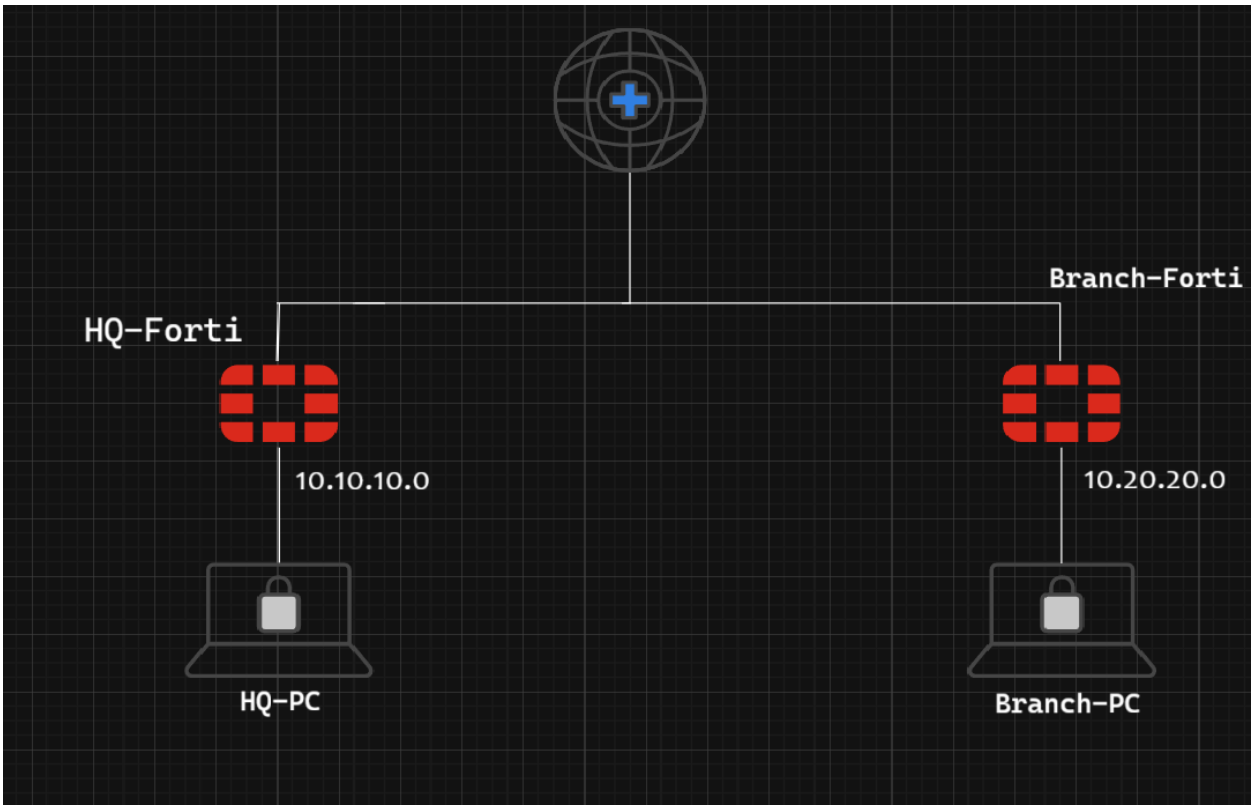
Week 2 – IPsec VPN Configuration Documentation

1. Objective

The main objective of this task is to establish a secure IPsec VPN tunnel between two FortiGate devices to ensure encrypted communication between two remote networks over the internet.

---

2. Network Topology



Description:

- Two FortiGate firewalls were used to connect two different LAN networks through the internet using an IPsec VPN tunnel.
- Each FortiGate represents a branch office / Headquarter office.

Example Topology:

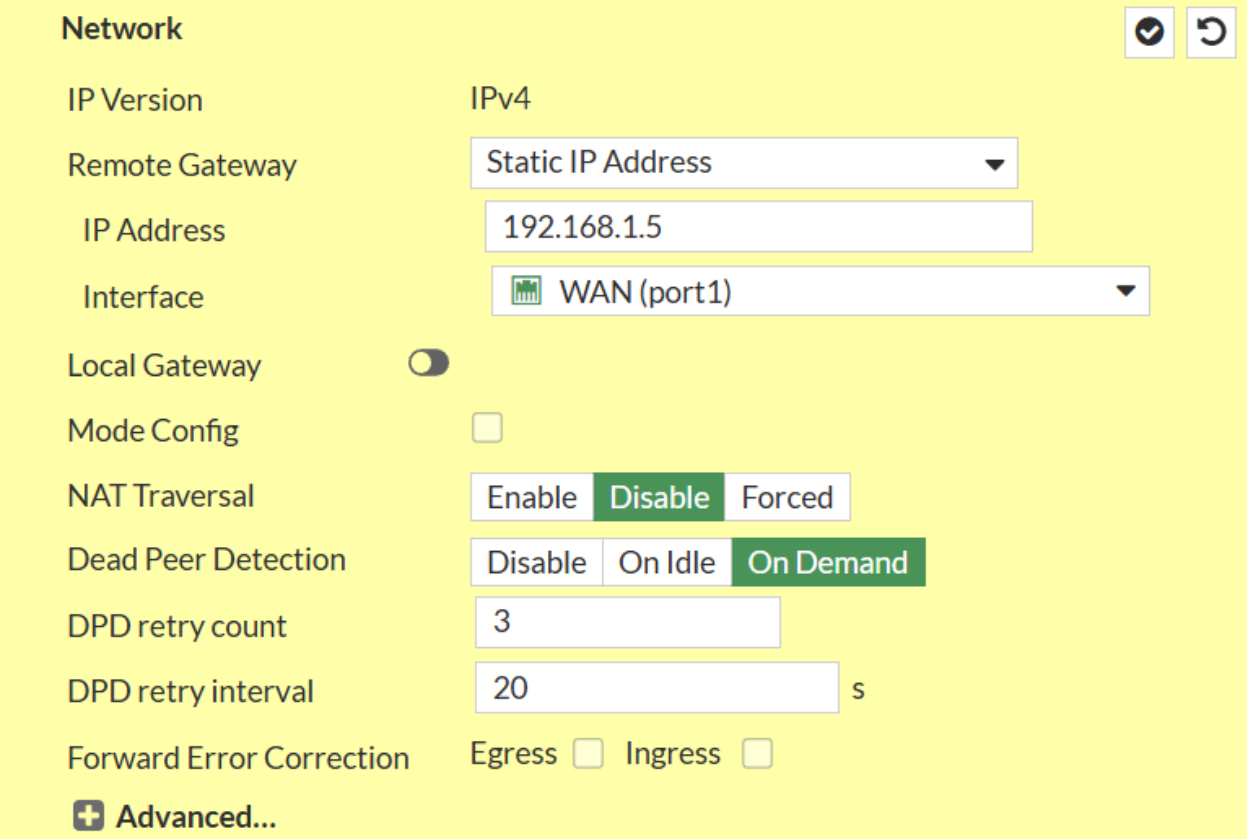
Site A LAN (10.10.10.0/24) --- FortiGate A ---- Internet ---- FortiGate B ---- Site B LAN (10.20.20.0/24)

