CHAPTER 13

AppleTalk Filtering

Main AppleTalk Filtering Editor Window

The AppleTalk Filtering editor window (Figure 13-1) is used in the VPN 5000 Manager for editing all AppleTalk filter sets, including those for AppleTalk Route, Zone List, and Packet filters. To access this window, select Global/Filtering/AppleTalk Filtering from the Device View.

Figure 13-1 Main AppleTalk 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 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.

AppleTalk Packet Filter Rules

The AppleTalk filter editor window allows a set of AppleTalk filtering rules to be defined, edited and identified with a specific name.

Once a set of rules is defined and named, those rules may be linked to several different AppleTalk filter interpreters to accomplish different types of filtering.

Each interpreter understands and uses a subset of the complete AppleTalk rules. The interpreters available are: general packet filtering, get-zone-list filtering and route (RTMP) filtering.

The interpreters will not reorder the rules as they are specified. They will be applied sequentially from the first rule through the last. Any filtered information not specifically allowed by the set of rules will be dropped silently. If that information is to be allowed, a final permit rule must be specified.

```
permit
```

There is an interaction between the packet filtering interpreter and the other interpreters. The packet filter interpreter will be applied to incoming packets before the other interpreters, and it will be applied to outgoing packets after the other interpreters. For example, a received get-zone-list request may be filtered by an input packet filter before it arrives at the get-zone-list interpreter and the reply may also be filtered again by an outgoing packet filter.

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

General Packet Filtering

This interpreter allows packets being forwarded by the device to be filtered on the input and output side of an interface. The only rules used in this interpreter are the **type**, **srcnet**, **dstnet**, **srcnode**, **dstnode**, **srcskt** and **dstskt** for all packets. For NBP request and reply packets the **NBPName**, **NBPType** and **NBPZone** rules are also used. All other rules are ignored.

Get Zone List

The get-zone-list interpreter allows the filtering of outgoing get-zone-list replies on an interface. These replies contain the zone list displayed by the Chooser on a Macintosh when it is opened. Thus, the get-zone-list interpreter allows control of the zones that are seen on a Macintosh behind a device. The only rules used in this interpreter are the **network**, **net-range** and **zone** rules. All other rules are ignored.

Routing Filters (RTMP)

The RTMP interpreter allows network numbers in input and output AppleTalk RTMP routing packets to be filtered on an interface. The only rules used in this interpreter are the **network** and **net-range** rules. All other rules are ignored.

Basic AppleTalk 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.

AppleTalk Filter Options

The basic action specified in the rule will almost always be accompanied with an option. AppleTalk filter options use some or all of a set of operators to determine whether the filter rule matches the information being examined 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/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 the packet/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 the packet/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 the packet/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 the packet/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 packet/information is not equal to the value specified in the option expression.

The options available for AppleTalk filter rules allow rules to be more narrowly specified to exclude packets or other information based on a number of additional factors.

- **type** <operator> <AppleTalk packet type> This option allows filtering of the packet type from the AppleTalk DDP header. The value must be between 1 and 255. The numbers of some well-known packet types are:
  - RTMP (1)
  - NBP (2)
  - ATP (3)
  - ECHO (4)
  - RTMP Request (5)
  - ZIP (6)
  - ADSP (7)
  - SNMP (8)

