

How to Configure Inline Firewall Authentication

<https://campus.barracuda.com/doc/41116015/>

Inline authentication intercepts unauthorized users HTTP or HTTPS connections and redirects them to a login page on the Barracuda NG Firewall. After successful authentication the user is forwarded to the original destination. This type of authentication is used to allow HTTP/HTTPS access to authenticated users. Access rules using inline authentication do not block non HTTP or HTTPS traffic even from unauthorized users.

In this article:

Before you Begin

Choose and configure the authentication scheme. For more information, see [Authentication](#).

Step 1. Configure the Firewall Authentication Settings

For a basic configuration, only a default HTTPS certificate and the corresponding key is required.

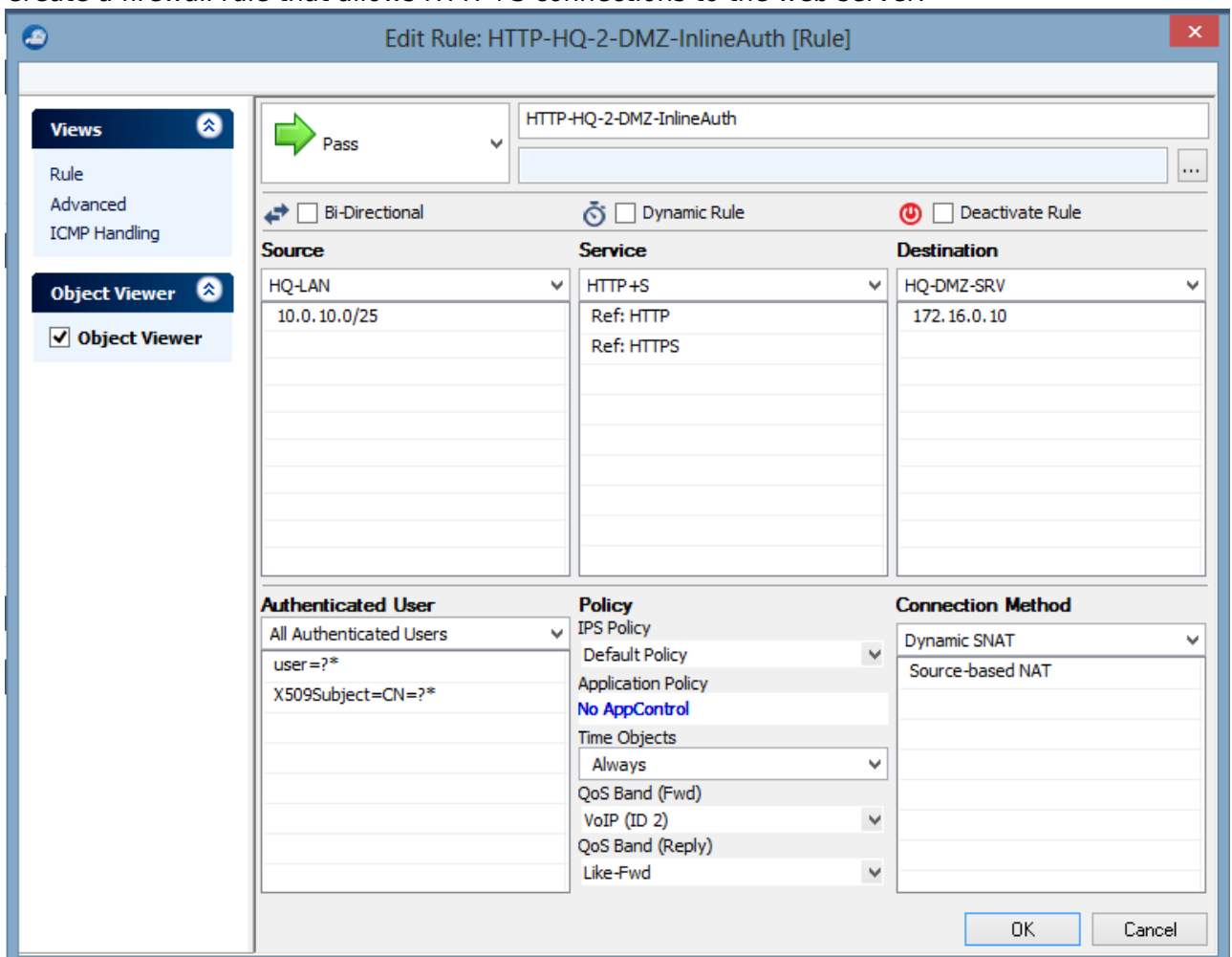
1. Go to the **Forwarding Settings** page (**Config > Box > Virtual Servers > your virtual server > Assigned Services > Firewall**).
2. In the left menu, select **Authentication**.
3. Click **Lock**.
4. To configure the firewall authentication, HTTP, and HTTPS settings, click **Edit** next to **Operational Settings**.
5. Click the **Operational Settings Edit** button. The **Operational Settings** window opens.
6. For each client network containing clients which need to authenticate click **+** in the **Automatic Authentication Redirection** section and enter the **network address**. E.g., `10.0.81.0/24`
7. (optional) Set **Refresh auth every ... min** to the number of minutes the authentication is valid for. Default: 5
8. (optional) Set **Refresh auth tolerance ... min** to the number of minutes that a peer does not have to authenticate again after reconnecting.
9. Click **OK**.
10. Import or create the **Default HTTPS Private Key** and **Default HTTPS Certificate**.

