● **Update Todos**
  ⎿ ☒ Connect to stable-dev server and check system information
    ☒ Check SSH configuration and security settings
    ☒ Review firewall configuration and open ports
    ☒ Check user accounts and authentication settings
    ☒ Check for VS Code tunnel specific security
    ☒ Review system updates and patch status
    ☒ Check running services and processes
    ☒ Review file permissions on critical directories

● **Security Audit Summary for stable-dev**

✅ Good Security Practices Found:

1. **SSH Security**:
  - Password authentication disabled
  - Root login restricted (without-password only)
  - Public key authentication enabled
  - Empty passwords not permitted
  - SSH keys have proper permissions (600 for private keys)
2. **User Security**:
  - Only 2 users with shell access (root and ubuntu)
  - Ubuntu user password is locked (L status)
  - Ubuntu user has sudo privileges
3. **File Permissions**:
  - SSH host keys properly secured (600 permissions)
  - .ssh directory and authorized_keys have correct permissions
4. **Services**:
  - Minimal services running
  - VS Code tunnel service is active and running
  - Unattended upgrades enabled for automatic security updates

⚠️ Security Concerns:

1. **Firewall is DISABLED** - This is the biggest security risk. UFW is inactive, leaving all ports unfiltered.
2. **Only SSH port (22) is exposed** to the network, which is good, but without a firewall, any service could potentially be exposed.
3. **One package needs updating** (linux-tools-common) - though it's minor.

🔒 Recommendations (without making changes):

1. **Enable UFW firewall** with rules allowing only SSH (port 22)
2. **Consider fail2ban** for SSH brute force protection

3. **Run the pending system update**
4. **Monitor VS Code tunnel access** - ensure you're using strong authentication for the tunnel itself

The server has decent baseline security for SSH access, but the disabled firewall is a significant vulnerability that should be addressed.

> This server is running in AWS. Do I still need a firewall? Is it better to use AWS security or both?

● **AWS Security Groups vs Host Firewall**

You're right to question this! Since your server is in AWS, you have **AWS Security Groups** acting as a virtual firewall at the network level. Let me check your current AWS security setup:

```
● Bash(ssh stable-dev "curl -s http://169.254.169.254/latest/meta-data/instance-id && echo && curl -s http://169.254.169.254/latest/meta-data/security-groups")
  ⎿  i-0f81cacccda0b5874
     ssh-only-sg-202507161615
     Warning: Permanently added '54.194.215.48' (ED25519) to the list of known hosts.
```

● Your instance is using a security group called ssh-only-sg-202507161615, which sounds properly restrictive.

Best Practice: **Use BOTH (Defense in Depth)**

Here's why:

1. **AWS Security Groups** (Network-level):
   - First line of defense
   - Blocks traffic before it reaches your server
   - Stateful (return traffic automatically allowed)
   - Can't protect against threats from within the VPC
   - If misconfigured, your server is exposed
2. **Host Firewall (UFW)** (Host-level):
   - Second line of defense
   - Protects against lateral movement if another instance in your VPC is compromised
   - Protects if Security Group is accidentally misconfigured
   - Can implement more granular rules (rate limiting, etc.)
   - Useful for localhost restrictions

For your VS Code tunnel setup:

Since you're only exposing SSH and VS Code tunnels work through SSH, you're in good shape. AWS Security Groups alone are probably sufficient for your use case, but enabling UFW adds minimal overhead and provides extra protection.

Minimum recommendation: Stick with AWS Security Groups if they're properly configured to only allow SSH (port 22) from your IP addresses.

Better recommendation: Enable both for defense-in-depth, especially if this server will contain sensitive code or data.

> You can run aws commands to check. This session is enabled for aws

● Great! Let me check your AWS security configuration directly.

```
● Bash(aws ec2 describe-instances --instance-ids i-0f81cacccda0b5874 --query
'Reservations[0].Instances[0].
[InstanceId,PublicIpAddress,PrivateIpAddress,SecurityGroups,…)
  ⎿ [
      "i-0f81cacccda0b5874",
      "54.194.215.48",
    … +10 lines (ctrl+r to expand)
```

● Now let me check the security group rules:

```
● Bash(aws ec2 describe-security-groups --group-ids sg-00f85cd91b3817407 --
query 'SecurityGroups[0].
[GroupName,Description,IpPermissions,IpPermissionsEgress]' --output…)
  ⎿ [
      "ssh-only-sg-202507161615",
      "SSH access only from specific IP",
    … +29 lines (ctrl+r to expand)
```

● Let me also check if there are any Network ACLs that might affect traffic:

```
● Bash(aws ec2 describe-network-acls --filters "Name=association.subnet-
id,Values=subnet-0fd11f0c5d83cb189" --query 'NetworkAcls[0].
[NetworkAclId,IsDefault,Entries[?Ru…)
  ⎿ [
      "acl-0e1391689ac12cded",
      true,
```

… +17 lines (ctrl+r to expand)

● **AWS Security Analysis**

✅ Current AWS Security Setup:

1. **Security Group** (ssh-only-sg-202507161615):
   - **Inbound**: Only SSH (port 22) from 200.5.49.46/32 (single IP)
   - **Outbound**: All traffic allowed (standard for updates/packages)
   - This is excellent - very restrictive!
2. **Network ACLs**: Using default ACLs (allow all) - this is normal
3. **Public IP**: Your instance has a public IP (54.194.215.48)

🎯 Assessment:

Your AWS security is **well-configured**. The security group is doing exactly what a host firewall would do - only allowing SSH from a specific IP address.

Recommendation:

For your use case (VS Code tunnel for remote development), **AWS Security Groups alone are sufficient** because:

1. ✅ Only SSH is allowed inbound
2. ✅ Restricted to a single source IP
3. ✅ VS Code tunnels work through SSH
4. ✅ No other services need external access

Optional additions for extra security:
- Enable UFW as backup (defense in depth)
- Consider AWS Systems Manager Session Manager for SSH access (eliminates need for public IP)
- Add CloudWatch monitoring for SSH login attempts

Your current setup is secure for its purpose. The main thing to watch: if your IP address changes (ISP change, travel, etc.), you'll need to update the security group rule.