CHAPTER 12

IPX Filtering

Main IPX Filtering Dialog Box

To access this dialog box (Figure 12-1), select Global/Filtering/IPX Filtering from the Device View.

Figure 12-1 Main IPX Filtering Configuration Dialog Box

IPX Route Filters

This set of pull-down menus allow you to select previously defined sets of internetworking device filter rules that operate on the IPX Routing Information Protocol (RIP). These rules are global for the device and are not associated with any interface. Up to four sets of rules can be selected.

IPX SAP Filters

This set of pull-down menus allow you to select previously defined sets of internetworking device filter rules that operate on the IPX Service Advertising Protocol (SAP). These rules are global for the device and are not associated with any interface. Up to four sets of rules can be selected.

IPX Filter Editor Window

The IPX Filter ditor window (Figure 12-2) is used in the VPN 5000 Manager for editing all IPX filter sets, including those for IPX Route, SAP, 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 12-2 IPX Filter Editor Window

Filter Editor Window 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 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 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.

IPX Packet Filter Rules

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

Packet filtering rules are applied on a per interface basis. Whether they are used as input filters, output filters, or both, depends on which pulldown is used to select them in the IPX 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 IPX packet not explicitly allowed by the rules will not be passed through the filter. To allow all other packets not filtered, the last rule must be:

```
permit
```

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 IPX Packet Filter Rules and Syntax

At a minimum, every non-comment line in a filter set must include an action. However, an action alone will not create a useful filter rule, except for setting a default 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 a packet meeting the conditions should be passed by the filter.
- Lines which begin with **deny** specify that a packet 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.

IPX Packet Filter Options

The basic action specified in the rule will almost always be accompanied with an option. IPX Packet filter options use some or all of a set of operators to determine whether the filter rule matches information in a packet or not. These operators are:

- **eq**, **==**, or **=** These are allowable ways of writing an “equality” operator which will match if the value in the packet is equal to the value specified in the option expression.
- **lt** or **<** These are allowable ways of writing a “less than” operator which will match a packet if its value is less than the value specified in the option expression.
- **lteq**, **le**, **<=**, or **=<** These are allowable ways of writing a “less than or equal to” operator which will match a packet if its value is less than or equal to the value specified in the option expression.
- **gt** or **>** These are allowable ways of writing a “greater than” operator which will match a packet if its value is greater than the value specified in the option expression.
- **gteq**, **ge**, **>=**, or **=>** These are allowable ways of writing a “greater than or equal to” operator which will match a packet if its value is greater than or equal to the value specified in the option expression.
- **ne**, **<>**, or **!=** These are allowable ways of writing an “inequality” operator which will match if the value in the packet is not equal to the value specified in the option expression.

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

The options available for IPX Packet filter rules allow rules to be more narrowly specified to exclude all but certain **types** of packets, packets with a given source network number (**srcnet**), packets with a specified destination network numbers (**dstnet**), packets with a particular source socket number (**srcskt**), packets with a selected destination socket number (**dstskt**), packets with a chosen source node address (**srcnode**), and/or packets with a stated destination node address (**dstnode**).

- **type** <operator> <IPX packet type> This option allows filtering using the IPX packet **type** contained in the packet. The IPX packet type value must be a hex number. The keyword **all** may be used to specify all network number values.

  For some versions of NetWare, the packet type field is not a reliable indicator of the type of packet encapsulated by the IPX header. Generally, the source and destination sockets should be used to implicitly filter the packet type. NetBIOS propagate packets (type 14h) are an exception to this rule.
- **srcnet** <operator> <network number> This option allows filtering of the source network number contained in the packet. The number is specified in hex. The keyword **all** may be used to specify all network number values.
- **dstnet** <operator> <network number> This option allows filtering of the destination network number contained in the packet. The number is specified in hex. The keyword **all** may be used to specify all network number values.
- **srcskt** <operator> <socket number> This rule allows filtering of the source socket contained in the packet. The number is specified in hex.

  The following keywords may be used for well known socket values: **NCP**(0451h), **SAP**(0452h), **RIP**(0453h), or **DIAG**(0456h). The keyword **all** may be used to specify all socket numbers.
- **dstskt** <operator> <socket number> This rule allows filtering of the destination socket contained in the packet. The number is specified in hex. The keywords listed for **srcskt** may also be used. The keyword **all** may be used to specify all socket numbers.
- **srcnode** <operator> <node address> This rule allows filtering of the source node address contained in the packet. The operator in this option can only be “equality” or “inequality.”

