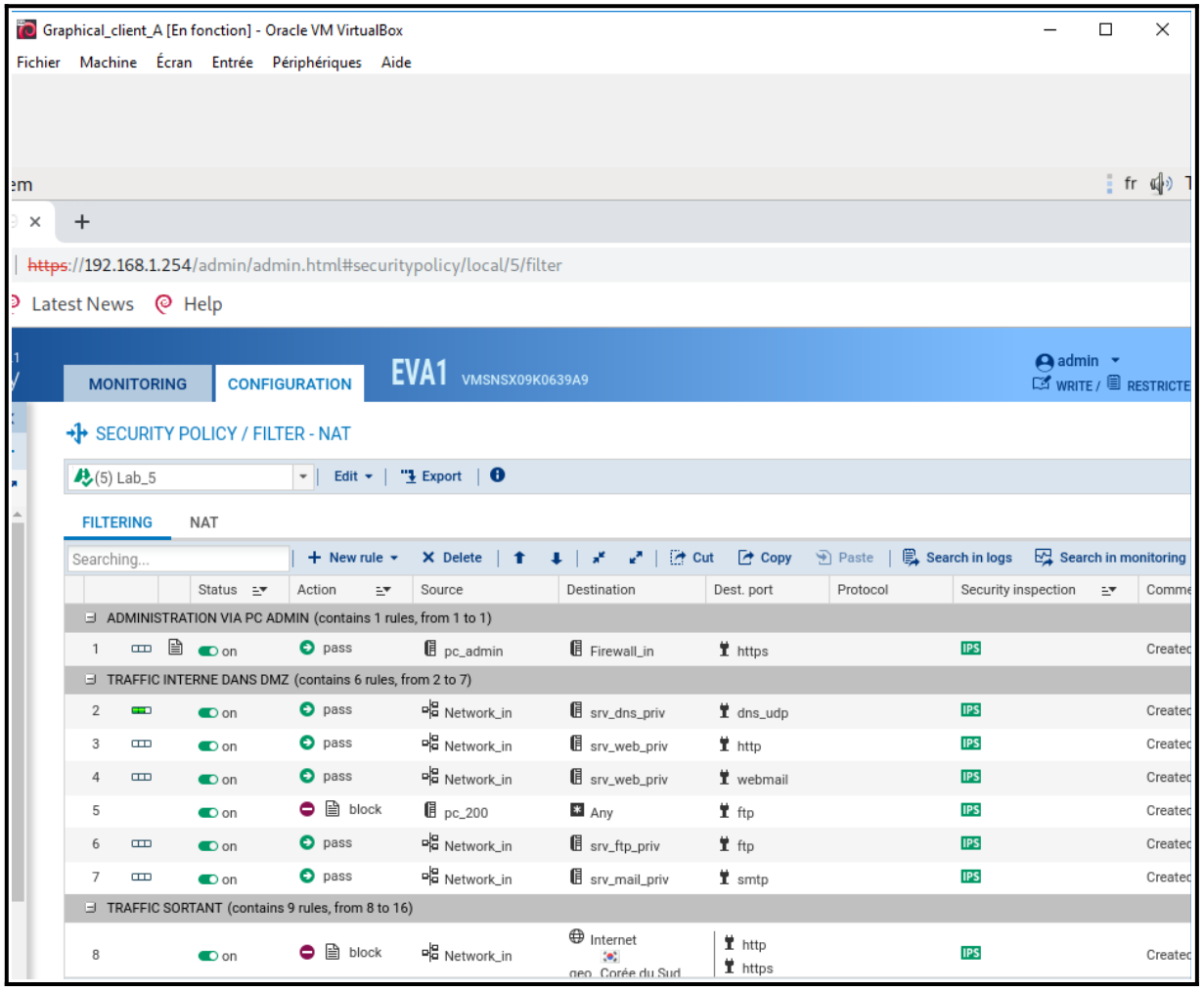
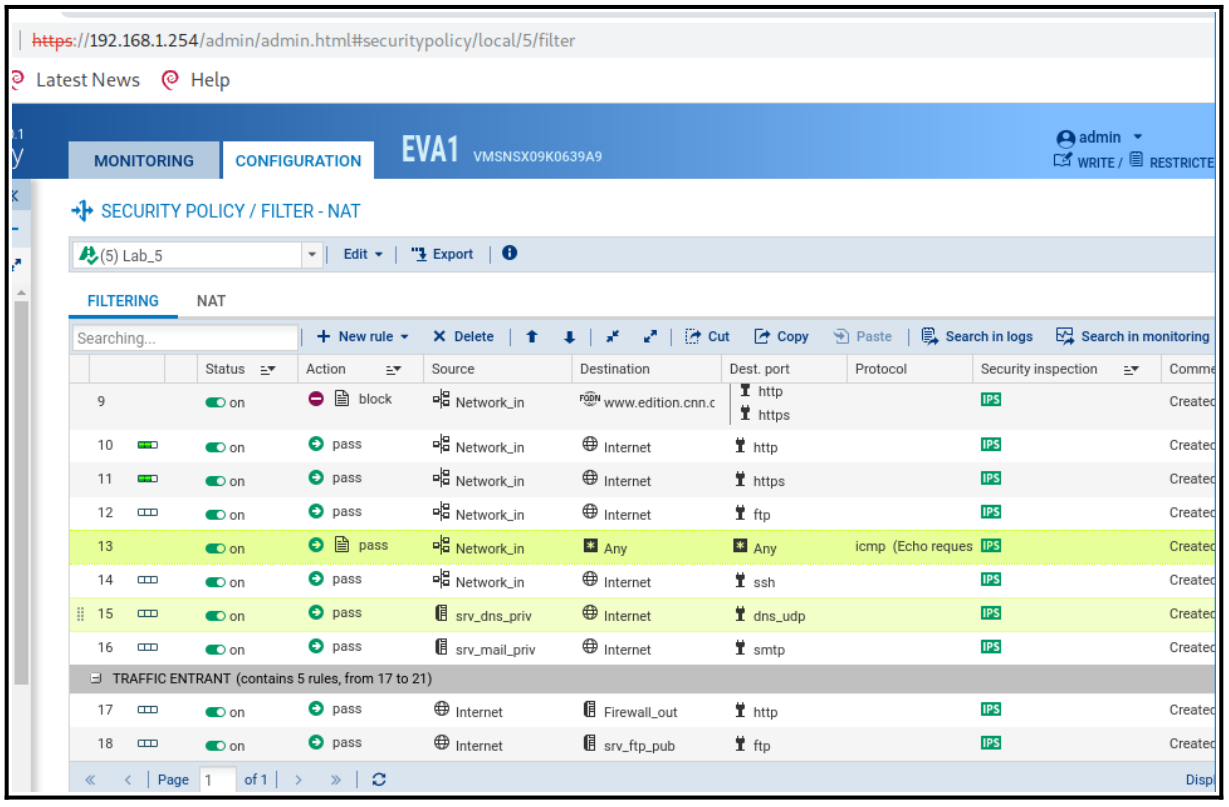
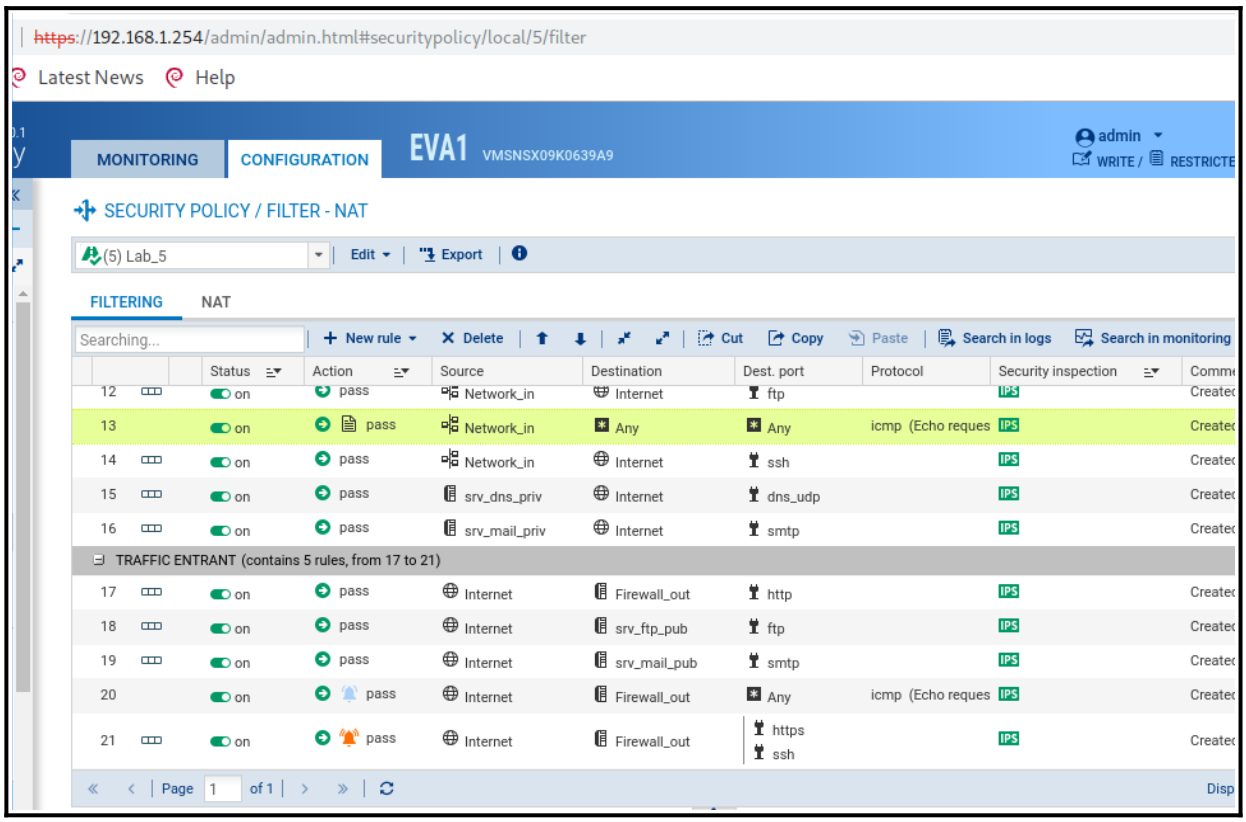
STORMSHIELD

