CHAPTER 11

TCP/IP Filtering

Main TCP/IP Filtering Dialog Box

To access this dialog box (Figure 11-1), select Global/Filtering/TCP/IP Filtering from the Device View.

Figure 11-1 Main TCP/IP Filtering Configuration Dialog Box

Route Filters Button

This button brings up a filter editor screen for creating route filters. The filter editor screen is described in the "TCP/IP Filter Editor Window" section on page 11-2.

Packet Filters Button

This button brings up a filter editor screen for creating packet filters.The filter editor screen is described in the "TCP/IP Filter Editor Window" section on page 11-2.

TCP/IP Route Filters

This set of pull-downs allows you to select previously defined sets of internetworking device filter rules. These rules are global for the device and are not associated with any interface. Up to four sets of rules can be selected.

Block IP Source Routing

This check box sets a filter in the device which drops any received packet which has the "source route" option set.

Log Rejected Source-Routed Packets

This checkbox tells the device to add a log entry (if logging is turned on) whenever the **Block IP Source Routing** checkbox is set and a packet is received with the source route option set. See the "Logging Configuration Dialog Box" section on page 14-25 for more information.

TCP/IP Filter Editor Window

The editor window (Figure 11-2) is used in the VPN 5000 Manager for editing all TCP/IP filter sets, including those for TCP/IP Route and Packet filters. The editor window type can be identified by the text at the top of the window, and will only allow you to create or select the type of filter set for which it was selected.

Figure 11-2 TCP/IP Filter Editor Window

Filter Editor Dialog Box Buttons and Controls

- The **Current Filter** pull-down menu lets you select a filter set for editing.
- The **New** button lets you create a new set of filter rules. A dialog box will pop up to ask you to name the filter set. The name must be 16 characters or less.
- The **Delete** button lets you delete the selected set of filter rules.
- The **Rename** button lets you rename the selected set of filter rules.

- The **Import** button lets you import a previously exported set of filter rules, or a text file in which you have stored filter rules. A file dialog box will pop up to ask you to locate an import file.
- The **Export** button lets you export a set of filter rules to disk. A dialog will pop up to ask you to name the export file.

TCP/IP Route Filter Rules

To access an editor window for TCP/IP route filters, open the Main TCP/IP Filtering dialog box (under Global/Filtering/TCP/IP Filtering) and then select the **Route Filters** button.

Route filtering rules are applied globally in the device and are not associated with any interface. However, they can be restricted to an interface using the "from" or "to" modifiers in the rule.

A device does not reorder rule sets as they have been specified before they are applied. They are applied in the order they were written. When multiple filter sets are selected with the VPN 5000 Manager, the filter sets will be concatenated in the device from first to last (top to bottom on screen).

Any IP network not explicitly allowed by the rules will not be included in the routing table on input or in the routing update on output. To allow all other network numbers not filtered, the last rule must be:

```
permit 0.0.0.0
```

Because direct and static routes are configured in the device and not received via an interface, they are always installed and cannot be filtered.

Rules that have been specified using the Manager may be edited or examined through the command line interface, and vice-versa. When the rules are downloaded into the device from the VPN 5000 Manager, they will be encrypted.

Rule sets that have been created with the TCP/IP Route Filter Editor Window must be applied using the pull-down menus in the Main TCP/IP Filtering dialog box.

Basic IP Route Filter Rules and Syntax

At a minimum, every non-comment line in a filter set must include an action, and an IP address. Together these components specify a filter rule that the device will follow when sending and/or receiving IP routing packets.

Every line in a route filter set must begin with the actions **permit** or **deny**, or the comment indicator **#**.

- Lines which begin with **permit** specify that information from routing packets meeting the conditions should be included in the IP routing table.
- Lines which begin with **deny** specify that information from packets meeting the conditions should not be included in the IP routing table.
- Lines which begin with **#** specify that the text on the line is a comment and should be ignored.

Every line which begins with permit or deny must be followed by an IP address. This IP address can be specified in a number of different ways.

- Addresses can be specified in **dotted-decimal notation**. If the rightmost components are 0, they are treated as wildcards. For example, 128.138.12.0 matches all hosts on the 128.138.12 subnet. An address with all zeros matches anything.

