



**STORMSHIELD**

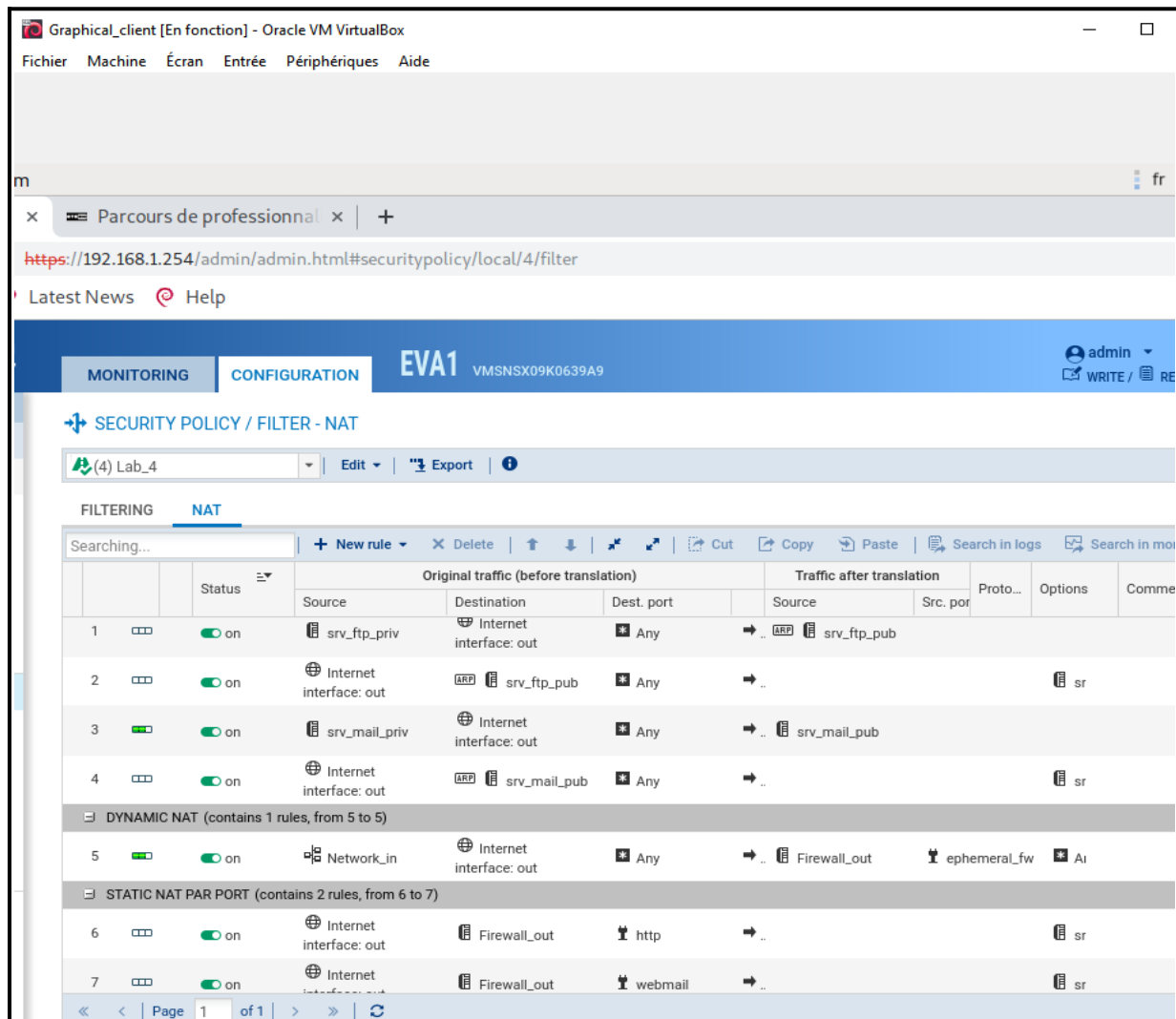
# **LAB 4 : Translation d'adresses**

## Réseau A :

The screenshot shows the Mikrotik WinBox interface within an Oracle VM VirtualBox window titled 'Graphical\_client [En fonction] - Oracle VM VirtualBox'. The menu bar includes 'Fichier', 'Machine', 'Écran', 'Entrée', 'Périphériques', and 'Aide'. The address bar displays the URL 'https://192.168.1.254/admin/admin.html#securitypolicy/local/4/filter'. The page title is 'test News' with a 'Help' link. The main interface has a blue header with 'MONITORING' and 'CONFIGURATION' tabs, and a user profile for 'admin' with a 'WRITE' button. Below the header, the breadcrumb 'SECURITY POLICY / FILTER - NAT' is visible. A dropdown menu shows '(4) Lab\_4' with 'Edit' and 'Export' options. The 'FILTERING' tab is active, showing a table of NAT rules. The table has columns for 'Status', 'Action', 'Source', 'Destination', 'Dest. port', 'Protocol', and 'Security inspection'. Three rules are listed, all with 'Status' 'on' and 'Action' 'pass'. The 'Source' for rules 1 and 2 is 'network\_internals', and for rule 3 it is 'Any'. The 'Destination' for all rules is 'Any'. The 'Dest. port' for rule 1 is 'plugins', and for rules 2 and 3 it is 'Any'. The 'Protocol' for all rules is 'Any'. The 'Security inspection' for all rules is 'IPS'.

