



STORMSHIELD

LAB 4 :
Translation d'adresses

Réseau A :

The screenshot shows the EVA1 security policy/filter-NAT interface. The URL in the address bar is `https://192.168.1.254/admin/admin.html#securitypolicy/local/4/filter`. The interface includes a navigation bar with Fichier, Machine, Écran, Entrée, Périphériques, and Aide. Below the address bar, there's a news feed with "Latest News" and a "Help" link. The main area has tabs for MONITORING and CONFIGURATION, with CONFIGURATION selected. The title is "SECURITY POLICY / FILTER - NAT". The table displays three filtering rules:

	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

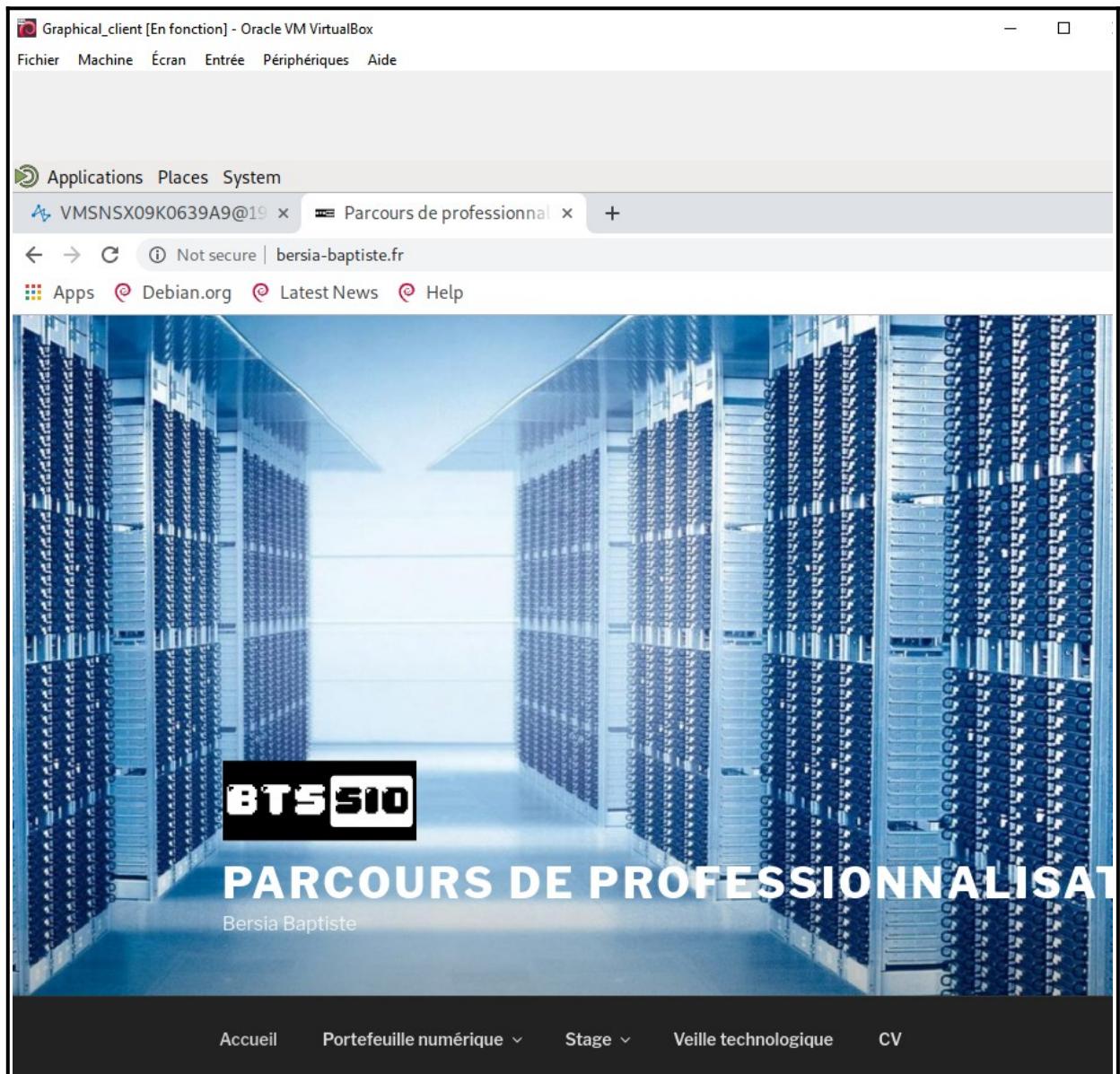
1ère étape : Nous activons la politique de filtrage/Nat numéro 4.

The screenshot shows the EVA1 configuration interface with the following details:

