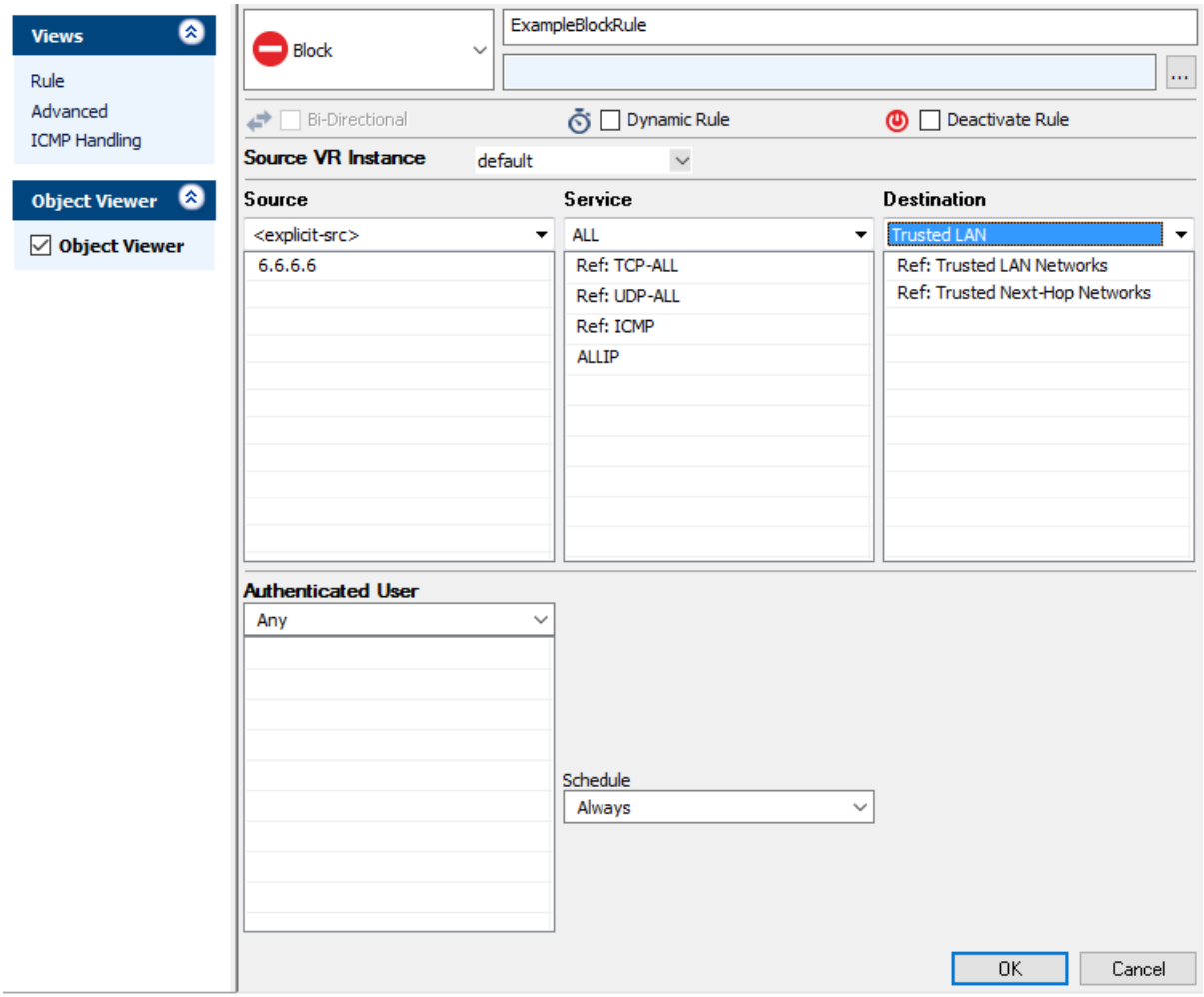
How to Create a Block Access Rule

https://campus.barracuda.com/doc/79462936/

A **Block** access rule prevents traffic from passing through the CloudGen Firewall. The sender is not notified that the traffic was blocked.