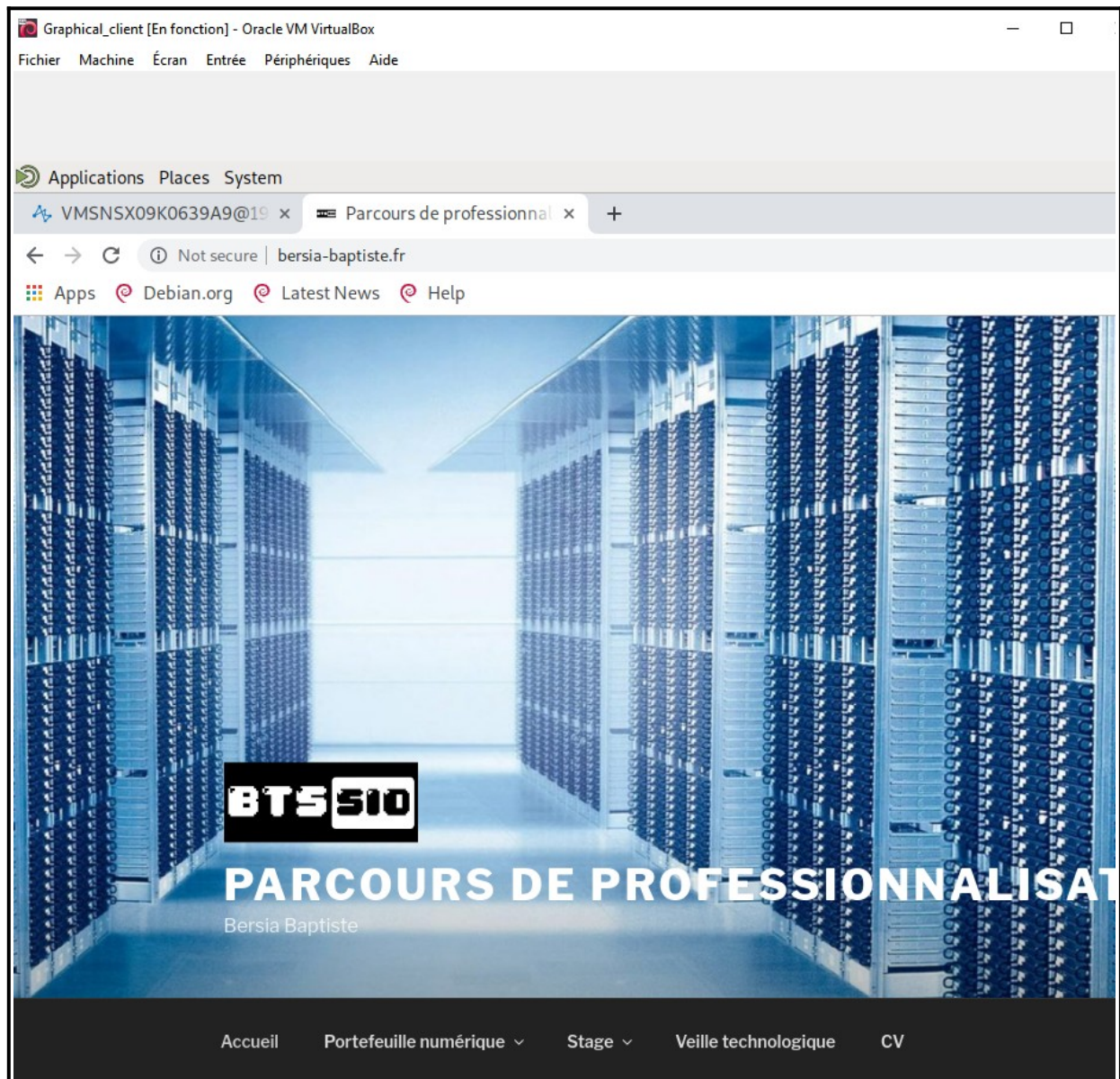
	Status	Action	Source	Destination	Dest. port	Protocol	Security inspection
1	on	pass	network_internals	Any	plugins	Any	IPS
2	on	pass	network_internals	Any	Any	Any	IPS
3	on	pass	Any	Any	Any	Any	IPS

