
GSB
Proxy / Firewall
Version <2.5>



Mise en place d'un PfSense

GSB	Version: <2.5>
Proxy / Firewall	Date: 04/03/2016

Historique des révisions

Date	Version	Description	Auteur
23/02/2016	<1.0>	Installation et configuration de Pfsense	Legrand Julien Brice Harismendy
01/03/2016	<1.5>	Configuration des règles du Pare-Feu	Legrand Julien Brice Harismendy
04/03/2016	<2.0>	Installation et configuration de "Squidguard"	Legrand Julien Brice Harismendy
07/03/2016	<2.5>	Derniers tests et rédaction finale	Legrand Julien Brice Harismendy

GSB	Version: <2.5>
Proxy / Firewall	Date: 04/03/2016

Table des matières

1. Introduction

- 1.1 Contexte du projet
- 1.2 Objectifs du document
- 1.3 Portée
- 1.4 Définitions, Acronymes et Abréviations
- 1.5 Schéma réseau

2. Installation et configuration de Pfsense

- 2.1 Installation
- 2.2 Configuration via l'interface Web
 - 2.2.1 Configuration du Pare-Feu 6
 - 2.2.2 Redirection des ports 11
 - 2.2.3 Translation d'adresses 13
 - 2.2.4 Configuration de la Supervision 14
- 2.3 Installation et configuration du Proxy (SQUID)
- 2.4 Installation "Squidguard"

3. Tests / Validations

- 3.1 Ping de la machine dans le LAN
- 3.2 Test accès web (après règle HTTP)
- 3.3 Test fonctionnement résolution DNS
- 3.4 Test connexion http par port 8080
- 3.5 Test d'accès au serveur web via l'adresse publique
- 3.6 Test du proxy par accès à "monip.org"
- 3.7 Test de la blacklist par accès à un réseau social

4. Conclusion

GSB	Version: <2.5>
Proxy / Firewall	Date: 04/03/2016

Mise en place d'un PfSense

1. Introduction

Nous allons mettre en place un Pare-Feu / Proxy qui permettra de filtrer l'accès à internet tant par les protocoles que par les adresses IP / URL. Pour cela, nous utiliserons le Pare-Feu intégré à Pfsense et un Proxy du nom de "Squidguard".

1.1 Contexte du projet

Ici nous mettons en place un filtrage d'accès via un Pfsense démarré en "vif" sur un ordinateur du réseau.

1.2 Objectifs du document

Ce document à pour objectif de permettre la mise en place d'un filtrage basique en un minimum de temps.

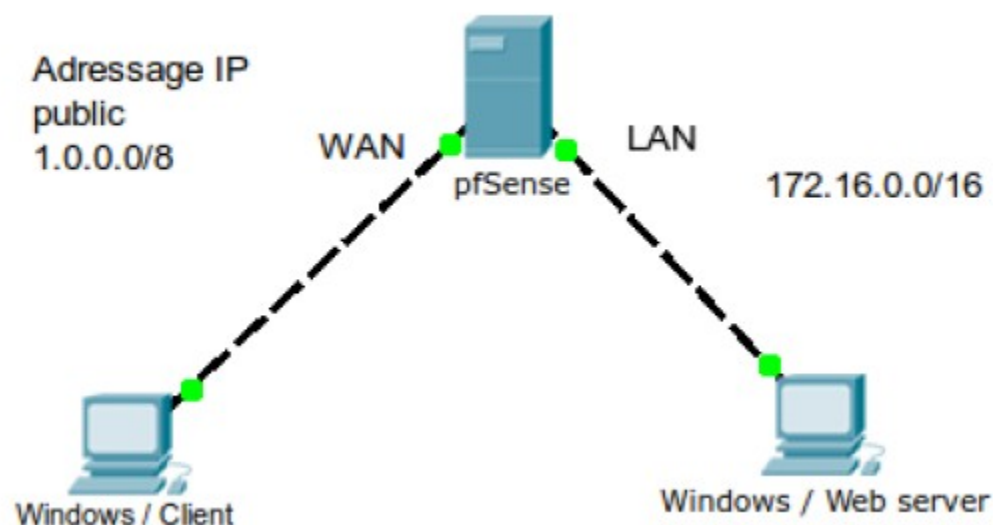
1.3 Portée

Ce document s'adresse avant tout aux équipes techniques et à l'administrateur réseau.