LAB 5 :
Filtrage

Réseau A :


Graphical_client_A [En fonction] - Oracle VM VirtualBox
Fichier Machine Écran Entrée Périphériques Aide
https://192.168.1.254/admin/admin.html#securitypolicy/local/5/filter
Latest News Help
MONITORING CONFIGURATION EVA1 VMSNSX09K0639A9
admin
SECURITY POLICY / FILTER - NAT
(5) Lab_5 Edit Export
FILTERING NAT
Searching... New rule Delete Cut Copy Paste Search in logs Search in monitoring
Status Action Source Destination Dest. port Protocol Security inspection
ADMINISTRATION VIA PC ADMIN (contains 1 rules, from 1 to 1)
1 on pass pc_admin Firewall_in https IPS Created
TRAFFIC INTERNE DANS DMZ (contains 6 rules, from 2 to 7)
2 on pass Network_in srv_dns_priv dns_udp IPS Created
3 on pass Network_in srv_web_priv http IPS Created
4 on pass Network_in srv_web_priv webmail IPS Created
5 on block pc_200 Any ftp IPS Created
6 on pass Network_in srv_ftp_priv ftp IPS Created
7 on pass Network_in srv_mail_priv smtp IPS Created
TRAFFIC SORTANT (contains 9 rules, from 8 to 16)
8 on block Network_in Internet geo_Corée du Sud http https IPS Created


https://192.168.1.254/admin/admin.html#securitypolicy/local/5/filter
Latest News Help
MONITORING CONFIGURATION EVA1 VMSNSX09K0639A9
admin
SECURITY POLICY / FILTER - NAT
(5) Lab_5 Edit Export
FILTERING NAT
Searching... New rule Delete Cut Copy Paste Search in logs Search in monitoring
Status Action Source Destination Dest. port Protocol Security inspection
9 on block Network_in FQDN www.edition.cnn.c http https IPS Created
10 on pass Network_in Internet http IPS Created
11 on pass Network_in Internet https IPS Created
12 on pass Network_in Internet ftp IPS Created
13 on pass Network_in Any Any icmp (Echo reques IPS Created
14 on pass Network_in Internet ssh IPS Created
15 on pass srv_dns_priv Internet dns_udp IPS Created
16 on pass srv_mail_priv Internet smtp IPS Created
TRAFFIC ENTRANT (contains 5 rules, from 17 to 21)
17 on pass Internet Firewall_out http IPS Created
18 on pass Internet srv_ftp_pub ftp IPS Created
Page 1 of 1



1ère étape : Depuis le réseau A nous mettons en place différentes règles dans la politique de filtrage numéro 5 :

Trafics internes :

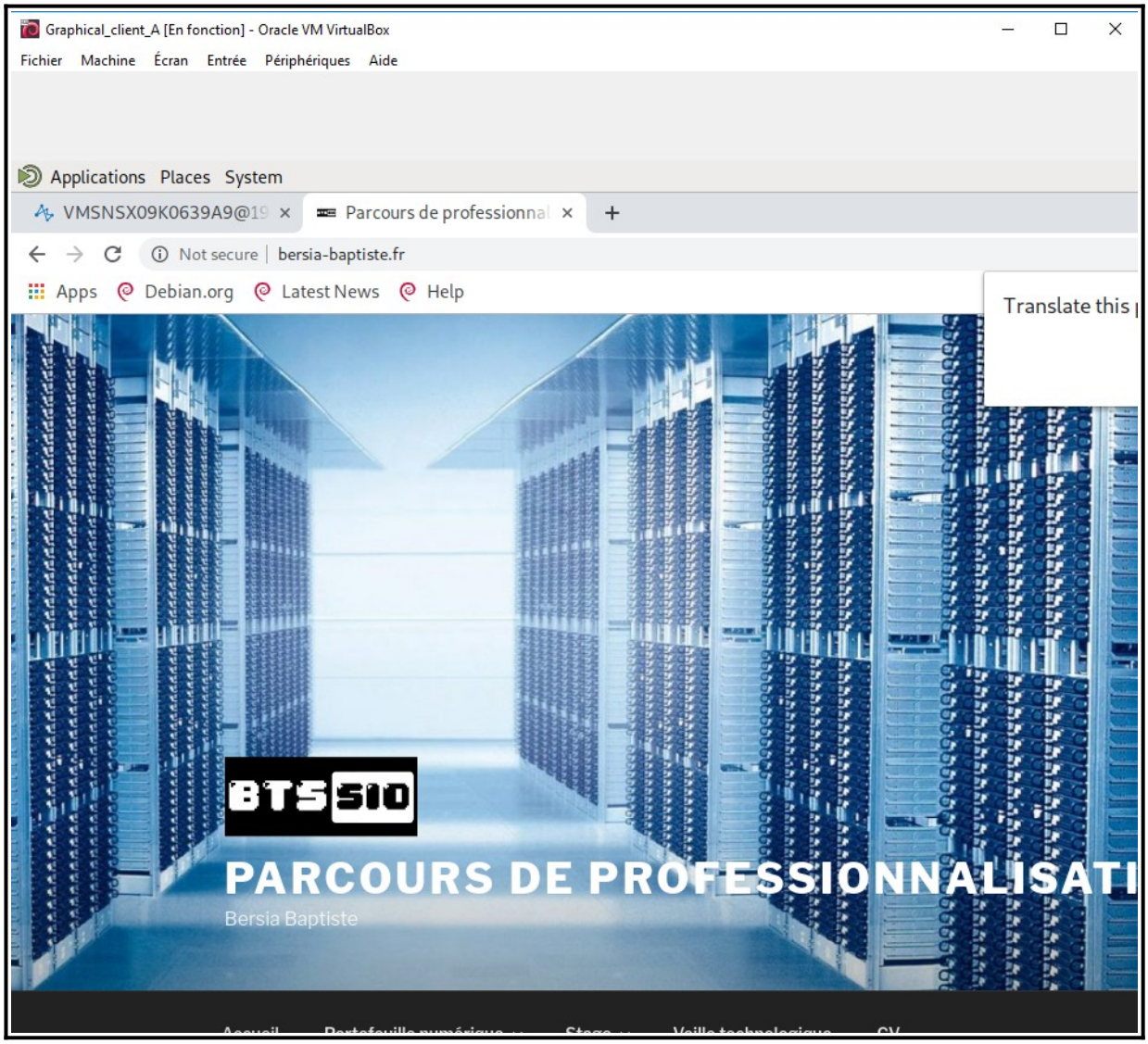
- Accès aux serveurs de notre DMZ (DNS,WEB, FTP, SMTP).

Trafics sortants :

