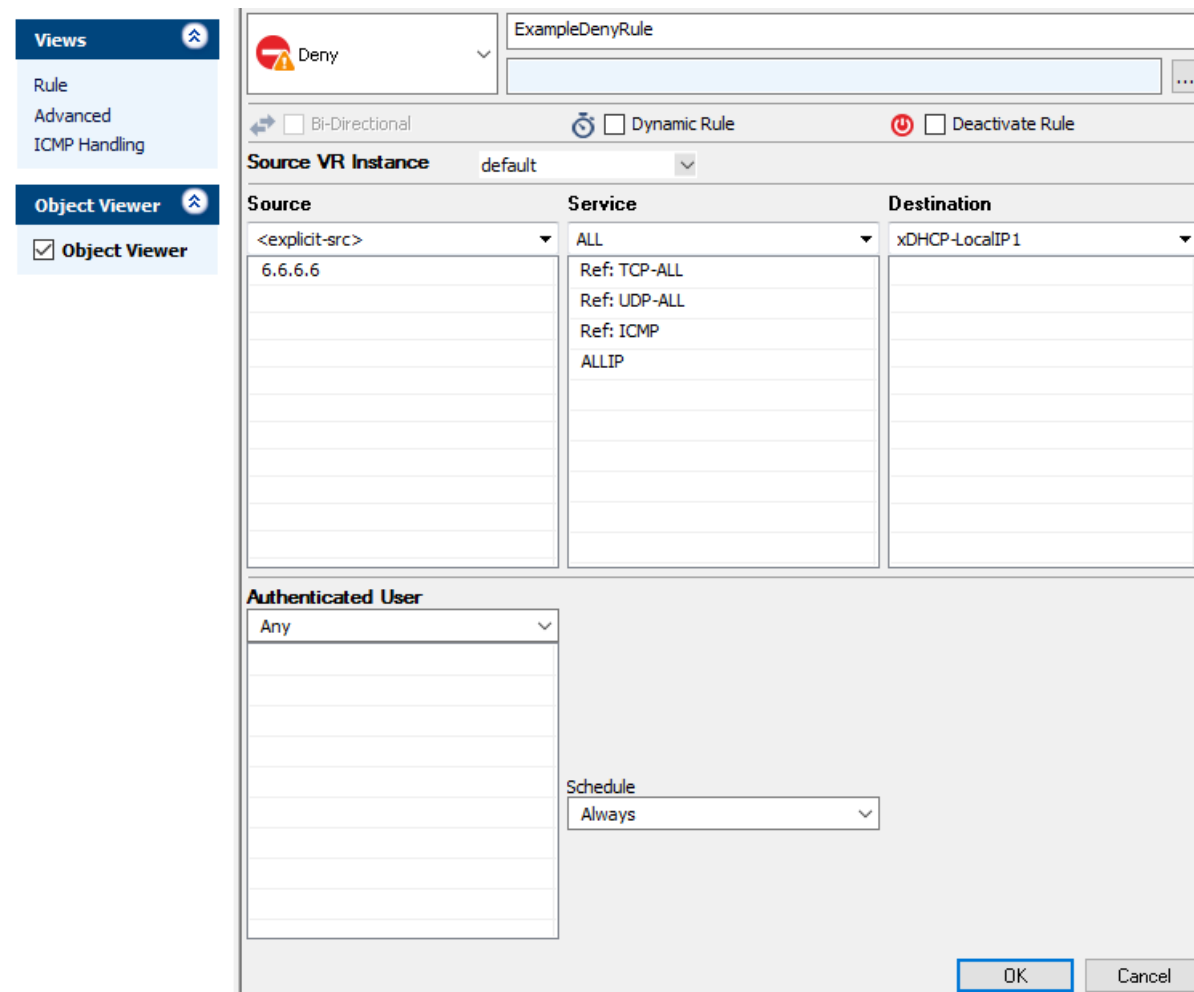


How to Create a Deny Access Rule

<https://campus.barracuda.com/doc/96026207/>

A **Deny** access rule terminates matching network sessions by replying **TCP-RST** for TCP requests, **ICMP Port Unreachable** for UDP requests, or **ICMP Denied by Filter** for other IP protocols. Because the remote host receives a reply, it knows that your system is up and running and protected by a firewall.