1.4 Définitions, Acronymes et Abréviations

URL : "Uniform Resource Locator"

1.5 Schéma réseau



GSB	Version: <2.5>
Proxy / Firewall	Date: 04/03/2016

2. Installation et configuration de Pfsense

2.1 Installation

Nous n'allons pas installer Pfsense sur le disque dur d'une machine mais l'utiliser en "vif". Pour cela, appuyer sur "**Entrée**" lors du premier menu et sur "**c**" au menu suivant. Il nous faut ensuite configurer les interfaces via le menu principal (option 2) :

WAN adresse IPv4 : **1.0.0.1/8**

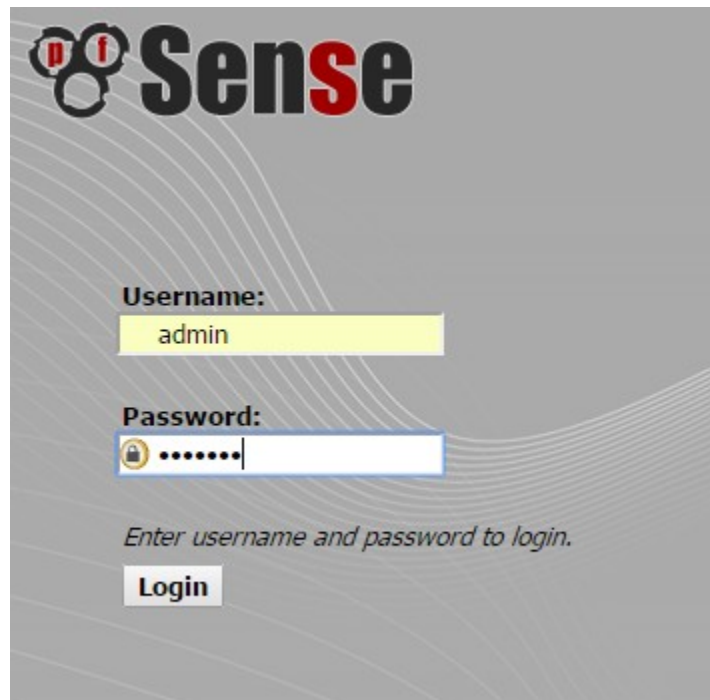
LAN adresse IPv4 : **172.16.0.254/16** (DHCP)

2.2 Configuration via l'interface Web

Nous allons nous connecter à l'interface web via le réseau WAN, dans notre cas, l'interface a pour IP : **1.0.0.1/8**

- Entrez cette IP dans votre navigateur (à adapter selon votre cas).

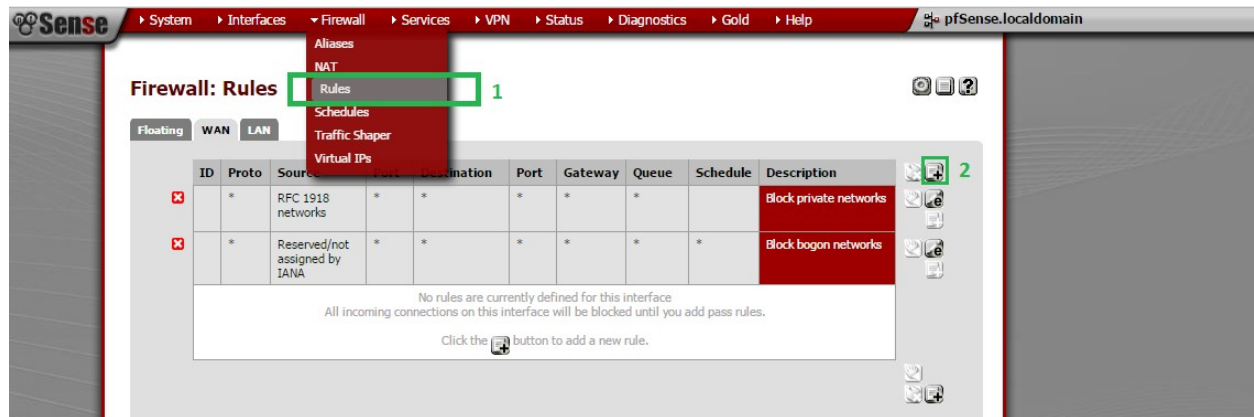
Le login par défaut est "**admin**" et le mot de passe "**pfsense**".



GSB	Version: <2.5>
Proxy / Firewall	Date: 04/03/2016

2.2.1 Configuration du Pare-Feu

Nous allons configurer le Pare-Feu, pour cela allez dans "**Firewall**" > "**Rules**" et rester sur l'onglet "**WAN**" par défaut. Cliquez sur l'icône "**Add new rule**" (voir 2).