- A **factorized format** can also be used where a set of components are substituted into an address. These addresses take the form of #.#.#.{#,#,...}. For example, 192.12.9.{1,2,15} matches the hosts 192.12.9.1, 192.12.9.2, and 192.12.9.15. The factor set must be at the end of the address, but addresses of the form #.{#,#,...}, #.#.{#,#,...}, etc., are allowed. Any components past the factor set's position are implicitly assumed to be 0.
- IP addresses may also be specified as a **hexadecimal number** (for example, 0x82cc0801 matches the host address 130.204.8.1).

Any address may have an optional **/bits** field at its end. This denotes the number of bits, starting with the most significant, that will be considered by the device when it compares the address in a routing packet to the filter rule. For example, an address specified in the rules as 192.15.32.0/19 would match all host addresses from 192.15.32.1 to 192.15.63.255.

Any part of an address which is past the number of significant bits specified is ignored and assumed to be zero.

IP Route Filter Rule Options

A direction can optionally be specified with **in**, **out** or **both**. If no direction is specified, **both** is assumed.

- Filter rules specifying **in** are only applied to routing packets coming into the device.
- Filter rules specifying **out** are only applied to routing packets being sent from the device.
- Filter rules specifying **both** are applied to routing packets in both directions.

IP Route Filter Rule Modifiers

Filter rules can be modified with the following parameters. When used, the modifiers must be put in a filter rule in the order shown. By default, a filter rule is applied to all routing data.

- **via** <protocol(s)> This modifier specifies that the filtering rule should only be applied to routing data being received or transmitted by the designated routing protocol. Allowed values are **icmp**, **rip**, and **ripv2**. Multiple protocols may be listed, each separated by white space. The **icmp** keyword implies redirected routes.
- **origin** <protocol(s)> This modifier limits output rules to routes originating from the designated protocol. Allowed values are **icmp**, **rip**, **ripv2**, **static**, and **direct**. Multiple protocols may be listed, each separated by white space.
- **metricin** <increment value> This modifier tells the device to increment the metric on incoming routes which match the filter rule. The metric is the number of routers on a route. By increasing or decreasing the metric, a particular route can be made more or less attractive. The value to increment by can be from 1 to 15.
- **metricout** <increment value> This modifier tells the device to increment the metric on outgoing routes which match the filter rule. The metric is the number of routers on a route. By increasing or decreasing the metric, a particular route can be made more or less attractive. The value to increment by can be from 1 to 15.
- **from** <IP address> *or* **from** <interface> This modifier tells the device to apply the rule only to routes coming from a specified IP address (where the address is in the same format), or interface (e.g. Ethernet 0, WAN 1, etc.).

- **to** <IP address> *or* **to** <interface> This modifier tells the device to apply the rule only to routes being sent to a specified IP address (where the address is in the same format), or interface (e.g. Ethernet 0, WAN 1, etc.).

IP Route Filter Rule Notification

Filter rule matches can optionally cause a log message to be sent. By default, no logging of matches is performed. See the "Logging Configuration Dialog Box" section on page 14-25 for more information.

- **log** The log option causes the device to log data about the packet to syslog when the condition of the rule is met.

IP Route Filter Rule Examples

The following example specifies a rule to allow routes to be input only from RIP and only from 198.41.11.1.

```
permit 0.0.0.0 in via rip from 198.41.11.1
```

The following specifies that routing information should only be sent which originates from RIP, directly connected routes, and static routes.

```
permit 0.0.0.0 out origin rip direct static
```

TCP/IP Packet Filter Rules

Due to the nature of the IP protocol, IP packet filtering can be quite complicated. If you are attempting to design and implement a comprehensive set of filters, or an Internet Firewall, there are a number of references you should consult.

Two good starting points are: Building Internet Firewalls, by D. Brent Chapman and Elizabeth D. Zwicky, O'Reilly & Associates, 1995, and Firewalls and Internet Security, by William R. Cheswick and Steven M. Bellovin, Addison-Wesley Publishing Company, 1994.

To access a filter editor window for TCP/IP packet filters, open the Main TCP/IP Filtering dialog box (under Global/Filtering/TCP/IP Filtering) and then select the **Packet Filters** button.

