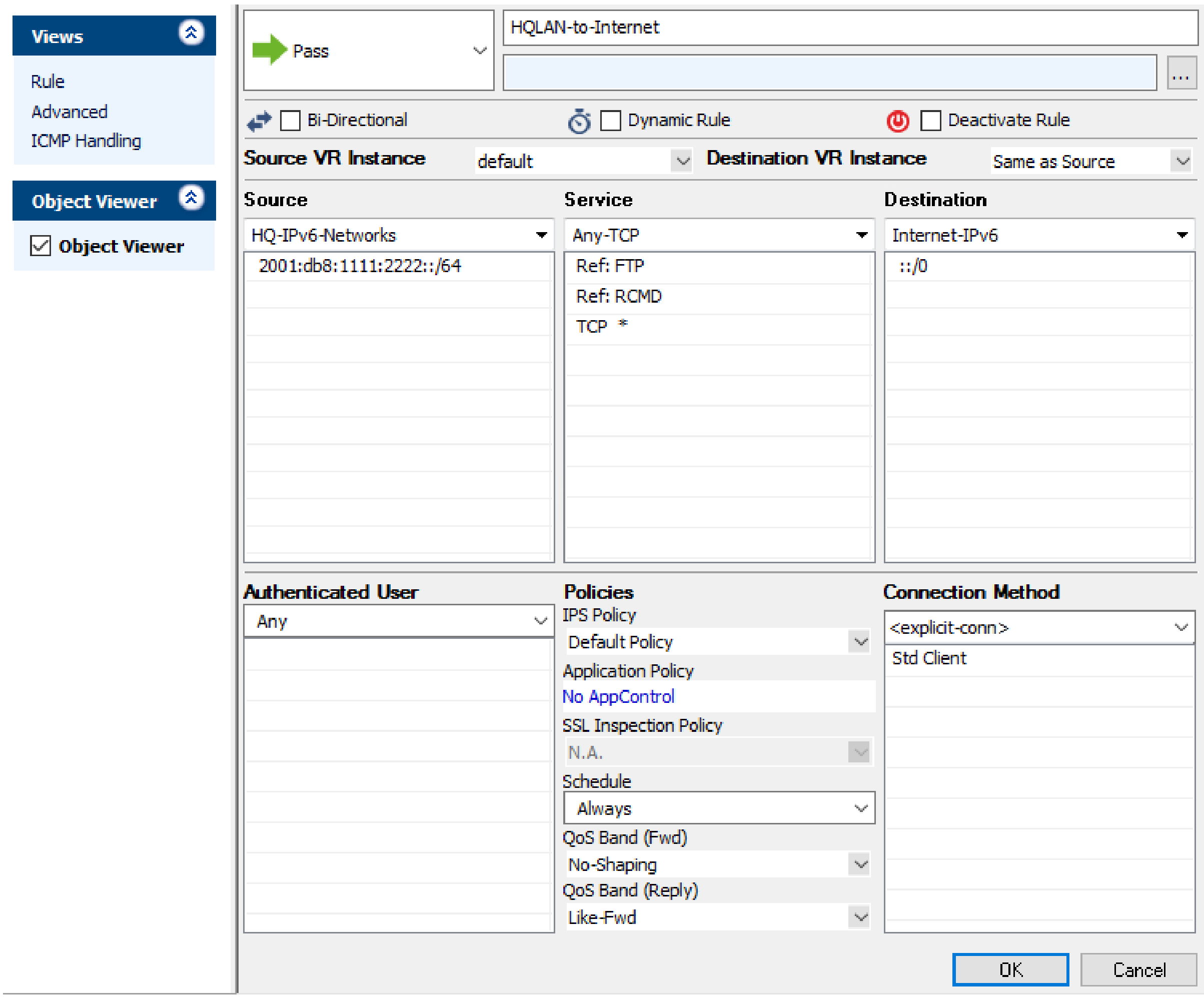
How to Create IPv6 Access Rules

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** .



Pass

HQLAN-to-Internet

☐ Bi-Directional ☐ Dynamic Rule ☐ Deactivate Rule

Source VR Instance: default
Destination VR Instance: Same as Source

Source: HQ-IPv6-Networks
2001:db8:1111:2222::/64

Service: Any-TCP
Ref: FTP
Ref: RCMD
TCP *

Destination: Internet-IPv6
::/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: <explicit-conn>
Std Client

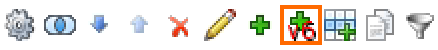
Before you Begin

- 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