# MANUEL D’UTILISATION

Installation

Pour simplifier l’installation du pare-feu, 2 scripts ont été prévu : le premier pour installer Python et le deuxième pour installer les librairies complémentaires.

**1ère étape : setup.bat**

1. Au lancement de setup.bat, une interface pour l’installation de python s’ouvre.
2. Cochez la case **Add Python 3.6 to PATH**
3. Cliquez sur **Install now**
4. Une fois l’installation terminée, sélectionnez **Disable path lenght limit**
5. L’installation étant terminée, cliquez sur **Close**

En cas de difficultés, vous pouvez télécharger Python depuis python.org, et reprendre l’installation à partir de l’étape 1.2

**2ème étape : setup-dependecies.bat**

1. Pour cette étape, aucune action n’est nécessaire. Il vous suffit de lancer le script

En cas de difficultés, vérifiez que Python a bien été ajouté au variables d’environnement de votre ordinateur. Ce problème peut survenir si Python était déjà installé. Vous pouvez également télécharger les librairies vous-même.

Un raccourcis a été ajouter sur votre bureau. Il ne vous reste plus qu’à l’exécuter en administrateur pour lancer l’invite de commande du pare-feu.

Invite de commande

Après le lancement du programme, une invite de commande se présente, vous pouvez entrer les premières commandes.  
Pour commencer, utilisez la commande « man ». Elle va lister une série de commandes utiles.

ATTENTION : l’invite doit être **obligatoirement** être lancé en tant qu’administrateur.

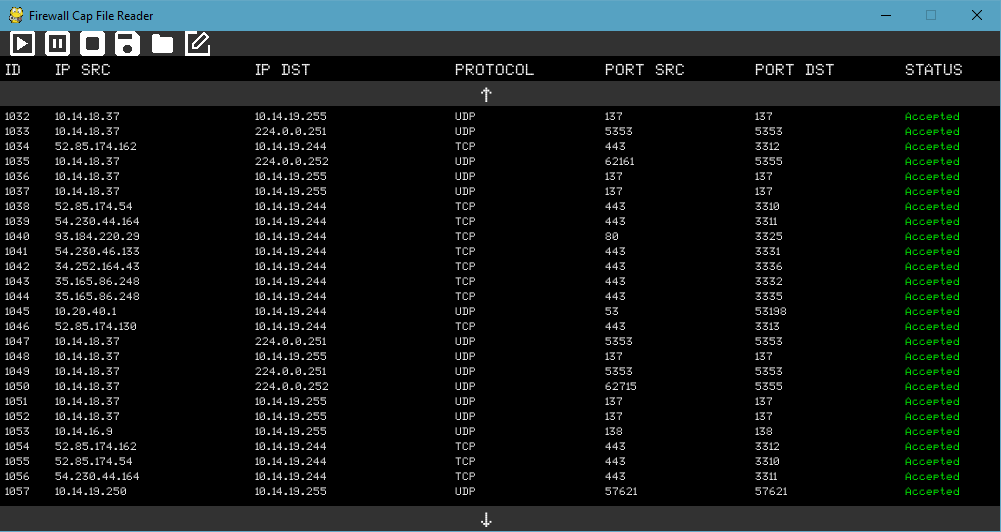
## Commandes

* **man :** affiche la liste des commandes disponibles.
* **start firewall :** lance le pare feu et l’analyse des paquets.
* **stop firewall :** interrompt le pare-feu et son processus d’analyse.
* **start interface :** affiche l’interface graphique.
* **stop interface :** masque l’interface graphique.
* **ban <host name> :** bloque l’accès à une adresse IP d’après son host name.

Ex : *ban rennes-atalante.fr*

* **unban <host name> :** révoque une interdiction d’accès. Ex : *unban rennes-atalante.fr*
* **add rule <rules> :** ajoute une règle et ses propriétés. Ex : *add rule protocol: TCP, portdest: 80*
* **delete rule <index> :** supprime une règle selon son index. Ex : *delete rule 27*
* **read file <path> :** permet de lire un fichier .cap. Ex : *read file C:\Users\user\desktop\mycapfile.cap*
* **show rules :** affiche une liste des règles mises en place.
* **show status :** affiche le statut du pare-feu et de l’interface (ON/OFF).
* **show packets :** affiche les paquets selon un schéma. *(ID, IP source, IP de destination, protocole, port source, port de destination)*
* **exit :** quitte l’invite de commande.

Interface graphique



**Affichage :**

** :** Numéro du paquet

**** : Adresse IP source

 : Adresse IP de destination

 : Protocole réseau utilisé

 : Port source

 : Port de destination

 : Statut du paquet traité

**Fonctionnalités** :

 : Permet la vision en direct des paquets une fois analysés.

 : Met en pause le flux de paquets.

 : Interrompt et masque le flux de paquets.

 : Créé un fichier de capture avec les paquets actuels ou sauvegarde les dernières règles ajoutées via l’interface (selon l’endroit dans lequel on se trouve dans l’interface : vue du flux ou gestionnaire de règles).

 : Permet d’ouvrir et de lire un fichier .pcap (uniquement).

 : Ouvre le gestionnaire de règles.