

PROJET SERVEUR MANDATAIRE (SQUID)

08/02/2018



Lycée Technologique Théodore Aubanel


Table des matières

Présentation	3
Installation Pfsense	3
Configuration Pfsense	7
1. Installation Squid et SquidGuard	7
2. Configuration Squid et SquidGuard	8
3. Configuration proxy sur les clients via GPO	13

PRESENTATION

Pour ce projet d'installation Squid nous avons utilisé l'OS Pfsense qui nous a permis une configuration plus rapide et simplifiée grâce à l'interface web.

INSTALLATION PFSENSE

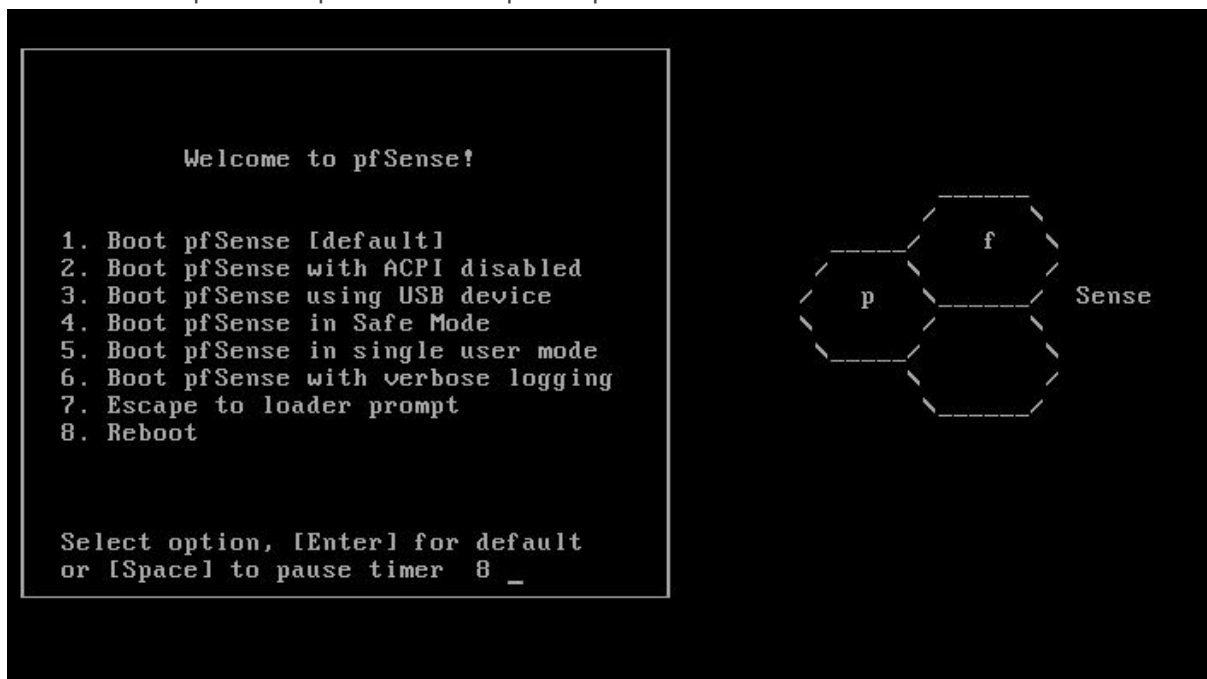
 L'installation est faite sur une machine virtuelle gérée par Hyper-V.