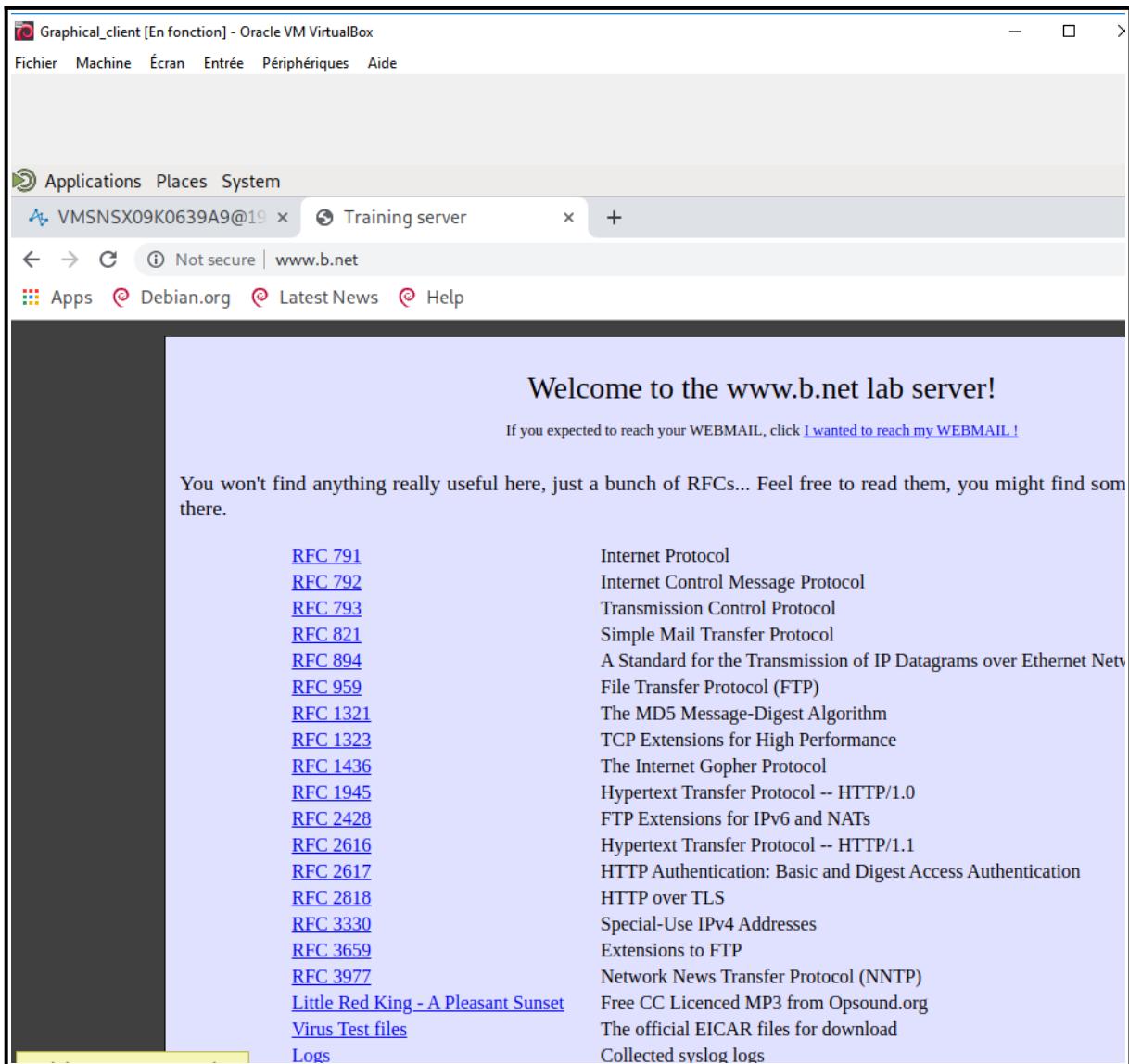
- Header:** Parcours de professionnel, https://192.168.1.254/admin/admin.html#securitypolicy/local/4/filter, Latest News, Help, admin WRITE / READ
- Breadcrumbs:** MONITORING > SECURITY POLICY / FILTER - NAT
- Table Headers:** (4) Lab_4, Edit, Export, Filtering, NAT
- Table Rows:**
 - Original traffic (before translation):**
 - 1: Source: srv_ftp_priv, Destination: Internet interface: out, Dest. port: Any, Action: ARP, Destination: srv_ftp_pub
 - 2: Source: Internet interface: out, Destination: srv_ftp_pub, Dest. port: Any, Action: ..
 - 3: Source: srv_mail_priv, Destination: Internet interface: out, Dest. port: Any, Action: ..
 - 4: Source: Internet interface: out, Destination: srv_mail_pub, Dest. port: Any, Action: ..
 - DYNAMIC NAT (contains 1 rules, from 5 to 5):**
 - 5: Source: Network_in, Destination: Internet interface: out, Dest. port: Any, Action: Firewall_out, Destination: ephemeral_fw, Protocol: Ai
 - STATIC NAT PAR PORT (contains 2 rules, from 6 to 7):**
 - 6: Source: Internet interface: out, Destination: Firewall_out, Dest. port: http, Action: ..
 - 7: Source: Internet interface: out, Destination: Firewall_out, Dest. port: webmail, Action: ..
- Page Navigation:** <, <, Page 1 of 1, >, >

2ème étape :

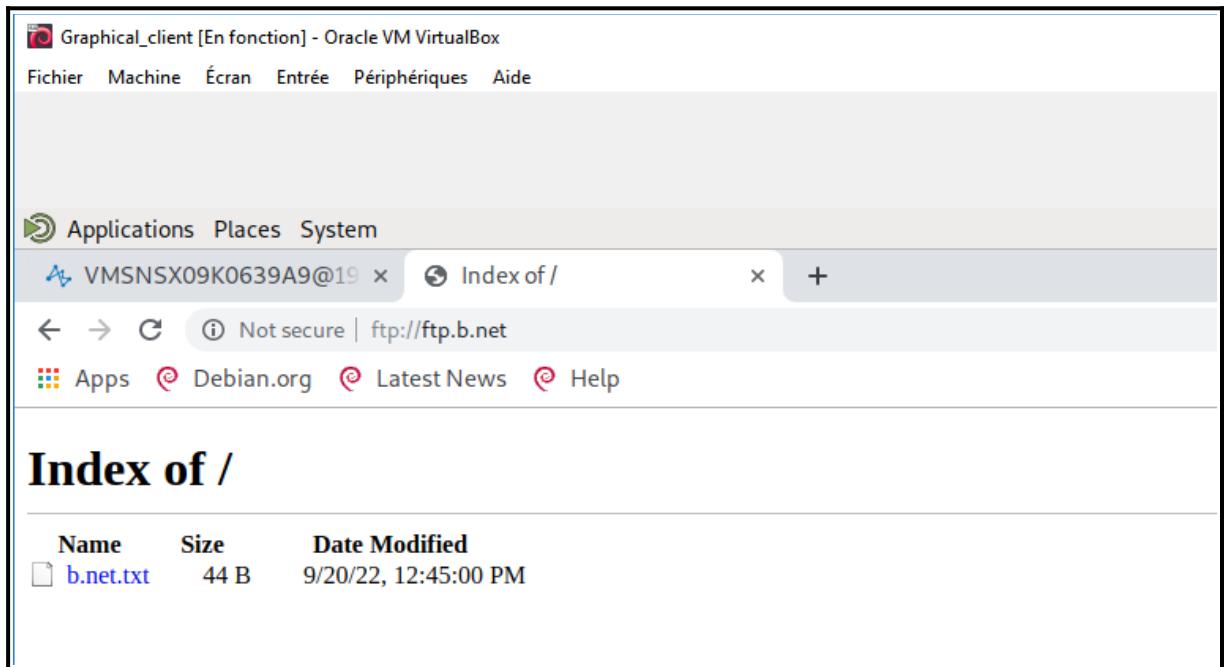
- Nous ajoutons une règle NAT ayant pour but que les machines de nos réseaux internes puissent accéder internet anonymement sans dévoiler leur adresse IP privée.
- Une règle permettant de joindre chaque serveur depuis le réseau externe grâce aux IP publiques.
- Une règle permettant de joindre le serveur 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.



