How to Configure Inline Firewall Authentication

https://campus.barracuda.com/doc/79463020/

Inline authentication intercepts unauthorized users HTTP or HTTPS connections and redirects them to a login page on the Barracuda CloudGen 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. To avoid browser certificate errors, use a signed SSL certificate or install the root certificate of the self-signed certificate on all client computers using Inline Authentication.

Before You Begin

Choose and configure the authentication scheme. For more information, see Authentication.

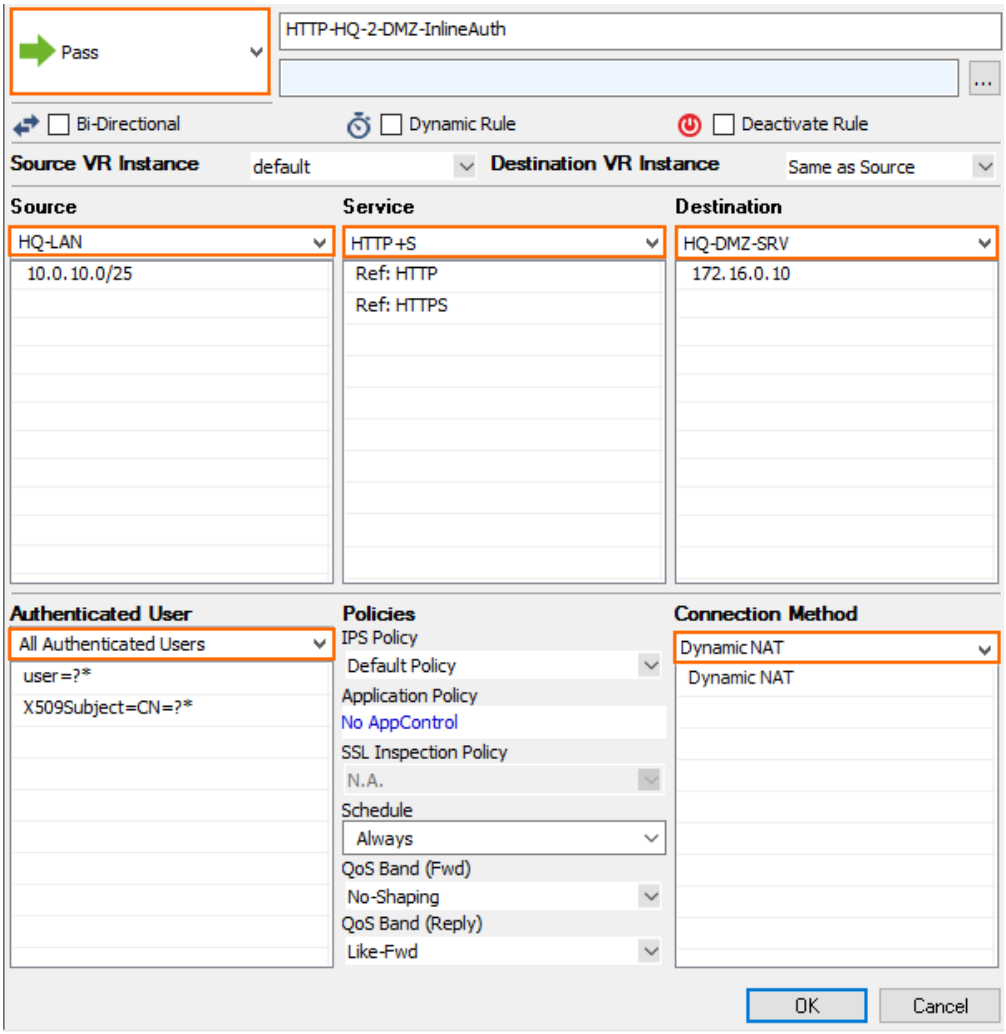
Step 1. Configure the Firewall Authentication Settings

For a basic configuration, only a default HTTPS certificate and the corresponding key is required. Download and install the root certificate on all client computers to avoid browser certificate errors.

