Firewall Rules Overview

https://campus.barracuda.com/doc/5799944/

Inbound and outbound firewall rules allow or deny access to remote networks, clients, services and ports. The Barracuda Link Balancer firewall helps prevent or mitigates distributed denial of service attacks by rate limiting the number of requests coming into your network. Firewall rules are arranged in tables from top to bottom in order of precedence. Only the first matching rule is executed.

Inbound Firewall Rules

By default, all connections initiated from outside are denied. Add inbound firewall rules to allow exceptions for specific IP addresses, ports and applications. Applications let you define rules that apply to more than one port. Use the **FIREWALL > Access Rules** page to create firewall rules for incoming packets. To create an inbound rule for an application that is not in the list presented when you add the rule, first go to the **POLICY > Applications** page and define a new application.

Inbound 1:1 NAT Rules

When the Barracuda Link Balancer firewall is enabled, externally reachable servers cannot have public IP addresses. You need to reconfigure these servers with private IP addresses. Identify the public IP addresses as Additional IP Addresses for a WAN interface with a static IP address. Then you can create 1:1 NAT rules to direct traffic to your servers. You can add the public IP addresses as Additional IP Addresses to more than one WAN interface with a static IP address. All incoming traffic will be forwarded according to the rules you create. This allows traffic from more than one WAN link to go to same internal server. 1:1 NAT applies to the IP address only, leaving ports the same on both IP addresses. 1:1 NAT is bidirectional – outbound traffic will include the servers' public IP addresses.

If the Barracuda Link Balancer firewall is disabled, you can create a NAT rule to map the destination IP address of the inbound traffic on one WAN link to another WAN link's IP address. This allows you to add a new WAN link without requiring an update to rules on your network firewall. See Adding, Updating or Viewing WAN Link Configuration for more details. When a 1:1 NAT rule is created, an inbound firewall rule to accept traffic for the external IP address is automatically generated. Without this rule, all connections initiated from outside are denied.

You can view and change this rule – it has a similar **Rule Name** – on the **FIREWALL > Access Rules** page. You may want to modify the rule to restrict access to only those ports or applications that you want to be publicly accessible. On the **FIREWALL > NAT** page, create 1:1 NAT rules and port forwarding rules. If you create a 1:1 NAT rule for an address, there is no need to also create a port forwarding rule.

Port Forwarding Rules

Create port forwarding rules to direct traffic on an external port to a port on an internal IP address. You must specify which WAN link to use to listen for incoming packets on the port. The return path is handled automatically. The listen IP address on a specific WAN interface could either be the WAN IP address or any other IP address on the same WAN interface. A WAN IP address used in any port forwarding rule can not also be used in a 1:1 NAT rule. You can forward traffic from a port on multiple WAN links to a port on a single internal IP address by creating a rule for each WAN link. When you add a port forwarding rule, an inbound firewall rule is created automatically to accept traffic on the listen link and port for the private IP address of the server. Without this rule, all connections initiated from outside are denied.
You can view and change this rule – it has a similar **Rule Name** – on the **FIREWALL > Access Rules** page. To add a new port forwarding rule, go to the **FIREWALL > NAT** page.

Outbound Firewall Rules

By default, all outbound connections are allowed. You can create outbound firewall rules to restrict outbound connectivity. For example, you may want to block access to certain online gaming sites that use specific ports. On the **FIREWALL > Access Rules** page, create, modify, or delete outbound firewall rules. The rules are arranged in the table from top to bottom in order of precedence. Only the first rule that matches the profile of the traffic is executed. If you want to create an outbound rule for an application that is not in the list presented when you add the rule, go to the **POLICY > Applications** page and define a **Custom Application**.

Firewall Logging

You can view executed rules and the impact on traffic (dropped or allowed) on the firewall log displayed on the **LOGS > Firewall Log** page. Only rules with **Log** selected in their rule entry (under the **Firewall** tab) are logged.