Create a Block 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 **Block** as the action.
5. Enter a **Name** for the rule. For example, `ExampleBlockRule`.
6. Specify the following settings that must be matched by the traffic to be handled by the access rule:

- **Source** – The source addresses.
- **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 block. 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.

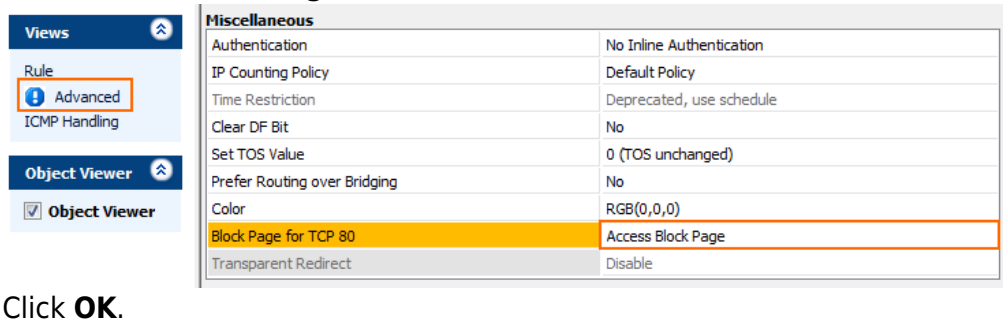
Additional Policy

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

Returning a Block Page for HTTP Traffic

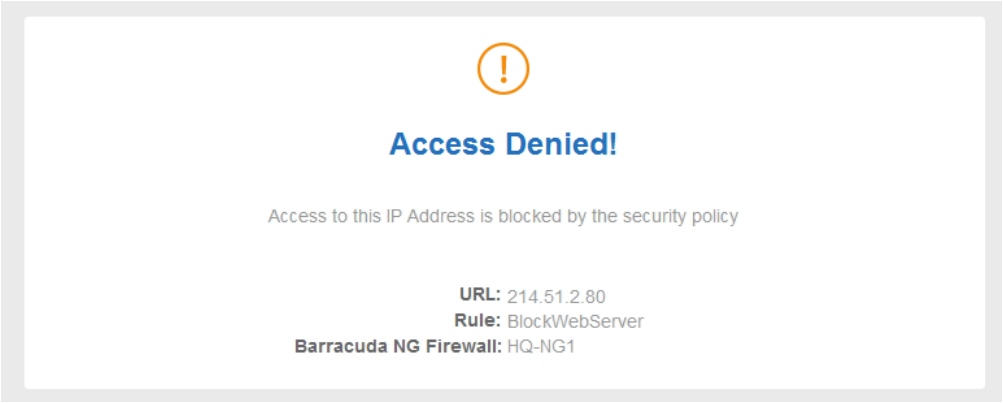
BLOCK and DENY access rules can return a block page if the user was blocked using the HTTP protocol on port 80. All other protocols and ports covered by the access rule will be blocked at TCP SYN level.

1. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > *your virtual server* > Assigned Services > Firewall > Forwarding Rules**.
2. Click **Lock**.
3. Edit a Block access rule. The **Edit Rule** window opens.
4. In the left menu click **Advanced**.
5. In the **Miscellaneous** section, set **Block Page for TCP 80** to **Access Block Page** or **Quarantine Block Page**.



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

When a user is blocked by this access rule while using HTTP on port 80, the customizable **Access Block Page** is displayed. For more information, see How to Configure Custom Block Pages and Texts.



Figures

1. block_rule.png
2. FW_Rule_Add01.png
3. FW_Block_Rule_Advanced_HTTP.png
4. FW_Block_Rule_HTTP_Page.png