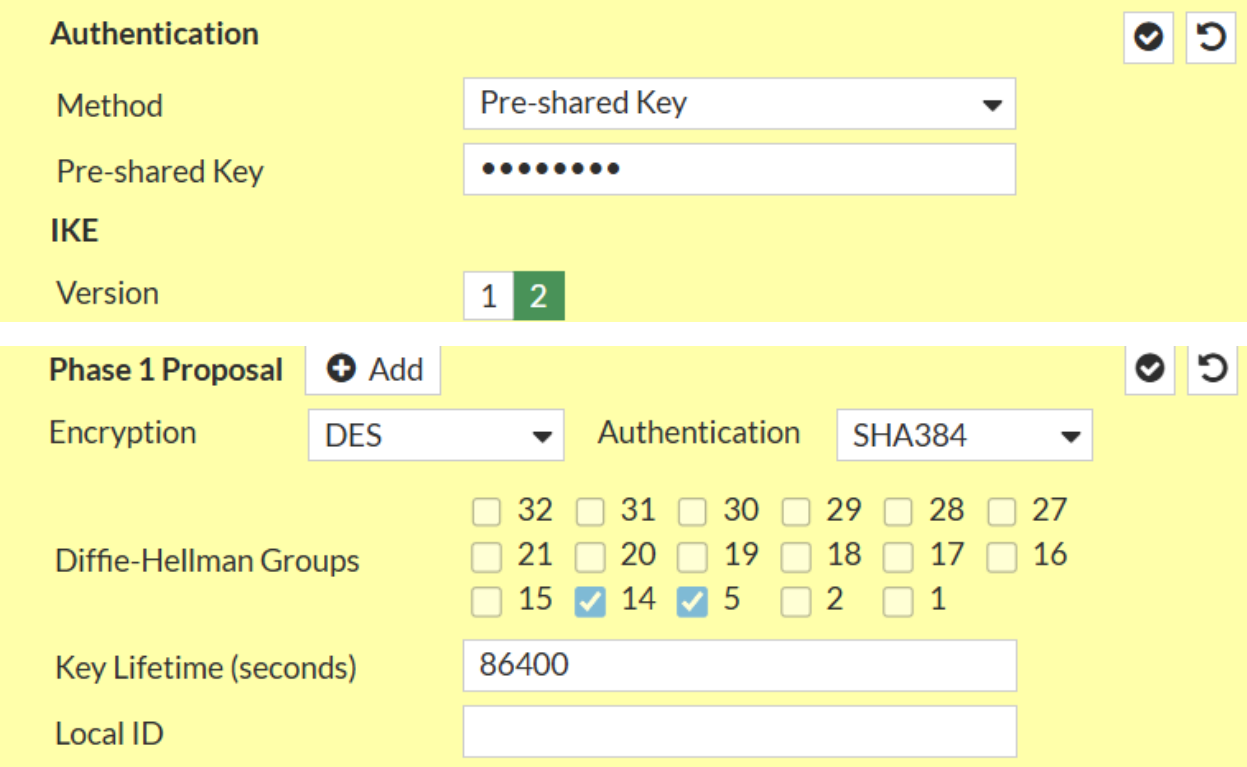
---

3. IPsec VPN Configuration Steps (HQ – Configuration)

Step 1: Phase 1 Configuration

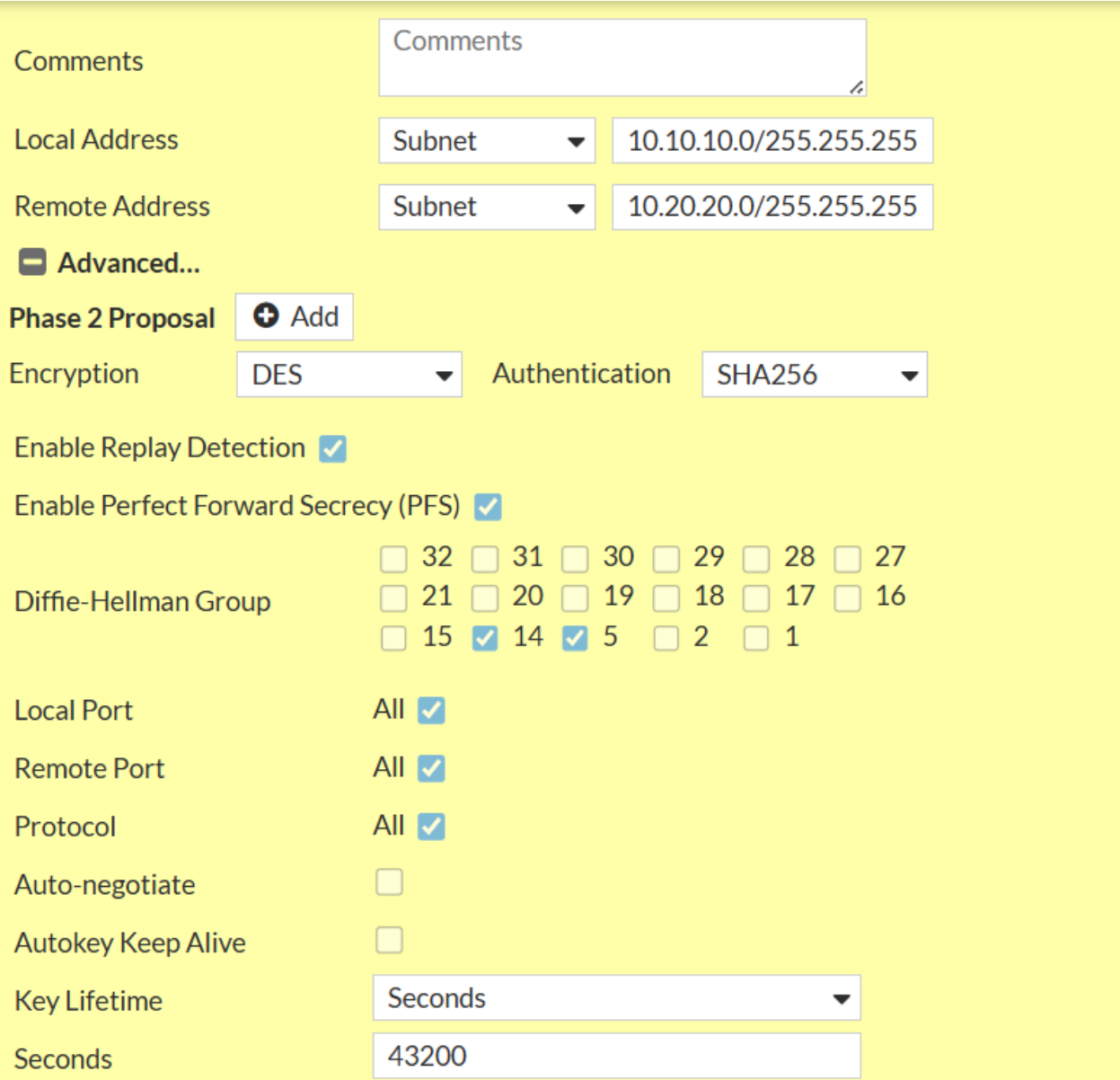
- Go to **VPN → IPsec Tunnels → Create New → Custom**.
- **Name:** HQ-to-Branch
- **Remote Gateway:** Static IP Address (192.168.1.5) **) *(HQ WAN IP)***
- **Interface:** WAN (port1)
- **Authentication Method:** Pre-shared Key
- **IKE Version:** IKEv2
- **Encryption:** DES
- **Authentication:** SHA384
- **DH Group:** 14,5
- **Key Lifetime:** 86400