Pour commencer on télécharge l'image ISO sur le site de Pfsense à cette adresse :

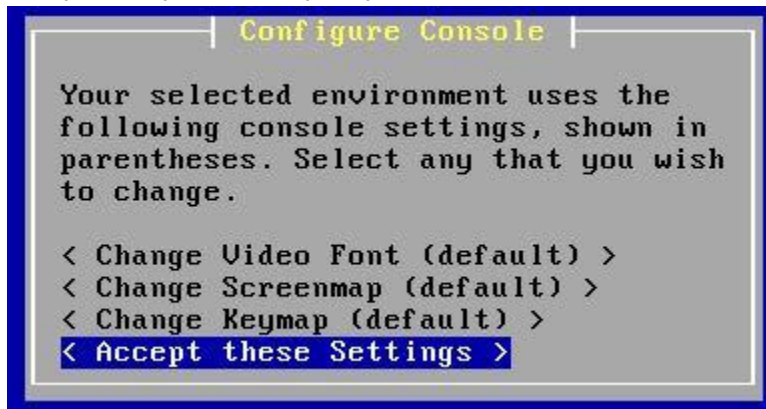
<https://www.pfsense.org/download/>

Au démarrage de la machine « bootez » sur l'image et installez Pfsense en suivant les étapes ci-dessous.

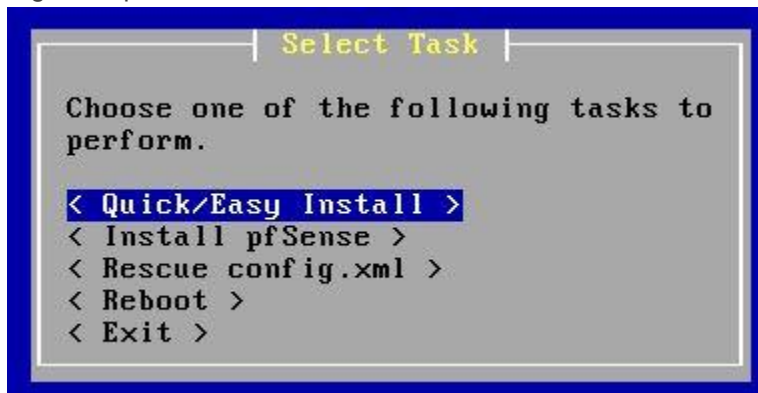
Sélectionnez l'option 1 ou patientez le temps indiqué en bas de la fenêtre.



Modifiez les paramètres que vous souhaitez changer, comme le placement des touches du clavier et acceptez les paramètres pour poursuivre l'installation.



Pour les débutant choisissez l'installation « Quick/Easy Install » ou « Install Pfsense » si vous souhaitez régler les paramètres vous-même.



Appuyer sur « N »

```
Welcome to pfSense 2.0.2-RELEASE ...

No core dumps found.
Creating symlinks.....done.
External config loader 1.0 is now starting... ad0s1b
Launching the init system... done.
Initializing..... done.
Starting device manager (devd)...done.
Loading configuration.....done.

Network interface mismatch -- Running interface assignment option.

Valid interfaces are:

em0   08:00:27:f2:97:f0   (up) Intel(R) PRO/1000 Legacy Network Connection 1.0.4
em1   08:00:27:1c:11:e3   (up) Intel(R) PRO/1000 Legacy Network Connection 1.0.4

Do you want to set up VLANs first?

If you are not going to use VLANs, or only for optional interfaces, you should
say no here and use the webConfigurator to configure VLANs later, if required.

Do you want to set up VLANs now [y/n]? █
```

Appuyer sur « A »

```
If you do not know the names of your interfaces, you may choose to use
auto-detection. In that case, disconnect all interfaces now before
hitting 'a' to initiate auto detection.

Enter the WAN interface name or 'a' for auto-detection: █
```

Appuyer sur « Entrer »

```
Enter the WAN interface name or 'a' for auto-detection: em0

Enter the LAN interface name or 'a' for auto-detection
NOTE: this enables full Firewalling/NAT mode.
(or nothing if finished): █
```

Une fois arrivé ici vous avez fini l'installation de Pfsense. Vous pouvez désormais accéder à votre interface web via l'adresse IP de votre machine.

