



**STORMSHIELD**

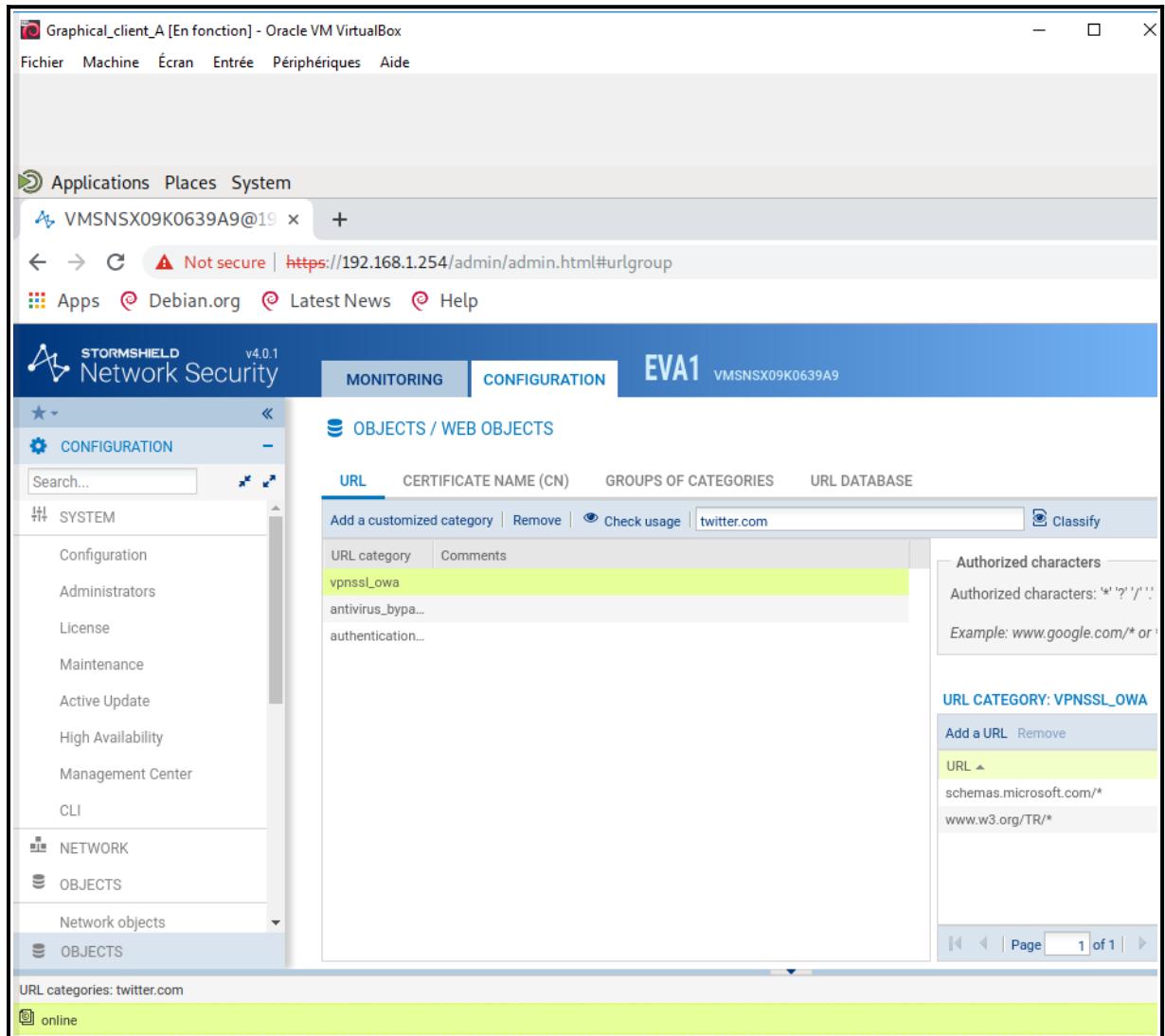
**LAB 6 :**  
**Filtrage de contenu**

## Réseau A :

The screenshot shows a web browser window titled "Graphical\_client\_A [En fonction] - Oracle VM VirtualBox". The address bar displays "VMSNSX09K0639A9@192.168.1.254/admin/admin.html#urlgroup". The page content is the "OBJECTS / WEB OBJECTS" section of the STORMSHIELD Network Security v4.0.1 configuration interface. The top navigation bar includes "MONITORING" and "CONFIGURATION" tabs, with "EVA1 VMSNSX09K0639A9" selected. The left sidebar shows a tree view with "SYSTEM", "NETWORK", "OBJECTS", and "OBJECTS" expanded, with "Network objects" selected. The main table lists categories and their comments:

URL	CERTIFICATE NAME (CN)	GROUPS OF CATEGORIES	URL DATABASE
URL database provider : Embedded URL database			
<b>Embedded URL database</b>			
Category	Comments		
academic	Université et Enseignement Supérieur		
ads	Publicité		
arts	Arts		
bank	Institutions financières		
business	Commerce et Finances		
employment	Emploi		
entertainment	Culture et Loisirs		
illegal	Contenu illicite		
it	Informatique		
news	Nouvelles et Information		
online	Jeux en ligne, Paris, Radios, Réseaux Sociaux et Partage de Fichiers		

**1ère étape :** Nous sélectionnons la base d'URL embarquée dans les objets WEB.



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

Fichier Machine Écran Entrée Périphériques Aide

Applications Places System

VMSNSX09K0639A9@19 Hôte injoignable | Hôte injoignable +

Not secure | https://192.168.1.254/admin/admin.html#urlgroup

Apps Debian.org Latest News Help

STORMSHIELD Network Security v4.0.1

MONITORING CONFIGURATION EVA1 VMSNSX09K0639A9

OBJETS / OBJETS WEB

URL	NOM DE CERTIFICAT (CN)	GROUPE DE CATÉGORIES	BASE D'URL
Ajouter une catégorie personnalisée	Supprimer	Vérifier l'utilisation	home.barclays
Catégorie d'URL	Commentaire		
vpnssl_owa			
antivirus_bypa...			
authentication...			

