iQuila Enterprise Security Policies

IQ22054r2

This Document Applies to:

iQuila Enterprise

Security Policies

Definition of Security Policy

The security policy function is one of the iQuila Server Virtual Switches sophisticated functions which allows only packets which have passed packet content inspection and policies to pass. In applying a security policy, the Virtual Switch interprets the header information of all virtual Ethernet frames flowing over it internally to a high layer (automatic recognition of ARP / IP / TCP / UDP / ICMP / DHCP etc) and determines whether their communication content conforms to a security policy based on the results of that interpretation. As a result, any virtual Ethernet frames which breach the security policies set for users by the Virtual Switch Administrator are discarded. In addition, these security policy violations are, depending on their contents, recorded in the Virtual Switches security log where they can later be inspected by the Virtual Switch Administrator.

Utilizing security policies also enables detailed VEN communication control such as band control.

Sequence for Applying Security Policies

Security policies can be set for users who can be defined on the Virtual Switch. Where a plurality of users is grouped together, security policies can also be applied to the group. The decision on what type of security policies will be applied to a session when a VEN connection is made to a Virtual Switch is decided automatically by the iQuila Server. The order of priority in determining this application is as follows.

When security policies are set for a user attempting to connect to the iQuila Server, the settings are applied.

When security policies are not set for a user attempting to connect to the iQuila Server and that user belongs to a group, the security policies set for that group are applied to the user.

Where the user is the Administrator, special Administrator security policies are set.

For all other scenarios, the default security policies are applied.

Default Security Policies

The default security policy values are as follows.

- [Allow access] is enabled
- [Maximum Number of TCP connections] is 32
- [Time-out Period] is 20 seconds

Setting Security Policies for Users & Groups

To apply security policy settings to user objects or group objects using the iQuila Server Manager, enable [Set Security Policy] checkboxes in the user or group edit window, then click the [Security Policy] button and edit as desired.

List of Security Policy Items

The IQuila iQuila Server's security policy settings have the following 20 policy items which can be modified.

Allow Access policy	
Description	Users for whom this policy is set are allowed to make a VEN connection to the iQuila Server.
Settable Values	[Enabled] and [Disabled]
Default Values	[Enabled]
Note	This security policy cannot be designated together with the connection settings of a cascade connection.
Filter DHCP Packets policy	
Description	Filters all DHCP packets in sessions for which this policy is set.
Settable Values	[Enabled] and [Disabled]
Default Values	[Disabled]
Note	None
Deny DHCP Server Operation policy	
Description	Forbids the computer connected to sessions for which this policy is set from acting as a DHCP Server and distributing IP addresses to DHCP clients.
Settable Values	[Enabled] and [Disabled]
Default Values	[Disabled]
Note	None
Enforce DHCP Allocated IP address policy	
Description	Prevents computers within sessions for which this policy is set from using any IP addresses other than those assigned by the DHCP Server on the virtual network.
Settable Values	[Enabled] and [Disabled]
Default Values	[Disabled]
Note	None
Deny Bridge Operation policy	
Description	Denies bridge connections in user sessions for which this policy is set. Communication is not possible even if an Ethernet bridge is set up on the user's client side.
Settable Values	[Enabled] and [Disabled]
Default Values	[Disabled]
Note	This security policy cannot be designated together with the connection settings of a cascade connection. Note that sessions connected by users on whom both the deny bridge and deny router operation policies are [Enabled] cannot connect to the virtual Switch as a [Router/ Bridge Mode] session. Contrarily, it is important to note that when either one or both of the deny bridge and deny router operation policies are [Disabled], the user is able connect to the virtual Switch as a [Router/ Bridge Mode] session.

