How to Configure SSH

https://campus.barracuda.com/doc/48203211/

The SSH daemon listens on all management IP address on TCP port 22. Connect to the firewall with SSH when performing software updates or other special maintenance tasks. You can use both external SSH clients, or connect via the SSH tab in NextGen Admin.

You can use an external SSH client to open an SSH connection to the Barracuda NextGen Firewall F-Series. You can also use the terminal integrated in Barracuda NextGen Admin; direct access to the Barracuda NextGen Firewall F-Series is provided via SSH version 2. To access the SSH terminal, click the **SSH** tab.

You can enable event notifications for SSH, as well as view the SSH log for information such as system access and remote command execution. In the **Select Log File** list on the **Logs** page, you can find the sshd log file in the **Box** directory.

Use an External SSH Client

If you prefer to use your own SSH client, configure NextGem Admin with the path to the executable:

1. Click on the **OPTIONS** tab in the top left corner.
2. Select **Settings**.
3. Expand the **Client Settings** section.
4. In the **External SSH Client** enter the command for for external SSH client. use **%ip** and **%user** to dynamically insert the IP address and user name. E.g., *C:\putty.exe %user@%ip*

Configure SSH

1. Go to **CONFIGURATION > Full Configuration > Box > Advanced Configuration > SSH**.
2. Click **Lock**.
3. To configure the general settings for SSH, click **Basic Setup** from the **Configuration** menu in the left navigation pane.
   Basic Setup Settings
   On the **Basic Setup** page for SSH, you can configure the following settings in the **General Settings** section:

Setting	Description

Event on SSH	Specifies if event notifications should be triggered when the system succeeds or fails to start up or shut down (Events Daemon Startup Failed/Succeeded [2070/2071] and Daemon Shutdown Failed/Succeeded [2072/2073]). You can select any of the following options: ◦ *Startup Failure* ◦ *Startup/Shutdown Failure* ◦ *Startup/Shutdown Failure + Startup Success* ◦ *Startup/Shutdown Failure + Startup/Shutdown Success* You are not notified when SSHd is killed manually or just dies unexpectedly. These settings only pertain to SSHd behavior during controlled start or stop sequences.
Allow TCP Forwarding	Specifies if TCP is enabled or disabled. This setting is only available in **Advanced View** mode. Disabling TCP forwarding does not improve security. You must also deny shell access to users because forwarders can be installed with the *ssh* command.
Login Timeout	The maximum length of time in seconds that a user has to successfully log in before the server disconnects. The minimum time limit is *10* seconds. The default length of time is *90* seconds.
Permit Root Login	Permits or prohibits SSH logins for the root user. If you prohibit SSH logins for the root user, the following configuration entities will not work: **Box Exec** tab and **Software Update** tab.
Check User Home	Specifies whether sshd should check file modes and ownership of the user's files and home directory before accepting login. This is normally desirable because novices sometimes accidentally leave their directories or files writable. The default is *yes*. This setting is only available in **Advanced View** mode.
Send Keepalives	Specifies if the server should send keepalive messages. Default: *yes*. ◦ To avoid hanging sessions, enable keepalive messages to monitor the connection. The server notices if the network goes down or the client host reboots. However, this may cause some inconveniences because connections are disconnected even when the route is temporarily down. ◦ If keepalive messages are disabled, sessions may hang indefinitely on the server, leaving "ghost" users and consuming server resources.
Supported Protocols	Specifies which SSH versions are supported by sshd. You can enable support for only version 2, or you can enable support for both versions 2 and 1 (with version 2 being the preferred choice). Barracuda Networks recommends that you only enable support for SSH version 2 because version 1 is vulnerable to man-in-the-middle attacks. By default, the Barracuda Networks client tries to use version 2. This setting is only available in **Advanced View** mode.