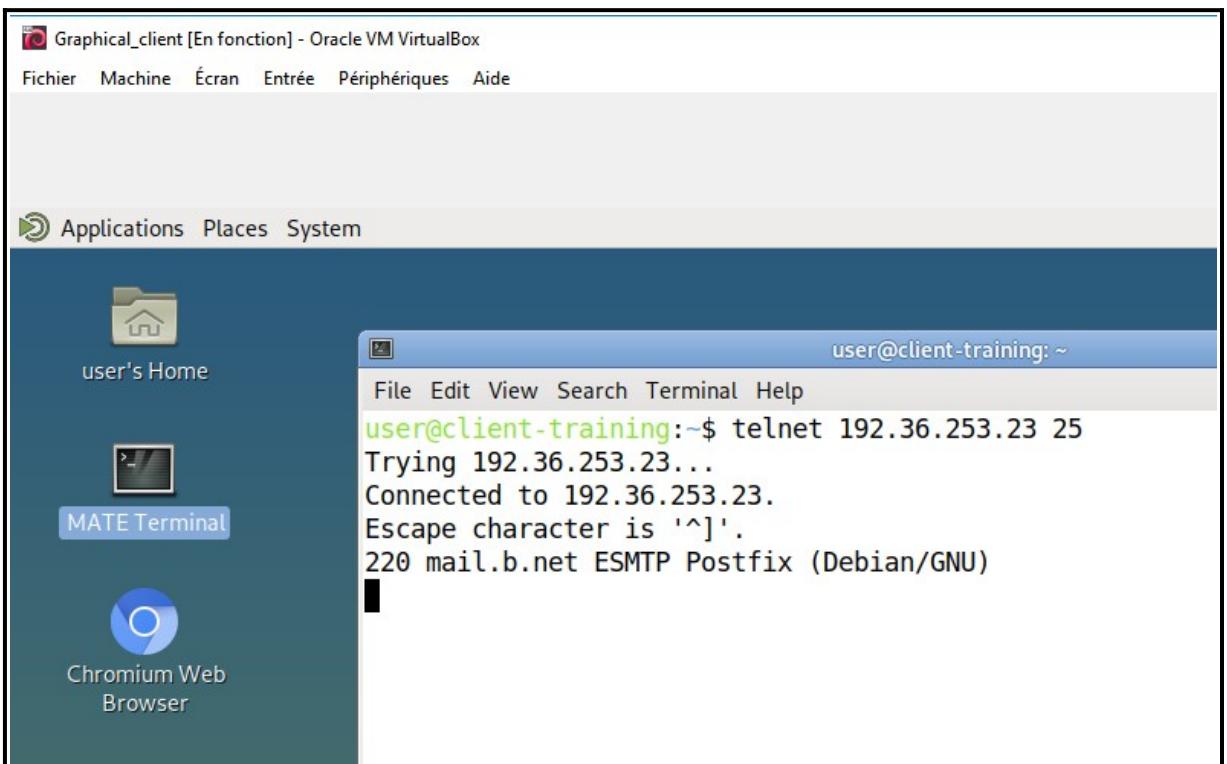
3ème étape : Test de l'accès à internet.