**1ère étape :** Nous activons la politique de filtrage/Nat numéro 4.

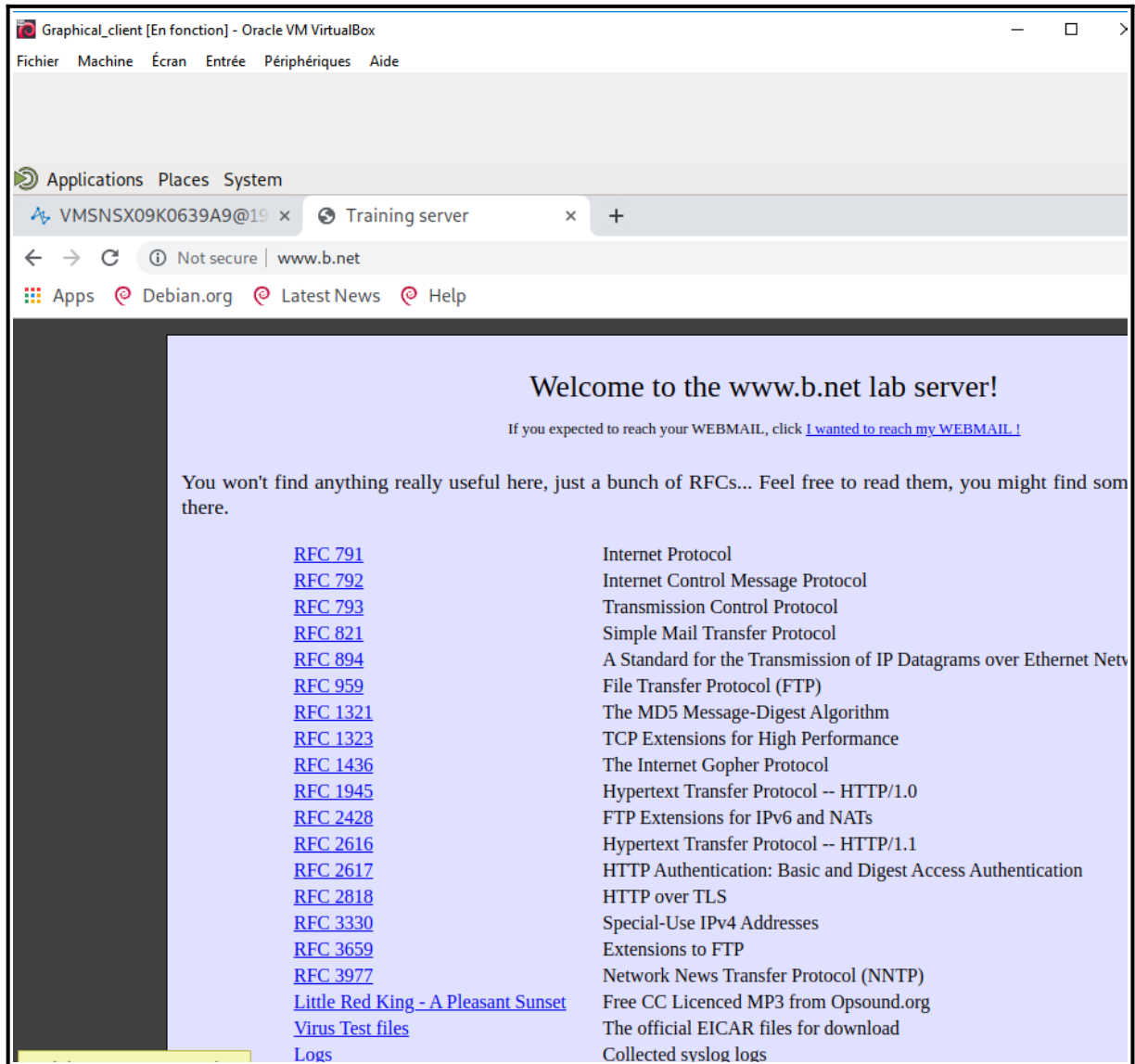


## 2ème étape :

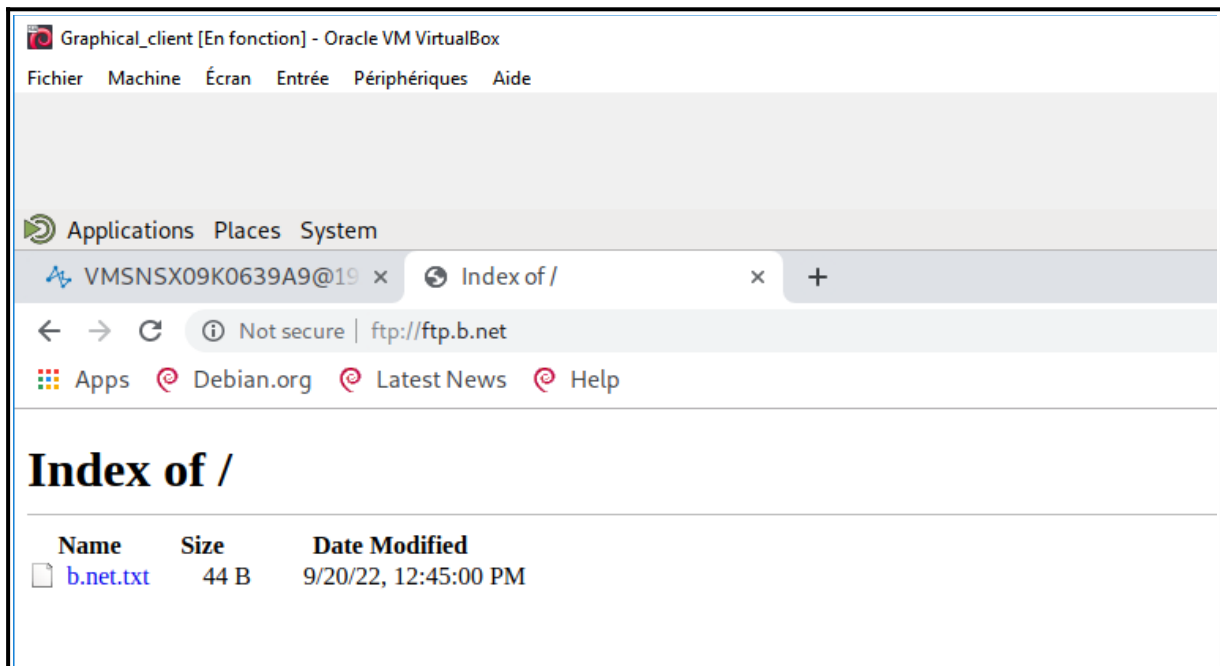
- Nous ajoutons une règle NAT ayant pour but que les machines de nos réseaux internes puissent accéder internet anonymement sans dévoiler leur adresse IP privée.
- Une règle permettant de joindre chaque serveur depuis le réseau externe grâce aux IP publiques.
- Une règle permettant de joindre le serveur WEB situé en DMZ grâce à une redirection de port via l'adresse IP publique.
- Une règle permettant à l'autre entreprise l'accès à l'ensemble des ressources.



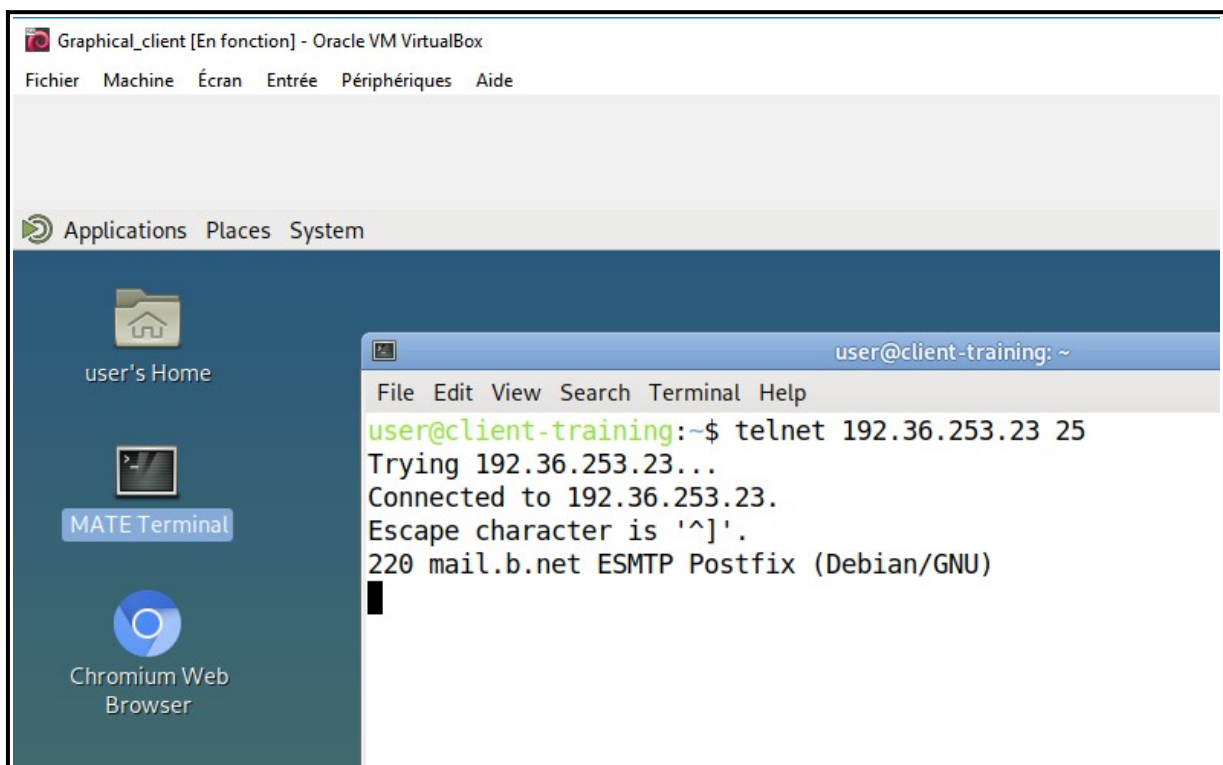
**3ème étape :** Test de l'accès à internet.



**4ème étape :** Le réseau A pouvant communiqué avec ses différents services celui-ci test donc l'accès au service du réseau distant B, notamment avec le serveur WEB.

