Host Firewall

https://campus.barracuda.com/doc/43846845/

The host firewall service is the firewall service responsible for governing traffic to and from local services running on the Barracuda NG Firewall and Control Center. The ruleset is split into four rule lists:

- **Inbound** – Predefined ruleset for inbound traffic to local services running on the Barracuda NG Firewall and NG Control Center. Also allows access to the management ports.
- **Inbound-User** – Add rules to restrict all inbound traffic to the unit. Management ACLs are not influenced by restricting traffic in the inbound-user rule list. Inbound-user rules are checked only if none of the rules in the inbound rule list matched.
- **Outbound** – Predefined ruleset for outbound traffic coming from local services running on the Barracuda NG Firewall or NG Control Center.
- **Outbound-User** – Add rules to restrict traffic from leaving the unit. Outbound-user rules are checked only if none of the rules in the outbound rule list matched.

Changes to the host firewall ruleset should only by done by an expert administrator as they can result in severe misconfigurations of your Barracuda NG Firewall or NG Control Center. If in doubt, contact Barracuda Networks Technical Support.

Host Firewall Features & Rule Types

The host firewall service restricts policies, rule and connection object types. Application Detection is not possible as Application Control 2.0 can only be used in the forwarding firewall service.

- **Traffic Shaping** – For more information, see Traffic Shaping.
- **Time restrictions** – For more information, see Schedule Objects.
- **IPS policies** – For more information, see Intrusion Prevention System (IPS)

You can create the following firewall rules types:

- **Block** – For more information, see How to Create a Block Access Rule
- **Deny** – For more information, see How to Create a Deny Access Rule
- **Pass** – For more information, see How to Create a Pass Access Rule
- **Dst NAT** – Only for Outbound and Outbound-User rule lists. For more information, see How to Create a Destination NAT Access Rule.

The following connection objects are available:

- **No Src NAT** – default.
- **Dynamic Src NAT** – Only for Outbound and Outbound-User rule lists.
- **Explicit** – Explicit connection object.