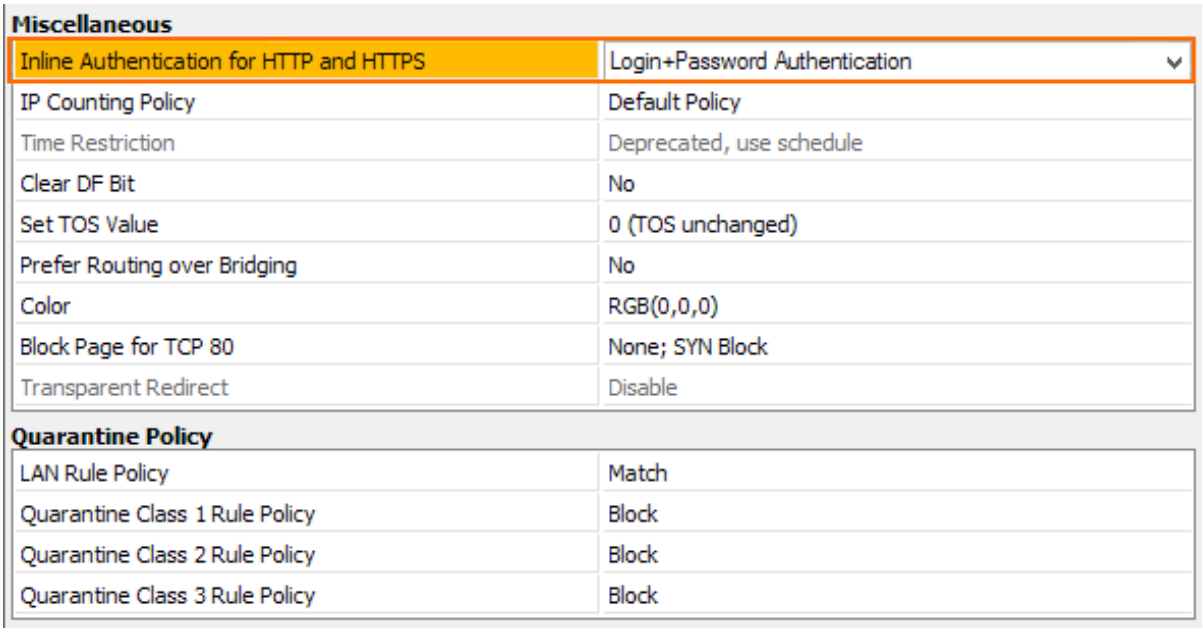
1. Go to **CONFIGURATION > Configuration Tree > Box > Assigned Services > Firewall > Forwarding Settings**.
2. In the left menu, select **Authentication**.
3. Click **Lock**.
4. Click the **Operational Settings Edit** button. The **Operational Settings** window opens.
5. (optional) Set **Refresh auth every... min** to the number of minutes the authentication is valid for. Default: 5
6. (optional) Set **Refresh auth tolerance... min** to the number of minutes that a peer does not have to authenticate again after reconnecting.
7. Click **OK**.
8. Import or create the **Default HTTPS Private Key** and **Default HTTPS Certificate**.
   The **Name** of the certificate must be the IP address or a FQDN resolving to the IP address of the Barracuda CloudGen Firewall. This value is used to redirect the client to the authentication daemon.
9. In the **Metadirectory Authentication** section, select a previously configured **Authentication Scheme**. For more information, see Authentication.
10. Click **Send Changes** and **Activate**.

Step 2. Create the Access Rule for Inline Authentication

1. Go to **CONFIGURATION > Configuration Tree > Box > Assigned Services > Firewall > Forwarding Rules**.
2. Create an access rule that allows HTTP+S connections to the web server.



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 *<explicit-user>*.
        - 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., 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.