Step 2: Phase 2 Configuration

- **Local Subnet:** 10.10.10.0/255.255.255.0
- **Remote Subnet:** 10.20.20.0/255.255.255.0
- **Encryption:** DES
- **Authentication:** SHA256
- **Enable Replay Detection**



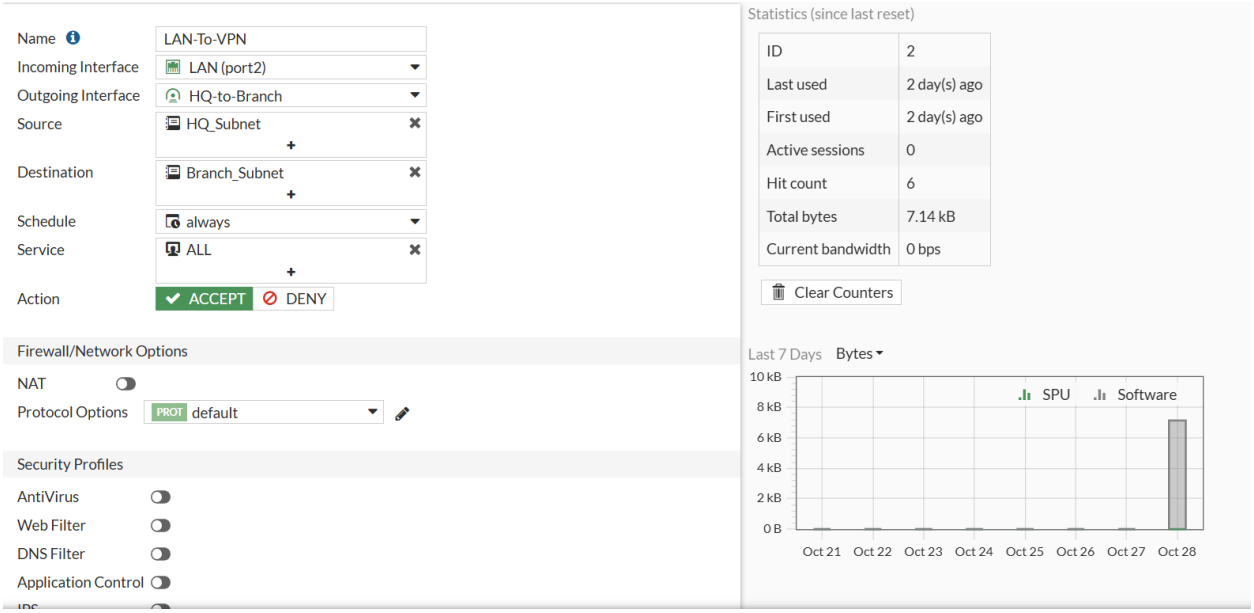
Step 3: Firewall Policies

- Create policies to allow traffic from LAN → VPN and VPN → LAN on both FortiGates.

