PHASE 9: VPN Access & Secure RDP Jump Box (DipeshCorp Lab)

This phase focuses on securely accessing internal infrastructure—like AD DS, Intune, File Server, or Jamf—from outside the corporate network using a VPN tunnel and a hardened Windows Server Jump Box. This simulates real-world IT admin practices used in enterprise settings.

We will:

- Deploy a Windows Server 2022 Jump Box
- Set up WireGuard VPN for secure encrypted access
- Lock down RDP access with GPO and optionally with MFA

🧰 Tools and VM Requirements

- Windows Server 2022 VM (used as the Jump Box)
- Optional: Second Windows Server or Ubuntu VM for WireGuard VPN
- WireGuard (https://www.wireguard.com/)
- Remote Desktop (RDP)
- Optional: Duo MFA (Free up to 10 users) or Entra Conditional Access
- Optional: Cloudflare Tunnel for public IP-free exposure

I. Build and Configure the Jump Box VM

Actions Completed:

1. Installed Windows Server 2022 Standard Edition
2. Renamed PC to: `jumpbox.dipeshcorp.local`

3. Set static IP or DHCP with static DNS:
    - Open Network Connections (ncpa.cpl)
    - Right-click Ethernet > Properties
    - Select Internet Protocol Version 4 (TCP/IPv4)
    - Set DNS to: Preferred DNS: “Same as Domain IP”
        - Verify DNS: Open PowerShell:
            i. `nslookup nxhz.local`
            ii. `ping dc01.nxhz.local`

    ✅ You should get a valid domain controller reply. If not, check DNS config.

3. Join the domain:
    - Right-click Start → System → Rename this PC (`jumpbox.dipeshcorp.local`)
    - Click Change → Domain → nxhz.local
    - Enter domain credentials: e.g., nxhz\Administrator

4. Joined the domain `dipeshcorp.local`

- Logged in as local admin
- System > Change Settings > Domain Join → `dipeshcorp.local`
- Rebooted
- Logged in as `dipesh.admin@dipeshcorp.local`

🛑 Error: To sign in remotely, you need the right to sign in through Remote Desktop Services

🛑 Then: Session access denied

✔️ Resolution:

1. Log in with a local admin (e.g., local account dipeshadmin)
2. Add domain user to Remote Desktop Users: Open PowerShell:

```
net localgroup "Remote Desktop Users" nxhz\dipesh.admin /add
```

3. Also grant local admin (for Docker):

```
net localgroup Administrators nxhz\dipesh.admin /add
```

4. Open Group Policy Editor (locally or from Domain Controller)

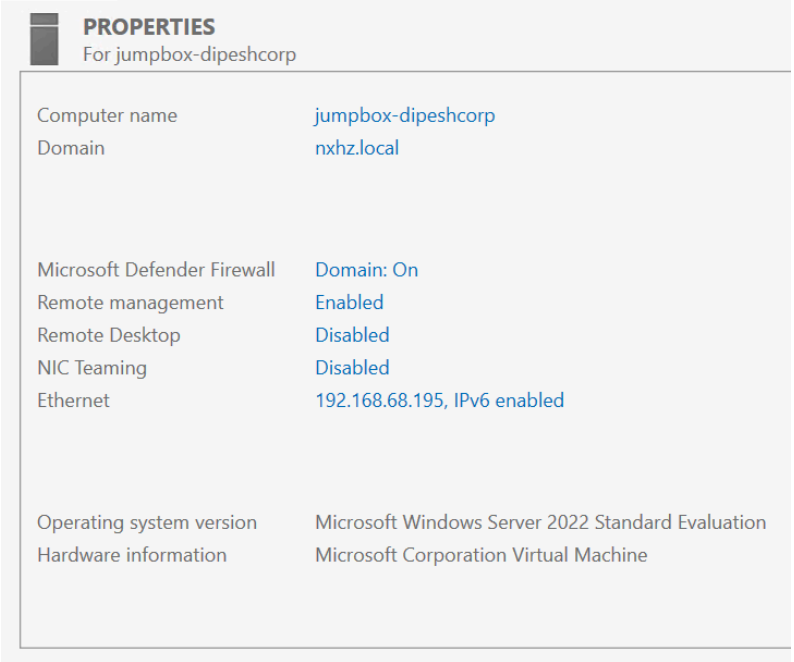
   - Run: gpedit.msc (or GPMC on DC)
   - Navigate: Computer Configuration → Windows Settings → Security Settings → Local Policies → User Rights Assignment
   - Double-click:

   ✅ Allow log on through Remote Desktop Services → Add: nxhz\dipeshadmin OR Remote Desktop Users

   ❌ Deny log on through Remote Desktop Services → Make sure nxhz\dipeshadmin is NOT listed

5. Run: `gpupdate /force`
6. Reboot the VM and test RDP with the domain account.

✅ Result: nxhz\dipesh.admin now has full RDP and admin rights.

