How to Configure the SSH Proxy

https://campus.barracuda.com/doc/43847278/

The following article provides step-by-step instructions on how to configure the Barracuda NG Firewall SSH proxy service.

In this article:

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. In the left menu, click **Switch to Advanced View**.
3. Click **Lock**.
4. From the **Authentication Scheme** list, select the login authentication scheme.
5. 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.
6. Enable **Allow Inbound Compression** if the SSH server supports compression. Barracuda recommends to disable inbound compression when deploying the SSH Proxy in LAN environments to avoid CPU load on the system.
7. If synchronization between HA partners (SSL based with user/key) is required, enable **HA Sync** and define the key for HA sync tasks. For more information, see High Availability.
8. From the **Inbound Log Level** list, select the log level for inbound connections.
9. In the **Service Identification section**, create or import the RSA or DSA host key for the server, depending on your requirements.
10. If you want to specify an explicit SSH proxy user, select the **Other** check box next to **Run as User** and enter the new username.
    This username is used when synchronizing the log with an HA partner (default: *sshprx*). The user ID is used as the HA sync port (default: *8099*). If using a different user ID, make sure that you also adjust the port in the service object for the HA synchronizations in the local firewall rule set.
    If multiple instances of the SSH proxy run on the same system, you must enter a different username and user ID for each service.
11. 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. In the left menu, click **Switch to Advanced View**.
5. Enable **Use Group Policies** to configure access restrictions by group information.
6. In the **Allowed User Groups** and **Blocked User Groups** tables, add user groups that should be allowed or denied access.
7. 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 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 left menu, click **Switch to Advanced View**.
5. 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).
   - **Client Alive Interval(s) –** (Applies to protocol version 2 only) Set the interval between messages sent by sshd through the encrypted channel to request a response from the client if no data has been received. If you want to disable these messages, enter *0*.

     The use of client alive messages is very different from KeepAlive. Client alive messages are sent through the encrypted channel and are not spoofable. The TCP keepalive option enabled by KeepAlive is spoofable. The client alive mechanism is important when the client or server must know when a connection has become inactive.
   - **Client Alive Max Count –** Specify the maximum number of client alive messages that

sshd will send before disconnecting the client and terminating the session.
- **DNS Reverse Lookup –** Enable if sshd should look up the remote host name.

6. 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.