2.2.1.1 Création d'une règle pour ICMP :

Création d'une règle indiquant au Pare-Feu de laisser passer les paquets ICMP. (règle essentielle car nous ne pouvons pas pinger le LAN)

```
Microsoft Windows [version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Tous droits réservés.

C:\Users\jleggrand>ping 172.16.0.3

Envoi d'une requête 'Ping' 172.16.0.3 avec 32 octets de données :
Réponse de 194.79.128.54 : Durée de vie TTL expirée lors du transit.
Réponse de 194.79.128.54 : Durée de vie TTL expirée lors du transit.
Réponse de 194.79.128.54 : Durée de vie TTL expirée lors du transit.
Réponse de 194.79.128.54 : Durée de vie TTL expirée lors du transit.

Statistiques Ping pour 172.16.0.3:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
```

Une fois le "**nmap**" fini, aucun client n'a répondu :

```
Nmap done: 1 IP address (0 hosts up) scanned in 4.57
seconds
    Raw packets sent: 7 (260B) | Rcvd: 3 (400B)|
```

- Voici les paramètres à entrer lors de la création de la règle :

GSB	Version: <2.5>
Proxy / Firewall	Date: 04/03/2016

Firewall: Rules: Edit



Edit Firewall rule

Action	Pass <div>Choose what to do with packets that match the criteria specified below. Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.</div>
Disabled	<input type="checkbox"/> Disable this rule Set this option to disable this rule without removing it from the list.
Interface	WAN <div>Choose which interface packets must be sourced on to match this rule.</div>
TCP/IP Version	IPv4 <div>Select the Internet Protocol version this rule applies to</div>
Protocol	ICMP <div>Choose which IP protocol this rule should match. Hint: in most cases, you should specify TCP here.</div>
ICMP type	any <div>If you selected ICMP for the protocol above, you may specify an ICMP type here.</div>
Source	<input type="checkbox"/> not Use this option to invert the sense of the match. Type: any Address: /
Destination	<input type="checkbox"/> not Use this option to invert the sense of the match. Type: any Address: /
Log	<input type="checkbox"/> Log packets that are handled by this rule Hint: the firewall has limited local log space. Don't turn on logging for everything. If you want to do a lot of logging, consider using a remote syslog server (see the Diagnostics: System logs: Settings page).
Description	<div>You may enter a description here for your reference.</div>

Save
Cancel

- Quand vous retournez à l'écran des règles pour le WAN, cliquez sur "**Apply changes**".
Test de ping une fois la règle ICMP ajoutée concluant.

2.2.1.2 Création d'une règle pour HTTP (ouverture du port 80) :

(Même principe pour créer la règle, voici les paramètres cette fois-ci)

GSB	Version: <2.5>
Proxy / Firewall	Date: 04/03/2016

Firewall: Rules: Edit



Edit Firewall rule

Action	<div>Pass ▾</div> <p>Choose what to do with packets that match the criteria specified below. Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.</p>
Disabled	<div><input type="checkbox"/> Disable this rule</div> <p>Set this option to disable this rule without removing it from the list.</p>
Interface	<div>WAN ▾</div> <p>Choose which interface packets must be sourced on to match this rule.</p>
TCP/IP Version	<div>IPv4 ▾</div> <p>Select the Internet Protocol version this rule applies to</p>
Protocol	<div>TCP ▾</div> <p>Choose which IP protocol this rule should match. Hint: in most cases, you should specify <i>TCP</i> here.</p>
Source	<div><input type="checkbox"/> not</div> <p>Use this option to invert the sense of the match.</p> <p>Type: any ▾</p> <p>Address: <input type="text"/> / <input type="text"/></p>
Source port range	<p>from: any ▾</p> <p>to: any ▾</p> <p>Specify the source port or port range for this rule. This is usually <i>random</i> and almost never equal to the destination port range (and should usually be "any"). Hint: you can leave the 'to' field empty if you only want to filter a single port.</p>
Destination	<div><input type="checkbox"/> not</div> <p>Use this option to invert the sense of the match.</p> <p>Type: any ▾</p> <p>Address: <input type="text"/> / <input type="text"/></p>
Destination port range	<p>from: HTTP (80) ▾</p> <p>to: HTTP (80) ▾</p> <p>Specify the port or port range for the destination of the packet for this rule. Hint: you can leave the 'to' field empty if you only want to filter a single port.</p>
Log	<div><input type="checkbox"/> Log packets that are handled by this rule</div> <p>Hint: the firewall has limited local log space. Don't turn on logging for everything. If you want to do a lot of logging, consider using a remote syslog server (see the Diagnostics: System logs: Settings page).</p>
Description	<div> <input type="text"/></div> <p>You may enter a description here for your reference.</p>