The screenshot shows the 'Deny' rule configuration window. The rule name is 'ExampleDenyRule'. The 'Source' is set to '6.6.6.6' (with '<explicit-src>' as the header). The 'Service' is set to 'ALL' (with references to TCP-ALL, UDP-ALL, ICMP, and ALLIP). The 'Destination' is set to 'xDHCP-LocalIP1'. The 'Authenticated User' is set to 'Any'. The 'Schedule' is set to 'Always'. The 'OK' button is highlighted.

Source	Service	Destination
<explicit-src>	ALL	xDHCP-LocalIP1
6.6.6.6	Ref: TCP-ALL Ref: UDP-ALL Ref: ICMP ALLIP	

Create a Deny Access Rule

1. Go to **CONFIGURATION > Configuration Tree > Box > 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 **Deny** as the action.
5. Enter a **Name** for the rule. For example, ExampleDenyRule.
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 deny. 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](#).

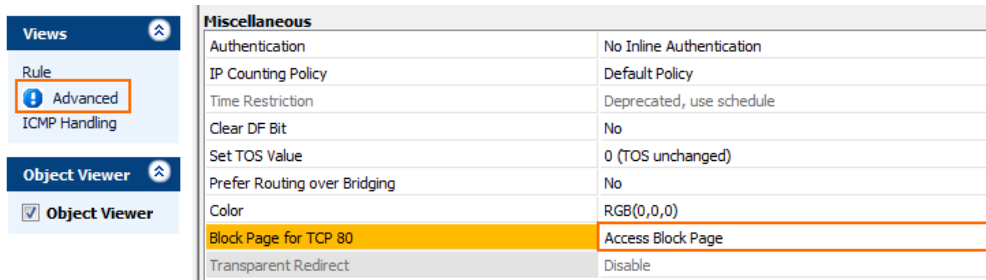
Additional Policy

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

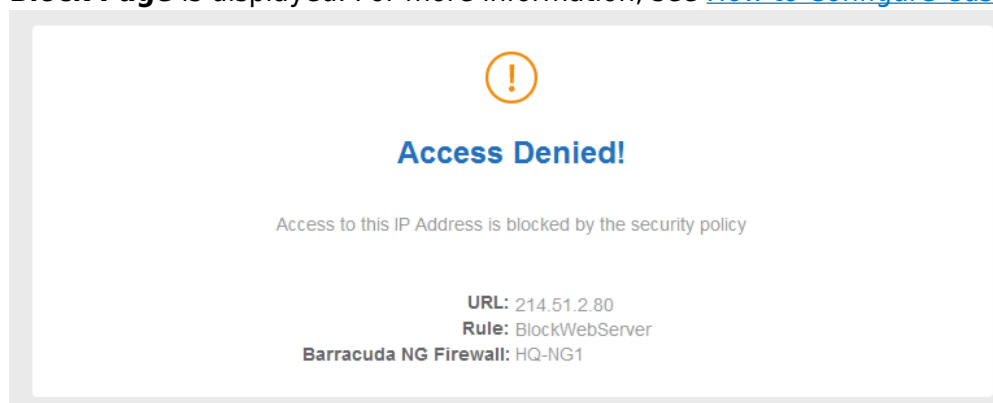
1. Go to **CONFIGURATION > Configuration Tree > Box > Assigned Services > Firewall > Forwarding Rules**.
2. Click **Lock**.
3. Edit a Block access rule. The **Edit Rule** window opens.
4. In the left menu click **Advanced**.
5. In the **Miscellaneous** section, set **Block Page for TCP 80** to **Access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



Miscellaneous	
Authentication	No Inline Authentication
IP Counting Policy	Default Policy
Time Restriction	Deprecated, use schedule
Clear DF Bit	No
Set TOS Value	0 (TOS unchanged)
Prefer Routing over Bridging	No
Color	RGB(0,0,0)
Block Page for TCP 80	Access Block Page
Transparent Redirect	Disable

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. deny_rule.png
2. FW_Rule_Add01.png
3. FW_Block_Rule_Advanced_HTTP.png
4. FW_Block_Rule_HTTP_Page.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.