Remote SSH Setup for moOde Pi

Purpose: Allow remote SSH access to moOde Pi from external network
Date: 2025-01-03

Prerequisites

• ■ moOde installed and running on Pi
• ■ SSH enabled on Pi
• ■ User configured (andre:0815)
• ■ Pi accessible on local network

Option 1: Port Forwarding (Router)

If you have access to router settings:

Steps:

1. **Find Pi's local IP:**
```
# On Pi or local network
ip addr show | grep "inet " | grep -v 127.0.0.1
# Or check router admin panel
```

2. **Configure router port forwarding:**
• External Port: 2222 (or any unused port)
• Internal IP: Pi's local IP (e.g., 192.168.10.2)
• Internal Port: 22 (SSH)
• Protocol: TCP

3. **Find your public IP:**
```
curl ifconfig.me
# Or check router admin panel
```

4. **Access from remote:**
```
ssh -p 2222 andre@YOUR_PUBLIC_IP
# Password: 0815
```

Option 2: VPN (Recommended)

Set up VPN on router or use PiVPN:

PiVPN Setup:

1. **Install PiVPN on Pi:**
```
curl -L https://install.pivpn.io | bash
```

2. **Follow setup wizard:**
• Choose WireGuard or OpenVPN
• Configure port (default 51820 for WireGuard)

• Set DNS

3. **Create client profile:**
```
pivpn add
```

4. **Transfer profile to client device**

5. **Connect from remote device**

6. **Access Pi via local IP:**
```
ssh andre@192.168.10.2
```

Option 3: SSH Tunnel/Reverse SSH

For temporary access:

From Pi (creates reverse tunnel):

```
ssh -R 2222:localhost:22 user@REMOTE_SERVER
```

Then access via:
```
ssh -p 2222 andre@REMOTE_SERVER
```

Option 4: Dynamic DNS + Port Forwarding

For dynamic IP addresses:

1. **Set up Dynamic DNS service** (No-IP, DuckDNS, etc.)
2. **Configure router port forwarding** (see Option 1)
3. **Access via:**
```
ssh -p 2222 andre@yourdomain.dyndns.org
```

Security Recommendations

1. Change Default Password

```
passwd andre
```

2. Use SSH Keys (Instead of Password)

```
# On client machine
ssh-keygen -t ed25519
ssh-copy-id andre@PI_IP

# Disable password authentication (optional, after keys work)
# Edit /etc/ssh/sshd_config:
# PasswordAuthentication no
```

3. Change SSH Port (Optional)

```
# Edit /etc/ssh/sshd_config:
# Port 2222
```

```
sudo systemctl restart sshd
```

4. Firewall Rules

```
# Allow SSH only from specific IPs (optional)
sudo ufw allow from TRUSTED_IP to any port 22
```

Connection Information Template

Create file with connection details:

```
Pi Hostname: GhettoBlaster
Pi Local IP: 192.168.10.2 (example)
Pi User: andre
Pi Password: 0815 (change after first login!)
SSH Port: 22 (or custom port if changed)

Router Public IP: [YOUR_PUBLIC_IP]
Router Port Forward: 2222 -> 192.168.10.2:22 (if configured)

VPN: [VPN details if using]
Dynamic DNS: [Domain if using]
```

Quick Access Commands

From Local Network:

```
ssh andre@192.168.10.2
```

From Remote (Port Forwarding):

```
ssh -p 2222 andre@YOUR_PUBLIC_IP
```

From Remote (VPN):

```
# Connect VPN first, then:
ssh andre@192.168.10.2
```

Troubleshooting

Cannot Connect:

1. Check Pi is online: `ping PI_IP`
2. Check SSH is running: `sudo systemctl status ssh`
3. Check firewall: `sudo ufw status`
4. Check router port forwarding (if using)
5. Check public IP hasn't changed (if using)

Connection Refused:

1. SSH service not running
2. Firewall blocking
3. Wrong port
4. Router blocking (check port forwarding)

Timeout:

1. Router firewall blocking
2. ISP blocking incoming connections
3. Wrong public IP
4. Port forwarding not configured correctly

Next Steps After Setup

1. ■ Test local SSH access
2. ■ Set up remote access method (VPN recommended)
3. ■ Test remote access
4. ■ Share credentials securely with colleague
5. ■ Set up SSH keys (more secure than password)
6. ■ Document connection details

Ready for remote SSH setup. Choose method based on your network setup.