



STORMSHIELD

LAB 5 :
Filtrage



Réseau A :

Graphical_client_A [En fonction] - Oracle VM VirtualBox

Fichier Machine Écran Entrée Périphériques Aide

fr

<https://192.168.1.254/admin/admin.html#securitypolicy/local/5/filter>

Latest News Help

EVA1 VMSNSX09K0639A9

MONITORING CONFIGURATION

SECURITY POLICY / FILTER - NAT

(5) Lab_5 Edit Export

FILTERING NAT

	Status	Action	Source	Destination	Dest. port	Protocol	Security inspection	Comments
1	on	pass	pc_admin	Firewall_in	https	IPS		Created
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
8	on	block	Network_in	Internet	http https	IPS		Created

<https://192.168.1.254/admin/admin.html#securitypolicy/local/5/filter>

Latest News Help

EVA1 VMSNSX09K0639A9

MONITORING CONFIGURATION

SECURITY POLICY / FILTER - NAT

(5) Lab_5 Edit Export

FILTERING NAT

	Status	Action	Source	Destination	Dest. port	Protocol	Security inspection	Comments
9	on	block	Network_in	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
17	on	pass	Internet	Firewall_out	http	IPS		Created
18	on	pass	Internet	srv_ftp_pub	ftp	IPS		Created

The screenshot shows the EVA1 security policy/filter-NAT interface. The top navigation bar includes links for Latest News and Help, and a user account for admin with WRITE / RESTRICTED permissions. The main content area displays a table of security rules. The table has columns for Rule ID, Status, Action, Source, Destination, Dest. port, Protocol, Security inspection, and Community. The rules are categorized into 'FILTERING' and 'NAT'. The 'FILTERING' section contains rules 12 through 16, which allow various protocols (ftp, ssh, dns_udp, smtp) from Network_in to Internet. The 'NAT' section contains rules 17 through 21, which map traffic from Internet to Firewall_out (http, ftp, smtp, https, ssh). The table also includes a section for 'TRAFFIC ENTRANT' (rules 17 to 21).

Rule	Status	Action	Source	Destination	Dest. port	Protocol	Security inspection	Community
12	on	pass	Network_in	Internet	ftp		IPS	Created
13	on	pass	Network_in	* Any	* Any	icmp (Echo request)	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
19	on	pass	Internet	srv_mail_pub	smtp		IPS	Created
20	on	pass	Internet	Firewall_out	* Any	icmp (Echo request)	IPS	Created
21	on	pass	Internet	Firewall_out	https ssh		IPS	Created

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

Trafics internes :

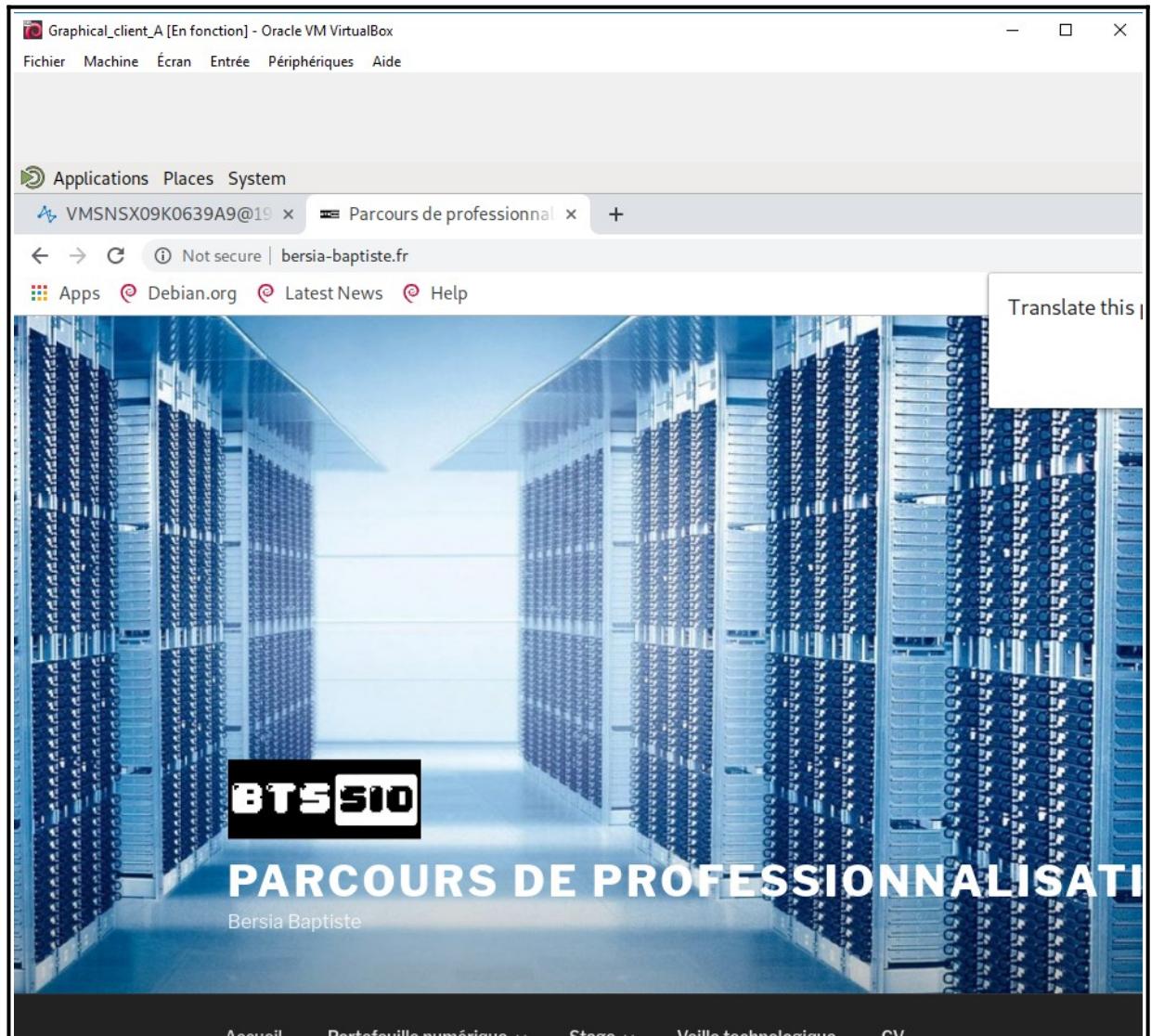
- Accès aux serveurs de notre DMZ (DNS,WEB, FTP, SMTP).