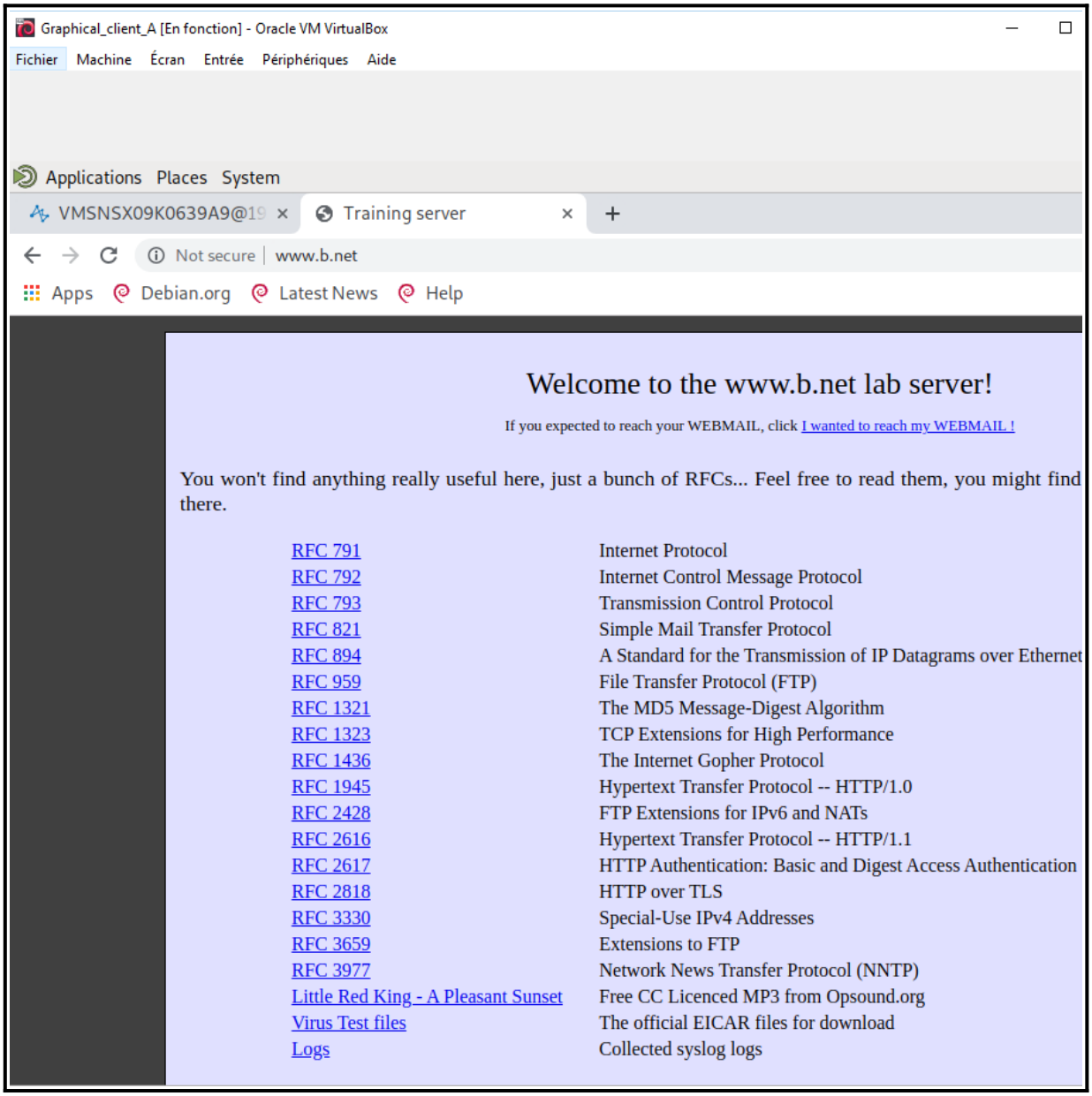
- Accès aux sites web d'internet en HTTP et HTTPS sauf sur les sites de la République de Corée.
- Accès au site ***https://edition.cnn.com*** bloqué.
- Un stagiaire possédant la machine pc_200 doit avoir interdiction d'effectuer une requête FTP.
- Accès aux serveurs FTP et WEB d'internet.
- Autorisation d'émettre un ping vers n'importe quelle destination.
- Accès à la connexion SSH au firewalls des autres sites.
- Seul le serveur DNS interne peut envoyer des requêtes DNS vers l'extérieur.
- Le serveur mail peut envoyer des mails vers n'importe quel serveur mail externe.

Trafics entrants :

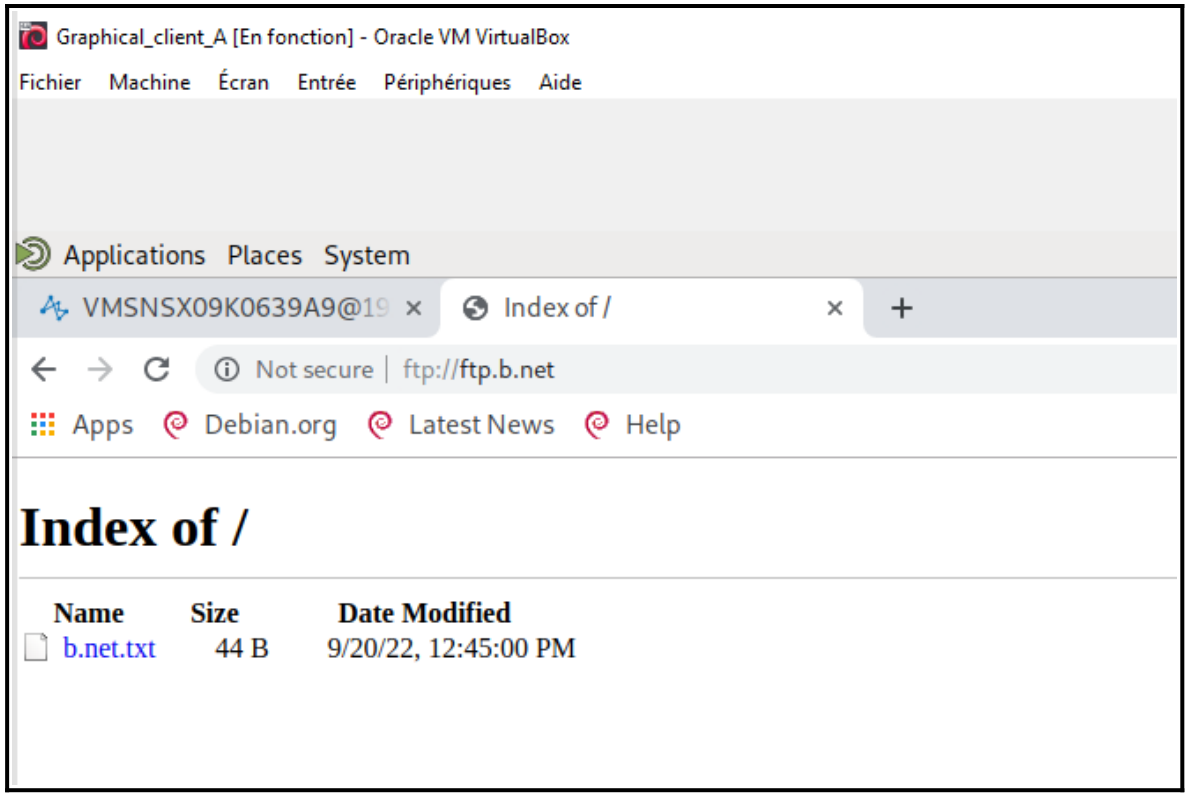
- Accès des réseaux externes à nos serveurs WEB et FTP publique.
- Autorisation des serveurs mail externes à transmettre des e-mails à notre serveur de messagerie.
- Autorisation des réseaux externes à pinger l'interface « out » de notre firewall, événement notifier avec une alarme mineure.
- Autorisation des réseaux externes à se connecter à notre firewall via l'interface web et SSH, événement notifier avec une alarme majeur.



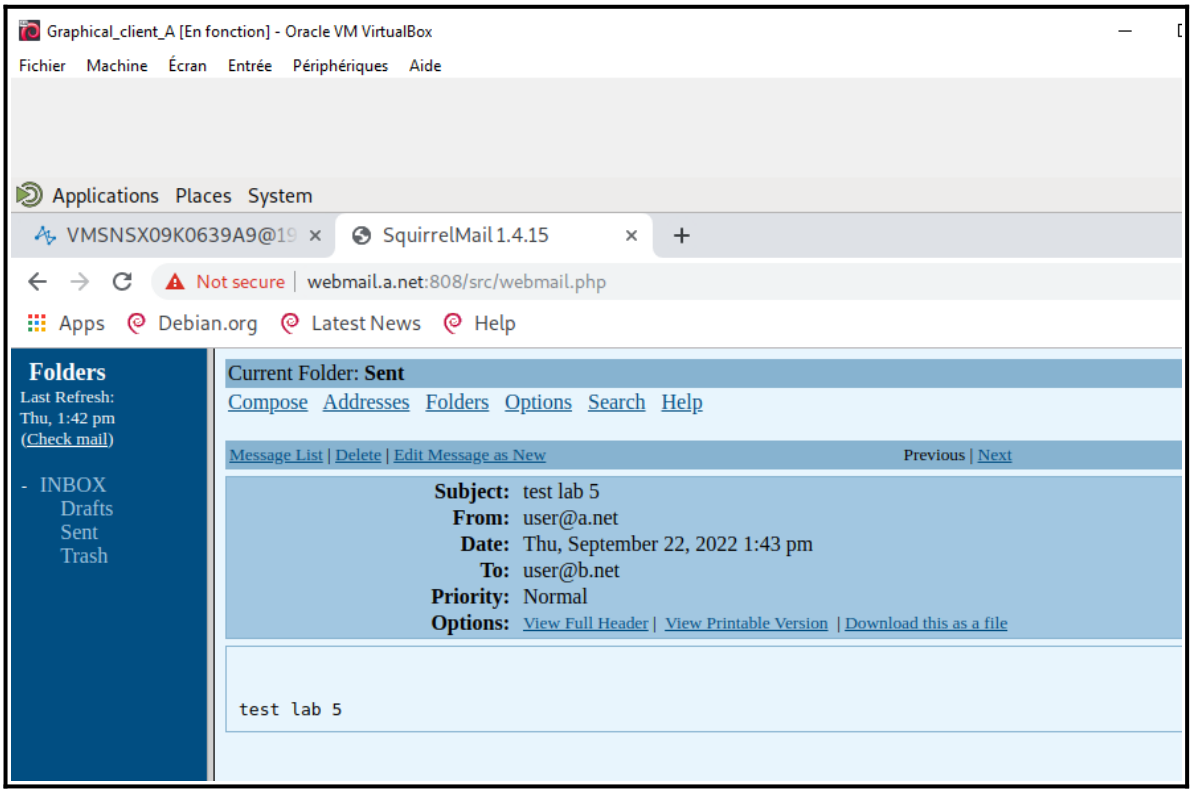
2ème étape : Test accès à un site internet en HTTP.



