

Access Rules

<https://campus.barracuda.com/doc/72515917/>

By default, without any access rules in the ruleset, all traffic is blocked by the firewall. To allow traffic, you must create rules for IPv4 and IPv6 traffic in the access ruleset and place them in the correct order. This ruleset determines the order in which incoming traffic is matched against the access rules. Rules are processed from the top to the bottom; the first access rule that matches is executed. If the traffic does not match the first rule, the next rule is then evaluated, continuing in this way from top to bottom until a matching rule is found. If none of the rules match, the connection is blocked. Place the more granular, specific rules toward the top of the ruleset, and the broader, general rules toward the bottom. An access rule will not match if a rule before it matches the same traffic.

Access-Rule Matching Criteria

For an access rule to match, you must configure the following matching criteria:

- **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. For more information, 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. For more information, see [Network Objects](#).
- **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.
- **(optional) Schedule/Time** – Use a schedule object as a matching criteria. For more information, see [Schedule Objects](#).
- **(optional) User** – Use a user object as as a matching criteria. For more information, see [User Objects](#).

Access Rule Actions

The action specifies how the firewall handles network traffic that matches the criteria of the rule. The following actions are available

- **Pass** – All traffic matching the access rule is forwarded.
- **Block** – All traffic matching the access rule is ignored. Matching connection attempts are not answered.
- **Deny** – All traffic matching this access rule is dismissed. 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 firewall rewrites the destination IP address, network, or port to a predefined network address.

- **Redirect to Service** – The firewall rewrites the destination IP address, network, or port and forwards the traffic to a service running on the firewall.

Connection Methods

The settings in the connection object determine the outgoing interface of the packet. For IPv4 traffic, you can also configure source NAT and PAT. The connection object also contains the policies of how traffic is distributed over the available interfaces in the **Failover and Load Balancing** section.

For more information, see [Connection Objects](#).

© Barracuda Networks Inc., 2019 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.