

Parefeu Pfsense

Sommaire

Objectif.....	1
Prérequis.....	1
Procédure de mise en place du Firewall pfSense.....	2
1. Installation de pfSense.....	2
2. Configuration via l'interface Web.....	3
3. Configuration du firewall.....	4
4. Mise en place du filtrage Web.....	8
4.2. Configuration de SquidGuard (Filtrage de contenu).....	11
4.3. Activation des logs LightSquid.....	12
AIDE.....	13
1. Annexe.....	13
2. Commandes utiles.....	13

Objectif

Prérequis

Procédure de mise en place du Firewall pfSense

1. Installation de pfSense

Télécharger l'image ISO

Rendez-vous sur : <https://www.pfsense.org/download/>.
Sélectionnez la version 2.7 en 64 bits.

Création de la machine virtuelle (VM) sur VirtualBox

Ouvrir VirtualBox et cliquer sur Nouvelle machine.

Type : BSD

Version : FreeBSD (64-bit)

Attribuer 2 Go de RAM et 10 Go de disque dur (VHD ou VDI, en mode dynamique).

Ajouter deux cartes réseau :

Carte 1 : Mode Bridge (connectée au WAN).

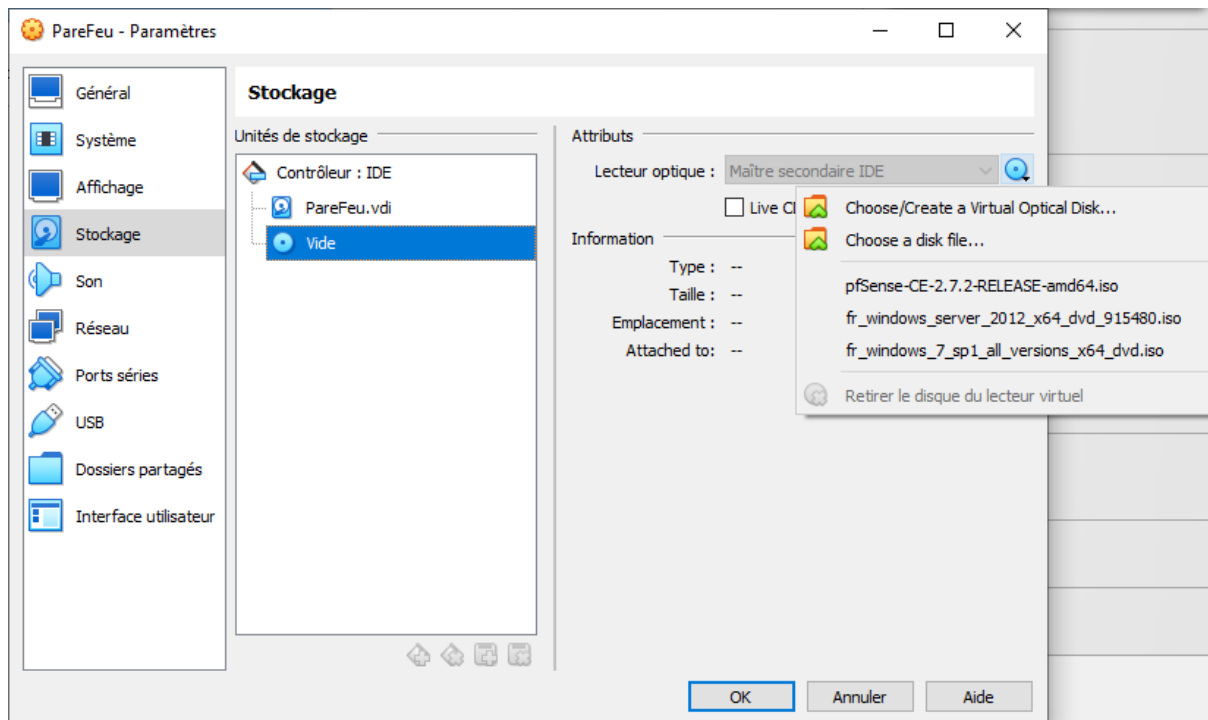
Carte 2 : Mode Réseau privé hôte (LAN).