Save

Cancel

2.2.1.3 Création d'une règle pour le DNS (port 53) :

GSB	Version: <2.5>
Proxy / Firewall	Date: 04/03/2016

Firewall: Rules: Edit



Edit Firewall rule

Action	<div>Pass ▾</div> <p>Choose what to do with packets that match the criteria specified below. Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.</p>
Disabled	<input type="checkbox"/> Disable this rule Set this option to disable this rule without removing it from the list.
Interface	<div>WAN ▾</div> <p>Choose which interface packets must be sourced on to match this rule.</p>
TCP/IP Version	<div>IPv4 ▾</div> Select the Internet Protocol version this rule applies to
Protocol	<div>TCP ▾</div> <p>Choose which IP protocol this rule should match. Hint: in most cases, you should specify <i>TCP</i> here.</p>
Source	<input type="checkbox"/> not Use this option to invert the sense of the match. Type: <div>any ▾</div> Address: <div></div> / <div>▾</div> <div>Advanced</div> - Show source port range
Destination	<input type="checkbox"/> not Use this option to invert the sense of the match. Type: <div>any ▾</div> Address: <div></div> / <div>▾</div>
Destination port range	from: <div>DNS (53) ▾</div> <div></div> to: <div>DNS (53) ▾</div> <div></div> <p>Specify the port or port range for the destination of the packet for this rule. Hint: you can leave the 'to' field empty if you only want to filter a single port.</p>
Log	<input type="checkbox"/> Log packets that are handled by this rule <p>Hint: the firewall has limited local log space. Don't turn on logging for everything. If you want to do a lot of logging, consider using a remote syslog server (see the Diagnostics: System logs: Settings page).</p>
Description	<div> <div></div></div> <p>You may enter a description here for your reference.</p>

Save

Cancel


2.2.1.4 Création d'une règle pour RDP (port 3389) :

GSB	Version: <2.5>
Proxy / Firewall	Date: 04/03/2016

Firewall: Rules: Edit



Edit Firewall rule


Action	<div>Pass ▾</div> <p>Choose what to do with packets that match the criteria specified below. Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.</p>
Disabled	<input type="checkbox"/> Disable this rule Set this option to disable this rule without removing it from the list.
Interface	<div>WAN ▾</div> <p>Choose which interface packets must be sourced on to match this rule.</p>
TCP/IP Version	<div>IPv4 ▾</div> Select the Internet Protocol version this rule applies to
Protocol	<div>TCP ▾</div> <p>Choose which IP protocol this rule should match. Hint: in most cases, you should specify TCP here.</p>
Source	<input type="checkbox"/> not Use this option to invert the sense of the match. Type: <div>any ▾</div> Address: <div></div> / <div>▾</div> <div>Advanced</div> - Show source port range
Destination	<input type="checkbox"/> not Use this option to invert the sense of the match. Type: <div>any ▾</div> Address: <div></div> / <div>▾</div>
Destination port range	from: <div>MS RDP (3389) ▾</div> <div></div> to: <div>MS RDP (3389) ▾</div> <div></div> <p>Specify the port or port range for the destination of the packet for this rule. Hint: you can leave the 'to' field empty if you only want to filter a single port</p>
Log	<input type="checkbox"/> Log packets that are handled by this rule <p>Hint: the firewall has limited local log space. Don't turn on logging for everything. If you want to do a lot of logging, consider using a remote syslog server (see the Diagnostics: System logs: Settings page).</p>
Description	<div> <div></div></div> <p>You may enter a description here for your reference.</p>

Save

Cancel

2.2.1.5 Suppression de la règle du pare-feu qui donne accès au port 80, puis création d'une règle qui autorise les flux TCP sur le port 8080 :

GSB	Version: <2.5>
Proxy / Firewall	Date: 04/03/2016

Edit Firewall rule	
Action	<div>Pass ▾</div> <p>Choose what to do with packets that match the criteria specified below. Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.</p>
Disabled	<input type="checkbox"/> Disable this rule Set this option to disable this rule without removing it from the list.
Interface	<div>WAN ▾</div> <p>Choose which interface packets must be sourced on to match this rule.</p>
TCP/IP Version	<div>IPv4 ▾</div> Select the Internet Protocol version this rule applies to
Protocol	<div>TCP ▾</div> <p>Choose which IP protocol this rule should match. Hint: in most cases, you should specify <i>TCP</i> here.</p>
Source	<input type="checkbox"/> not Use this option to invert the sense of the match. Type: <div>any ▾</div> Address: <div></div> / <div>▾</div> <div>Advanced</div> - Show source port range
Destination	<input type="checkbox"/> not Use this option to invert the sense of the match. Type: <div>any ▾</div> Address: <div></div> / <div>▾</div>
Destination port range	from: <div>(other) ▾</div> <div>8080</div> to: <div>(other) ▾</div> <div>8080</div> <p>Specify the port or port range for the destination of the packet for this rule. Hint: you can leave the 'to' field empty if you only want to filter a single port</p>
Log	<input type="checkbox"/> Log packets that are handled by this rule <p>Hint: the firewall has limited local log space. Don't turn on logging for everything. If you want to do a lot of logging, consider using a remote syslog server (see the Diagnostics: System logs: Settings page).</p>
Description	<div></div> <div></div> <p>You may enter a description here for your reference.</p>

Save

Cancel

2.2.2 Redirection des ports

Pour la suite nous allons devoir supprimer la règle sur le port 8080. Ensuite sur Pfsense, il nous faut aller dans **"Firewall"** > **"NAT"** puis créer une règle de la même manière que le pare-feu, qui transformera les adresses de type **172.16.0.1:80** en **172.16.0.1:8080**.

