

Fiche   
pfsense 2.4.1 – squid, squidguard et lightsquid

Dans cette fiche …

[Pfsense 2.4.1 – squid et squidguard 1](#_Toc496770943)

[Installation de pfsense 2](#_Toc496770944)

[Ouverture de session 3](#_Toc496770945)

[Installation des paquetage squid et squidguard 4](#_Toc496770946)

[Configuration de base de squid proxy server 5](#_Toc496770947)

[Mise en place des filtres à l’aide des listes noires (*blacklists*) 6](#_Toc496770948)

[Ajout de règles avec *easyrule* 8](#_Toc496770949)

Département d’informatique  
Collège de Maisonneuve  
3800 est, rue Sherbrooke,  
Montréal (Québec) H1X 2A2  
514.251-7131 poste 4800

Document proposé par Louis Savard, M. Ing. TI  
Dernière révision : Octobre 2017

# Pfsense 2.4.1 – squid, squidguard et lightsquid

## Installation de pfsense

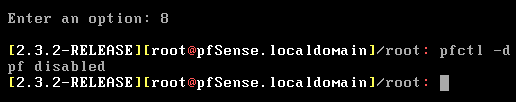
L’installation rapide devrait donner comme résultat ce qui suit …



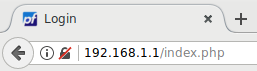
L’interface WAN sera client DHCP sur le réseau du collège (Interface par pont VMware).  
L’interface LAN aura une adresse IP privée (Segment LAN VMware).

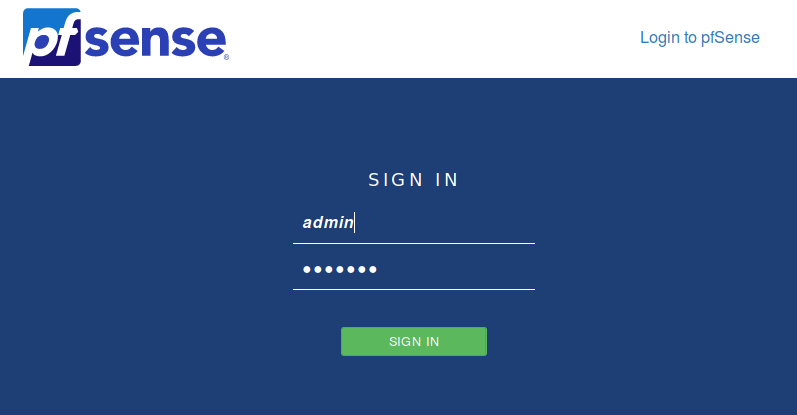
**Astuce**Il peut être utile de reprendre la main sur l'interface web de gestion depuis n'importe quelle interface du pare-feu, et ce en outrepassant toutes les règles.

**Désactivation du pare-feu (console)**



## Ouverture de session





Nom d’usager … ***admin***  
Mot de passe par défaut … ***pfsense***

Une fois ceci fait, vous pouvez ajouter des règles permettant la gestion …

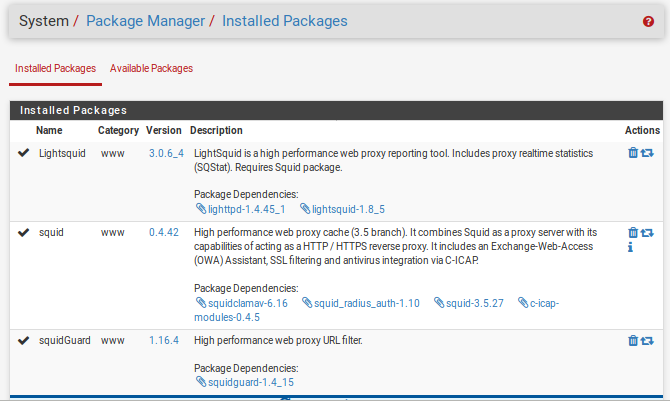
* Firewall > Rules
* Cliquer sur WAN, puis sur l'icône d'ajout d'une règle "+"
  + interface : WAN
  + protocol : TCP
  + source : l'IP ou le réseau de gestion
  + destination : WAN address
  + destination port range : 22, 80, 443
  + description : gestion admin

Vous devrez ajouter une règle pour chaque port ou définir un alias de port pour n'avoir qu'une seule règle.  
Une fois que tout est paramétré, confirmez avec *Apply changes*, ce qui réactivera le pare-feu au passage.   
Si vos règles sont bonnes alors l'accès à l'interface web fonctionnera.

