CPSC 526 Assignment 4: Firewall Simulator

By: Pauline Telan (10124075, T02) and Michael Pascual (10107219, T01)

A simple firewall simulator written in Python 3 that reads a list of "rules" contained in a file, reads "packets" fed through standard input one line at a time until eof, and outputs the action taken on the packet.

How to compile/run:

```
python3 fw.py <configfile>
```

configfile	File containing rules for the firewall, containing one rule per line

Rule format:

```
<direction> <action> <ip> <port> [flag]
```

<direction>	Specifies for which direction of traffic this rule applies. Allowed values are "in" or "out"
<action>	Specifies the action (ie. what to do) to be taken when the packet matches this rule. Allowed values are "accept", "drop" and "deny"
<ip>	Defines the IP range for this rule. There are two different ways to specify this: • IP range using CIDR notation, e.g. 136.159.22.0/24 • wildcard for matching any address. i.e. "*"
<ports>	Defines the list of destination ports for which this rule will apply. Each port is an integer between 0-65535. The list can contain one or more ports separated by commas. It is also possible to specify "any" port by using the wildcard "*".
[flag]	This optional field describes whether the rule will be applied only to packets that are part of an established connection or to all packets. If the field is not present, the rule will apply to all packets. If present, the rule will only apply to established packets. If present, the only allowed value is "established".

Packet format:

```
<direction> <ip> <port> <flag>
```

<direction>	Specifies the direction of the packet. Each packet is either incoming or outgoing. The only allowed values are "in" and "out".
<ip>	For incoming packets this specifies the source IP address. For outgoing packets this specifies the destination IP address. In either case, the address will be specified in dot-decimal notation, e.g. 136.159.5.22.
<port>	This specifies the destination port of the packet, and it is an integer between 0-65535.
<flag>	Boolean flag (0 or 1) specifying whether the packet is part of a new (0) session or established (1) session.

Output format:

```
<action>(<rule num>) <direction> <ip> <port> <flag>
```

<action>	The action that the firewall decided should be taken. If no rule could be found for a packet, the action should be "drop".
<rule num>	The line number where the rule responsible for this action can be found. The lines are numbered starting from 1. If no rule could be found for a packet, the line number should be omitted. Note that all lines in the configuration file are numbered, including empty lines and comment lines.
<direction> <ip> <port> <flag>	The fields of the packet.