Trafics sortants :

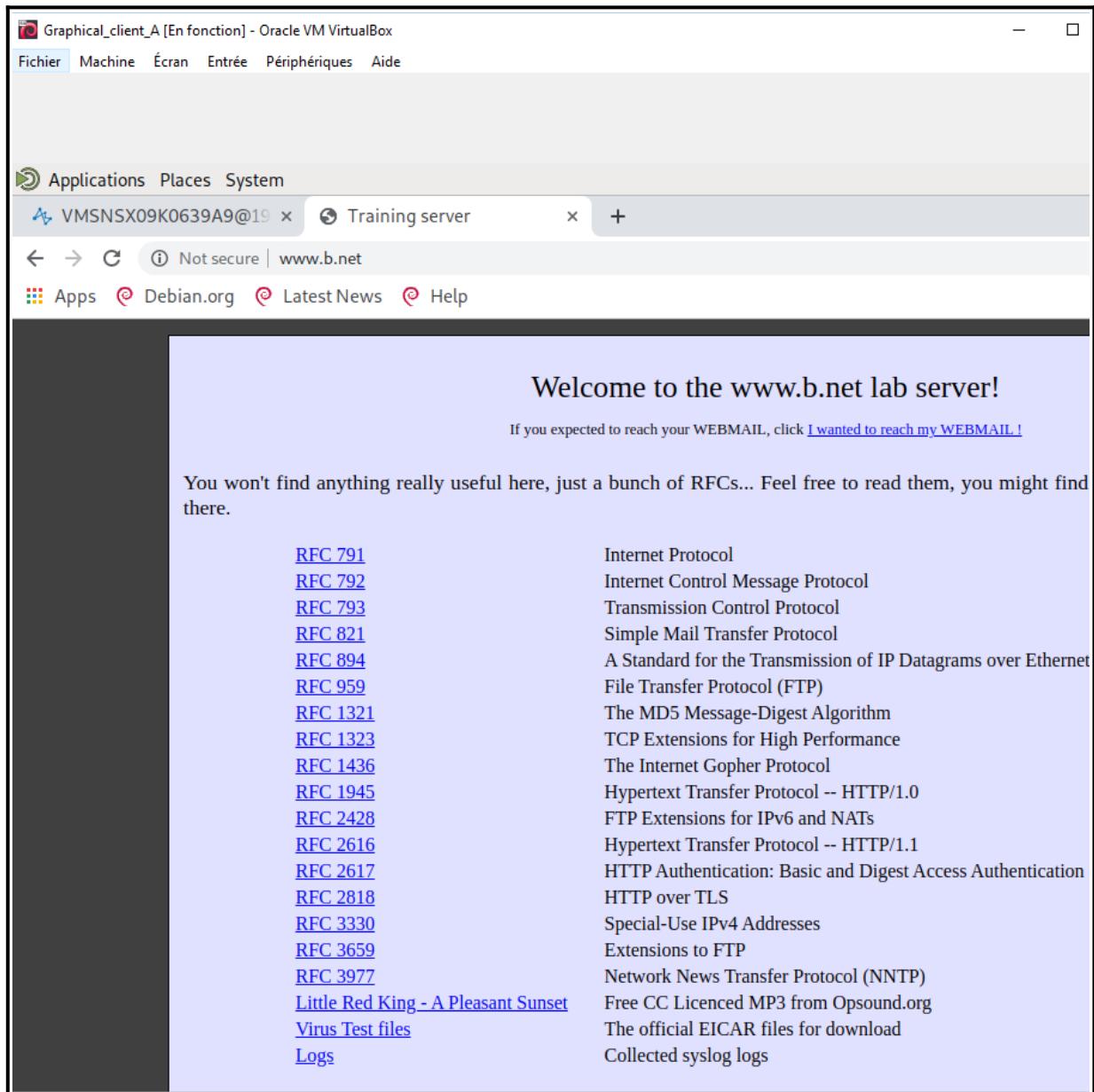
- Accès aux sites web d'internet en HTTP et HTTPS sauf sur les sites de la République de Corée.
- Accès au site <https://edition.cnn.com> bloqué.
- Un stagiaire possédant la machine pc_200 doit avoir interdiction d'effectuer une requête FTP.
- Accès aux serveurs FTP et WEB d'internet.
- Autorisation 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 :

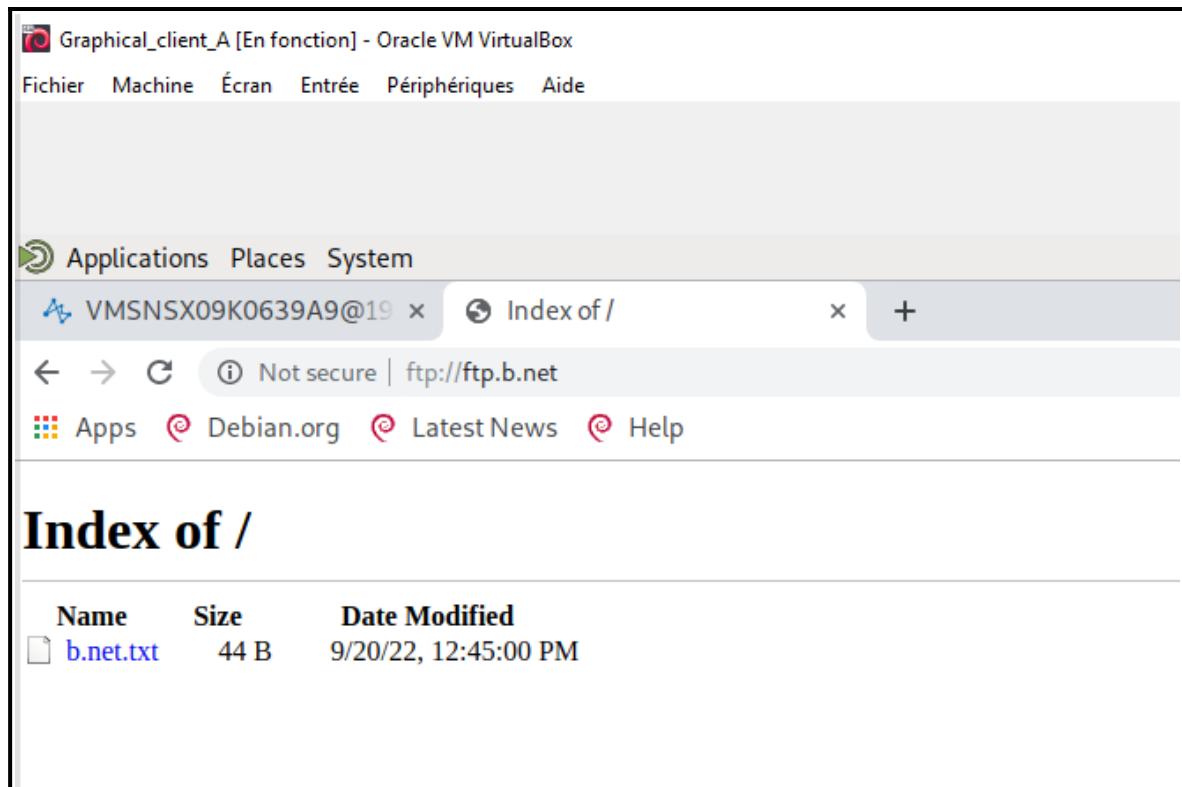
- Accès des réseaux externes à nos serveurs WEB et FTP publique.
- Autorisation des serveurs mail externes à transmettre des e-mails à notre serveur de messagerie.
- Autorisation des réseaux externes à pinger l'interface « out » de notre firewall, événement notifier avec une alarme mineure.
- Autorisation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