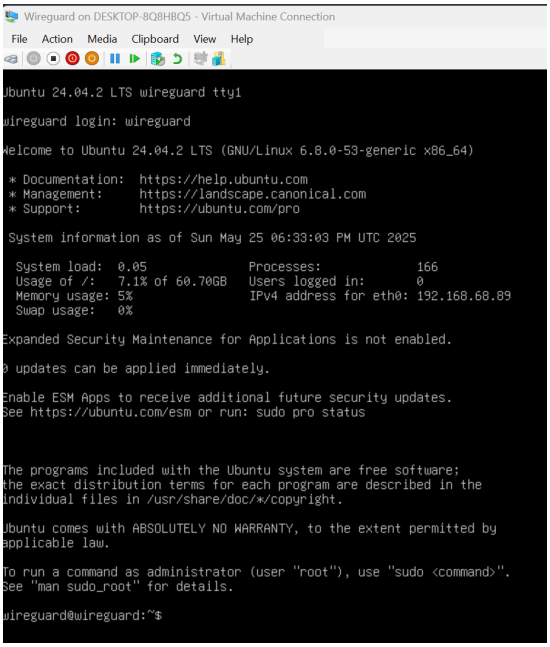


II. Set Up WireGuard VPN for Secure Access

WireGuard is a lightweight, fast, and open-source VPN. We installed it on a dedicated Ubuntu Server VM (VPN-Server).

Actions Completed:

1. Created a new VM: `VPN-Server` with Ubuntu 24.04 LTS
    - Deploy a VM running Ubuntu 24.04 LTS and prepare for secure boot under Microsoft UEFI.
    - Hyper-V or VirtualBox → Create new VM
        - OS: Ubuntu Server 24.04 LTS
        - RAM: 4 GB, CPU: 2 cores, Disk: 127 GB
        - In VM settings:
        - Go to: Security > Enable Secure Boot
        - Select: Microsoft UEFI Certificate Authority (not default template)

    📌 Install Ubuntu Server normally.

    - Follow guided install steps
    - Set hostname (e.g., wireguard)
    - Choose static or DHCP IP
    - At software selection screen → Select: Docker (optional) or none (we'll install Apache manually)

2. Installed WireGuard:

    `sudo apt update && sudo apt install wireguard -y`

3. Generated server keys:

    `umask 077`

    `wg genkey | tee server_private.key | wg pubkey > server_public.key`

⚠️ Note: These are real keys — no need to replace `<server_private_key>` manually. WireGuard outputs the key, and you copy it into your config file.

4. Configured WireGuard server config: Run sudo nano `/etc/wireguard/wg0.conf`:

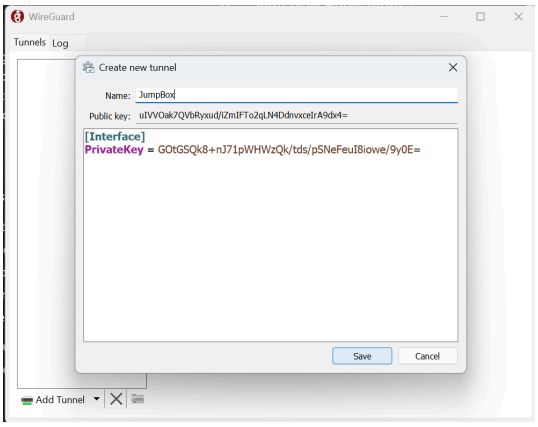
```
[Interface]
PrivateKey = <Type : server_private_key>
Address = 10.13.13.1/24
ListenPort = 51820

[Peer]
PublicKey = <Type: client_public_key>
AllowedIPs = 10.13.13.2/32
```

