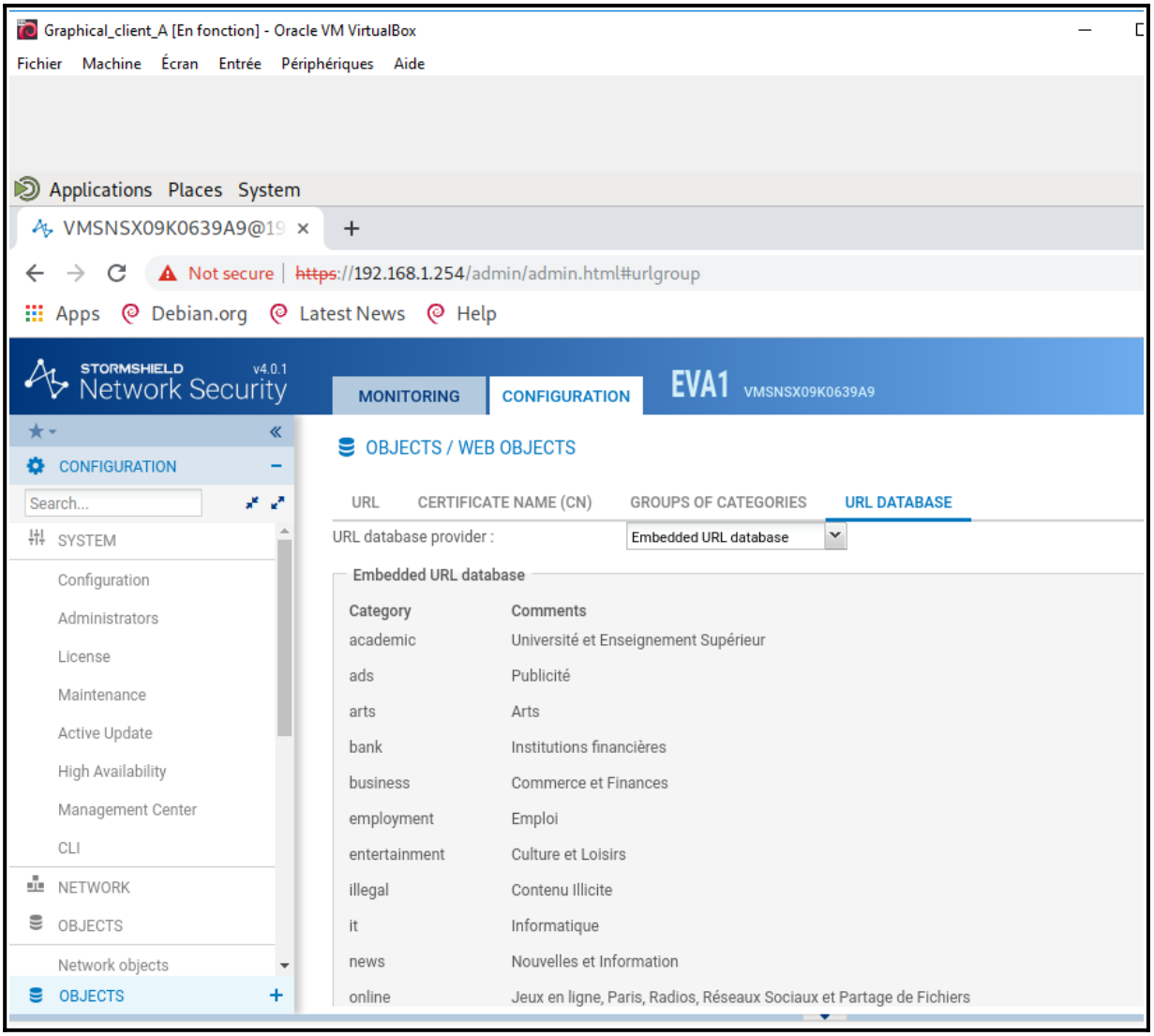
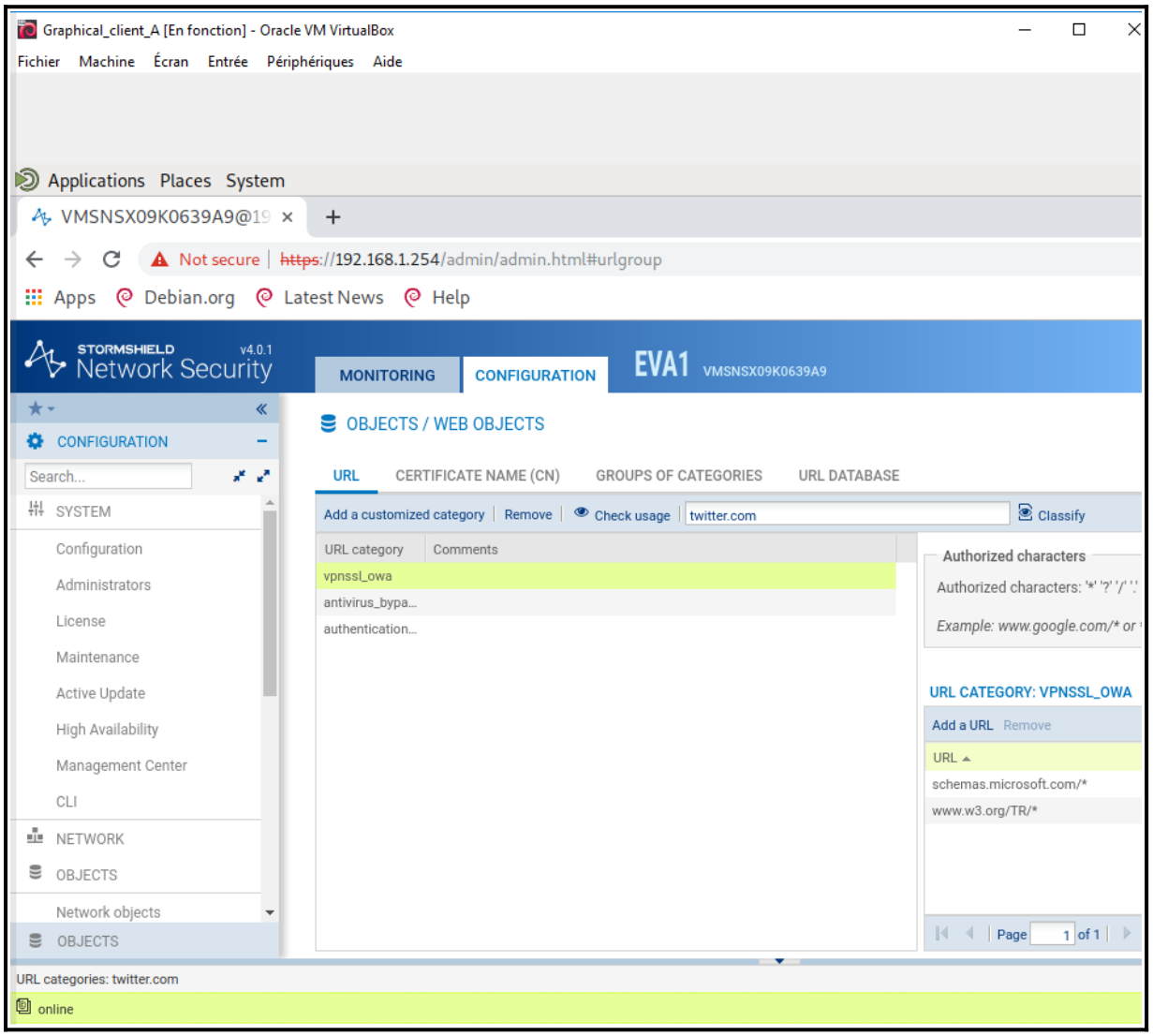
STORMSHIELD

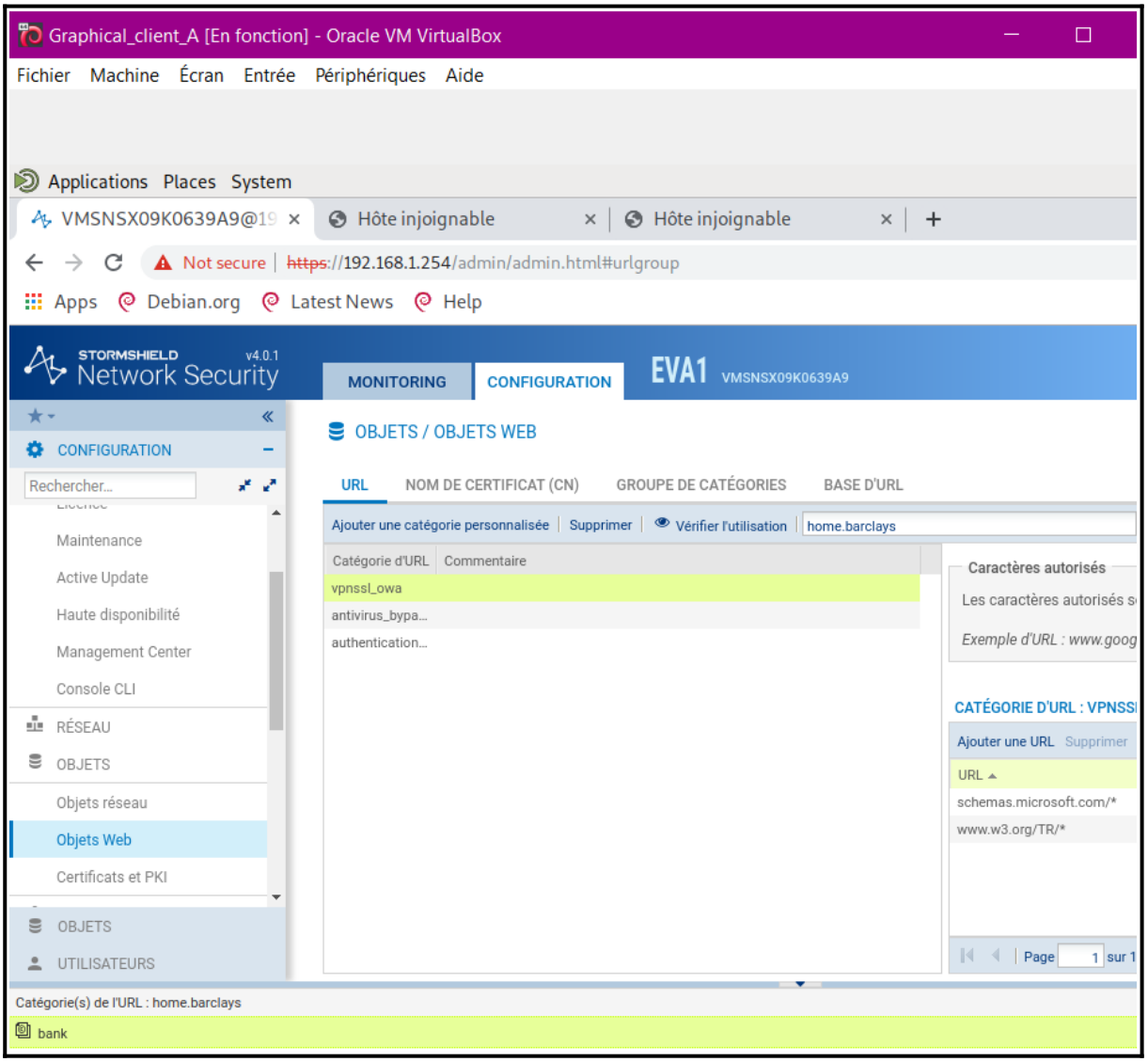
LAB 6 :
Filtrage de contenu

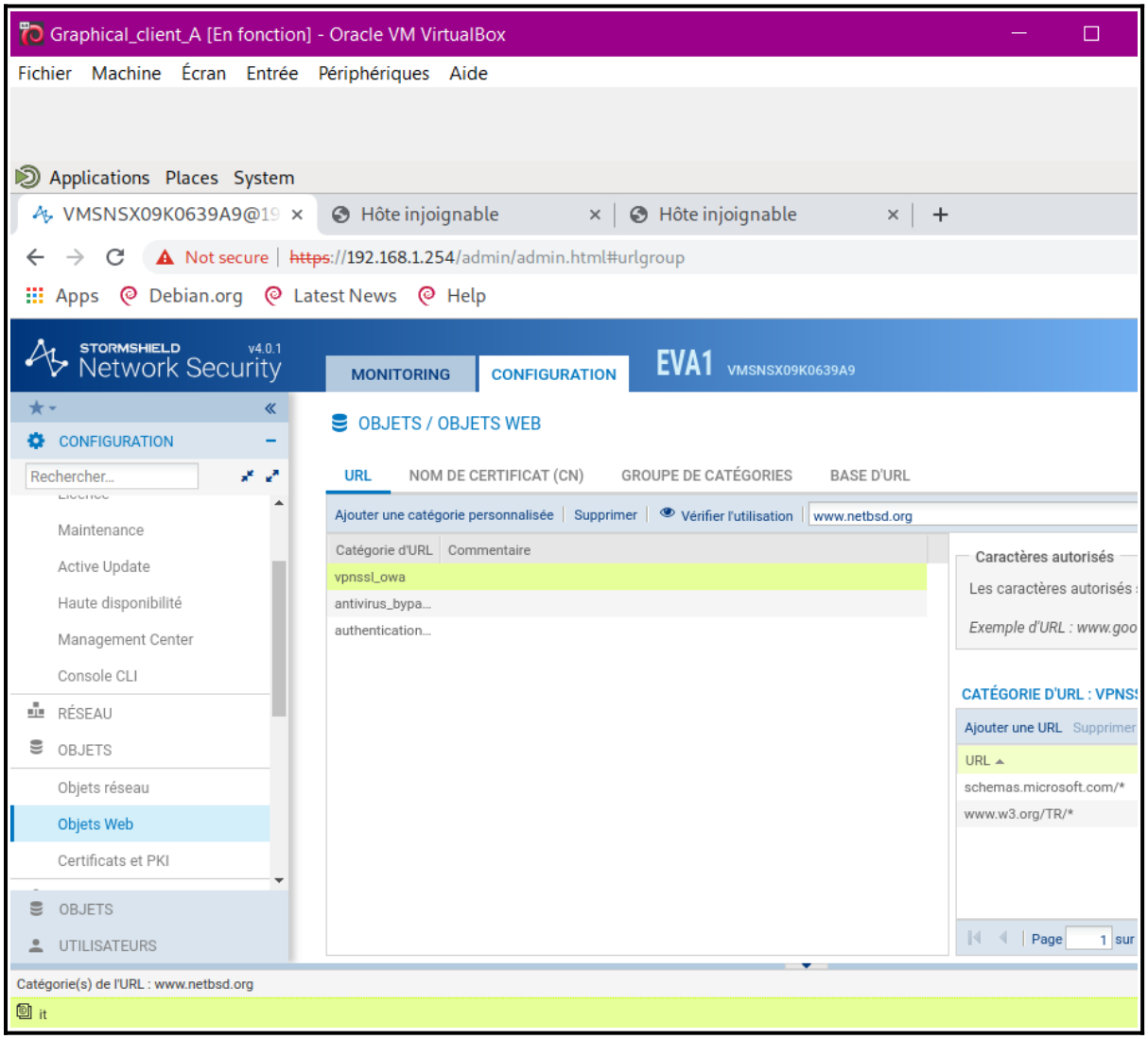
Réseau A :