Caractères autorisés

Les caractères autorisés s

Exemple d'URL : www.goog

CATÉGORIE D'URL : VPNSS

Ajouter une URL Supprimer

URL

schemas.microsoft.com/\*

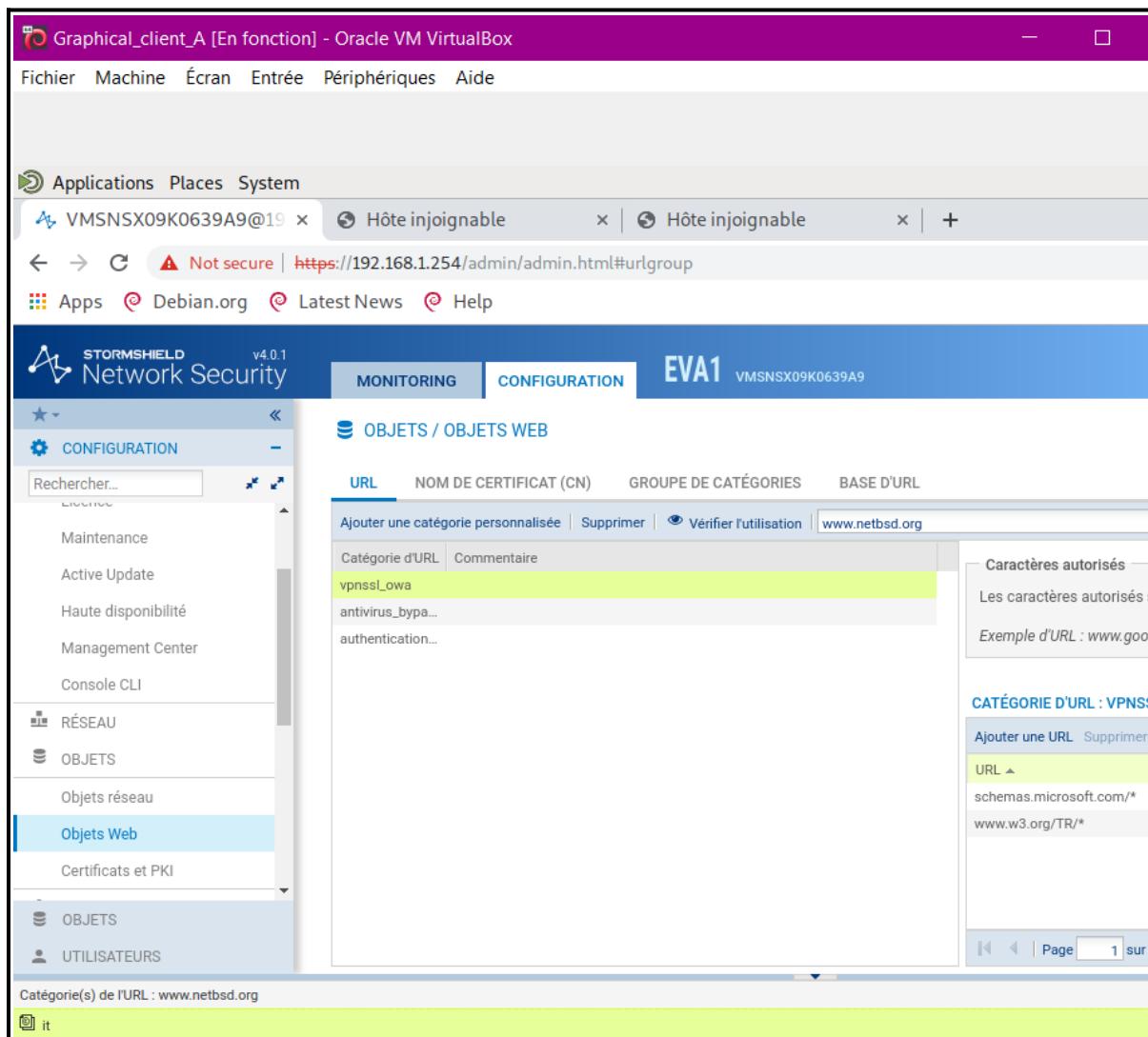
www.w3.org/TR/\*

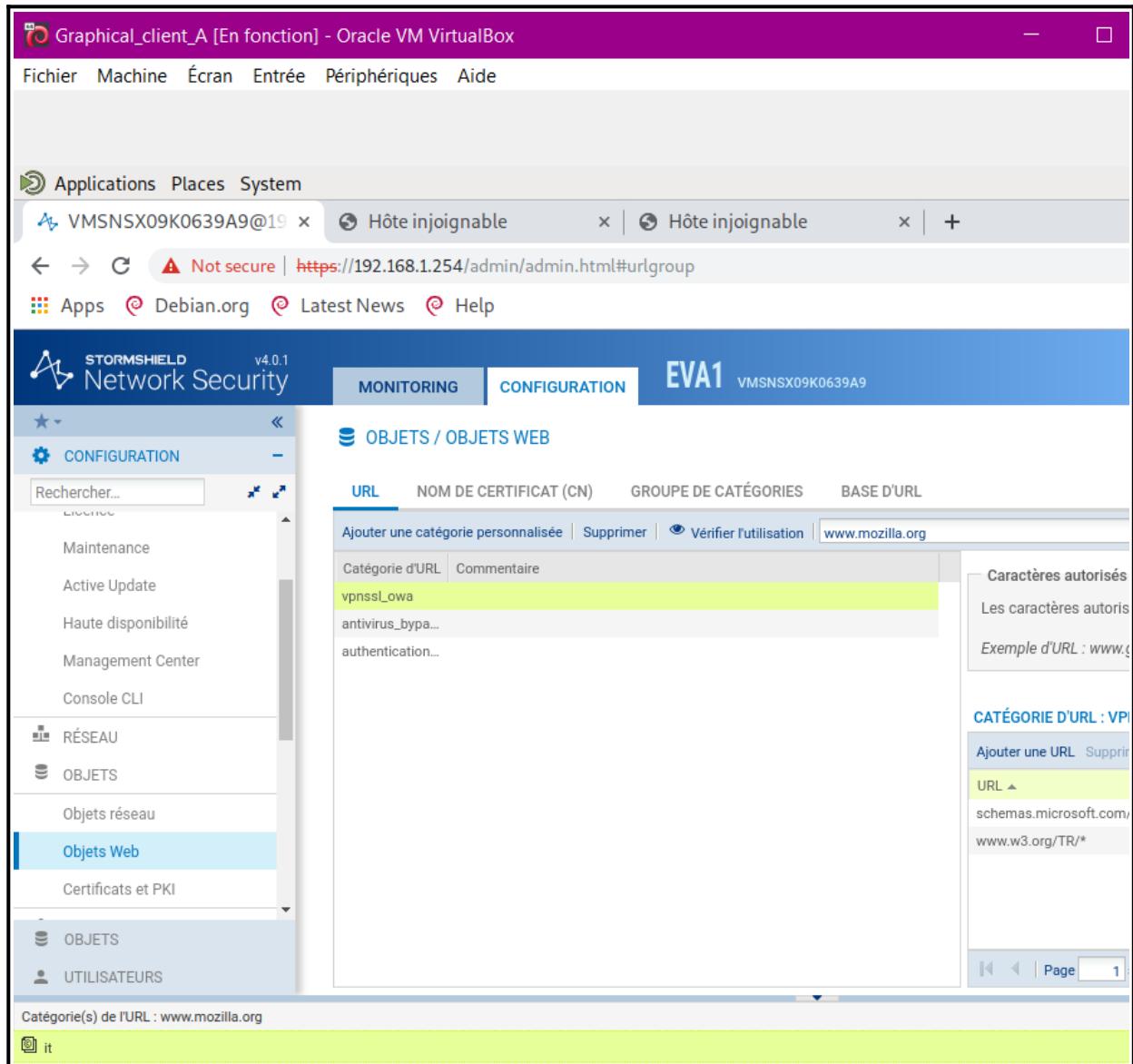
Page 1 sur 1

Catégorie(s) de l'URL : home.barclays

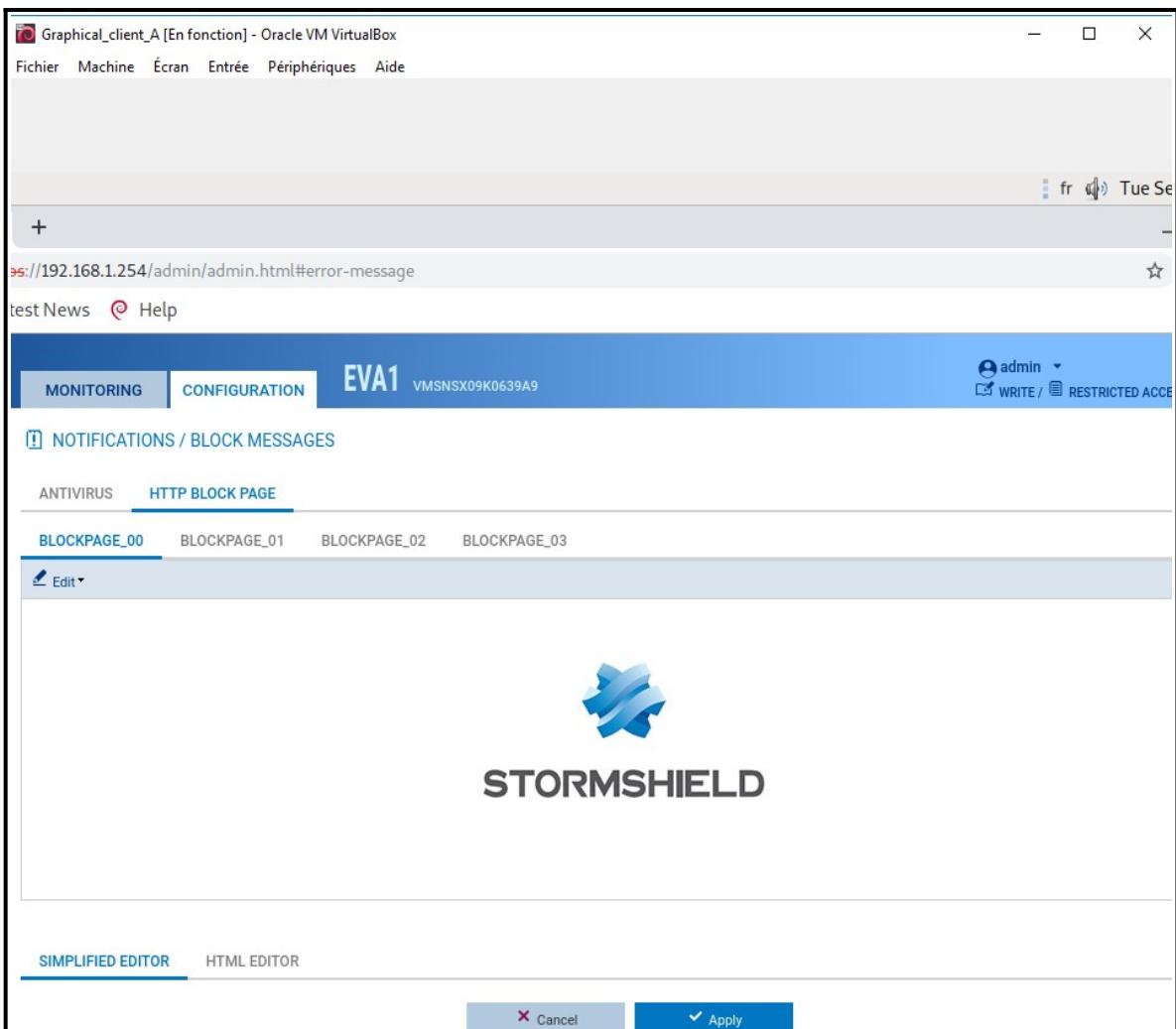
bank

Detailed description: This screenshot shows the configuration interface of the STORMSHIELD Network Security software. The main window title is 'Graphical\_client\_A [En fonction] - Oracle VM VirtualBox'. The menu bar includes 'Fichier', 'Machine', 'Écran', 'Entrée', 'Périphériques', and 'Aide'. Below the menu is a toolbar with icons for Applications, Places, and System. The main content area has tabs for 'MONITORING' and 'CONFIGURATION', with 'CONFIGURATION' selected. The title bar for the configuration tab shows 'EVA1' and 'VMSNSX09K0639A9'. The central part of the screen is titled 'OBJETS / OBJETS WEB' and contains a table with columns for URL, Nom de Certificat (CN), Groupe de Catégories, and Base d'URL. A new row is being added with the URL 'vpnssl\_owa'. A sidebar on the right provides information about URL categories and character restrictions, with examples like 'schemas.microsoft.com/\*' and 'www.w3.org/TR/\*'.





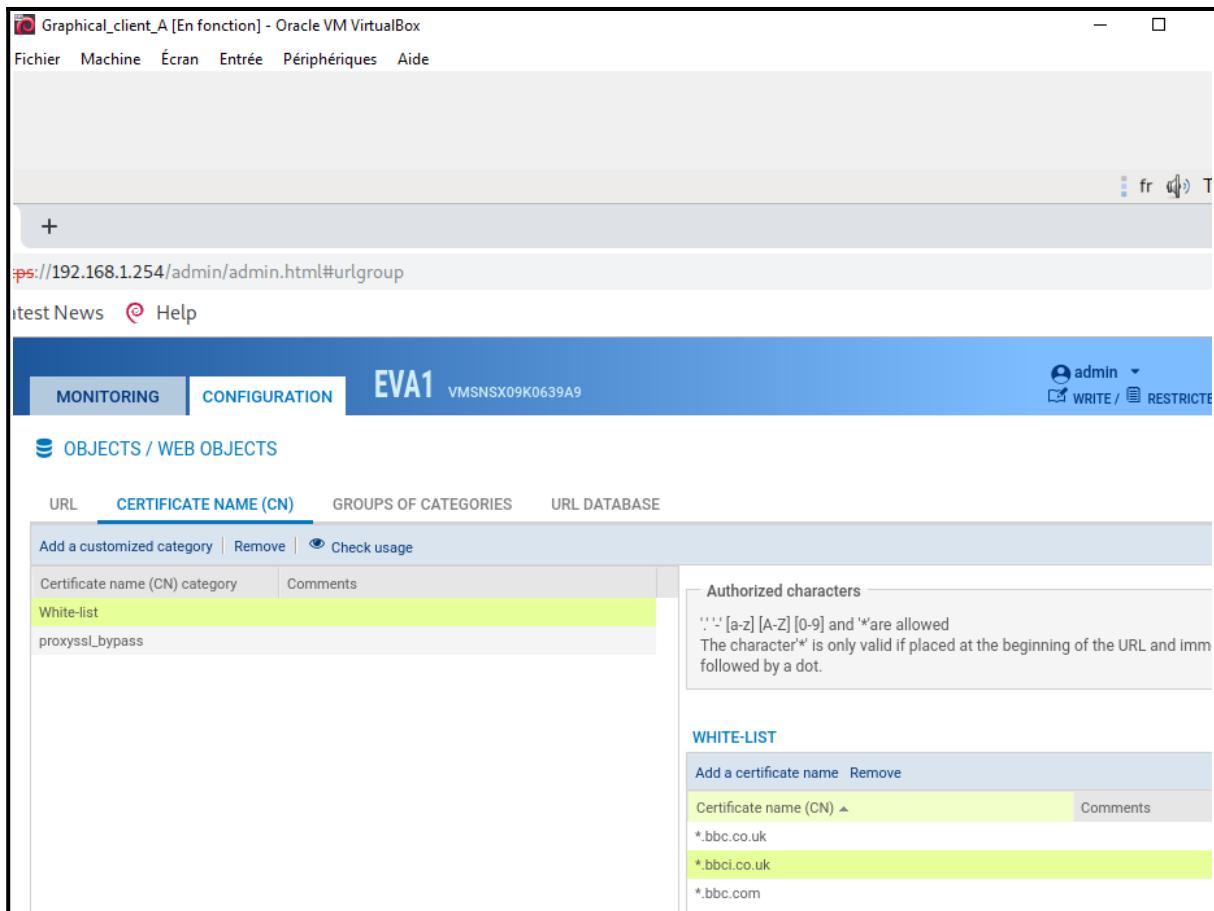
**2ème étape :** Nous vérifions la classification des URL ci-dessus.