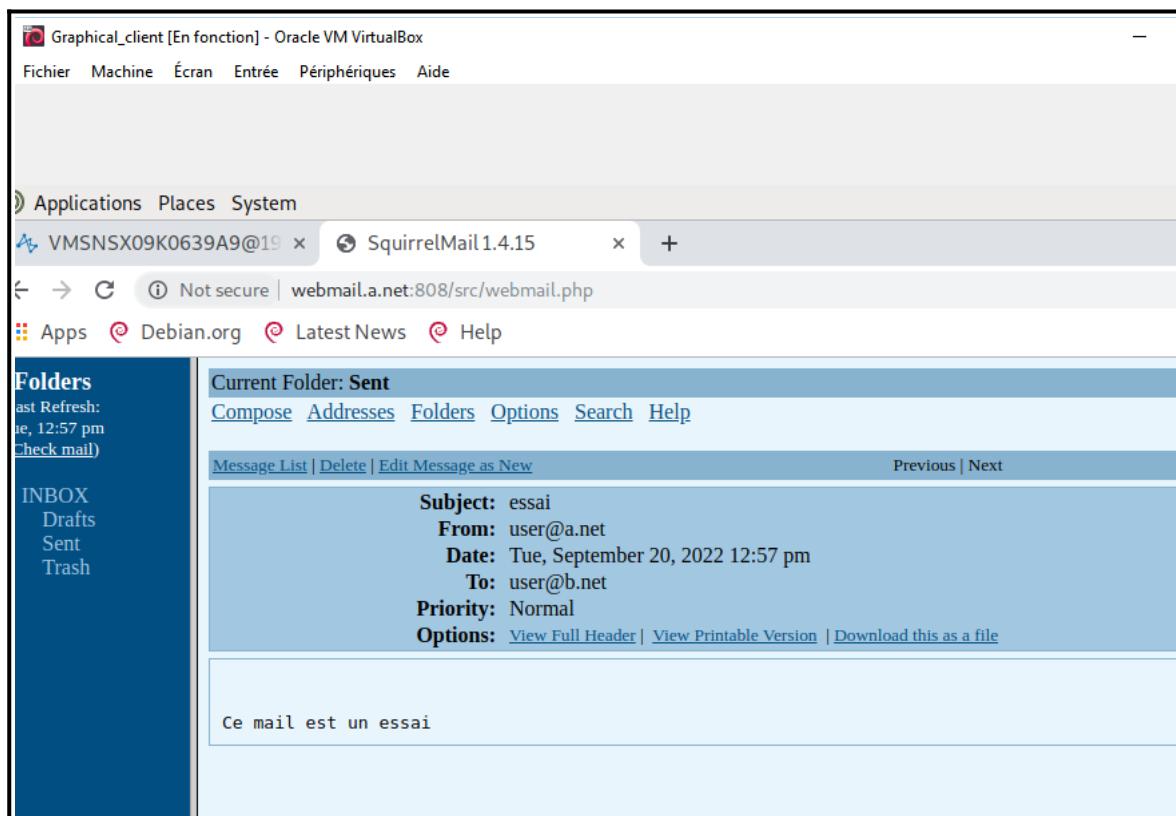
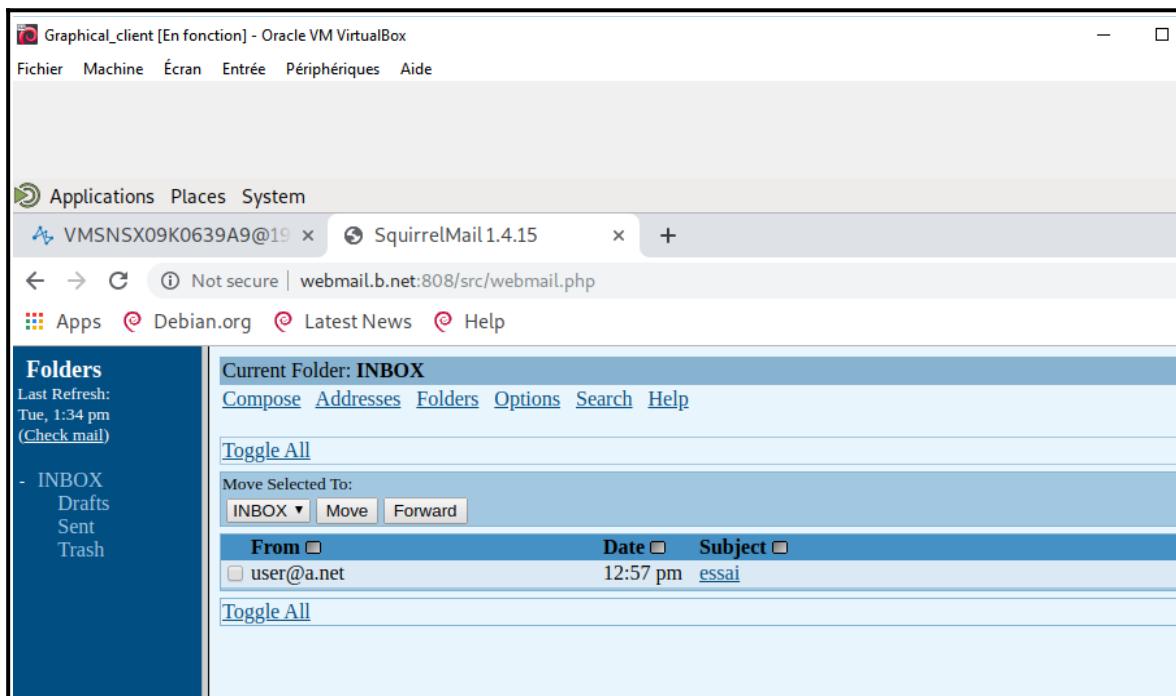
4ème étape : Le réseau A pouvant communiquer avec ses différents services celui-ci test donc l'accès au service du réseau distant B, notamment avec le serveur WEB.



