Host Firewall

https://campus.barracuda.com/doc/79463054/

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

- **Inbound** – Predefined ruleset for inbound traffic to local services running on the CloudGen Firewall or 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 CloudGen Firewall or 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.

Unlike the forwarding firewall, the host firewall does NOT re-evaluate active sessions. This means that the behavior of a current session will not change if a new inbound/outbound rule is introduced or changed or if an existing inbound/outbound block rule is modified. Affected sessions will not be terminated.

Changes to the host firewall ruleset should only be done by an expert administrator because they can result in severe misconfigurations of your device. If in doubt, contact Barracuda Networks Technical Support.

Host Firewall Features

The host firewall service restricts policies, rule and connection object types. Application Detection is not possible because Application Control 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).

Access Rule Actions

- **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.

For more information, see Access Rules.

Connection Objects

Depending on the ruleset, the following connection object **Translated Source IP Policies** are available:

- **Original Source IP** – The source IP address of the packet is not changed.
- **Dynamic NAT** – The firewall uses the routing table to find a suitable interface for routing the packet and uses the IP address of the relevant interface as the new source IP address.
- **Network Interface** – Source NAT using the first IP address assigned to the network interface. Only use for dynamic interfaces such as dhcp or ppp.
- **Explicit IP** – Source NAT using the entered IP address as the translated source IP address.
- **Explicit Network Mapping** – Maps the source IP address to a new source network. Make sure that the source range using this connection is equal to or smaller than the map range. If not, the firewall will wrap the larger source net into the smaller bind net. E.g., If you use X.X.X.X/24 network as source and a Y.Y.Y.Y/25 as the map range, the IP address X.X.X.128 is mapped to Y.Y.Y.1.

For more information, see Connection Objects.