SOFTWARE DEFINED NETWORKS

iQuila Zero Trust Packet filtering For Microsoft Azure

iQ22113r1

This Document Applies to:

iQuila Enterprise for Microsoft Azure

Securing Azure Traffic

Overview

iQuila is a powerful tunnelling platform, allowing you to extend your corporate network across multiple locations while keeping the tightest of security across your network. Using iQuila bridges you are easily able to link in hosted services to the Azure network. The advance A.I. manages the multicast traffic over your network, and the security policy centre allows you to control what data can travel to what destination you select over your network, keeping your data secure at all times.

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.

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

Basic Setting

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 is 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.

Filtering Option for IP Headers

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 that 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.

The 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.

Access List Entries Match

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.

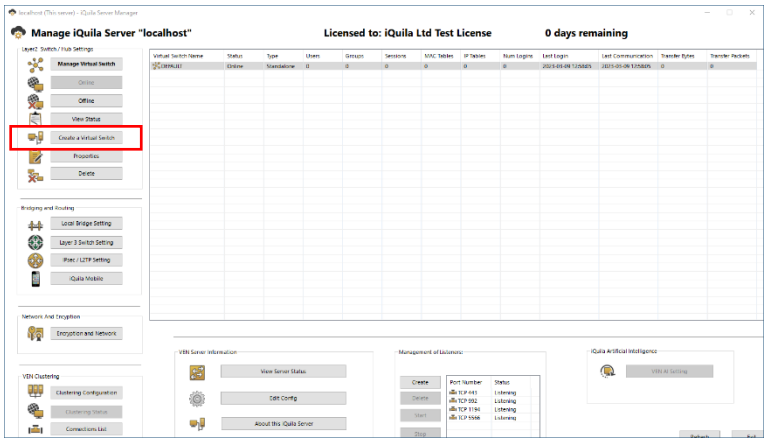
Adding, Deleting & Editing Access List Entries.

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 connected.

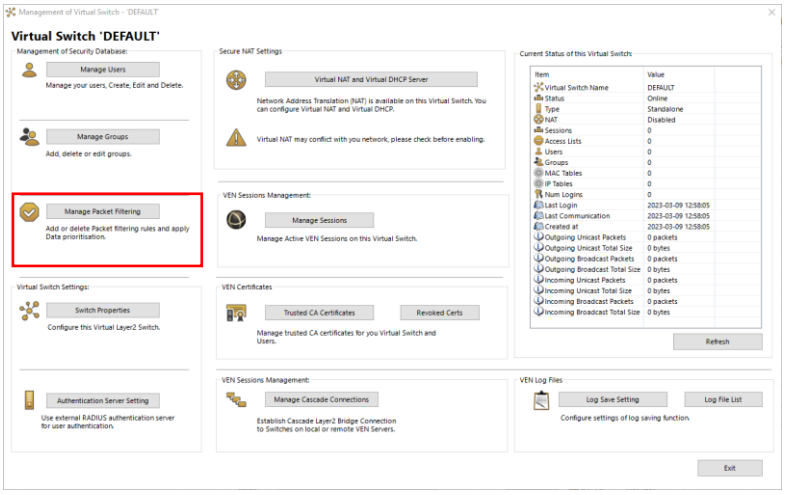
To modify the access list with the command line utility, use the [AccessAdd], [AccessList], [AccessDelete], [AccessEnable] and [AccessDisable] commands.

to configure the Zero trust Packet filtering via IP subnet restrictions please use the steps below.

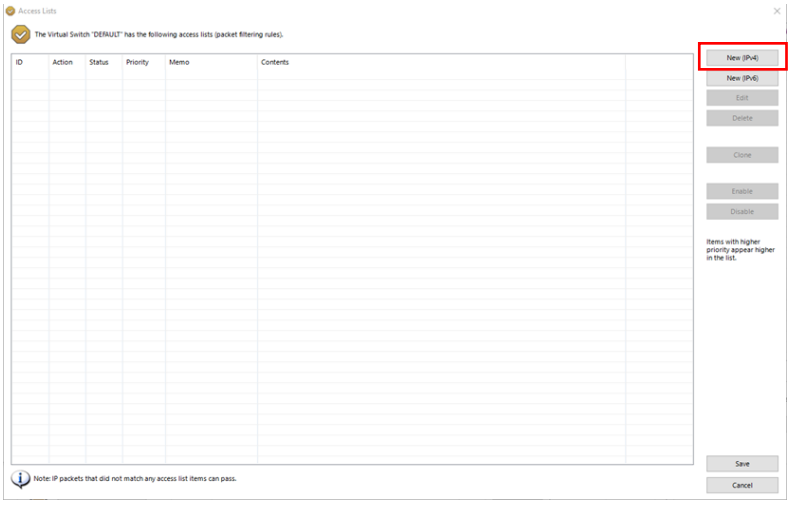
In the iQuila Manager select the virtual switch and select Manage Virtual Switch.



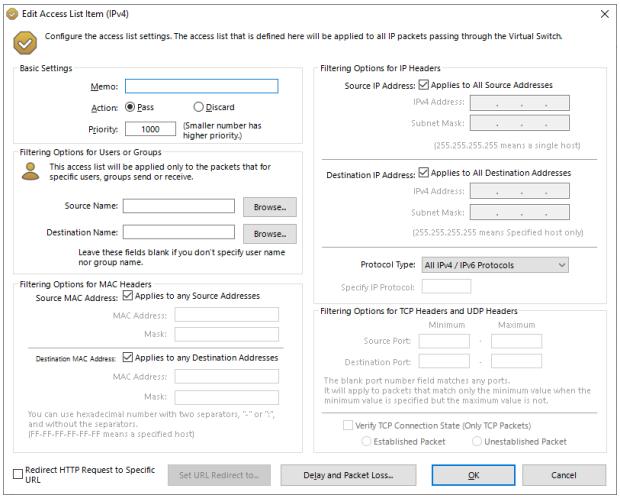
Select Manage Packet Filtering.



The Action list view will be displayed, select New (IPv4)



The New rule configuration windows will display



In the Memo field enter a name for your rule.

The Action setting allows data to be passed or dropped across this switch depending on your filter rules, as a default all data will be passed.

The Pirorty section allows you to give the rule a priority, the lower the priority the higher the rule will be applied.

Defining the filtering options

in the section Filtering Options for IP headers Source IP address uncheck the box and fill out the source IP address and subnet of your source network.

In the Destination IP address section uncheck the box and fill out the IP and subnet of the Azure servers you would like the client to access

In the Protocol section enter the protocols and relevant ports to be used by the client for this connection, you may add multiple rules using the same source and destination address.

As default, all data is passed through the virtual switch, for allow rules to be applied you will need a discard rule.