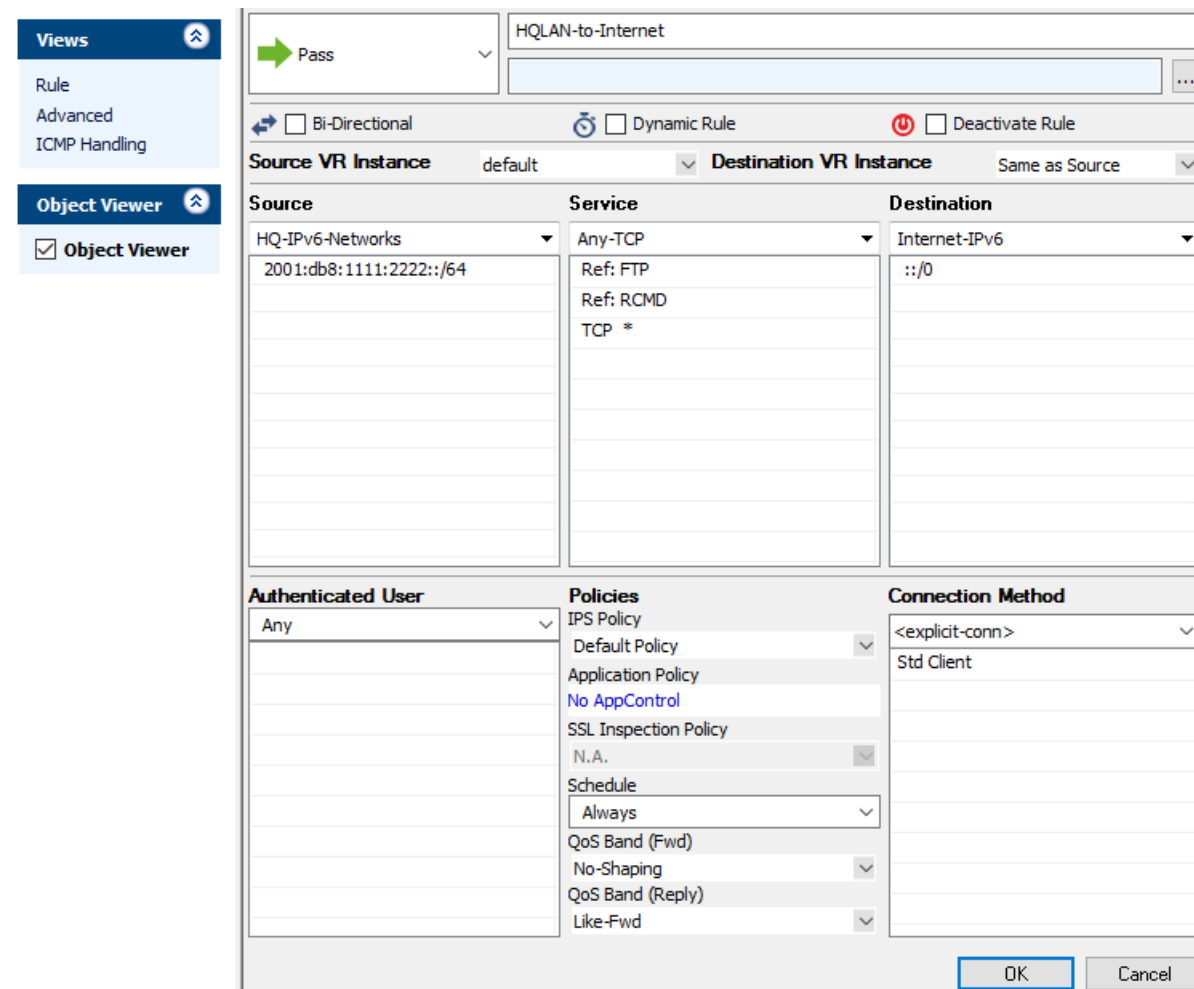


How to Create IPv6 Access Rules

<https://campus.barracuda.com/doc/96026194/>

An IPv6 access rule applies the selected action to the IPv6 traffic coming from the **Source** to the selected **Destination** for a specific **Service**.



The screenshot shows the 'Rule' configuration window in the Barracuda CloudGen Firewall interface. The left sidebar has 'Views' (Rule, Advanced, ICMP Handling) and 'Object Viewer' (Object Viewer checked). The main configuration area is titled 'HQLAN-to-Internet' and shows the following settings:

- Action:** Pass (indicated by a green arrow icon)
- Bi-Directional:** ☐ (unchecked)
- Dynamic Rule:** ☐ (unchecked)
- Deactivate Rule:** ☐ (unchecked)
- Source VR Instance:** default
- Destination VR Instance:** Same as Source
- Source:**
 - Object: HQ-IPv6-Networks
 - Address: 2001:db8:1111:2222::/64
- Service:**
 - Object: Any-TCP
 - References: Ref: FTP, Ref: RCMD, TCP *
- Destination:**
 - Object: Internet-IPv6
 - Address: ::/0
- Authenticated User:** Any
- Policies:**
 - IPS Policy: Default Policy
 - Application Policy: No AppControl
 - SSL Inspection Policy: N.A.
 - Schedule: Always
 - QoS Band (Fwd): No-Shaping
 - QoS Band (Reply): Like-Fwd
- Connection Method:**
 - Method: <explicit-conn>
 - Client: Std Client

At the bottom right, there are 'OK' and 'Cancel' buttons.


Before you Begin

- Enable IPv6 and assign box- and service-level IPv6 addresses. For more information, see [How to Enable IPv6](#).

Create an IPv6 Access Rule

1. Go to **CONFIGURATION > Configuration Tree > Box > Assigned Services > Firewall >**

Forwarding Rules.

2. Click **Lock**.
3. Either click the **+v6** icon at the top right of the ruleset, or right-click the ruleset and select **New > IPv6 Rule**.

4. Select **Block**, **Deny** or **Pass** as the action.
5. Enter a **name** for the rule.
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.
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

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

Additional Policies

- **IPS Policy** – For more information, see [Intrusion Prevention System \(IPS\)](#).

Figures

1. IPv6_rule_00.png
2. IPv6_rule_01.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.