How to Configure Permission Profiles

https://campus.barracuda.com/doc/41115922/

The Barracuda SSL VPN service lets you configure a default permission profile to define monitoring and access control settings for users who connect to the SSH proxy. If some of the configurable settings should apply only to specific users, you can also configure custom permission profiles and add them to specific users. The following article provides step-by-step instructions on how to configure default and custom permission profile settings.

In this article:

Configure Default Permissions

To configure the default permission profile that applies to all users who connect to the SSH proxy, complete the following steps:

Step 1. Configure User Monitoring

1. Open the **SSH Proxy** page (**Config** > **Full Config** > **Box** > **Virtual Servers** > ***your Server*** > **Assigned Services**).
2. In the left menu, click **Default Permission Profiles**.
3. Click **Lock**.
4. If terminal sessions of users should be recorded to a local file, enable **Record Terminal Session**.
5. In the **Recorded Users** table, add the login names of the users whose sessions should be recorded.
6. In the **Inactivity Grace Time** field, specify the maximum inactivity time in seconds a user may spend within the proxy menu before being disconnected.
7. Click **Send Changes** and **Activate**.

Step 2. Configure Target Access Control

1. Open the **SSH Proxy** page (**Config** > **Full Config** > **Box** > **Virtual Servers** > ***your Server*** > **Assigned Services**).
2. In the left menu, click **Switch to Advanced View**.
3. Click **Lock**.
4. In the **Target Access Control** section, enable **Allow Console Access** if local addresses on the firewall should be accepted as legitimate targets.
5. From the **Access Control Policy** list, specify how users should be granted access to certain destinations:

1. **By Explicit Network Restriction –** Users are given access based on the list of addresses in the **Explicit Network ACL** table.
    - In the **Explicit Network ACL** table, add users who are not in the **Blocked User Groups** table if you want to give them additional access rights due to source network restrictions.
2. **By Referenced Target Access List –** Users are given access to certain destinations based on destination hosts defined in an access list.
    - Select a configured list from the **Target Access List** menu. For more information on creating target access lists, see How to Configure the SSH Proxy.

6. In the **Custom Source IP field**, define the source IP address for outbound SSH connections.
7. Select the SSH protocol version used for connecting to remote targets.
   Because SSHv1 is considered insecure, Barracuda Networks highly recommends that you select *v2-only*.
8. From the **Outbound Compression Policy** list, select how the SSH proxy should handle outbound compression.
   This setting determines if compression shall be requested for outbound connections to targets. This may negatively impact the firewall as the use of compression can create a significant system load.
9. If users are supposed to make X-Windows connections through the proxy service, enable **Forward X11 connections**.
10. If connecting users should be allowed to authenticate themselves at a target system with public key authentication, enable **Allow Public Keys**.
11. Enable **Support Agent Forwarding** if the connection to the authentication agent (if any) is forwarded to the connecting user's machine.
    This is required when users are allowed to use cascaded agent forwarding. Agent forwarding should be enabled with caution. Users with the ability to bypass file permissions on the connecting host (for the agent's Unix-domain socket) can access the local agent through the forwarded connection. Attackers cannot obtain key material from the agent. However, they can perform operations on the keys that enable them to authenticate using the identities loaded into the agent.
12. In the **Target Alive Interval[s]** field, define the timeout interval in seconds after which, if no data has been received from the server, the proxy should send a message through the encrypted channel to request a response. (0 means that no messages are sent.)
13. In the **Target Alive Max Count** field, define the number of server alive messages which may be sent without the proxy receiving any messages back from the target server. If this threshold is reached while server alive messages are being sent, the proxy will disconnect from the server, terminating the session.
14. From the **Outbound Log Level** list, select the log level for outbound connections.
15. From the **SSH Escape Character** list, select the escape character if required.
    The escape character is only recognized at the beginning of a line. The escape character followed by a dot '.' closes the connection; followed by CTRL-Z suspends the connection; and followed by itself sends the escape character once. 'none' disables any escapes. Value 'hash' stands for character '#'
16. Click **OK**.
17. Click **Send Changes** and **Activate**.

Configure Custom Permission Profiles

If some of the configurable settings should apply only to specific users, configure custom permission profiles. The settings for the default and custom permission profiles are similar. To configure custom permission profiles,

1. Open the **SSH Proxy** page (**Config** > **Full Config** > **Box** > **Virtual Servers** > ***your Server*** > **Assigned Services**).
2. In the left menu pane, click **Custom Permission Profiles**.
3. Click **Lock**.
4. In the left menu, click **Switch to Advanced View**.
5. Next to **Profile Settings**, click **+**, enter a name for the profile and click **OK** to open the **Profile Settings** configuration.
6. Configure the custom profile settings as described in **Configure Default Permission Profiles**.
7. Click **OK**.
8. Click **Send Changes** and **Activate**.

Apply Permission Profiles to Users

After configuring custom permission profiles, you can apply them to specific users.

1. Open the **SSH Proxy** page (**Config** > **Full Config** > **Box** > **Virtual Servers** > ***your Server*** > **Assigned Services**).
2. In the left menu, click **User Authorization**.
3. Click **Lock**.
4. In the **User Authorization** table, add profiles for your users. For each entry, configure the following settings:
   - **User Names –** In this table, add the names of users to which the profile settings will be applied.
   - **Applicable Permission Profile –** Select the permission profile to be applied to the users listed in the **User Names** table.
5. Click **OK**.
6. Click **Send Changes** and **Activate**.