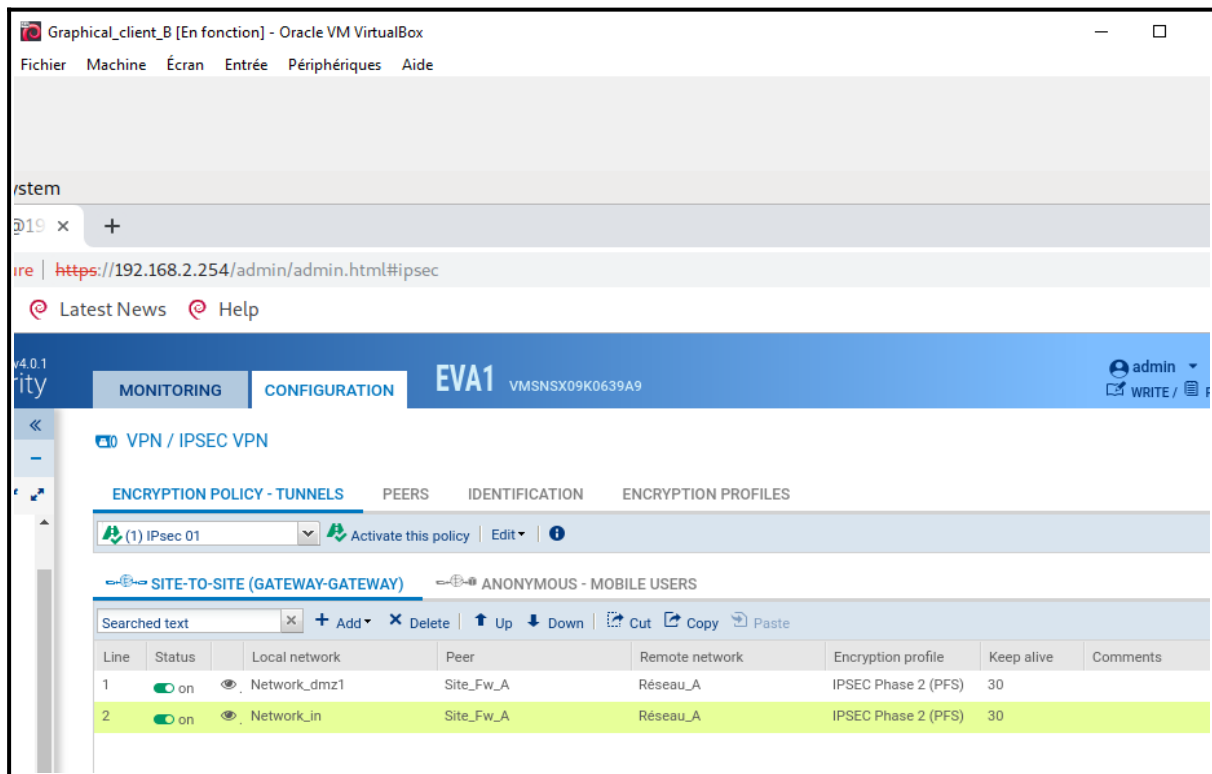
	Algorithm	Strength
1	hmac_sha512	512

**ENCRIPTION PROPOSALS**

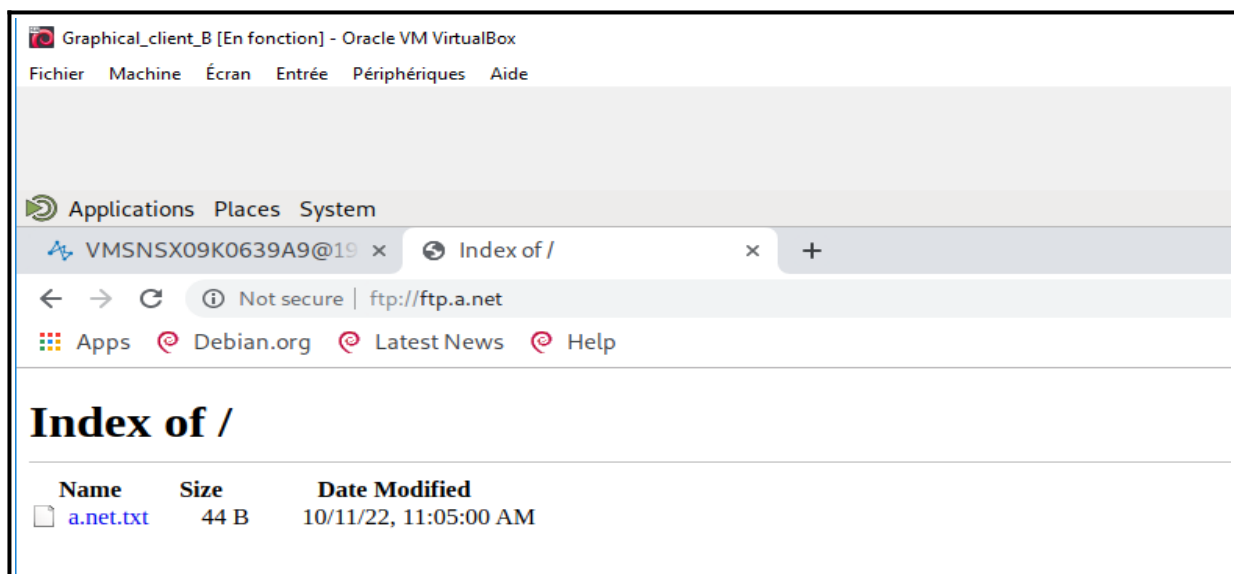
+ Add - Delete

	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.

```
Graphical_client_B [En fonction] - Oracle VM VirtualBox
Fichier Machine Écran Entrée Périphériques Aide

Applications Places System

user's Home
MATE Terminal
Chromium Web Browser
network_config.sh

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=1.27 ms
64 bytes from 192.168.2.254: icmp_seq=2 ttl=64 time=1.28 ms
64 bytes from 192.168.2.254: icmp_seq=3 ttl=64 time=1.43 ms
^C
--- 192.168.2.254 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 4ms
rtt min/avg/max/mdev = 1.274/1.326/1.427/0.071 ms
user@client-training:~$ ping 172.16.2.254
PING 172.16.2.254 (172.16.2.254) 56(84) bytes of data.
64 bytes from 172.16.2.254: icmp_seq=1 ttl=64 time=0.431 ms
64 bytes from 172.16.2.254: icmp_seq=2 ttl=64 time=1.13 ms
64 bytes from 172.16.2.254: icmp_seq=3 ttl=64 time=2.53 ms
^C
--- 172.16.2.254 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 20ms
rtt min/avg/max/mdev = 0.431/1.362/2.531/0.874 ms
user@client-training:~$