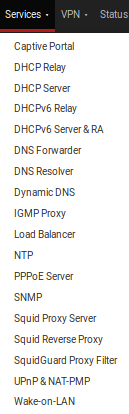
## Installation des paquetage squid et squidguard

**System /Package Manager / Avaliable Packages**

Installer **squid** et **squidguard**

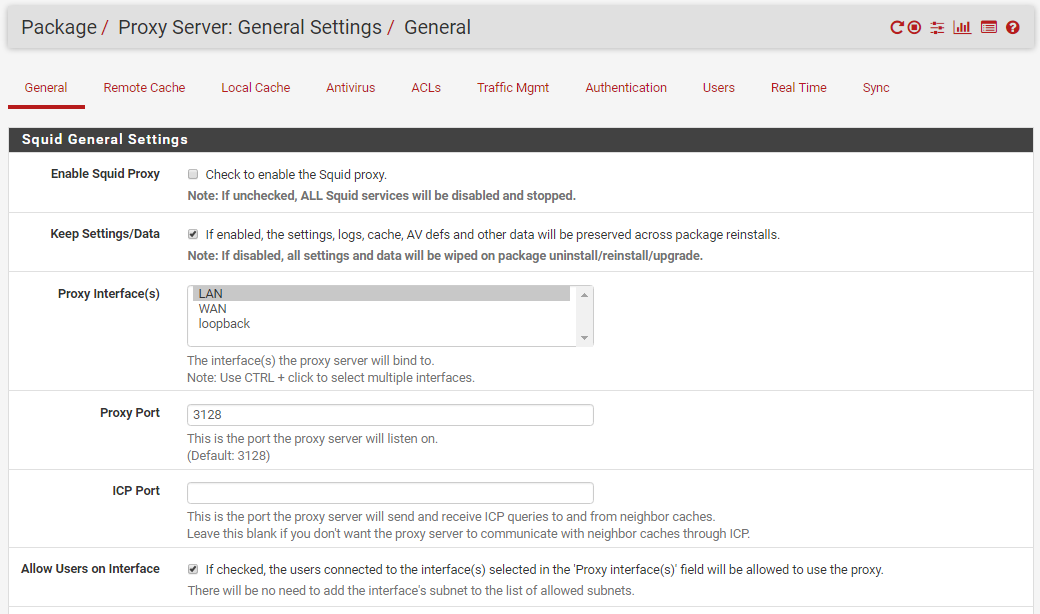


Les nouveaux services installés sont accessibles par le menu Services.

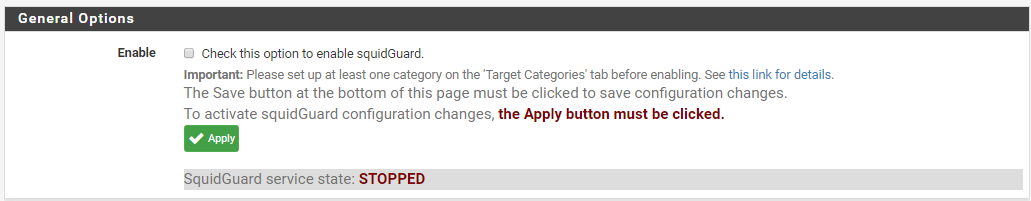


## Configuration de base de squid proxy server

**Services / Squid Proxy Server / General settings**   
Il faut s’assurer des paramètres suivants (par défaut) …  
Proxy interface(s) … **LAN**  
Proxy port … **3128**