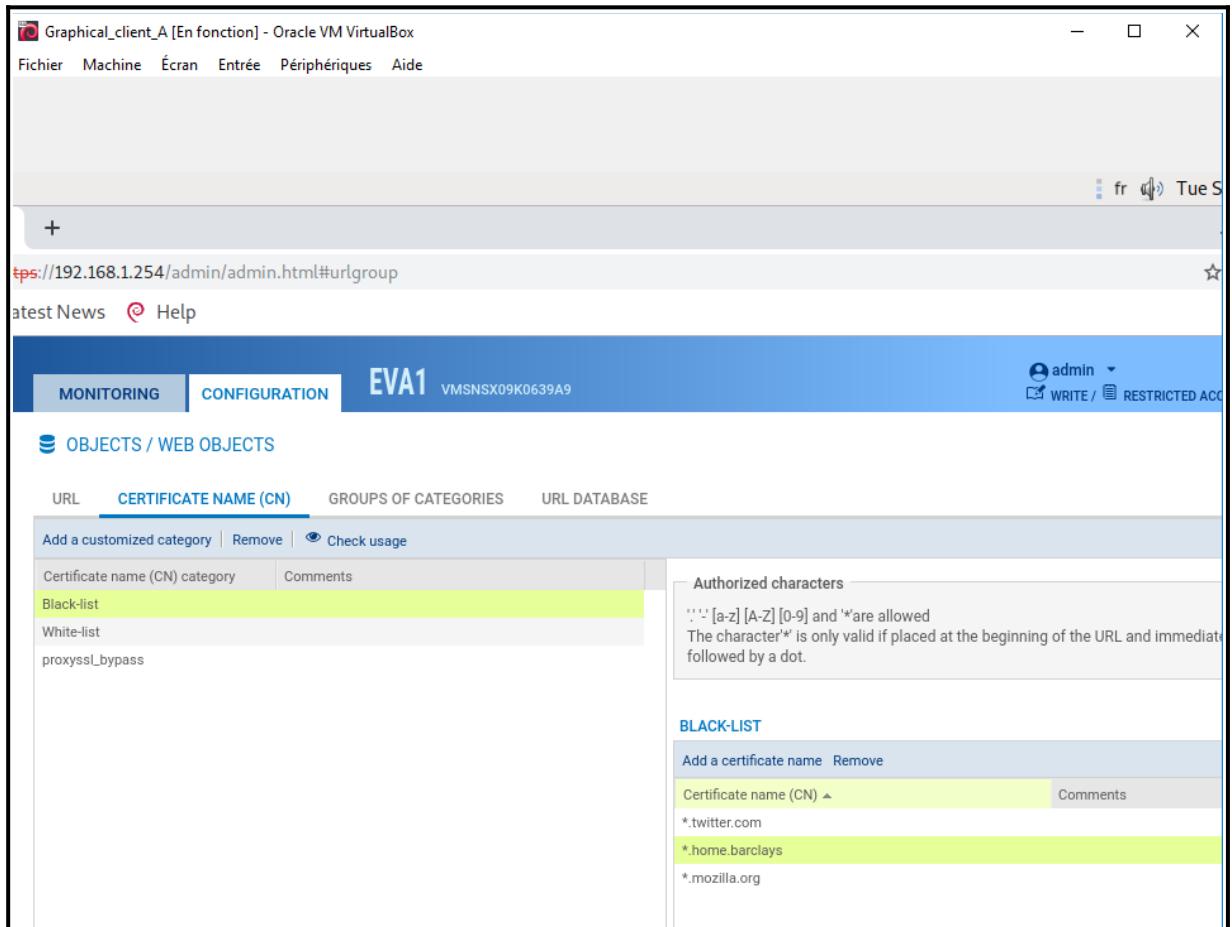
Access to this website is forbidden in accordance with the internet access policy of your company.

User: \$user  
Website: \$host\$url  
Category: \$url\_group  
link: [Request access to this website](#)

**3ème étape :** Nous modifions la page de blocage.



**4ème étape :** Création d'une catégorie White-list contenant les noms de certificat indiqués.



**5ème étape :** Création d'une catégorie Black-list contenant les noms de certificat indiqués.

The screenshot shows the STORMSHIELD Network Security interface version 4.0.1. The main window title is "Graphical\_client\_A [En fonction] - Oracle VM VirtualBox". The menu bar includes "Fichier", "Machine", "Écran", "Entrée", "Périphériques", and "Aide". The toolbar has icons for "Applications", "Places", and "System". A tab bar shows "VMSNSX09K0639A9@19" and a "+" button. Below the toolbar is a navigation bar with back, forward, refresh, and search buttons, and links for "Not secure | https://192.168.1.254/admin/admin.html#sslfiltering/0", "Apps", "Debian.org", "Latest News", and "Help". The main content area is titled "STORMSHIELD Network Security v4.0.1" and "EVA1 VMSNSX09K0639A9". It displays the "MONITORING" and "CONFIGURATION" tabs, with "CONFIGURATION" selected. On the left, a sidebar shows "CLI", "NETWORK", "OBJECTS", "Network objects", and "Web objects". The central panel is titled "SECURITY POLICY / SSL FILTERING" and shows a table for "(0) SSLFilter\_00". The table columns are "Status", "Action", "URL - CN", and "Comments". The rows are:

Status	Action	URL - CN	Comments
on	Pass without decrypting	*	White-list
on	Block without decrypting	*	Black-list
on	Block without decrypting	*	shopping
on	Block without decrypting	*	news
on	Pass without decrypting	*	Any

**6ème étape :** Nous modifions la politique de filtrage SSL en ajoutant nos nouvelles catégories.

The screenshot shows the STORMSHIELD Network Security interface version 4.0.1. The main window title is "Graphical\_client\_A [En fonction] - Oracle VM VirtualBox". The menu bar includes "Fichier", "Machine", "Écran", "Entrée", "Périphériques", and "Aide". The toolbar has icons for "Applications", "Places", and "System". A tab bar shows "VMSNSX09K0639A9@19" and a "+" button. Below the toolbar is a navigation bar with back, forward, refresh, and search buttons, and links for "Not secure | https://192.168.1.254/admin/admin.html#urlfiltering/0", "Apps", "Debian.org", "Latest News", and "Help". The main content area is titled "STORMSHIELD Network Security v4.0.1" and "EVA1 VMSNSX09K0639A9". It displays the "MONITORING" and "CONFIGURATION" tabs, with "CONFIGURATION" selected. On the left, a sidebar shows "Certificates and PKI", "USERS", "SECURITY POLICY", "Filter - NAT", and "URL filtering" (which is highlighted). The central panel is titled "SECURITY POLICY / URL FILTERING" and shows a table for "(0) URLFilter\_00". The table columns are "Status", "Action", "URL category", and "Comments". The rows are:

Status	Action	URL category	Comments
on	Page de blocage lab-6	shopping	
on	Page de blocage lab-6	news	
on	Pass	Any	

**7ème étape :** Nous modifions également le filtrage URL.

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

Fichier Machine Écran Entrée Périphériques Aide

fr Tue S

+  
http://192.168.1.254/admin/admin.html#securitypolicy/local/6/filter  
test News Help

MONITORING CONFIGURATION EVA1 VMSNSX09K0639A9 admin WRITE / RESTRICTED ACC

SECURITY POLICY / FILTER - NAT

(6) Lab\_6 Edit Export

FILTERING NAT

	Status	Action	Source	Destination	Dest. port	Protocol	Security inspection	Comments
8	on	block	Network_in	Internet geo Corée du Sud	http https	IPS	Created on 2	
9	on	block	Network_in	www.edition.cnn.c	http https	IPS	Created on 2	
10	on	pass	Network_in	Internet	http	IPS	URL filter: lab_6 Created on 2	
11	on	decrypt	Network_in	Internet	https	IPS	SSL filter: lab_6 Created on 2	
12	on	pass	Network_in	Internet	http https	IPS	Created on 2	