Les identifiants par défaut sont :

- Identifiant : admin
- Mot de passe : pfsense

```
FreeBSD/i386 (pfSense.localdomain) (ttyv0)
*** Welcome to pfSense 2.0.2-RELEASE-pfSense (i386) on pfSense ***

WAN (wan)          -> em0          -> 10.0.2.15 (DHCP)
LAN (lan)          -> em1          -> 192.168.1.1

0) Logout (SSH only)          8) Shell
1) Assign Interfaces          9) pfTop
2) Set interface(s) IP address 10) Filter Logs
3) Reset webConfigurator password 11) Restart webConfigurator
4) Reset to factory defaults  12) pfSense Developer Shell
5) Reboot system              13) Upgrade from console
6) Halt system                 14) Enable Secure Shell (sshd)
7) Ping host

Enter an option: █
```

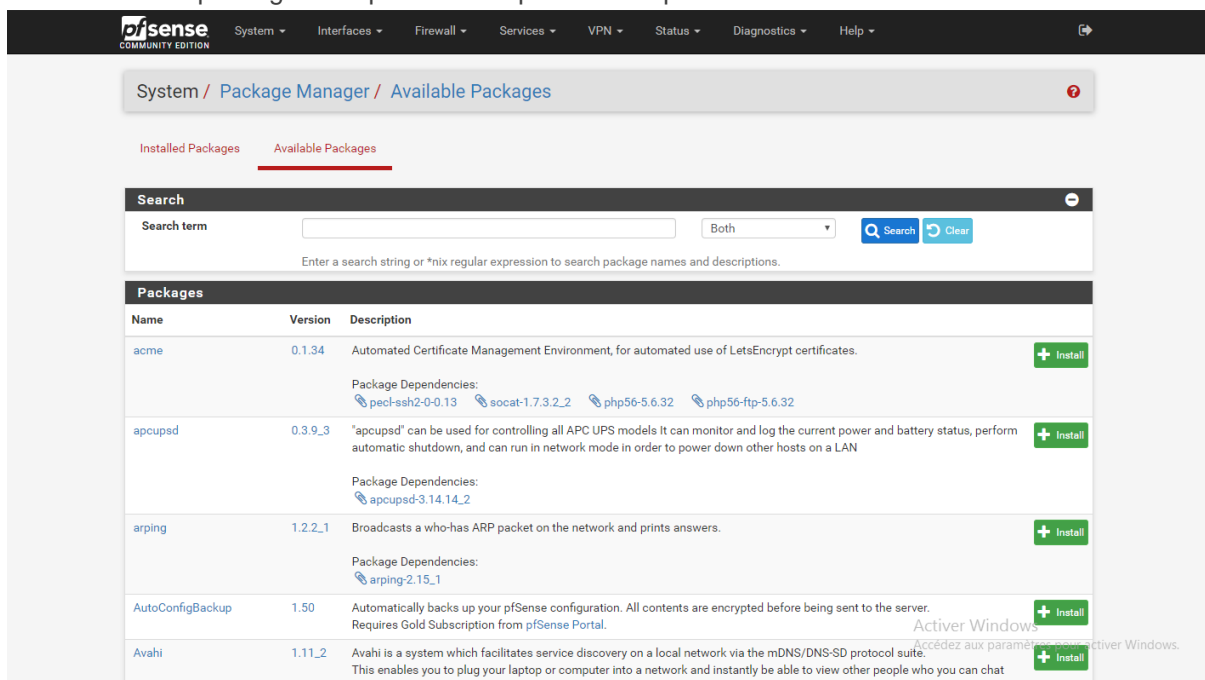
CONFIGURATION PFSENSE

1. Installation Squid et SquidGuard

Pour notre proxy vous devez installer Squid qui va être le serveur mandataire et SquidGuard qui s'appuie sur celui pour permettre l'utilisation de BlackLists en ligne.

 Si vous ne souhaitez pas utiliser de BlackLists en ligne mais la faire par vous-même, l'installation de SquidGuard n'est pas requise.

Rendez-vous dans « System -> Package Manager »
Recherchez les packages « Squid » et « SquidGuard » pour les installer.