Packet filtering rules are selected for individual device interfaces. Whether they are used as input filters, output filters, or both, depends on which pulldown is used to select them in the TCP/IP Filtering dialog box for a particular interface.

A device does not reorder rule sets as they have been specified before they are applied. They are applied in the order they were written. When multiple filter sets are selected with the Manager, the filter sets will be concatenated in the device from first to last (top to bottom on screen).

Any IP packet not explicitly allowed by the rules will be filtered. To allow all other packets not filtered, the last rule must be:

```
permit 0.0.0.0 0.0.0.0 ip
```

Rules that have been specified using the Manager may be edited or examined through the command line interface, and vice-versa. When the rules are downloaded into the device from the VPN 5000 Manager, they will be encrypted.

Basic IP Packet Filter Rules and Syntax

At a minimum, every non-comment line in a filter set must include an action, a source IP address, and a destination IP address. Together these components specify the action to be taken when a packet meets the condition of the rule.

Every line in a packet filter set must begin with the actions **permit** or **deny**, or the comment indicator **#**.

- Lines which begin with **permit** specify that packets meeting the conditions should be passed through the filter.
- Lines which begin with **deny** specify that packets meeting the conditions should be dropped by the filter.
- Lines which begin with **#** specify that the text on the line is a comment and should be ignored.

Every line which begins with permit or deny must be followed by a source and destination IP address. These IP addresses can be specified in a number of different ways.

- Addresses can be specified in **dotted-decimal notation**. If the rightmost components are 0, they are treated as wildcards. For example, 128.138.12.0 matches all hosts on the 128.138.12 subnet. An address with all zeros (0.0.0.0) matches anything.
- A factorized format can also be used where a set of components are substituted into an address. These addresses take the form of #.#.#.{#,#,...}. For example, 192.12.9.{1,2,15} matches the hosts 192.12.9.1, 192.12.9.2, and 192.12.9.15. The factor set must be at the end of the address, but addresses of the form #.{#,#,...}, #.#.{#,#,...}, etc., are allowed. Any components past the factor set's position are implicitly assumed to be 0.

When the factorized format is used, one line is substituted for many. However, when the device reads the filters and installs them, it expands each address into a separate rule. In the example given, three rules would be created. This can make the number of rules to process greater, which can affect performance.

- IP addresses may also be specified as a hexadecimal number (for example, 0x82cc0801 matches the host address 130.204.8.1).

Any address may have an optional **/bits** field at its end. This denotes the number of bits, starting with the most significant, that will be considered by the device when it compares the address in a packet to the filter rule. For example, an address specified in the rules as 192.15.32.0/19 would match all host addresses from 192.15.32.1 to 192.15.63.255.

Any part of an address which is past the number of significant bits specified is ignored and assumed to be zero.

IP Packet Filter Rule Operators and Port Names

Filter rules can accept certain modifiers, described in the "IP Packet Filter Rule Modifiers" section on page 11-8. All of these modifiers use a set of expression operators to allow information in a packet to be compared to the modifier's parameters.

- **eq**, **==**, or **=** These are allowable ways of writing an "equality" operator which will match a packet if its port number is equal to the port specified in the modifier.
- **lt** or **<** These are allowable ways of writing a "less than" operator which will match a packet if its port number is less than the port specified in the modifier.
- **lteq**, **le**, **<=**, or **=<** These are allowable ways of writing a "less than or equal to" operator which will match a packet if its port number is less than or equal to the port specified in the modifier.

- **gt** or **>** These are allowable ways of writing a "greater than" operator which will match a packet if its port number is greater than the port specified in the modifier.
- **gteq**, **ge**, **>=**, or **=>** These are allowable ways of writing a "greater than or equal to" operator which will match a packet if its port number is greater than or equal to the port specified in the modifier.
- **ne**, **<>**, or **!=** These are allowable ways of writing an "inequality" operator which will match a packet if its port number is not equal to the port specified in the modifier.

In rules where expressions are used, the syntax checker requires a space before and a space after the expression operator(s).

All of the modifiers also require a port number between 0 and 65535. Port numbers can also be specified using the names in of services with known ports in Table 1.