1- LAN-To-VPN

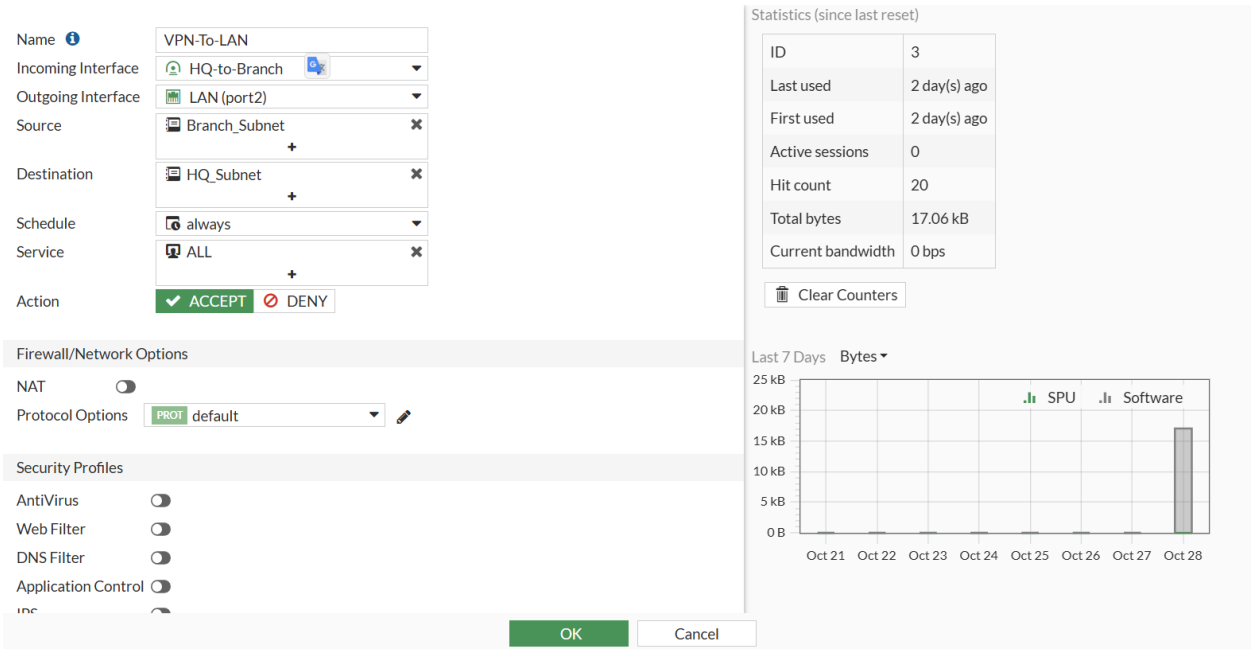
- **Incoming Interface:** LAN (port2)
- **Outgoing Interface:** HQ-to-Branch
- **Action:** Accept
- **NAT:** Disabled

- **Source :** HQ Subnet (10.10.10.0/24)
- **Destination :** HQ Subnet (10.20.20.0/24)