The screenshot shows the pfSense Package Manager interface. The top navigation bar includes the pfSense logo and menu items: System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, and Help. The breadcrumb trail is System / Package Manager / Available Packages. Below the breadcrumb, there are tabs for 'Installed Packages' and 'Available Packages', with the latter being selected. A search bar is present with a search term field, a dropdown menu set to 'Both', and 'Search' and 'Clear' buttons. Below the search bar, a table lists available packages with columns for Name, Version, and Description. Each row includes an 'Install' button.

Name	Version	Description	Install
acme	0.1.34	Automated Certificate Management Environment, for automated use of LetsEncrypt certificates. Package Dependencies: pect-ssh2-0-0.13 socat-1.7.3.2_2 php56-5.6.32 php56-ftp-5.6.32	+ Install
apcupsd	0.3.9_3	"apcupsd" can be used for controlling all APC UPS models It can monitor and log the current power and battery status, perform automatic shutdown, and can run in network mode in order to power down other hosts on a LAN Package Dependencies: apcupsd-3.14.14_2	+ Install
arping	1.2.2_1	Broadcasts a who-has ARP packet on the network and prints answers. Package Dependencies: arping-2.15_1	+ Install
AutoConfigBackup	1.50	Automatically backs up your pfSense configuration. All contents are encrypted before being sent to the server. Requires Gold Subscription from pfSense Portal .	+ Install
Avahi	1.11_2	Avahi is a system which facilitates service discovery on a local network via the mDNS/DNS-SD protocol suite. This enables you to plug your laptop or computer into a network and instantly be able to view other people who you can chat	+ Install

2. Configuration Squid et SquidGuard

Une fois les deux programmes installés vous allez configurer Squid pour que votre proxy puisse fonctionner.

Dans « Service -> Squid Proxy Server » configurez les paramètres généraux comme vous le souhaitez. Cochez « Enable Squid Proxy » et choisissez vos paramètres.

Squid General Settings	
Enable Squid Proxy	<input checked="" type="checkbox"/> Check to enable the Squid proxy. Important: If unchecked, ALL Squid services will be disabled and stopped.
Keep Settings/Data	<input checked="" type="checkbox"/> If enabled, the settings, logs, cache, AV defs and other data will be preserved across package reinstalls. Important: If disabled, all settings and data will be wiped on package uninstall/reinstall/upgrade.
Proxy Interface(s)	<input type="text" value="WAN"/> loopback The interface(s) the proxy server will bind to. Use CTRL + click to select multiple interfaces.
Proxy Port	<input type="text" value="8080"/> This is the port the proxy server will listen on. Default: 3128
ICP Port	<input type="text"/> This is the port the proxy server will send and receive ICP queries to and from neighbor caches. Leave this blank if you don't want the proxy server to communicate with neighbor caches through ICP.
Allow Users on Interface	<input checked="" type="checkbox"/> If checked, the users connected to the interface(s) selected in the 'Proxy interface(s)' field will be allowed to use the proxy. There will be no need to add the interface's subnet to the list of allowed subnets.
Patch Captive Portal	This feature was removed - see Bug #5594 for details!
Resolve DNS IPv4 First	<input type="checkbox"/> Enable this to force DNS IPv4 lookup first. This option is very useful if you have problems accessing HTTPS sites.
Disable ICMP	<input type="checkbox"/> Check this to disable Squid ICMP pinger helper.
Use Alternate DNS Servers for the Proxy Server	<input type="text"/> To use DNS servers other than those configured in System > General Setup, enter the IP(s) here. Separate entries by semi-colons (;)

Headers Handling, Language and Other Customizations	
Visible Hostname	<input type="text" value="localhost"/> This is the hostname to be displayed in proxy server error messages.
Administrator's Email	<input type="text" value="admin@localhost"/> This is the email address displayed in error messages to the users.
Error Language	<input type="text" value="en"/> Select the language in which the proxy server will display error messages to users.
X-Forwarded Header Mode	<input type="text" value="(on)"/> Choose how to handle X-Forwarded-For headers. Default: on ⓘ
Disable VIA Header	<input type="checkbox"/> If not set, Squid will include a Via header in requests and replies as required by RFC2616.
URI Whitespace Characters Handling	<input type="text" value="strip"/> Choose how to handle whitespace characters in URL. Default: strip ⓘ
Suppress Squid Version	<input type="checkbox"/> Suppresses Squid version string info in HTTP headers and HTML error pages if enabled.

