5.1 Short Manual

The program can be run in two modes, which is set in a configuration file before program start. The absolute path to the configuration file is given as the first and only argument to the program. Wire.py supports two modes: In mode 0 the program will do IP-header manipulations, redirecting traffic. In mode 1 the program will extract payload targeted at a given IP and send it to an external controller via sockets. The section ‘Socket’ holds the information about the socket the program will connect to. Since Wire.py works with unix domain sockets, it needs to be given a path, not an IP/port combination. The socket information is only used in layer 7 mode. The section ‘Filter’ is holding the filtering rules. The field ‘ip’ is the IP:PORT-destination, which will get filtered. In mode 0 the filtered traffic is redirected to ‘targetip’, which is not used in mode 1. It is possible to define ‘ip’ as a ip-port combination, e.g. 10.10.10.11:80. This will then redirect any traffic sent with destination 10.10.10.10:80 to ‘targetip’:80 while all traffic not targeted at the defined port is dropped. It is possible to define multiple ip and ip:port rules. In mode 1 only one IP rule is allowed, along with a arbitrary number of ports. Note that port numbers not filtered will NOT get dropped in mode 1, but are forwarded to the destination host without payload extraction. In both modes, if an IP-rule without port is given, all packets with destination ‘ip’ get filtered, the port is getting ignored. The section ‘Log’ is for logging purposes only. ‘path’ determines where the logfile is written, with any existing file in this place getting overwritten. ‘verbosity’ sets the amount and level of logging.

Wire.py is designed to be run with dpipe, a bidirectional pipe, which is part of VDE (http://vde.sourceforge.net/). Furthermore it is possible to connect several instances of Wire.py to set multiple filters in mode 1 or to get the possibility of filtering for layer 3/4 and layer 7 traffic.

Examples:

```
$ dpipe vde_plug /tmp/vdeswitch1 = python2 Wire.py config =
vde_plug /tmp/deswitch2
$ dpipe vde_plug /tmp/vdeswitch1 = python2 Wire.py config1 =
python2 Wire.py config2 = vde_plug /tmp/vdeswitch2
```