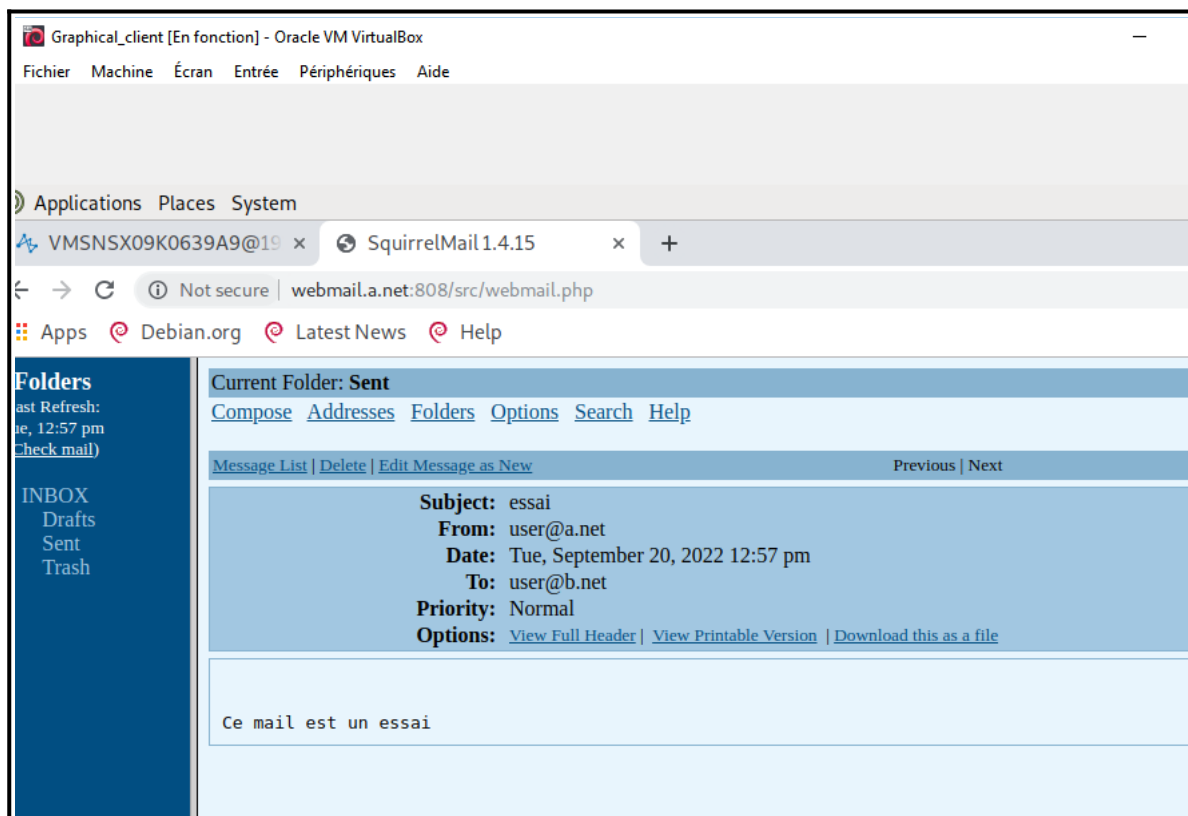
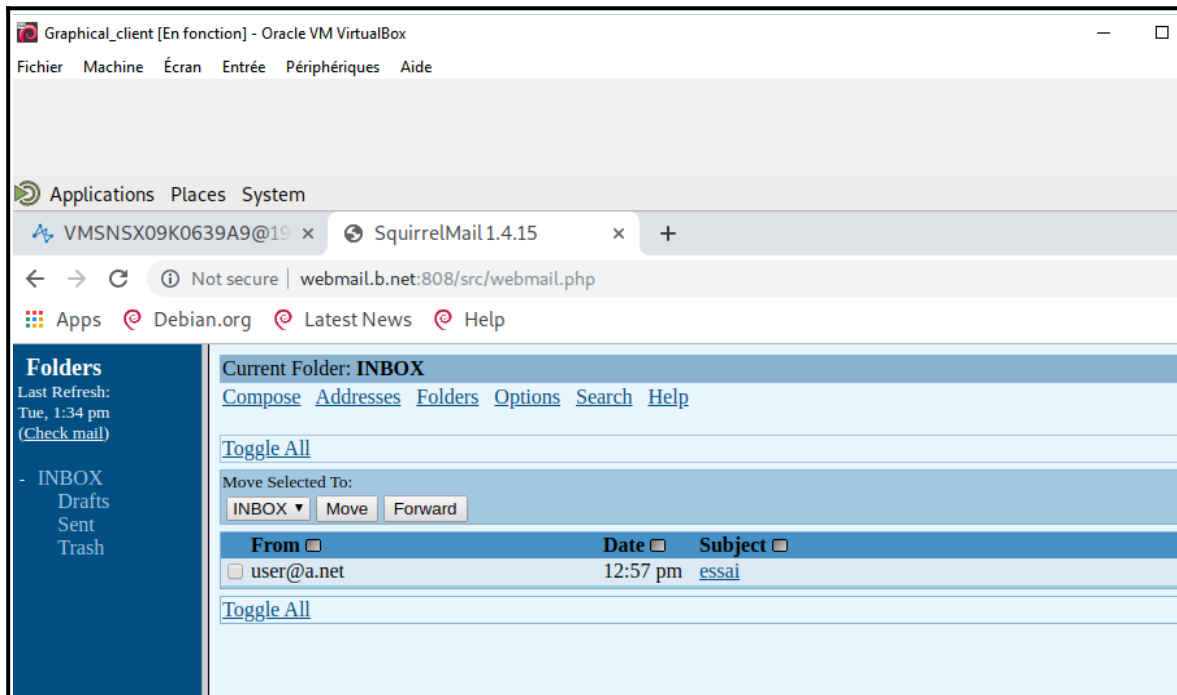