The **Name** of the certificate must be the FQDN resolving to the IP address of the Barracuda NG Firewall. This value is used to redirect the client to the authentication daemon.

11. In the **Metadirectory Authentication** section, select a previously configured **Authentication Scheme**. For more information, see [Authentication](#).
12. Click **Send Changes** and **Activate**.

Step 2. Create the Firewall Rule for Inline Authentication

1. Go to the **Forwarding Rules** page (**Config > Box > Virtual Servers > your virtual server > Assigned Services > Firewall**).
2. Create a firewall rule that allows HTTP+S connections to the web server.



The screenshot shows the 'Edit Rule' window for 'HTTP-HQ-2-DMZ-InlineAuth [Rule]'. The interface includes a left sidebar with 'Views' (Rule, Advanced, ICMP Handling) and 'Object Viewer' (checked). The main area is divided into several sections:

- Action:** A green arrow icon and a dropdown menu set to 'Pass'.
- Options:** Checkboxes for 'Bi-Directional', 'Dynamic Rule', and 'Deactivate Rule'.
- Source:** A dropdown menu set to 'HQ-LAN' with the IP address '10.0.10.0/25' listed below.
- Service:** A dropdown menu set to 'HTTP+S' with references for 'HTTP' and 'HTTPS' listed below.
- Destination:** A dropdown menu set to 'HQ-DMZ-SRV' with the IP address '172.16.0.10' listed below.
- Authenticated User:** A dropdown menu set to 'All Authenticated Users' with filters 'user=?*' and 'X509Subject=CN=?*' listed below.
- Policy:** A dropdown menu set to 'Default Policy' with other options like 'Application Policy', 'No AppControl', 'Time Objects', 'QoS Band (Fwd)', 'VoIP (ID 2)', 'QoS Band (Reply)', and 'Like-Fwd' listed below.
- Connection Method:** A dropdown menu set to 'Dynamic SNAT' with 'Source-based NAT' listed below.

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

3. In the left menu of the rule editor window, click **Advanced**.
4. In the **Miscellaneous** section, select **Login+Password Authentication** from the **Inline Authentication for HTTP and HTTPS** list.

Miscellaneous	
Inline Authentication for HTTP and HTTPS	Login+Password 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	None; SYN Block
Transparent Redirect	Disable
Quarantine Policy	
LAN Rule Policy	Match
Quarantine Class 1 Rule Policy	Block
Quarantine Class 2 Rule Policy	Block
Quarantine Class 3 Rule Policy	Block

5. In the left menu, click **Rule**.
6. In the **Authenticated User** section, specify the users this rule should match for. You can either define a user group object or create an explicit user condition for this rule.
 - To grant access to all authenticated users, select *All Authenticated Users*.
 - To create an explicit user condition:
 - Select .
 - Right-click the table and select **Edit**.
 - In the **Edit/Create User Object** window, click **New**.
 - In the **User Condition** window, specify all authenticated users that are allowed access to the web server.
 - Click **OK**.
7. Click **Send Changes** and **Activate**.

Figures

1. inline_auth01.png
2. inline_auth02.png

© Barracuda Networks Inc., 2019 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.