Page 1 of 1

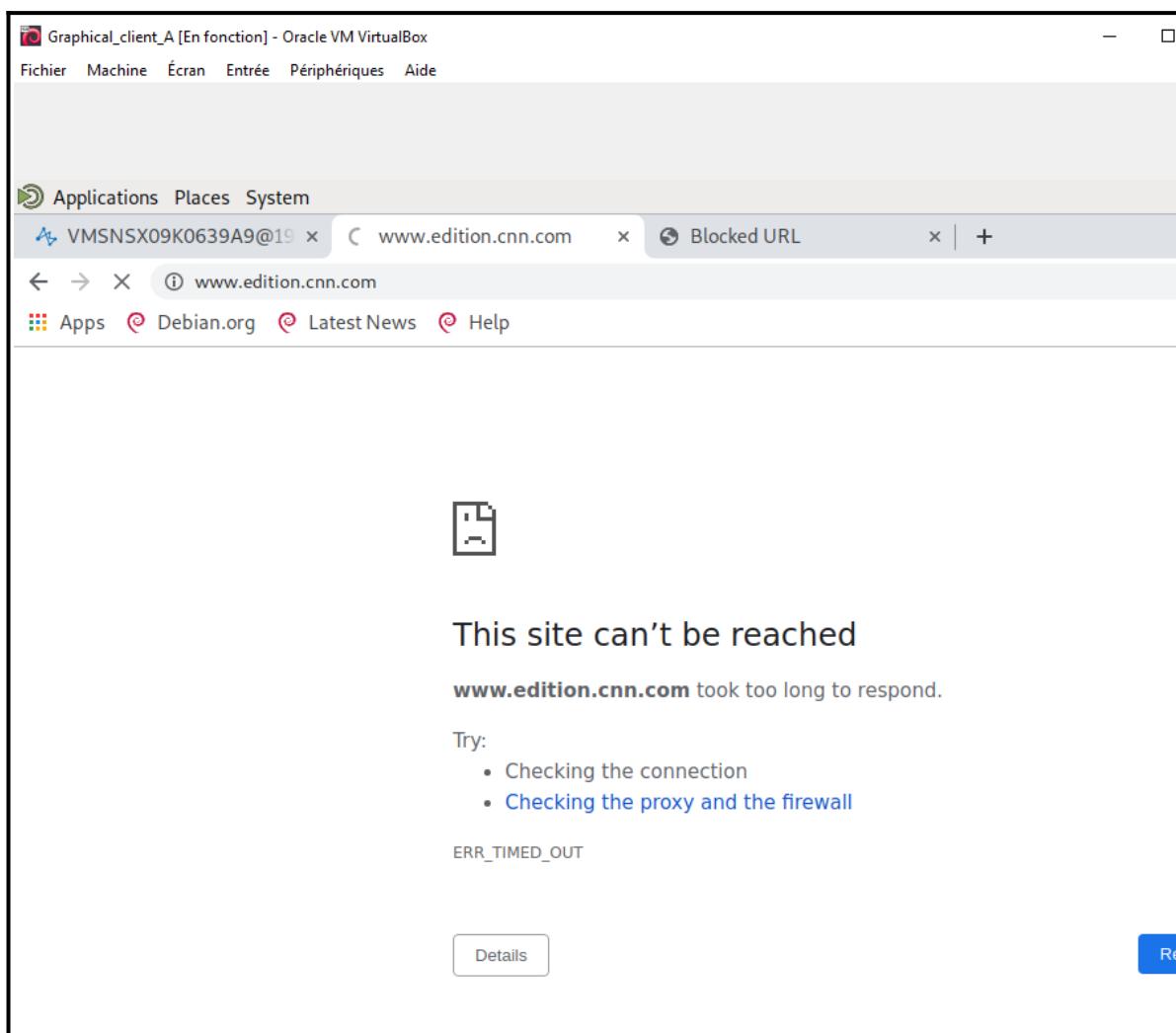
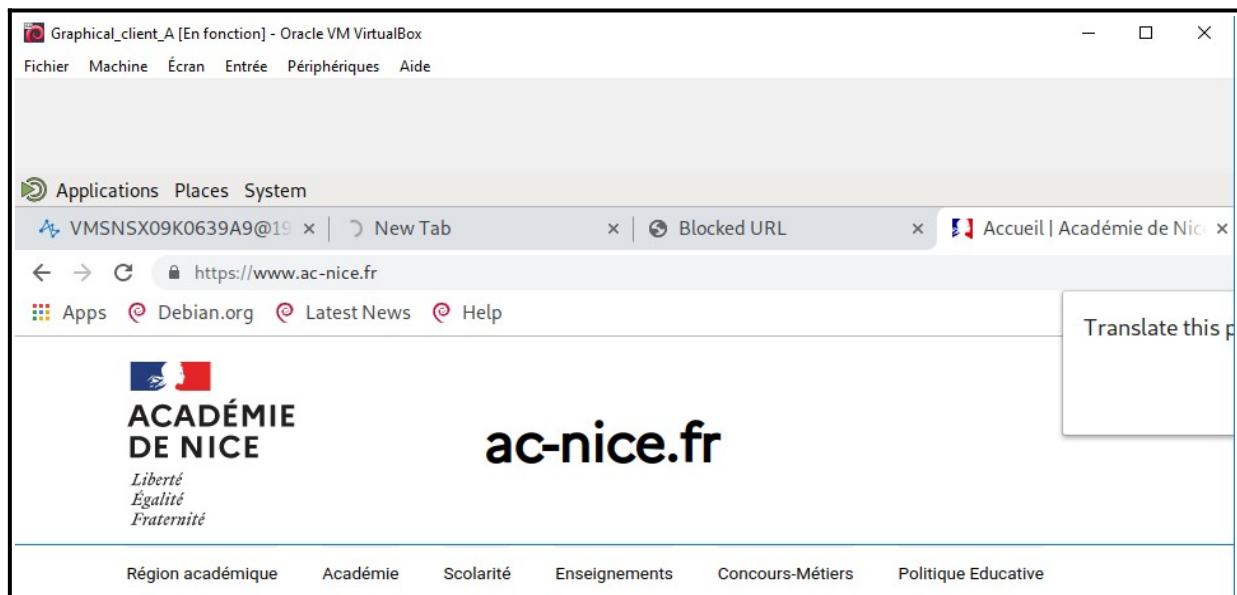
CHECKING THE POLICY

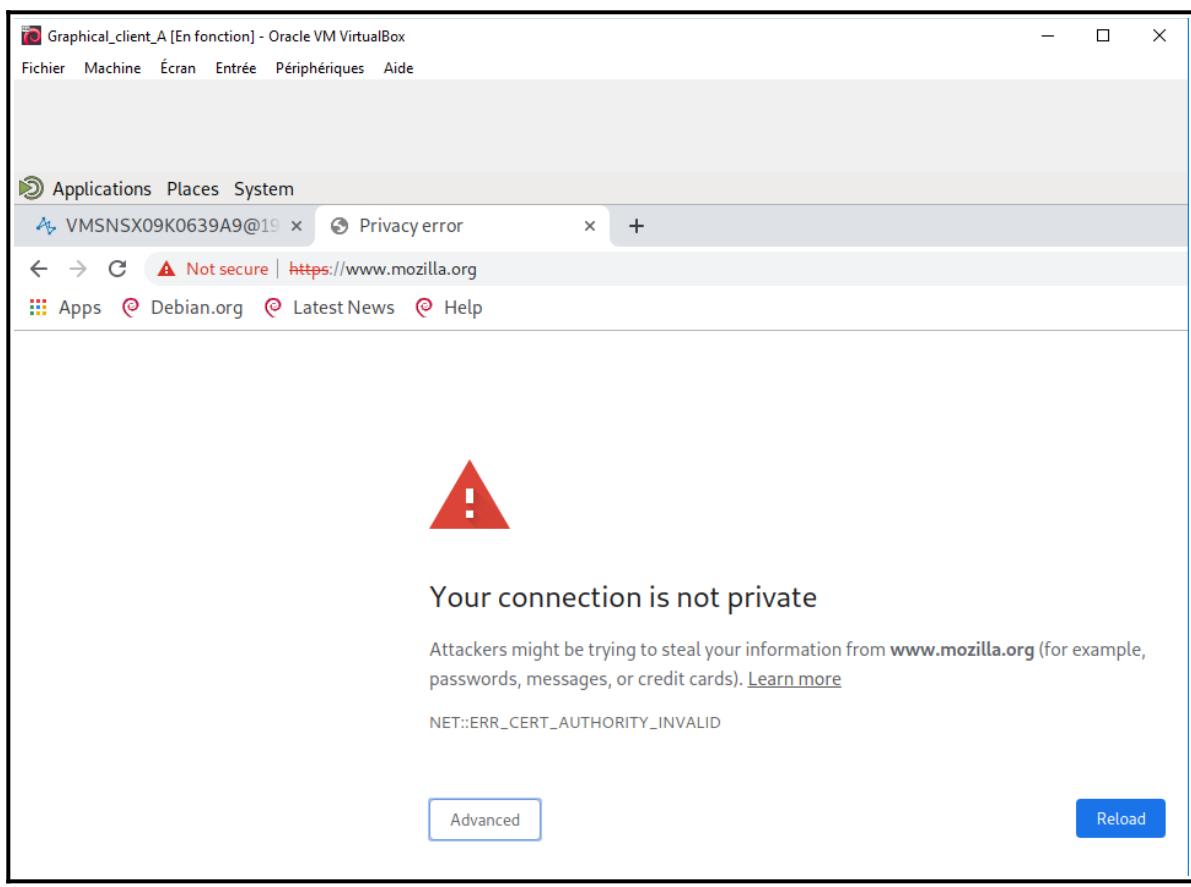
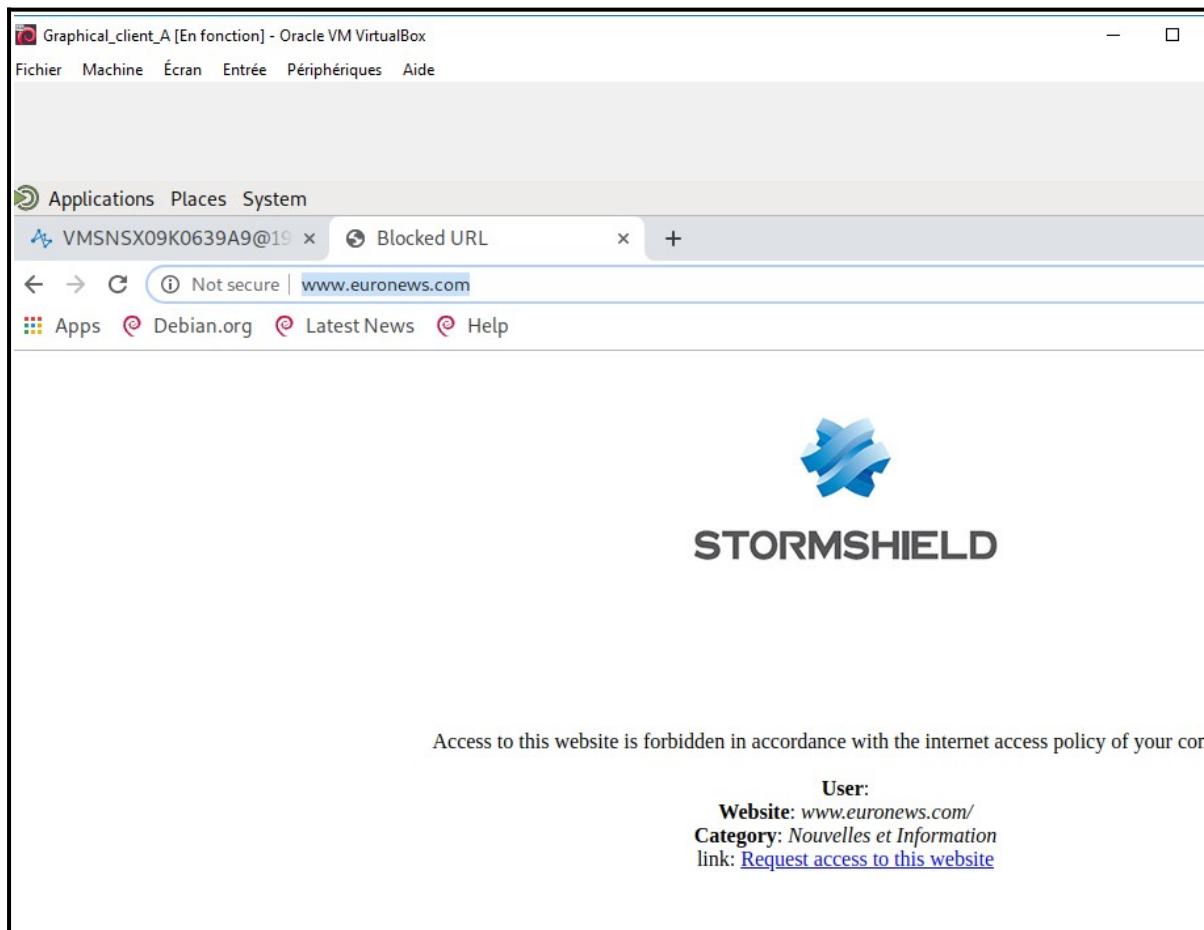
[Rule 1] This rule may be covered by an implicit rule and may never be applied.