Table 1 IP Pack Filter Rule Modifiers

TCP ports:		
systat (11)	netstat (13)	ftp-data (20)
ftp (21)	telnet (23)	smtp, mail (25)
whois (43)	gopher (70)	rje (77)
pop-2 (109)	pop-3 (110)	auth (113)
nntp, usenet (119)	netbios-ssn (139)	news (144)
rexec (512)	rlogin (513)	rshell (514)
printer, lpd (515)	uucp (540)	listen, rfs (1025)
x, xwin (6000)	irc (6667)	www, http (80)
UDP PORTS:		
name (42)	bootps (67)	bootpc (68)
tftp (69)	snmp (161)	snmp-trap (162)
biff, comsat (512)	rwho (513)	syslog (514)
talk (517)	ntalk (518)	route, rip (520)
timed (525)	mount (635)	pcnfs (640)
nfs (2049)		
COMMON UDP AND TCP PORTS:		
echo (7)	discard (9)	daytime (13)
chargen (19)	time (37)	dns, domain (53)
sunrpc, rpc, portmapper (111)	ntp (123)	netbios-ns (137)
netbios-dgm (138)		
ICMP TYPES:		
echo-reply (0)	dest-unrch (3)	src-quench (4)
redirect (5)	echo, ping (8)	time-exceed (11)
param-prob (12)	time (13)	time-reply (14)
info (15)	info-reply (16)	mask (17)
mask-reply (18)		

RFC 1700 "Assigned Numbers" contains a listing of all currently assigned IP protocol keywords and numbers.

IP Packet Filter Rule Modifiers

These modifiers act to restrict the type of packets which will match a filter rule.

1. **IP**

   This option specifies that all packets from the source and destination IP address and mask will match this rule. If no particular IP protocol packet type (**TCP**, **UDP**, **ICMP**, **GRE**, **AH**, **ESP** or **OSPF**) is specified, **IP** is assumed.

2. The IP protocols, other than IP itself, may be specified as a decimal number or as a keyword. The supported keywords are followed by their protocol numbers for your reference.

   - TCP (6)
   - UDP (17)
   - ICMP (1)
   - GRE (47)
   - AH (51)
   - OSPF (89)
   - ESP (50)

3. **TCP**

   or TCP src <expression> <port>

   or TCP dst <expression> <port>

   or TCP est

   or TCP src <expression> <port> est

   or TCP dst <expression> <port> est

   This modifier allows filtering on TCP (Transmission Control Protocol) packets. A source or destination port may be filtered by including the **src** or **dst** specifiers, followed by a logical expression and a port.

4. **est** keyword allows a rule to be established in which an external connection to a particular port is not allowed, but two way traffic established by an internal machine will pass through the device.

   The device performs this operation by examining the flags in the TCP header. When a session is being established, the first packet only contains the "SYN" flag while subsequent packets contain the "ACK" flag. A permit packet filter rule using the **est** keyword will not match a packet with only the "SYN" flag and the packet will be dropped. Unless another rule allows it through, the "SYN" packet doesn't reach its destination, no reply will be returned to the sender, and a connection will never be established.

   Examples using the **est** keyword are shown later in this chapter.

5. **UDP**

   or UDP src <expression> <port>

   or UDP dst <expression> <port>

   This modifier allows filtering on UDP (User Datagram Protocol) packets. A source or destination port may be filtered by including the optional **src** and **dst** specifiers, followed by a logical expression and a port, as described in Table 1.

   The VPN 5000 Manager uses UDP port 33020. Care should be taken not to deny this port if Manager configuration is desired.

6. **ICMP**, or **ICMP type** <expression> <port>

   This modifier allows filtering on ICMP (Internet Control Message Protocol) packets. The ICMP type may be filtered by using the type specifier and the list of types from Table 1.

7. **GRE**

   This modifier allows filtering on GRE (Generic Routing Encapsulation) packets. GRE provides a simple, general purpose mechanism to encapsulate network protocols into IP for the purpose of tunneling across the Internet.

   If VPN tunneling without authentication is enabled on an interface to which an IP filter is applied, then the filter must specifically **permit** GRE packets.