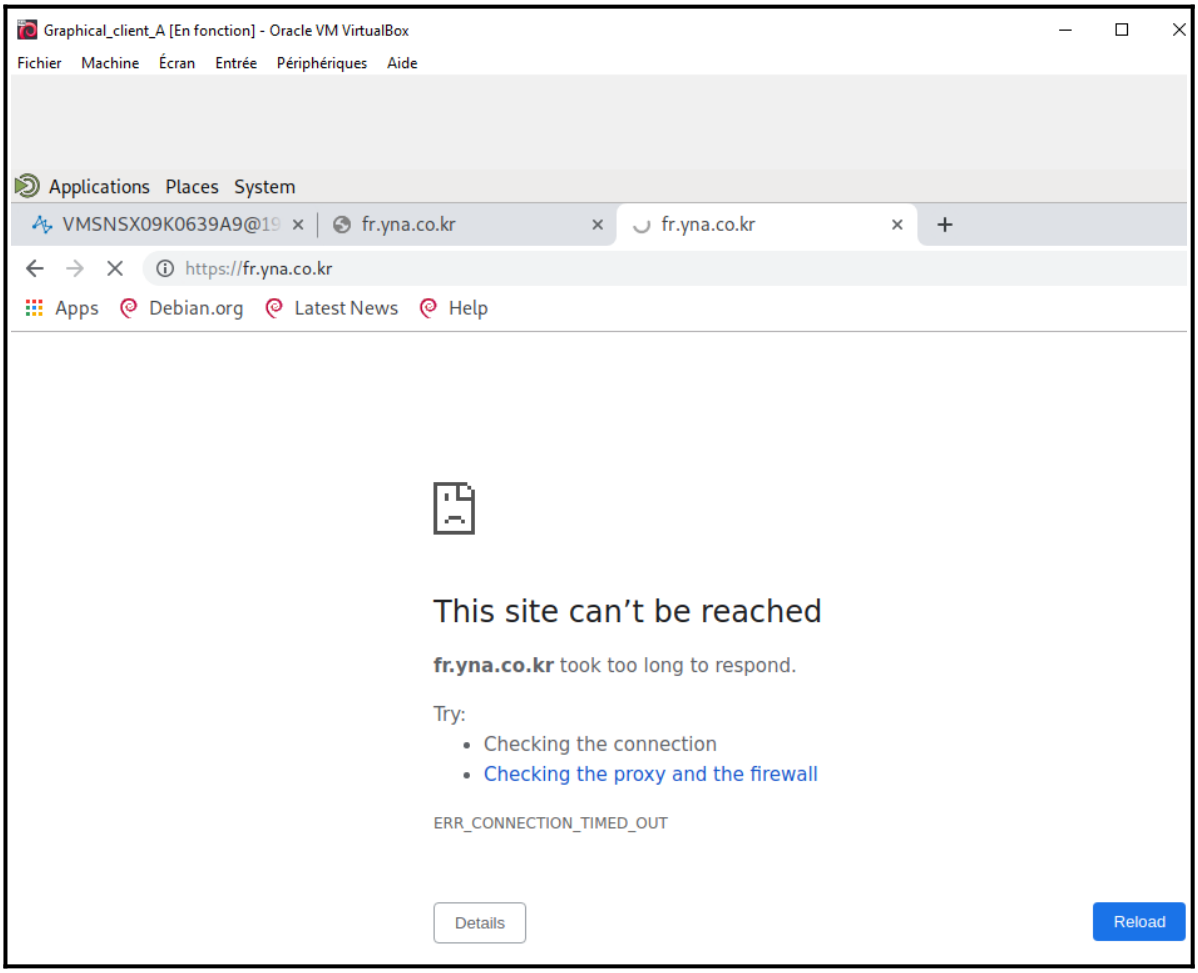
3ème étape : Test accès serveur WEB de B.



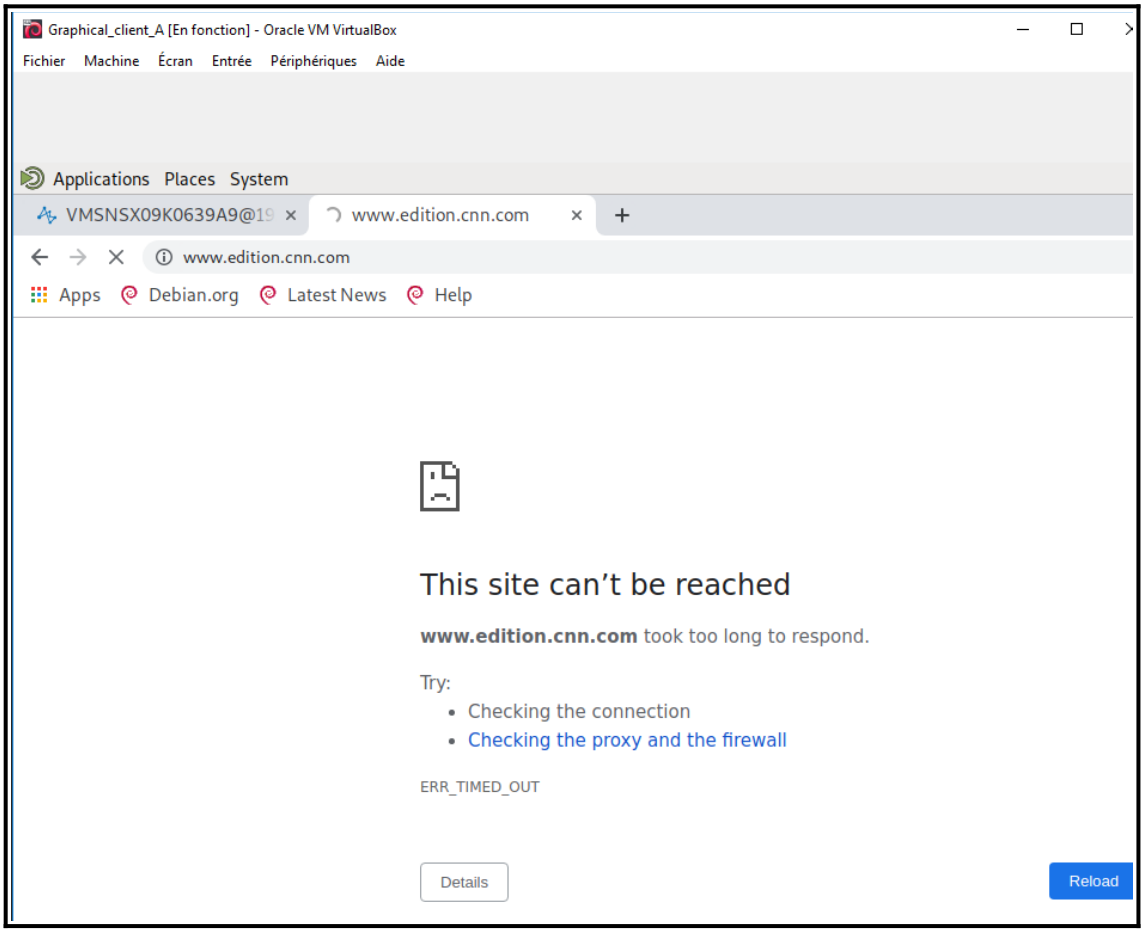
4ème étape: Test accès serveur FTP de B.



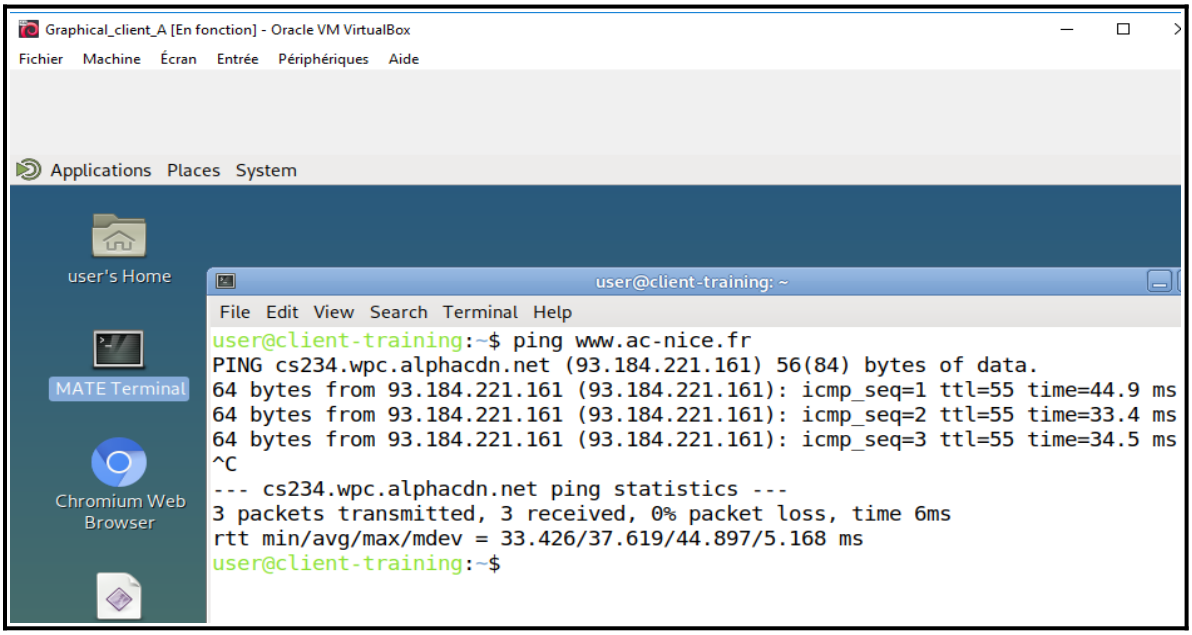
5ème étape : Test envoie d'un mail à B depuis la webmail de A.