Si vous rencontrez une erreur avec Local Cache il suffit d'aller dans l'onglet et sauvegarder la configuration pour régler le problème.

Maintenant passons à la configuration de SquidGuard

Si vous utilisez SquidGuard vous pouvez ajouter une Blacklist.

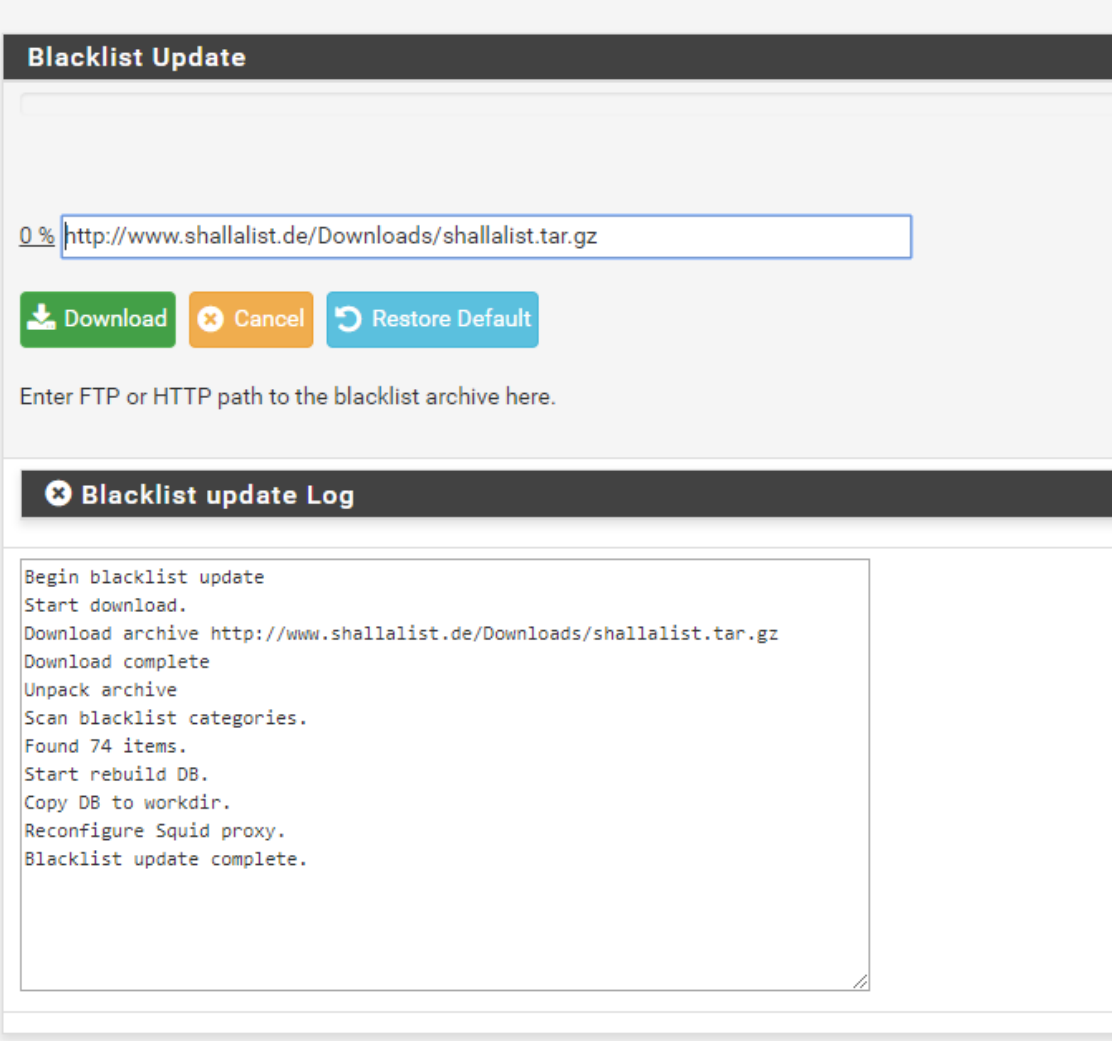
Par défaut Pfsense est configuré pour fonctionner avec les BlackLists Anglaises.