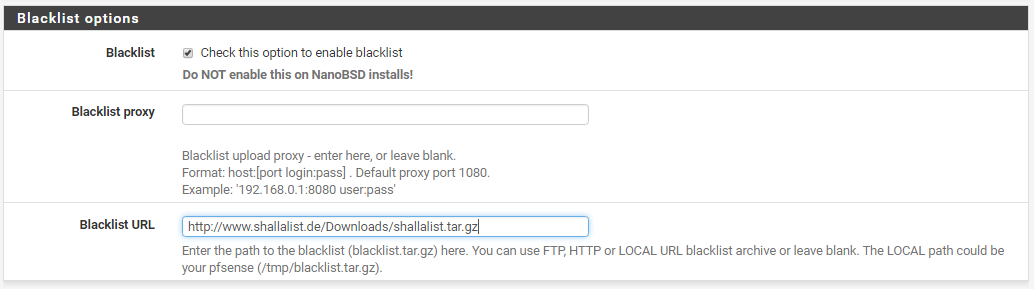


**Services / Squidguard Proxy Filter / General settings**   
Par défaut, squidguard n’est pas activé.



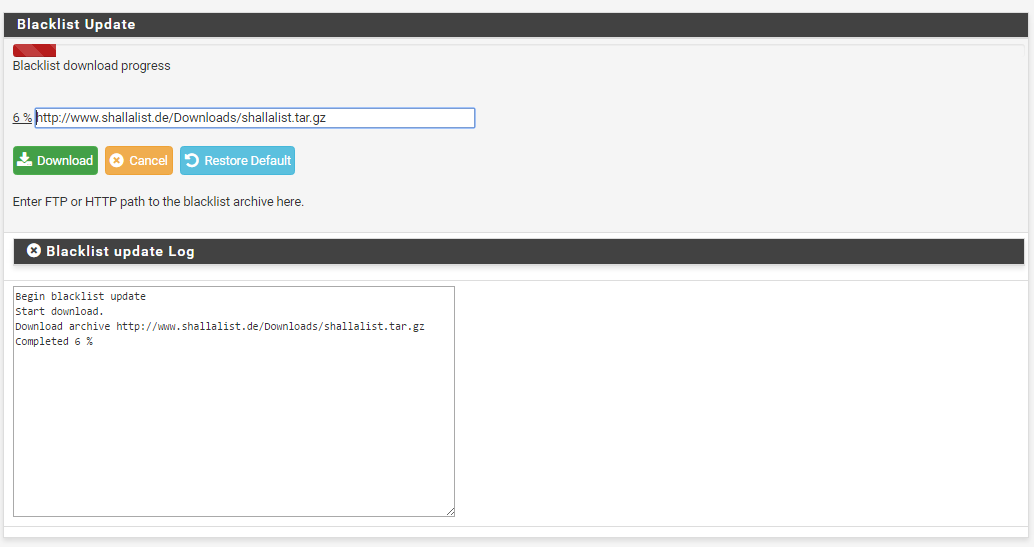
## Mise en place des filtres à l’aide des listes noires (*blacklists*)

**Services / Squid Proxy Server / General settings**   
Dans la section Blacklists options …  
Activer ***Check this option to enable blacklist***  
Entrez dans la case *Blacklist URL* l’adresse [**http://www.shallalist.de/Downloads/shallalist.tar.gz**](http://www.shallalist.de/Downloads/shallalist.tar.gz)

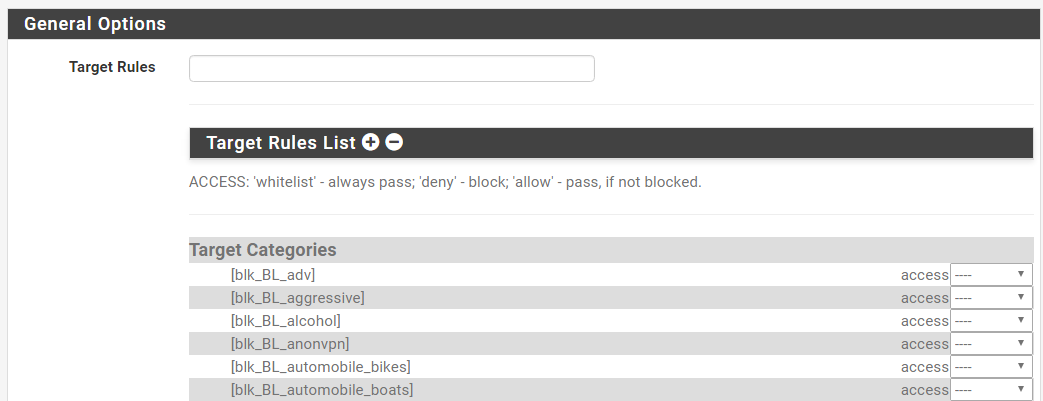


Confirmez avec **Apply**.