Installation de pfSense

Démarrer la VM avec l'ISO pfSense.

Suivre les étapes d'installation en gardant les paramètres par défaut.

Éteindre la VM et retirer l'iso :



Après redémarrage, configurer les interfaces réseau :

WAN : 172.17.245.13/16

LAN : 192.168.1.254/24

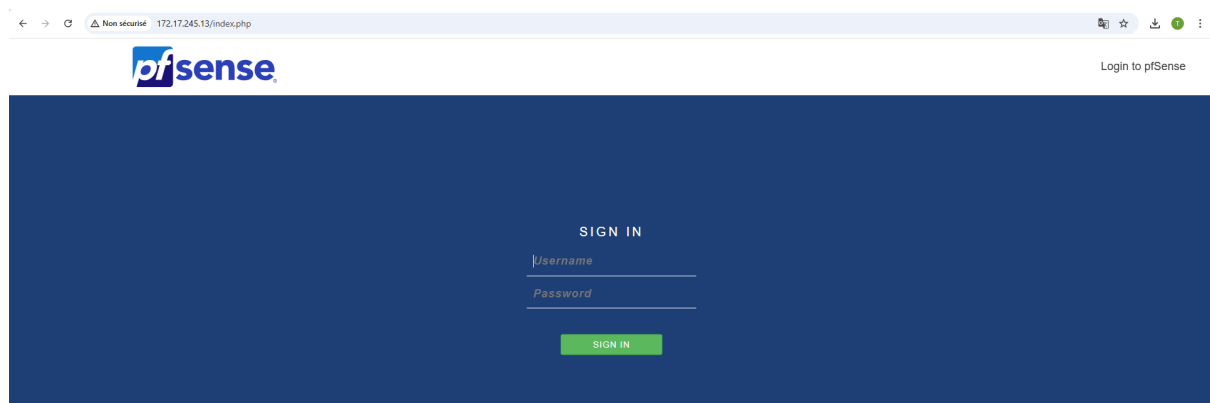
Désactiver DHCP et IPv6 sur l'interface LAN.

2. Configuration via l'interface Web

Connexion à l'interface

Depuis un poste du réseau LAN, ouvrez un navigateur et entrez :

<http://172.17.245.13> ou seulement 172.17.245.13



Si ça ne fonctionne pas :
entrez en mode commande shell

Pour se connecter :

Utilisateur : admin

Mot de passe : pfsense

Suivre l'assistant de configuration :

Nom d'hôte : redline.local

DNS : 8.8.8.8

Serveur NTP : 0.fr.pool.ntp.org

Pensez à modifier le mot de passe administrateur.

3. Configuration du firewall

Vérifier le NAT

Accéder à Firewall > NAT > Outbound.

Vérifier que le NAT automatique est activé pour tradater le LAN vers le WAN.

Autoriser le ping sur WAN



Aller dans Firewall > Rules > WAN.

Désactiver la règle qui bloque tout le trafic privé.

Créez une règle qui autorise uniquement le réseau 172.17.0.0/16 à faire des pings et activez les logs :

Edit Firewall Rule

Action

Pass

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.

Disabled

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

Interface

WAN

Choose the interface from which packets must come to match this rule.

Address Family

IPv4

Select the Internet Protocol version this rule applies to.

Protocol

ICMP

Choose which IP protocol this rule should match.

ICMP Subtypes

Alternate Host
Datagram conversion error
Echo reply
Echo request

For ICMP rules on IPv4, one or more of these ICMP subtypes may be specified.

Source

Source

☐ Invert match

Network

172.17.0.0

/

1

Destination

Destination

☐ Invert match

This Firewall (self)

Destination Address

/

Extra Options

Log

☒ Log packets that are handled by this rule
Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the [Status: System Logs: Settings](#) page).