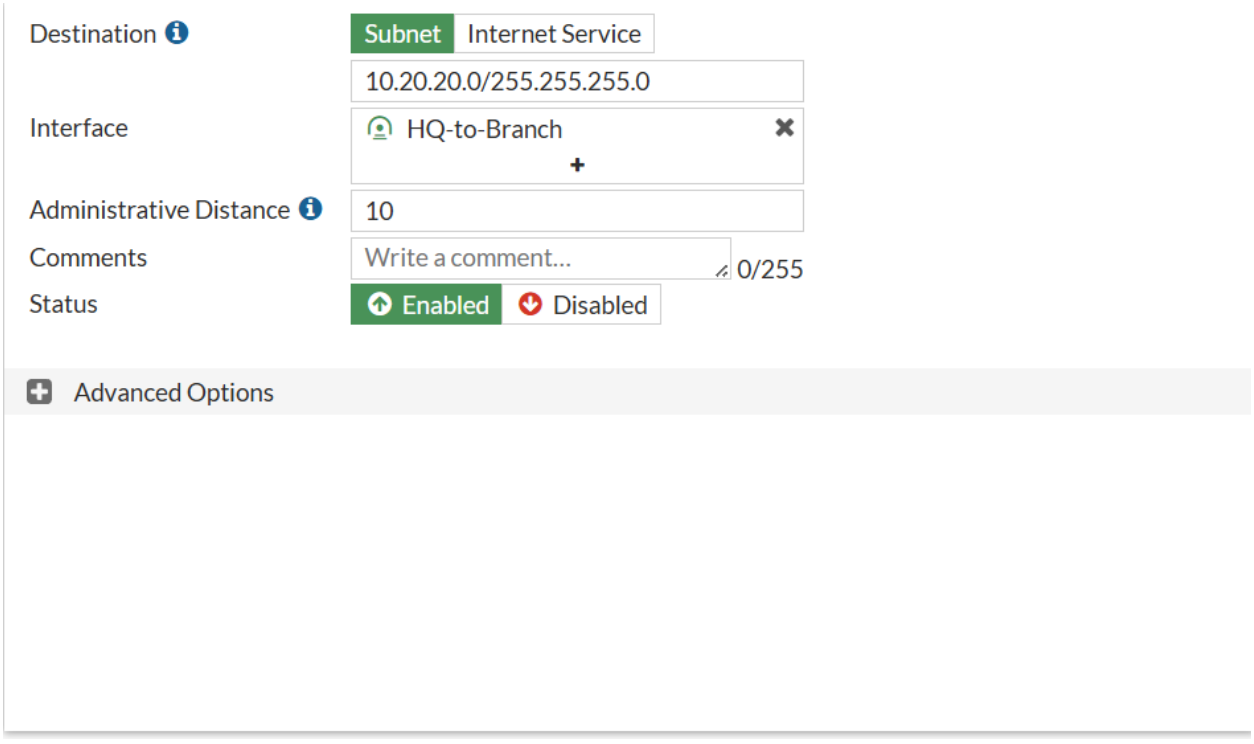
2- VPN-to-LAN

- **Incoming Interface:** HQ-to-Branch
- **Outgoing Interface:** LAN (port2)
- **Action:** Accept
- **NAT:** Disabled
- **Source :** Branch Subnet (10.20.20.0/24)
- **Destination :** HQ Subnet (10.10.10.0/24)



Step 4: Static Routes

- Add static routes to reach the remote subnet through the VPN tunnel.\
- Destination : Subnet (10.20.20.0 / 255.255.255.0)
- Interface : HQ-to-Branch