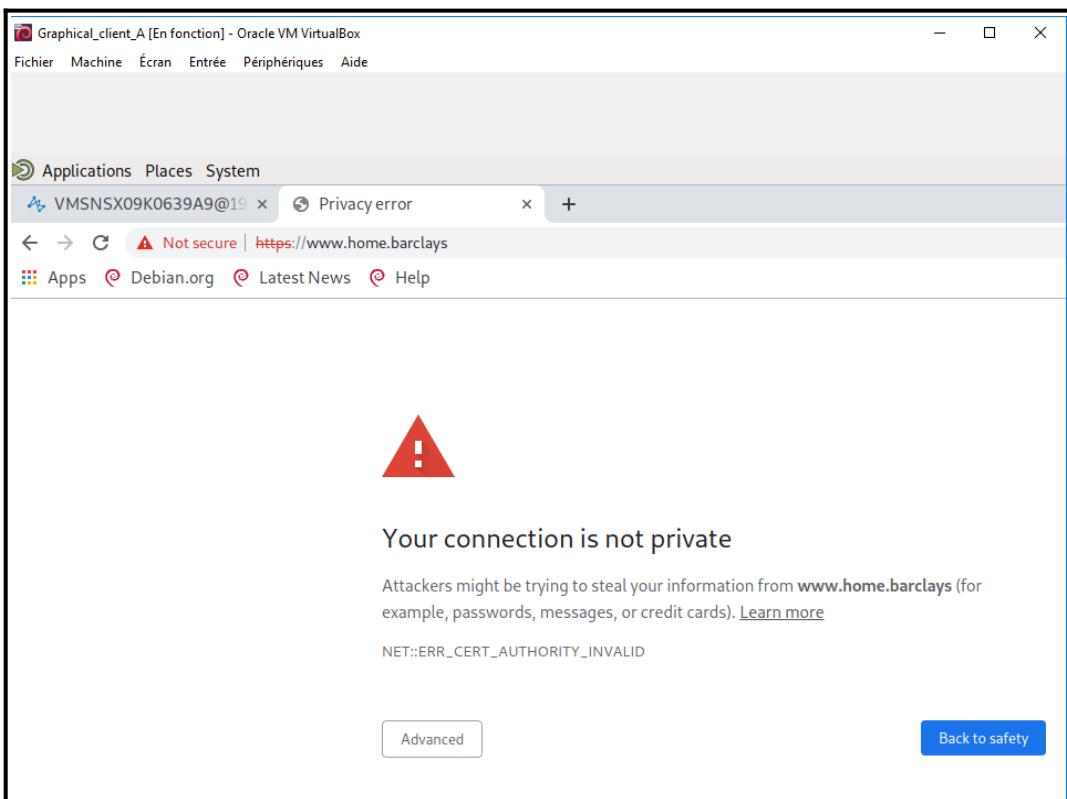
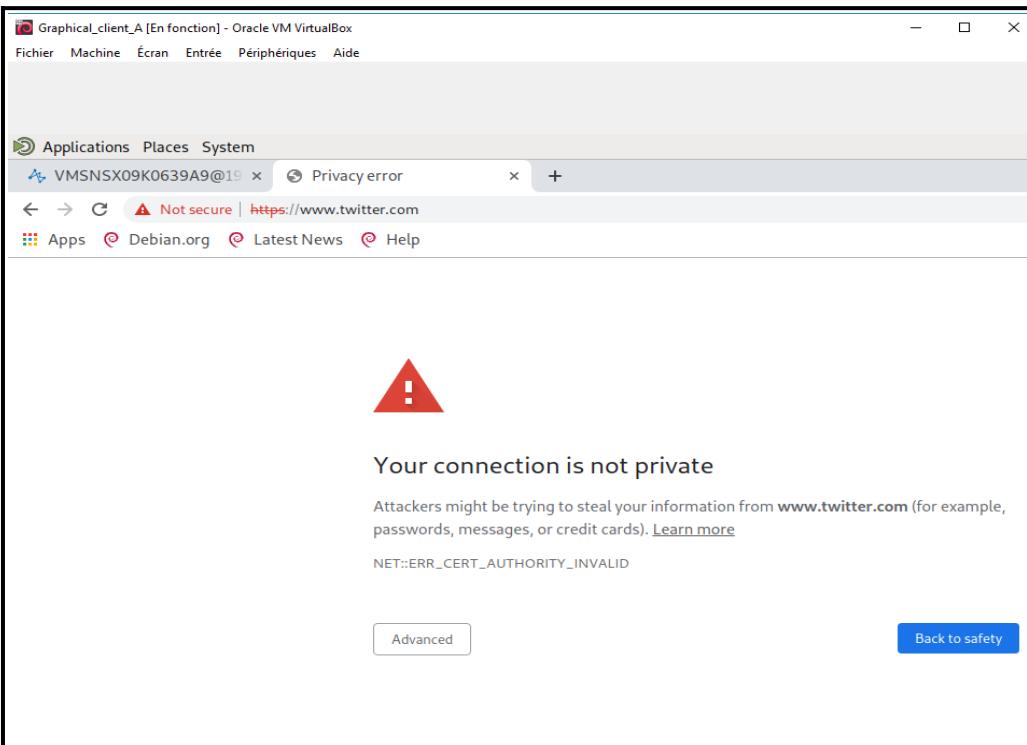
X CANCEL ✓ APPLY

The screenshot shows the EVA1 security policy configuration interface. The 'FILTERING' tab is selected. A table lists 12 rules. Rule 10 is highlighted in green and has a yellow border, indicating it is selected or active. The columns represent rule number, status, action, source, destination, destination port, protocol, security inspection, and comments. Rule 10's comment field contains 'URL filter: lab\_6'. Other rules include blocking traffic from South Korea and specific websites like www.edition.cnn.c. Rule 11 performs SSL decryption. Rule 12 is an implicit rule. A note at the bottom states that Rule 1 might be covered by an implicit rule and never be applied.

**8ème étape :** Nous modifions la politique de filtrage concernant les règles HTTP et HTTPS.







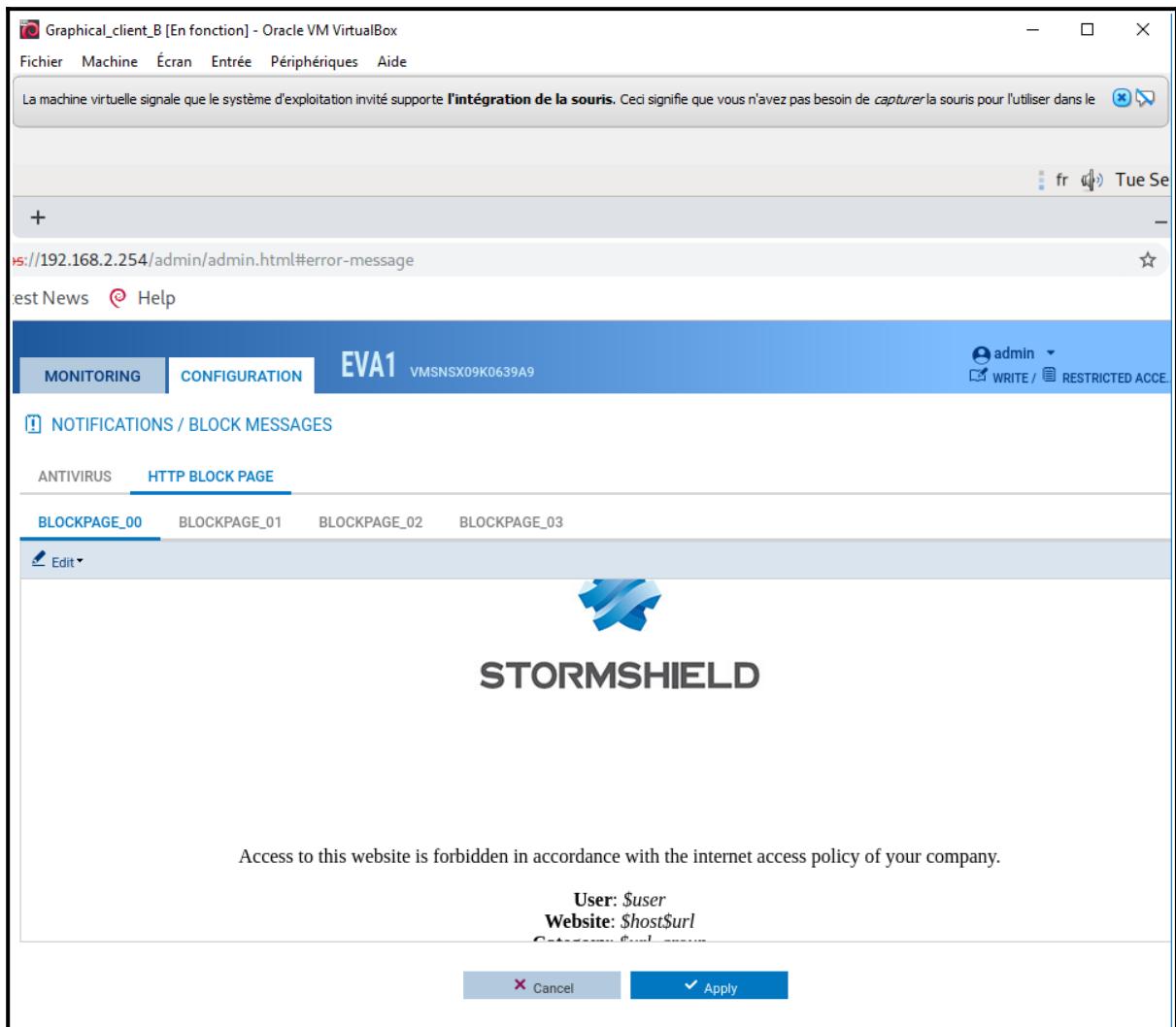
**9ème étape :** Nous effectuons nos différents tests afin de vérifier si tout fonctionne, seulement le site edition.cnn n'affiche pas la page de rejet du trafic SSL puisque celui-ci est déjà bloqué par une règle de filtrage avec un objet FQDN.

