

## NAME

config.ipfextra - ipf modification configuration file

## DESCRIPTION

Normally the ipf(7) package generates IP filter rules suitable for a firewall under normal circumstances. Sometimes however it is necessary to add or overrule one or more filter lines. This is accomplished through the file config.ipfextra(5). The rules therein are added after the general block rules for packets with IP options on and for ICMP packets of undesirable types, but before all standard anti-spoofing rules.

## EXAMPLES

Normally the generated rules will log all broadcast packets. Use the following rule to overrule this behavior, e.g. to ignore typical DHCP broadcasts on interface eb1 (wrapped for readability):

```
@0 block in quick on eb1 proto udp from 0.0.0.0/32 port eq 68
      to 255.255.255.255/32 port eq 67
```

Normally the firewall will answer all ICMP echo request (ping) packets it receives, even if the packet destination is not (on) the firewall. By using the following two rules the firewall will return an ICMP *host prohibited* response when the destination is not (on) the firewall, e.g. for interface eb1 with IP-address 172.16.2.33:

```
@0 block return-icmp(host-prohib) in log quick on eb1 proto icmp
      from any to any icmp-type echo
@0 pass in quick on eb1 proto icmp from any to 172.16.2.33 icmp-type echo
```

Note the reverse order of the rules because of the use of @0.

For a complete description of the filter syntax see ipf(5).

**FILES**

`/usr/local/config/config.ipfextra`  
Location of the configuration file.

**SEE ALSO**

`config.ipf(5)`, `ipf(7)`.

**BUGS**

Please report bugs to `fwsupport@tunix.nl`.

**AUTHOR**

Copyright 1999-2003 TUNIX Internet Security & Opleidingen

**VERSION**

Version \$Revision: 1.2 \$ \$Date: 2003/05/05 14:03:33 \$ (\$Name: IPF\_01 \$)