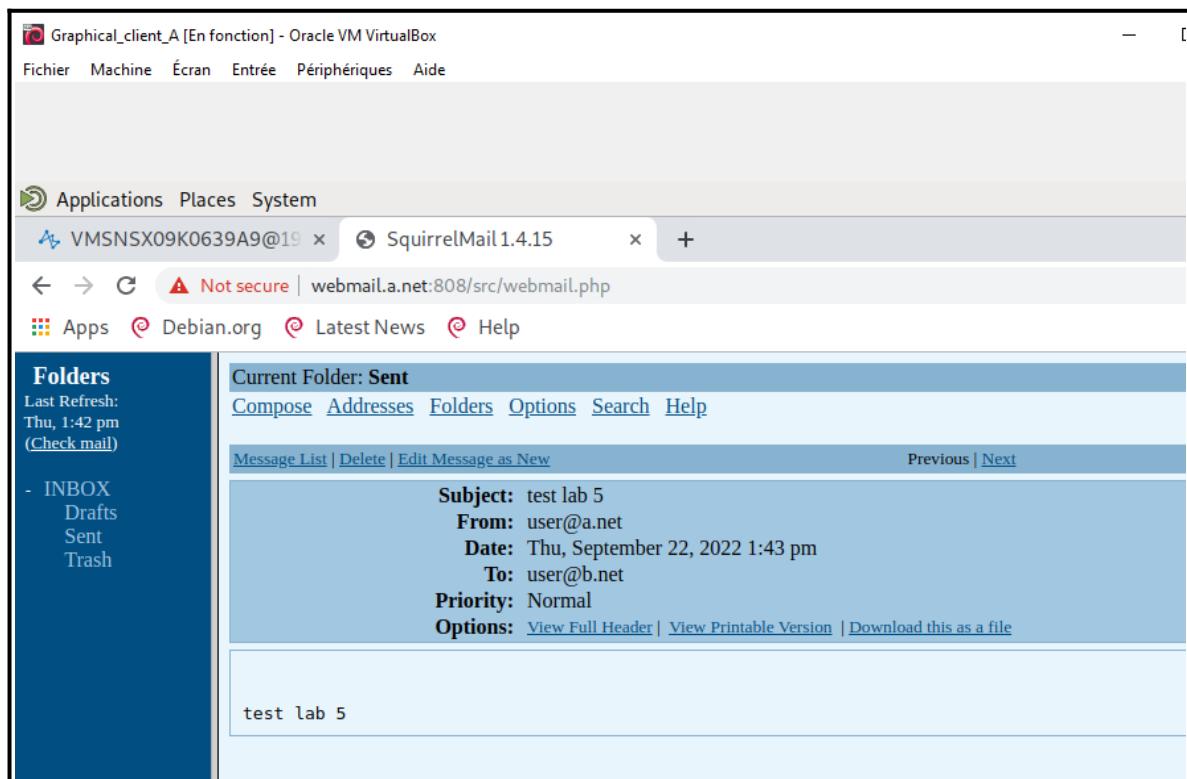
2ème étape : Test accès à un site internet en HTTP.



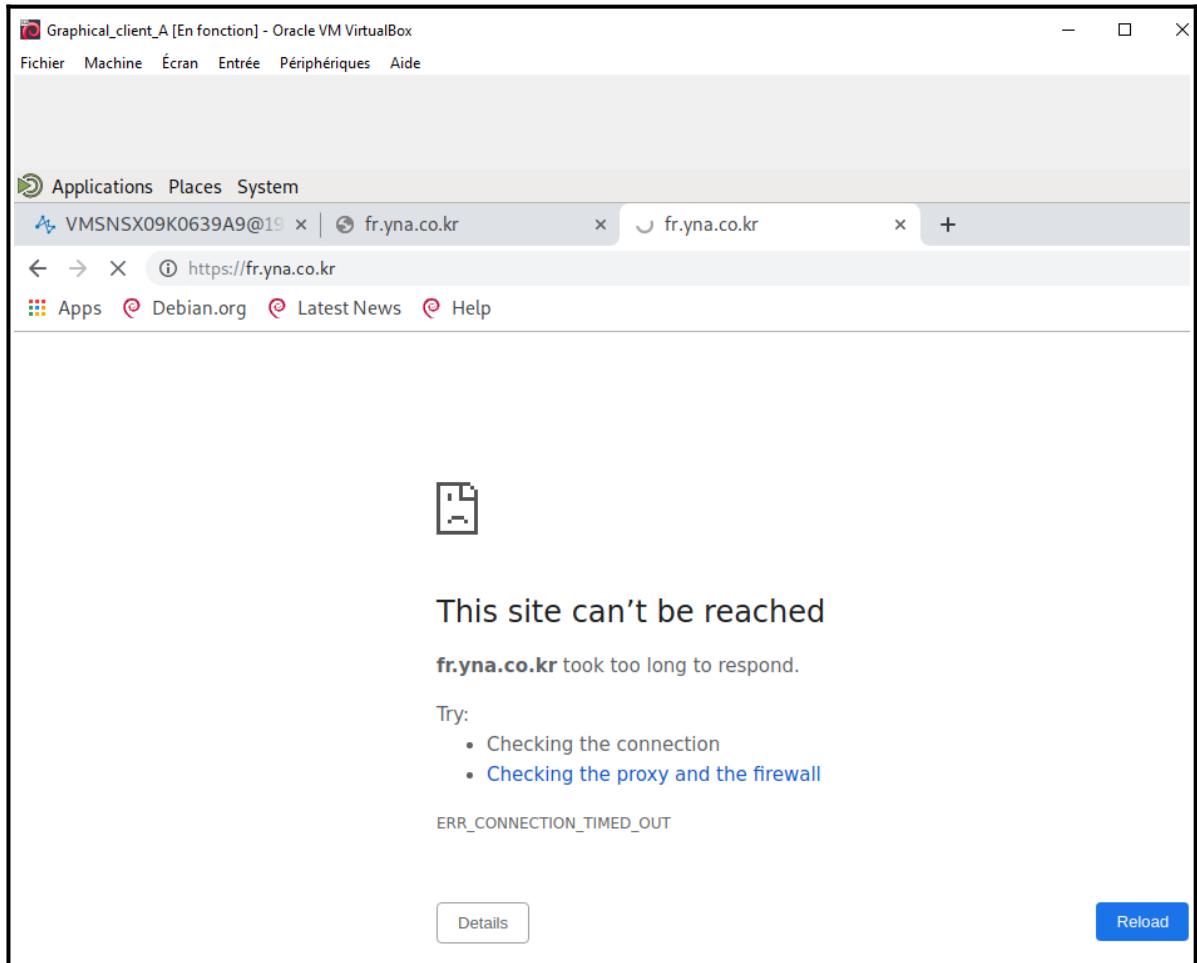
3ème étape : Test accès serveur WEB de B.