**5ème étape :** Nous testons l'accès au serveur FTP de B depuis le réseau A.

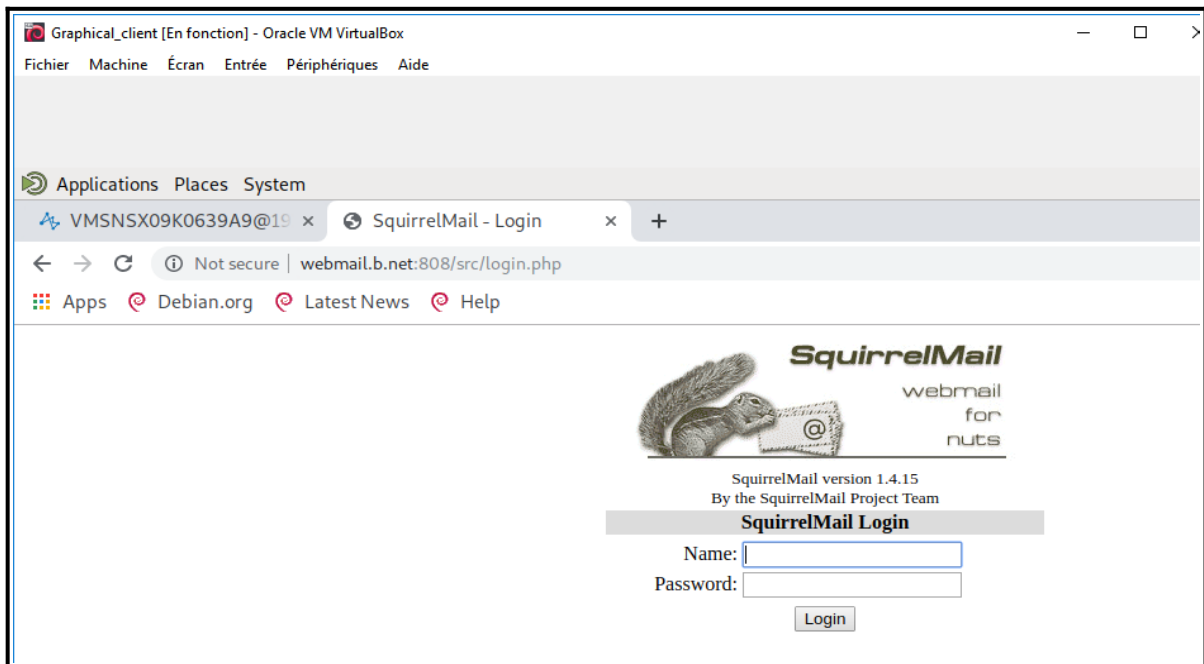
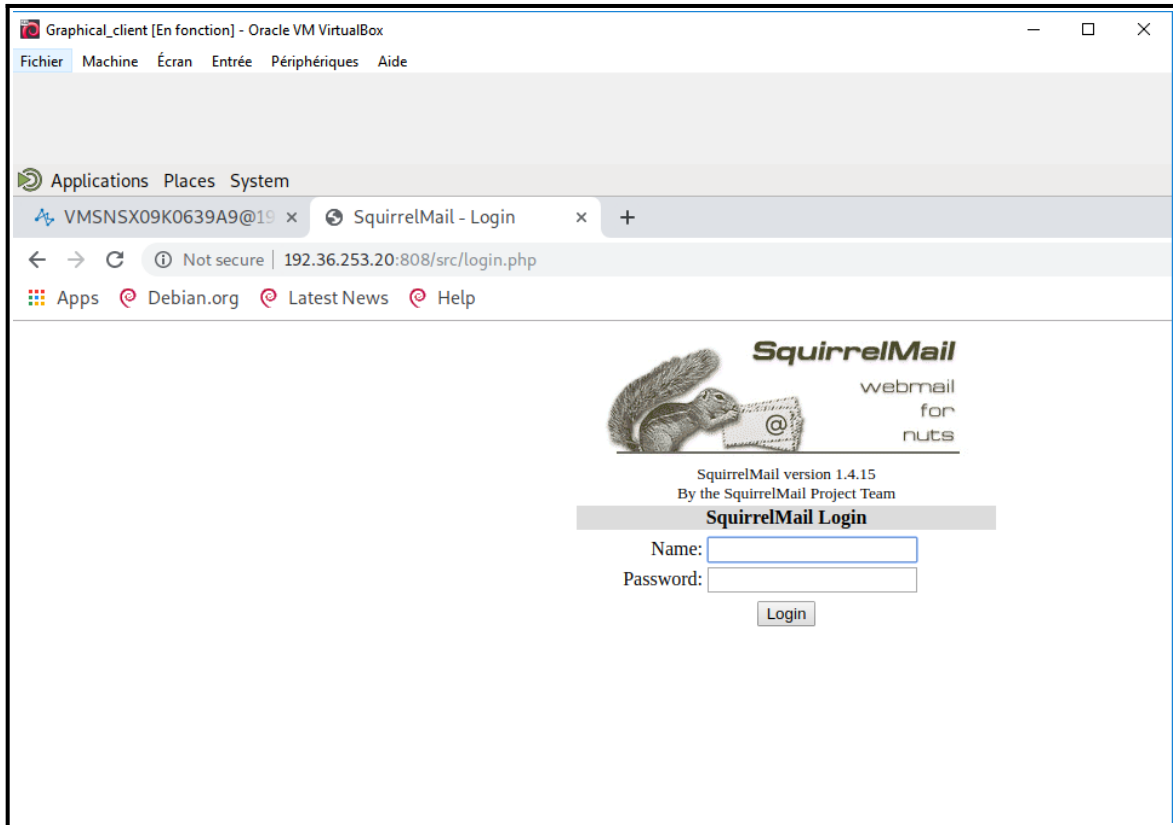


