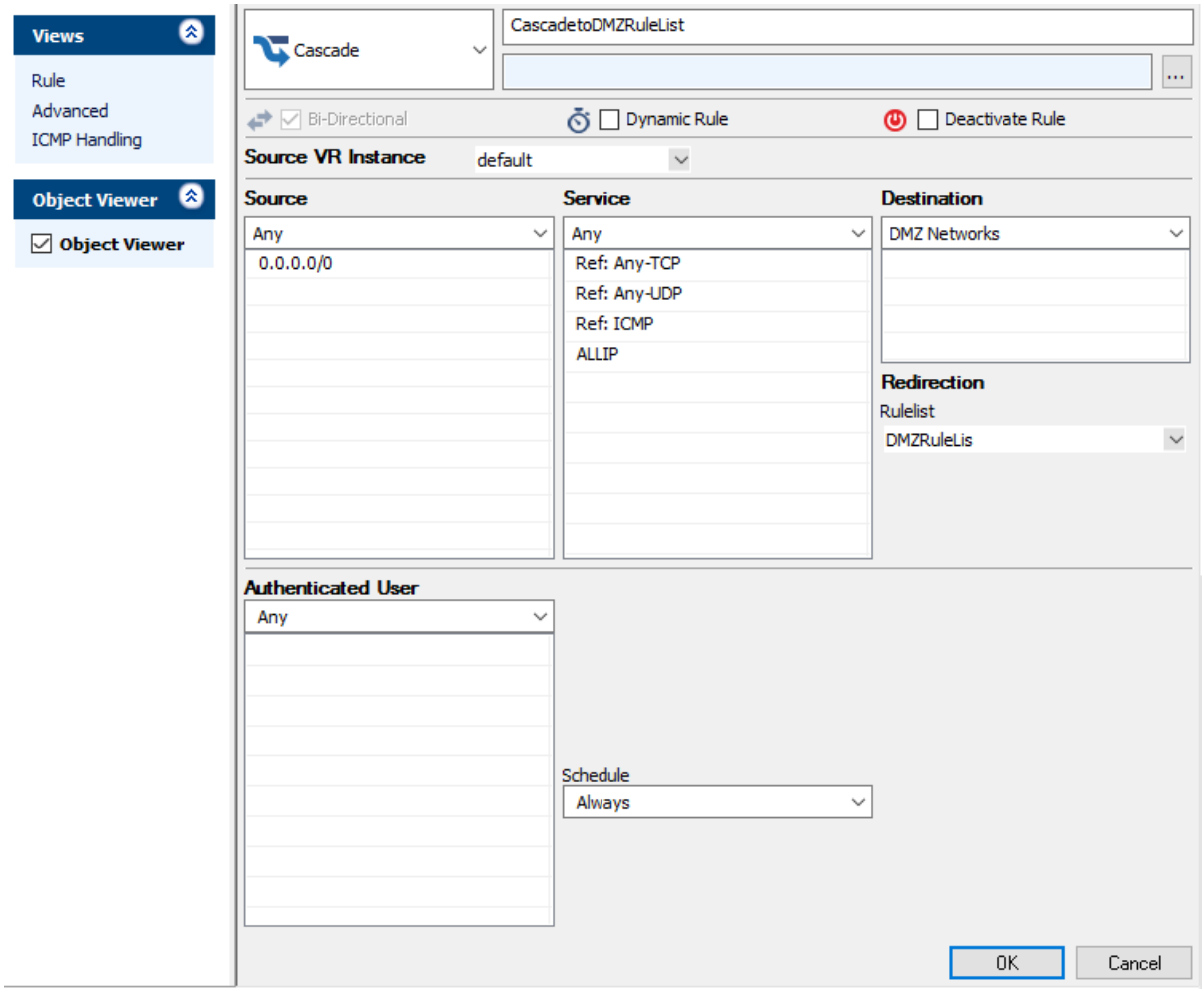
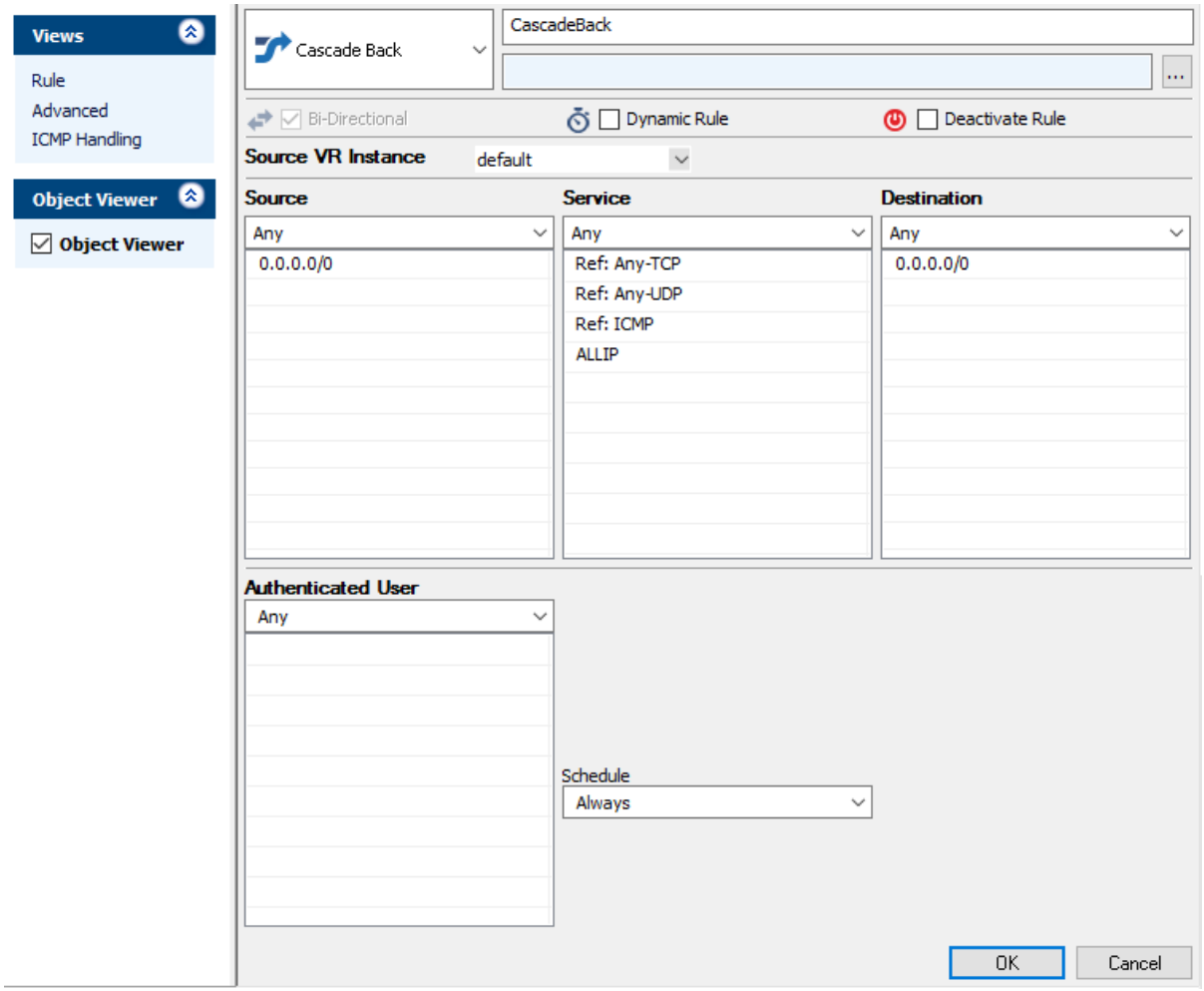
How to Create Cascade and Cascade Back Access Rules