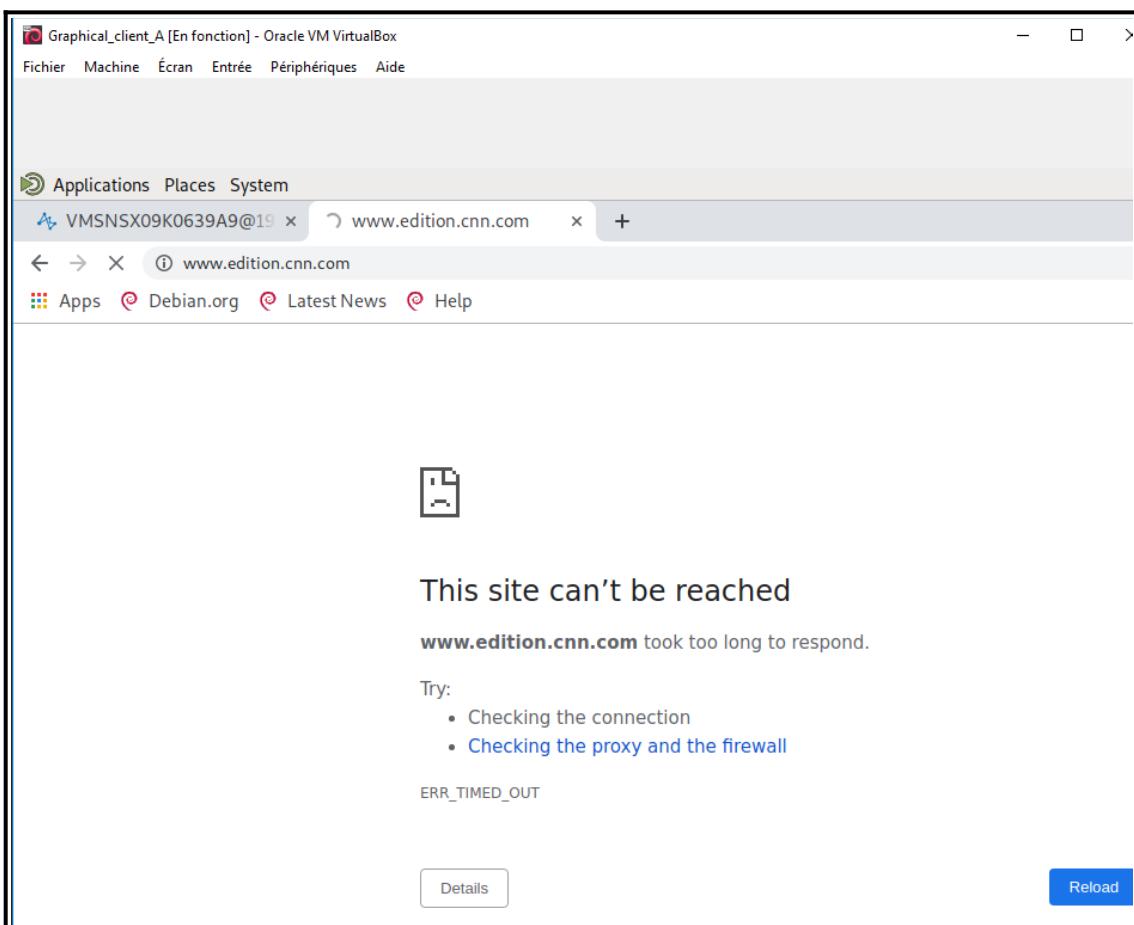
4ème étape: Test accès serveur FTP de B.



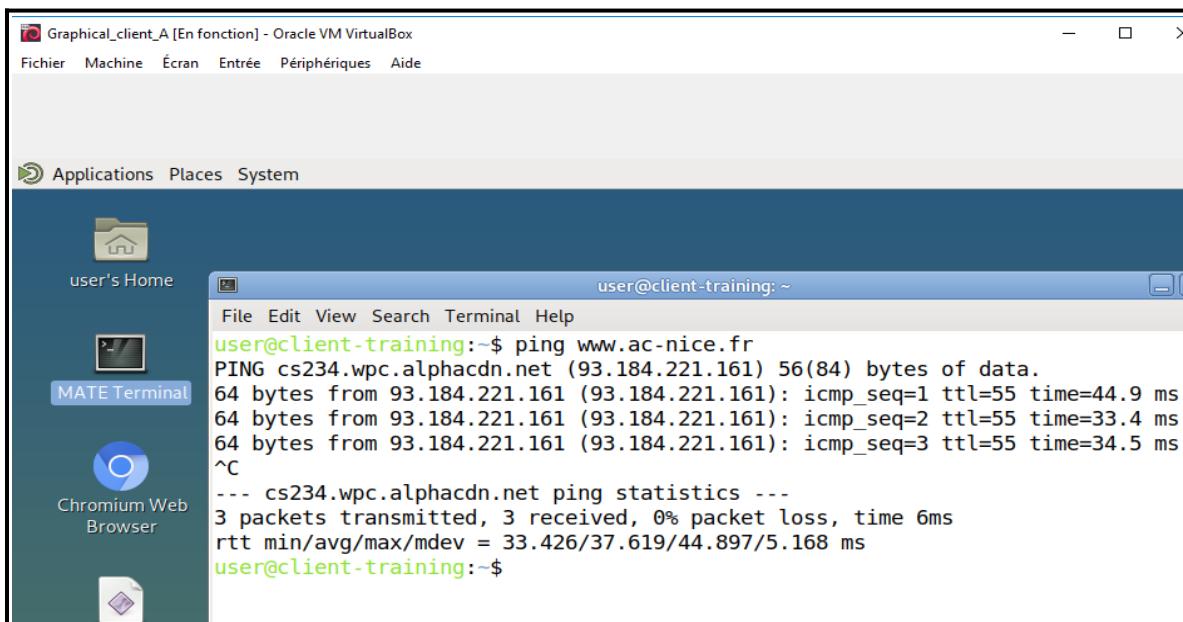
5ème étape : Test envoie d'un mail à B depuis la webmail de A.



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

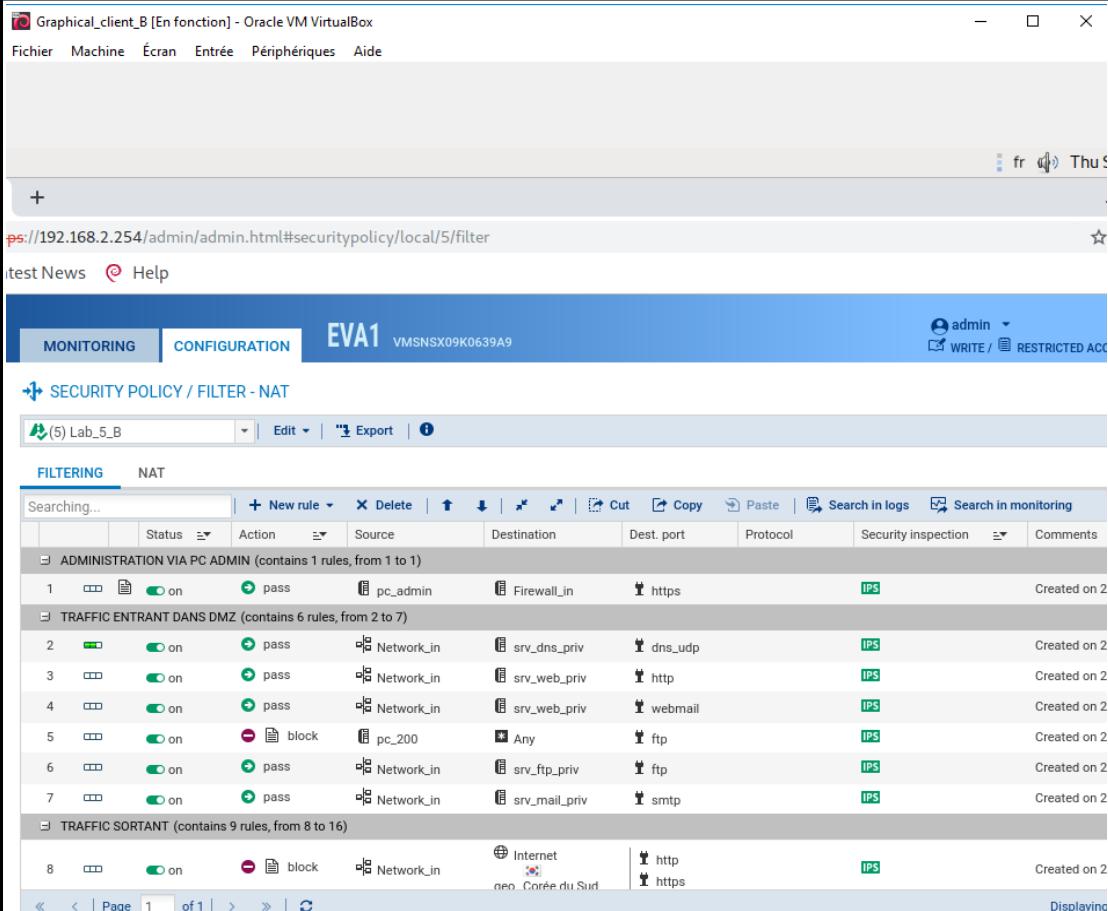


7ème étape : Tentative de connexion au site web edition.cnn. Celui-ci n'est donc pas accessible.



