Port forwarding from jump server to target Linux machine

11 admin September 3, 2026 Productivity & Efficiency Features 16175

How to do Port forward from jump server to target Linux machine added in the bastion host

Overview: This article will help you access the service running on a remote server, with the port forwarded to the gateway server. It can be accessed using the IP or host of the gateway with the forwarded port number.

Step 1. Login to the gateway server and **enable TCP** forwarding.

Enabling TCP forwarding in the gateway will allow the user to jump into the remote server without accessing the gateway server. Make sure to disable the view password option for users.

```
rooot@gateway:~# grep -i tcp /etc/ssh/sshd_config

AllowTcpForwarding yes
```

Step 2. Log in **to ezsh** and navigate to the **specific server** and **press ' [' to open the tunnel.**





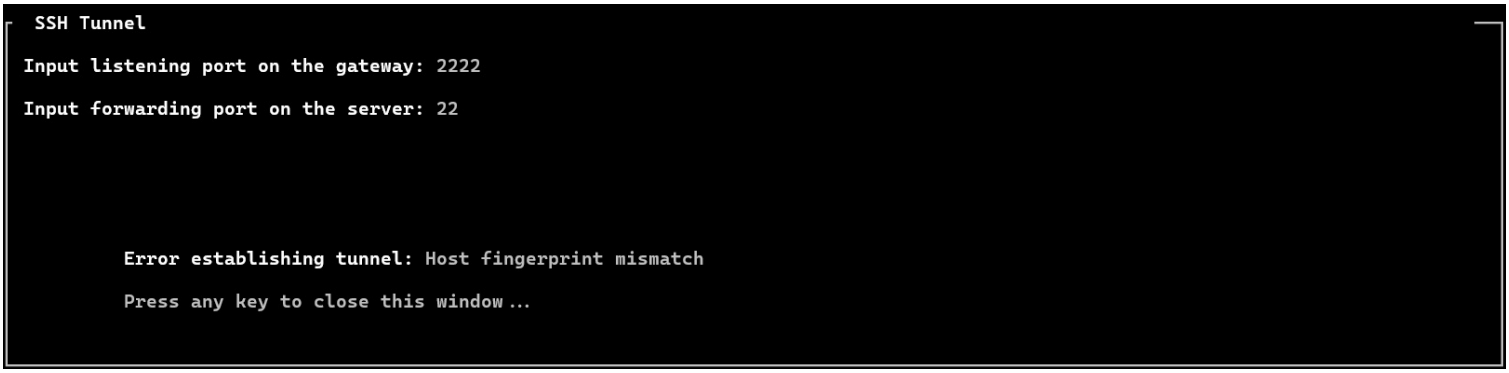
Now you can access the port/service via EZTUNNEL.

For example, in the above configuration, it forwarded port 2222 on the Ezeelogin gateway server to port 22 (SSH) of the remote server.

You can now SSH into the remote server via EZTUNNEL from your desktop

Common errors while establishing tunnel connection **and their Fixes:**

1. Error establishing tunnel: **Host fingerprint mismatch**



Fix: Reset the fingerprint of the server to fix the error

2. Error establishing tunnel: **Authentication failed (2)**



Fix: Check the ezsh.log of the gateway user and confirm password or key-based authentication is working correctly.

```
root@gateway:~# tail /home/{username}/ezsh.log

Authentication by SSH key failed (debian.server, root): Username/PublicKey combination invalid
Authentication by password not supported!
```