Vous pouvez donc télécharger différentes BlackLists via le site de SquidGuard à cette adresse :

<http://www.squidguard.org/blacklists.html>




Ici nous avons choisis d'utiliser la liste « Shalla's Blacklists ».

Allez donc dans « Service -> SquidGuard Proxy Filter -> Blacklist » et ajoutez-y le lien de la Blacklist choisis puis cliquez sur « Download » en patientant jusqu'à la fin du processus.



Blacklist Update

0 %

 Download  Cancel  Restore Default

Enter FTP or HTTP path to the blacklist archive here.

Blacklist update Log

```
Begin blacklist update
Start download.
Download archive http://www.shallalist.de/Downloads/shallalist.tar.gz
Download complete
Unpack archive
Scan blacklist categories.
Found 74 items.
Start rebuild DB.
Copy DB to workdir.
Reconfigure Squid proxy.
Blacklist update complete.
```

Allez dans « Common ACL » puis cliquez sur le « + » du bandeau noir intitulé « Target Rules List ». Tout en bas de la liste vous devez « allow » Default access [all] pour tout autoriser et ainsi pouvoir « deny » les catégories de sites que vous souhaitez bloquer.

Target Categories		
[blk_BL_adv]	access	---
[blk_BL_aggressive]	access	deny
[blk_BL_alcohol]	access	deny
[blk_BL_anonvpn]	access	---
[blk_BL_automobile_bikes]	access	---
[blk_BL_automobile_boats]	access	---
[blk_BL_automobile_cars]	access	---
[blk_BL_automobile_planes]	access	---
[blk_BL_chat]	access	deny
[blk_BL_costtraps]	access	---
[blk_BL_dating]	access	deny
[blk_BL_downloads]	access	deny
[blk_BL_drugs]	access	deny
[blk_BL_dynamic]	access	---
[blk_BL_education_schools]	access	---
[blk_BL_finance_banking]	access	---
[blk_BL_finance_insurance]	access	---
[blk_BL_finance_moneylending]	access	---
[blk_BL_finance_other]	access	---
[blk_BL_finance_realestate]	access	---
[blk_BL_finance_trading]	access	---
[blk_BL_fortunetelling]	access	---
[blk_BL_forum]	access	---
[blk_BL_gamble]	access	deny
[blk_BL_government]	access	---
[blk_BL_hacking]	access	deny
[blk_BL_hobby_cooking]	access	---
[blk_BL_hobby_games-misc]	access	deny
[blk_BL_hobby_games-online]	access	deny
[blk_BL_hobby_gardening]	access	---
[blk_BL_hobby_pets]	access	---
[blk_BL_homestyle]	access	---
[blk_BL_hospitals]	access	---
[blk_BL_imagehosting]	access	---
[blk BL isd]	access	---

Une fois les configurations effectuées vous pouvez sauvegarder en bas de la page.

Dans « General Settings » vous pouvez ajouter le lien de votre Blacklist pour qu'elle s'actualise automatiquement

Blacklist options

Blacklist Check this option to enable blacklist
Do NOT enable this on NanoBSD installs!

Blacklist proxy

Blacklist upload proxy - enter here, or leave blank.
Format: host:[port login:pass] . Default proxy port 1080.
Example: '192.168.0.1:8080 user:pass'

Blacklist URL

Enter the path to the blacklist (blacklist.tar.gz) here. You can use FTP, HTTP or LOCAL URL, blacklist archive or leave blank. The LOCAL path could be your pfSense (/tmp/blacklist.tar.gz).