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

Réseau B :



The screenshot shows the EVA1 security policy configuration interface for a NAT rule. The interface includes a header with tabs for MONITORING and CONFIGURATION, and a sub-header for SECURITY POLICY / FILTER - NAT. The main area displays a table of 16 NAT rules, grouped into sections: ADMINISTRATION VIA PC ADMIN (1 rule), TRAFFIC ENTRANT DANS DMZ (6 rules), and TRAFFIC SORTANT (9 rules). The table columns include Status, Action, Source, Destination, Dest. port, Protocol, Security inspection, and Comments. Rule 8 is highlighted, showing it blocks traffic from the Internet (geo. Corée du Sud) to ports 80 and 443. The interface also features a toolbar with buttons for New rule, Delete, Copy, Paste, and search functions.

	Status	Action	Source	Destination	Dest. port	Protocol	Security inspection	Comments
1	on	pass	pc_admin	Firewall_in	https	IPS		Created on 2
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
8	on	block	Network_in	Internet geo. Corée du Sud	http https	IPS		Created on 2

The screenshot shows the EVA1 security policy configuration interface. The top navigation bar includes 'Fichier', 'Machine', 'Écran', 'Entrée', 'Périphériques', 'Aide', and a language switch to 'fr'. The main title is 'Graphical_client_B [En fonction] - Oracle VM VirtualBox'. The interface is in French. The top right shows the user 'admin' with 'WRITE / RESTRICTED ACCESS' permissions. The main content area is titled 'SECURITY POLICY / FILTER - NAT' and shows a table of filtering rules. The table has columns for Rule ID, Status, Action, Source, Destination, Dest. port, Protocol, Security inspection, and Comments. The table shows 18 rules, with rule 13 highlighted in yellow. The rules include various actions like 'block', 'pass', and specific protocols like 'http', 'https', 'ftp', 'ssh', 'dns_udp', and 'smtp'. The last row shows a summary for 'TRAFFIC ENTRANT (contains 5 rules, from 17 to 21)'.

Rule	Status	Action	Source	Destination	Dest. port	Protocol	Security inspection	Comments
9	on	block	Network_in	www.edition.cnn.com	http, https	IPS		Created on 2023-09-11
10	on	pass	Network_in	Internet	http	IPS		Created on 2023-09-11
11	on	pass	Network_in	Internet	https	IPS		Created on 2023-09-11
12	on	pass	Network_in	Internet	ftp	IPS		Created on 2023-09-11
13	on	pass	Network_in	Any	Any	icmp (Echo request)	IPS	Created on 2023-09-11
14	on	pass	Network_in	Internet	ssh	IPS		Created on 2023-09-11
15	on	pass	srv_dns_priv	Internet	dns_udp	IPS		Created on 2023-09-11
16	on	pass	srv_mail_priv	Internet	smtp	IPS		Created on 2023-09-11
TRAFFIC ENTRANT (contains 5 rules, from 17 to 21)								
17	on	pass	Internet	Firewall_out	http	IPS		Created on 2023-09-11
18	on	pass	Internet	srv_ftp_pub	ftp	IPS		Created on 2023-09-11

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

Rule	Status	Action	Source	Destination	Dest. port	Protocol	Security inspection	Comments
12	on	pass	Network_in	Internet	ftp		IPS	Created on 20
13	on	pass	Network_in	Any	Any	icmp	(Echo request)	Created on 20
14	on	pass	Network_in	Internet	ssh		IPS	Created on 20
15	on	pass	srv_dns_priv	Internet	dns_udp		IPS	Created on 20
16	on	pass	srv_mail_priv	Internet	smtp		IPS	Created on 20
TRAFFIC ENTRANT (contains 5 rules, from 17 to 21)								
17	on	pass	Internet	Firewall_out	http		IPS	Created on 20
18	on	pass	Internet	srv_ftp_pub	ftp		IPS	Created on 20
19	on	pass	Internet	srv_mail_pub	smtp		IPS	Created on 20
20	on	pass	Internet	Firewall_out	Any	icmp	(Echo request)	Created on 20
21	on	pass	Internet	Firewall_out	https		IPS	Created on 20
ssh								

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

Trafics internes :

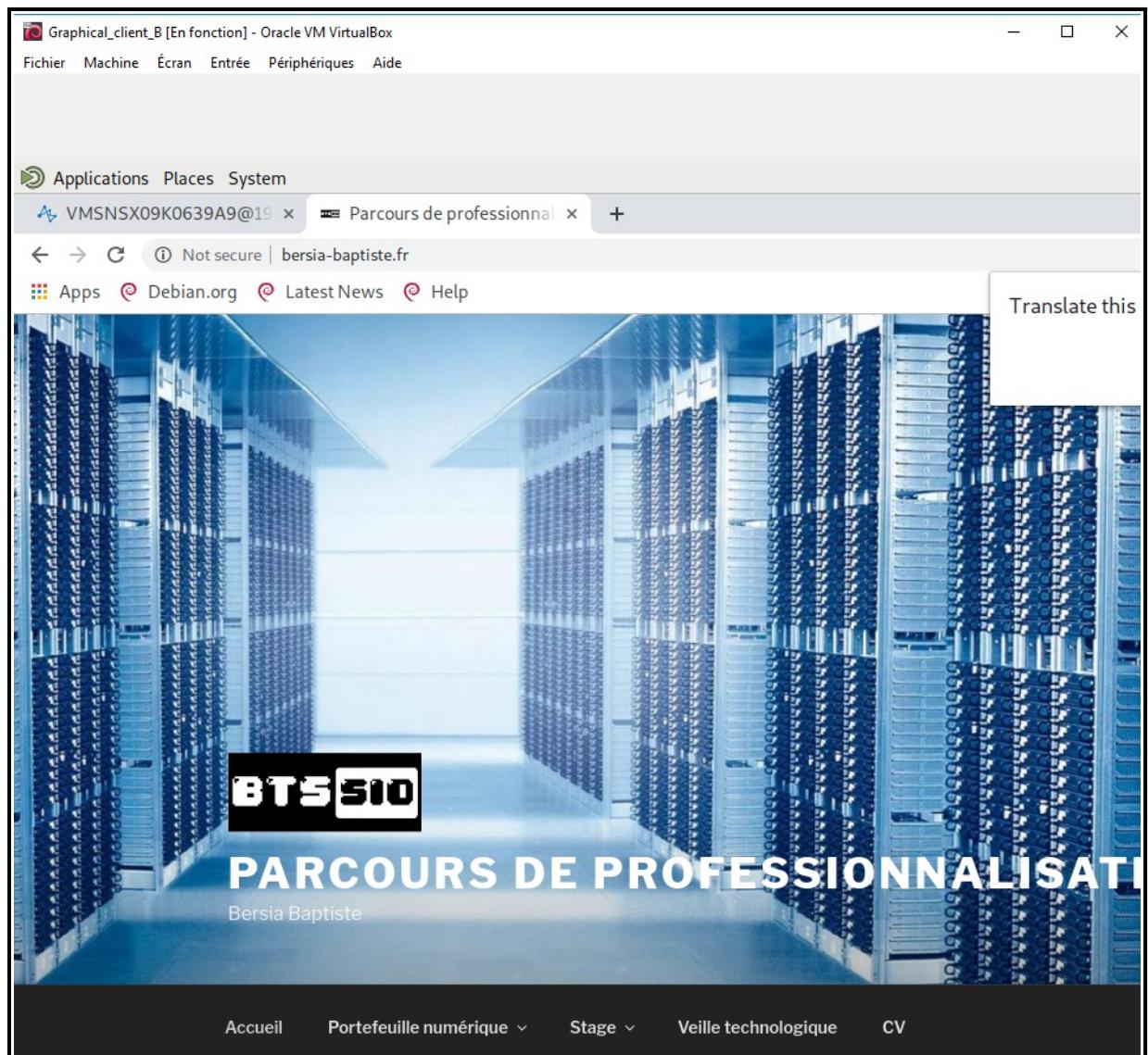
- Accès aux serveurs de notre DMZ (DNS,WEB, FTP, SMTP).

