IP Filtering

The IP Filtering window allows you view and modify matching criteria used to selectively block certain IP datagrams from being sent or received. Each row in the table corresponds to a single filter or set of matching criteria.

To Add or Remove a filter table entry, select a row from the table if desired. This will copy the corresponding information to the edit fields in the "Configure Entry" area. Use the edit fields and controls in this area to change the information as desired, and then press "Add" or "Remove" to update the table. New filters are added at the top of the list.

The "Port Name" column specifies the physical port on which the filter will be applied.

The "Direction" column specifies whether the filter is applied to datagrams being sent, or being received from the corresponding port.

The "Action" column specifies what IPNetRouter should do when it detects a matching datagram. "Pass" lets the datagram through immediately without comparing against any other filters. "Block" deletes the datagram immediately. "NoDial" will prevent matching datagrams from initiating a PPP connection if Dial On Demand is enabled while allowing the packet through. "Trigger" blocks the datagram and also causes IPNetRouter to install a filter to block subsequent traffic from that source IP address for approximately 2 hours. Triggers can be used to block port scanning based attacks. When a port scanner hits a trigger port, that host is immediately cut off from accessing your network without any response. To the host scanning for an open port, your gateway or network does not appear to exist. Selecting Action "Log" sends the first 64 bytes of any matching datagrams to a companion application (IPNetSentry) that has requested logging information and allows the packet through (similar to Pass). Normally only rejected (blocked) packets are logged along with a reason code for why they were rejected (bad header checksum, filter match, etc.). The "Log" feature can be used to examine packet headers (IP, TCP, UDP, ICMP,...) for all traffic that matches a particular service or address for example.

The "Protocol" column allows the filter to match a specific protocol (from the IP header), or any protocol.

The "TCP Ack" column allows you to specify whether the ACK bit in the TCP header must be zero or one.

The "Source Net" and "Dest Net" are used to specify a range of IP addresses for the source and destination address in the IP header. The network number or range of addresses is specified as an IP address followed by a prefix length (also known as a CIDR aggregate). For example: "192.168.0.1/24" matches all IP datagrams to/from network 192.168.0.x (192.168.0.0-192.168.0.255). You can use the Subnet Calculator to compute the CIDR aggregates for a range of IP addresses. If you omit the prefix

length, the entire IP address will be matched (prefix length 32). If you leave the network number empty (or 0.0.0.0), any IP address will be matched. You can use IP address 0.0.0.1 to represent the dynamically assigned IP address used as the Apparent address for IP masquerading.

The "Source Ports" and "Dest Ports" are used to specify a range of TCP or UDP protocol port numbers. You can specify a single port number such as "80" or a range of port numbers such as "1-1023". If you leave the port range empty, any port number will be matched. For ICMP datagrams, the Source Ports match the ICMP Type and the Dest Ports match the ICMP Code. To block all echo requests (pings) for example, you could create a filter to match ICMP type=8.

Each filter is checked in the order listed. If a packet matches a "block" filter, it is deleted immediately. If a packet matches a "pass" filter, it is allowed through immediately (regardless of any block filters that may follow). If a packet does not match any filters, it is allowed through. Filtering is performed before Network Address Translation (NAT) for outgoing packets, and after NAT for incomming packets (so LAN clients can be distinguished).

Use the "Refresh" button to update the display of filters currently defined. Any filters you specify will be remembered as part of an IPNetRouter configuration when you Save from the File menu. A maximum of 250 filters can be specified at this time.

Detailed instructions for using IPNetRouter are available on the Sustainable Softworks web site at <http://www.sustworks.com>.