Vous pouvez aussi activer les logs qui permettront d'avoir un meilleur suivi des requêtes utilisateurs et pour finir cliquez sur « Apply » pour valider le tout.

Package / Proxy Inter SquidGuard: General settings / General settings

General settings | Common ACL | Groups ACL | Target categories | Times | Rewrites | Blacklist | Log | XMLRPC Sync

General Options

Enable Check this option to enable squidGuard.
Important: Please set up at least one category on the 'Target Categories' tab before enabling. See this link for details.
The Save button at the bottom of this page must be clicked to save configuration changes.
To activate squidGuard configuration changes, **the Apply button must be clicked.**

SquidGuard service state: **STARTED**

LDAP Options

Enable LDAP Filter Enable options for setup ldap connection to create filters with ldap search

LDAP DN
Configure your LDAP DN (ex: cn=Administrator,cn=Users,dc=domain)

LDAP DN Password
Password must be initialize with letters (Ex: Change123), valid format: [a-zA-ZV][a-zA-Z0-9/_\-\.\:\%\+\?=&]

Strip NT domain name Strip NT domain name component from user names (/ or \ separated).

Strip Kerberos Realm Strip Kerberos Realm component from user names (@ separated).

LDAP Version

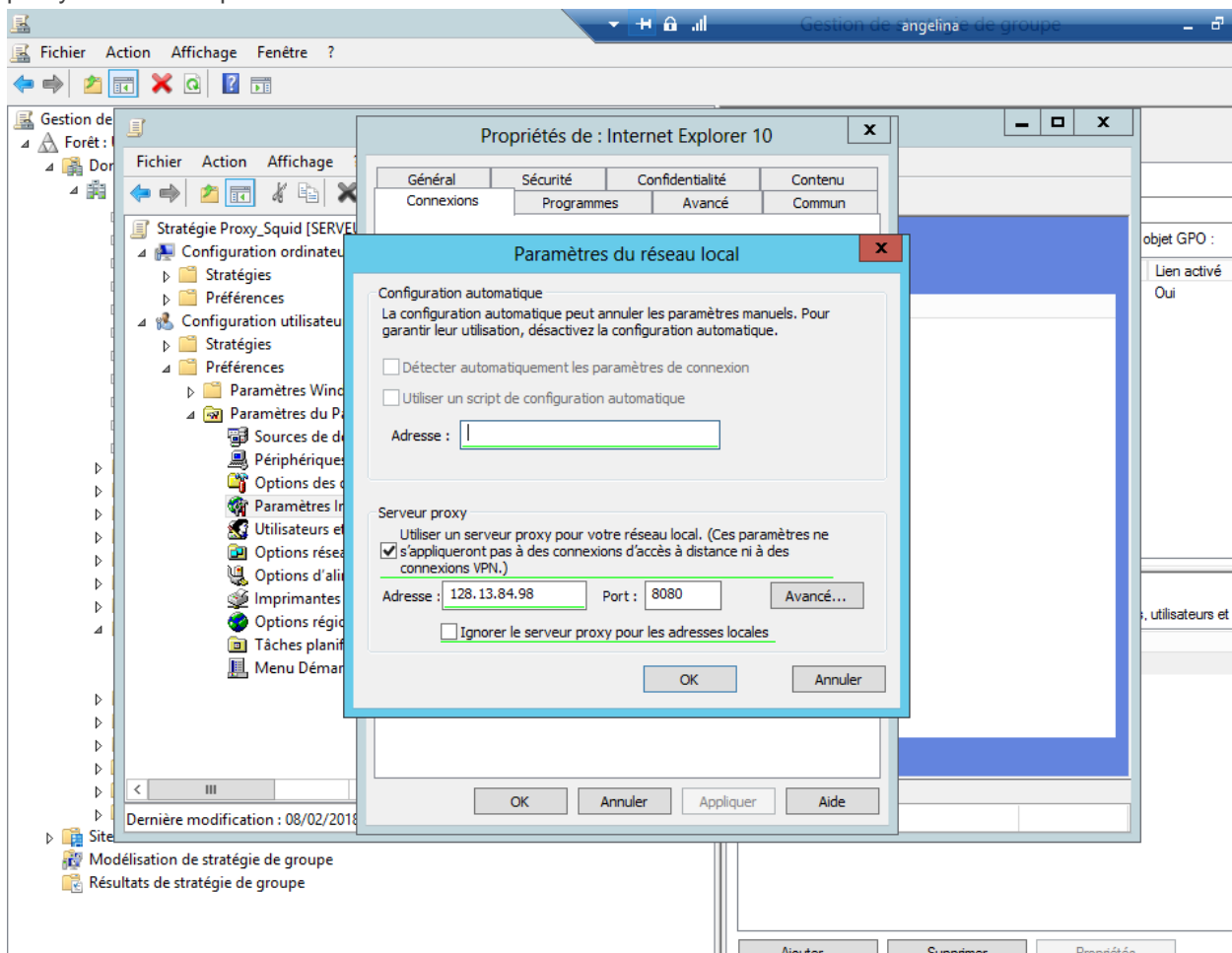
Activier Windows
Accédez aux paramètres pour activer Windows.