  - IP-in-AppleTalk (22)
  - DECnet-in-AppleTalk (68)
- **srcnet** <operator> <network number> This option allows filtering of packets by the source network from the AppleTalk DDP header. The value must be between 1 and 65279. The keyword **all** may be used to specify all network numbers.
- **dstnet** <operator> <network number> This option allows filtering of packets by the destination network from the AppleTalk DDP header. The value must be between 1 and 65279. The keyword **all** may be used to specify all network numbers.
- **srcnode** <operator> <node address> This option allows filtering of packets by the source node from the AppleTalk DDP header. The node value must be between 1 and 253.
- **dstnode** <operator> <node address> This option allows filtering of packets by the destination node from the AppleTalk DDP header. The node value must be between 1 and 253.
- **srcskt** <operator> <socket number> This option allows filtering of packets by the source socket from the AppleTalk DDP header. The value must be between 1 and 255.
- **dstskt** <operator> <socket number> This option allows filtering of packets by the destination socket from the AppleTalk DDP header. The value must be between 1 and 255.
- **network** <operator> <network number> This option allows by the network number in Get Zone List and RTMP packets. The value must be between 1 and 65279. The keyword **all** may be used to specify all network numbers.
- **net-range** <operator> <network range> This option allows filtering of Get Zone List and RTMP packets using a network range. Two network numbers separated by a space make up the network range. Each number must be between 1 and 65279, and the first number must be equal to or smaller than the second. The operator in this option can only be “equality” or “inequality.”
- **zone** <operator> <zone name> This option allows filtering of the zone name in Get Zone List and RTMP packets. The zone name must be enclosed in quotes (e.g. “My Zone”), no greater than 32 characters long, and cannot contain the Ý symbol or *. The operator in this option can only be “equality” or “inequality.”
- **NBPName** <operator> <NBP name> This option allows filtering of the NBP name in an NBP request or reply packet. The NBP name must be between 1 and 32 characters long and enclosed in quotes (e.g. “LaserWriter”). The name may contain Ý. The operator in this option can only be “equality” or “inequality.”
- **NBPType** <operator> <NBP type> This option allows filtering of the NBP type in an NBP request or reply packet. The NBP name must be between 1 and 32 characters long and enclosed in quotes (e.g. “AFP Server”). The name may contain Ý. The operator in this option can only be “equality” or “inequality.”
- **NBPZone** <operator> <zone name> This option allows filtering of the NBP zone name in an NBP request or reply packet. The NBP name must be between 1 and 32 characters long and enclosed in quotes (e.g. “Administration Zone”). The name may contain Ý. The operator in this option can only be “equality” or “inequality.”
- **log** The log option causes the device to log data about the packet to syslog when the condition of the rule is met.

Simple AppleTalk Packet Filter Rule Examples

The following is an AppleTalk packet filter which denies echo packets (type 4) from network 55, and permits everything else.

```
deny srcnet = 55 type = 4
permit
```

The following is an AppleTalk packet filter which denies NBP lookups for the printer named "Engineering Printer," permits NBP lookups for the printer named "HP Printer" by the NBP zone "Sales," and permits everything else.

```
deny NBPName = "Engineering Printer"
permit NBPName = "HP Printer" NBPZone = "Sales"
permit
```

AppleTalk Get Zone List Filter Rule Set Examples

AppleTalk Get Zone List filter rules filter what is seen in the Chooser of Macintoshes attached to the network to which the rules are assigned. The example would: deny all zone names from networks 1-10; permit the zone name "Engineering;" deny the zone name "Sales;" permit all networks not equal to 100; and permit everything else.

```
deny net-range = 1 10
permit zone = "Engineering"
deny zone = "Sales"
permit network != 100
permit
```

AppleTalk RTMP Filter Rule Set Examples

AppleTalk RTMP filter rules can be used to limit the network numbers that are allowed into the routing table or to be advertised from the device. The example performs the following actions: deny networks with a number of 100; permit networks between 200 and 300; deny networks numbered greater than 301; and permit everything else.

```
deny network = 100
permit net-range = 200 300
deny network > 301
permit
```

AppleTalk Filtering: Interface Dialog Box

To access the AppleTalk Filtering dialog box for your interface (Figure 13-2), select Interface/Filtering/AppleTalk Filtering from the Device View.

Figure 13-2 Interface AppleTalk Filtering Configuration Dialog Box

Input RTMP Filters

This set of pull-down menus allow you to select previously defined sets of routing (RTMP) filter rules. These rules will be applied to information arriving on this interface. Up to four sets of rules can be selected.

Output RTMP Filters

This set of pull-down menus allow you to select previously defined sets of routing (RTMP) filter rules. These rules will be applied to information which is to be sent on this interface. Up to four sets of rules can be selected.

Zone List Filters

This set of pull-down menus allow you to select previously defined sets of get-zone-list filter rules. These rules will be applied to replies to AppleTalk get-zone-list requests which are received on this interface. Up to four sets of rules can be selected.

Input Packet 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 Packet 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.