4. To configure settings that are specific to each SSH version, click **Advanced Setup** from the **Configuration** menu in the left navigation pane.
   SSH Version 2 Options
   For SSH version 2, you can configure the following settings in the **Protocol Version 2 Options** section:

Setting	Description
Allow Compression	Specifies if compression should be enabled or disabled for SSH clients.
Force Key Authentication	Specifies if key usage is mandatory or optional for SSH clients. If key usage is mandatory for external SSH clients and you want to automate user logins, the private key of the client certificate on the Windows system must be generated in a UNIX compatible format. For instructions on how to generate the required key, see the following Handling Forced Key Authentication section. This setting is only available in **Advanced View** mode.
Secure FTP Support	Specifies if sshd implements the sftp subsystem. Secure FTP may be viewed as a more comfortable alternative to the *humble scp* command when trying to transfer bulk data to or from the box. This setting is only available in **Advanced View** mode.

SSH Version 1 Options

For SSH version 1, you can configure the following settings in the **Protocol Version 1 Options** section:

Setting	Description
Server Key Length (Bits)	Defines the number of bits in the ephemeral protocol version 1 server key. The minimum value is *512*, and the default is *768*.
Key Regeneration Period	Specifies the interval in seconds that the ephemeral server key is automatically regenerated after being used. Regenerating the key prevents the decryption of captured sessions if the keys are stolen. The key is only stored in memory. If you do not want the key to be regenerated, enter *0*. The Barracuda Networks default is *900* (seconds).

5. Click **Send Changes** and **Activate**.

Handling Forced Key Authentication

For various administrative purposes (such as collecting statistics with external tools), it may be desired to randomly connect to a system with an external SSH client, thereby omitting user interaction. Using the Microsoft Management Console (MMC), you can export a private key in encrypted PFX file format from the Certificate Store. However, this file is not usable by the Barracuda NextGen Firewall F-Series. You must convert the PFX file to an unencrypted private key in PEM format.

1. Create an Administrative Login

1. Go to **CONFIGURATION > Full Configuration > Box > Administrators**.
2. Click **+** to add a new administrative account.
3. Enter a name for the account and click **OK**.
4. In the **Administrator Authentication** section of the **Administrators** window, set

Authentication Level to *Key*.
5. Import the public RSA key that has been issued for this user from the Microsoft Certificate Management Store.

2. Export the Private Key from the Certificate Management Store

1. On the Windows client, open the Certificate Management Store. At the DOS prompt, enter: *C:\windows\system32\certmgr.msc*
2. Browse to **Personal** > **Certificates**.
3. Right-click the certificate and select **All Tasks** > **Export**.
4. In the **Certificate Export Wizard**, select **Yes** to export the private key.
5. In the **PKCS #12** tab, clear the **Enable strong protection** check box.
6. Enter a password.
7. Specify a file name. For example, *private_key.pfx*.

3. Copy the PKCS12 (.pfx) file to a UNIX Client Supporting OpenSSL

Copy the PFX file to a UNIX client that supports OpenSSL, such as the Barracuda NextGen Firewall F-Series.

4. Convert the RSA Key from PKCS12 Format to PEM Format (encrypted)

On the UNIX client, browse to the RSA key. At the command line, enter:

 # openssl pkcs12 -in private_key.pfx
-nocerts -out priv.key

where *priv.key* specifies the file name after conversion.

5. Extract the Private Key and Generate an OpenSSH SSH-2 Private Key (unencrypted)

At the command line, enter:

 # openssl rsa -in priv.key > ~/.ssh/
id_rsa_my_priv_key

where *id_rsa_my_priv_key* specifies the file name after decryption, and *~/.ssh/* is an arbitrarily chosen path on the UNIX client.

6. Log into the Barracuda NextGen Firewall F-Series

At the command line, enter:

 # ssh -i ~/.ssh/id_rsa_my_priv_key

-lloginname dest-ip

where *loginname* specifies the name of the administrative account as defined in **Step 1**, and *dest-ip* specifies the Barracuda NextGen Firewall F-Series's login IP address.

Depending on the client that the key was converted on, you may need to change the file permissions of the private key file. If the gateway refuses to use the key, change the file permissions of the key by entering:

chmod 600 ~/.ssh/id_rsa_my_priv_key

You can use the transformed private key with third-party remote SSH clients. For example, you can use it with SSH agents or import it into PuTTYGen for conversion into the file format for PuTTY (.ppk).