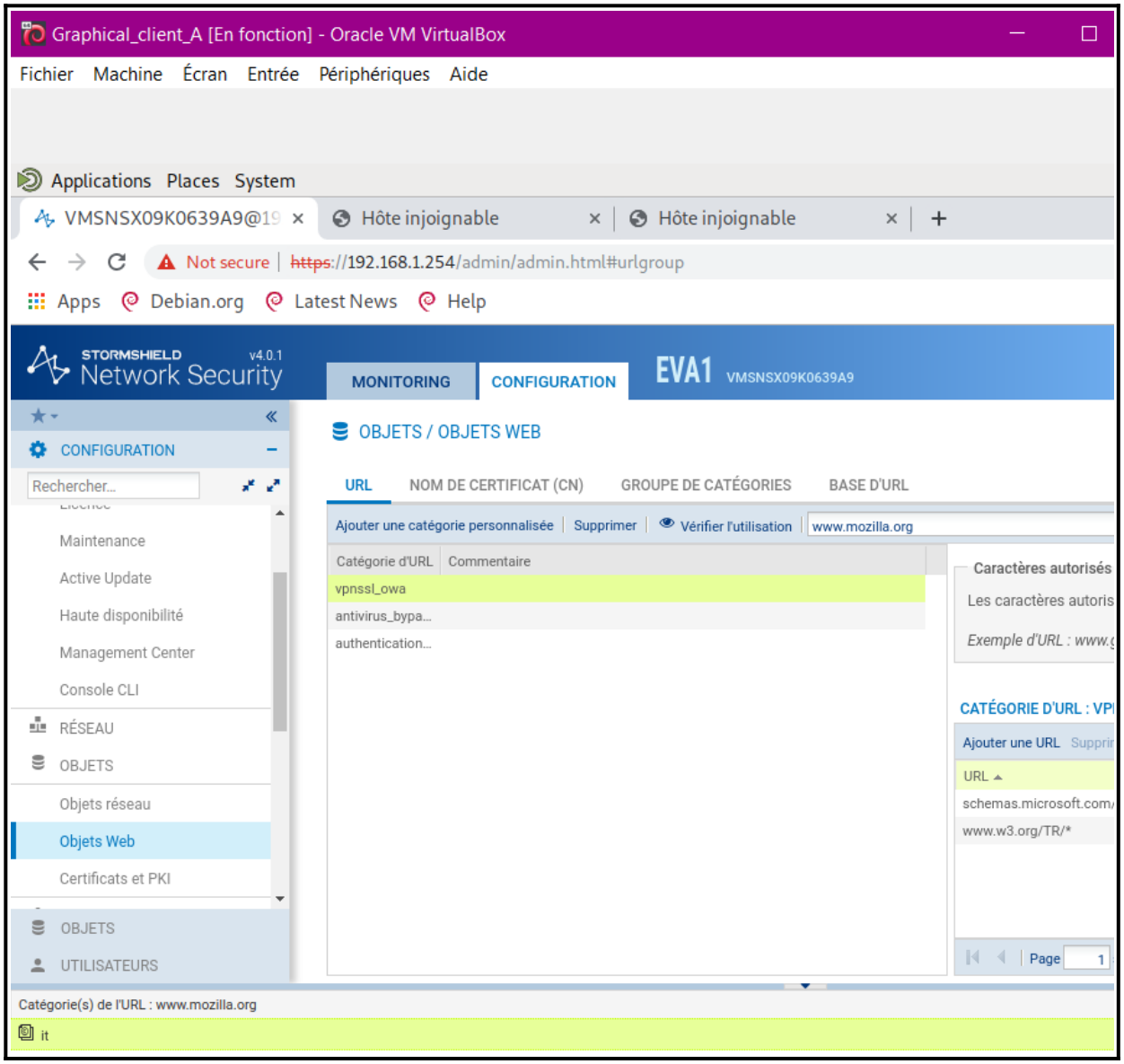


1ère étape : Nous sélectionnons la base d'URL embarquée dans les objets WEB.

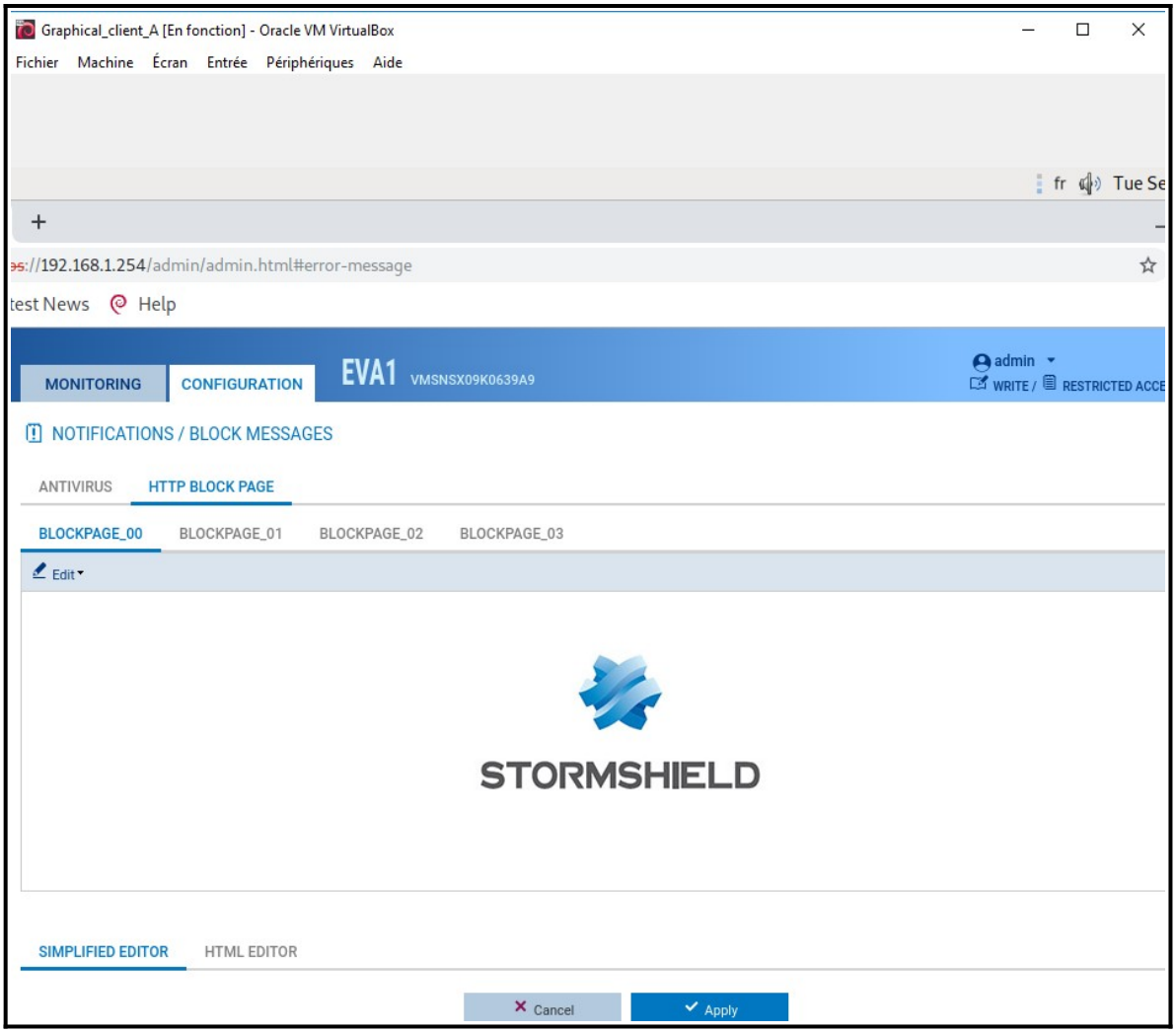

Graphical_client_A [En fonction] - Oracle VM VirtualBox
Fichier Machine Écran Entrée Périphériques Aide
Applications Places System
VMSNSX09K0639A9@19
Not secure https://192.168.1.254/admin/admin.html#urlgroup
Apps Debian.org Latest News Help
STORMSHIELD Network Security v4.0.1
MONITORING CONFIGURATION EVA1 VMSNSX09K0639A9
CONFIGURATION
Search...
SYSTEM
Configuration
Administrators
License
Maintenance
Active Update
High Availability
Management Center
CLI
NETWORK
OBJECTS
Network objects
OBJECTS
OBJECTS / WEB OBJECTS
URL CERTIFICATE NAME (CN) GROUPS OF CATEGORIES URL DATABASE
Add a customized category Remove Check usage twitter.com Classify
URL category Comments
vpnssl_owa
antivirus_bypa...
authentication...
Authorized characters
Authorized characters: '*' '?' '/' '.'
Example: www.google.com/* or
URL CATEGORY: VPNSSL_OWA
Add a URL Remove
URL
schemas.microsoft.com/*
www.w3.org/TR/*
Page 1 of 1
URL categories: twitter.com
online


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
CONFIGURATION
Rechercher...
Maintenance
Active Update
Haute disponibilité
Management Center
Console CLI
RÉSEAU
OBJETS
Objets réseau
Objets Web
Certificats et PKI
OBJETS
UTILISATEURS
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


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
CONFIGURATION
Rechercher...
Maintenance
Active Update
Haute disponibilité
Management Center
Console CLI
RÉSEAU
OBJETS
Objets réseau
Objets Web
Certificats et PKI
OBJETS
UTILISATEURS
OBJETS / OBJETS WEB
URL
NOM DE CERTIFICAT (CN)
GROUPE DE CATÉGORIES
BASE D'URL
Ajouter une catégorie personnalisée
Supprimer
Vérifier l'utilisation
www.netbsd.org
Catégorie d'URL
Commentaire
vpnssl_owa
antivirus_bypa...
authentication...
Caractères autorisés
Les caractères autorisés
Exemple d'URL : www.goo
CATÉGORIE D'URL : VPNS
Ajouter une URL
Supprimer
URL
schemas.microsoft.com/*
www.w3.org/TR/*
Page 1 sur
Catégorie(s) de l'URL : www.netbsd.org
it



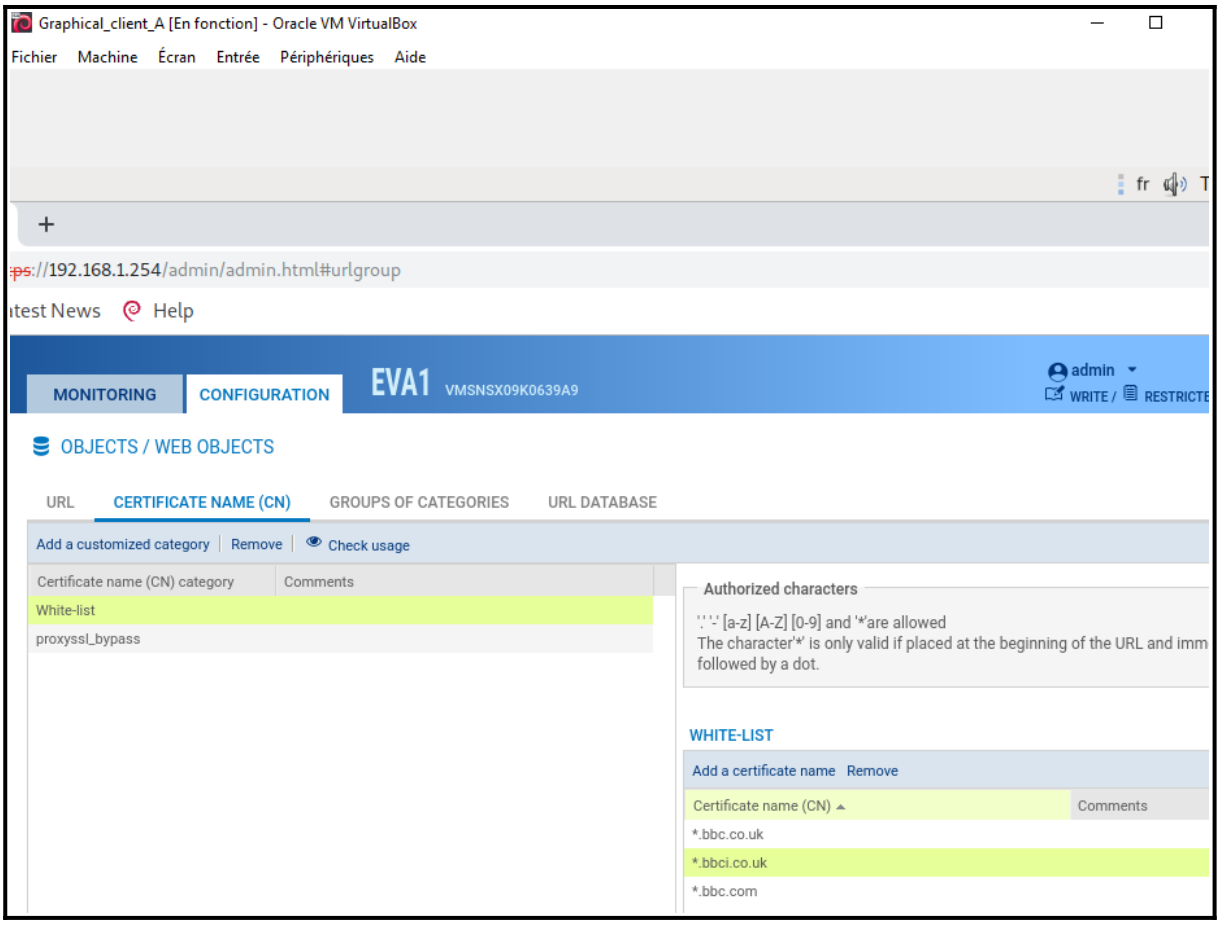
2ème étape : Nous vérifions la classification des URL ci-dessus.