Voici un exemple de log d'un utilisateur tentant d'accéder à des sites bloqués par le proxy.

Show 50 entries starting at << 0 >>			
08.02.2018 11:53:23	128.13.84.102/128.13.84.102	9gag.com:443	Request(default/blk_BL_recreation_humor/-) - CONNECT REDIRECT
08.02.2018 11:53:19	128.13.84.102/128.13.84.102	fr-fr.facebook.com:443	Request(default/blk_BL_socialnet/-) - CONNECT REDIRECT
08.02.2018 11:53:13	128.13.84.102/128.13.84.102	fr-fr.facebook.com:443	Request(default/blk_BL_socialnet/-) - CONNECT REDIRECT
08.02.2018 11:53:11	128.13.84.102/128.13.84.102	fr-fr.facebook.com:443	Request(default/blk_BL_socialnet/-) - CONNECT REDIRECT
08.02.2018 11:50:04	128.13.84.102/128.13.84.102	soundcloud.com:443	Request(default/blk_BL_music/-) - CONNECT REDIRECT
08.02.2018 11:47:17	128.13.84.102/128.13.84.102	www.youporn.com:443	Request(default/blk_BL_porn/-) - CONNECT REDIRECT
08.02.2018 11:46:30	128.13.84.102/128.13.84.102	www.google.com:443	Request(default/none/-) - CONNECT REDIRECT
08.02.2018 11:46:30	128.13.84.102/128.13.84.102	www.google.com:443	Request(default/none/-) - CONNECT REDIRECT
08.02.2018 11:46:28	128.13.84.102/128.13.84.102	http://detectportal.firefox.com/success.txt	Request(default/none/-) - GET REDIRECT
08.02.2018 11:46:25	128.13.84.102/128.13.84.102	http://detectportal.firefox.com/success.txt	Request(default/none/-) - GET REDIRECT
08.02.2018 11:46:22	128.13.84.102/128.13.84.102	http://detectportal.firefox.com/success.txt	Request(default/none/-) - GET REDIRECT
08.02.2018 11:46:18	128.13.84.102/128.13.84.102	http://detectportal.firefox.com/success.txt	Request(default/none/-) - GET REDIRECT

3. Configuration proxy sur les clients via GPO

Pour configurer le proxy des clients nous utilisons notre domaine pour forcer les utilisateurs à utiliser le proxy et aussi bloquer la modification de celui-ci.



Petite subtilité !

Une fois les paramètres rentrés si tout est encore souligné en rouge il suffit d'appuyer sur « F5 » afin d'appliquer les paramètres.