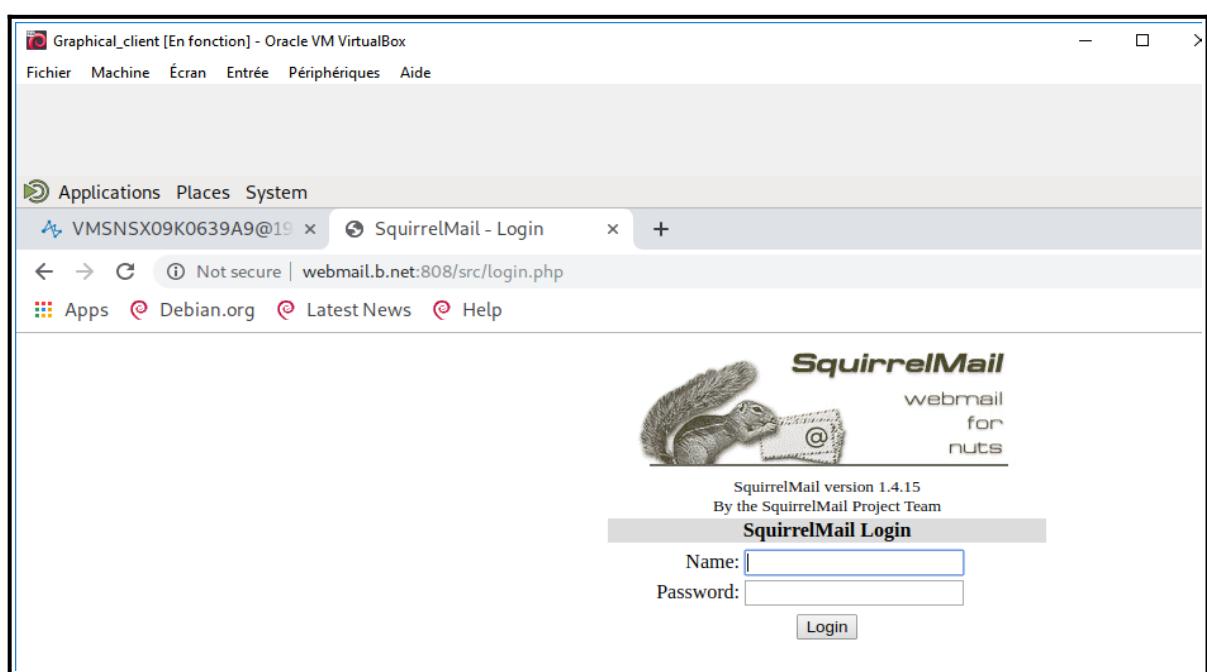
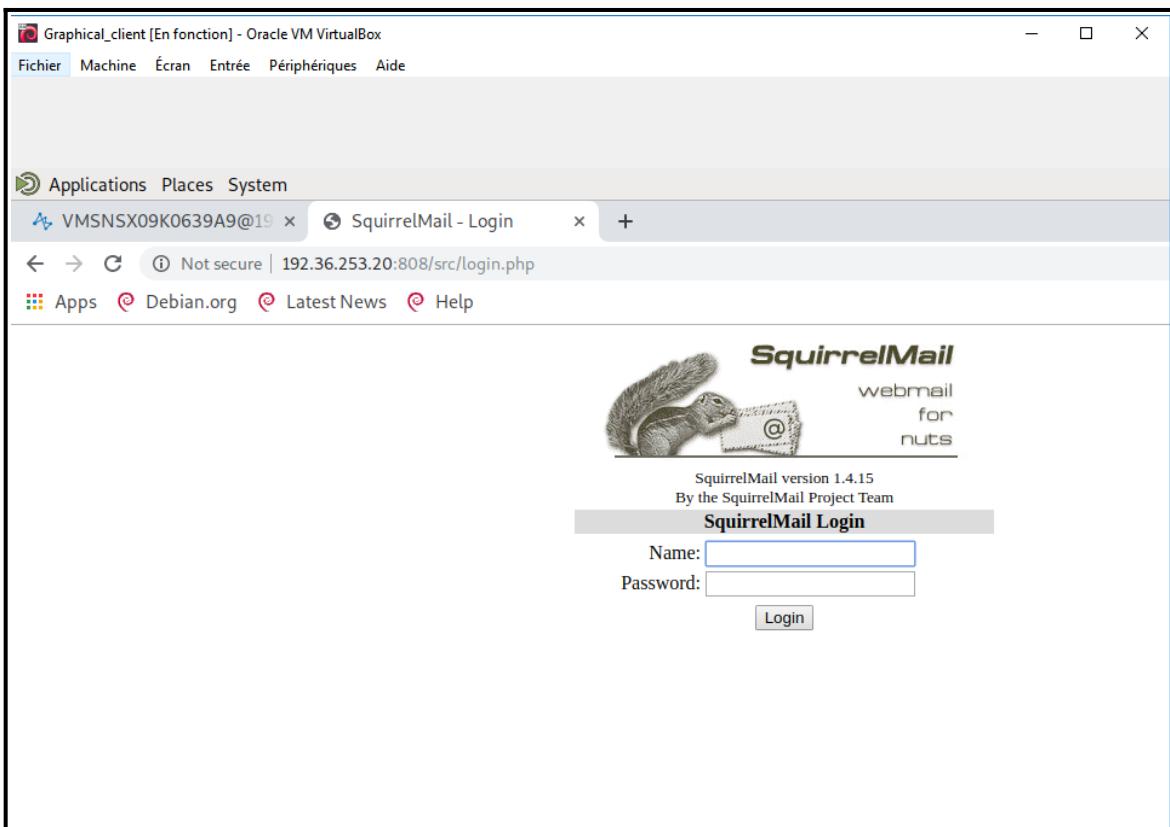
5ème étape : Nous testons l'accès au serveur FTP de B depuis le réseau A.



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 :

The screenshot shows the EVA1 security policy/filter-NAT interface. The top navigation bar includes 'Fichier', 'Machine', 'Écran', 'Entrée', 'Périphériques', and 'Aide'. Below the bar, there's a language selection 'fr' and a '+' button. The URL in the address bar is <https://192.168.2.254/admin/admin.html#securitypolicy/local/4/nat>. The main header displays 'EVA1 VMSNSX09K0639A9' and a user 'admin' with 'WRITE / R...' permissions. The interface has tabs for 'MONITORING' and 'CONFIGURATION', with 'CONFIGURATION' selected. A sub-header ' SECURITY POLICY / FILTER - NAT' is visible. Below it, a table lists three security rules:

	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

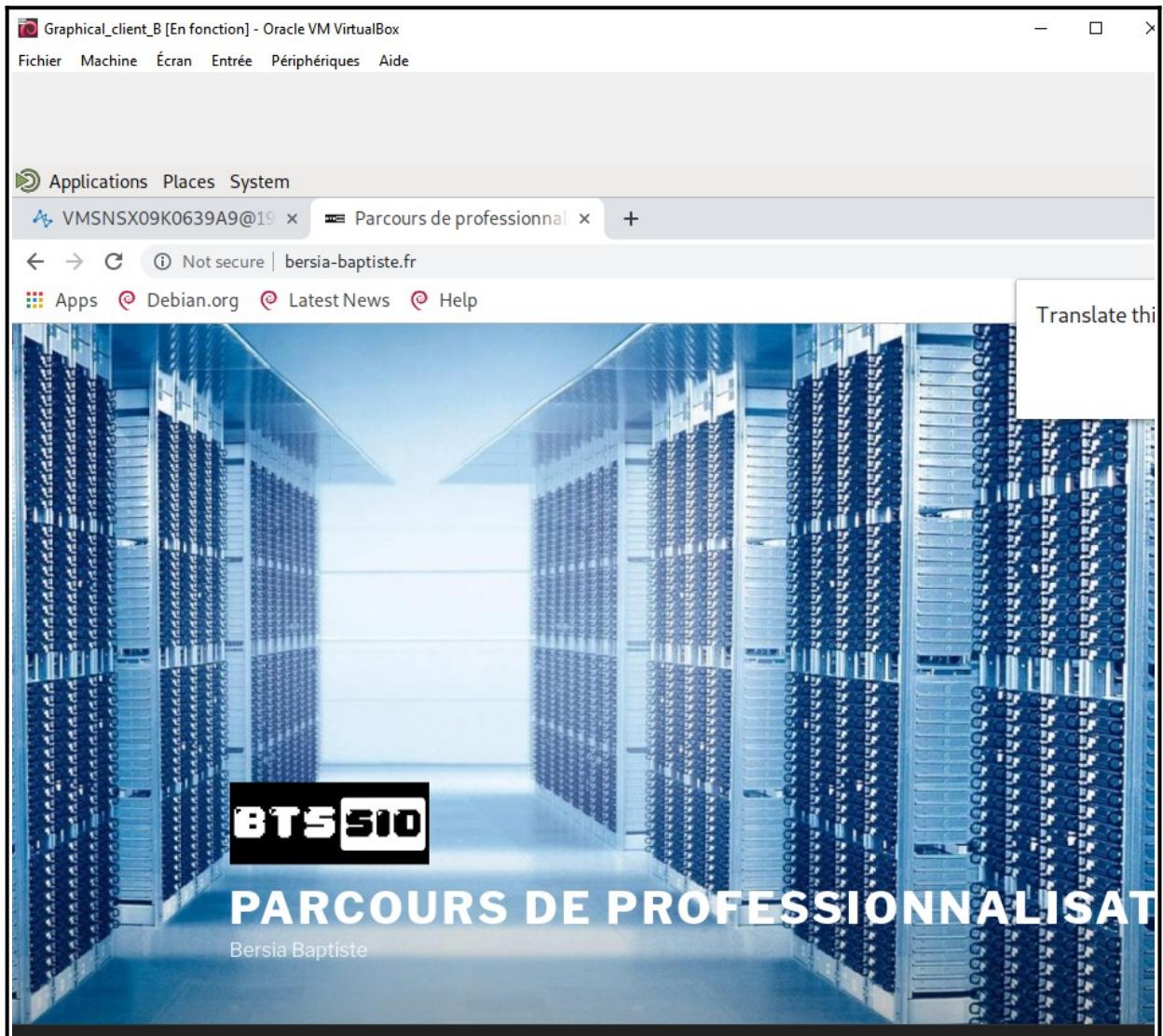
1ère étape : Nous activons la politique de filtrage/Nat numéro 4.

The screenshot shows the EVA1 security policy configuration interface. The top navigation bar includes 'Fichier', 'Machine', 'Écran', 'Entrée', 'Périphériques', and 'Aide'. The status bar indicates 'fr Tue'. The main area displays a table of NAT rules:

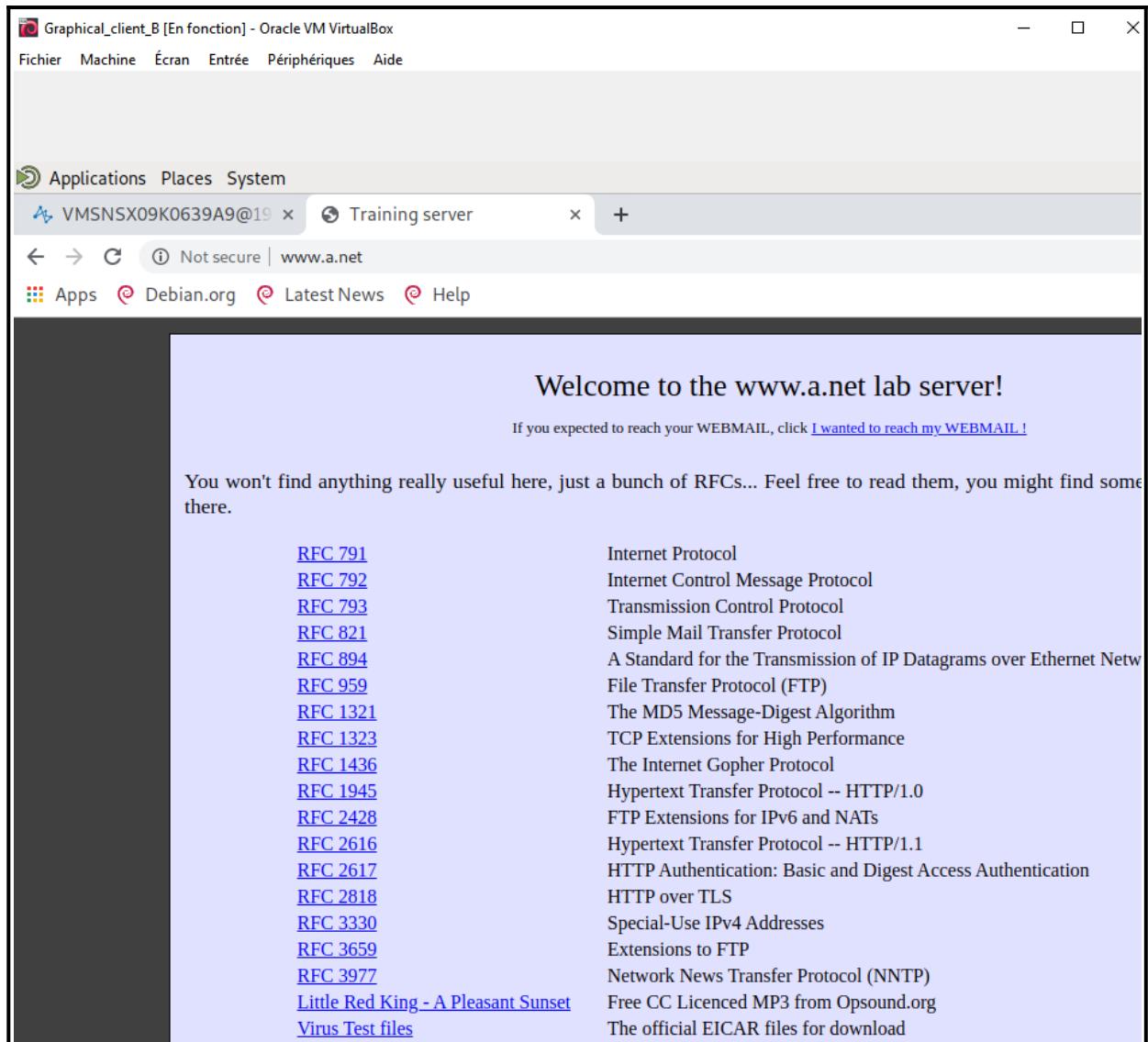
Index	Status	Original traffic (before translation)			Traffic after translation			
		Source	Destination	Dest. port	Source	Src. port	Destination	Dest. port
1	on	srv_ftp_priv	interface: out	Any	..	srv_ftp_pub		
2	on	Internet	interface: out	..	srv_ftp_pub		Any	
3	on	srv_mail_priv	interface: out	Any	..	srv_mail_pub		
4	on	Internet	interface: out	..	srv_mail_pub		Any	
DYNAMIC NAT (contains 1 rules, from 5 to 5)								
5	on	Network_in	Internet	Any	..	Firewall_out	Any	
STATIC NAT PAR PORT (contains 2 rules, from 6 to 7)								
6	on	Internet	Firewall_out	http	..	srv_web_priv		
7	on	Internet	Firewall_out	webmail	..	srv_web_priv		