https://campus.barracuda.com/doc/73719217/

To better organize the access rule set, you can create additional rule lists. At the point in the rule list where you want to evaluate another rule list create a **Cascade** access rule. If none of the rules in the additional rule list you cascaded to matched, create a **Cascade Back** access rule to continue evaluating the rules in the main rule list. If you do not define a **Cascade-Back** rule in the additional rule list and none of the rules match, the default policy (**BLOCK** or **ALLOW**) is executed at the end of the rule list.





Before you Begin

- Create one or more rule lists. For more information, see How to Create New Rule Lists.

Create a Cascade Access Rule

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

4. Select **Cascade** as the action.
5. Enter a **Name** for the rule. For example, `CascadetoDMZRuleList`.
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. Select the **Rulelist** that you want to also evaluate the traffic. E.g., **DMZRuleList**.
8. Click **OK**.
9. 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.
10. Click **Send Changes** and **Activate**.

Create a Cascade Back Access Rule

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

4. Select **Cascade Back** as the action.
5. Enter a **Name** for the rule. For example, CascadeBack.
6. Specify the following settings that must be matched by the traffic that will 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 to the order that you want. Usually this rule is placed last in the rule list, but you can drag it further up the rule list as well.
9. Click **Send Changes** and **Activate**.

Additional Matching Criteria

- **Authenticated User** – For more information, see User Objects.

Additional Policies

- **Time Objects** – For more information, see Schedule Objects.

Figures

1. FW_Cascade.png
2. FW_CascadeBack.png
3. FW_Rule_Add01.png
4. FW_Rule_Add01.png

© Barracuda Networks Inc., 2020 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.