6ème étape : Tentative de connexion à un site web de la République de Corée. Celui-ci n'est donc pas accessible.

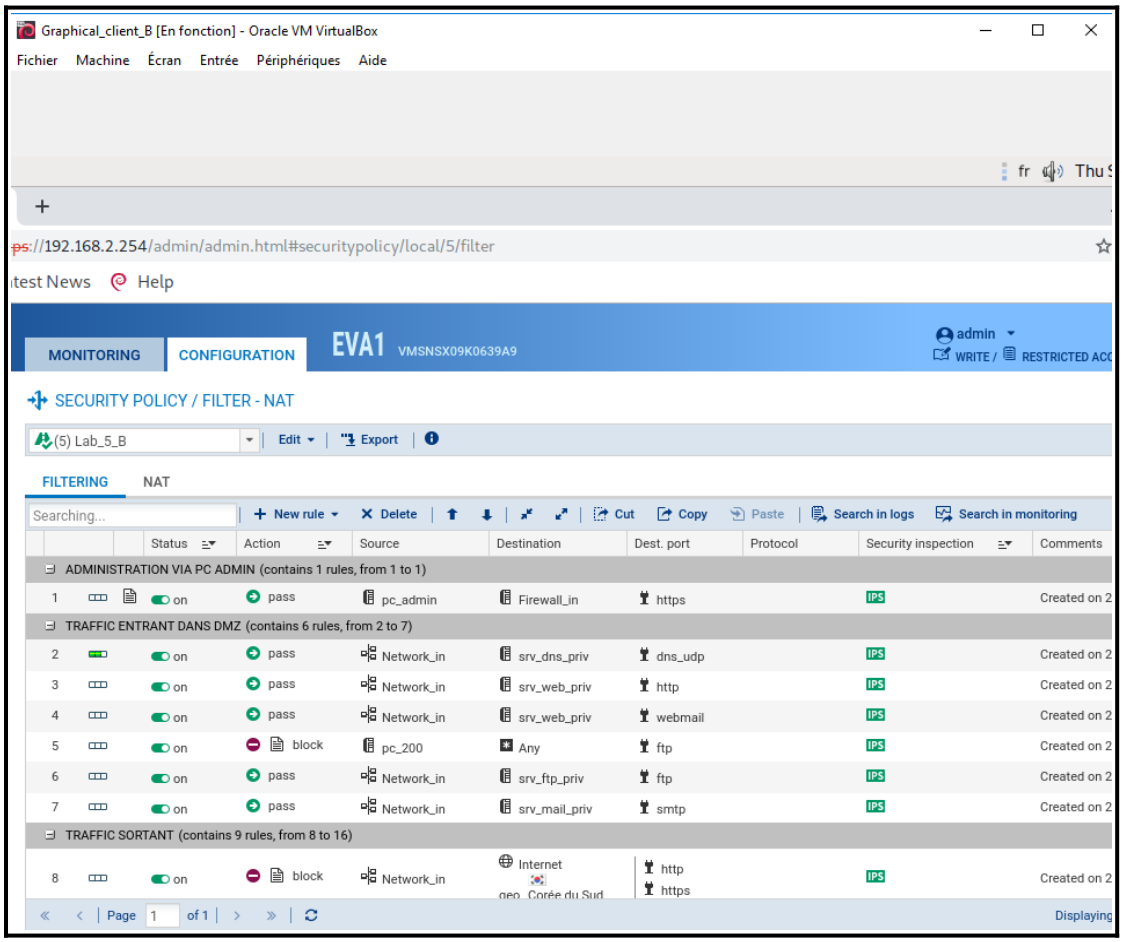


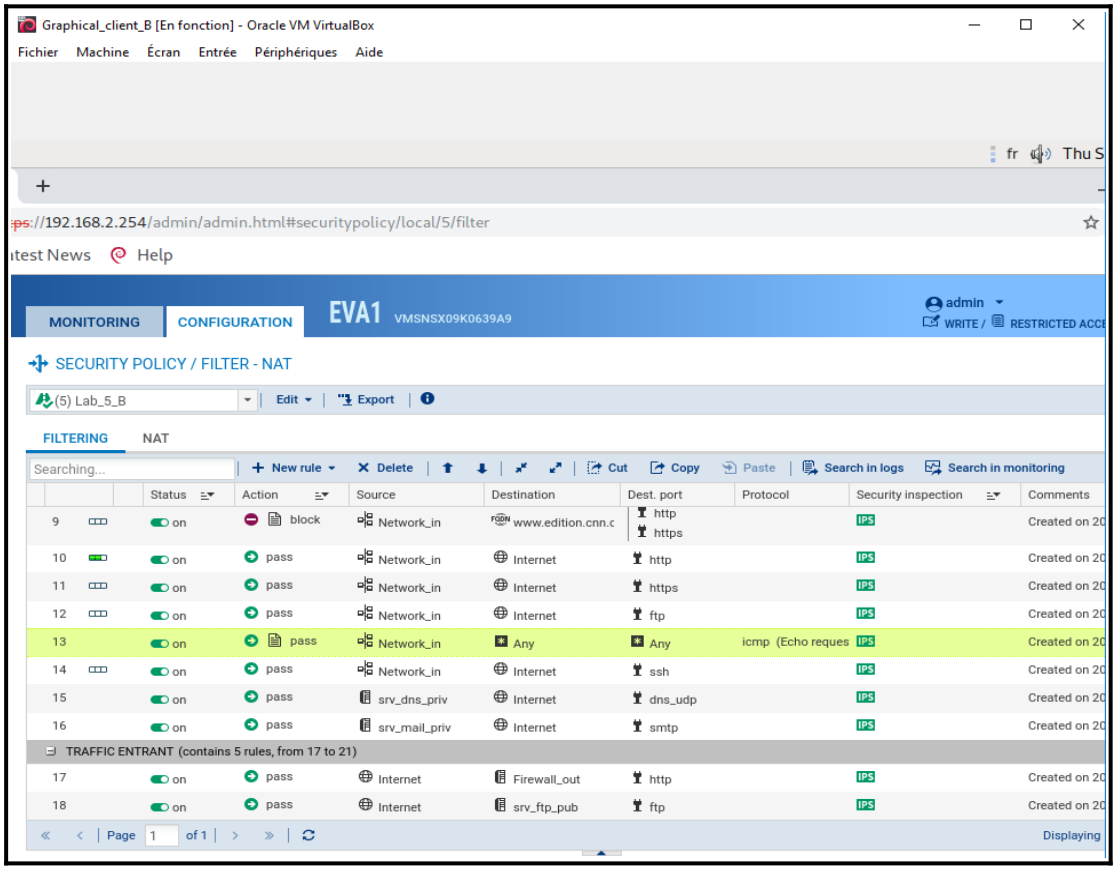
7ème étape : Tentative de connexion au site web edition.cnn. Celui-ci n'est donc pas accessible.



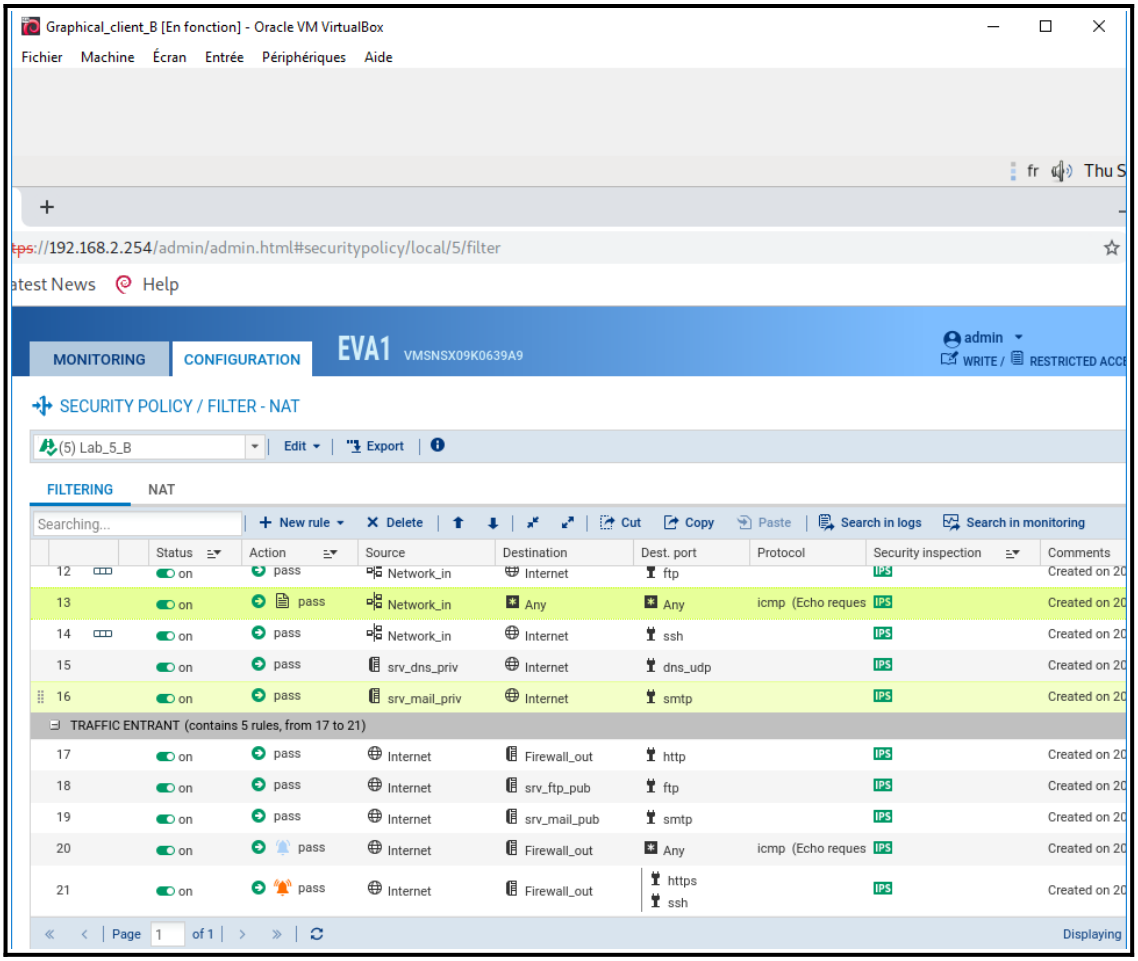
8ème étape : Test d'un ping vers n'importe quelle destination, dans le cas présent ac-nice.fr .