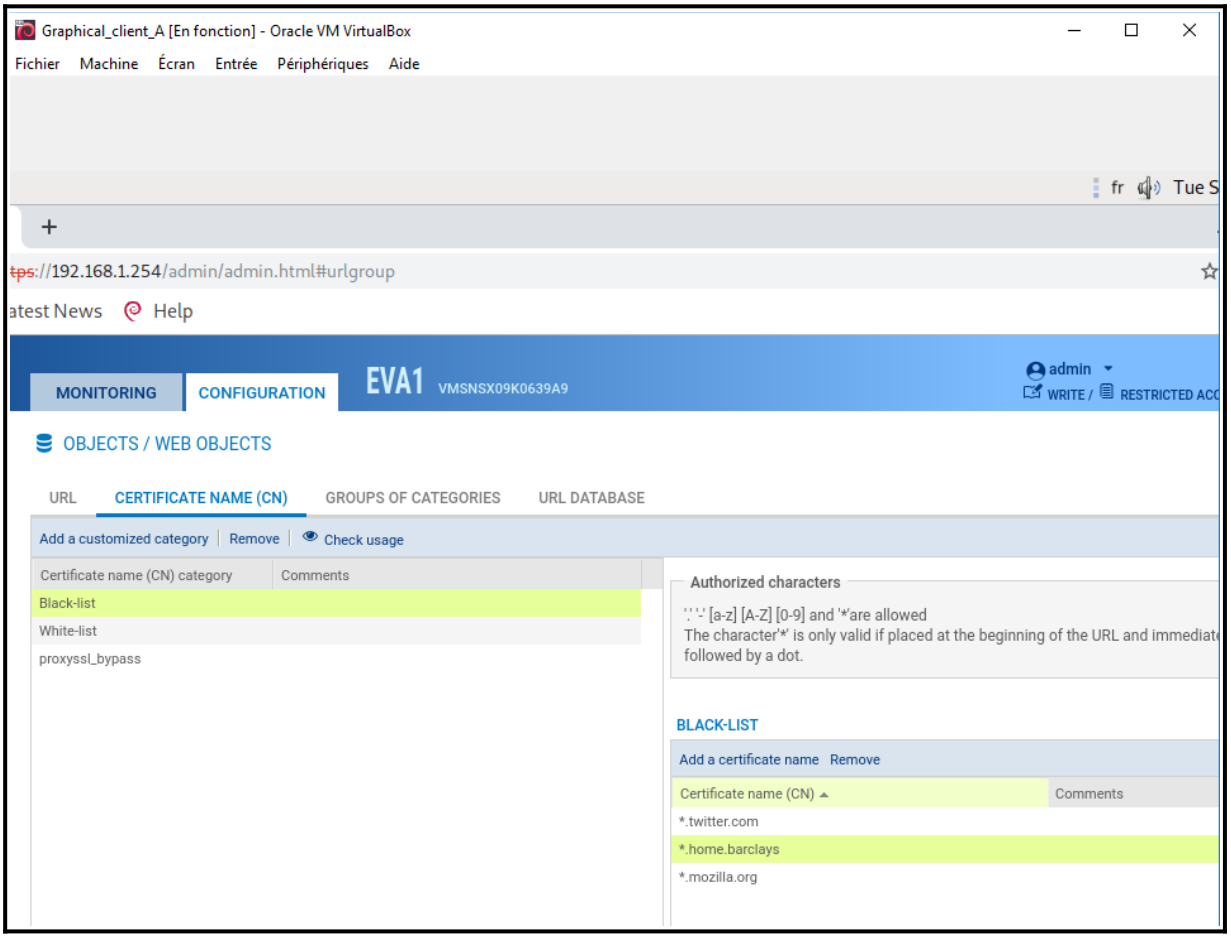
Access to this website is forbidden in accordance with the internet access policy of your company.

User: *$user*
Website: *$host$url*
Category: *$url_group*
link: Request access to this website

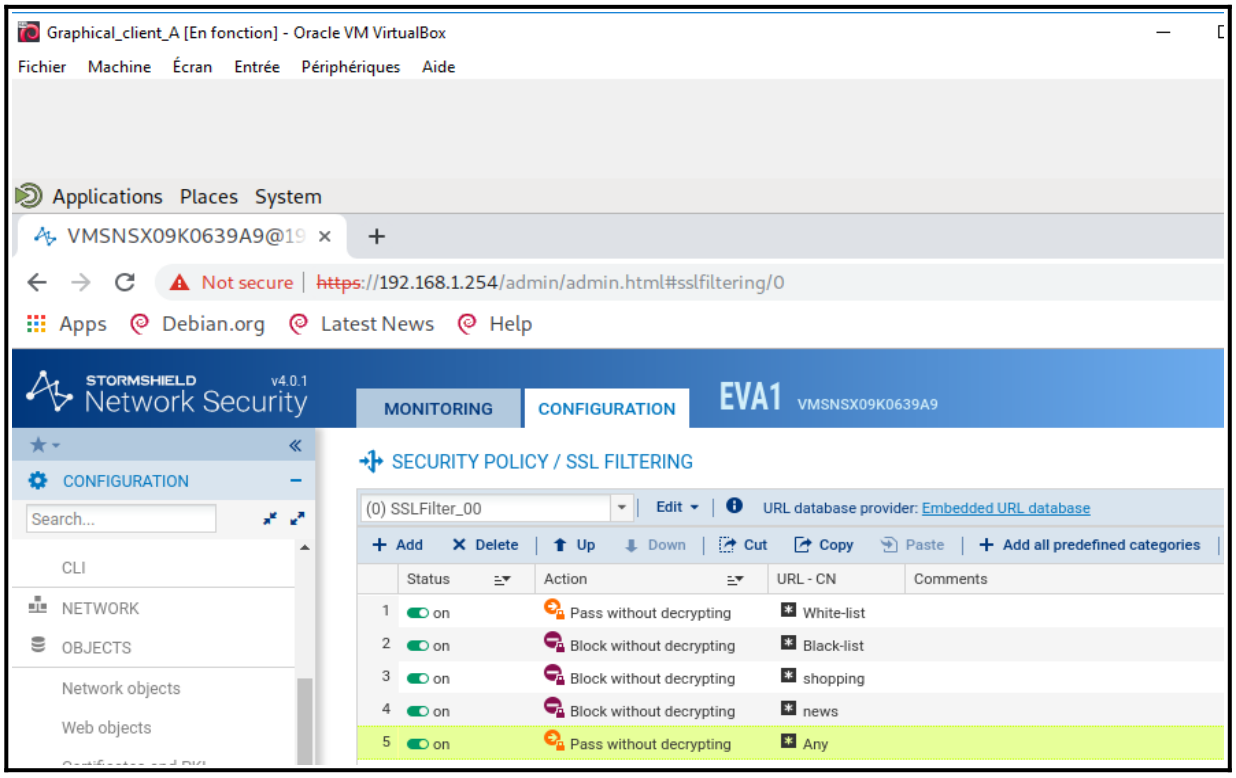
3ème étape : Nous modifions la page de blocage.



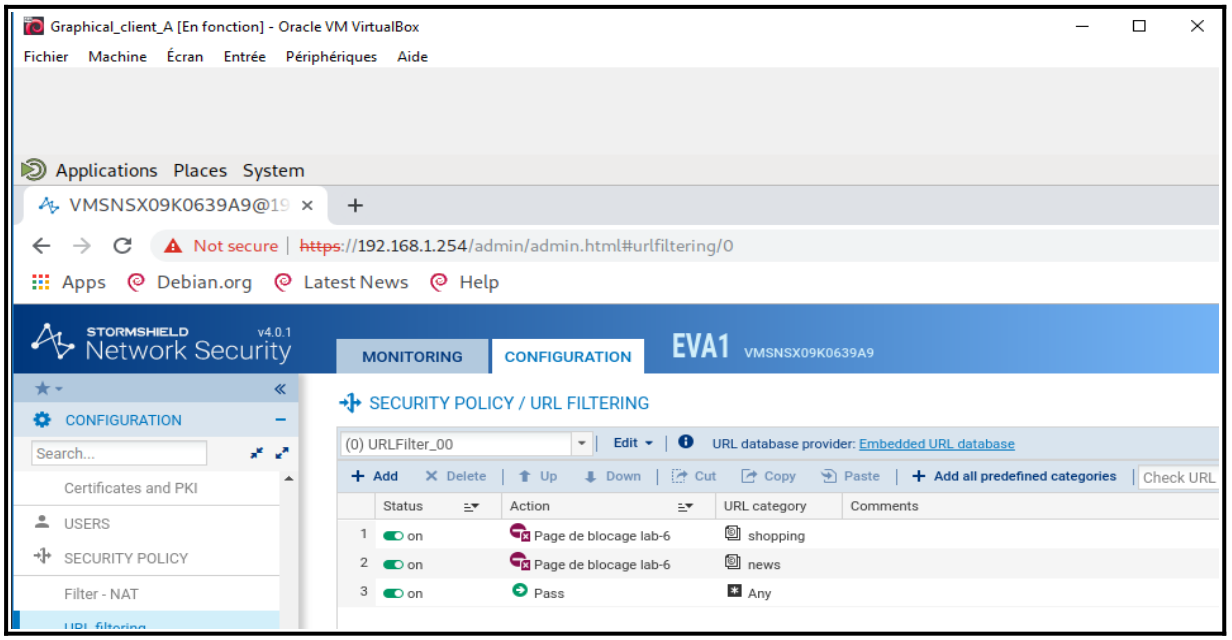
4ème étape : Création d'une catégorie White-list contenant les noms de certificat indiqués.



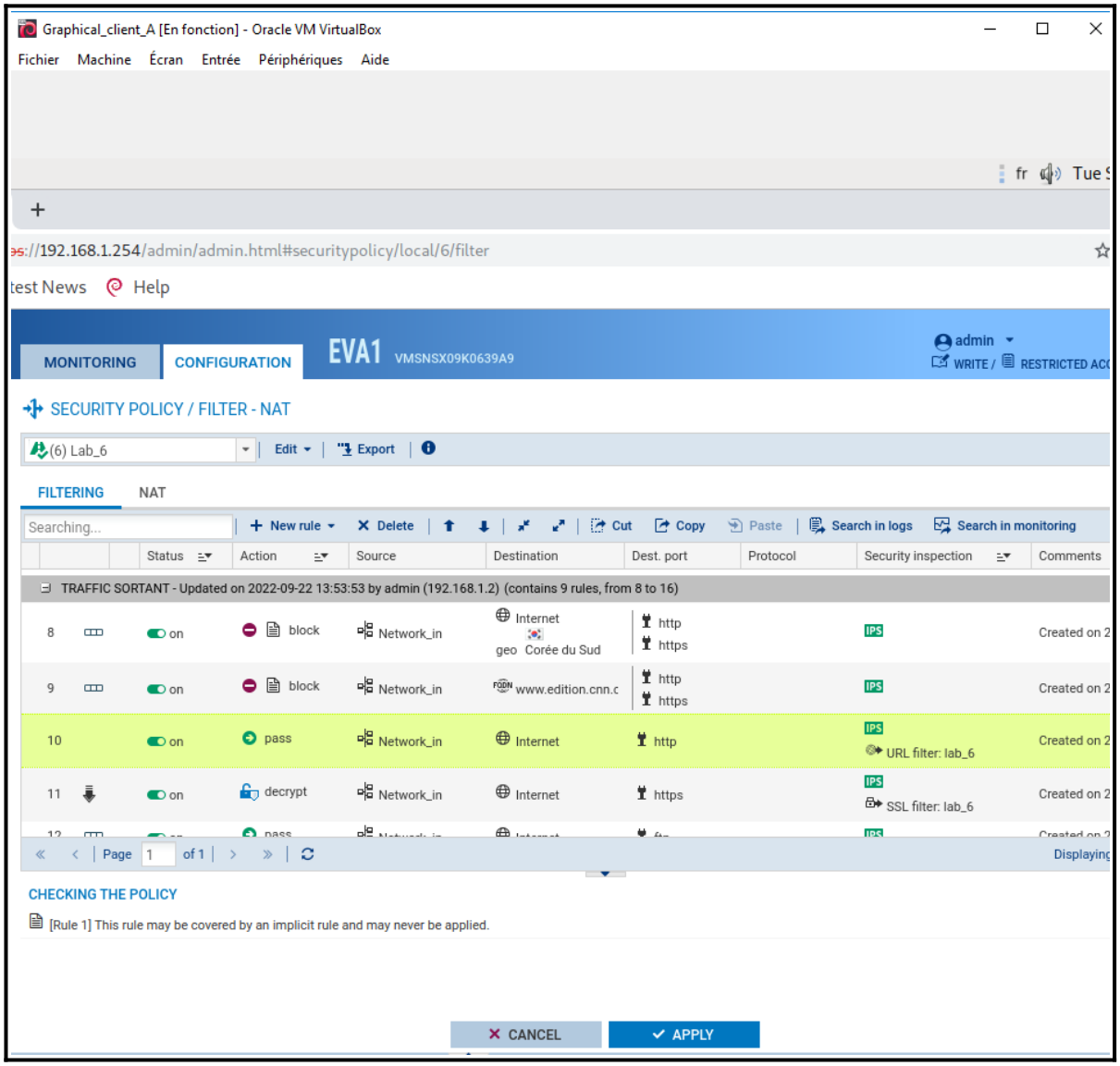
5ème étape : Création d'une catégorie Black-list contenant les noms de certificat indiqués.



