



[Date]

Proxy Web HTTP

Sur le Pare-feu **Stormshield**



Mamadou CAMARA
[NOM DE LA SOCIETE]

1. Principe du proxy web

Un proxy est un **composant logiciel et/ou matériel informatique** qui joue le rôle d'**intermédiaire** (mandataire) en se plaçant entre deux hôtes pour faciliter ou surveiller leurs échanges. Le proxy se situe au niveau de la **couche application**.

Le service proxy web est indispensable en entreprise, car il assure les fonctions suivantes :

- **examine le trafic web** afin d'identifier les contenus suspects ;
- **bloque** des catégories de **sites**, des **URL**, des **mots-clés** ;
- **journalise** l'ensemble des informations liées au protocole **http** (couche 4 du modèle TCP/IP ou couche 5 à 7 du modèle OSI) et offre ainsi des informations plus complètes que les logs émanant d'un pare-feu **stateful** standard.
- dispose d'une **fonction de cache** lui permettant de stocker les pages web consultées et de les fournir, par la suite, aux clients souhaitant accéder à ces mêmes pages.

2. Configuration du service proxy Web HTTP

La fonction de **filtrage des URL** permet de contrôler l'accès aux sites web d'Internet pour l'ensemble des utilisateurs. Pour contrôler ces accès, la politique de filtrage URL va se baser sur une **liste d'URL** classées en **catégories** ou de **mots clés personnalisés**.

Pour voir ces listes, on va dans le menu **Configuration / Objets / URL** puis l'onglet **Base d'URL**. La base par défaut est la Base URL embarquée :

STORMSHIELD Network Security v4.3.30

MONITORING CONFIGURATION EVA1 VMNSX09K0639A9

OBJECTS / URL

URL CERTIFICATE NAME (CN) GROUPS OF CATEGORIES URL DATABASE

URL database provider : Embedded URL database

Category	Comments
Academic (academic)	Sites sponsored by educational institutions and schools of all types including distance education. Includes general educational and reference materials, such as dictionaries, encyclopedias, online courses, teaching aids and discussion guides.
Advertisement (ads)	Sites that provide advertising graphics or other ad content files that appear on web pages.
Anonymizers and proxies (proxy)	Sites that act as an intermediary for surfing to other websites in an anonymous fashion, whether to circumvent web filtering or for other reasons.
Art (arts)	Sites with artistic content or relating to artistic institutions such as theaters, museums, galleries, dance companies, photography, and digital graphic resources.
Banking (bank)	Sites related to banking, finance, payment or investment, including banks, brokerages, online stock trading, stock quotes, fund management, insurance companies, credit unions, credit card companies, and so on.
Business activity (business)	Sites that obtain sales information such as corporate websites. Information, products or services that help organizations of all sizes to conduct their daily business activity. Business websites
Entertainment (entertainment)	Sites containing programming guides to television, movies, music and video (including video on demand), celebrity sites, and entertainment news.
Illegal content (illegal)	Sites presenting information (purchase, manufacture or required equipment) on illegal substances such as drugs
IT and technology (it)	Sites that contain information such as product reviews, discussions, and news about computers, software, hardware, peripheral and computers services.
Job search (employment)	Sites containing job listings, career information, assistance with job searches (such as resume writing, interviewing tips, etc.), employment agencies or head hunters.
News (news)	Sites covering news and current events such as newspapers, newswire services, personalized news services,

On peut créer une base URL personnalisée si les catégories de sites web prédéfinies par votre base d'URL ne sont pas exactement adaptées à vos besoins.

Dans cette activité, nous allons bloquer le site du lycée Valadon pour le test.

Dans le menu Configuration/URL/URL

OBJETS / URL

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

Ajouter une catégorie personnalisée Supprimer Vérifier l'utilisation Vérifier la classification d'une URL Classifier

Catégorie d'URL	Com...
vpns_Lowa	
antivirus_bypass	
authentication_bypass	
facebook_block	

Caractères autorisés

Les caractères autorisés sont : '*' '?' '/' ':' ';' ',' [a-z] [A-Z] [0-9]

Exemple d'URL : www.google.com/* ou *.yahoo.com/*

CATÉGORIE D'URL : FACEBOOK_BLOCK

Ajouter une URL Supprimer

URL	Commentaire
pedagogie.ac-limoges.fr/lyc-v...	