Trafics sortants :

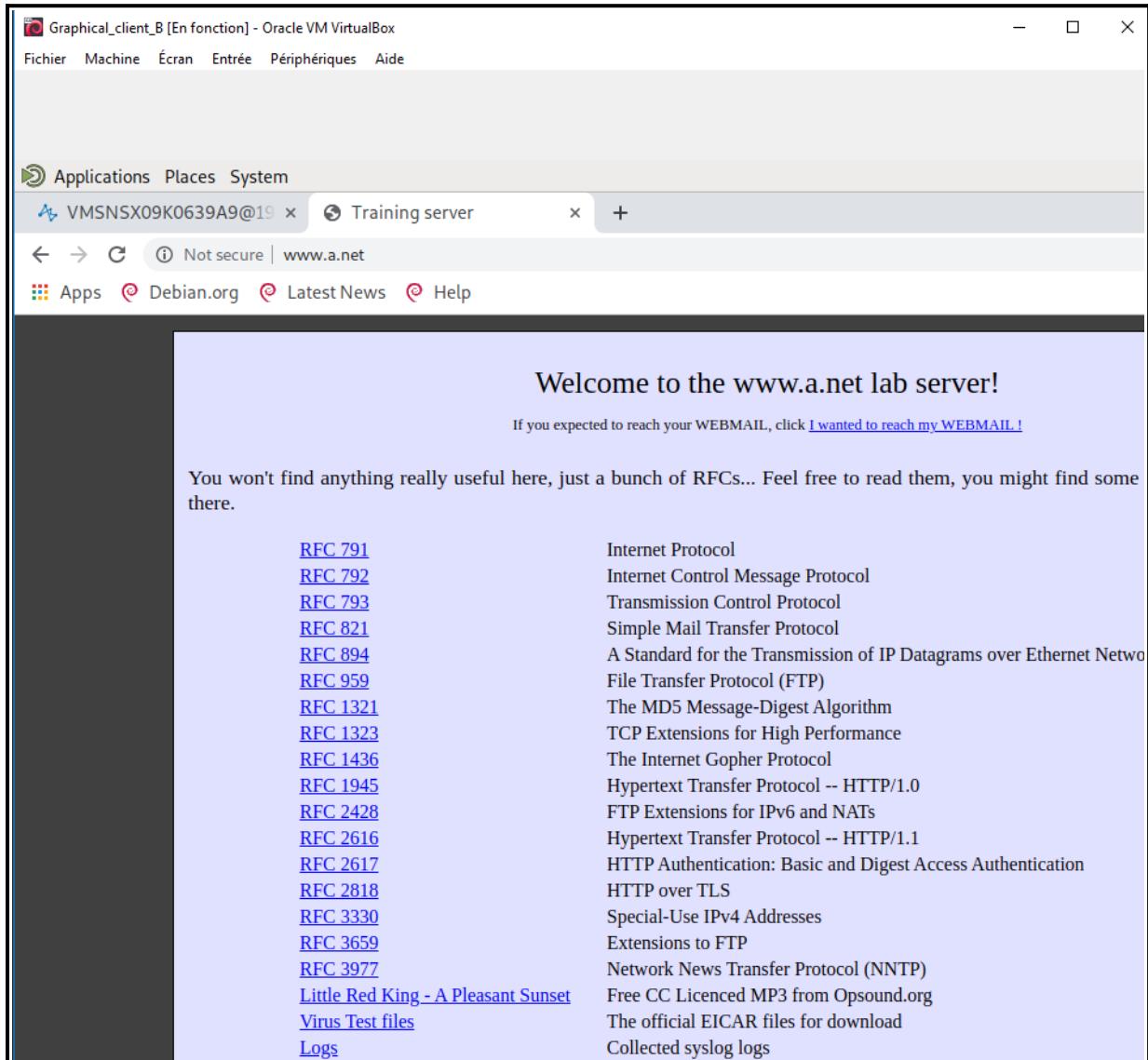
- Accès aux sites web d'internet en HTTP et HTTPS sauf sur les sites de la République de Corée.
- Accès au site <https://edition.cnn.com> bloqué.
- Un stagiaire possédant la machine pc_200 doit avoir interdiction d'effectuer une requête FTP.
- Accès aux serveurs FTP et WEB d'internet.
- Autorisation 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.

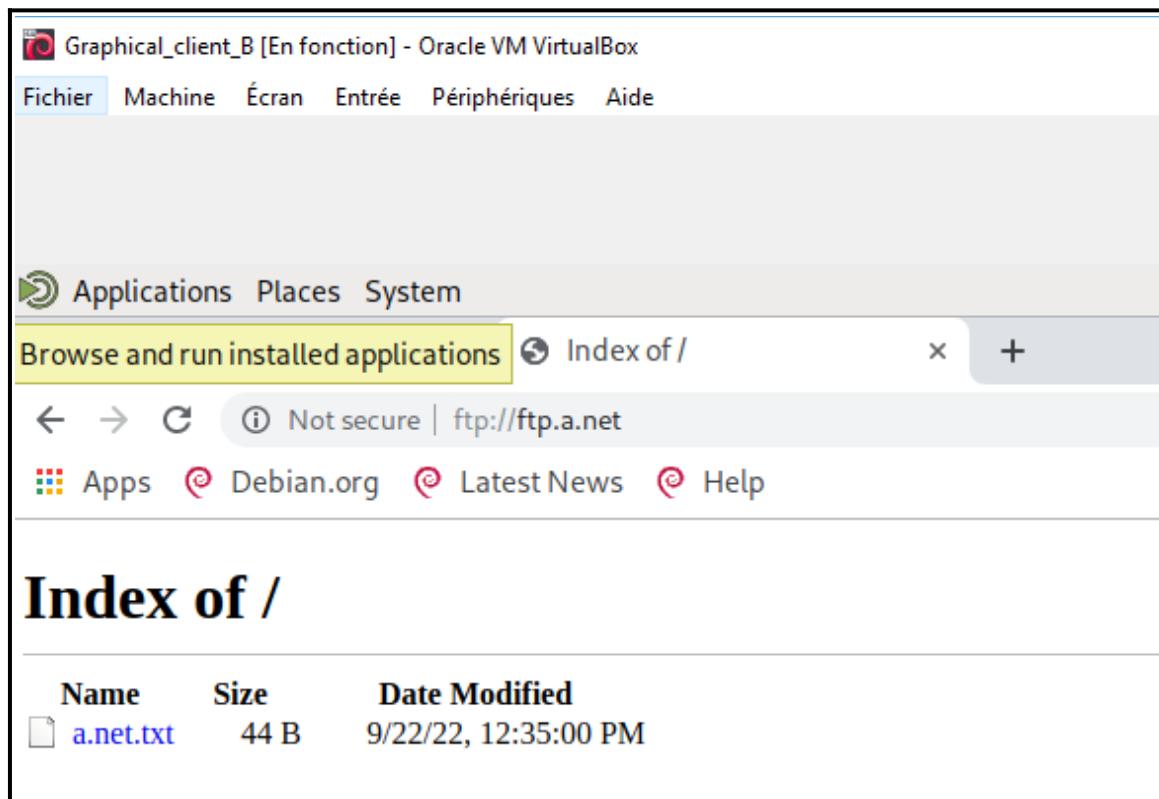


2ème étape : Test accès à un site internet en HTTP.

