

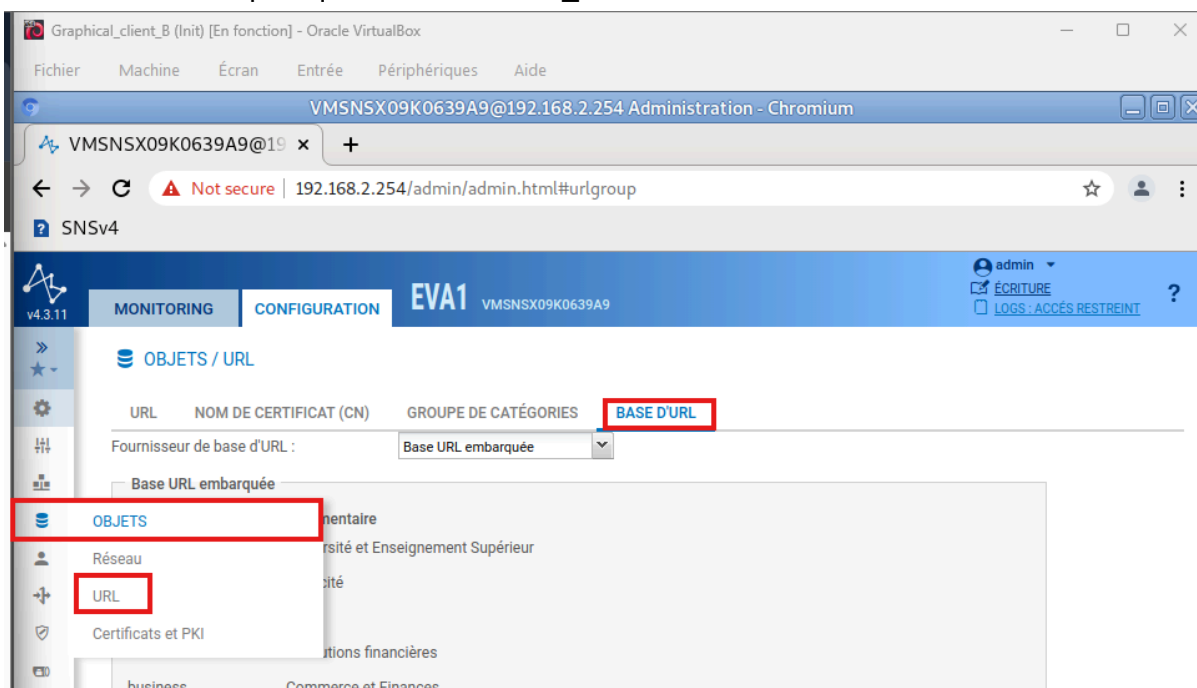
Lab 6 – Filtrage de contenu (HTTP et HTTPS)

Table des matières :

1. Copie et activation de la politique Lab_6.....	2
2. Identification des catégories des sites.....	3
3. Mise en place du filtrage URL et SSL.....	5
4. Test d'accès et analyse du comportement de blocage.....	7

1. Copie et activation de la politique Lab_6

- Dans un premier temps, nous avons copié la politique de filtrage/NAT du Lab 5 afin de créer une nouvelle politique nommée « Lab_6 ».



