

ARCHITECTURE

**2ARC**

Projet de fin d’année : Pare-feu

As. Sc. 2

BRAUN Baptiste 224367

DURRHEIMER Alban 223195

SCARATO Romain 225241

THOMAS Quentin 226432

VERRIER Lucas 215196

WURTH François 223616

Version 1.0

Last update: 08/06/2018

Use: Students/Staff

Author: François Wurth

SOMMAIRE



[1 Règles d’analyse (*parsing rules*) Erreur ! Signet non défini.](#_Toc428797841)

[2 Filtrage 3](#_Toc428797850)

[3 Manuel d’utilisation 3](#_Toc428797855)

# Règles d’analyses (*Parsing rules*)

Tous les paquets entrants provenant de toutes les adresses IP sont acceptés par défaut. Dans le cas où l’une des adresses IP est répertoriée dans le fichier de configuration, la ou les règles la concernant sont appliquées.

Par défaut, aucun port n’accepte de connexion entrante ; dans le fichier de configuration seront déterminées les règles spécifiques pour chaque port.

# Filtrage

Les paquets sont redirigés vers une file d’attente personnalisée grâce à *NFQueue* (une méthode de mise en attente des paquets devant être traités) avant d’être traités suivant les règles définies dans le fichier de configuration du pare-feu. Cela déterminera ainsi si le paquet sera autorisé à entrer ou non. En cas d’interdiction, le paquet sera tout simplement rejeté.Haut du formulaire

# Manuel d’utilisation

## Prérequis

Bibliothèque *libpcap*

Afin de pouvoir recompiler le programme, l’installation de la bibliothèque *libpcap* est nécessaire.

* sudo apt install libpcap-dev

(*apt-get* sur des versions antérieures)

Avant de compiler le firewall, il faut installer les bibliothèques *libnfnetlink* et *libnetfilter\_queue* :

* <https://netfilter.org/projects/libnfnetlink/downloads.html>
* <https://netfilter.org/projects/libnetfilter_queue/downloads.html>

Après avoir décompressé les bibliothèques, il faut exécuter les commandes suivantes pour les installer :

./configure

make

sudo make install

Avant d’exécuter le firewall, il faut configurer *iptables* :

sudo iptables -A OUTPUT -p tcp -j NFQUEUE –queue-num 0

sudo sh -c "iptables-save > /etc/iptables.rules"

sudo nano /etc/network/interfaces

add line: pre-up iptables-restore < /etc/iptables.rules