

The Recent Match

- It creates a **dynamic database** of **blacklisted** source IP addresses.

Example:

```
iptables -A FORWARD -m recent --name badguys --update --seconds 60 -j DROP  
iptables -A FORWARD -p tcp -i eth0 --dport 8080 -m recent --name badguys --set -j DROP
```

The list with blacklisted IP addresses is found in: `/proc/net/xt_recent/LIST_NAME`

The Recent Match

Recent match options:

- name:** creates a list in which the source IP address will be added and checked.
- set:** adds the source IP address to the list.
- update:** checks if the source IP address is in the list and updates the "**last seen time**".
- rcheck:** checks if the source IP address is in the list and **DOESN'T update** the "last seen time".
- seconds:** used with **--update** or **--rcheck**. Matches the packet only if the source IP address is in the list and the last seen time is valid.