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

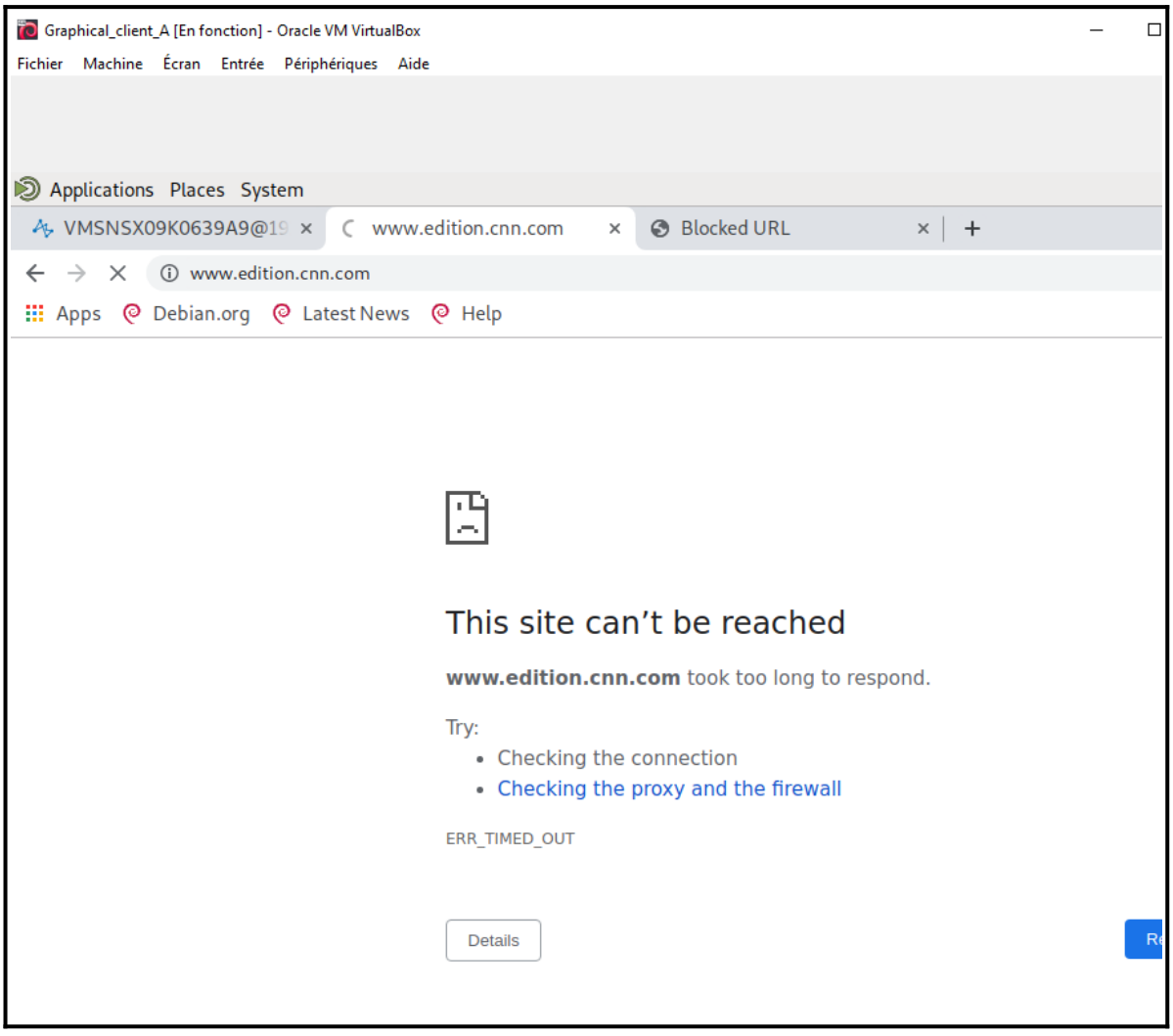


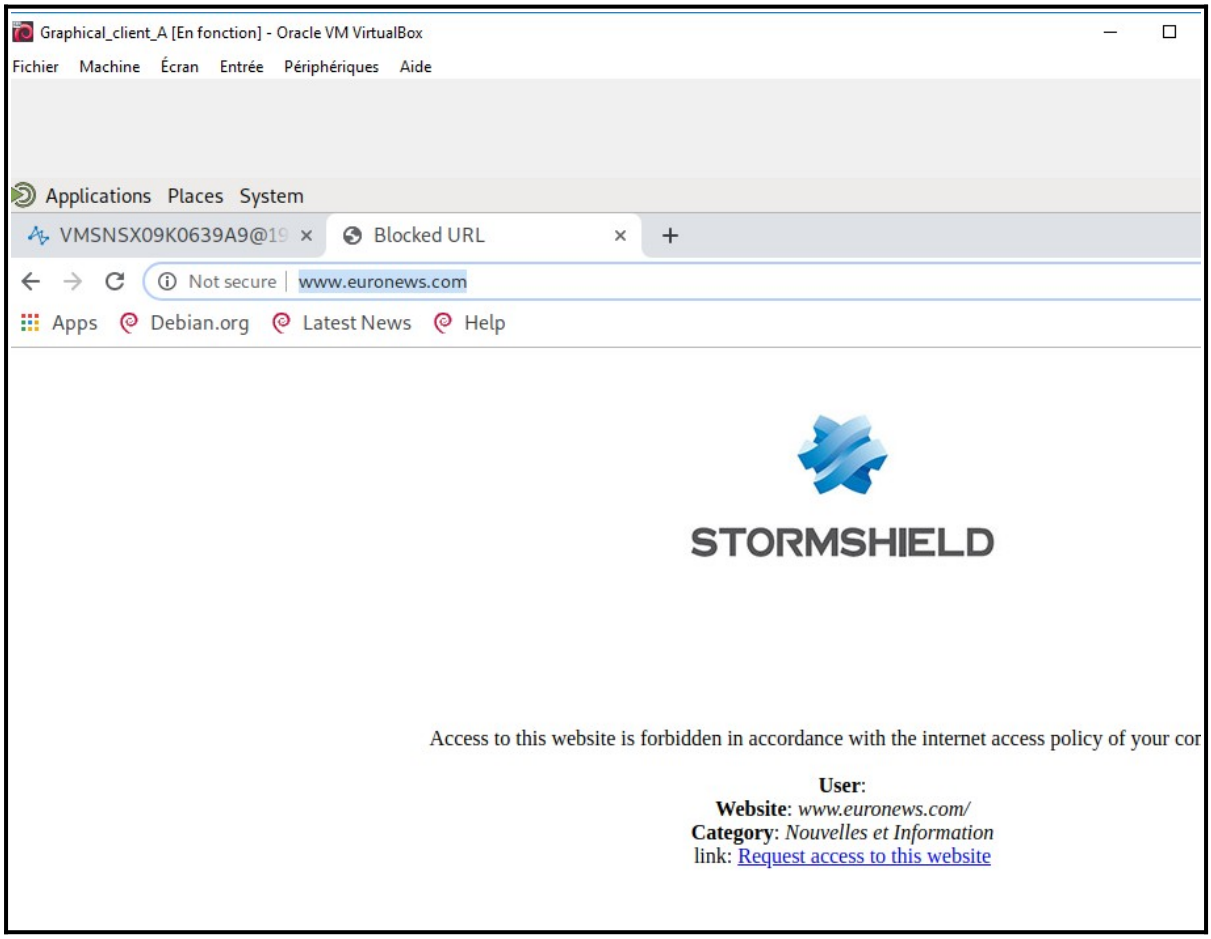
7ème étape : Nous modifions également le filtrage URL.

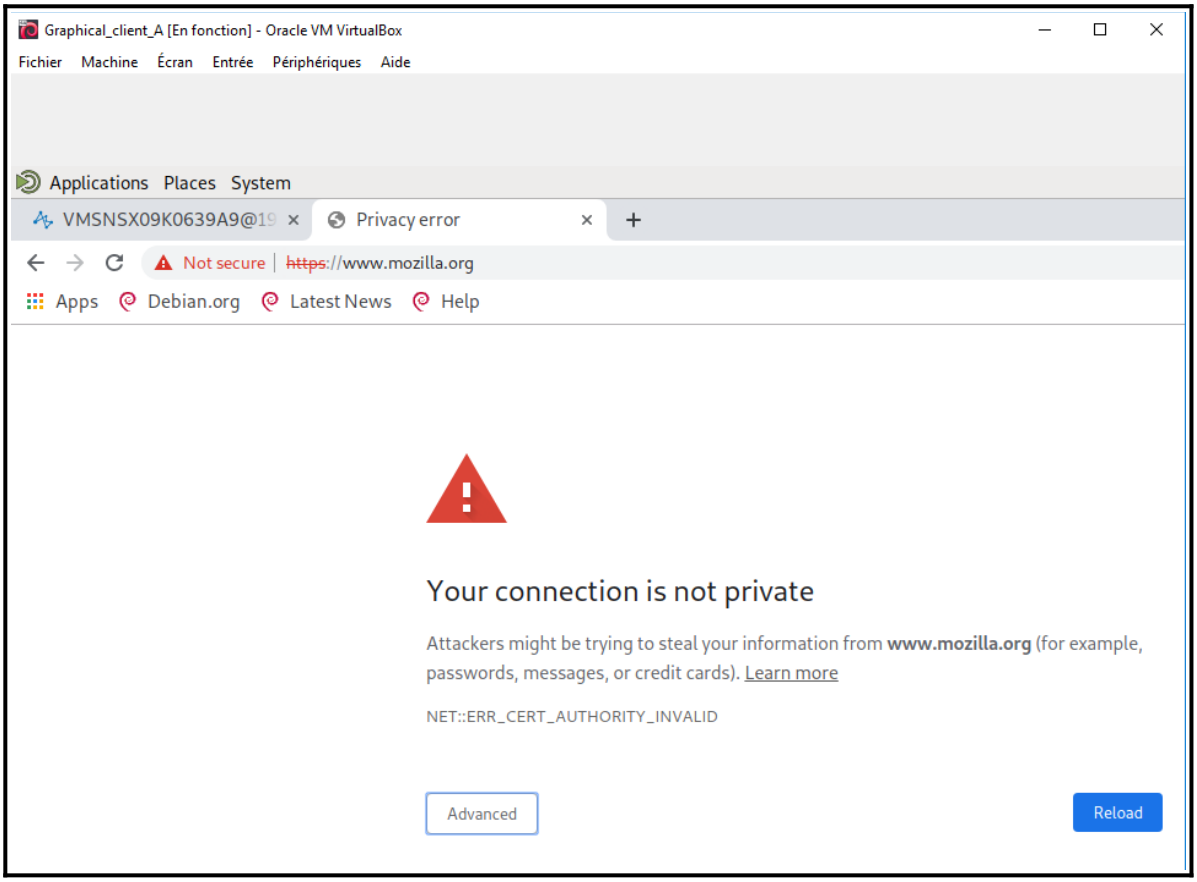


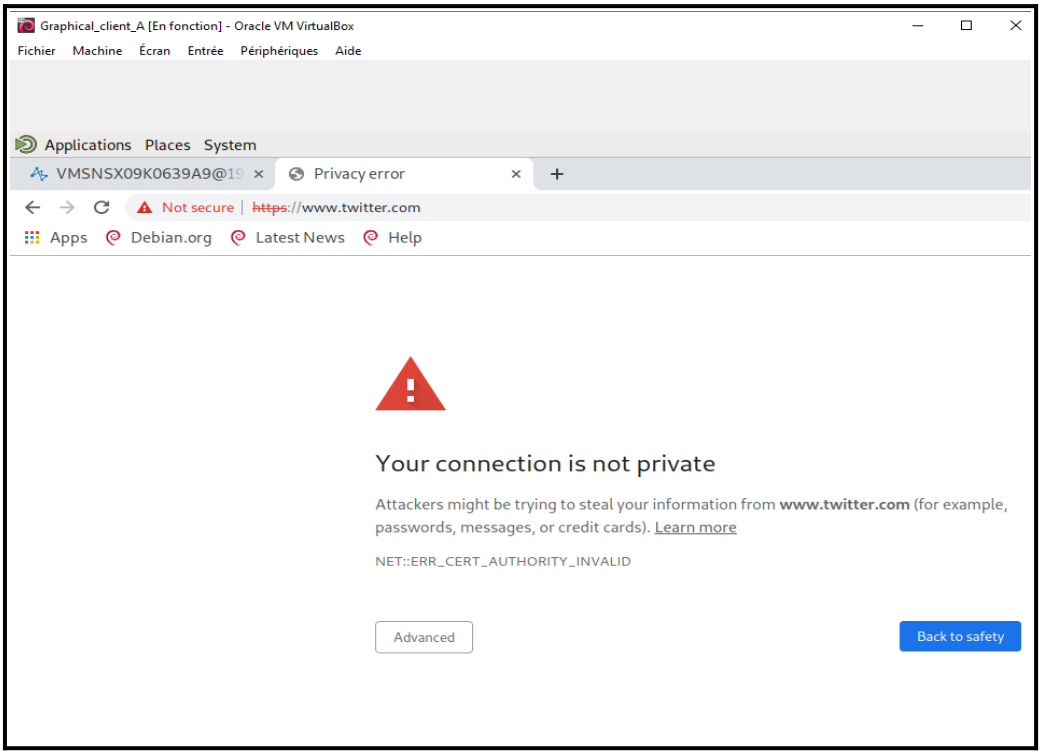
8ème étape : Nous modifions la politique de filtrage concernant les règles HTTP et HTTPS.