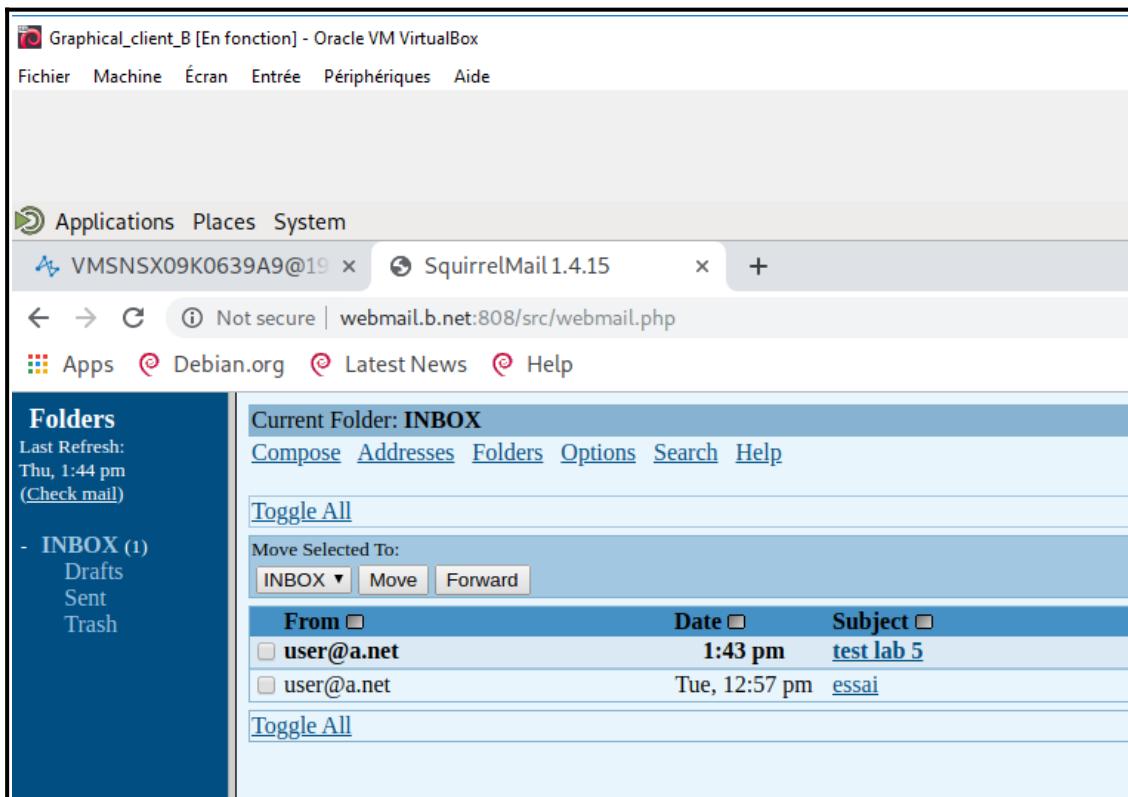


RFC 791	Internet Protocol
RFC 792	Internet Control Message Protocol
RFC 793	Transmission Control Protocol
RFC 821	Simple Mail Transfer Protocol
RFC 894	A Standard for the Transmission of IP Datagrams over Ethernet Networks
RFC 959	File Transfer Protocol (FTP)
RFC 1321	The MD5 Message-Digest Algorithm
RFC 1323	TCP Extensions for High Performance
RFC 1436	The Internet Gopher Protocol
RFC 1945	Hypertext Transfer Protocol -- HTTP/1.0
RFC 2428	FTP Extensions for IPv6 and NATs
RFC 2616	Hypertext Transfer Protocol -- HTTP/1.1
RFC 2617	HTTP Authentication: Basic and Digest Access Authentication
RFC 2818	HTTP over TLS
RFC 3330	Special-Use IPv4 Addresses
RFC 3659	Extensions to FTP
RFC 3977	Network News Transfer Protocol (NNTP)
Little Red King - A Pleasant Sunset	Free CC Licensed MP3 from Opsound.org
Virus Test files	The official EICAR files for download
Logs	Collected syslog logs

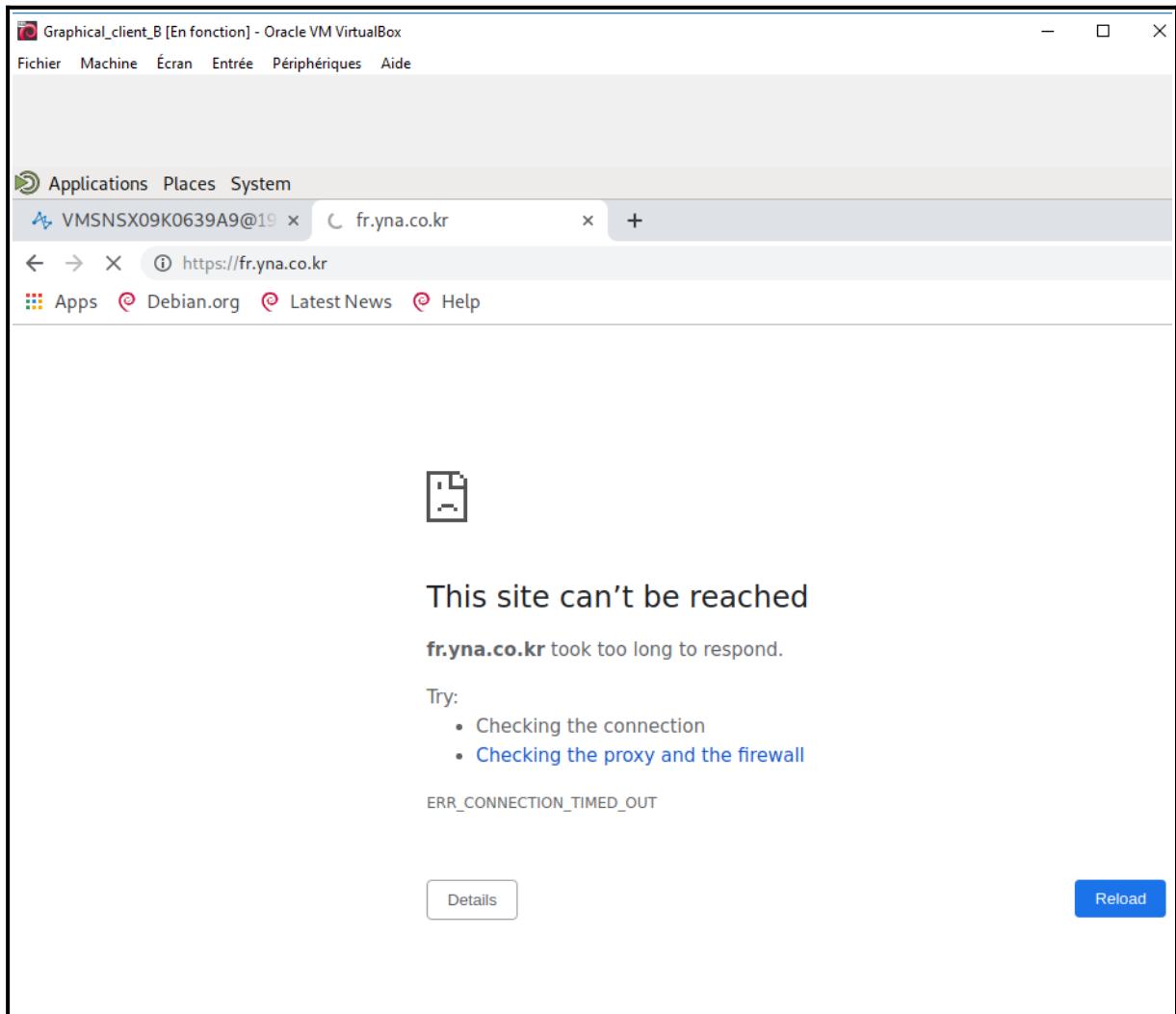
3ème étape : Test accès serveur WEB de B.