8. **AH**

   This modifier allows filtering on AH (Authentication Header) packets. AH is used for authentication of tunneled packets across the Internet.

   If VPN tunneling with authentication is enabled on an interface to which an IP filter is applied, then the filter must specifically **permit** AH packets.

9. **ESP**

   This modifier allows filtering on ESP (Encapsulating Security Payload) packets. ESP is used for encryption of tunneled packets across the Internet.

   If VPN tunneling with encryption only (i.e. no authentication) is enabled on an interface to which an IP filter is applied, then the filter must specifically **permit** ESP packets.

10. **OSPF**

    This modifier allows filtering on OSPF (Open Shortest Path First) packets. OSPF IP packets carry OSPF routing data.

11. **proto** <operator> <protocol number>

    This modifier allows general filtering of IP protocol numbers that don't have established keywords. The rule also allows an expression to be specified which allows filtering on ranges of protocol numbers (i.e. proto > 51).

IP Packet Filter Rule Notification

There are two notification actions which the device can take when a packet matches a particular rule. By default, no logging or notification of matches is performed.

- **log** The log option causes the device to log data about the packet to syslog when the condition of the rule is met. See the “Logging Configuration Dialog Box” section on page 14-25 for more information.
- **icmp** The icmp option is valid only on a **deny** rule and directs the device to return an ICMP notification to the source of the matching packet.

Simple IP Packet Filter Rule Examples

This rule allows TCP packets with a source port greater than or equal to 1024 and a destination port of 25 (SMTP mail):

```
permit 0.0.0.0 0.0.0.0 TCP src >= 1024 dst = 25
```

A rule to allow UDP packets with a source port greater than 910 and a destination port of 53 (Domain Name Service) would look like:

```
permit 0.0.0.0 0.0.0.0 UDP src > 910 dst = 53
```

A rule to deny ICMP echo request (pings) would look like:

```
deny 0.0.0.0 0.0.0.0 ICMP type = 8
```

This rule would drop all packets with the source host address 192.15.1.10:

```
deny 192.15.1.10 0.0.0.0
```

A rule to drop all packets with a source network address of 192.15.1.0. All packets from hosts on that network would be denied:

```
deny 192.15.1.0/24 0.0.0.0
```

IP Packet Filter Rule Set Examples

The following rule set allows only inbound and outbound mail from 192.15.14.1.

The input-filter:

```
permit 0.0.0.0 192.15.14.1 TCP src >= 1024 dst = 25
permit 0.0.0.0 192.15.14.1 TCP src = 25 dst >= 1024
```

The output-filter:

```
permit 192.15.14.1 0.0.0.0 TCP src = 25 dst >= 1024
permit 192.15.14.1 0.0.0.0 TCP src >= 1024 dst = 25
```

These sets of rules are intended to filter out all traffic and only allow incoming and outgoing mail to a server inside a net with an IP address of 192.15.14.1. However they aren't enough to prevent access from someone outside using source port 25. This is because a connection to destination ports greater than 1024 can be initiated according to the second rule in the input filter. To prevent this from happening, add the **est** keyword to the second rule in the input filter:

```
permit 0.0.0.0 192.15.14.1 TCP src = 25 dst >= 1024 est
```

The **est** keyword in this rule tells the device to only accept TCP packets on the input to this interface when the connection has already been established. A TCP packet which is attempting to initiate a connection will have only the "SYN" flag set. If someone tries to establish a connection from the outside using source port 25, the rule won't match (no permit will occur). The connection can't be established since the packet will be dropped by the default rule.

TCP/IP Packet Filtering: Interface Dialog Box

To access this dialog box (Figure 11-3), select Interface/Filtering/TCP/IP Filtering from the Device View. This can be done for any type of interface except IP subinterfaces.

Figure 11-3 Interface TCP/IP Packet Filtering Configuration Dialog Box

Input Filters

This set of pulldowns allows you to select previously defined sets of packet filter rules. These rules will be applied to packets arriving on this interface. Up to four sets of rules can be selected.

Output Filters

This set of pulldowns allows you to select previously defined sets of packet filter rules. These rules will be applied to packets which are to be sent on this interface. Up to four sets of rules can be selected.