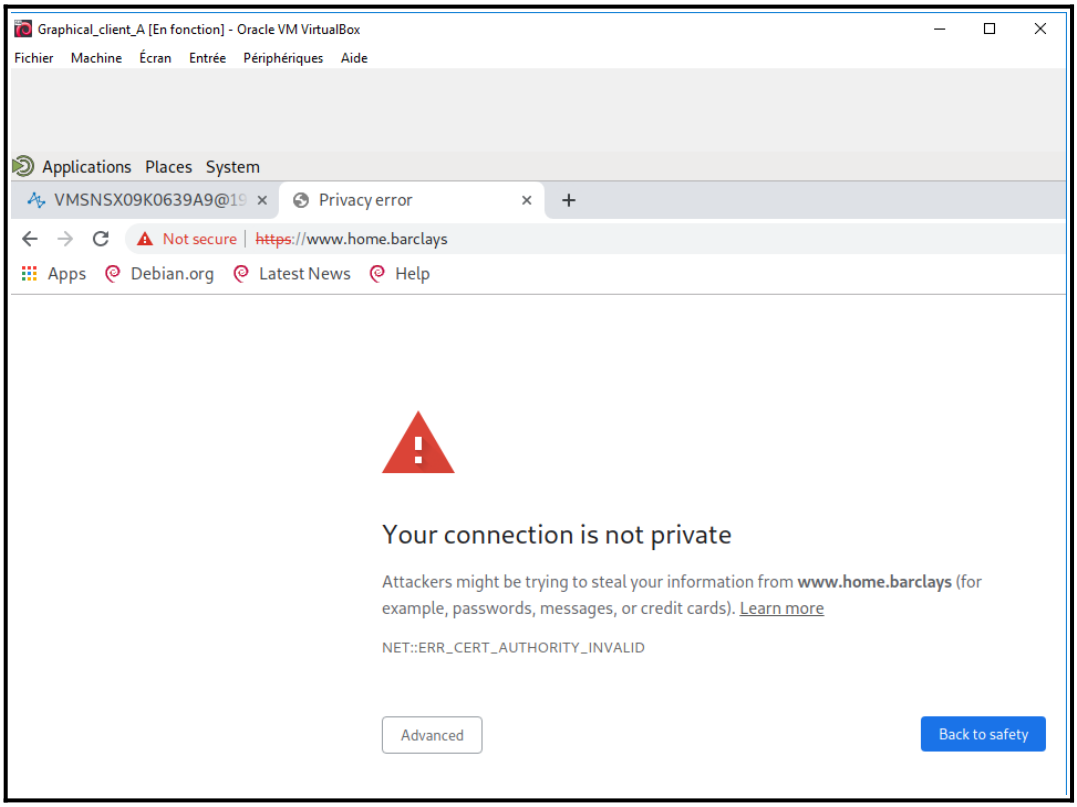

Graphical_client_A [En fonction] - Oracle VM VirtualBox
Fichier Machine Écran Entrée Périphériques Aide
Applications Places System
VMSNSX09K0639A9@19
New Tab
Blocked URL
Accueil | Académie de Nic
https://www.ac-nice.fr
Apps Debian.org Latest News Help
Translate this p
ACADÉMIE DE NICE
Liberté
Égalité
Fraternité
ac-nice.fr
Région académique Académie Scolarité Enseignements Concours-Métiers Politique Educative


Graphical_client_A [En fonction] - Oracle VM VirtualBox
Fichier Machine Écran Entrée Périphériques Aide
Applications Places System
VMSNSX09K0639A9@19
www.edition.cnn.com
Blocked URL
www.edition.cnn.com
Apps Debian.org Latest News Help
This site can’t be reached
www.edition.cnn.com took too long to respond.
Try:
Checking the connection
Checking the proxy and the firewall
ERR_TIMED_OUT
Details


Graphical_client_A [En fonction] - Oracle VM VirtualBox
Fichier Machine Écran Entrée Périphériques Aide
Applications Places System
VMSNSX09K0639A9@19
Blocked URL
Not secure | www.euronews.com
Apps Debian.org Latest News Help
STORMSHIELD
Access to this website is forbidden in accordance with the internet access policy of your cor
User:
Website: www.euronews.com/
Category: Nouvelles et Information
link: Request access to this website

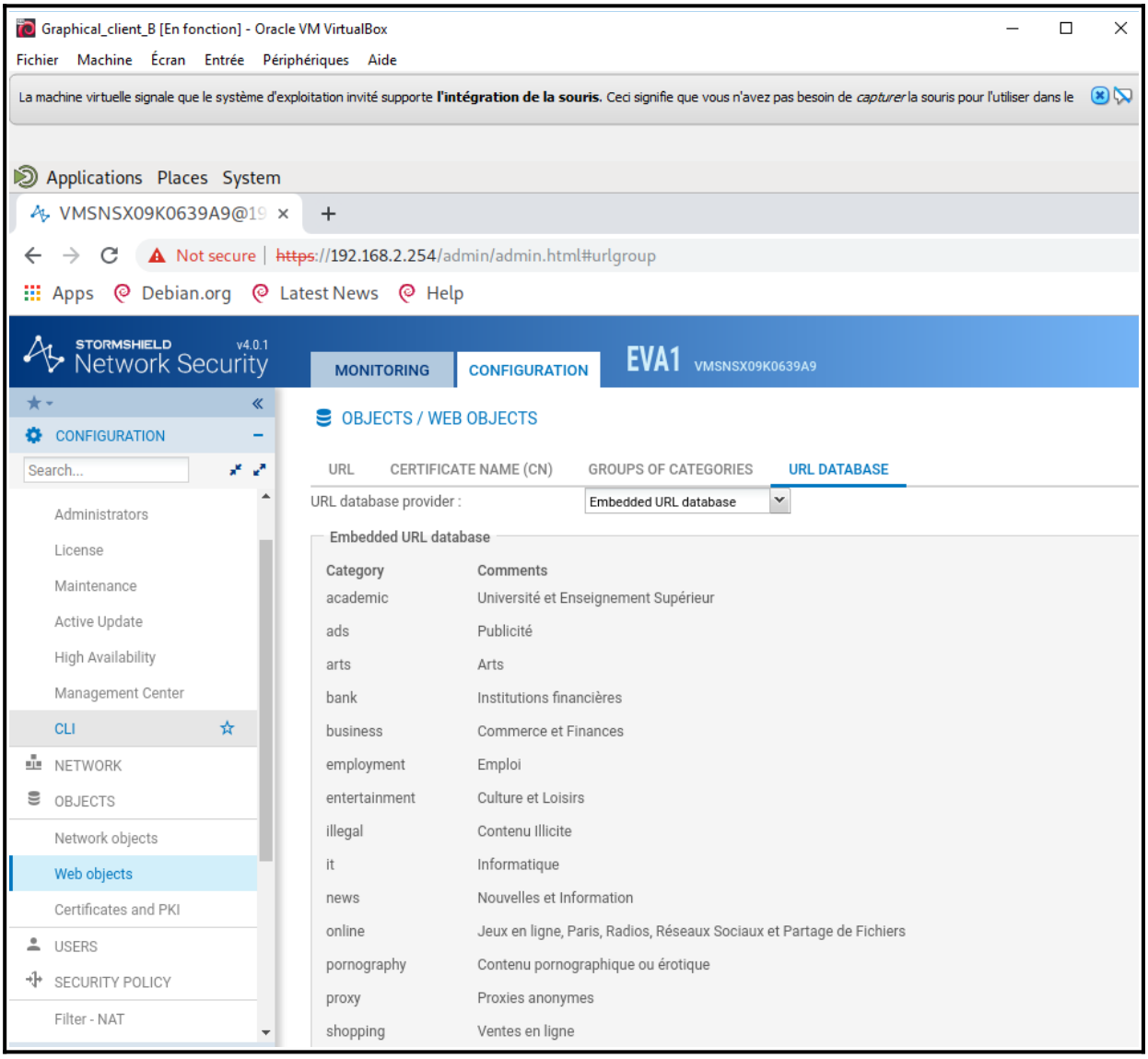

Graphical_client_A [En fonction] - Oracle VM VirtualBox
Fichier Machine Écran Entrée Périphériques Aide
Applications Places System
VMSNSX09K0639A9@19
Privacy error
Not secure | https://www.mozilla.org
Apps Debian.org Latest News Help
Your connection is not private
Attackers might be trying to steal your information from www.mozilla.org (for example, passwords, messages, or credit cards). Learn more
NET::ERR_CERT_AUTHORITY_INVALID
Advanced
Reload



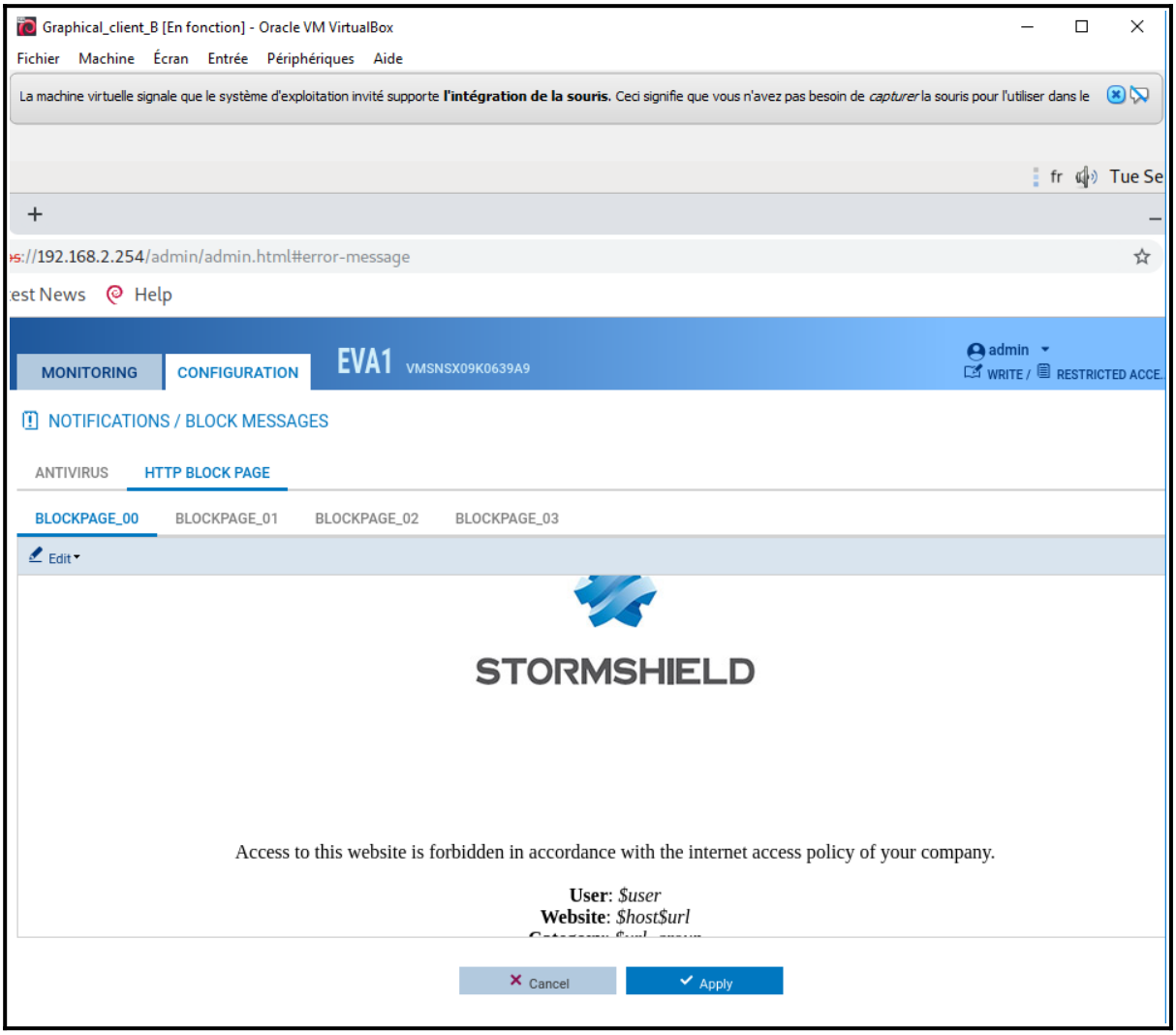


9ème étape : Nous effectuons nos différents tests afin de vérifier si tout fonctionne, seulement le site edition.cnn n'affiche pas la page de rejet du trafic SSL puisque celui-ci est déjà bloqué par une règle de filtrage avec un objet FQDN.