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/5/filter
test News Help
MONITORING CONFIGURATION EVA1 VMSNSX09K0639A9
admin
WRITE / RESTRICTED ACC
SECURITY POLICY / FILTER - NAT
(5) Lab_5_B Edit Export
FILTERING NAT
Searching... New rule Delete Cut Copy Paste Search in logs Search in monitoring
Status Action Source Destination Dest. port Protocol Security inspection Comments
ADMINISTRATION VIA PC ADMIN (contains 1 rules, from 1 to 1)
1 on pass pc_admin Firewall_in https IPS Created on 2
TRAFFIC ENTRANT DANS DMZ (contains 6 rules, from 2 to 7)
2 on pass Network_in srv_dns_priv dns_udp IPS Created on 2
3 on pass Network_in srv_web_priv http IPS Created on 2
4 on pass Network_in srv_web_priv webmail IPS Created on 2
5 on block pc_200 Any ftp IPS Created on 2
6 on pass Network_in srv_ftp_priv ftp IPS Created on 2
7 on pass Network_in srv_mail_priv smtp IPS Created on 2
TRAFFIC SORTANT (contains 9 rules, from 8 to 16)
8 on block Network_in Internet geo_Corée du Sud http https IPS Created on 2
Page 1 of 1
Displaying



1ère étape : Depuis le réseau A nous mettons en place différentes règles dans la politique de



1ère étape : Depuis le réseau A nous mettons en place différentes règles dans la politique de filtrage numéro 5 :

Trafics internes :

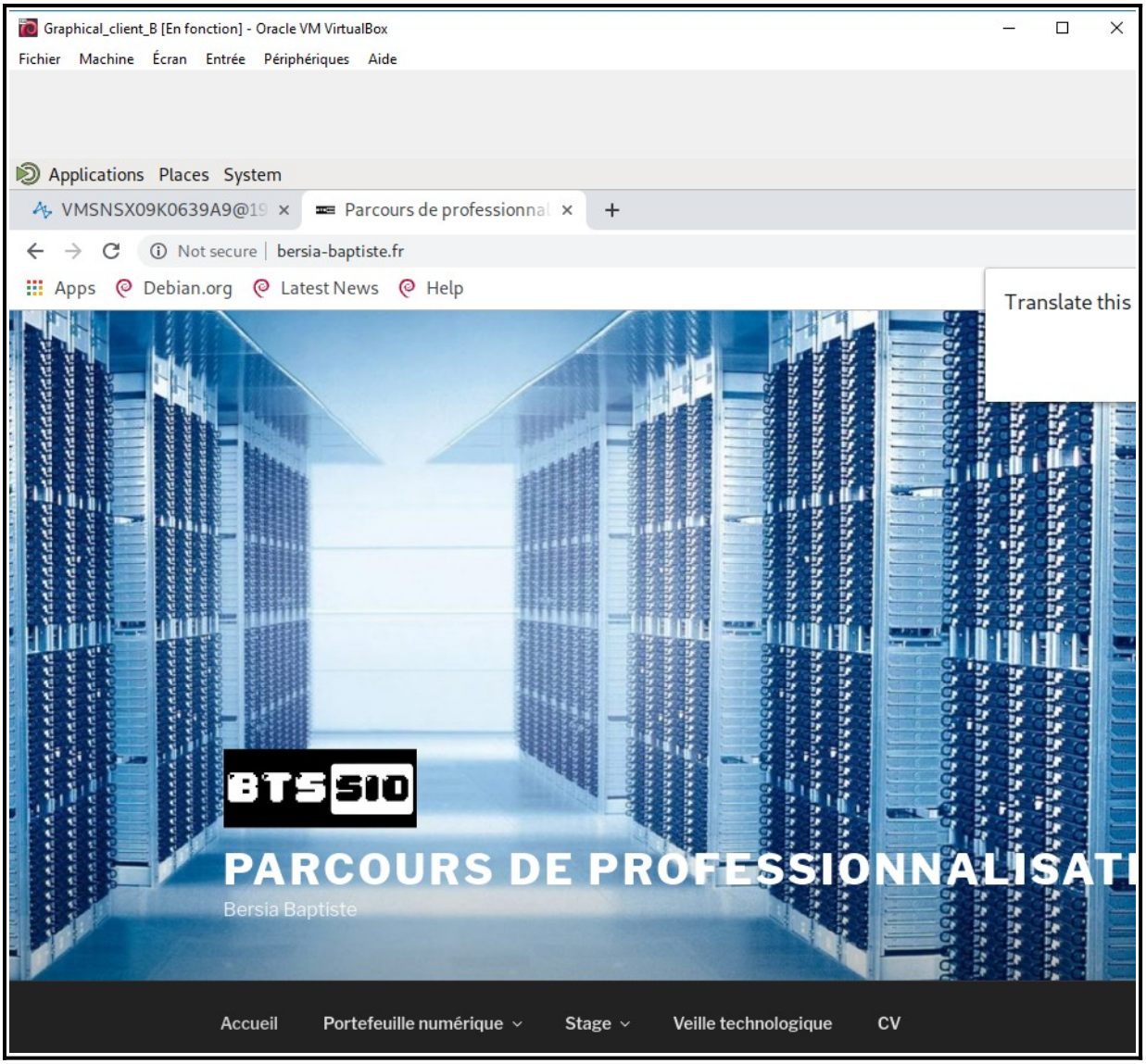
- Accès aux serveurs de notre DMZ (DNS,WEB, FTP, SMTP).

Trafics sortants :

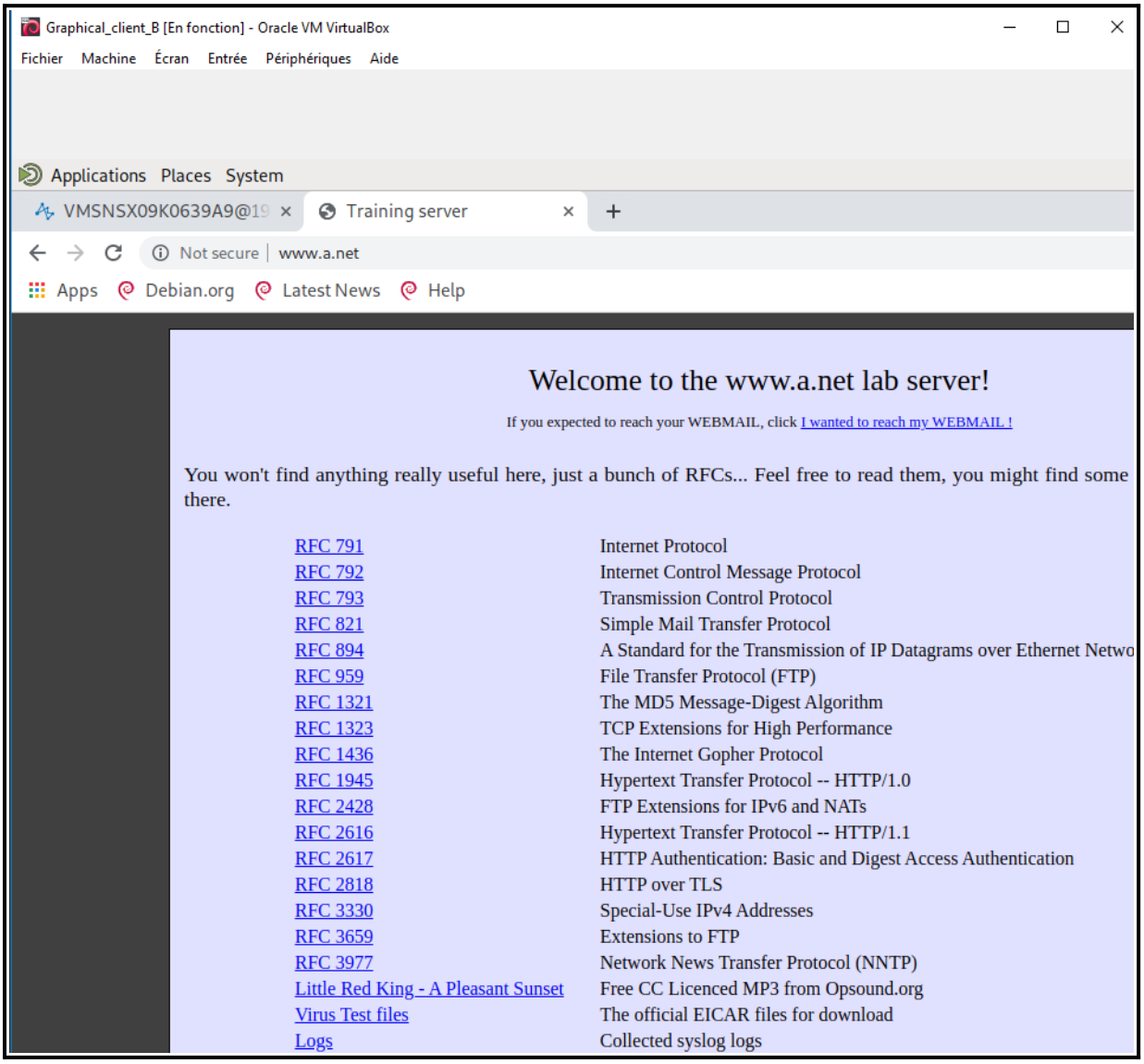
- Accès aux sites web d'internet en HTTP et HTTPS sauf sur les sites de la République de Corée.
- Accès au site ***https://edition.cnn.com*** bloqué.
- Un stagiaire possédant la machine pc_200 doit avoir interdiction d'effectuer une requête FTP.
- Accès aux serveurs FTP et WEB d'internet.
- Autorisation d'émettre un ping vers n'importe quelle destination.
- Accès à la connexion SSH au firewalls des autres sites.
- Seul le serveur DNS interne peut envoyer des requêtes DNS vers l'extérieur.
- Le serveur mail peut envoyer des mails vers n'importe quel serveur mail externe.