5. Started the VPN:

```
sudo systemctl enable wg-quick@wg0
sudo systemctl start wg-quick@wg0
```

6. On your Windows 10/11 Pro laptop:
   a. Download and install WireGuard for Windows from https://www.wireguard.com/install/
   b. Open WireGuard → Click "Add Tunnel" → "Add empty tunnel"
   c. Click "Generate key pair" → This automatically fills in the private/public key fields
   d. Save the private key and public key somewhere safe
   e. PrivateKey = GOtGSQk8+nJ71pWHWzQk/tds/pSNeFeuI8iowe/9y0E=
   f. Publick Key = uIVVOak7QVbRyxud/iZmIFTo2qLN4DdnvxceIrA9dx4=



7. Configure the client tunnel: Click "Edit" and enter the following:

```
[Interface]
PrivateKey = <client private key>
```

```
Address = 10.13.13.2/24


[Peer]
PublicKey = <server public key>
Endpoint = <VPN-Server Public IP>:51820
AllowedIPs = 10.0.0.0/8, 192.168.0.0/16
PersistentKeepalive = 25
```

8. Save and activate the tunnel
   a. You'll see the status switch to "Active"
   b. Open Command Prompt → Run: `ping 192.168.1.100` → You should receive replies from the Jump Box

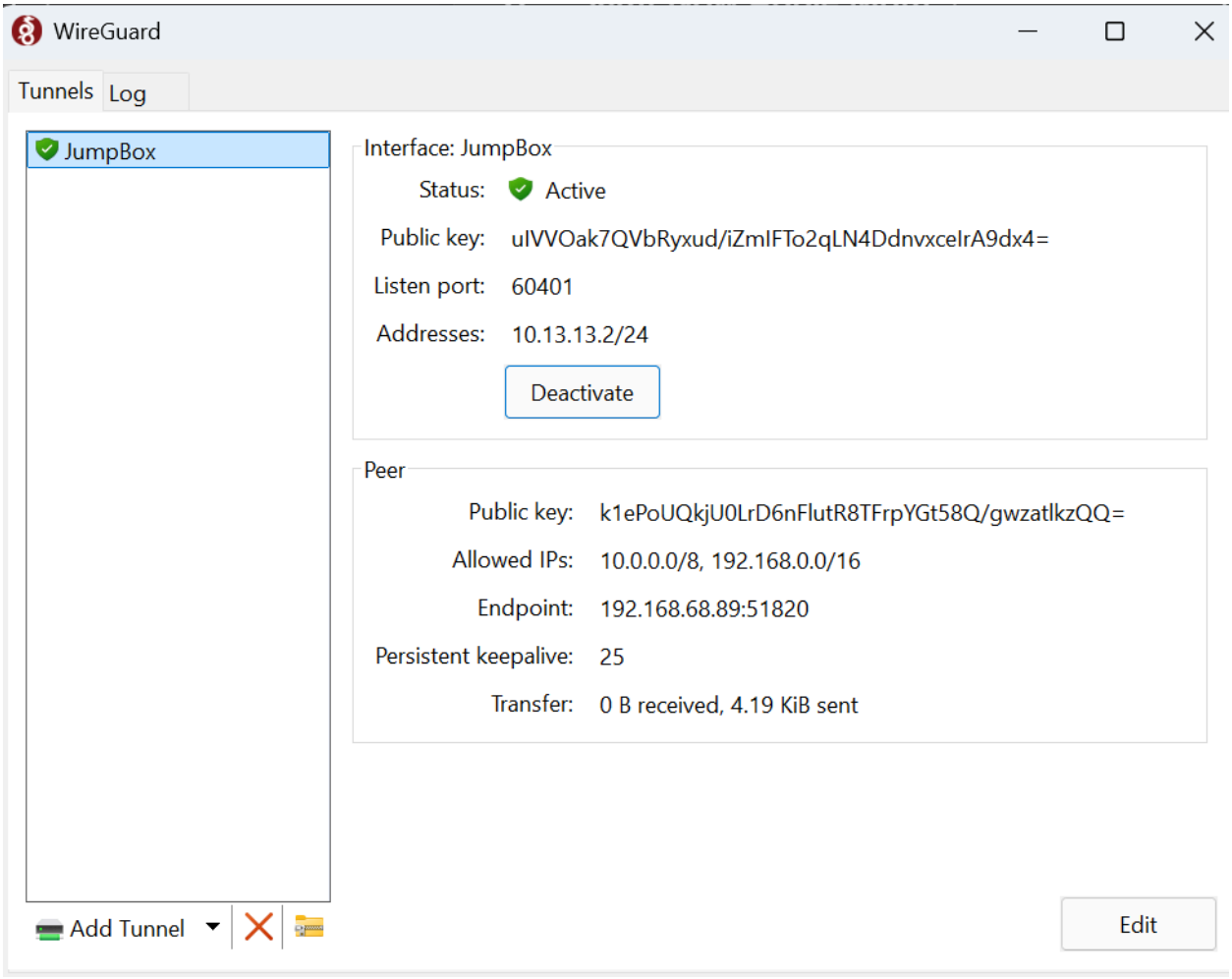
⚠️ Notes:

- Do not include quotes in the keys
- Always match key pairs correctly: client public key goes to server peer; server public key goes to client peer

🔧 Troubleshooting:

- ❌ No response from ping:
  - Check firewall on VPN server and Jump Box
  - Ensure you added `AllowedIPs = 10.13.13.2/32` in the server config
  - Ensure both tunnels are active (client & server)
- ❌ DNS not resolving:
  - Add internal DNS (e.g., 192.168.1.10) to client config: `DNS = 192.168.1.10`
    - If port 51820 blocked: Check firewall (UFW or Windows Defender)
    - If no DNS resolution: Add internal DNS to WireGuard config
    - If "Cannot access RDP" → Ensure Jump Box allows incoming from 10.13.13.0/24

✅ At this stage, you have securely connected from your local laptop to your internal AD network over WireGuard VPN.



III. Lock Down the Jump Box with Group Policy

Actions Completed:

1. On DC01, open Group Policy Management
2. Create a new OU named `JumpBoxes`
3. Move `jumpbox.dipeshcorp.local` to the `JumpBoxes` OU
4. Right-click the OU → Create GPO named `JumpBox Lockdown`

5. Edit the GPO and configure the following:

Security Hardening Policies:

- Disable Command Prompt:
  - User Configuration → Admin Templates → System → Prevent access to the command prompt → Enabled
- Disable PowerShell:
  - User Configuration → Admin Templates → System → Don't run specified Windows applications → Add `powershell.exe`
- Disable USB ports:
  - Computer Configuration → Admin Templates → System → Device Installation → Prevent installation of removable devices → Enabled
- Disable Control Panel:
  - User Configuration → Admin Templates → Control Panel → Prohibit access to Control Panel and PC settings → Enabled
- Disable Edge and Internet Explorer:
  - User Configuration → Admin Templates → Windows Components → Internet Explorer → Prevent access → Enabled
- Enable auto screen lock:
  - User Configuration → Admin Templates → Control Panel → Personalization → Screen saver timeout: 300 seconds
  - Enable screen saver and require password on resume
- Set legal login banner:
  - Computer Configuration → Windows Settings → Security Settings → Local Policies → Security Options →
    - Interactive logon: Message text for users attempting to log on
    - Interactive logon: Message title → "DipeshCorp Authorized Access Only"

6. Run `gpupdate /force` on the Jump Box

7. Test with a non-admin user to verify all restrictions apply

---

IV. Mail Flow Rules (Transport Rules)

Define organization-wide email governance policies using conditional mail rules.

Actions Completed:

Use Case 1: Block Executable Attachments

1. EAC → Mail Flow > Rules > Add a rule
2. Rule Name: Block EXE Attachments
3. Apply this rule if:
   - Any attachment | file extension includes these words > “exe”
4. Do the following:
   - Block the message | Reject the message with explanation: “Executable attachments are not allowed.”

Use Case 2: External Email Disclaimer

1. Rule Name: External Email Disclaimer
2. Apply this rule if:
   - The Sender | is external/internal > “Outside the organization”
3. Do the following:
   - Apply a disclaimer to the message | Append a disclaimer > Select text: “This is an external email. Please exercise caution.”

Validation:

1. Attempted sending .exe attachment → Rejection confirmed

2. Sent email from external Gmail account → Disclaimer appended in received email

---

V. Add MFA to RDP

You can add Multi-Factor Authentication (MFA) to your RDP logins for additional security using either Microsoft Entra ID (Azure AD)

Entra ID Conditional Access (If using Entra Hybrid Join)

Actions Completed:

1. Go to: https://entra.microsoft.com → Protection → Conditional Access
2. Create new policy: “Require MFA for RDP Access”
3. Assign to: IT Admins, JumpBox, or test users
4. Cloud apps: Select "Microsoft Remote Desktop"
5. Grant Controls → Require MFA → Save and Enable policy
6. Tries logging into Jump Box from RDP client. MFA prompt was appear.

⚠️ Note: This requires Entra Join or Hybrid Join and Azure AD RDP integration