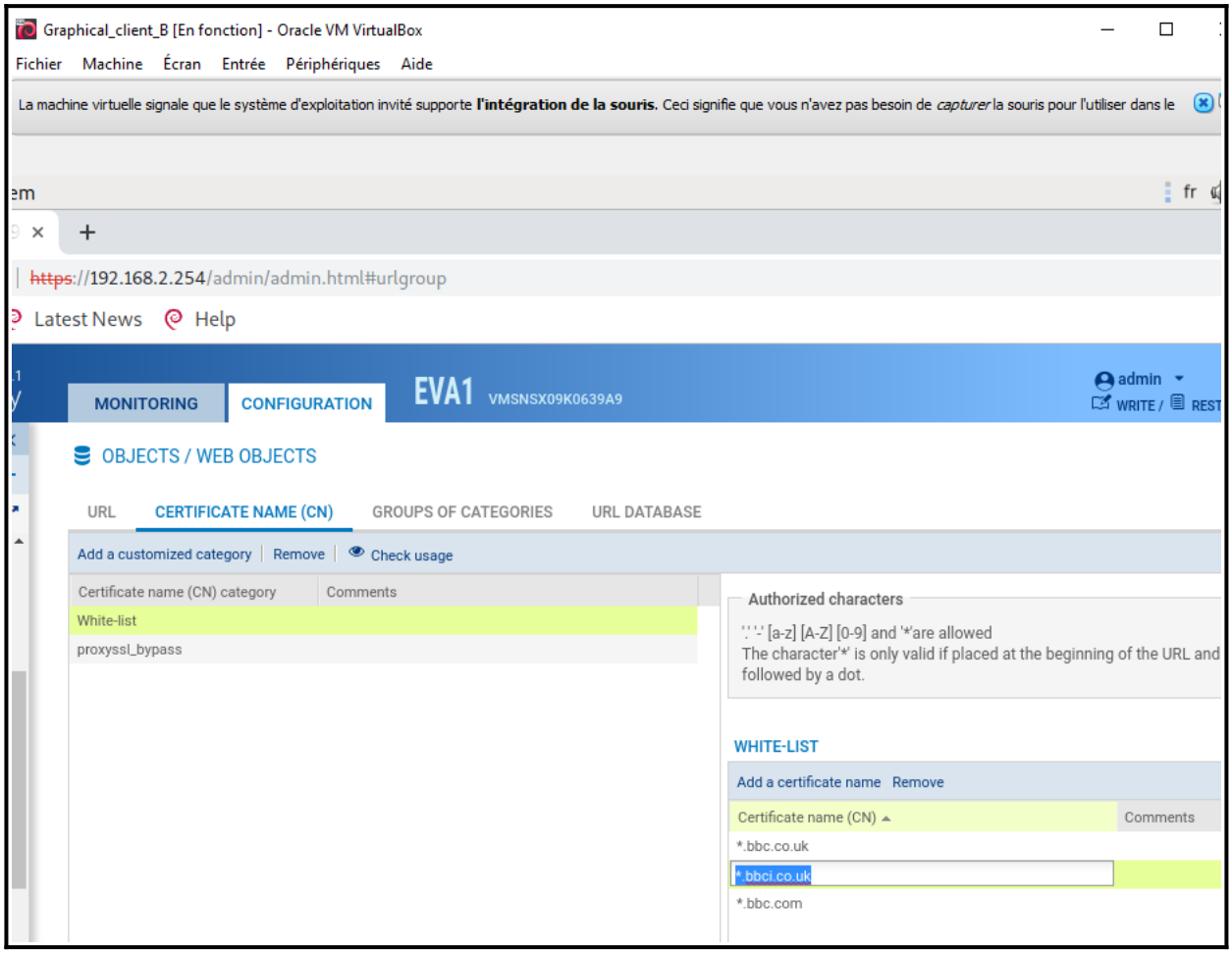
Réseau B :



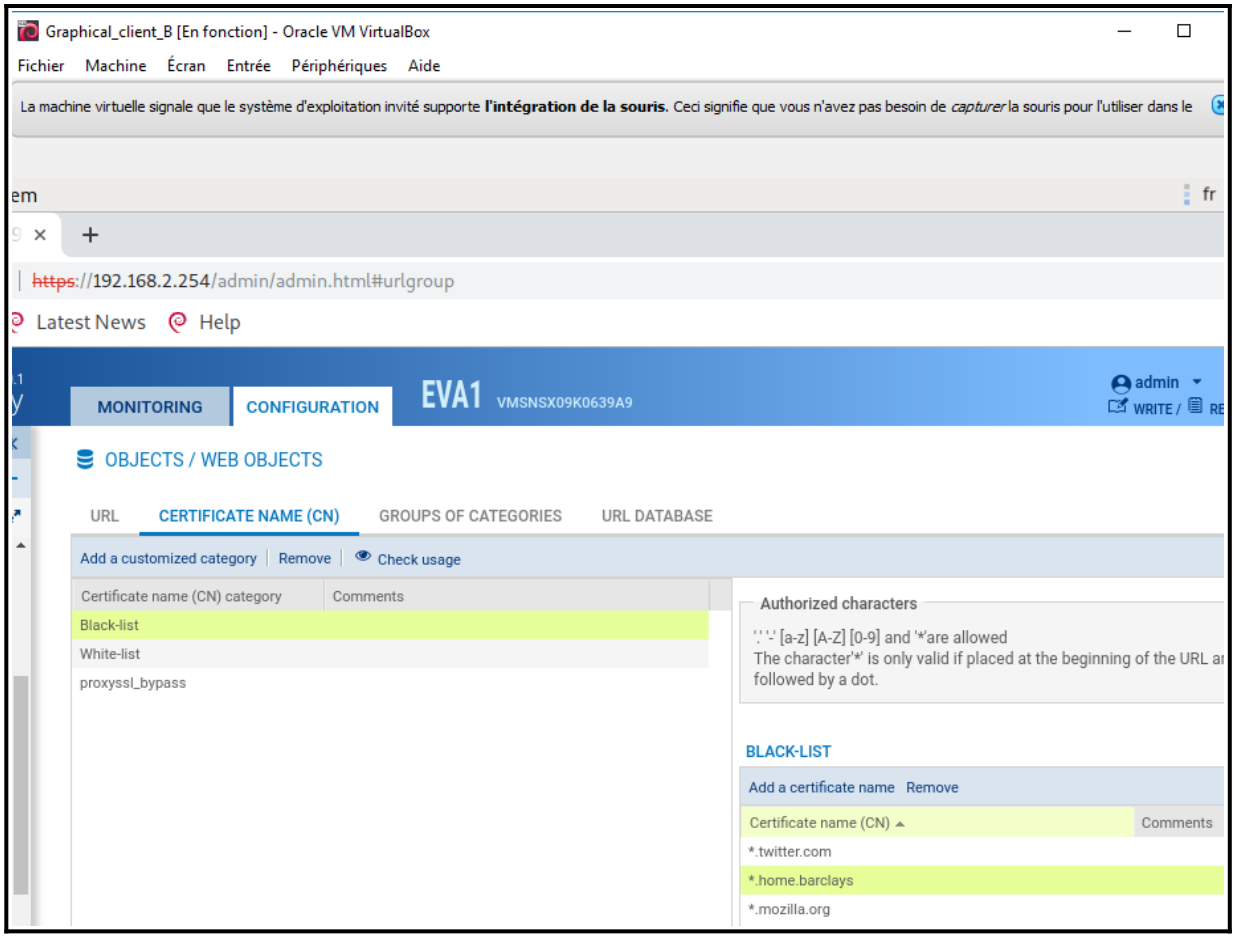
1ère étape : Nous sélectionnons la base d'URL embarquée dans les objets WEB.



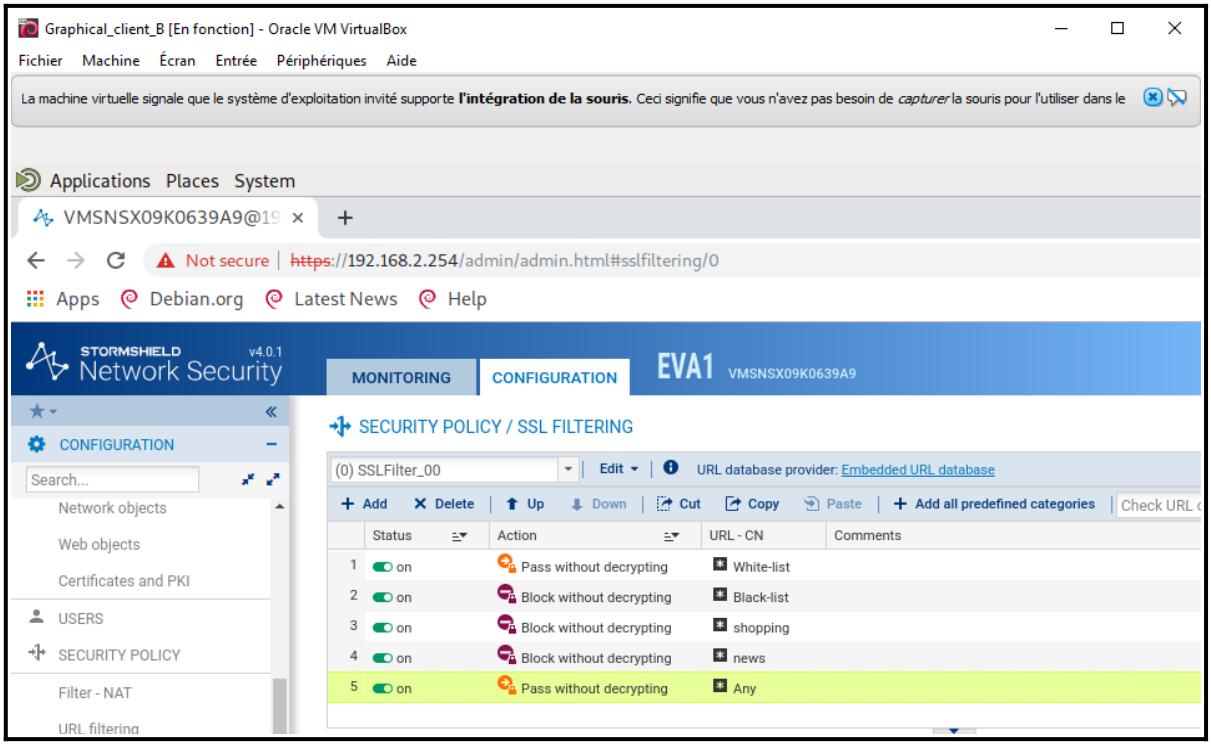
2ème étape : Nous modifions la page de blocage.



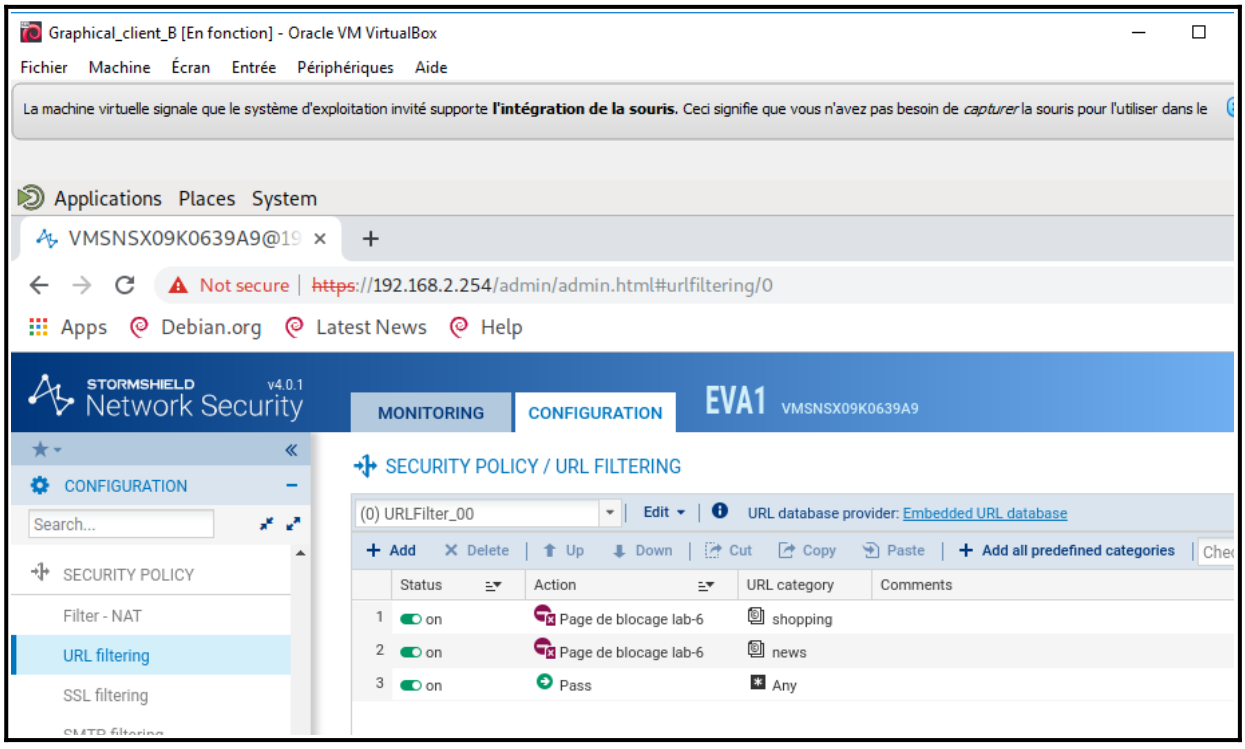
3ème étape : Création d'une catégorie White-list contenant les noms de certificat indiqués.