  The node address parameter is the IPX server node number specified as an Ethernet address. An Ethernet address is specified as six hexadecimal octets separated by dots or colons (e.g. 0.0.A5.0.0.1 or 0:0:A5:0:0:1). The keyword **all** may be used to specify all node values.
- **dstnode** <operator> <node address> This rule allows filtering of the destination node address contained in the packet. The operator in this option can only be “equality” or “inequality.” The address parameter should be entered as shown for **srcnode**. The keyword **all** may also be used.

IPX Packet 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 keyword causes the device to send information about the packet to syslog when the condition of the rule is met.

IPX Packet Filter Rule Examples

Drop all packets where the source network number is greater than or equal to 1000 and permit all other packets:

```
deny srcnet >= 1000
permit type = ALL
```

Drop all packets from a specific IPX network and node and permit all other packets:

```
deny srcnet = FAB4 srcnode = 0.0.A5.0.0.1
permit
```

Drop all packets where the source socket is a diagnostic packet, log the denial and permit all other packets through:

```
deny srcskt = DIAG log
permit
```

IPX Route Filter Rules

To access an editor window for IPX Route filters, open the Main IPX Filtering dialog box (under Global/Filtering/IPX 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 IPX 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 network = ALL
```

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 Manager, they will be encrypted.

Rule sets that have been created with the IPX Route Filter Editor Window must be selected using the pull-downs in the Main IPX Filtering dialog box.

Basic IPX Route Filter Rules and Syntax

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

Every line in an IPX Route filter set must begin with the actions **permit** or **deny**, or the comment indicator **#**.

- Lines which begin with **permit** specify that information meeting the conditions should be included in the IPX routing table.
- Lines which begin with **deny** specify that information meeting the conditions should not be included in the IPX routing table.

- Lines which begin with **#** specify that the text on the line is a comment and should be ignored.

The network expression uses a set of operators to specify the conditions under which the rule will be satisfied. These operators are:

- **eq**, **==**, or **=** These are acceptable ways of writing an "equality" operator which will match if the value in the routing information is equal to the value specified in the network expression.
- **lt** or **<** These are acceptable ways of writing a "less than" operator which will match if the value in the routing information is less than the value specified in the network expression.
- **lteq**, **le**, **<=**, or **=<** These are acceptable ways of writing a "less than or equal to" operator which will match if the value in the routing information is less than or equal to the value specified in the network expression.
- **gt** or **>** These are acceptable ways of writing a "greater than" operator which will match if the value in the routing information is greater than the value specified in the network expression.
- **gteq**, **ge**, **>=**, or **=>** These are acceptable ways of writing a "greater than or equal to" operator which will match if the value in the routing information is greater than or equal to the value specified in the network expression.
- **ne**, **<>**, or **!=** These are acceptable ways of writing an "inequality" operator which will match if the value in the routing information is not equal to the value specified in the network expression.

The keyword **all** may be used to specify all network number values in the network expression.

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

IPX Route Filter Rule Options

Filter rules can optionally include the following parameter. When used, the options must be inserted after the required part of the rule, but before any modifiers.

The direction is specified with **in**, **out**, or **both**. If no direction is specified, **both** is assumed.

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

IPX Route Filter Rule Modifiers

The source address, destination address, source interface or destination interface can be specified using the **from** and **to** modifiers. These keywords modify the global nature of a RIP filter rule.

- **from** <IPX address> *or* **from** <interface> This modifier tells the device to apply the rule only to routes coming from a specified IPX address, or interface (e.g. Ethernet 0, WAN 1, etc.).

  The IPX address parameter is specified as a hexadecimal network number and node number separated by a dash (e.g. A011-0:0:A5:0:0:1 indicates a node with the hexadecimal network number of A011 and a node address of 0:0:A5:0:0:1).
- **to** <IPX 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.).

Filter rules can also optionally be set to modify some RIP information as it is handled by the device.

- **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. 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.

IPX 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 keyword causes the device to send information about the packet to syslog when the condition of the rule is met.

IPX Route Filter Rule Examples

The following example specifies a rule to allow routes to be input from any IPX network except network number 7.

```
permit network != 7
```

The rule in the following example specifies that routing information should only be accepted from the Ethernet 0 interface.

