SOFTWARE DEFINED NETWORKS

iQuila Enterprise

Packet Filtering & Data Prioritisation

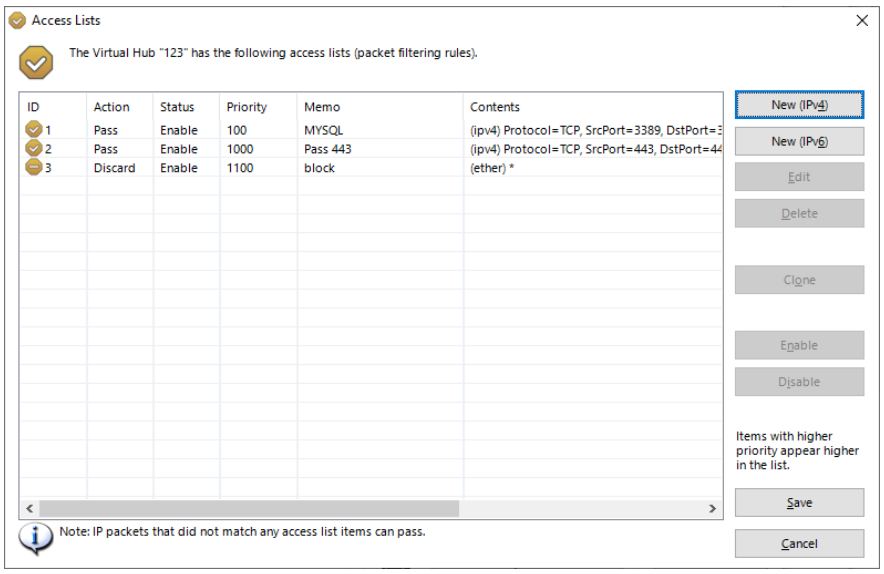
IQ22053r1

This Document Applies to:

iQuila Enterprise

Packet Filtering & Data Prioritisation

iQuila Enterprise Packet Filtering and Data Prioritisation enables you to secure your network whilst prioritising your important data, depending on your Licensing up to 4,096 entries can be defined in a Virtual Switch. Packet Filtering is a function which either passes or discards IP packets passing through network devices according to designated rules commonly referred to as packet filtering rules, rules are processed on the priority number assigned to each rule, the lower the priority number set the more important the rule. Multiple rules can be created for both IPv4 and IPv6



Packet Filtering administration window.

Data which can be Defined by Packet Filtering Entries

The following data can be defined by the access list registered in the Virtual Switch.

Data which can be Defined by Packet Filtering Entries

The following data can be defined by the access list registered in the Virtual Switch.

Access List Memo
Enter a description of the access list entry. This entry enables the setting of an arbitrary character string to clarify the entry for the Virtual Switch Administrator, and its contents has no effect on packet filtering operation.

Action
Designates how an IP packet should be treated when a matching entry definition is found in the access list. Sets to [Pass] or [Discard].

Priority

Designates the priority of an entry within the access list as an integer. The lower the integer, the higher the priority the packet has over the VEN connection. If there are access list entries with the same priority, it is undefined as to which is applied first.

Source IP address

Designates the sending IP address as the packet's matching criteria. It is also possible to designate a subnet range including multiple IP addresses by designating the network address and subnet mask. All sending IP addresses match when no range is designated.

Destination IP address
Designates the destination IP address as the packet's matching criteria. It is also possible to designate a subnet range including multiple IP addresses by designating the network address and subnet mask. All destination IP addresses match when no range is designated.

Protocol Type

Designates the protocol number of that IP packet as the packet's matching criteria. It is possible to match all IP protocols. The numbers which can be designated can be entered as integers although 6 (TCP/IP), 17 (UDP/IP) and 1 (ICMP) are already defined.

Source / destination port number range

Minimum or maximum source port and destination port numbers can be designated as the packet's matching criteria when TCP/IP or UDP/IP is selected as the protocol type. All port numbers are regarded as matching when no values are designated.

Source user name

A user name can be designated as the packet's matching criteria when wishing to match only those packets sent by a specific user (strictly speaking, it is the packet sent by the VEN session of a specific user name). Sending user names are not checked when no name is designated.

Destination user name

A user name can be designated as the packet's matching criteria when wishing to match only those packets to be received by a specific user (strictly speaking, it is the packet intended to be received by the VEN session of a specific user name). Destination user names are not checked when no name is designated.

When none of the Access List Entries Match

When multiple access lists are registered on a Virtual Switch and the IP packet does not match any of the entries contained therein, a [Pass] action is decided by default.

Adding, Deleting & Editing Access List Entries

To add, delete or edit entries in the access list, click on the [Manage Access lists] button in the iQuila Server Manager. Next click on the [Add], [Delete] or [Edit] buttons. Be sure to click the [Save] button after completing any changes to the access list, as changes are not applied to the Virtual Switch unless saved. Furthermore, the access list is enabled from the instant it is set (also applies to iQuila VEN sessions which are already connecte.

To modify the access list with the command line utility, use the [AccessAdd], [AccessList], [AccessDelete], [AccessEnable] and [AccessDisable] commands.