2. Identification des catégories des sites

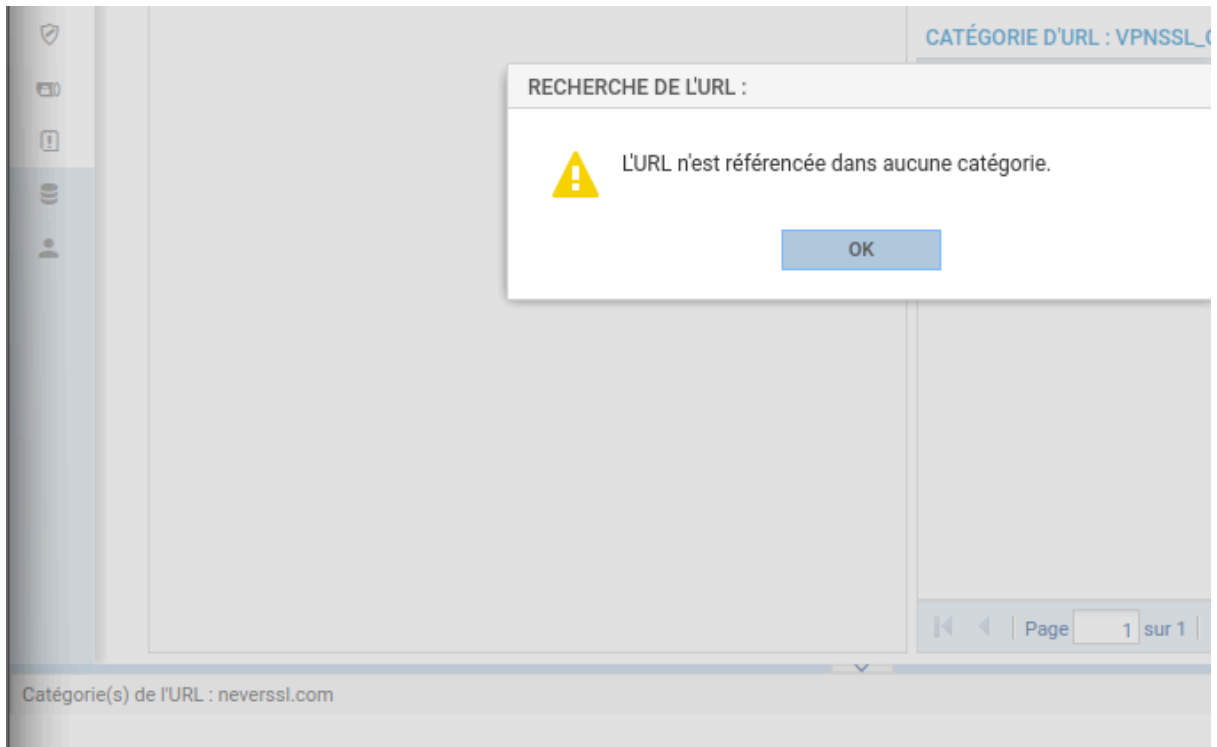
▪ Ensuite, j'ai utilisé la base d'URL embarquée pour rechercher les catégories des sites suivants :

- twitter.com
- www.netbsd.org
- www.mozilla.org
- neverssl.com

The screenshot shows the StormShield administration interface in a Chromium browser. The URL bar shows `192.168.1.254/admin/admin.html#urlgroup`. The interface is in the 'CONFIGURATION' section, specifically the 'OBJETS / URL' tab. A search bar contains 'twitter.com' and a 'Classifier' button is visible. Below the search bar, a table lists categories with columns for 'Catégorie d'UR...', 'Commentaire', and 'BASE D'URL'. The 'twitter.com' entry is highlighted in green. A sidebar on the left shows a navigation menu with icons for various functions. At the bottom of the interface, a status bar indicates 'Catégorie(s) de l'URL : twitter.com' and 'online'.

The screenshot shows the StormShield interface displaying the classification result for the URL `www.netbsd.org`. The status bar indicates 'Catégorie(s) de l'URL : www.netbsd.org' and the classification is 'it'.

The screenshot shows the StormShield interface displaying the classification result for the URL `www.mozilla.org`. The status bar indicates 'Catégorie(s) de l'URL : www.mozilla.org' and the classification is 'it'.



3. Mise en place du filtrage URL et SSL

▪ Nous avons configuré une politique de filtrage URL ainsi qu'une politique de filtrage SSL afin de bloquer :

- les sites listés au point 2,
- les sites appartenant aux catégories « shopping » et « news ».