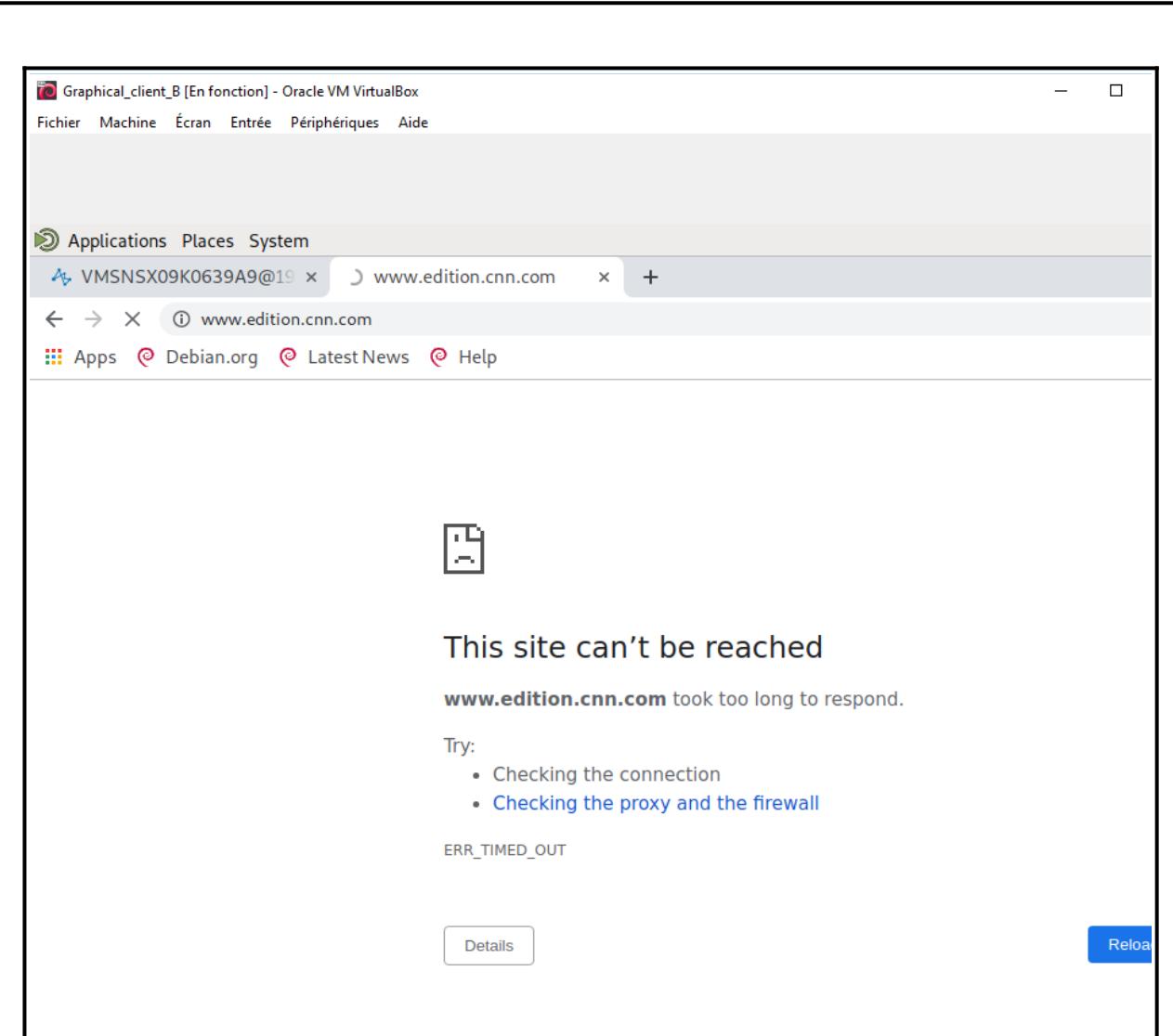
4ème étape: Test accès serveur FTP de A.



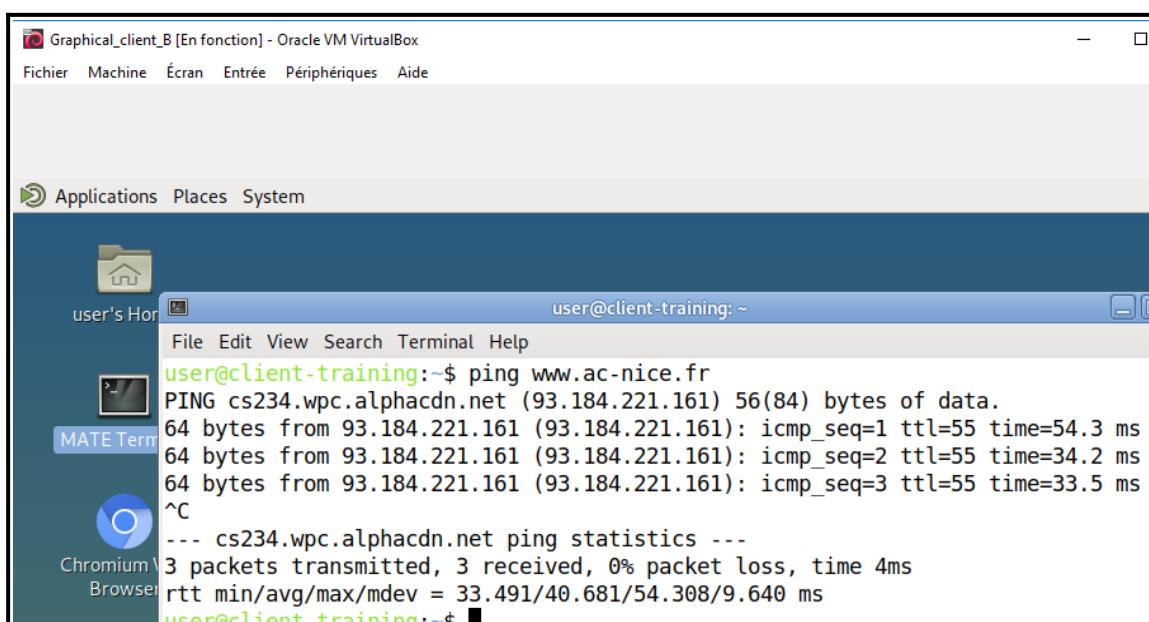
5ème étape : On remarque que B a bien reçu le mail envoyé depuis A.



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 .