Trafics entrants :

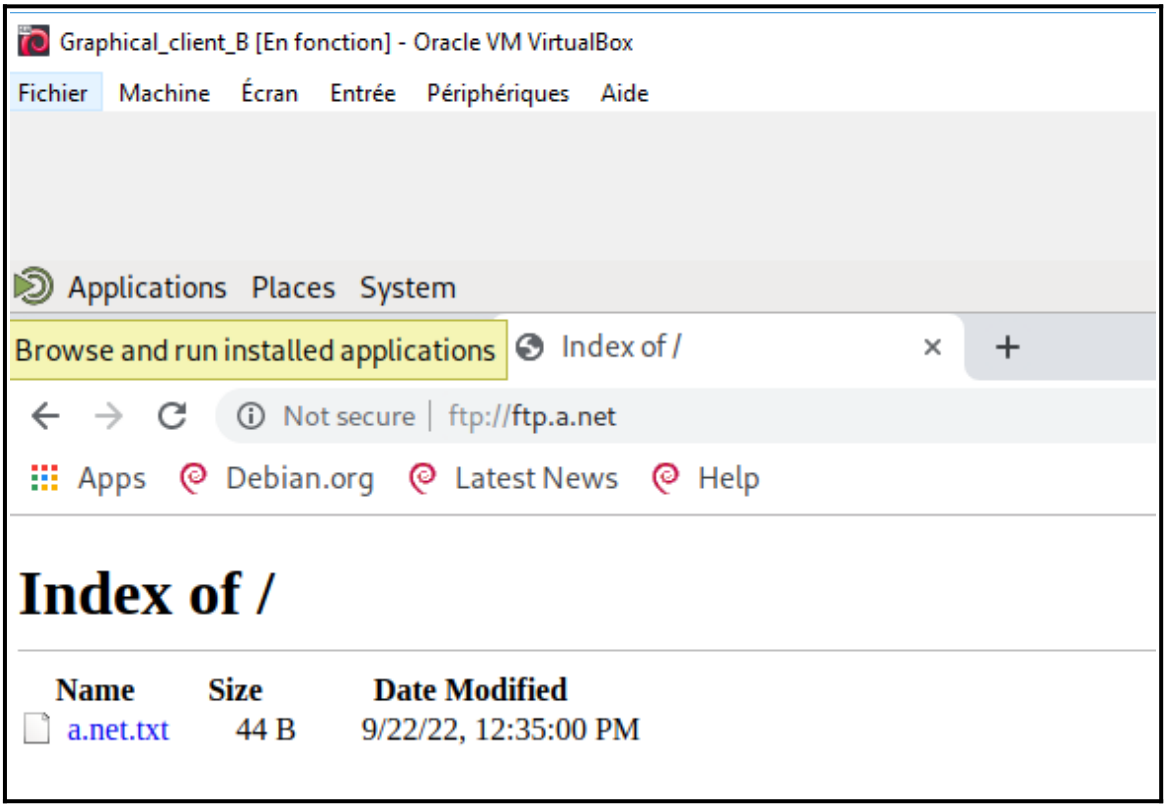
- Accès des réseaux externes à nos serveurs WEB et FTP publique.
- Autorisation des serveurs mail externes à transmettre des e-mails à notre serveur de messagerie.
- Autorisation des réseaux externes à pinger l'interface « out » de notre firewall, événement notifier avec une alarme mineure.
- Autorisation des réseaux externes à se connecter à notre firewall via l'interface web et SSH, événement notifier avec une alarme majeur.



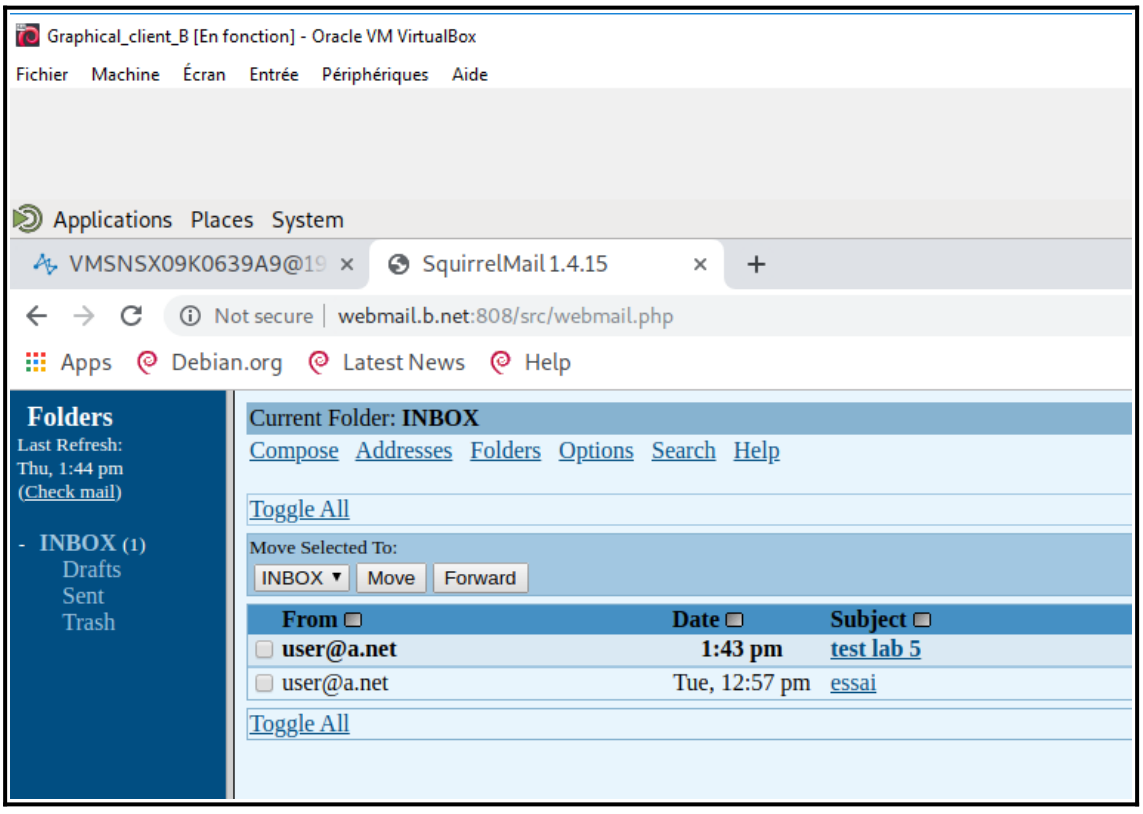
2ème étape : Test accès à un site internet en HTTP.