URL **NOM DE CERTIFICAT (CN)** GROUPE DE CATÉGORIES BASE D'URL

Ajouter une catégorie personnalisée | Supprimer | Vérifier l'utilisation

Catégorie de noms de certificat (CN)	Commentaire
Black-list	
White-list	
proxysl_bypass	

Caractères autorisés

Les caractères autorisés sont : ' ' [a-z] [A-Z] [0-9] et '*'
Le caractère '*' n'est valide que s'il est placé en début d'URL et immédiatement suivi d'un point.

CATÉGORIE DE CERTIFICATS : WHITE-LIST

Ajouter un nom de certificat | Supprimer

Nom de certificat (CN) ▲	Commentaire
*.bbc.co.uk	
*.bbc.com	
*.bbci.co.uk	

URL **NOM DE CERTIFICAT (CN)** GROUPE DE CATÉGORIES BASE D'URL

Ajouter une catégorie personnalisée | Supprimer | Vérifier l'utilisation

Catégorie de noms de certificat (CN)	Commentaire
Black-list	
White-list	
proxysl_bypass	

Caractères autorisés

Les caractères autorisés sont : ' ' [a-z] [A-Z] [0-9] et '*'
Le caractère '*' n'est valide que s'il est placé en début d'URL et immédiatement suivi d'un point.

CATÉGORIE DE CERTIFICATS : BLACK-LIST

Ajouter un nom de certificat | Supprimer

Nom de certificat (CN) ▲	Commentaire
*.mozilla.org	
*.x.com	

v4.3.11 MONITORING CONFIGURATION EVA1 VMSNSX09K0639A9 ECRITURE LOGS : ACCÈS RESTREINT ?

POLITIQUE DE SÉCURITÉ / FILTRAGE SSL

(0) SSLFilter_00 | Editer | Fournisseur de base URL : Base URL embarquée

+ Ajouter | X Supprimer | ↑ Monter | ↓ Descendre | Couper | Copier | Coller | + Ajouter toutes les catégories prédéfinies | Vérifier

État	Action	URL - CN	Commentaire
1 <input checked="" type="checkbox"/> on	Passer sans déchiffrer	White-list	
2 <input checked="" type="checkbox"/> on	Bloquer sans déchiffrer	Black-list	
3 <input checked="" type="checkbox"/> on	Bloquer sans déchiffrer	shopping	
4 <input checked="" type="checkbox"/> on	Bloquer sans déchiffrer	news	
5 <input checked="" type="checkbox"/> on	Passer sans déchiffrer	Any	

Graphical_client_A (Init) [En fonction] - Oracle VirtualBox

Fichier Machine Écran Entrée Périphériques Aide

BBC Home - Breaking News, World News, US News, Sports, Business, Innovation, Climate, Culture, Travel, Video & Audio - Chrome


VMSNSX09K0639A9@19 x BBC Home - Breaking News x +

← → ↻ 🔒 bbc.com ☆ 👤 ⋮

SNSv4

≡ Q


B B C Register Sign In



Moldova's pro-EU party wins vote mired in claims of Russian interference

The election was seen as critical for Moldova's EU path, and President Maia Sandu warned the country's future was in danger.