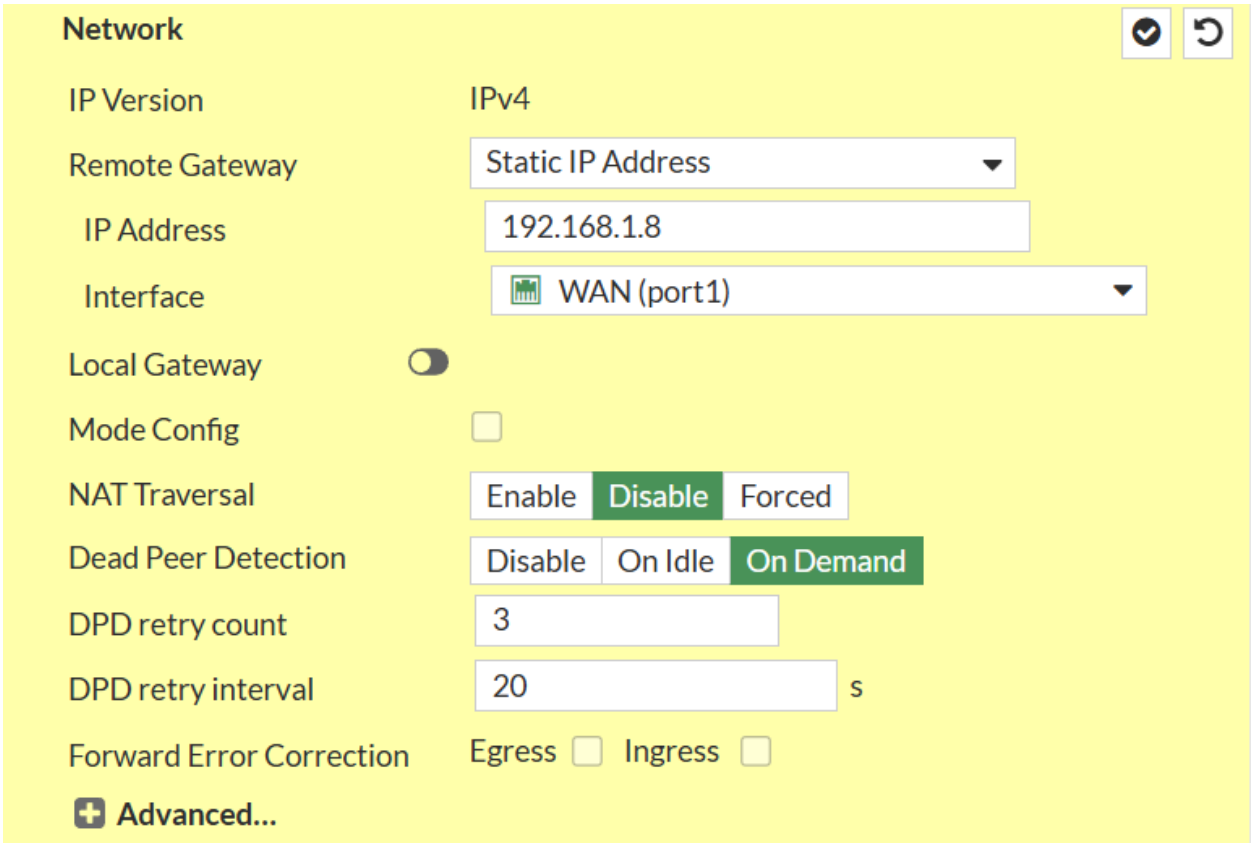


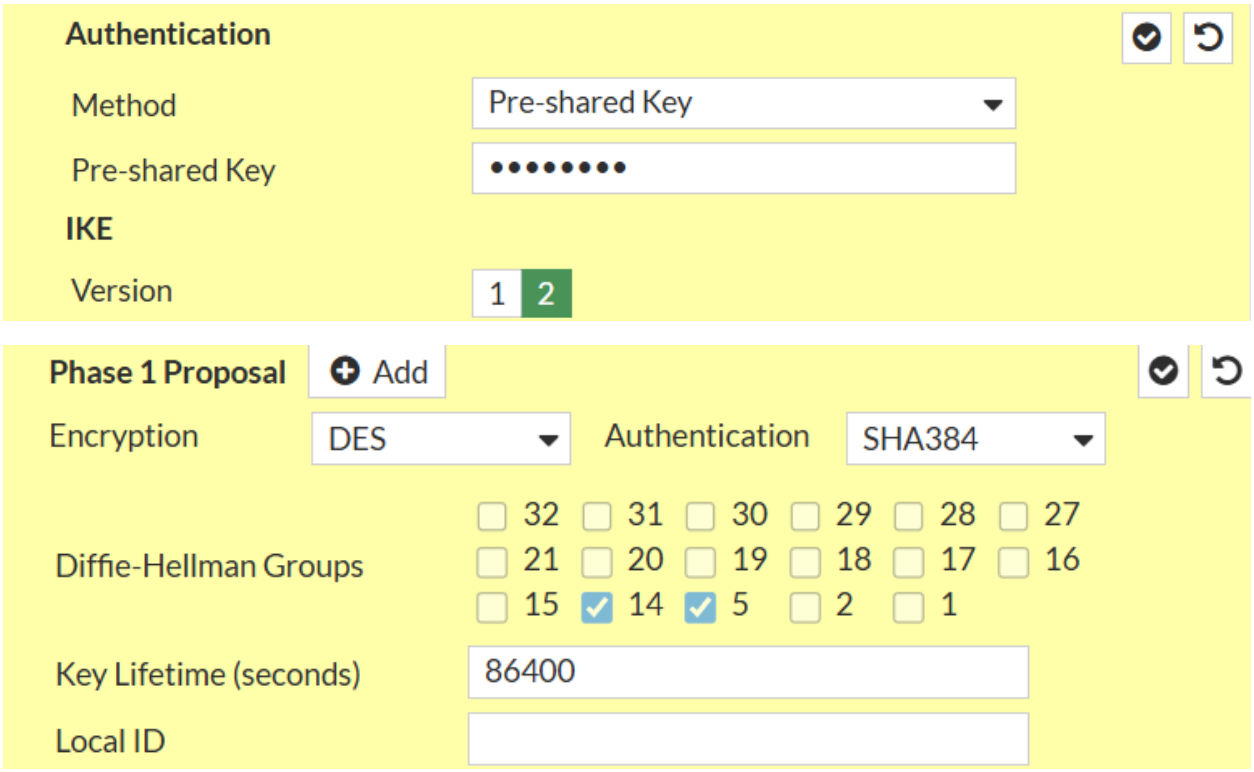
---

4. Branch FortiGate Configuration

Step 1: Phase 1 Configuration

- **Go to VPN → IPsec Tunnels → Create New → Custom.**
- **Name: Branch-to-HQ**
- **Remote Gateway: Static IP Address (192.168.1.8) *(HQ WAN IP)***
- **Interface: WAN (port1)**
- **Authentication Method: Pre-shared Key**
- **IKE Version: IKEv2**
- **Encryption: DES**
- **Authentication: SHA384**
- **DH Group: 14,5**
- **Key Lifetime: 86400**