GSB	Version: <2.5>
Proxy / Firewall	Date: 04/03/2016

Firewall: NAT: Port Forward: Edit



Edit Redirect entry	
Disabled	<input type="checkbox"/> Disable this rule Set this option to disable this rule without removing it from the list.
No RDR (NOT)	<input type="checkbox"/> Enabling this option will disable redirection for traffic matching this rule. Hint: this option is rarely needed, don't use this unless you know what you're doing.
Interface	<div>WAN ▾</div> Choose which interface this rule applies to. Hint: in most cases, you'll want to use WAN here.
Protocol	<div>TCP ▾</div> Choose which IP protocol this rule should match. Hint: in most cases, you should specify TCP here.
Source	<div>Advanced</div> - Show source address and port range
Destination	<input type="checkbox"/> not Use this option to invert the sense of the match. Type: <div>Single host or alias ▾</div> Address: <div>172.16.0.1 / ▾</div>
Destination port range	from: <div>HTTP ▾</div> <div></div> to: <div>HTTP ▾</div> <div></div> Specify the port or port range for the destination of the packet for this mapping. Hint: you can leave the 'to' field empty if you only want to map a single port
Redirect target IP	<div>172.16.0.1</div> Enter the internal IP address of the server on which you want to map the ports. e.g. 192.168.1.12
Redirect target port	<div>(other) ▾</div> <div>8080</div> Specify the port on the machine with the IP address entered above. In case of a port range, specify the beginning port of the range (the end port will be calculated automatically). Hint: this is usually identical to the 'from' port above
Description	<div></div> You may enter a description here for your reference (not parsed).
No XMLRPC Sync	<input type="checkbox"/> Hint: This prevents the rule on Master from automatically syncing to other CARP members. This does NOT prevent the rule from being overwritten on Slave.
NAT reflection	<div>Use system default ▾</div>
Filter rule association	<div>Rule NAT ▾</div> View the filter rule

Rule Information	
Created	3/1/16 09:48:30 by admin@172.16.0.1
Updated	3/1/16 09:53:15 by admin@172.16.0.1

[Save](#) [Cancel](#)

Maintenant, il faut que le serveur continue d'écouter sur le port 8080, mais il faut uniquement qu'à partir du client on puisse y accéder par le port 80, c'est ici qu'est utile la redirection de port. On crée de ce fait ici une règle de type "NAT : Port Forward" :

GSB	Version: <2.5>
Proxy / Firewall	Date: 04/03/2016

Firewall: NAT: Port Forward



Port Forward 1:1 Outbound NPT

If	Proto	Src. addr	Src. ports	Dest. addr	Dest. ports	NAT IP	NAT Ports	Description
WAN	TCP	*	*	WAN address	80 (HTTP)	172.16.0.1	8080	

pass
linked rule

2.2.3 Translation d'adresses

- La destination doit être changée (l'adresse que doit joindre le client) :

Edit Redirect entry

Disabled ☐ **Disable this rule**
Set this option to disable this rule without removing it from the list.

No RDR (NOT) ☐ Enabling this option will disable redirection for traffic matching this rule.
Hint: this option is rarely needed, don't use this unless you know what you're doing.

Interface
Choose which interface this rule applies to.
Hint: in most cases, you'll want to use WAN here.

Protocol
Choose which IP protocol this rule should match.
Hint: in most cases, you should specify TCP here.

Source - Show source address and port range

Destination ☐ **not**
Use this option to invert the sense of the match.
Type:
Address: /

Destination port range
from: to:
Specify the port or port range for the destination of the packet for this mapping.
Hint: you can leave the 'to' field empty if you only want to map a single port

Redirect target IP
Enter the internal IP address of the server on which you want to map the ports.
e.g. 192.168.1.12

Redirect target port
Specify the port on the machine with the IP address entered above. In case of a port range, specify the beginning port of the range (the end port will be calculated automatically).
Hint: this is usually identical to the 'from' port above

Description
You may enter a description here for your reference (not parsed).

