Firewall Access Rules

https://campus.barracuda.com/doc/43847161/

The firewall service compares the incoming traffic to the access rules until it has found a match and then executes the policy defined in the matching rule. The following article explains the configuration and interaction of access rules on the Barracuda NG Firewall.

Access Rule Settings

For each access rule you can configure the following settings:

- **Name** – The name of the access rule. This name is displayed on the **Firewall >** **Live**and **History** pages.
- **Description** – An additional field in which you can enter a description of the access rule, to help you and others determine the purpose of the access rule in case the rule must be edited it later.
- **Action** – Specifies how the Barracuda NG Firewall handles network traffic that matches the criteria of the rule. The following actions are available:
  - **Pass** – The Barracuda NG Firewall passes all network traffic that matches the access rule.
  - **Block** – The Barracuda NG Firewall ignores all network traffic that matches the access rule and does not answer to any packet from this particular network session.
  - **Deny**– The Barracuda NG Firewall dismisses all network traffic that matches the access rule. Matching network sessions are terminated by replying **TCP-RST** for TCP requests, **ICMP Port Unreachable** for UDP requests, and **ICMP Denied by Filter** for other IP protocols.
  - **Dst NAT** – The Barracuda NG Firewall rewrites the destination IP address, network, or port to a predefined network address.
  - **Map** – The Barracuda NG Firewall rewrites IP ranges or networks to a predefined network or IP range.
  - **App Redirect** – The Barracuda NG Firewall redirects the traffic locally to one of the services running on the Barracuda NG Firewall.
  - **Broad Multicast** – The Barracuda NG Firewall forwards broadcasts for bridged networks.
  - **Cascade** – Jump and evaluate a different rule list.
  - **Cascade Back** – Jump back to the global rule list and resume evaluation the access rules below the cascade rule.
- **Service** – The protocol and protocol/port range of the matching traffic. You can define one or more services for the access rule. You can select a predefined service object or create your own service objects (see: Service Objects).
- **Source** – The source IP address/netmask of the connection to be handled by the rule. You can select a network object or explicitly enter a specific IP address/netmask.
- **Destination** – The destination IP address/netmask of the connection that is affected by the

rule. You can select a network object or explicitly enter a specific IP address/netmask.
- **Connection Method** – The outgoing interface and source (NAT) IP address for traffic matching the access rule, using connection objects (see below).

Connection Objects

The following table lists the five default connection objects.

Predefined Connection Object	Outgoing Interface and IP Address Determined by
Dynamic SNAT (Source-based NAT)	Change the source IP address of network packets to the IP address to that of the matching interface with the lowest metric according to the routing table.
No SNAT (No Src NAT - Client)	Connection is established using the original source IP address.
SNAT with DSL IP	Source NAT with the IP address of the ppp1 device
SNAT with 3G IP	Source NAT with the IP address of the ppp5 device (3G uplink)
SNAT with DHCP IP	Source NAT with the IP address of the dhcp device (DHCP uplink)
NAT Tables	Source NAT for networks or IP ranges. Multiple rewrite conditions can be configured per connection object.
Application Based Link selection Connection Objects	Source NAT based on application type.

You can also create custom connection objects. For more information, see Connection Objects.

Troubleshooting Blocked Connections Video

To get a feel for how to use access rules, and how NG Admin allows you to determine which rules to create, watch the following video:


Connection Blocked
Troubleshooting
Barracuda NG Firewall