Ajouter une règle bloquant tout le reste :

Edit Firewall Rule	
Action	Block 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.
Disabled	☐ Disable this rule Set this option to disable this rule without removing it from the list.
Interface	WAN Choose the interface from which packets must come to match this rule.
Address Family	IPv4 Select the Internet Protocol version this rule applies to.
Protocol	TCP Choose which IP protocol this rule should match.
Source	
Source	☐ Invert match Any Source Address /
Destination	
Destination	☐ Invert match This Firewall (self) Destination Address /
Destination Port Range	any From Custom any To Custom Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.
Extra Options	
Log	☒ Log packets that are handled by this rule Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the Status: System Logs: Settings page).

Tester avec un ping depuis un client du réseau WAN.

✗	Mar 11 13:37:14	WAN	Default deny rule IPv4 (1000000103)	i 172.17.12.30:138	i+ 172.17.255.255:138
✓	Mar 11 13:37:19	WAN	USER_RULE (1741626246)	i 172.17.13.11	i+ 172.17.245.13
✗	Mar 11 13:37:24	WAN	Default deny rule IPv4 (1000000103)	i 172.17.12.30:138	i+ 172.17.255.255:138
✗	Mar 11 13:37:25	LAN	Default deny rule IPv4 (1000000103)	i 192.168.1.252	i+ 192.168.1.254
✗	Mar 11 13:37:30	LAN	Default deny rule IPv4 (1000000103)	i 192.168.1.252	i+ 192.168.1.254
✗	Mar 11 13:37:35	LAN	Default deny rule IPv4 (1000000103)	i 192.168.1.252	i+ 192.168.1.254
✗	Mar 11 13:37:40	LAN	Default deny rule IPv4 (1000000103)	i 192.168.1.252	i+ 192.168.1.254

4. Mise en place du filtrage Web

4.1. Installation de Squid (Proxy)

Installation des paquets

Aller dans System > Package Manager > Available Packages.

Installer Squid, SquidGuard et LightSquid.

Configuration de Squid

Si ça marche pas :

Mettre la passerelle dans l'interface web :

Static IPv4 Configuration

IPv4 Address: 172.17.245.13 / 16

IPv4 Upstream gateway: WANGW - 172.17.0.254 [+ Add a new gateway](#)

If this interface is an Internet connection, select an existing Gateway from the list or add a new one using the "Add" button. On local area network interfaces the upstream gateway should be "none". Selecting an upstream gateway causes the firewall to treat this interface as a [WAN type interface](#). Gateways can be managed by [clicking here](#).

Taper cette command dans la vm pfsense :

```
pkg-static install -fy pkg pfSense-repo pfSense-upgrade
```

Aller dans System > Cert Manager.

Donnez un nom au certificat (CSI CA), ne changez rien d'autre.

Accéder à Services > Squid Proxy Server.

Configurez Squid (Local Cache)

- Heap LFUDA, low 90% et high 95%
- Taille du cache 500
- Cache System ufs
- Level 1 directories 16
- Cache location /var/squid/cache
- Memory 64

Dans l'onglet « Général », activez « Enable Squid Proxy » et « Resolve DNS Ipv4 first » :

Squid General Settings

Enable Squid Proxy ☒ Check to enable the Squid proxy.
Important: If unchecked, ALL Squid services will be disabled and stopped.

Resolve DNS IPv4 First ☒ Enable this to force DNS IPv4 lookup first.
This option is very useful if you have problems accessing HTTPS sites.

Activez le proxy transparent (interface LAN)

Transparent Proxy Settings

Transparent HTTP Proxy ☒ Enable transparent mode to forward all requests for destination port 80 to the proxy server.

Transparent proxy mode works without any additional configuration being necessary on clients.
Important: Transparent mode will filter SSL (port 443) if you enable 'HTTPS/SSL Interception' below.
Hint: In order to proxy both HTTP and HTTPS protocols **without intercepting SSL connections**, configure WPAD/PAC options on your DNS/DHCP servers.

Activez “HTTPS/SSL Interception SSL filtering”, sélectionner “Splice All” et le Certificat précédemment créé “CSI CA”.

SSL Man In the Middle Filtering

HTTPS/SSL Interception ☒ Enable SSL filtering.

CA CSI CA 
Select Certificate Authority to use when SSL interception is enabled. 