52 mins ago | Europe



Death toll rises to four after Michigan church

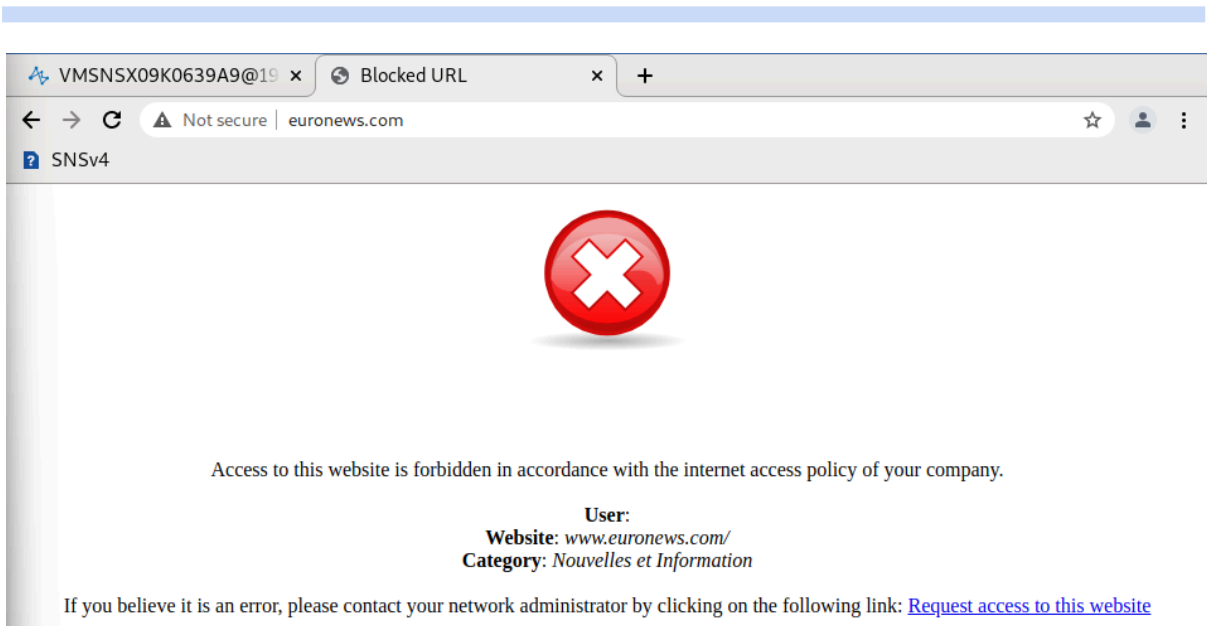
4. Test d'accès et analyse du comportement de blocage

- Dans cette partie, j'ai testé l'accès au site cnn.com, puis à euronews.com.
 - Pour cnn.com, aucune page de rejet SSL ne s'affiche car le site est déjà bloqué par une règle antérieure basée sur un objet FQDN.
 - En revanche, pour euronews.com, la page de blocage apparaît correctement lorsqu'on tente d'y accéder via HTTP, et le filtrage SSL intervient pour les connexions HTTPS.

The image shows two screenshots. The top one is a firewall rule configuration table for 'Outgoing traffic'. The bottom one is a browser error page for 'cnn.com'.

Rule ID	Status	Action	Source	Destination	Ports	Filter
8	on	bloquer	Network_in	Internet geo Corée du Sud	http, https	IPS
9	on	bloquer	Network_in	www.cnn.com	https, http	IPS
10	on	passer	Network_in	Internet	http	IPS, Filtrage URL : URLFilt
11	on	déchiffrer	Network_in	Internet	https	IPS, Filtrage SSL : SSLFilt
12	on	passer	Network_in	Internet	ftp	IPS

The browser screenshot shows an error page for 'cnn.com' with the message: 'This site can't be reached. cnn.com took too long to respond. Try: • Checking the connection • Checking the proxy and the firewall. ERR_TIMED_OUT. There are 'Details' and 'Reload' buttons at the bottom.



The screenshot shows a web browser window with the following details:

- Address bar: [VMNSX09K0639A9@19](#) x [Blocked URL](#) x +
- Page title: Not secure | euronews.com
- Page content: A large red circle with a white 'X' in the center, indicating a blocked URL.
- Message: Access to this website is forbidden in accordance with the internet access policy of your company.
- Metadata:
 - User:**
 - Website:** www.euronews.com/
 - Category:** *Nouvelles et Information*
- Footer: If you believe it is an error, please contact your network administrator by clicking on the following link: [Request access to this website](#)