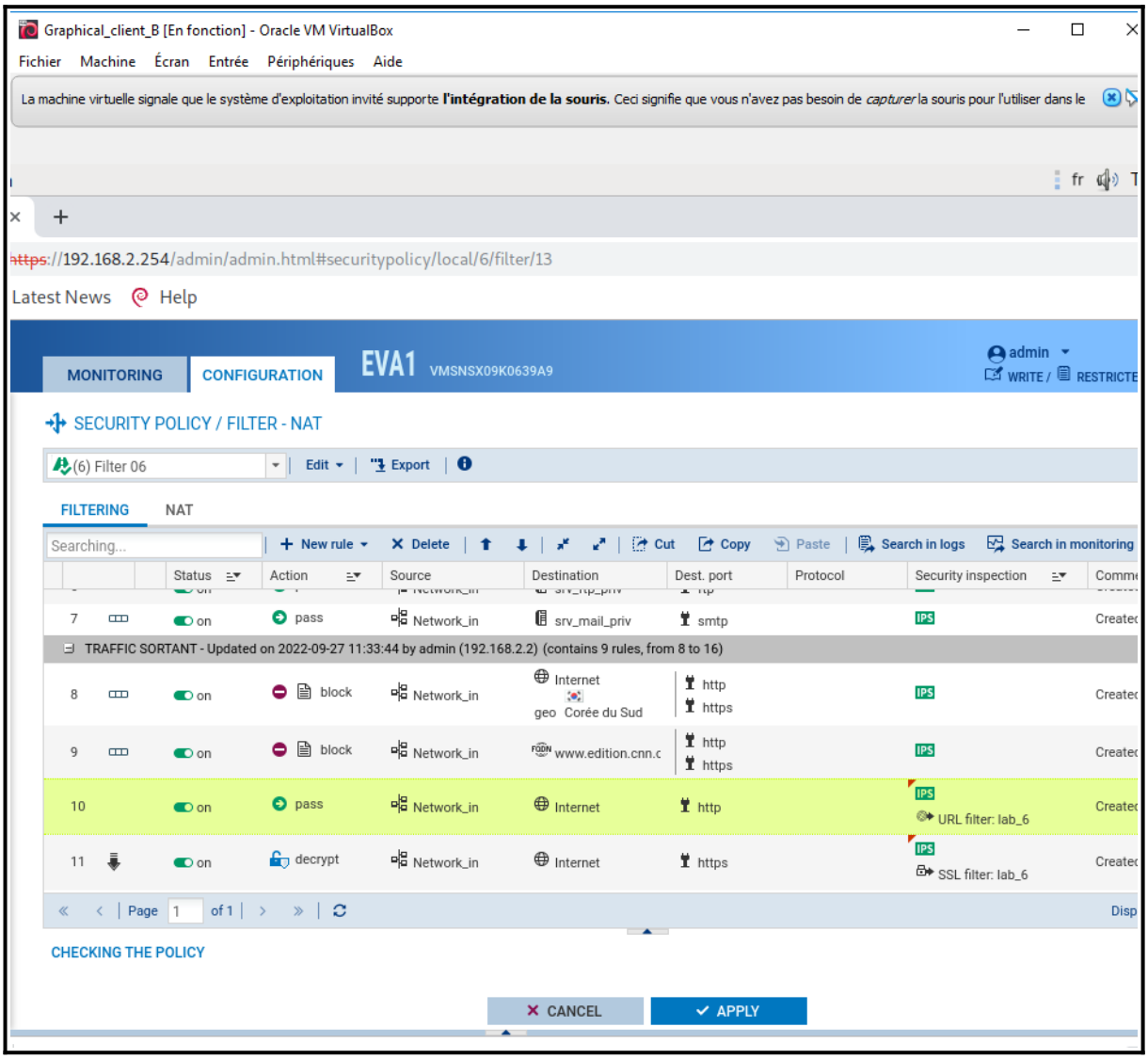
4ème étape : Création d'une catégorie Black-list contenant les noms de certificat indiqués.



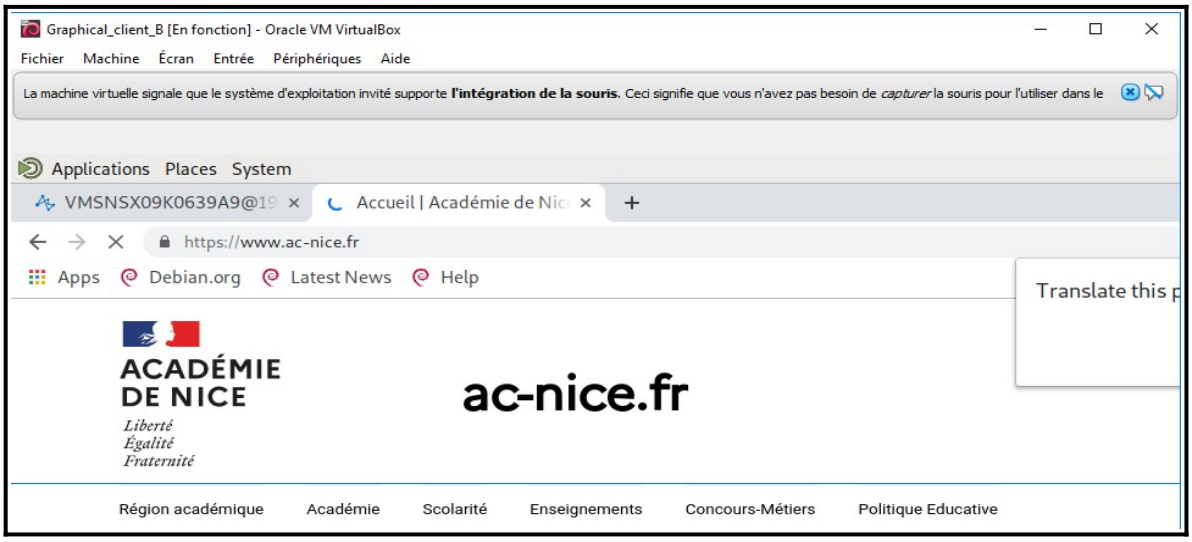
5ème étape : Nous modifions la politique de filtrage SSL en ajoutant nos nouvelles catégories.

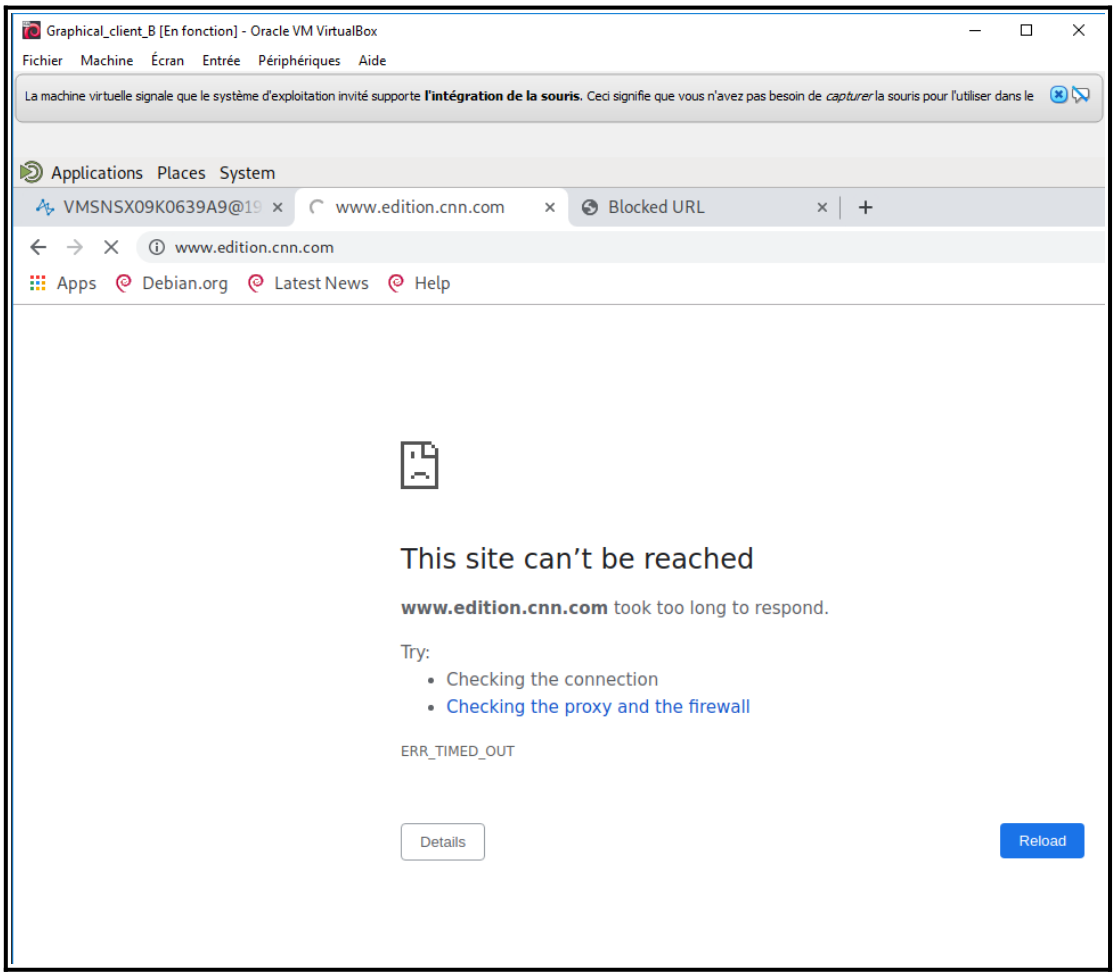


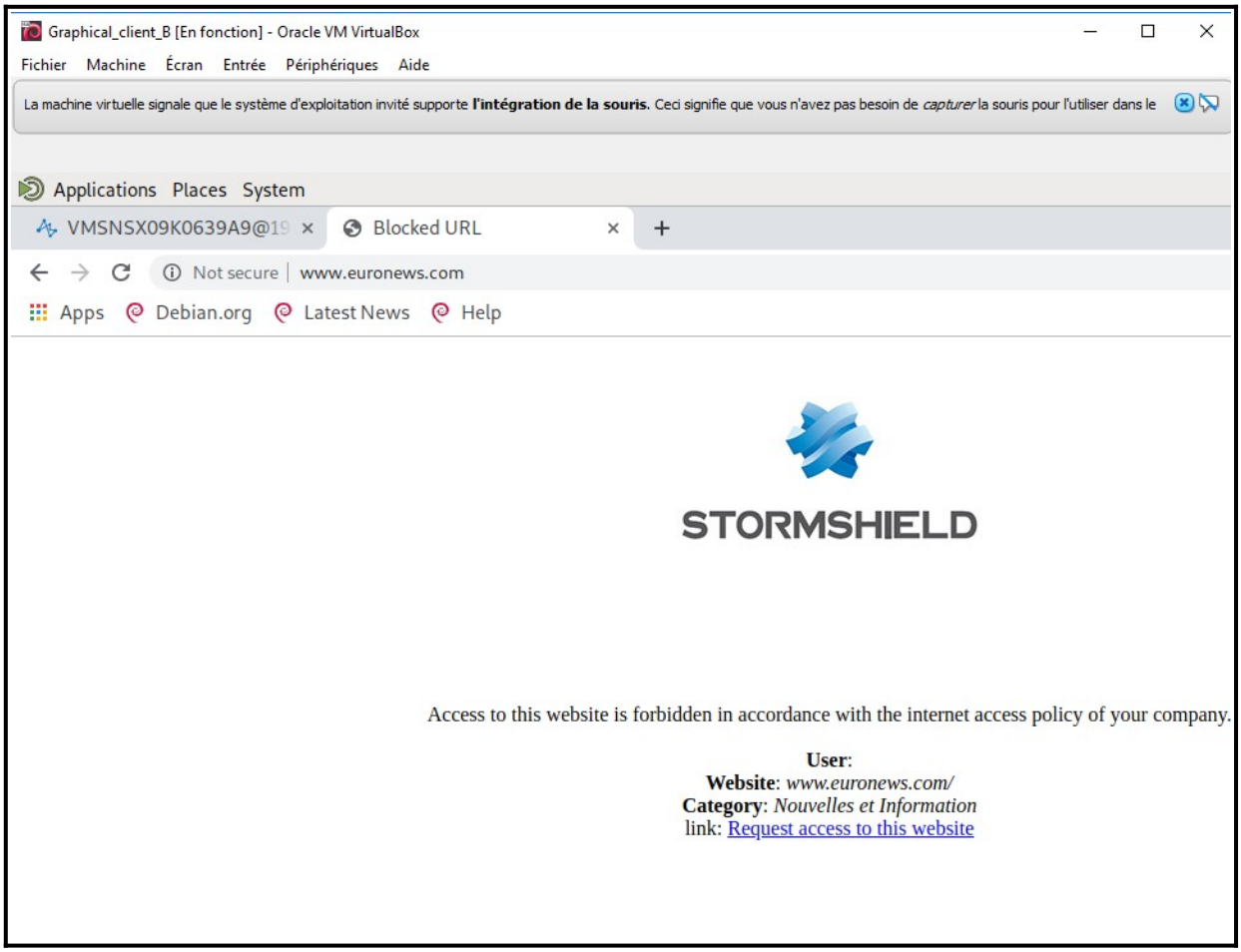
6ème étape : Nous modifions également le filtrage URL.