3. Error establishing tunnel: **Could not open the direct-tcpip channel.**



Fix: Enable TCP forwarding on the gateway server, then re-login to the shell and attempt to reconnect the tunnel connection.

```
root@gateway:~# grep -i tcp /etc/ssh/sshd_config

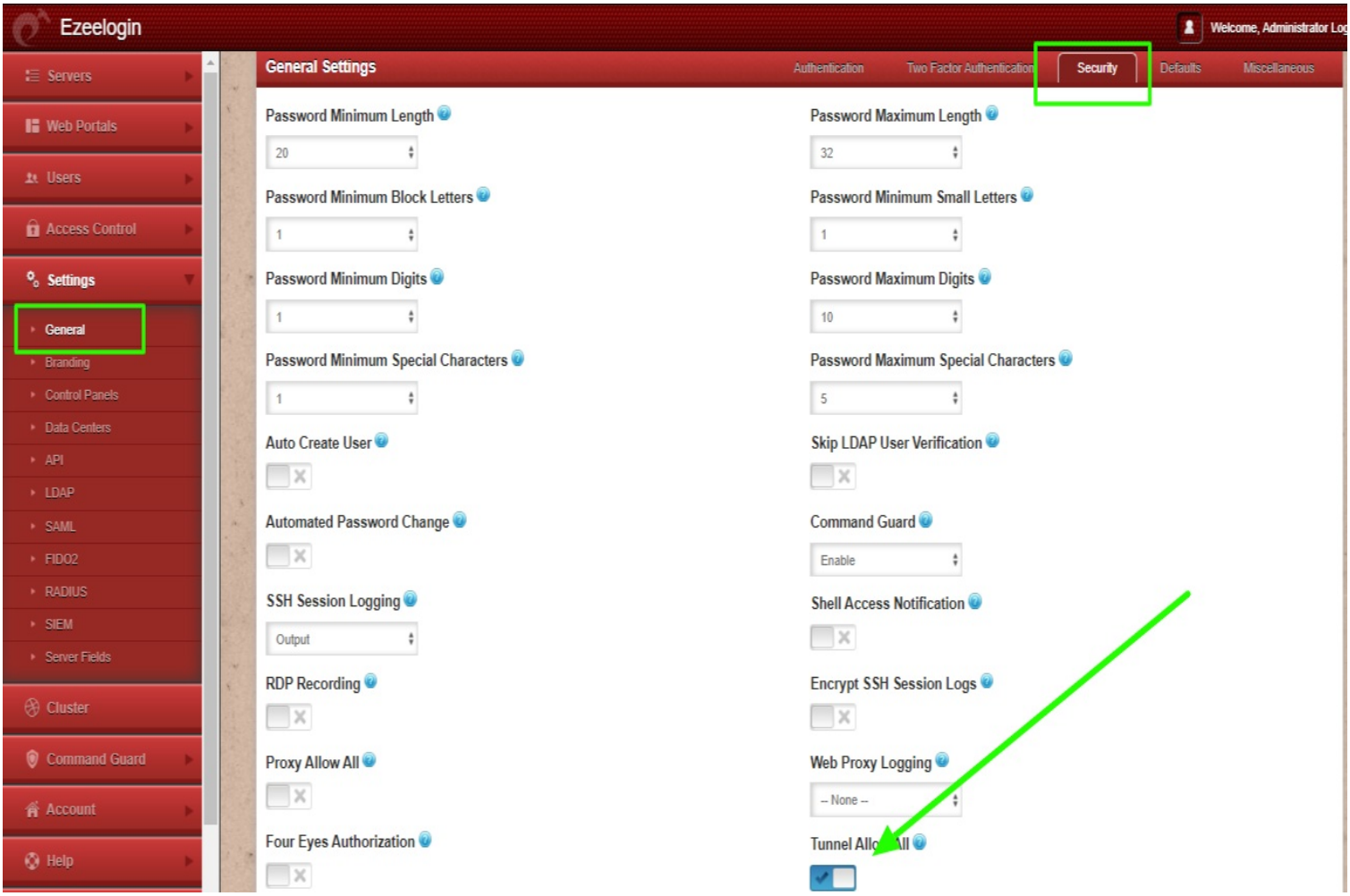
AllowTcpForwarding yes
```

4. If you are not able to access the port forwarded via tunnel, then check the ezsh.log of the gateway user

```
root@gateway:~# tail /home/{username}/ezsh.log

Tunnel is not allowed from all IPs
Client IP is not the same as SSH remote IP
Tunnel access from unauthorized IP: 192.168.1.7 (127.0.0.1)
```

Fix: Enable **Tunnel Allow All** from **Ezeelogin GUI > Settings > General > Security > Tunnel Allow ALL.**



Check out the example video to forward RDP. Access RDP Through SSH Tunnel

The video shows how a tunnel to an RDP port 3389 is set up and toward the end of the video, you will find the SSH tunnel being setup for RDP on the Windows server on which the Bitvise SSHD server was installed.

Basically, the above video shows how the user is able to connect to a remote Windows server RDP on port 3389, by using your.gateway_ip:3389 using the RDP client on the user's desktop.

SSH tunneling sessions are not recorded.

Make sure to close the tunnel session properly using the EZSH shell. If you close the terminal or SSH client directly, the tunnel will remain active, and you will need to manually terminate the process.

Input listening port on the gateway: The gateway server needs to listen on a specific port number. Ensure that this port is not already assigned to any services on the gateway server.

Input forwarding port on the server: The port number to be forwarded to the gateway server must be specified. Ensure that the port number corresponds to the required service.

Related Articles:

Add servers that are accessible via port forwarding via the SSH gateway server
Add Windows server for RDP via browser

Online URL: https://www.ezeelogin.com/kb/article/port-forwarding-from-jump-server-to-target-linux-machine-11.html