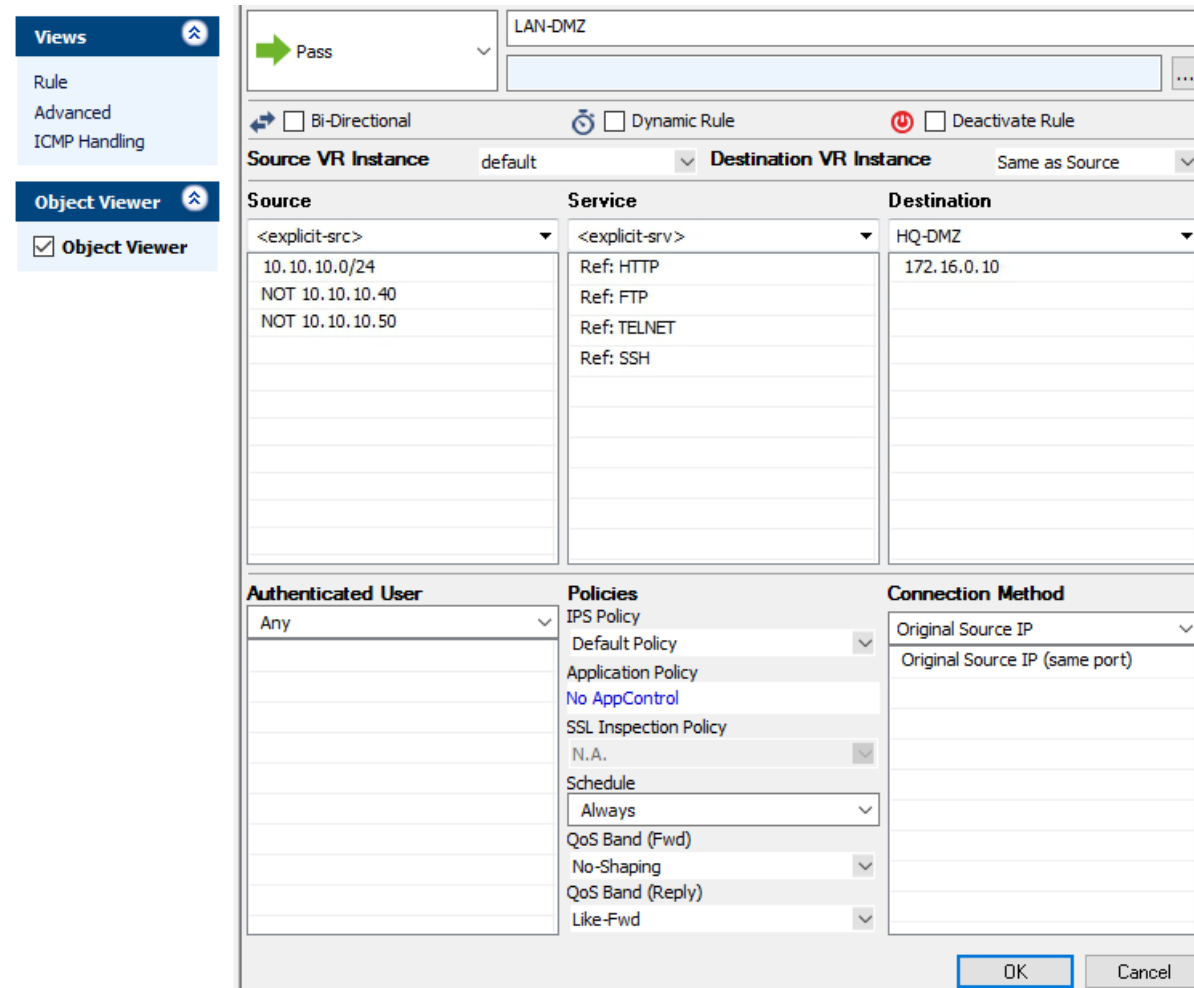


How to Create a Pass Access Rule

<https://campus.barracuda.com/doc/96026199/>

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 'Pass' rule configuration window. The left sidebar has 'Views' (Rule, Advanced, ICMP Handling) and 'Object Viewer' (Object Viewer). The main area is titled 'LAN-DMZ' and contains the following fields:

- Action:** Pass (indicated by a green arrow icon)
- Bi-Directional:** ☐
- Dynamic Rule:** ☐
- Deactivate Rule:** ☐
- Source VR Instance:** default
- Destination VR Instance:** Same as Source

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

Authenticated User	Policies	Connection Method
Any	IPS Policy	Original Source IP
	Default Policy	Original Source IP (same port)
	Application Policy	
	No AppControl	
	SSL Inspection Policy	
	N.A.	
	Schedule	
	Always	
	QoS Band (Fwd)	
	No-Shaping	
	QoS Band (Reply)	
	Like-Fwd	

Buttons: OK, Cancel

Create a Pass Access Rule

- Go to **CONFIGURATION > Configuration Tree > Box > 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.

5. Enter a **name** for the rule. For example, LAN-DMZ.
6. 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](#).
- **SSL Inspection Policy** – For more information, see [SSL Inspection in the Firewall](#).
- **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., 2024 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.