Deny Routing Operation policy	
Description	Denies IP routing in sessions for which this policy is set. Communication is not possible even if an IP router is operating on the user's client side.
Settable Values	[Enabled] and [Disabled]
Default Values	[Disabled]
Note	This security policy cannot be designated together with the connection settings of a cascade connection. Note that sessions connected by users on whom both the deny bridge and deny router operation policies are [Enabled] cannot connect to the virtual Switch as a [Router/ Bridge Mode] session. Contrarily, it is important to note that when either one or both of the deny bridge and deny router operation policies are [Disabled], the user is able connect to the virtual Switch as a [Router/ Bridge Mode] session.
Deny MAC Addresses Duplication policy	
Description	Prevents the use of MAC address tables currently in use by a computer in a separate session in sessions for which this policy is set.
Settable Values	[Enabled] and [Disabled]
Default Values	[Disabled]
Note	None
Deny IP addresses Duplication policy	
Description	Prevents the use of MAC address tables currently in use by a computer in a separate session in sessions for which this policy is set.
Settable Values	[Enabled] and [Disabled]
Default Values	[Disabled]
Note	None
Deny Non-ARP/ DHCP broadcasts policy	
Description	Denies the transmission and receipt of all broadcast packets on the virtual network other than ARP protocol and DHCP protocol broadcast packets in sessions for which this policy is set.
Settable Values	[Enabled] and [Disabled]
Default Values	[Disabled]
Note	None
Privacy Filter Mode policy	
Description	Filters all direct intersession communication in sessions for which the Privacy Filter Mode policy is set.
Settable Values	[Enabled] and [Disabled]
Default Values	[Disabled]
Note	This security policy cannot be designated together with the connection settings of a cascade connection.
Deny Operation as TCP/IP server policy	
Description	Denies computers in sessions for which this policy is set from operating as servers in TCP/IP protocol. In other words, that session is unable to respond to a SYN packet in TCP from a separate session.
Settable Values	[Enabled] and [Disabled]
Default Values	[Disabled]
Note	None

No limit on Number of Broadcasts policy	
Description	Does not automatically limit the number of broadcast packets sent to the virtual network from computers for which this policy is set, even if said number differs greatly from one which would be considered normal.
Settable Values	[Enabled] and [Disabled]
Default Values	[Disabled]
Note	None
Allow Monitoring Mode policy	
Description	Allows users for whom this policy is set to connect to a virtual switch in Monitoring Mode. Monitoring Mode sessions can monitor (intercept) all packets flowing within the virtual switch.
Settable Values	[Enabled] and [Disabled]
Default Values	[Disabled]
Note	This security policy cannot be designated together with the connection settings of a cascade connection.
Maximum Number of TCP Connections policy	
Description	Sets the maximum number of TCP connections which can be assigned for each session in sessions for which this policy is set.
Settable Values	1 - 32 (connections)
Default Values	32 connections
Note	This security policy cannot be designated together with the connection settings of a cascade connection.
Time-out Period policy	
Description	Sets the timeout time in seconds until a session disconnects when a failure occurs in communication between the VEN Client and the iQuila Server in sessions for which this policy is set.
Settable Values	5 - 60 (seconds)
Default Values	20 seconds
Note	This security policy cannot be designated together with the connection settings of a cascade connection.
Maximum Number of MAC Addresses policy	
Description	Sets the number of MAC addresses which can be registered per session in sessions for which this policy is set.
Settable Values	[No setting] or 1 - 65,535 (addresses)
Default Values	[No setting]
Note	None
Maximum Number of IP Addresses policy	
Description	Sets the number of IP addresses which can be registered per session in sessions for which this policy is set.
Settable Values	[No setting] or 1 - 65,535 (addresses)
Default Values	[No setting]
Note	None

Upload Bandwidth policy	
Description	Limits the bandwidth of external traffic entering the virtual switch in sessions for which this policy is set.
Settable Values	[No setting] or 1 - 4,294,967,295 bps (about 4 Gbps)
Default Values	[No setting]
Note	None
Download bandwidth policy	
Description	Limits the bandwidth of internal traffic leaving the virtual switch in sessions for which this policy is set.
Settable Values	[No setting] or 1 - 4,294,967,295 bps (about 4 Gbps)
Default Values	[No setting]
Note	None
Deny Changing Password policy	
Description	Denies users for whom this policy is set from changing their own password using the VEN Client Manager and so on at user password verification.
Settable Values	[Enabled] and [Disabled]
Default Values	[Disabled]
Note	There is no point in applying this policy to a group. In addition, this security policy cannot be designated together with the connection settings of a cascade connection.
Maximum Number of Multiple Logins policy	
Description	Denies users for whom this policy is set from performing more than a set number of simultaneous logins. This security policy can only be enabled in the iQuila Server which features the multiple login limit function.
Settable Values	[No setting] or 1 - 65,535 (logins)
Default Values	[No setting]
Note	None
Deny VoIP / QoS Function policy	
Description	Denies use of VoIP / QoS response function in user VPEN connection sessions for which this policy is set. This security policy can only be enabled in the iQuila Server which features the VoIP / QoS response function.
Settable Values	[Enabled] and [Disabled]
Default Values	[Disabled]
Note	None

Confirming Contents of Applied Security Policies

Users are able to confirm the values of security policy settings applied to the current session when a VEN Client is connected to an iQuila Server Virtual Switch.