## Réseau B :

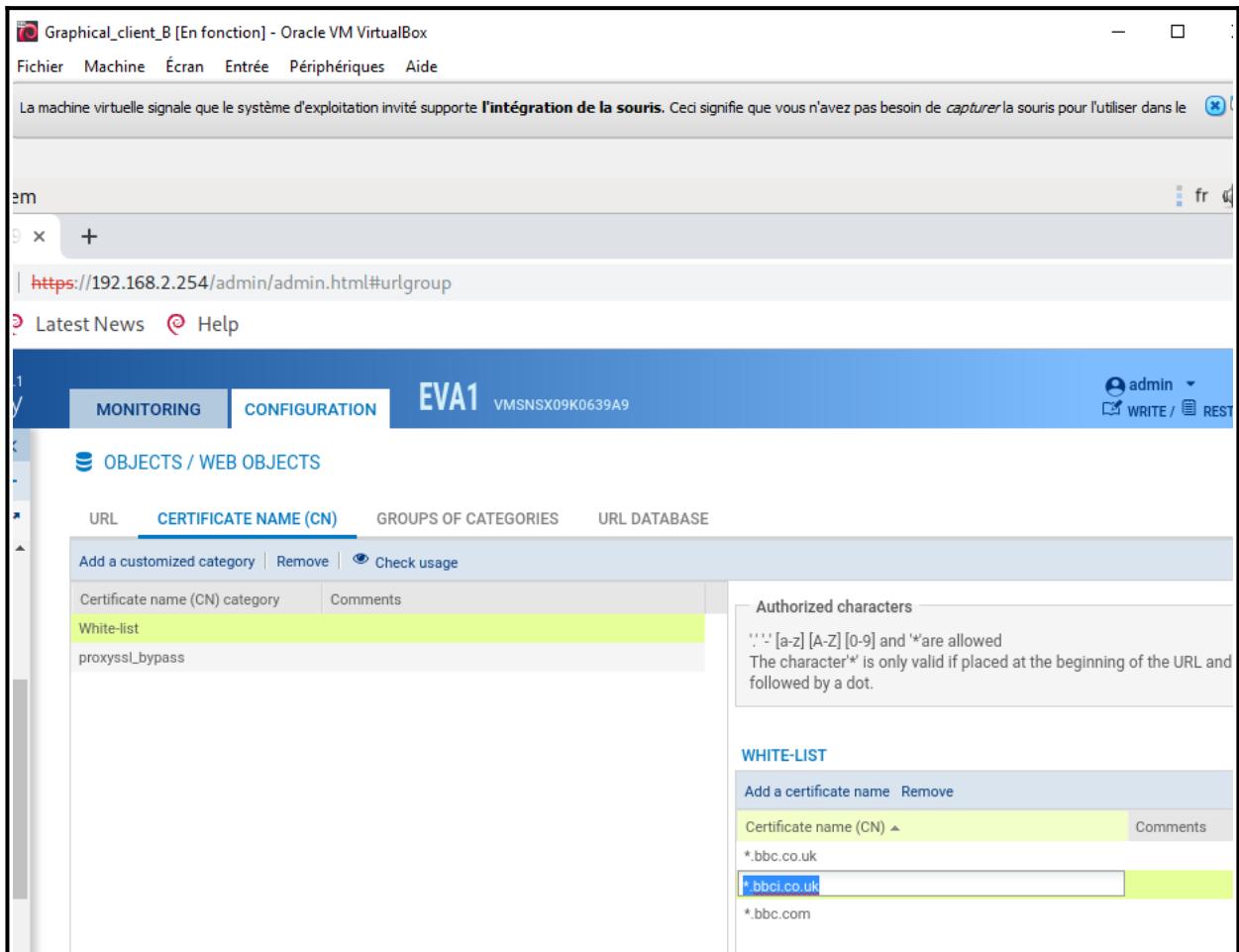
The screenshot shows a Linux desktop environment with a window titled "Graphical\_client\_B [En fonction] - Oracle VM VirtualBox". The window contains a browser tab for "VMSNSX09K0639A9@192.168.2.254" with the URL "https://192.168.2.254/admin/admin.html#urlgroup". The page displays the "STORMSHIELD Network Security v4.0.1" interface, specifically the "CONFIGURATION" section for "OBJECTS / WEB OBJECTS". The left sidebar shows navigation categories like "CLI", "NETWORK", "OBJECTS", "Network objects", "Web objects" (which is selected), "Certificates and PKI", "USERS", "SECURITY POLICY", and "Filter - NAT". The main content area shows a table with columns: URL, CERTIFICATE NAME (CN), GROUPS OF CATEGORIES, and URL DATABASE. A dropdown menu under "URL DATABASE" is set to "Embedded URL database". Below the table, a list of categories and their comments is provided:

Category	Comments
academic	Université et Enseignement Supérieur
ads	Publicité
arts	Arts
bank	Institutions financières
business	Commerce et Finances
employment	Emploi
entertainment	Culture et Loisirs
illegal	Contenu Illicite
it	Informatique
news	Nouvelles et Information
online	Jeux en ligne, Paris, Radios, Réseaux Sociaux et Partage de Fichiers
pornography	Contenu pornographique ou érotique
proxy	Proxies anonymes
shopping	Ventes en ligne

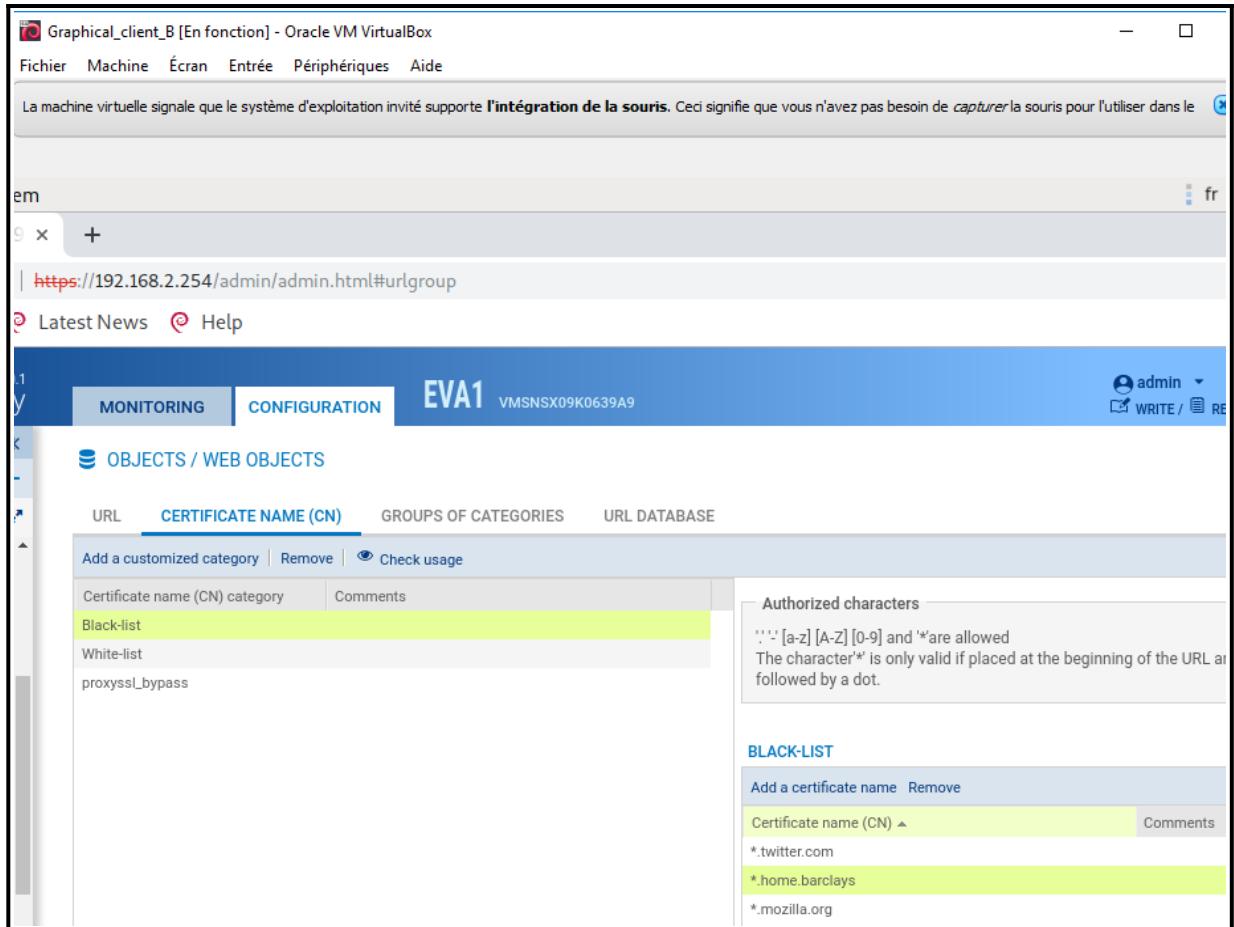
**1ère étape :** Nous sélectionnons la base d'URL embarquée dans les objets WEB.



**2ème étape :** Nous modifions la page de blocage.



**3ème étape :** Création d'une catégorie White-list contenant les noms de certificat indiqués.



**4ème étape :** Création d'une catégorie Black-list contenant les noms de certificat indiqués.

The screenshot shows the STORMSHIELD Network Security interface version 4.0.1. The left sidebar has a 'CONFIGURATION' section with 'Search...', 'Network objects', 'Web objects', 'Certificates and PKI', 'USERS', 'SECURITY POLICY', 'Filter - NAT', and 'URL filtering'. The 'SECURITY POLICY / SSL FILTERING' tab is selected, showing a table with five rows:

Status	Action	URL - CN	Comments
on	Pass without decrypting	White-list	
on	Block without decrypting	Black-list	
on	Block without decrypting	shopping	
on	Block without decrypting	news	
on	Pass without decrypting	Any	

**5ème étape :** Nous modifions la politique de filtrage SSL en ajoutant nos nouvelles catégories.

The screenshot shows the STORMSHIELD Network Security interface version 4.0.1. The left sidebar has a 'SECURITY POLICY' section with 'Search...', 'SECURITY POLICY', 'Filter - NAT', 'URL filtering' (which is selected), and 'SSL filtering'. The 'SECURITY POLICY / URL FILTERING' tab is selected, showing a table with three rows:

Status	Action	URL category	Comments
on	Page de blocage lab-6	shopping	
on	Page de blocage lab-6	news	
on	Pass	Any	

**6ème étape :** Nous modifions également le filtrage URL.

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

Fichier Machine Écran Entrée Périphériques Aide

La machine virtuelle signale que le système d'exploitation invité supporte l'intégration de la souris. Ceci signifie que vous n'avez pas besoin de capturer la souris pour l'utiliser dans le

fr T

x +

<https://192.168.2.254/admin/admin.html#securitypolicy/local/6/filter/13>

Latest News Help

EVA1 VMSNSX09K0639A9 admin WRITE / RESTRICTED

**SECURITY POLICY / FILTER - NAT**

(6) Filter 06 | Edit | Export | i

FILTERING NAT

Searching... | + New rule | X Delete | ↑ ↓ | x | Cut | Copy | Paste | Search in logs | Search in monitoring