2ème étape :

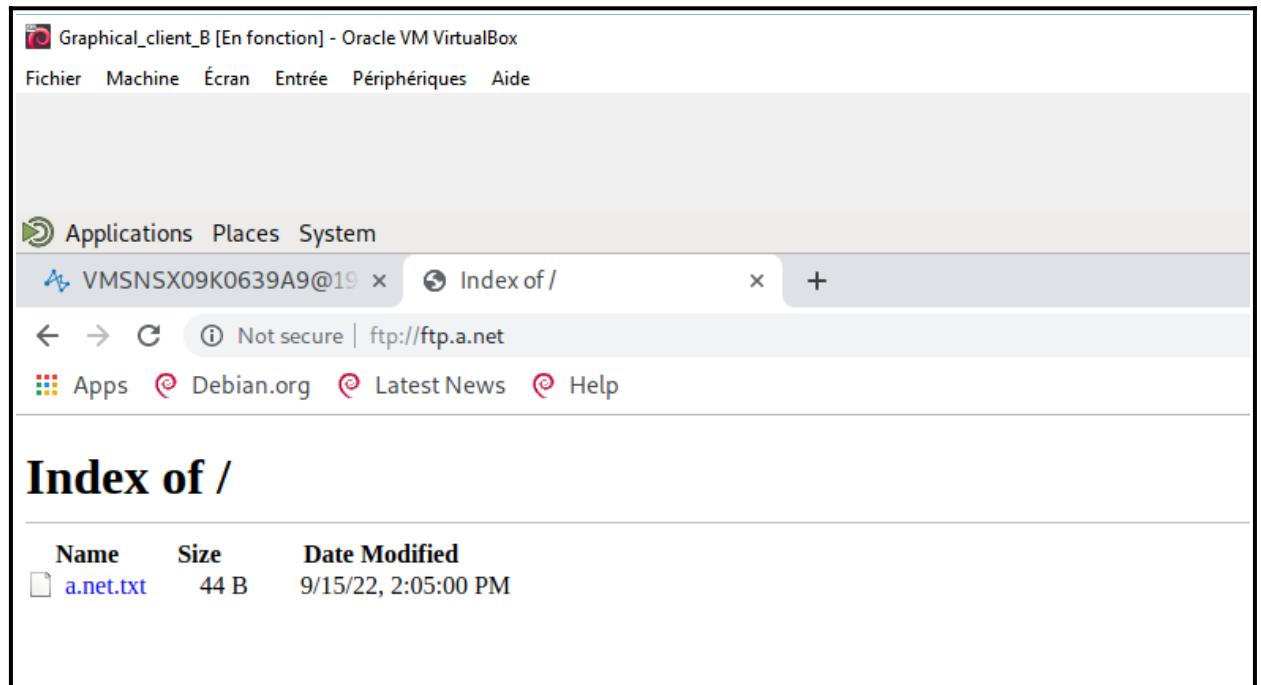
- Nous ajoutons une règle NAT ayant pour but que les machines de nos réseaux internes puissent accéder internet anonymement sans dévoiler leur adresse IP privée.
- Une règle permettant de joindre chaque serveur depuis le réseau externe grâce aux IP publiques.
- Une règle permettant de joindre le serveur 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.