```
permit network = ALL from ethernet 0
```

IPX SAP Filter Rules

To access a dialog box for IPX SAP filters, open the Main IPX Filtering dialog box (under Global/Filtering/IPX Filtering) and then select the **SAP Filters** button.

SAP 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 server not explicitly allowed by the rules will not be included in the SAP table on input or in the SAP update on output. To allow all other servers not filtered, the last rule must be:

```
permit
```

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 Manager, they will be encrypted.

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

Basic IPX SAP Filter Rules and Syntax

At a minimum, every non-comment line in a filter set must include an action. However, an action alone will not create a useful filter rule, except for setting a default rule.

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

- Lines which begin with **permit** specify that server information meeting the conditions should be inserted into the device's SAP table.
- Lines which begin with **deny** specify that server information meeting the conditions should not be included in the device's SAP table.
- Lines which begin with **#** specify that the text on the line is a comment and should be ignored.

IPX SAP Filter Options

The basic action specified in the rule will almost always be accompanied with an option. IPX SAP options use some or all of a set of operators to determine whether the filter rule matches information in a SAP packet or not. These operators are:

- **eq**, **==**, or **=** These are allowable ways of writing an "equality" operator which will match if the value in the server information is equal to the value specified in the option expression.
- **lt** or **<** These are allowable ways of writing a "less than" operator which will match server information if its value is less than the value specified in the option expression.
- **lteq**, **le**, **<=**, or **=<** These are allowable ways of writing a "less than or equal to" operator which will match server information if its value is less than or equal to the value specified in the option expression.
- **gt** or **>** These are allowable ways of writing a "greater than" operator which will match server information if its value is greater than the value specified in the option expression.
- **gteq**, **ge**, **>=**, or **=>** These are allowable ways of writing a "greater than or equal to" operator which will match server information if its value is greater than or equal to the value specified in the option expression.
- **ne**, **<>**, or **!=** These are allowable ways of writing an "inequality" operator which will match if the value in the server information is not equal to the value specified in the option expression.

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

The options available for IPX SAP filter rules allow rules to be more narrowly specified to exclude all but certain **types** of servers, an individual **service**, servers on certain **networks**, servers with a certain **node** address, and/or servers using a certain IPX **socket** address.

- **type** <operator> <server type> This option allows filtering using the server **type** contained in the SAP update tuple. The server type value must be a hex number. The keyword **all** may be used to specify all types.
- **service** <operator> <server name> This option allows filtering using the **service** name contained in the SAP update tuple. The operator in this option can only be "equality" or "inequality." The name must be 48 characters or less, and enclosed in quotation marks ("").
- **network** <operator> <network number> This option allows filtering of the server **network** number contained in the SAP table. The number is specified in hex. The keyword **all** may be used to specify all network number values.

- **node** <operator> <node address> This rule allows filtering of the server **node** address contained in the SAP table. The operator in this option can only be "equality" or "inequality."

  The node address parameter is the IPX server node number specified as an Ethernet address. An Ethernet address is specified as six hexadecimal octets separated by dots or colons (e.g. 0.0.A5.0.0.1 or 0:0:A5:0:0:1). The keyword **all** may be used to specify all node values.

- **socket** <operator> <socket number> This rule allows filtering of the server **socket** contained in the SAP table. The number is specified in hex. The keyword **all** may be used to specify all socket numbers.

A final option is the ability to specify a direction using **in**, **out**, or **both**. If no direction is specified, **both** is assumed.

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

IPX SAP Filter Rule Modifiers

The source address, destination address, source interface or destination interface can be specified using the **from** and **to** options. These keywords modify the global nature of a SAP filter rule.

- **from** <IPX address> *or* **from** <interface> This modifier tells the device to apply the rule only to server information coming from a specified IPX address, or interface (e.g. Ethernet 0, WAN 1, etc.).

  The IPX address parameter is specified as a hexadecimal network number and node number separated by a dash (e.g. A011-0:0:A5:0:0:1 indicates a node with the hexadecimal network number of A011 and a node address of 0:0:A5:0:0:1).

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

Filter rules can also optionally be set to modify some SAP information as it is handled by the device.

- **metricin** <increment value> This modifier tells the device to increment the metric on incoming servers which match the filter rule. 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 servers which match the filter rule. The value to increment by can be from 1 to 15.

IPX SAP 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 keyword causes the device to send information about the packet to syslog when the condition of the rule is met.

IPX SAP Filter Rule Examples

The following example specifies a rule set to ignore any server named "Test Server." The permit line states that all other servers should be entered into the device's SAP table.

```
deny server = "Test Server"
permit
```

The rule in the following example specifies that only servers from network 7 should be entered into the device's SAP table. All other SAP types will be dropped.

```
permit network = 7
```

IPX Packet Filtering: Interface Dialog Box

To access this dialog box (Figure 12-3), select Interface/Filtering/IPX Filtering from the Device View.

Figure 12-3 Interface IPX Packet Filtering Configuration Dialog Box

Input Filters

This set of pull-down menus allow 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 pull-downs allow 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.