# **Secure Connection with a bastion Host (Jump Box)**

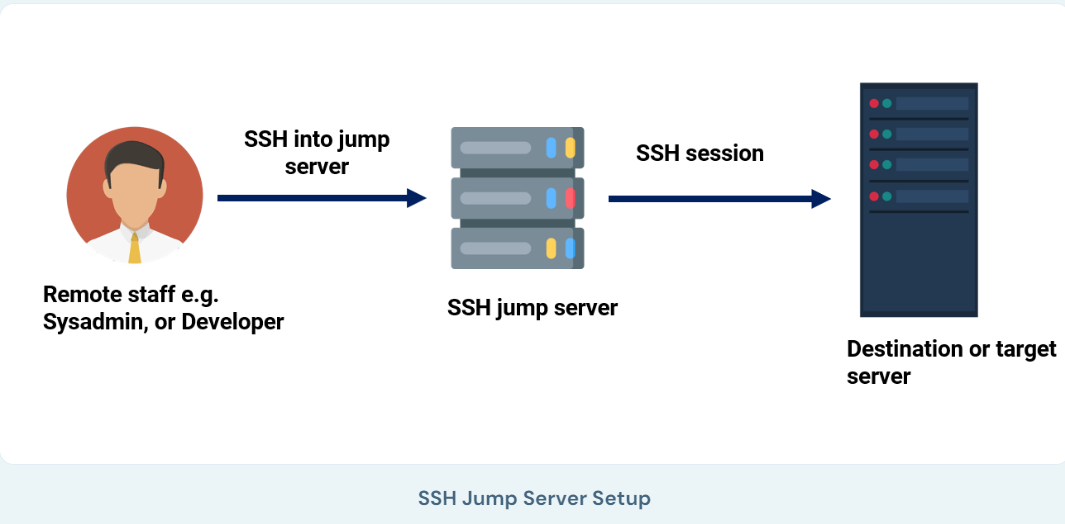
A jumpbox or bastion host is a special-purpose server designed to provide a secure gateway or intermediary for accessing and managing servers within a private network. Usually, a network of servers that’s not publicly available adds a higher layer of security by employing the use of a jump box. This differs from a proxy server; the jump box is the only server exposed to the public Internet. All administrative access to internal servers is routed through this secure access point between an untrusted network (e.g., the Internet) and a trusted internal network.

Jump boxes are often configured to log all access and activities, providing a centralized point for monitoring and auditing administrative actions.

**Use Cases**

* **Administrative Access:** Administrators use the jump box to securely access internal servers for management tasks, ensuring the internal network remains shielded from direct exposure to potential threats.
* **Security Gateway**: It enforces strict access controls, requiring users to authenticate before gaining access to internal resources.
* **Compliance and Auditing:** It helps organizations meet regulatory and compliance requirements by providing a controlled and monitored access point.

**The setup**



* **Single Point of Entry:** Only the jump box has a public IP address and is accessible from the Internet. All other servers within the private network do not have public IP addresses and can only be accessed via the jump box.
* **Multi-Factor Authentication (MFA):** Often configured with MFA to enhance security. With applications like Google authenticator that supplies a security code whenever you log in
* **Hardened Security:** The jump box usually has strict security policies, including firewall rules, intrusion detection/prevention systems, and regular updates.

**Step-by-step guide**

**Prerequisites:**

* **Jump Box (Bastion Host)**: An accessible intermediary server with SSH access.
* **Target Server**: The server you want to reach via the jump box.
* **SSH Keys**: SSH key pairs are set up on the jump box and the target server.
* **SSH Client**: Installed on your local machine (e.g., OpenSSH for Unix/Linux/macOS or PuTTY for Windows).

**Steps:**

**SSH Configuration (Recommended):**

First, SSH keys are generated on the bastion host. Then, the SSH public key is shared with the SSH client (your local machine), which is used to connect remotely to the bastion server. Once you have successfully connected to the bastion host, a secure SSH connection from the jump box can be established to the target server. You can simplify the connection process by configuring your SSH client using the ~/.ssh/config file.

1. **Edit the SSH config file**:

| nano ~/.ssh/config |
| --- |

* **Add the configuration for the jump box and the target server**:

Replace the placeholders (<jumpbox\_ip>, <jumpbox\_user>, etc.) with your actual details.

| Host jumpbox  HostName <jumpbox\_ip>  User <jumpbox\_user>  IdentityFile ~/.ssh/id\_rsa\_jumpbox  Host targetserver  HostName <target\_server\_ip>  User <target\_server\_user>  IdentityFile ~/.ssh/id\_rsa\_target  ProxyJump jumpbox |
| --- |

* **Connect to the target server using the alias**:

| ssh targetserver |
| --- |

**2. Direct SSH Command**

If you prefer not to modify the SSH config file, use the ProxyJump option directly in the SSH command.

* **Run the following command**:

| ssh -J <**jumpbox\_user**>@<**jumpbox\_ip**>  <**target\_server\_user**>@<**target\_server\_ip**> |
| --- |

This command tells SSH to connect to the jump box first and then use it as a proxy to reach the target server.