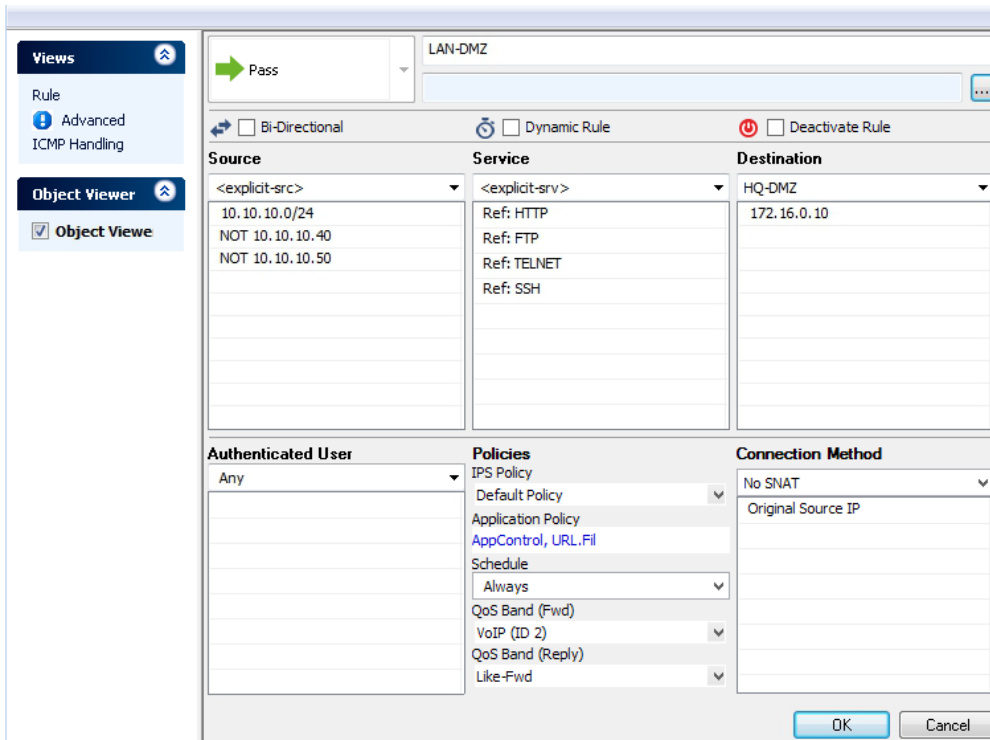


How to Create a Pass Access Rule

<https://campus.barracuda.com/doc/48203301/>

A **Pass** access rule permits traffic for a specific **Service** coming from the **Source** to access the selected **Destination**. For the **Source** and **Destination**, you can specify network objects, IP addresses, networks, or [geolocation objects](#).



The screenshot shows the configuration window for a 'Pass' rule. The rule name is 'LAN-DMZ'. The configuration is as follows:


Source	Service	Destination
<explicit-src> 10.10.10.0/24 NOT 10.10.10.40 NOT 10.10.10.50	<explicit-srv> Ref: HTTP Ref: FTP Ref: TELNET Ref: SSH	HQ-DMZ 172.16.0.10

Additional settings:

- Authenticated User:** Any
- Policies:** IPS Policy, Default Policy, Application Policy, AppControl, URL.Fil, Schedule, Always, QoS Band (Fwd), VoIP (ID 2), QoS Band (Reply), Like-Fwd
- Connection Method:** No SNAT, Original Source IP

Buttons: OK, Cancel

Create a Pass access rule

- Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > your virtual server > Assigned Services > Firewall > Forwarding Rules**.
- Click **Lock**.
- Either click the plus icon (+) at the top right of the rule set, or right-click the rule set and select **New > Rule**.

- Select **Pass** as the action.
- Enter a **name** for the rule. For example, LAN-DMZ.
- Specify the following settings that must be matched by the traffic to be handled by the access rule:
 - Source** – The source addresses of the traffic.
 - Destination** – The destination addresses of the traffic.
 - Service** – Select a service object, or select **Any** for this rule to match for all services.

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](#).

7. Click **OK**.
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.
9. Click **Send Changes** and **Activate**.

Additional matching criteria

- **Authenticated User** – For more information, see [User Objects](#).
- **Schedule Objects** – For more information, see [Schedule Objects](#).
- **Connection Method** – For more information, see [Connection Objects](#).

Additional policies

- **IPS Policy** – For more information, see [Intrusion Prevention System \(IPS\)](#).
- **Application Control** – For more information on Application Control features, see [Application Control](#).
- **QoS Band (Fwd) or QoS Band (Reply)** – For more information, see [Traffic Shaping](#).

Figures

1. pass_rule.png
2. FW_Rule_Add01.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.