- Dans l'onglet URL, cliquer sur **Ajouter une catégorie personnalisée** puis donnez-lui un nom (par exemple **facebook_block**).
- Dans la zone **Catégorie d'URL**, cliquer sur **Ajouter l'URL du site que vous voulez bloquer**.

Politique de filtrage d'URL pré-définie

Une seule politique de filtrage est prédéfinie par défaut (quelle que soit la politique choisie, ce sont les deux même règles qui apparaissent).

- Ouvrir le menu **Configuration / Politique de sécurité / Filtrage URL**
- Dans la liste déroulante des politiques de sécurité, choisissez **(0) URLFilter_00**.

✚ POLITIQUE DE SÉCURITÉ / FILTRAGE URL

État	Action	Catégorie d'URL	Commentaire
1 <input type="checkbox"/> off	➔ Passer	📁 authenticati...	authorize the URLs of authentication_bypass group
2 <input checked="" type="checkbox"/> on	➔ Passer	📁 any	default rule (pass all)

La règle numéro 1 (non activée) autorise les URL qui font partie du groupe **authentication_bypass** qui peut être consulté dans le menu Objets Web, il s'agit des sites qui permettent les mises à jour Microsoft.

La règle numéro 2 laisse explicitement passer tous les flux.

Les règles de filtrage d'URL sont composées d'une colonne **Action** et d'une colonne **Catégorie d'URL**.

La colonne **Action** permet de **Bloquer** ou de **Passer** ou de **rediriger** vers l'une des 4 pages de blocage personnalisables.

La colonne **Catégorie d'URL** contient la liste des catégories prédéfinies de la base **URL embarquée** et les catégories personnalisées que vous avez créées.

The screenshot shows the configuration interface for the URL filtering policy. On the left is a navigation menu with categories like SYSTEM, NETWORK, OBJECTS, USERS, and SECURITY POLICY. The main area displays the 'SECURITY POLICY / URL FILTERING' configuration for '(0) cub_url'. It features a table with columns for Status, Action, URL category, and Comments. Rule 1 is disabled (off) with a 'Pass' action and 'authentication...' category. Rule 2 is enabled (on) with a 'BlockPage_00' action and 'facebook_bl...' category. Rule 3 is enabled (on) with a 'Pass' action and 'Any' category. The interface includes various control buttons like 'Add', 'Delete', 'Up', 'Down', 'Cut', 'Copy', 'Paste', 'Add all predefined categories', 'Purge rules', and 'Check URL clé'.

ICI on choisit les catégories de sites à autoriser, bloquer ou à rediriger vers l'une des 4 pages de blocage personnalisables (par exemple **BlockPage**). Le contrôle de cohérence en temps réel affiche les erreurs détectées dans votre politique.

Affectation d'une politique de filtrage URL

- Ouvrir **Configuration / Politique de sécurité / Filtrage et NAT**, et choisir la politique de sécurité actuellement appliquée.
- Dans l'onglet **Filtrage**, ouvrir la ou les règles qui autorisent l'accès à Internet avec le protocole **http**. Dans l'onglet **Inspection de sécurité**, dans la zone **Inspection** choisir, dans la liste **Filtrage URL**, la politique de filtrage URL à appliquer.

EDITING RULE NO 11

General
Action
Source
Destination
Port - Protocol
Inspection

SECURITY INSPECTION

General

Inspection level:

Inspection profile:

Application inspection

Antivirus ⓘ :

Sandboxing ⓘ :

Antispam:

URL filtering: cub_url

SMTP filtering:

FTP filtering:

SSL filtering:

Test :

Dans cette politique de filtrage, nous avons bloqué le site du **lycée valadon pour les utilisateurs internes de notre zone via le pare-feu Stormshield**



L'accès à ce site web a été bloqué conformément à la politique d'accès à Internet de votre société.

Utilisateur:

Site Web: *pedagogie.ac-limoges.fr/lyc-valadon/spip.php?rubrique95*

Catégorie: *facebook_block*

Si vous pensez que c'est une erreur, merci d'en informer votre administrateur réseau en cliquant sur ce lien : [Demander l'accès à ce site web](#)