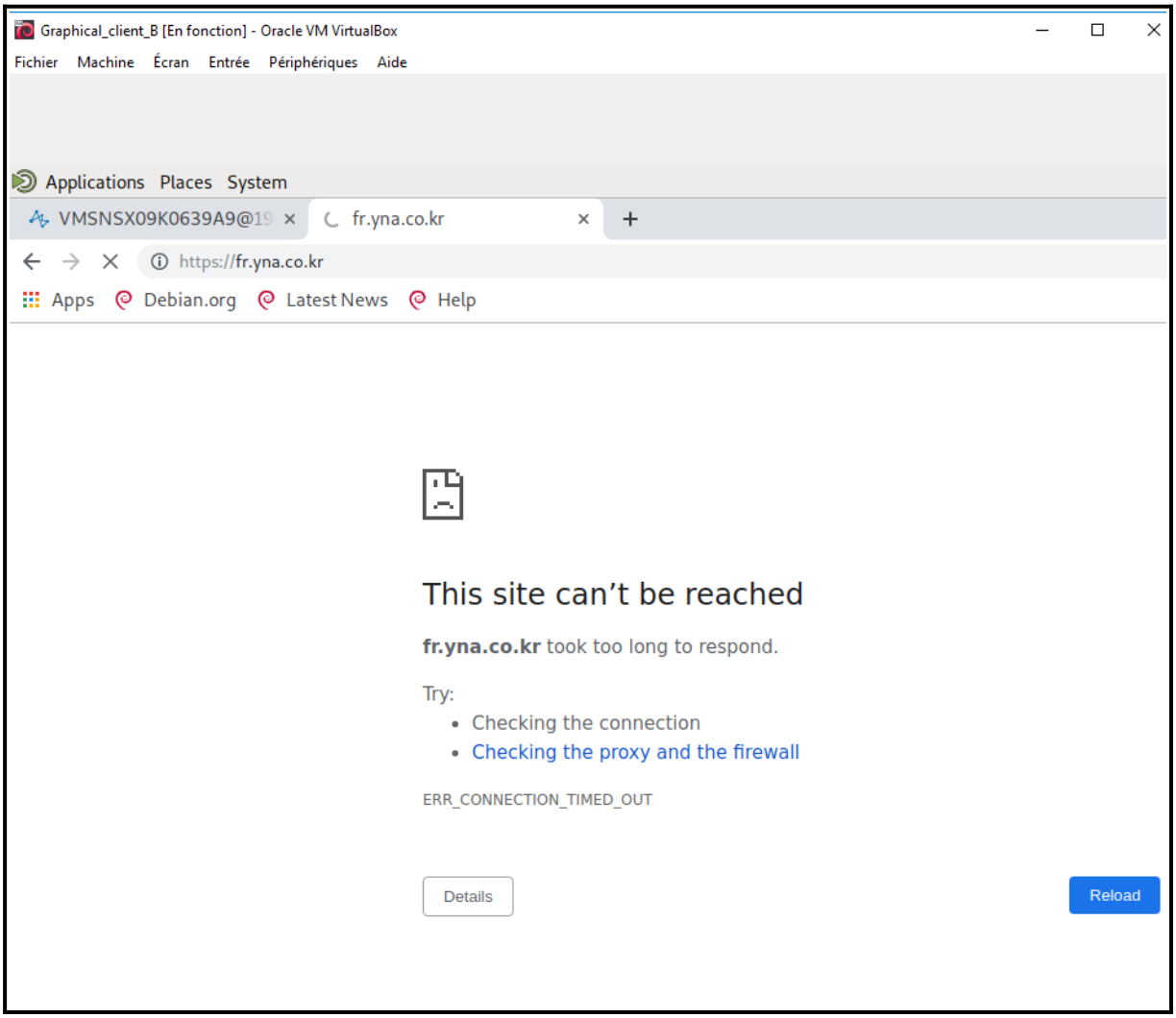
3ème étape : Test accès serveur WEB de B.



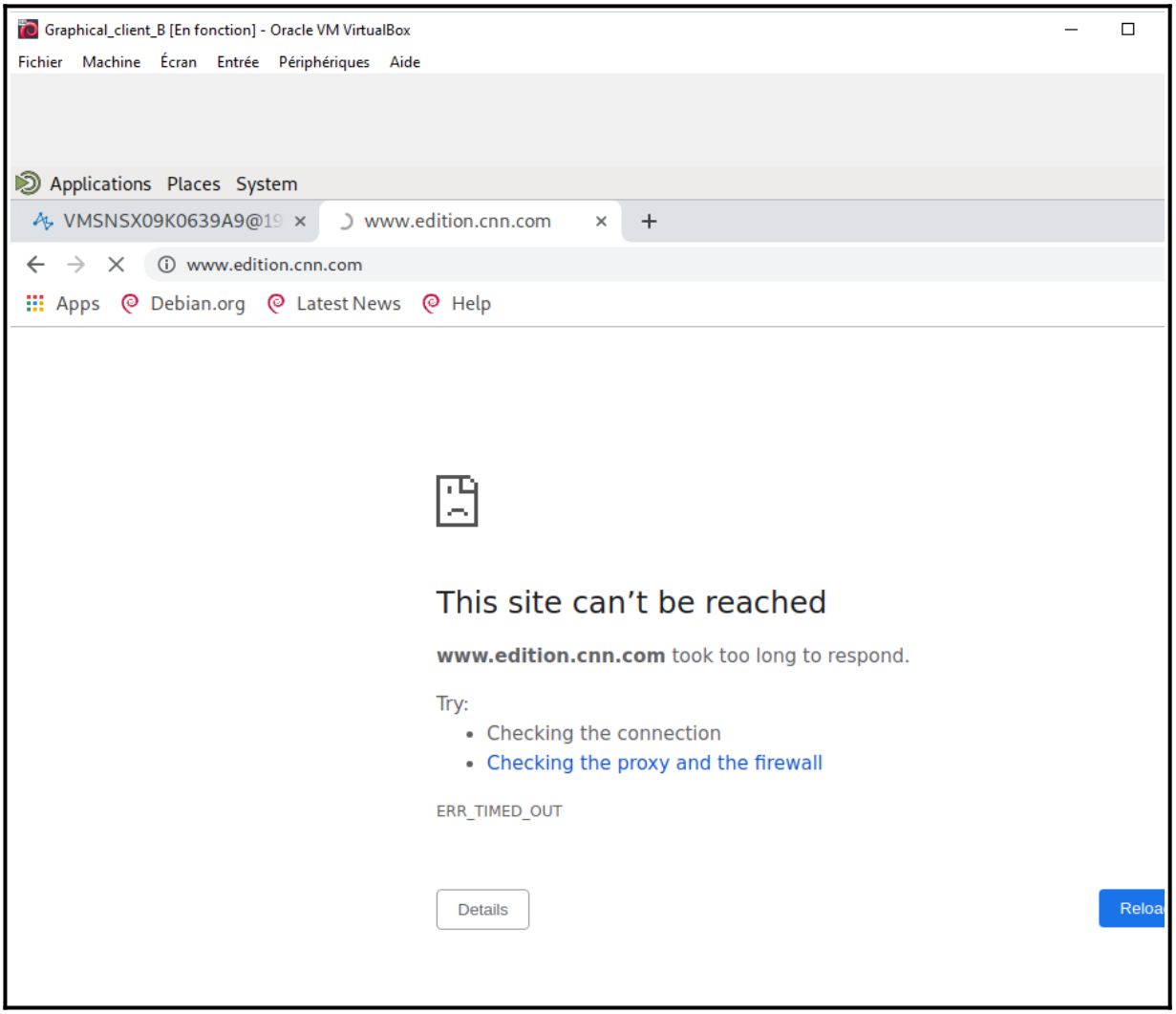
4ème étape: Test accès serveur FTP de A.



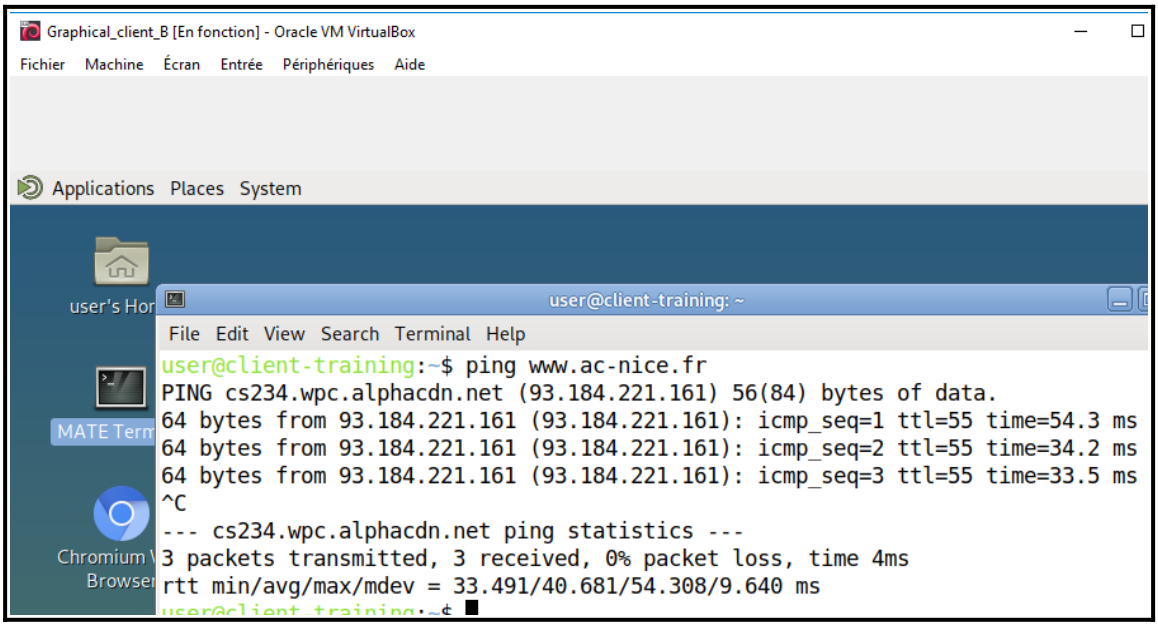
5ème étape : On remarque que B a bien reçu le mail envoyé depuis A.



6ème étape : Tentative de connexion à un site web de la République de Corée. Celui-ci n’est donc pas accessible.



7ème étape : Tentative de connexion au site web edition.cnn. Celui-ci n’est donc pas accessible.



8ème étape : Test d’un ping vers n’importe quelle destination, dans le cas présent ac-nice.fr .