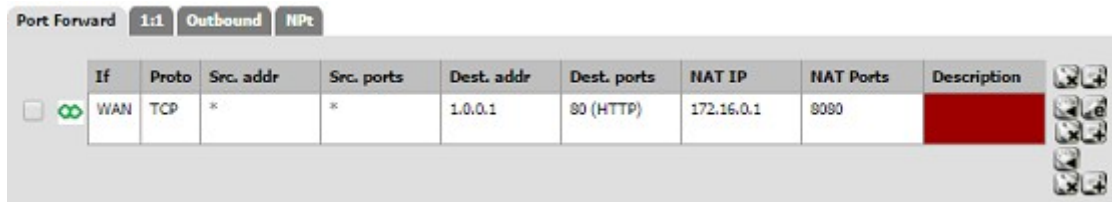
No XMLRPC Sync ☐
Hint: This prevents the rule on Master from automatically syncing to other CARP members. This does NOT prevent the rule from being overwritten on Slave.

NAT reflection

Filter rule association
View the filter rule

GSB	Version: <2.5>
Proxy / Firewall	Date: 04/03/2016

- On modifie ensuite la règle de “**Port Forward**” pour que la translation fonctionne, car l'on veut à présent masquer l'adresse IP interne de notre serveur web :



2.2.4 Configuration de la Supervision

Nous allons ajouter Pfsense à notre serveur de supervision, pour cela, nous allons configurer la partie SNMP sur le Proxy/Firewall (aller dans “**Services**” > “**SNMP**”) :



2.3 Installation et configuration du Proxy (SQUID)

Nous souhaitons configurer notre proxy web par Pfsense afin que les machines ne puissent plus accéder à internet directement. Pour cela, nous installons le package “**SQUID**” aller dans “**System**” > “**Packages**” et “**Available Packages**” :



- Cliquer sur “**Confirm**” dès la demande de confirmation puis attendez la fin de l'installation :



GSB	Version: <2.5>
Proxy / Firewall	Date: 04/03/2016

- Allez ensuite dans “**Services**” > “**Proxy Server**” et cochez la case en face de “**Transparent Proxy**” :

Proxy server: General settings



General Upstream Proxy Cache Mgmt Access Control Traffic Mgmt Auth Settings Local Users

Proxy interface: LAN, WAN, loopback
The interface(s) the proxy server will bind to.

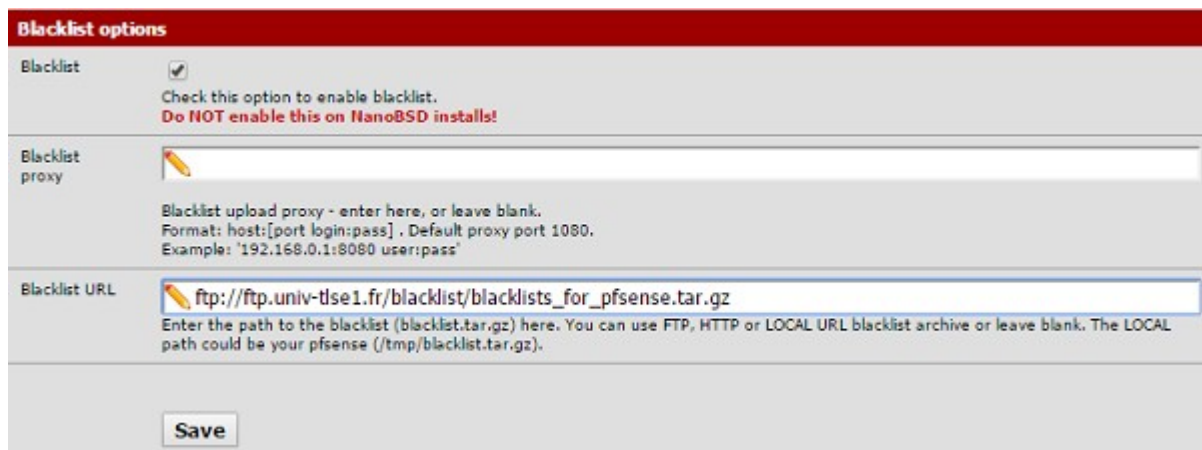
Allow users on interface: ☒
If this field is checked, the users connected to the interface selected in the 'Proxy interface' field will be allowed to use the proxy, i.e., there will be no need to add the interface's subnet to the list of allowed subnets. This is just a shortcut.

Transparent proxy: ☒
If transparent mode is enabled, all requests for destination port 80 will be forwarded to the proxy server without any additional configuration necessary.

2.4 Installation “Squidguard”

Nous allons installer le package “**Squidguard**” cette fois, afin de pouvoir filtrer tout les accès au niveau des URLs. L'installation de “Squidguard” se fait de **la même manière que pour “Squid”** :

- Allez dans “**Général Settings**” et activez les blacklists puis entrez une URL de blacklist.



