Network Access Control Lists

https://campus.barracuda.com/doc/17989784/

You configure network Access Control Lists (ACLs) to match IP traffic with a corresponding firewall action. If there is a rule match, the specified firewall action is executed. ACLs can be created by matching a source network/host, or by designating an IP Reputation pool as the source. Network ACL rules regulate traffic passing between a source IP address and a destination IP address. Geo ACL rules regulate traffic originating from a specific geographic location based on its IP reputation (configured on the **NETWORK > IP Reputation** page).

The following types of ACLs can be configured:

- Global Start
  - Global Network ACL
  - Global Geo ACL
- Service
  - Service Network ACL
  - Service Geo ACL
  - Default ACL
- Global End
  - Global Network ACL
  - Global Geo ACL

The ACLs configured under global_start are the system rules associated with all Services configured on the Barracuda Load Balancer ADC. The global ACL (global_start) rules override ACLs configured under the Service (if configured).

The following outlines when rule actions are performed:

1. Incoming packets are checked for a match with the global_start ACLs. If there is a match, the corresponding action (allow/deny) is applied.
2. If not, the packets are matched with the ACLs configured under the Service (if any).
3. If the packet does not match global_start ACLs (Network or Geo) and Service ACLs (Network or Geo), the packet is matched with the Services Default ACL rule and the corresponding firewall action is performed.
4. If the packet does not match any of these ACLs, the packets are matched with the global_end Network ACL rules.
5. If no ACL rules are configured under global_end, the packets are passed through.

Multiple Network and Geo ACLs can be configured for a Service. Each ACL is prioritized in ascending order and defines the permission rights for clients or servers attempting to access the contents of a Service. IP addresses set within any ACL should be unique and not derived from any other ACLs.

To create a Network or Geo ACL rule:

1. Go to the **NETWORK > Network Firewall** page.
2. In the **Network ACLs** section:
    - Click **Network** or **Geo** next to **global_start** or **global_end** (if you want to add a global ACL rule that will be matched with all incoming packets).
    - Click **Network** or **Geo** next to a Service to add a Service specific ACL rule.
3. Specify values for the given fields and click **Save**.

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

ACLs for Forwarded Traffic

ACLs allow traffic from designated clients to pass through the Barracuda Load Balancer ADC to the back-end servers without any security validations.

To add ACLs for Forwarded Traffic:

1. Go to the **NETWORK > Network Firewall** page.
2. In the **ACLs for NAT/Forwarded Traffic** section, click **Add ACL**.
3. In the **Add ACL for NAT/Forwarded Traffic** window, specify the values for the given fields and click **Save**.

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