The error indicates that your SSH client on Ubuntu cannot connect to the SSH server at 10.0.2.15 on port 22. This could be due to several reasons, including network issues, the SSH server being down, or a firewall blocking the connection.

Here are the steps to troubleshoot and resolve the issue:

Step 1: Check Network Connectivity

Ensure that the SSH server (10.0.2.15) is reachable.

bash

Copy code

```
ping 10.0.2.15
```

- If there's no response, the server might be down, or there's a network issue.

Step 2: Check SSH Port Connectivity

Verify that port 22 is open and accessible.

bash

Copy code

```
nc -zv 10.0.2.15 22
```

- If the port is closed or unreachable, check the firewall settings on the server or any intermediate devices.

Step 3: Verify SSH Server is Running

Log into the SSH server locally or using other available means (e.g., console access) and ensure that the SSH service is running.

bash

Copy code

```
sudo systemctl status ssh
```

If the service is not running, start it:

bash

Copy code

```
sudo systemctl start ssh
```

Enable it to start on boot:

bash

Copy code

```
sudo systemctl enable ssh
```

Step 4: Check Firewall Rules

Ensure the firewall on the server allows incoming SSH connections.

bash

Copy code

```
sudo ufw status
```

If SSH is not listed as allowed, enable it:

bash

Copy code

```
sudo ufw allow 22
sudo ufw reload
```

Step 5: Verify SSH Configuration

Ensure the SSH server configuration allows connections on port 22.

bash

Copy code

```
sudo nano /etc/ssh/sshd_config
```

- Confirm the line Port 22 is present and not commented out (# at the start).
- Confirm the line PermitRootLogin yes if you're attempting to log in as root (not recommended for security reasons).

Restart the SSH service after any changes:

bash

Copy code

```
sudo systemctl restart ssh
```

Step 6: Test SSH Connection

Try connecting from the client again:

bash

Copy code

```
ssh user@10.0.2.15
```

Replace user with the username on the server.

Step 7: Debug SSH Connection

Use verbose mode to get detailed connection logs:

bash

Copy code

```
ssh -v user@10.0.2.15
```

Analyze the output for specific issues.

Example Commands:

On the SSH server:

bash

Copy code

```
sudo systemctl start ssh
sudo ufw allow 22
sudo ufw reload
```

On the SSH client:

bash

Copy code

```
ping 10.0.2.15
nc -zv 10.0.2.15 22
ssh -v user@10.0.2.15
```

If these steps don't resolve the issue, please provide the output of the verbose SSH command for further analysis.

4o

You said:

to 10.0.2.15, port 22. Windows error 10060: A connection attempt failed because the connected party did not properly respond after a period of time, or established connection failed because connected host has failed to respond. 50:26.048 The SSH connection has been terminated. Log in solve this error ?

ChatGPT said:

ChatGPT

The error message indicates that the SSH client is unable to establish a connection to the SSH server at 10.0.2.15 on port 22. The Windows error 10060 typically occurs when a connection attempt times out because:

1. The SSH server is not reachable or not responding.
2. Port 22 is not open or is blocked by a firewall or security rule.
3. The SSH service on the target machine is not running or misconfigured.

Here's how to troubleshoot and resolve the issue step by step:

Step 1: Ensure the SSH Server is Reachable

Run the following command to check connectivity:

bash

Copy code

```
ping 10.0.2.15
```

- If the server does not respond, it may be down, or there might be a network issue. Verify the network settings and ensure the server is powered on.

Step 2: Verify SSH Port Accessibility

Test if port 22 is open and accessible:

bash

Copy code

```
nc -zv 10.0.2.15 22
```

- If this fails, port 22 might be blocked or not listening on the server. Proceed to check the SSH server setup.

Step 3: Confirm SSH Service is Running

Log into the server (10.0.2.15) directly or through another accessible method (e.g., console or GUI) and verify the SSH service:

bash

Copy code

```
sudo systemctl status ssh
```

- If the SSH service is not running, start it:

bash

Copy code

```
sudo systemctl start ssh
```

- Enable it to start on boot:

bash

Copy code

```
sudo systemctl enable ssh
```

Step 4: Check Firewall Rules on the Server

Verify that the firewall allows incoming SSH connections:

bash

Copy code

```
sudo ufw status
```

- If SSH is not allowed, enable it:

bash

Copy code

```
sudo ufw allow 22
sudo ufw reload
```

Step 5: Verify SSH Server Configuration

Inspect the SSH server's configuration file to ensure it is listening on port 22:

bash

Copy code

```
sudo nano /etc/ssh/sshd_config
```

- Look for the line Port 22 and ensure it is not commented out.
- Confirm that the configuration allows the intended user to log in.

Restart the SSH service after any changes:

bash

Copy code

```
sudo systemctl restart ssh
```

Step 6: Test Connection from the Client

From the client machine, test the SSH connection:

bash

Copy code

```
ssh -v user@10.0.2.15
```

Replace user with the username you are using to connect. The -v flag provides detailed logs that can help identify the problem.

Step 7: Check Intermediate Firewalls or NAT

If the server is behind a NAT or a firewall (e.g., a router), ensure that port 22 is forwarded correctly to the internal IP address of the server (10.0.2.15).

Common Scenarios and Fixes

1. **Server is not running SSH service**: Start the SSH service on the server.
2. **Firewall blocking port 22**: Open port 22 on the server and any intermediate devices.
3. **Wrong IP Address**: Verify the correct IP address of the server.
4. **SSH Configuration Issues**: Double-check the /etc/ssh/sshd_config file.

Example Commands Summary:

On Server:

bash

Copy code

```
sudo systemctl start ssh

sudo systemctl enable ssh

sudo ufw allow 22

sudo systemctl restart ssh
```

On Client:

bash

Copy code

```
ping 10.0.2.15

nc -zv 10.0.2.15 22

ssh -v user@10.0.2.15
```

If these steps do not resolve the issue, share the detailed output of the ssh -v command for further analysis.