**6ème étape :** Test du serveur FTP également possible avec Telnet.





**7ème étape :** Nous effectuons le test d'envoyer un mail depuis le réseau A vers B.



**8ème étape :** Test de l'accès au serveur mail de B depuis A via l'adresse IP et le nom de domaine.



## Réseau B :

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

Fichier Machine Écran Entrée Périphériques Aide

https://192.168.2.254/admin/admin.html#securitypolicy/local/4/nat

Latest News Help

MONITORING CONFIGURATION EVA1 VMSNSX09K0639A9 admin WRITE / R

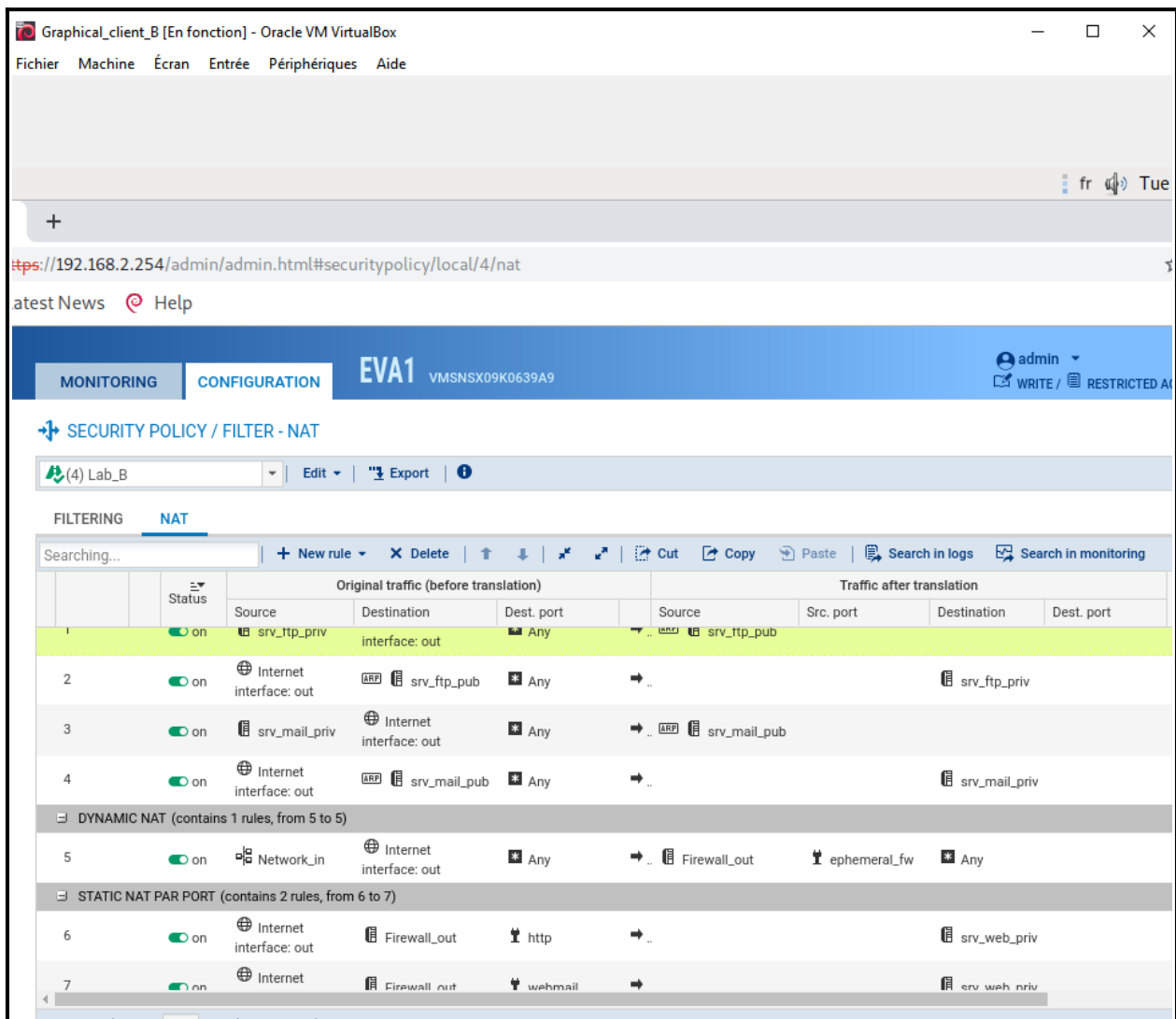
SECURITY POLICY / FILTER - NAT

(4) Lab\_B Edit Export

FILTERING NAT

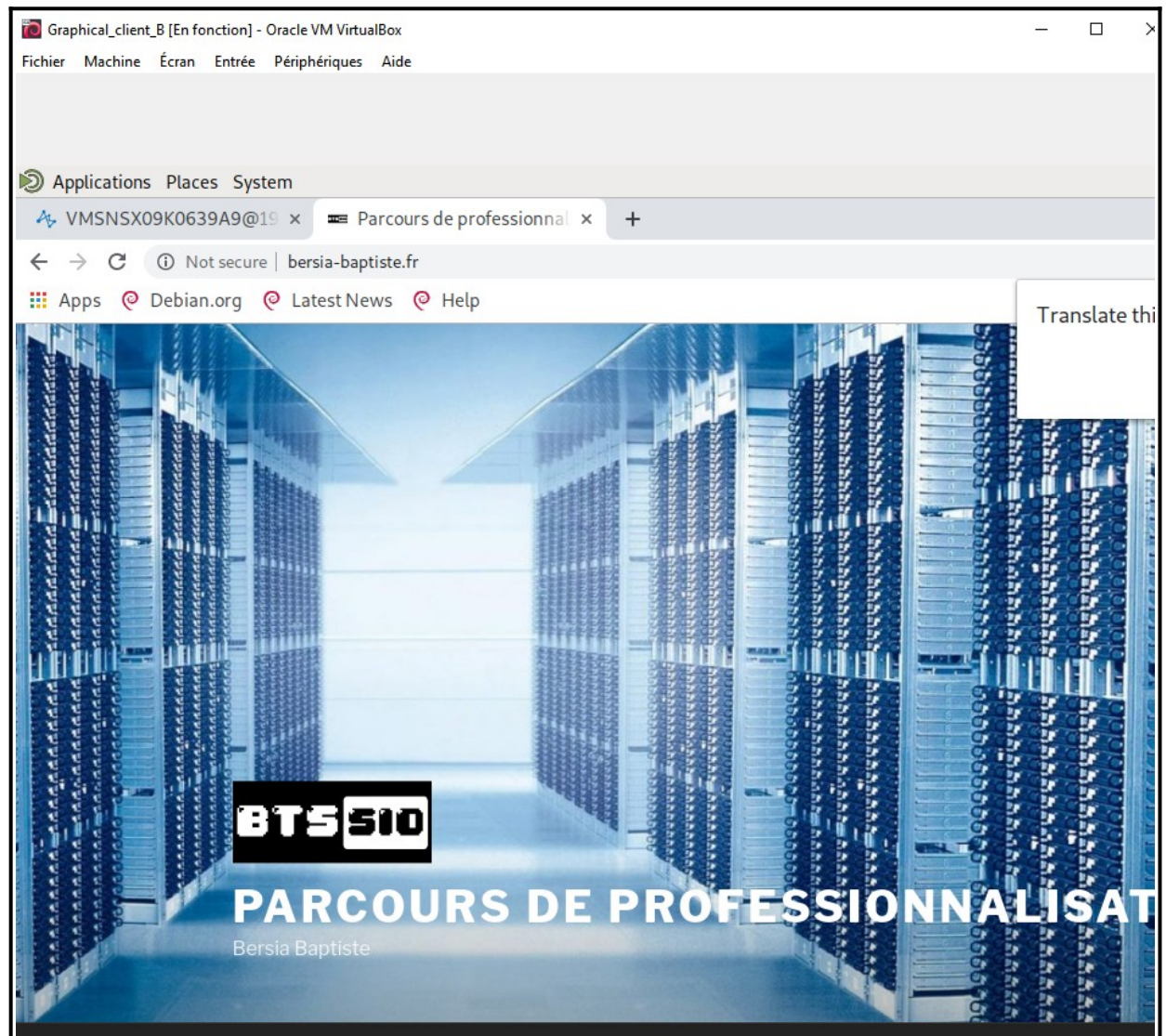
	Status	Action	Source	Destination	Dest. port	Protocol	Security inspection
1	on	pass	network_internals	Any	plugins		IPS
2	on	pass	network_internals	Any	Any		IPS
3	on	pass	Any	Any	Any		IPS