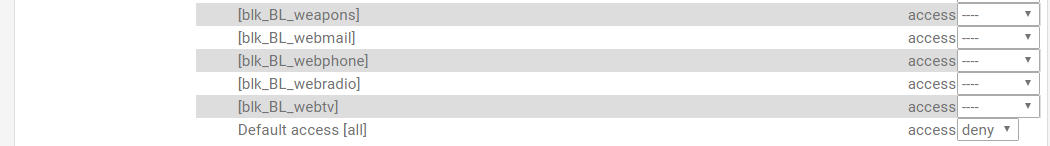
**Services / Squid Proxy Server / Blacklist**   
Cliquez sur **Download**.



**Services / Squid Proxy Server / Common ACL**Cliquez sur **Target Rules list +**.

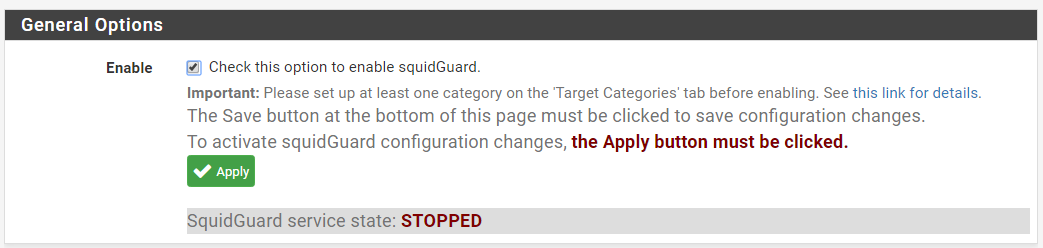


…



Les catégories offertes par *Shalla Secure Services* sont celles affichées.  
Par défaut, elles sont tous avec la paramètre **Deny**.

Il suffit maintenant d’activer la fonction de filtrage …  
**Services / Squid Proxy Server / General settings**   
Sélectionner la case à cocher **Enable**  
Confirmer avec **Apply**.



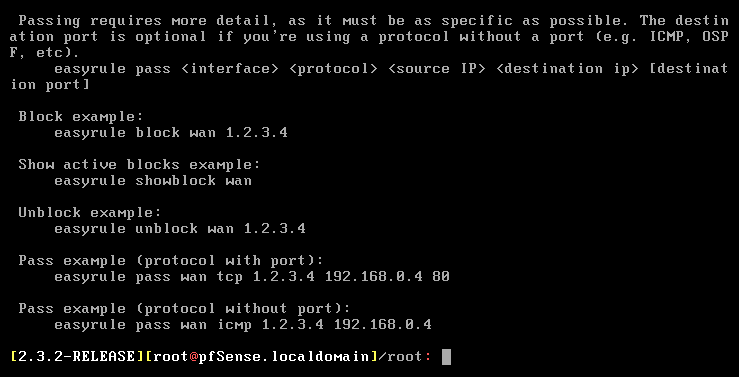
## Ajout de règles avec *easyrule*

L’utilitaire *easyRule* peut être utilisé depuis l'interface graphique ou encore depuis la ligne de commande afin d’ajouter rapidement des règles de pare-feu.

À la ligne de commande depuis l’interface principal de *pfsense*…

**easyrule block <interface> <IP source>  
easyrule pass <interface> <protocole> <IP source> <IP dest.> [port dest.]**

Exemples …  
**easyrule block wan 1.2.3.4  
easyrule pass wan tcp 1.2.3.4 192.168.0.4 80**   
**easyrule pass wan icmp 1.2.3.4 192.168.0.4**



Normalement, l'interface Web n'est accessible que depuis l'interface LAN de gestion (ou LAN par défaut).   
Si vous, pour une raison quelconque, vous êtes verrouillé ou avez besoin d'accéder à partir d'une adresse IP différente via l'interface WAN, il est possible d’utiliser la ligne de commande *easyrule* afin d’ajouter temporairement une règle qui donne un accès depuis une adresse IP distante.

La commande suivante ajoute une règle de pare-feu, permettant le trafic TCP sur le port 443 à partir de l'adresse IP 206.167.44.10 vers l'adresse IP WAN sur 10.80.240.100  
**easyrule pass wan tcp 206.167.44.10 10.80.240.100 443**

Vous pouvez également autoriser l'accès SSH et configurer un port distant …  
(ssh -L localport:remoteip:remoteport remoteip)  
**easyrule pass wan tcp 206.167.44.100 10.80.240.100 22**