

Proxy (SNS)

Prérequis :

- Un SNS Stormshield physique ou virtualisé.

Résumé :

- On commence par aller dans la catégorie Configuration/Objet/URL du SNS.
- On saisit l'url "stormshield.eu" puis on clique sur vérifier et normalement dans la zone commentaire on devrait avoir it ce qui signifie que stormshield appartient au groupe de base d'URL : it.

URL categories: stormshield.eu



- On se dirige ensuite dans Configuration/Politique de sécurité/filtrage d'URL.
- On sélectionne **(0) URLFilter_00.** comme politique de sécurité.
- Pour créer une règle de filtrage d'URL il faut remplir ces critères :

Status	Action	URL category	Comments
--------	--------	--------------	----------

C'est-à-dire le **statuts** : ON/OFF **l'action** : PASS/BLOCK **url**
category : le groupe d'url que l'on a créé pour et
comments : ce que l'on veut

- Pour créer une URL category il faut :
- Aller dans Configuration/Objects/URL et cliquer sur ajouter une catégorie personnalisée.

 OBJECTS / URL

URL CERTIFICATE NAME (CN) GROUPS OF CATEGORIES URL DATABASE

Add a customized category | Remove |  Check usage |  Classify

- On la nomme comme on le souhaite pour nous se sera black_list.

URL CERTIFICATE NAME (CN) GROUPS OF CATEGORIES URL DATABASE

Add a customized category | Remove |  Check usage |  Classify

URL category ▼	Comments
black_list	
vpnsst_owa	
authentication_bypass	
antivirus_bypass	

- On peut ajouter les URL dans black_list dans URL category :

URL CATEGORY: BLACK_LIST

Add a URL Remove

URL	Comments ▼
-----	------------

- Ajoutons par exemples : *.badssl.com/*

URL CATEGORY: BLACK_LIST

Add a URL Remove	
URL ▲	Comments
.badssl.com/	

Ne pas oublier les deux étoiles pour bien interdire toutes les âges sous-jacentes.

Par contre on ne pourra bloquer les url en http car ce n'est pas un proxy ssl.

- Ensuite il faut créer la règle qui bloquera notre category black_list :

(0) Proxy_CUB		Edit ▼	URL database provider: Embedded URL database	
+ Add	✕ Delete	↑ Up	↓ Down	Cut Copy Paste + Add all predefined categories ✕ Purge rules
	Status	Action	URL category	Comments
1	off	Pass	authentificati...	authorize the URLs of authentication_bypass group
2	on	BlockPage_00	black_list	
3	on	Pass	any	default rule (pass all)

Attention à bien la mettre avant la règle d'autorisation finale.

- On remplace URL category par la notre: black_list

SECURITY POLICY / URL FILTERING

(0) Proxy_CUB		Edit ▼	URL database provider: Embedded URL database	
+ Add	✕ Delete	↑ Up	↓ Down	Cut Copy Paste + Add all predefined categories ✕ Purge rules
	Status	Action	URL category	Comments
1	off	Pass	authentificati...	authorize the URLs of authentication_bypass group
2	on	Pass	any	default rule (pass all)
3	on	BlockPage_00	black_list	

- Il faut ensuite ajouter dans notre règle de filtrage qui autorise les flux http d'utiliser le proxy que l'on vient de créer :

EDITING RULE NO 3

General

Action

Source

Destination

Port - Protocol

Inspection

SECURITY INSPECTION

General

Inspection level: IPS

Inspection profile: Depending on traffic direction

Application inspection

Antivirus ⓘ : Off

Sandboxing ⓘ : Off

Antispam: Off

URL filtering: Proxy_CUB

SMTP filtering: Off

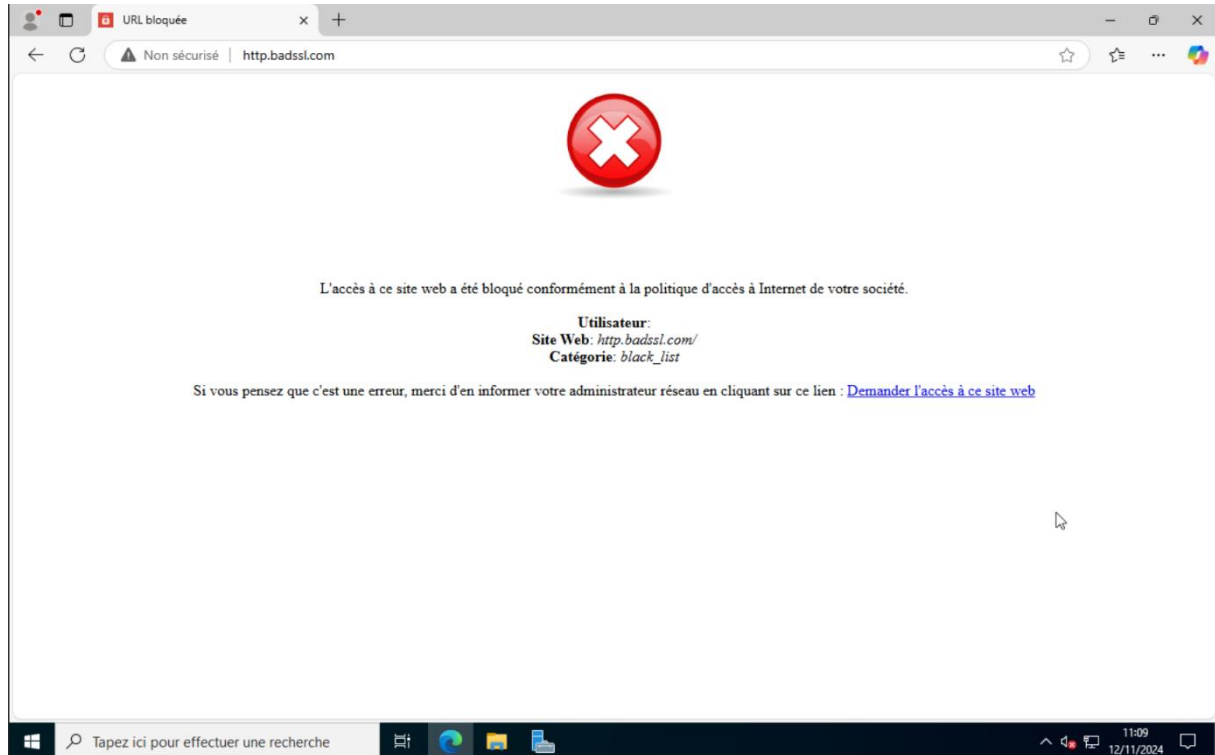
FTP filtering: Off

SSL filtering: Off

✖ CANCEL

✔ OK

- Pour tester il faut se rendre sur une vm qui se trouve dans le réseau et on essaye d'accéder au site badssl et cela renvoi normalement une erreur :



Remarque : Ce proxy ne sert à filtrer qu'uniquement les sites en http (qui ne sont pas protégés par ssl)