Blacklist options

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

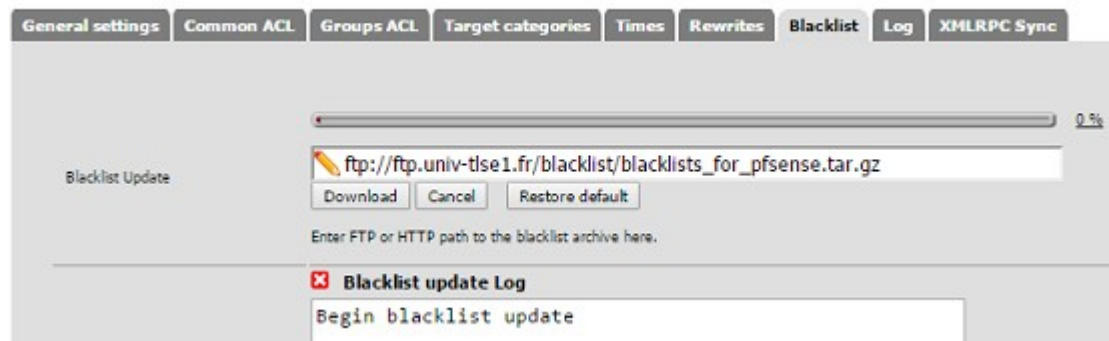
Blacklist proxy:
Blacklist upload proxy - enter here, or leave blank.
Format: host:[port login:pass] . Default proxy port 1080.
Example: '192.168.0.1:8080 user:pass'

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).

Save

- Cliquez sur “**Download**” pour télécharger la blacklist :

Proxy filter SquidGuard: Blacklist page



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

Blacklist Update:
Download Cancel Restore default
Enter FTP or HTTP path to the blacklist archive here.

Blacklist update Log: ☒ Begin blacklist update



GSB	Version: <2.5>
Proxy / Firewall	Date: 04/03/2016

- Cliquez sur “Target Rules List” :

Proxy filter SquidGuard: Common Access Control List (ACL) ?

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

Target Rules

Target Rules List (click here)  

Do not allow IP-Addresses in URL ☐ To make sure that people do not bypass the URL filter by simply using the IP-Addresses instead of the FQDN you can check this option. This option has no effect on the whitelist.

[blk_blacklists_social_networks]	access deny
[blk_blacklists_special]	access ----
[blk_blacklists_sports]	access ----
[blk_blacklists_strict_redirector]	access ----
[blk_blacklists_strong_redirector]	access ----
[blk_blacklists_translation]	access ----
[blk_blacklists_tricheur]	access ----
[blk_blacklists_update]	access ----
[blk_blacklists_warez]	access ----
[blk_blacklists_webmail]	access ----
Default access [all]	access allow

Nous activons dans Squidguard la blacklist “social-network”.

3. Tests / Validations

3.1 Ping de la machine dans le LAN

```
C:\Users\jlegrand>ping 172.16.0.3

Envoi d'une requête 'Ping' 172.16.0.3 avec 32 octets de données :
Réponse de 172.16.0.3 : octets=32 temps=1 ms TTL=63
Réponse de 172.16.0.3 : octets=32 temps=1 ms TTL=63
Réponse de 172.16.0.3 : octets=32 temps=1 ms TTL=63
Réponse de 172.16.0.3 : octets=32 temps=1 ms TTL=63

Statistiques Ping pour 172.16.0.3:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
    Durée approximative des boucles en millisecondes :
        Minimum = 1ms, Maximum = 1ms, Moyenne = 1ms
```

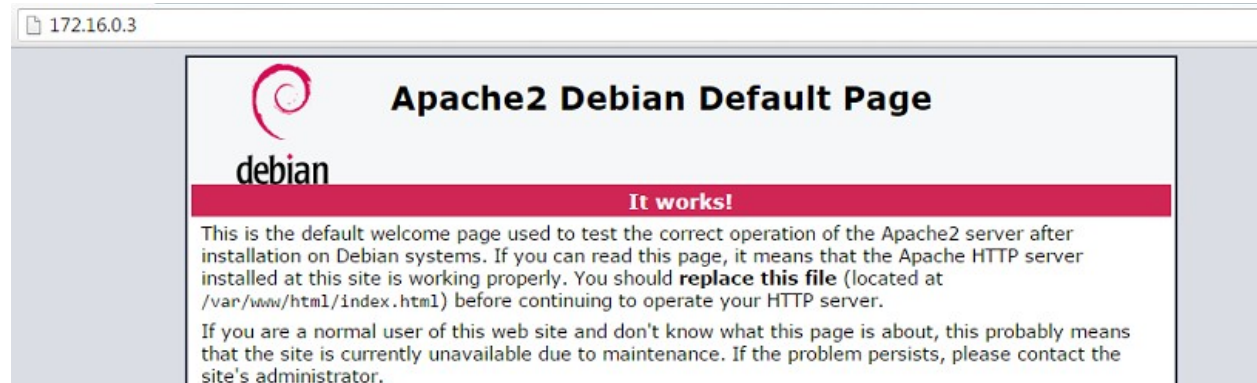
(cette fois le “nmap” détecte bien que l'hôte est actif)