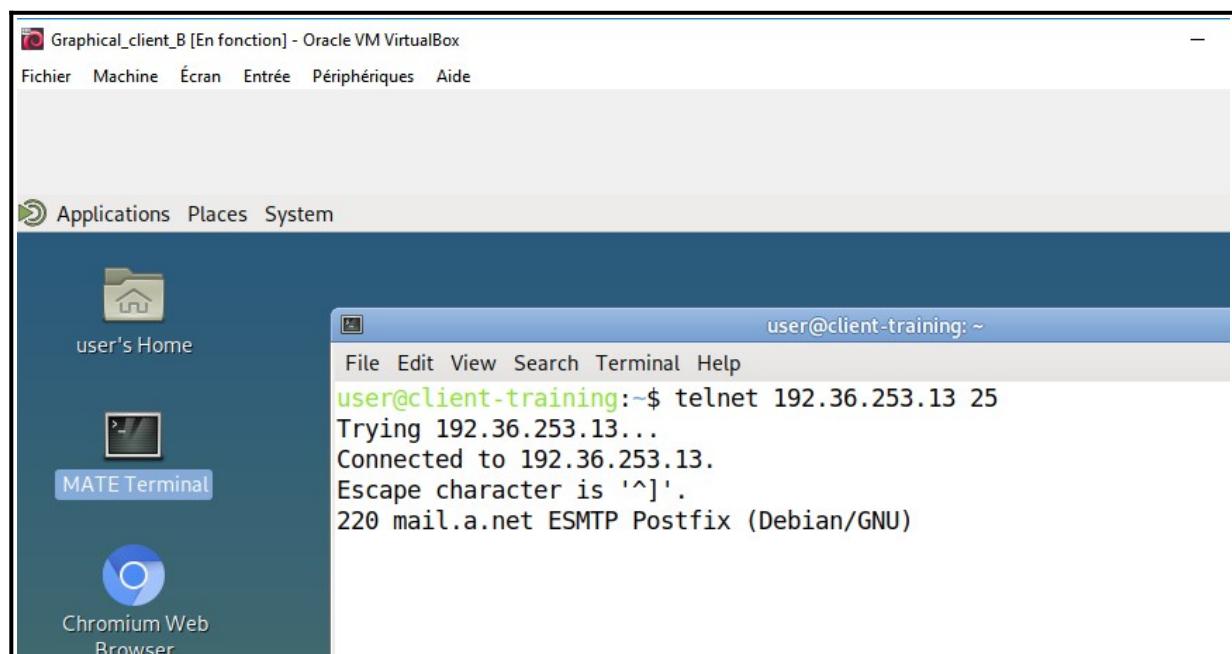
3ème étape : Test de l'accès à internet.



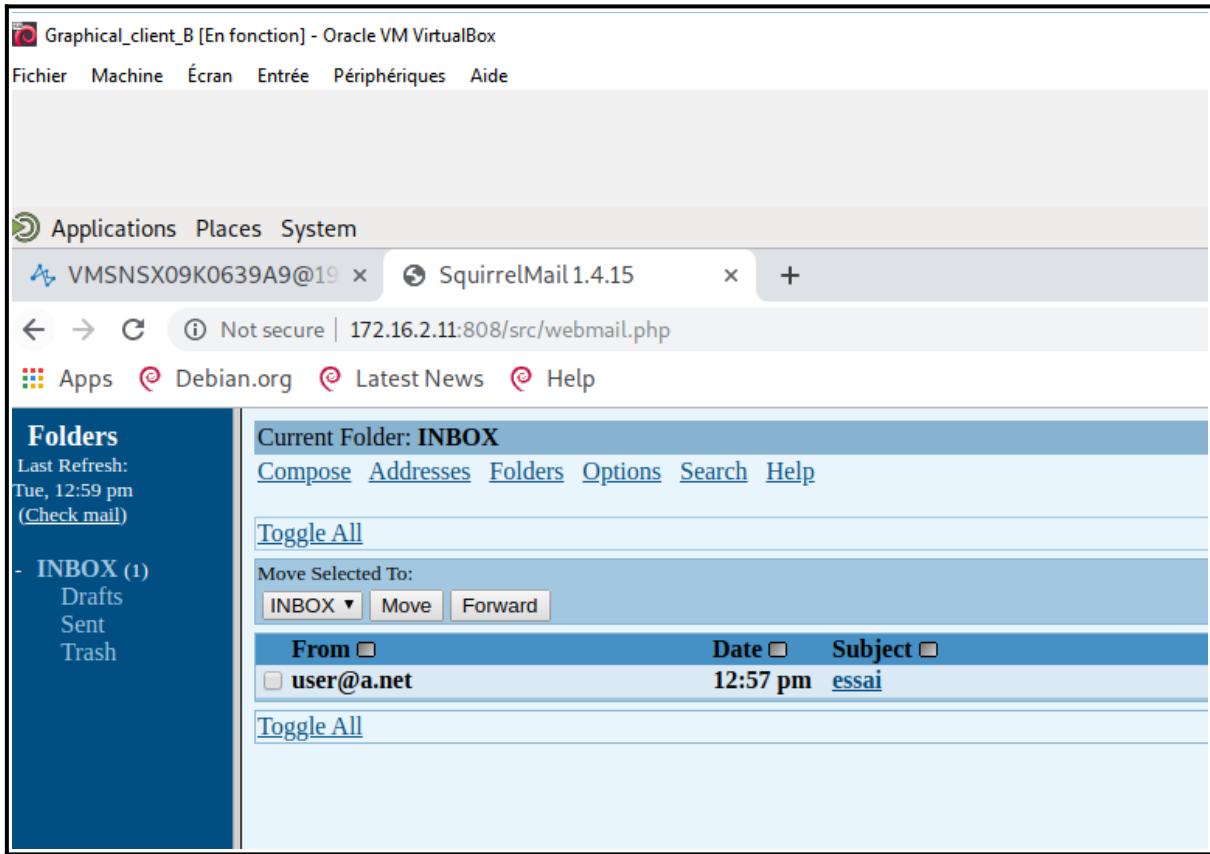
4ème étape : Le réseau B pouvant communiquer avec ses différents services celui-ci test donc l'accès au service du réseau distant A, notamment avec le serveur WEB.



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.