Activez “Enable Access Logging” et définir combien de jours les logs seront conservés (365 jours).

Logging Settings

Enable Access Logging ☒ This will enable the access log.
Warning: Do NOT enable if available disk space is low.

Log Store Directory /var/squid/logs
The directory where the logs will be stored; also used for logs other than the Access Log above. Default: /var/squid/logs
Important: Do NOT include the trailing / when setting a custom location.

Rotate Logs 365
Defines how many days of logfiles will be kept. Rotation is disabled if left empty.

Sélectionnez “fr” pour “Error language” et Activer “Suppress Squid Version”

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

Cliquez sur “Save” pour enregistrer toutes les modifications effectuées dans Squid

4.2. Configuration de SquidGuard (Filtrage de contenu)

Activer SquidGuard

Aller dans Services > SquidGuard Proxy Filter.

Activer Enable SquidGuard et Enable Log.

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.**

☒ Apply

SquidGuard service state: **STOPPED**

Logging options

Enable GUI log

☐ Check this option to log the access to the Proxy Filter GUI.

Enable log

☒ Check this option to log the proxy filter settings like blocked websites in Common ACL, Group ACL and Target Categories. This option is usually used to check the filter settings.

Enable log rotation

☐ Check this option to rotate the logs every day. This is recommended if you enable any kind of logging to limit file size and do not run out of disk space.

Ajouter une liste noire

Blacklist options

Blacklist

☒ Check this option to enable blacklist

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'

Dans l'onglet Blacklist, insérer l'URL :

http://dsi.ut-capitole.fr/blacklists/download/blacklists_for_pfsense.tar.gz

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).

cliquez sur "Save"

Dans l'onglet "Blacklist" : Cliquer sur "Download" pour télécharger les listes de filtrage.

Blacklist Update

0 %



Enter FTP or HTTP path to the blacklist archive here.

Dans l'onglet 'Common ACL', cliquez, dans "Target Rules List" sur le " + "

Target Rules List + -

ACCESS: 'whitelist' - always pass; 'deny' - block; 'allow' - pass, if not blocked.

Sélectionner les catégories à bloquer ou à autoriser (Sélectionner "Allow" pour Default access [all])

Default access [all]

access

Cochez "Do not allow IP addresses in URL" et "Use SafeSearch engine" puis cliquer "Save".

**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.

**Use SafeSearch
engine**

☒ Enable the protected mode of search engines to limit access to mature content.
At the moment it is supported by Google, Yandex, Yahoo, MSN, Live Search, Bing, DuckDuckGo, OneSearch, Rambler, Ecosia and Qwant. Make sure that the search engines can be accessed. It is recommended to prohibit access to others.
Note: This option overrides 'Rewrite' setting.

4.3. Activation des logs LightSquid

Configurer LightSquid

Accéder à Status > Squid Proxy Reports.

Décochez "LightSquid Web SSL" pour une connexion Web en HTTP et définissez le mot de passe de l'utilisateur admin.

Lightsquid Web SSL

☐ Use SSL for Lightsquid Web Access

This option configures the Lightsquid web server to use SSL and uses the WebGUI HTTPS certificate.

**Lightsquid Web
Password**

.....

Password used to access lighttpd. (Default: pfsense)

Sélectionnez le language French

Sélectionnez "SquidAuth" pour "IP Resolve Method" et "60min" pour "Refresh Scheduler" puis cliquez "Save" et "Refresh Full".

Reporting Settings and Scheduler

IP Resolve Method

Squidauth

Select which method(s) should be attempted (in the order listed below) to resolve IPs to hostnames.

Click Info for details. (Default: DNS) 

AIDE

1. Annexe

2. Commandes utiles

- Pour examiner les erreurs système et les événements. : `journalctl -xe`
- Fichier pour voir les logs : `cat /var/log/syslog`
- voir les 25 dernière ligne d'un fichier : `tail -n 25 /var/log/syslog`
- Voir le début d'un fichier : `head /var/log/syslog`
- Voir l'état du service : `systemctl status *nom du service*`