GSB	Version: <2.5>
Proxy / Firewall	Date: 04/03/2016

Nmap done: 1 IP address (1 host up) scanned in 60.60 seconds
 Raw packets sent: 2050 (93.148KB) | Rcvd: 15 (988B)

3.2 Test accès web (après règle HTTP)

- Nous pouvons désormais accéder à l'interface web à partir du client :



```
PORT      STATE SERVICE VERSION
80/tcp    open  http   Apache httpd 2.4.10 ((Debian))
|_ http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
|_ http-server-header: Apache/2.4.10 (Debian)
|_ http-title: Apache2 Debian Default Page: It works
```

(Et maintenant "nmap" peut voir que le port 80 est ouvert)

3.3 Test fonctionnement résolution DNS

Initiating Parallel DNS resolution of 1 host. at 11:46
 Completed Parallel DNS resolution of 1 host. at 11:46, 16.56s elapsed

("nmap" nous montre bien que les flux DNS sont autorisés)

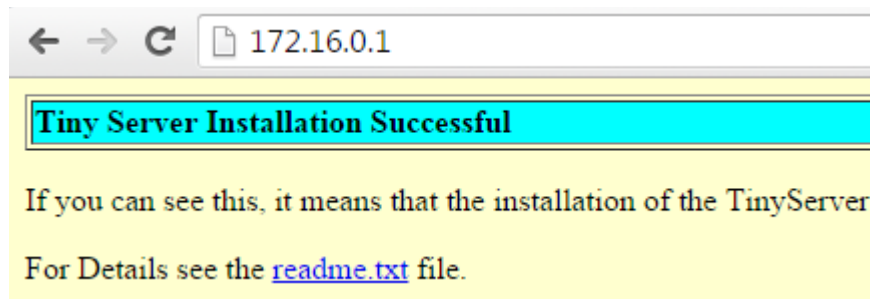
3.4 Test connexion http par port 8080

Network Distance: 2 hops

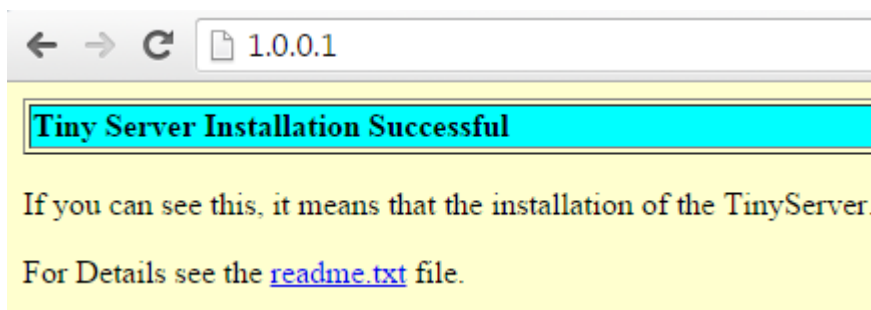
```
TRACEROUTE (using port 8080/tcp)
HOP RTT ADDRESS
1 0.00 ms 1.0.0.1
2 0.00 ms 172.16.0.1
```

Le "nmap" nous montre bien que TCP utilise le port 8080, et le navigateur fonctionne lui aussi :

GSB	Version: <2.5>
Proxy / Firewall	Date: 04/03/2016



3.5 Test d'accès au serveur web via l'adresse publique



3.6 Test du proxy par accès à “monip.org”

- On peut voir que l'accès web se fait bien par le proxy :

IP : 213.41.208.71

--- btsig.edu.nerim.net ---
1.1 localhost:3128 (squid/2.7.STABLE9)

Proxy detecté / Proxy detected

ORG_IP : 172.16.0.1

--- 172.16.0.1 ---
Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/48.0.2564.116 Safari/537.36

GSB	Version: <2.5>
Proxy / Firewall	Date: 04/03/2016

3.7 Test de la blacklist par accès à un réseau social

L'accès aux réseaux sociaux est maintenant coupé grâce à la blacklist.



4. Conclusion

Nous avons donc mis en place un Pare-Feu / Proxy sous Pfsense sur notre réseau, il nous permet de filtrer les accès et de bloquer certaines communications par l'intermédiaire d'une blacklist grâce au module Squidguard. A l'aide du Pare-Feu, nous pouvons créer une DMZ afin de filtrer les ports. La limite de cette solution Pfsense est que l'on peut faire passer des communications non-autorisées par des ports qui le sont, et nous allons gérer ce problème dans la suite avec la mise en place d'un IDS.