Access Control List (ACL)

Access Control List (ACL) specifies the IP address firewall access rules applied to a packet.The rules are compared to each packet, and if a packet matches a rule, the configured action for that rule is performed. The action ALLOW accepts the packet allowing access; the action DENY drops the packet denying access.

- ACLs can constrain the flow of traffic by individual IP address or by a range of IP addresses.
- ACLs can be bound to specific interfaces (LAN, WAN or MGMT) of the Barracuda Web Application Firewall allowing configuration of distinct restrictions for front-end and back-end traffic.

An ACL rule can be created in the **NETWORKS > ACL** page., In the **Add ACL** section, click **Show** and specify values for the fields.

For more information, click **Help** on the relevant page of the web interface.

Auto Created Network ACLs

Auto Created Network ACLs are generated at system boot time and persist on the system across any configuration change. The auto created ACLs include the following predefined allow deny rules:

- Allow rules to access support tunnel, DNS server and the secure shell (for CLI).
- Deny rules to MGMT and WAN interfaces. Any traffic passing through MGMT and WAN interfaces are blocked. The administrator must create ACL rules to allow designated traffic to pass through these interfaces.

By default, the **Log Status** is set to *Off* for all auto created network ACLs. Any traffic that matches these ACL rules is not logged under **NETWORKS > Network Firewall Logs**. To enable logging, click the **Edit** icon next to the ACL rule and set the **Log Status** to *On*.