Configuring IPv6 Firewalls with ip6fw

János Mohácsi

NIIF/HUNGARNET

FreeBSD ip6fw Packet Filtering

Native IPv6 packet filtering interface since FreeBSD4 – without state keeping

Implemented as a multifunction user command

In the kernel it requires:

IPV6FIREWALL – enable, IPV6FIREWALL_VERBOSE – logging, PFIL_HOOKs required in the case of FreeBSD5

The packet passed to the compared firewall is against each of the rules in the firewall ruleset.

When a match is found, the action corresponding to the matching rule is performed and the search terminates.

rule match is updating the rule counters: packet count, byte count

General syntax

- ipfw [rule number] action [log] proto from src to dst

ip6fw actions

- allow | accept | pass | permit
  - Allow packets that match rule. The search ends.
- deny | drop
  - Discard packets that match rule. The search ends.
- unreach code
  - Discard packets that match rule and send ICMPv6 unreachable: admin, notneighbor, addr, noroute, noport
- reset
  - Send TCP reset to initiator
- count
  - Update counters for all packets that match rule. The search continues with the next rule

ip6fw options

- proto
  - all | ipv6
    - All packets match.
  - tcp/udp
    - Only tcp/udp packets match.
  - ipv6-icmp
    - Only ICMPv6 packets match.
- src and dst
  - <address/prefixlend> [ports]
- options
  - frag - non first packets of fragmented packets
  - in/out – way in/way out
  - ipv6options hopopt/route/frag/esp/ah/nonxt/opts
  - icmptypes

ip6fw examples

- Allow DAD
  - ip6fw add pass ipv6-icmp from :: to ff02::/16
- Allow RA,RS, NS, NA and redirect
  - ip6fw add pass ipv6-icmp from fe80::/10 to fe80::/10
  - ip6fw add pass ipv6-icmp from fe80::/10 to ff02::/16
- Allow link-local multicast traffic
  - ip6fw add pass all from fe80::/10 to ff02::/16
  - ip6fw add pass all from ${net}/${prefixlen} to ff02::/16

ip6fw examples/2

- Allow ICMPv6 destination unreachable
  - ip6fw add pass ipv6-icmp from any to any icmptype 1
- Allow PATH-MTU – do not filter!
  - ip6fw add pass ipv6-icmp from any to any icmptype 2
- Allow NS/NA - do not filter!
  - ip6fw add pass ipv6-icmp from any to any icmptype 135,136

End

- Further information
  - The FreeBSD/NetBSD ip6fw manual pages:
    - http://www.freebsd.org/cgi/man.cgi?query=ip6fw
    - mailing list with archive