```

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

Graphical\_client\_B [En fonction] - Oracle VM VirtualBox

Fichier Machine Écran Entrée Périphériques Aide

Applications Places System

VMSNSX09K0639A9@19 x Hôte injoignable x +

← → ↻ ⚠ Not secure | <https://192.168.2.254/admin/admin.html#vtigre/ipsec>

Apps @ Debian.org @ Latest News @ Help

**STORMSHIELD** v4.0.1  
Network Security

MONITORING CONFIGURATION EVA1 VMSNSX09K0639A9

CONFIGURATION

Search...

High Availability  
Management Center  
CLI

NETWORK / VIRTUAL INTERFACES

IPSEC INTERFACES (VTI) GRE INTERFACES LOOPBACK

Search + Add X Delete | Check usage

Status	Name ↑	IPv4 address	IPv4 mask	Comments
Enabled	VTI_to_A	192.168.120.1	255.255.255.254	

Graphical\_client\_B [En fonction] - Oracle VM VirtualBox

Fichier Machine Écran Entrée Périphériques Aide

Applications Places System

VMSNSX09K0639A9@19 x Hôte injoignable x +

→ ↻ ⚠ Not secure | <https://192.168.2.254/admin/admin.html#networkrouting/routing>

Apps @ Debian.org @ Latest News @ Help

**STORMSHIELD** v4.0.1  
Network Security

MONITORING CONFIGURATION EVA1 VMSNSX09K0639A9

CONFIGURATION

ch...

