Bruteforce prevention

Here is an example of how to defend against bruteforce attacks on an SSH port. Please note, that ssh allows 3 login attempts per connection, and the address lists are not cleared upon a successful login, so it is possible to blacklist yourself accidentally.

```
/ip firewall filter
add action=add-src-to-address-list address-list=bruteforce_blacklist address-list-timeout=1d chain=input
comment=Blacklist connection-state=new dst-port=22 protocol=tcp src-address-list=connection3
add action=add-src-to-address-list address-list=connection3 address-list-timeout=1h chain=input comment="Third
attempt" connection-state=new dst-port=22 protocol=tcp src-address-list=connection2
add action=add-src-to-address-list address-list=connection2 address-list-timeout=15m chain=input comment="Second
attempt" connection-state=new dst-port=22 protocol=tcp src-address-list=connection1
add action=add-src-to-address-list address-list=connection1 address-list-timeout=5m chain=input comment="First
attempt" connection-state=new dst-port=22 protocol=tcp
add action=accept chain=input dst-port=22 protocol=tcp src-address-list=!bruteforce_blacklist
```

If the timeouts were kept at 1min for all three lists - connection1/2/3 - then someone could perform 9 guesses every minute, with the above structure they can do a maximum of 3 guesses per 5min.

⚠ Address list naming is following the naming of the Port knocking article. Similar naming scheme is used, trusted address list is named as "secured".