Watcher-1.5 - Release notes

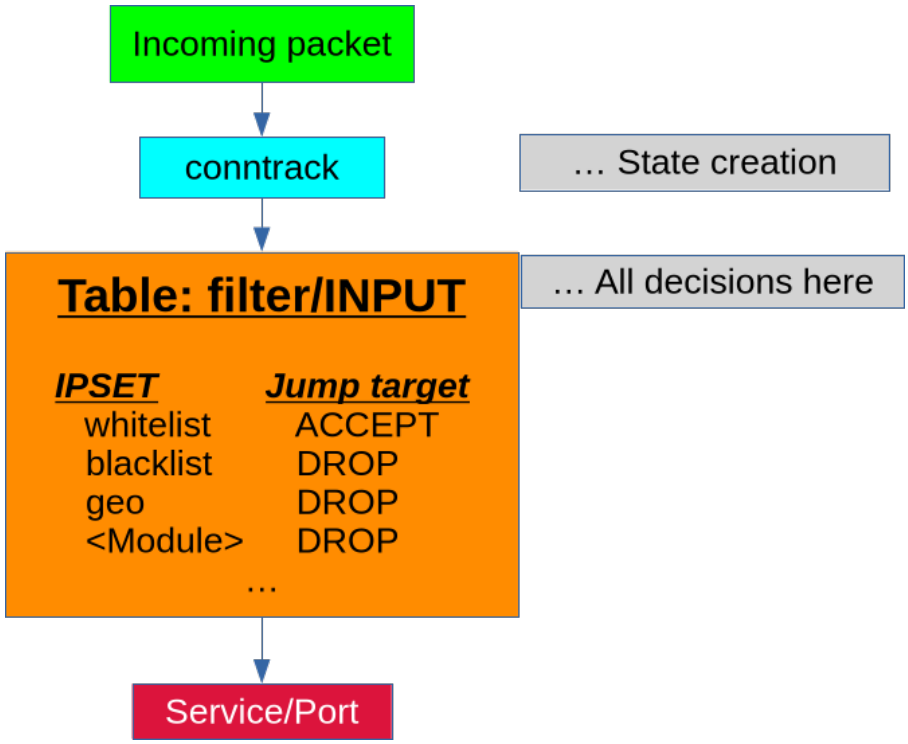
Watcher 1.5 is a consolidation release of Watcher 1.4/Prod

Major changes

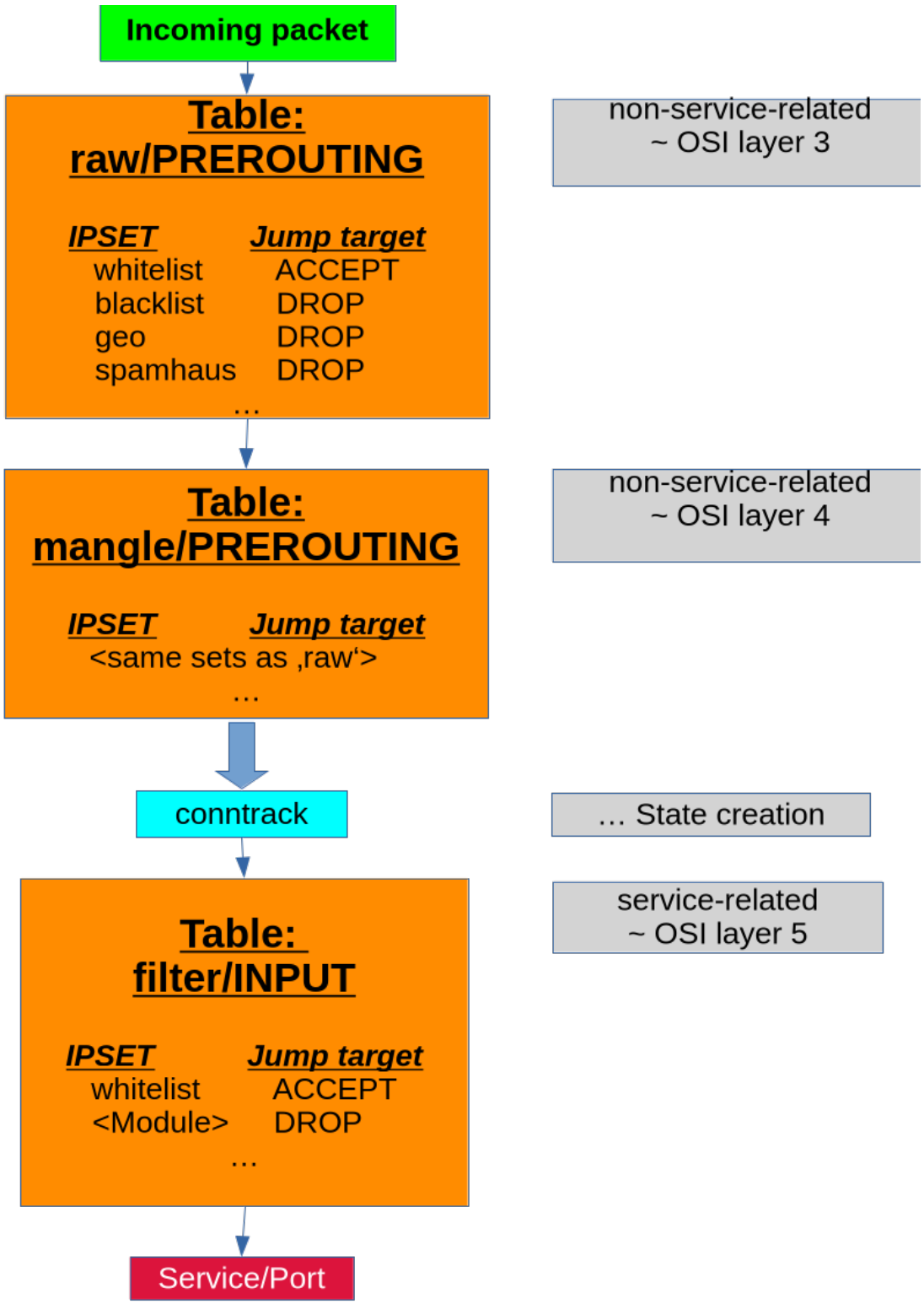
Watcher 1.4 established all IPSETs in the iptables 'filter' table (~OSI level 5; application layer). With the introduction of Geo-Blocking (dynloader 'geo') and Geo-Tracking (Pseudo-module 'GeoTrack')