	Status	Action	Source	Destination	Dest. port	Protocol	Security inspection	Comments
7	on	pass	Network_in	srv.mail_priv	smtp		IPS	Created
8	on	block	Network_in	Internet geo Corée du Sud	http https		IPS	Created
9	on	block	Network_in	www.edition.cnn.c	http https		IPS	Created
10	on	pass	Network_in	Internet	http		IPS URL filter: lab_6	Created
11	on	decrypt	Network_in	Internet	https		IPS SSL filter: lab_6	Created

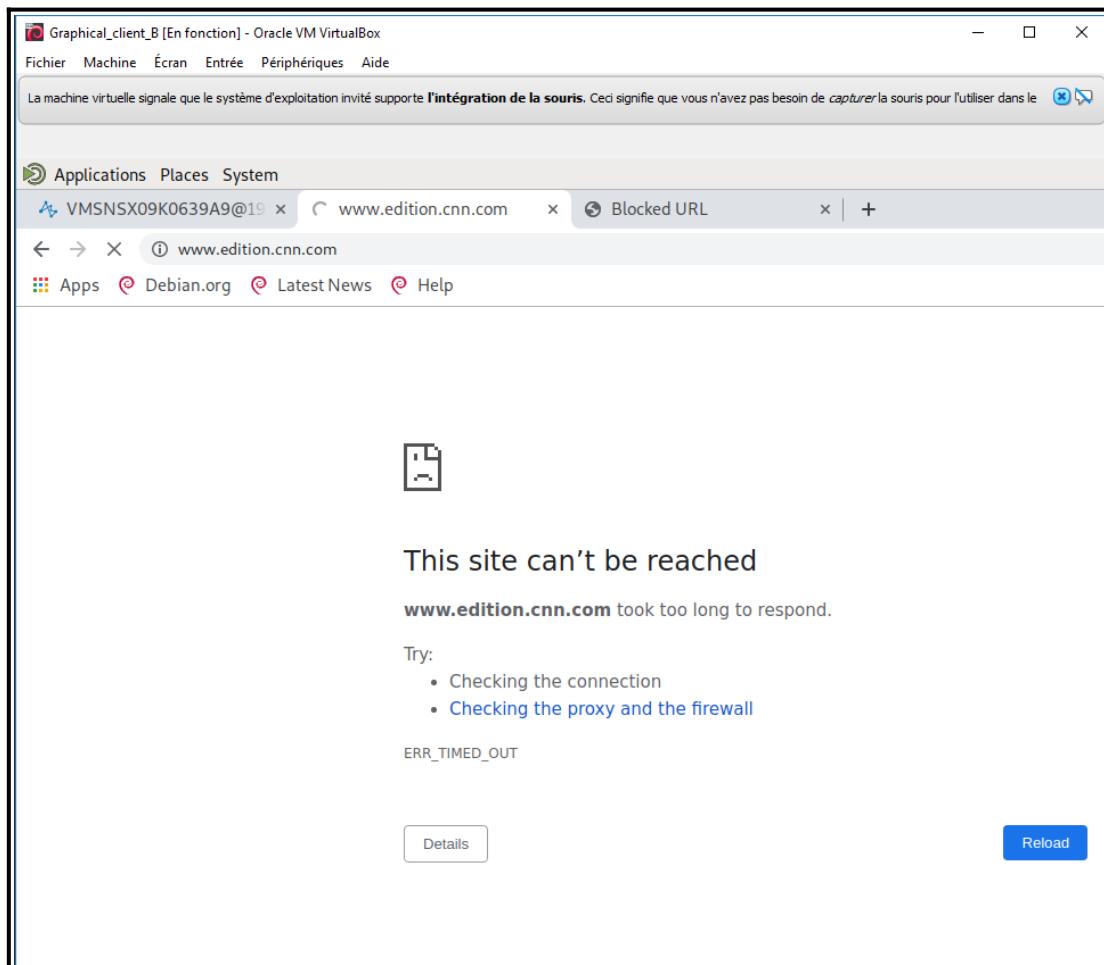
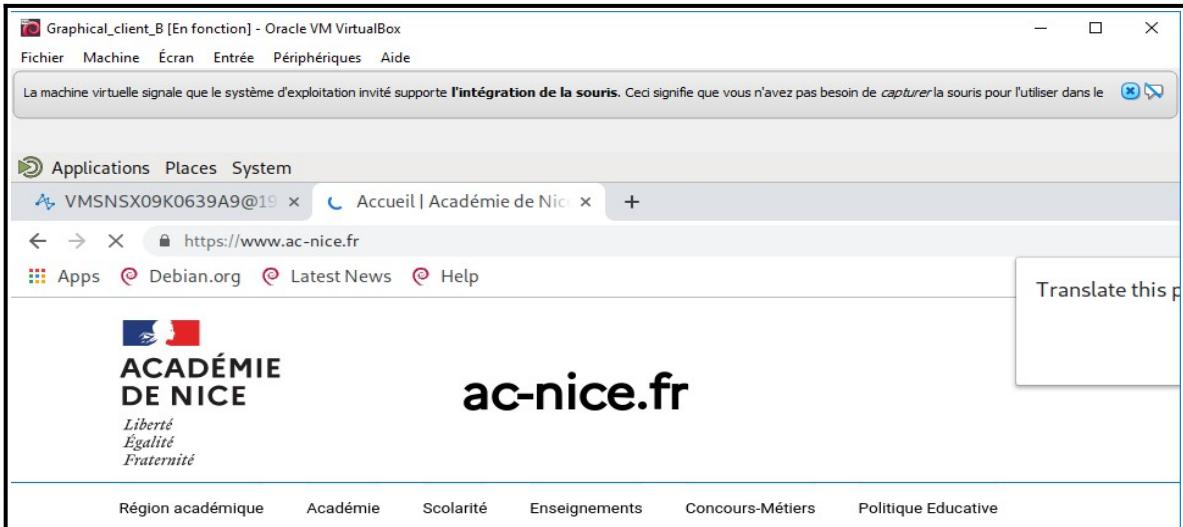
TRAFFIC SORTANT - Updated on 2022-09-27 11:33:44 by admin (192.168.2.2) (contains 9 rules, from 8 to 16)