**1ère étape :** Nous activons la politique de filtrage/Nat numéro 4.

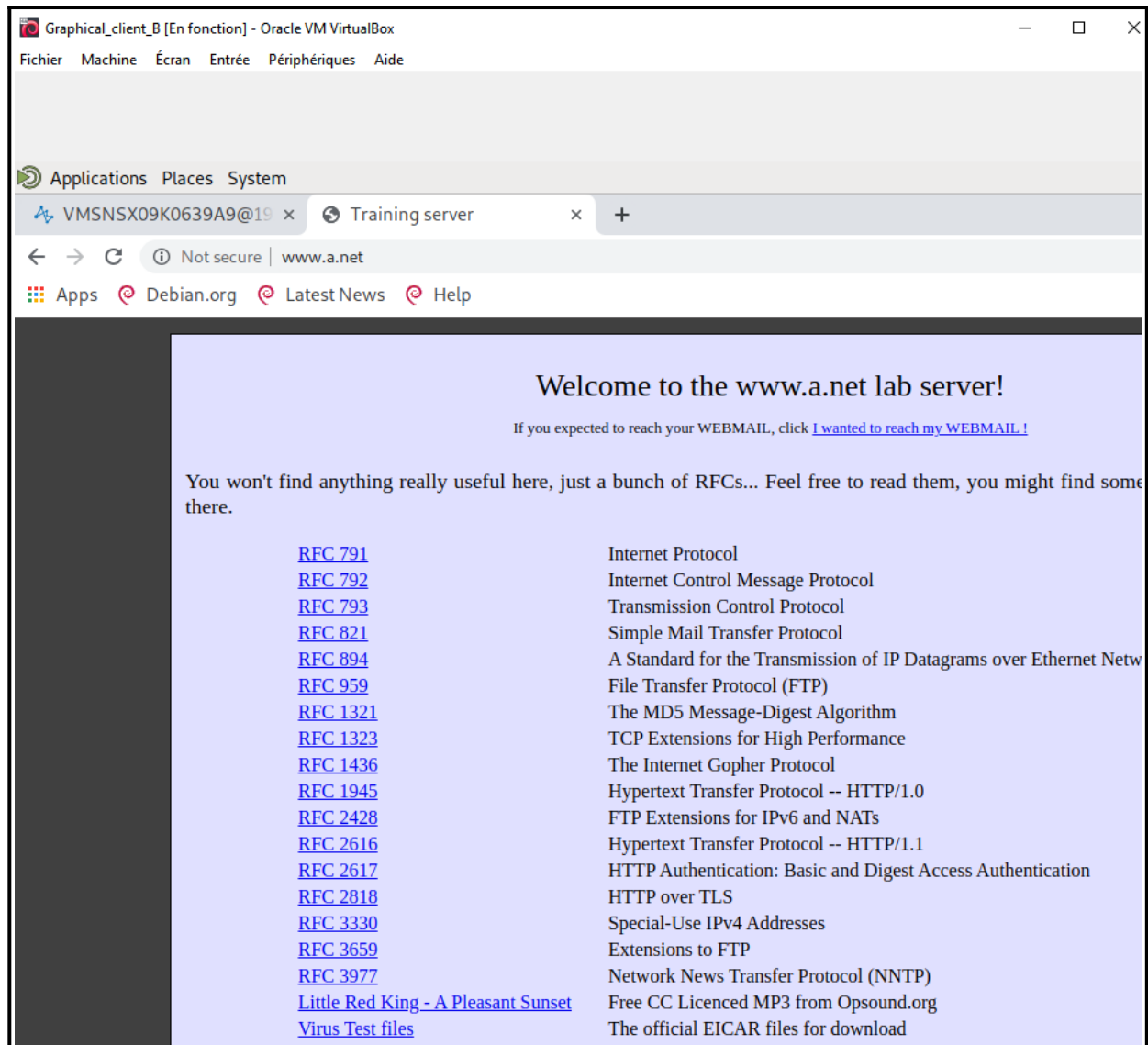


## 2ème étape :

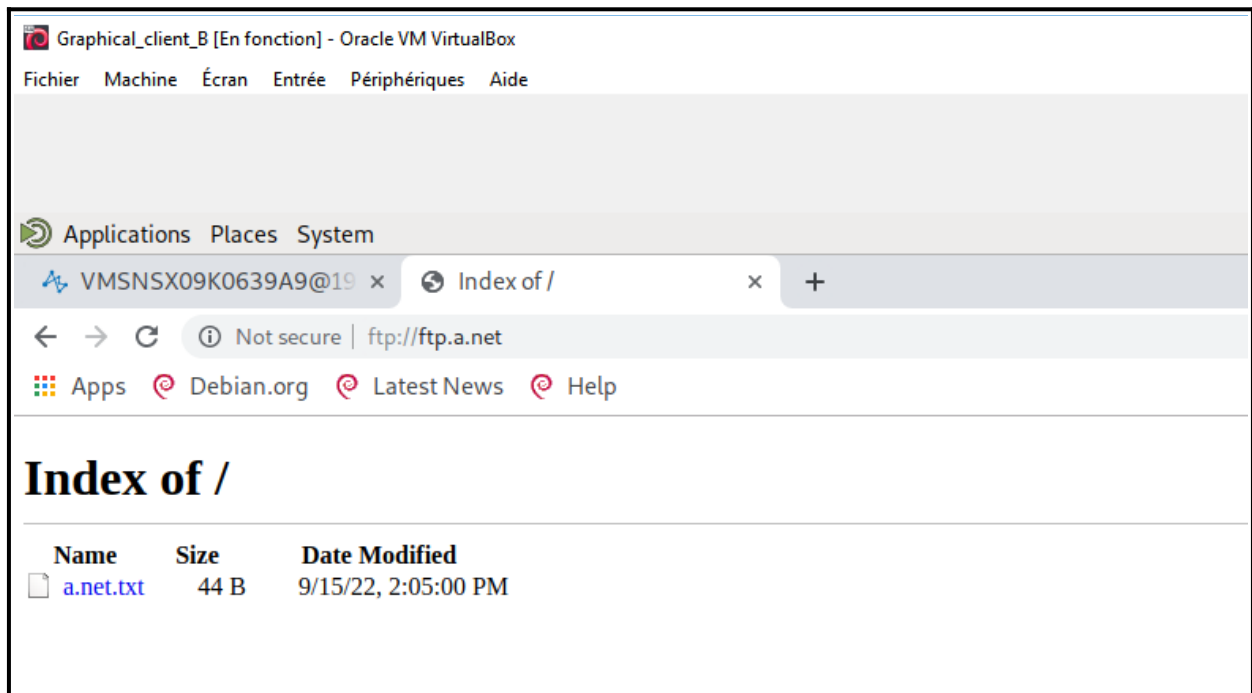
- Nous ajoutons une règle NAT ayant pour but que les machines de nos réseaux internes puissent accéder internet anonymement sans dévoiler leur adresse IP privée.
- Une règle permettant de joindre chaque serveur depuis le réseau externe grâce aux IP publiques.
- Une règle permettant de joindre le serveur WEB situé en DMZ grâce a une redirection de port via l'adresse IP publique.
- Une règle permettant à l'autre entreprise l'accès à l'ensemble des ressources.