This showed some flaws under certain circumstances where attackers unleashed requests to service ports that Watcher does not manage, or foreign protocols like ICMP in flood-pings, attacking the network adapter.

Such packets fell through to the 'filter' table and erratically pushed-up the packet counters.



Watcher 1.5 now blocks packets that are 'not_service_related' at 'raw/mangle; PREROUTING' stage which is ~OSI level 3; i.e., simply by their IP address without taking care of protocol and/or service port. This means illegal protocols and or service ports are strictly getting a DROP before reaching the 'filter' stage.



This strictly separates attacks on the NIC (e.g. flood-pings and illegal/unmanaged ports) from attacks on services and avoids that the counters in 'filter' are not pushed-up erratically and reflect the legal access to the services at the 'application layer' (~OSI 5)

(Efficiency-Report; 'Watcher-Report -e')

```
[root@comserve-it-services Watcher-1.5]# Watcher-Report -e
WatcherV1 1.5 - Watcher-Report3 on comserve-it-services.de

===== Connection attempts of DROPed bandits ================
Time stamp    : 2025-12-13 11:03:14
Since         : 2025-12-12 09:42:55
Watcher uptime: 1 d, 01:20:19
IPset comment                          Packets           Bytes
-------------------------------------------------------------

» filter/INPUT (~ OSI level: 5)
Untreated,WBanalyse,404                    296           17720
WatchLG-DB,Login,FAKEHOST                  239           14055
WatchLG-DB,Login,KICKOFF                   384           21624
WatchLG-DB,Login,NXDOMAIN                  864           51644
WatchMX-DB,Mail,FAKEHOST                   147            8756
WatchMX-DB,Mail,NXDOMAIN                  3807          172284
WatchMX-DB,Mail,TRUEHOST                   383           22530
WatchWB-DB,WEB,Bot                        1822          102133
WatchWB-DB,WEB,Destroyer                    36            1751
WatchWB-DB,WEB,Forbidden                   144            8640
WatchWB-DB,WEB,Illegal-Wordpress             1              40
WatchWB-DB,WEB,Illegal-joomla              207           12420
WatchWB-DB,WEB,Trialbaloons                143            8172
custody-[inject],Login,FAKEHOST            668           41848
custody-[inject],Login,NXDOMAIN            582           36568
custody-[inject],Login,TRUEHOST           2350          143588
custody-[kickoff],Login,FAKEHOST           252           15120
custody-[kickoff],Login,NXDOMAIN          1882          115160
custody-[kickoff],Mail,NXDOMAIN           1144           73040
custody-[kickoff],Mail,TRUEHOST              55            2966
custody-[kickoff],WEB                     4932          348051
tarpit,WEB,5                                69           28530

» raw/PREROUTING (~ OSI level: 3)
GeoTrack-DB,GeoTrack,CN                      1              40
blacklisted                                677           74757
custody-low,GeoTrack,IN                    133            7928
custody-low,GeoTrack,PK                     16            1096
custody-low,GeoTrack,RU                    217           12727
geo-ae                                     105            5692
geo-ar                                     119            6672
geo-br                                   13824          834528
geo-by                                       1              52
geo-cn                                    5327          941533
geo-eg                                      58            2984
geo-et                                      12             640
geo-id                                     627           33915
geo-in                                    1547           70753
geo-ir                                     143            7984
geo-pk                                      61            3344
geo-ru                                    2497          146028
```

```
geo-sa                                      8             400
geo-ve                                     31            1616
geo-vn                                    288           16212
geo-za                                     50            2800
spamhaus,drop                           10333          476985

           Total DROPed connections:    56482         3895326
-------------------------------------------------------------

***** Summary ***********************************
           Total DROPed connections:          56482
           Total passed connections:           3737
         Total passthru connections:          13521
          Total records in firewall:          53481

_____ Efficiency ___________________________________
                            Current:          93.70%
                            ... min:          93.10%
                            ... max:          94.60%

..... Legend .....................................

      passthru   - Count of 'white bots'
      TD/TP            ~ Total dropped/passed
      Efficiency = TD / (TD+TP)

[report_efficiency] took 3129 ms
```

Unusually high packet rates now get you a clue whether berserks are messing with access to your NIC (unmanaged ports, flood-pings with ICMP protocll …)

The usual efficiency is at about 86%. A value tremendously above this (far beyond 90%) indicate, that your NIC is attacked by berserks with (D)DOS attacks through flood-ping, port scanners and such.
.