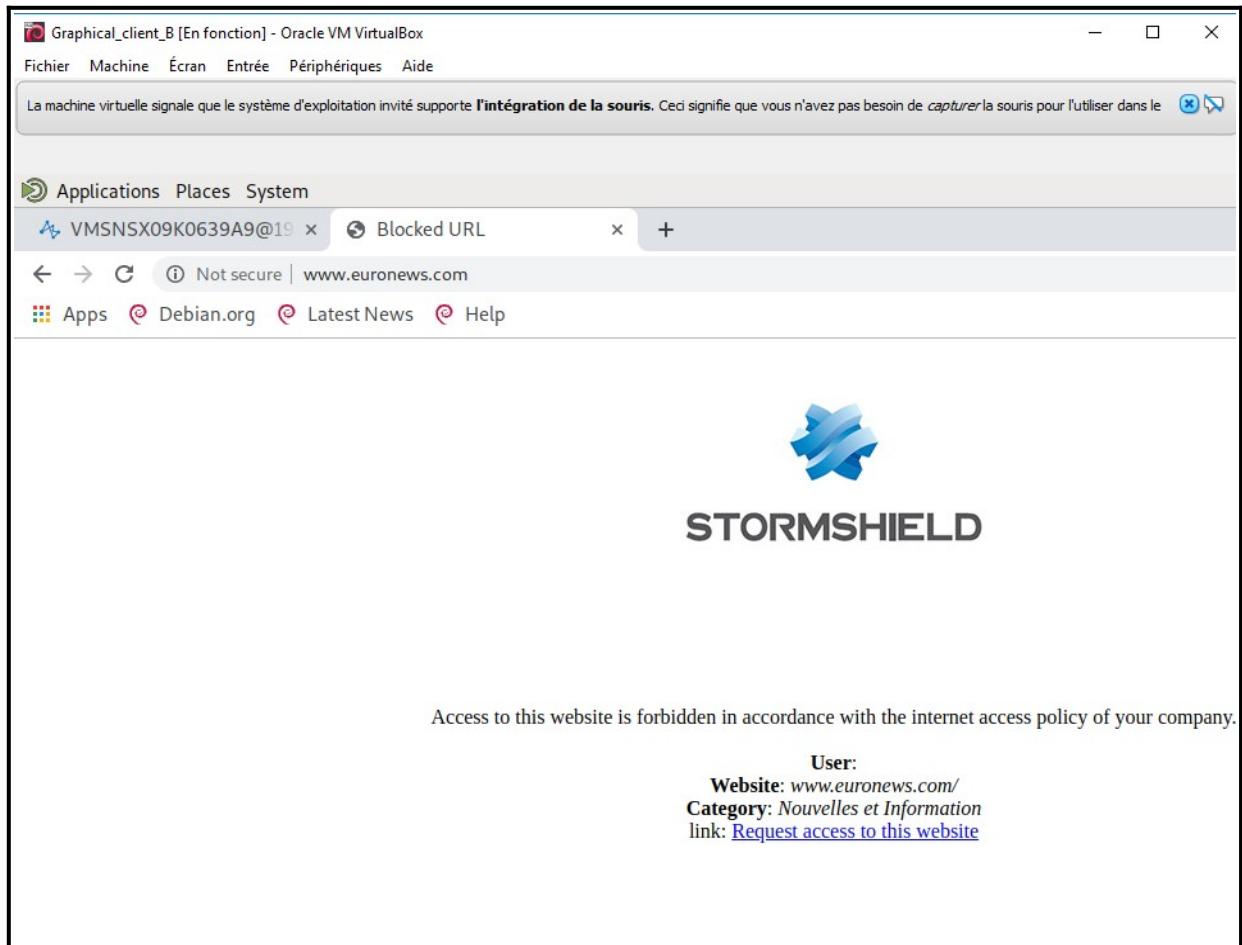
< < | Page 1 of 1 | > >> | Disp

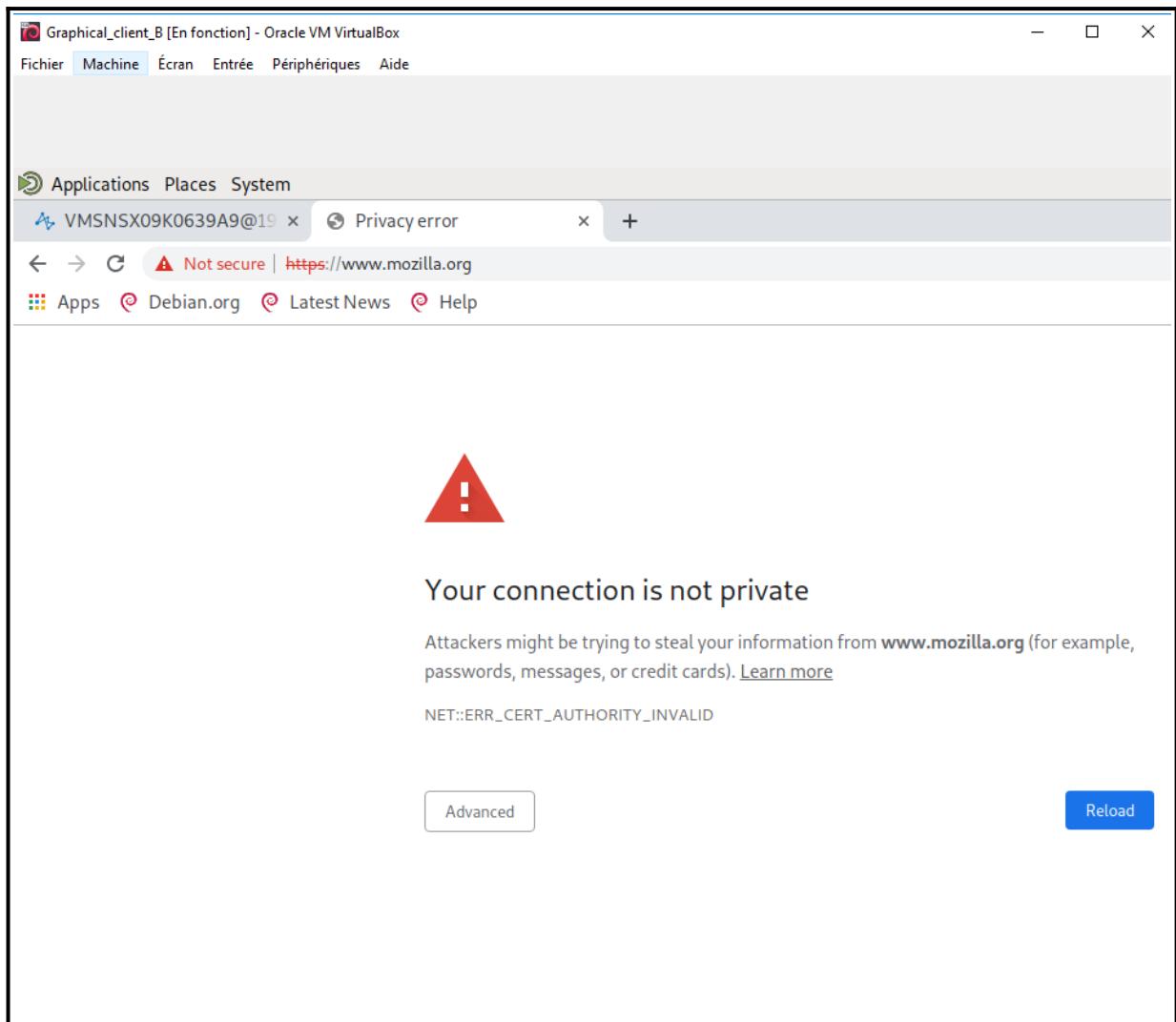
CHECKING THE POLICY

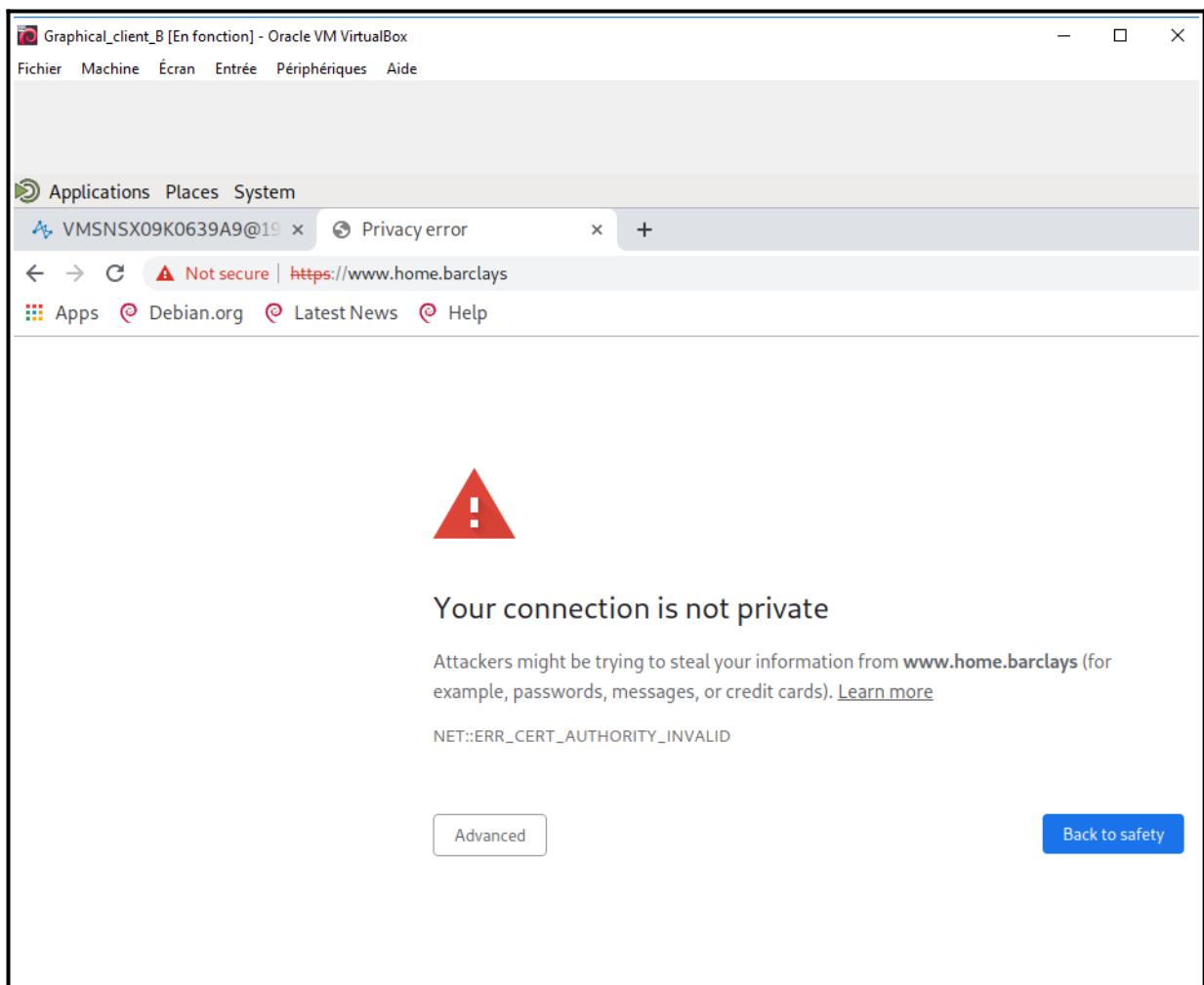
X CANCEL ✓ APPLY

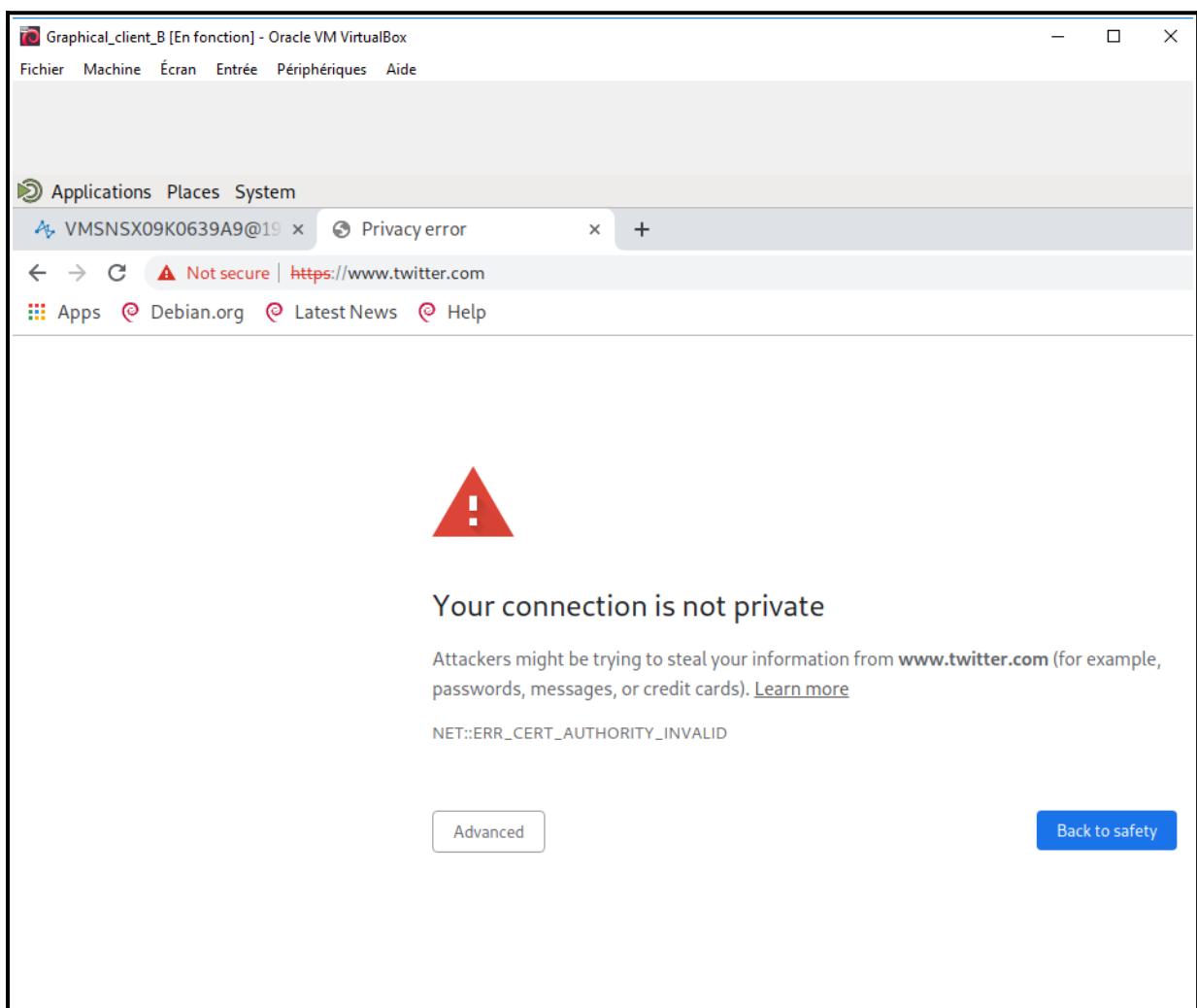
**7ème étape :** Nous modifions la politique de filtrage concernant les règles HTTP et HTTPS.











**8ème étape :** Nous effectuons nos différents tests afin de vérifier si tout fonctionne, seulement le site edition.cnn n'affiche pas la page de rejet du trafic SSL puisque celui-ci est déjà bloqué par une règle de filtrage avec un objet FQDN.