High Availability  
Management Center  
CLI

NETWORK

interfaces  
virtual interfaces  
Routing

NETWORK / ROUTING

IPv4 STATIC ROUTES IPv4 DYNAMIC ROUTING IPv4 RETURN ROUTES

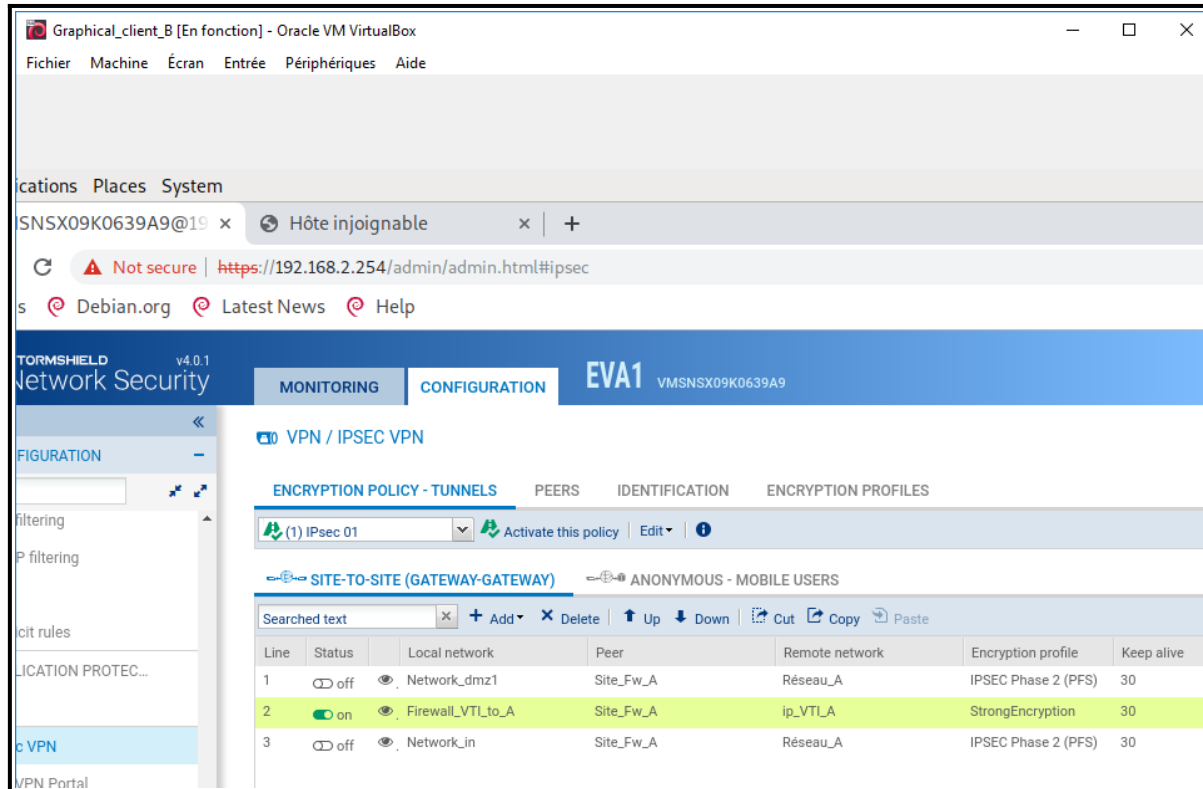
General

Default gateway (router): gw\_default

STATIC ROUTES

Searching... + Add X Delete

Status	Destination network (host, netw...	Interface	Address range	Gateway
on	Lan_in_A	VTI_to_A	192.168.1.0/24	ip_VTLA



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