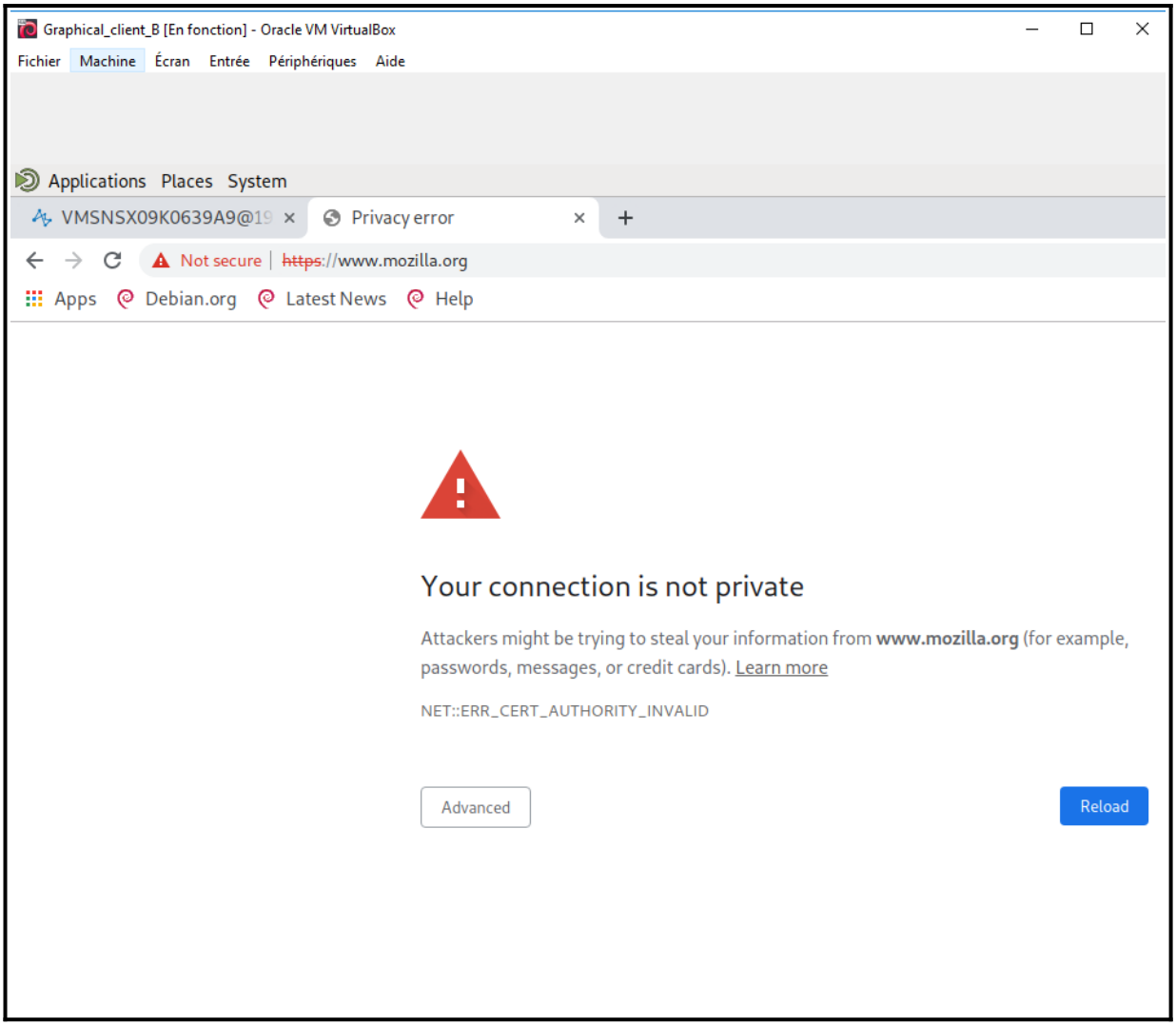


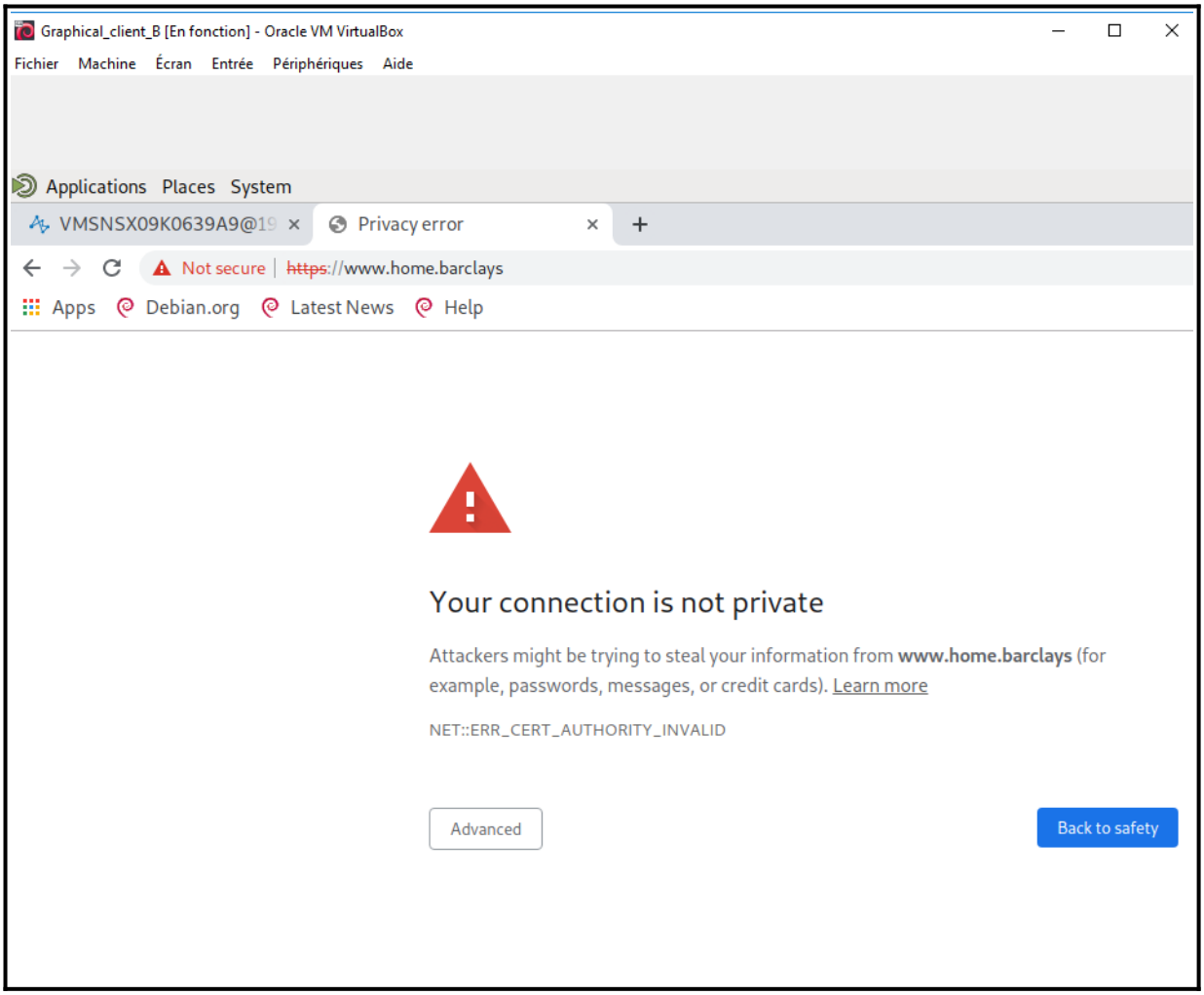
7ème étape : Nous modifions la politique de filtrage concernant les règles HTTP et HTTPS.

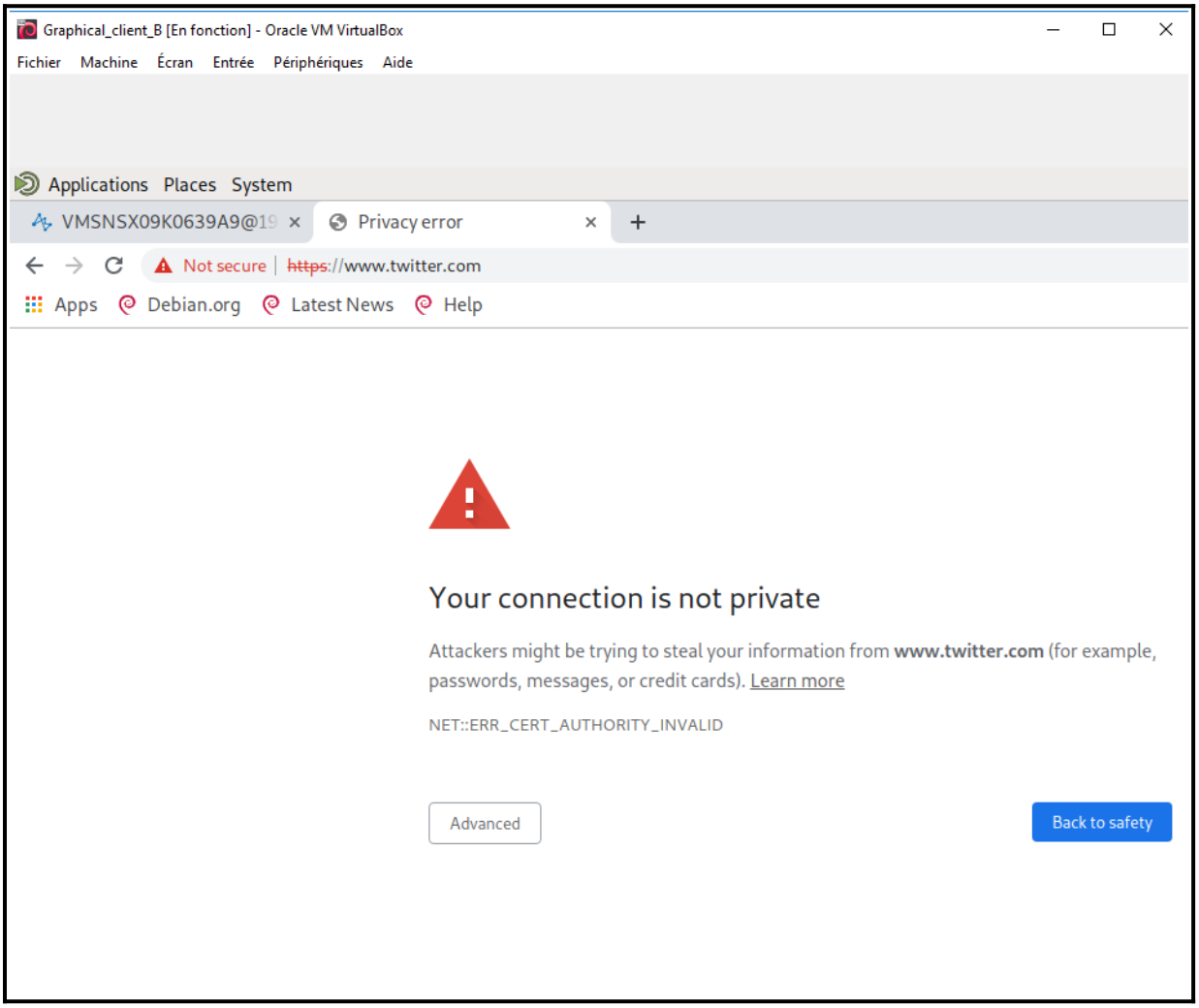

Graphical_client_B [En fonction] - Oracle VM VirtualBox
Fichier Machine Écran Entrée Périphériques Aide
La machine virtuelle signale que le système d'exploitation invité supporte l'intégration de la souris. Ceci signifie que vous n'avez pas besoin de capturer la souris pour l'utiliser dans le
Applications Places System
VMSNSX09K0639A9@19
Accueil | Académie de Nic
https://www.ac-nice.fr
Apps Debian.org Latest News Help
Translate this p
ACADÉMIE DE NICE
Liberté
Égalité
Fraternité
ac-nice.fr
Région académique Académie Scolarité Enseignements Concours-Métiers Politique Educative


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
Applications Places System
VMSNSX09K0639A9@19
www.edition.cnn.com
Blocked URL
www.edition.cnn.com
Apps Debian.org Latest News Help
This site can't be reached
www.edition.cnn.com took too long to respond.
Try:
Checking the connection
Checking the proxy and the firewall
ERR_TIMED_OUT
Details
Reload


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
Applications Places System
VMSNSX09K0639A9@19
Blocked URL
Not secure | www.euronews.com
Apps Debian.org Latest News Help
STORMSHIELD
Access to this website is forbidden in accordance with the internet access policy of your company.
User:
Website: www.euronews.com/
Category: Nouvelles et Information
link: Request access to this website


Graphical_client_B [En fonction] - Oracle VM VirtualBox
Fichier Machine Écran Entrée Périphériques Aide
Applications Places System
VMSNSX09K0639A9@19
Privacy error
Not secure | https://www.mozilla.org
Apps Debian.org Latest News Help
Your connection is not private
Attackers might be trying to steal your information from www.mozilla.org (for example, passwords, messages, or credit cards). Learn more
NET::ERR_CERT_AUTHORITY_INVALID
Advanced
Reload


Graphical_client_B [En fonction] - Oracle VM VirtualBox
Fichier Machine Écran Entrée Périphériques Aide
Applications Places System
VMSNSX09K0639A9@19
Privacy error
Not secure | https://www.home.barclays
Apps Debian.org Latest News Help
Your connection is not private
Attackers might be trying to steal your information from www.home.barclays (for example, passwords, messages, or credit cards). Learn more
NET::ERR_CERT_AUTHORITY_INVALID
Advanced
Back to safety



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.