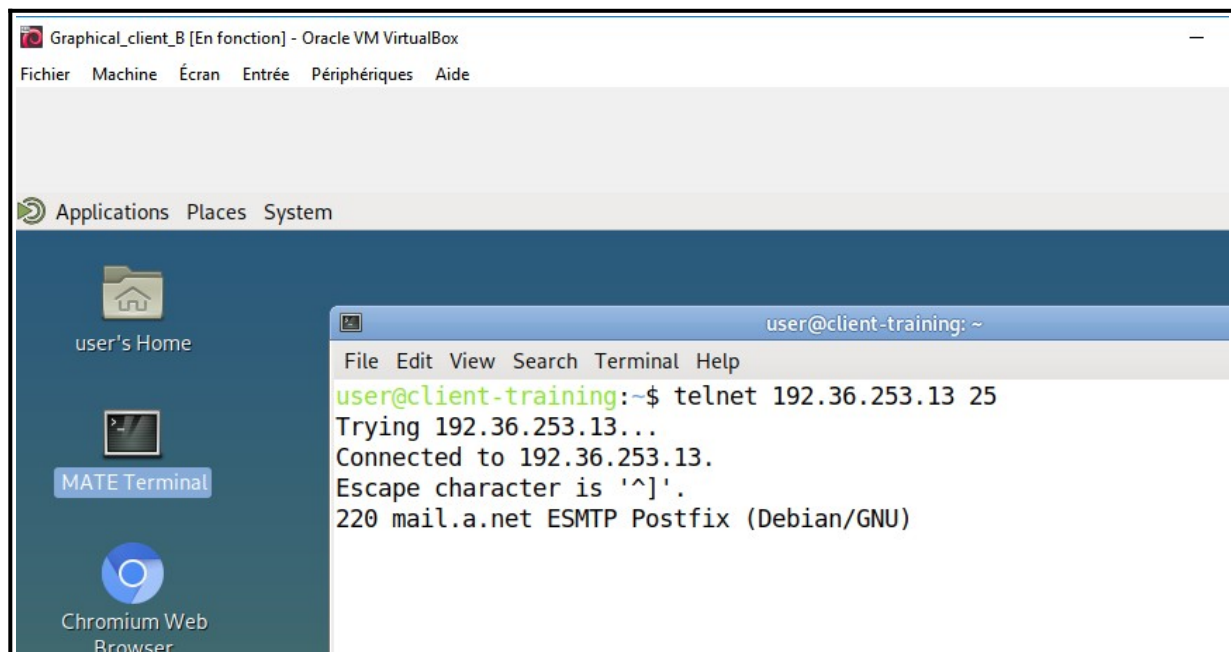
**3ème étape :** Test de l'accès à internet.



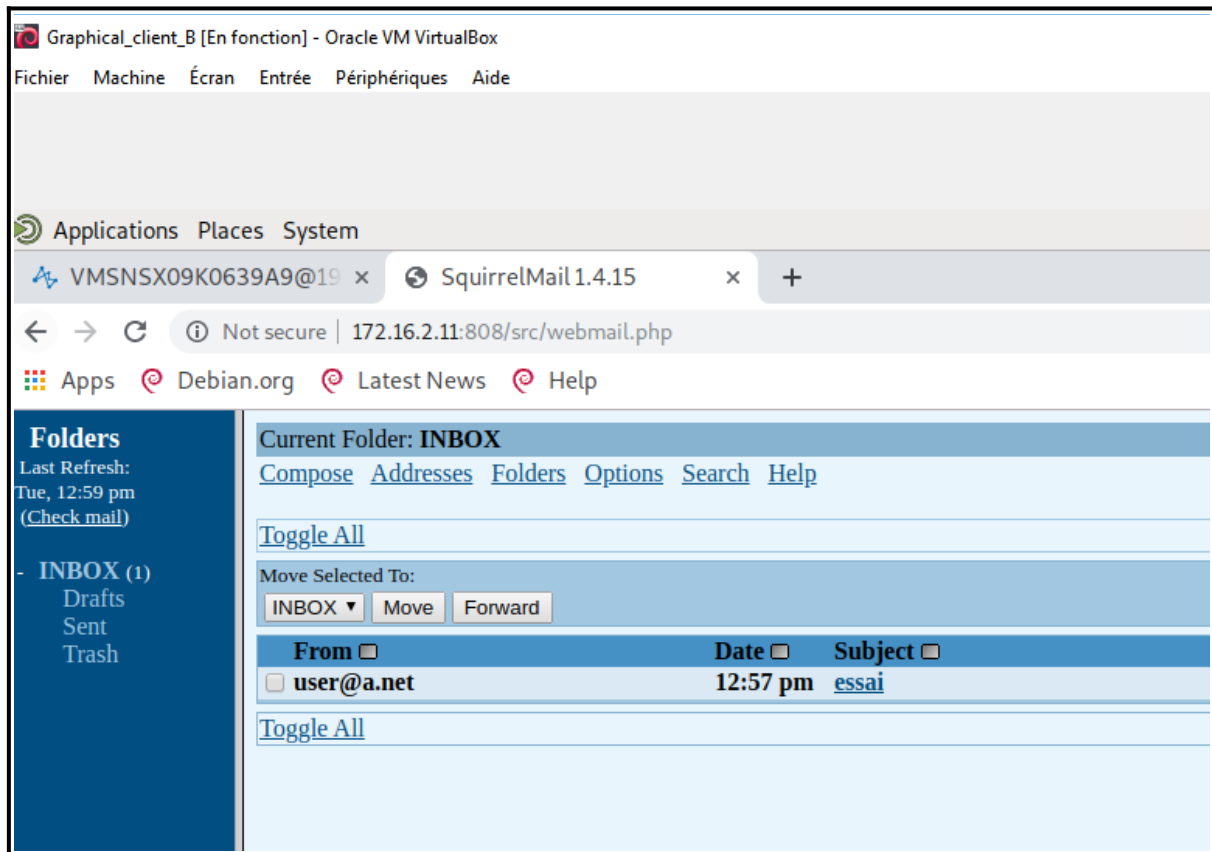
**4ème étape :** Le réseau B pouvant communiqué avec ses différents services celui-ci test donc l'accès au service du réseau distant A, notamment avec le serveur WEB.



**5ème étape :** Nous testons l'accès au serveur FTP de A depuis le réseau B.



**6ème étape :** Test du serveur FTP également possible avec Telnet.



**7ème étape :** Nous observons que le teste d'envoyer un précédemment a correctement fonctionné puisque nous constatons le reçu du mail venant du A. Procédure fonctionnant dans les deux sens.