fail2ban for NAT hosts

Centralised fail2ban for NAT firewall

I have a fairly simple setup of a virtual NAT with lxc containers on my host. There's a central rsyslog server running on the host system, all the log from the containers are arriving in there. Therefore setting up iptables per container would not be the best approach, rather creating a single setup on the host itself.

The only issue is, that usually fail2ban uses the INPUT chain, which is not used by the NAT (preroute) table - we need FORWARD. While there is an option to change, named `chain` in the actions.d files, it did not work for me at all, so I ended up with the following actions file for multiport-nat:

```apache
# Fail2Ban configuration file
#
# Author: Cyril Jaquier
# Modified by: Peter Molnar for NAT
#              Yaroslav Halchenko for multiport banning
# $Revision$
#

[Definition]

# Option:  actionstart
# Notes.:  command executed once at the start of Fail2Ban.
# Values:  CMD
#
actionstart = iptables -N fail2ban-<name>
              iptables -A fail2ban-</name><name> -j RETURN
              iptables -I FORWARD -p <protocol> -m multiport --
dports <port> -j fail2ban-<name>

# Option:  actionstop
# Notes.:  command executed once at the end of Fail2Ban
# Values:  CMD
```

```
#
actionstop = iptables -D FORWARD -p <protocol> -m multiport --
dports <port> -j fail2ban-<name>
             iptables -F fail2ban-</name><name>
             iptables -X fail2ban-</name><name>

# Option:  actioncheck
# Notes.:  command executed once before each actionban command
# Values:  CMD
#
actioncheck = iptables -n -L FORWARD | grep -q fail2ban-</
name><name>

# Option:  actionban
# Notes.:  command executed when banning an IP. Take care that
the
#          command is executed with Fail2Ban user rights.
# Tags:    <ip>  IP address
#          <failures>  number of failures
#          <time>  unix timestamp of the ban time
# Values:  CMD
#
actionban = iptables -I fail2ban-<name> 1 -s <ip> -j DROP

# Option:  actionunban
# Notes.:  command executed when unbanning an IP. Take care
that the
#          command is executed with Fail2Ban user rights.
# Tags:    </ip><ip>  IP address
#          <failures>  number of failures
#          <time>  unix timestamp of the ban time
# Values:  CMD
#
actionunban = iptables -D fail2ban-<name> -s <ip> -j DROP

[Init]

# Defaut name of the chain
#
name = default
```

```
# Option:  port
# Notes.:  specifies port to monitor
# Values:  [ NUM | STRING ]  Default:
#
port = ssh

# Option:  protocol
# Notes.:  internally used by config reader for interpolations.
# Values:  [ tcp | udp | icmp | all ] Default: tcp
#
protocol = tcp

# Option:  chain
# Notes    specifies the iptables chain to which the fail2ban
rules should be
#          added
# Values:  STRING  Default: INPUT
chain = FORWARD
```