
How to Create a Pass Access Rule

<https://campus.barracuda.com/doc/72515947/>

A Pass access rule permits traffic for a specific network service coming from the source to access the selected destination. For the source and destination, you can specify network objects, IP addresses, or networks.

Create a Pass Access Rule

1. Go to **FIREWALL > Access Rules**.
2. Click **Add Access Rule** to create a new rule. The **Add Access Rule** window opens.
3. Select **Pass** as the action.
4. Enter a **Name** for the rule. E.g., LAN-DMZ
5. Specify the following settings that must be matched by the traffic to be handled by the access rule, and click **+** after each entry:
 - **Source** - The source addresses of the traffic.
 - **Network Services** - Select a service object, or select **Any** for this rule to match for all services.
 - **Destination** - The destination addresses of the traffic.
6. (optional) Configure **Advanced** settings. For more information, see [Advanced Access Rule Settings](#).

Add Access Rule ?

General
Advanced

Action:

➔

DNAT (port forwarding) - Redirect traffic to a specific IP address.
 Redirect to Service - Redirect traffic to a service on the Barracuda NextGen Firewall.
 Bi-directional - Source and destination networks are interchangeable.

Name:

Description:

Connection:

Adjust Bandwidth:

The interface must have bandwidth management enabled on the NETWORK > IP Configuration page for this policy to be applied.

Bi-directional: Yes No

Disable: Yes No

IPS: Yes No

Application Control: Yes No

SSL Interception: Yes No

URL Filter: Yes No

Virus Scanner: Yes No

ATP: Yes No

Mail Security: Yes No

Safe Search: Yes No

Source

HQ-DMZ	+
Ref: Trusted LAN	-

Network Objects IP Addresses Geo Loc.

Network Services

Any	+
Any	-

Destination

HA Management IP	+
Ref: HQ-DMZ	-

Network Objects IP Addresses Geo Loc.

7. Click **Save**.

8. Drag and drop the access rule so that it is the first rule that matches the traffic that you want it to forward. Ensure that the rule is located *above* the BLOCKALL rule; rules located below the BLOCKALL rule are never executed.

For the example access rule displayed in the figure above, a network object named **HQ-DMZ** containing the IP address of the DMZ server has been created. For more information, see [How to Create Network Objects](#).

Additional Matching Criteria

- **Connection** – For more information, see [Connection Objects](#).
- **Valid for Users** – For more information, see [User Objects](#).
- **Apply only during this time** – For more information, see [Schedule Objects](#).

Additional Policies

- **IPS** – For more information, see [Intrusion Prevention System \(IPS\)](#).
- **Application Control** – For more information on Application Control features, see [Application Control](#).
- **Adjust Bandwidth** – For more information, see [Traffic Shaping](#).

Figures

1. pass_rule.png

© 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.