How to Configure the SSH Proxy

https://campus.barracuda.com/doc/73719362/

Follow the step-by-step instructions to configure the SSH Proxy service. All information applies to SSH version V2 or higher.

Step 1. Configure Networking Settings

Configure basic network and service identification settings for the SSH proxy service.

1. Go to **CONFIGURATION** > **Configuration Tree** > **Box** > **Virtual Servers** > ***your virtual server*** > **Assigned Services** > **SSH Proxy**.
2. Click **Lock**.
3. From the **Authentication Scheme** list, select the login authentication scheme.
4. In the **TCP Listen Port** field, specify the listening port of your SSH Proxy service, if required (default: *22*). If you change this to a port other than 22, clients trying to use this service will need to explicitly set this port in their configuration.
5. In the **Service Identification section**, create or import the ECDSA, RSA, or DSA host key that the SSH frontend is being identified by:
   - **ECDSA** – Use this key if you want increased security and lower CPU usage.
   - **DSA** – Predecessor for ECDSA and recommended for systems that do not support ECDSA. DSA provides the same security level as ECDSA but has a multiple key length.
   - **RSA** – Predecessor for DSA and recommended for older systems that do not support DSA or ECDSA.
6. Click **Send Changes** and **Activate**.

Step 2. Configure Access Policies

Configure access policies for users and groups that are allowed or denied access to the SSH Proxy.

1. Go to **CONFIGURATION** > **Configuration Tree** > **Box** > **Virtual Servers** > ***your virtual server*** > **Assigned Services** > **SSH Proxy**.
2. In the left menu, select **Service Access Protection**.
3. Click **Lock**.
4. Enable **Use Group Policies** to configure access restrictions by group information.
5. In the **Allowed User Groups** and **Blocked User Groups** tables, add user groups that should be allowed or denied access.
6. Click **Send Changes** and **Activate**.

Step 3. Configure DoS Protection

Configure client alive intervals and remote host verification to protect your network against denial of service (DoS) attacks. With DNS reverse lookup, SSHD performs a lookup on the remote host name and verifies that the resolved host name for the remote IP address maps back to the very same IP address.

1. Go to **CONFIGURATION** > **Configuration Tree** > **Box** > **Virtual Servers** > ***your virtual server*** > **Assigned Services** > **SSH Proxy**.
2. In the left menu, select **Service Access Protection**.
3. Click **Lock**.
4. In the **Denial of Service (DoS) Protection** section, adjust the following settings according to your requirements:
   - **Login Grace Time** – Specify the maximum length of time for a login attempt (default: *120* seconds).
   - **Pending Session Limit** – Specify the maximum number of pending sessions (initiated but not established). (Default: 20 sessions)
5. Click **Send Changes** and **Activate**.

Step 3. Configure the Target Access List

1. Go to **CONFIGURATION** > **Configuration Tree** > **Box** > **Virtual Servers** > ***your virtual server*** > **Assigned Services** > **SSH Proxy**.
2. In the left menu, select **Target Access Lists**.
3. Click **Lock**.
4. In the **Access Lists** table, add allowed target hosts. For each host, configure the following settings:
   - **User Visible Name** – The name of the target host. This name is displayed to the user when connecting to the SSH Proxy.
   - **Target FQDN** – The fully qualified domain name of the target host defined in DNS.
   - **Target IP Address** – The IP address of the target host that is allowed to connect. This IP address is displayed to the user when connecting to the SSH Proxy.
   - **Target Port** – The network port of the target host that is allowed to connect. This port is displayed to the user when connecting to the SSH Proxy.
5. Click **OK**.
6. Click **Send Changes** and **Activate**.

Step 4. Configure Permission Profiles

Configure default and custom permission profiles for users that are allowed access to the SSH Proxy. For more information, see How to Configure Permission Profiles.