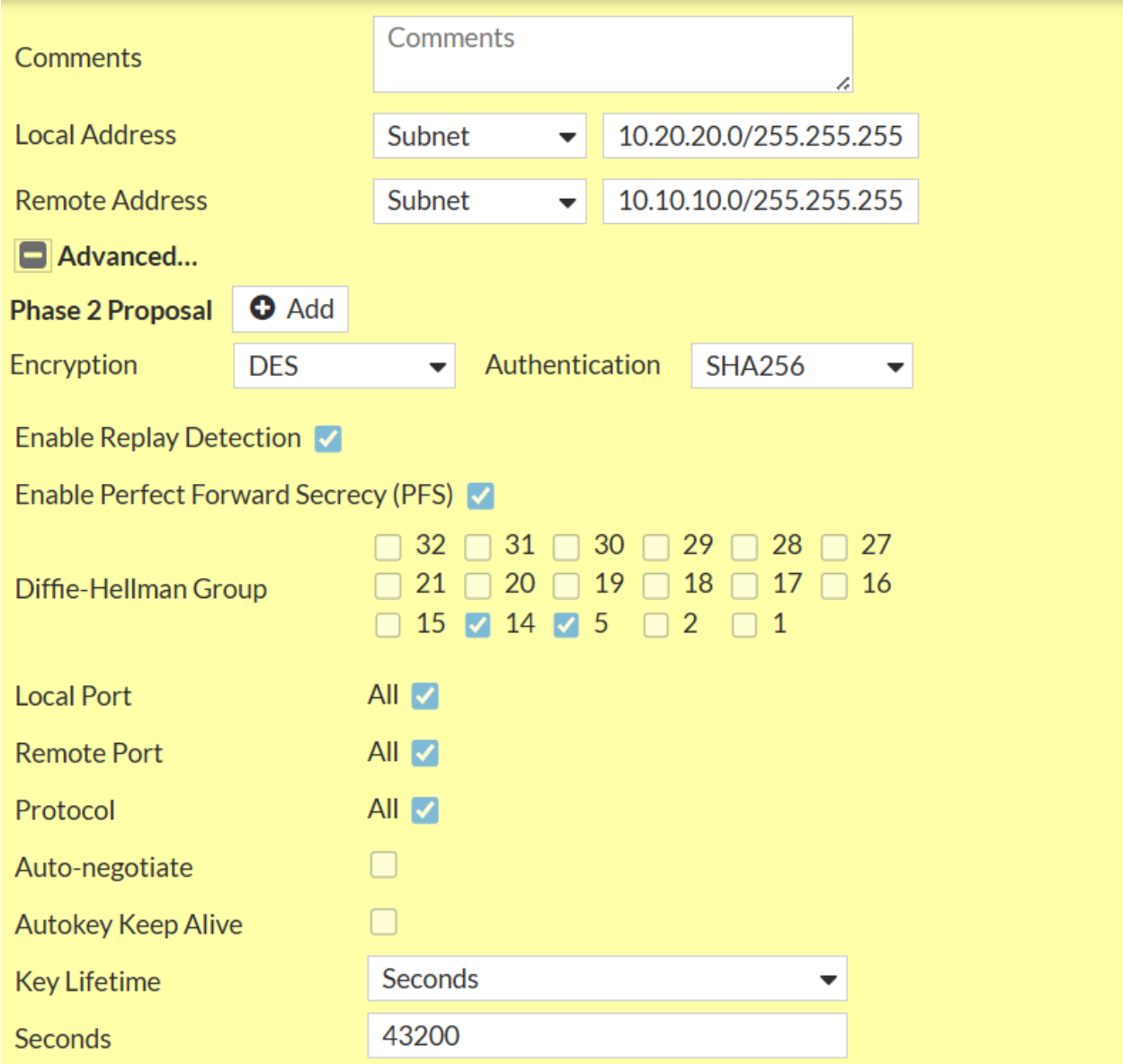


Note:
Make sure the Pre-shared Key matches exactly with the one configured on HQ.

Step 2: Phase 2 Configuration

- **Local Subnet: 10.20.20.0 / 255.255.255.0**
- **Remote Subnet: 10.10.10.0 / 255.255.255.0**
- **Encryption: DES**
- **Authentication: SHA256**

- **Enable Replay Detection: Enabled**

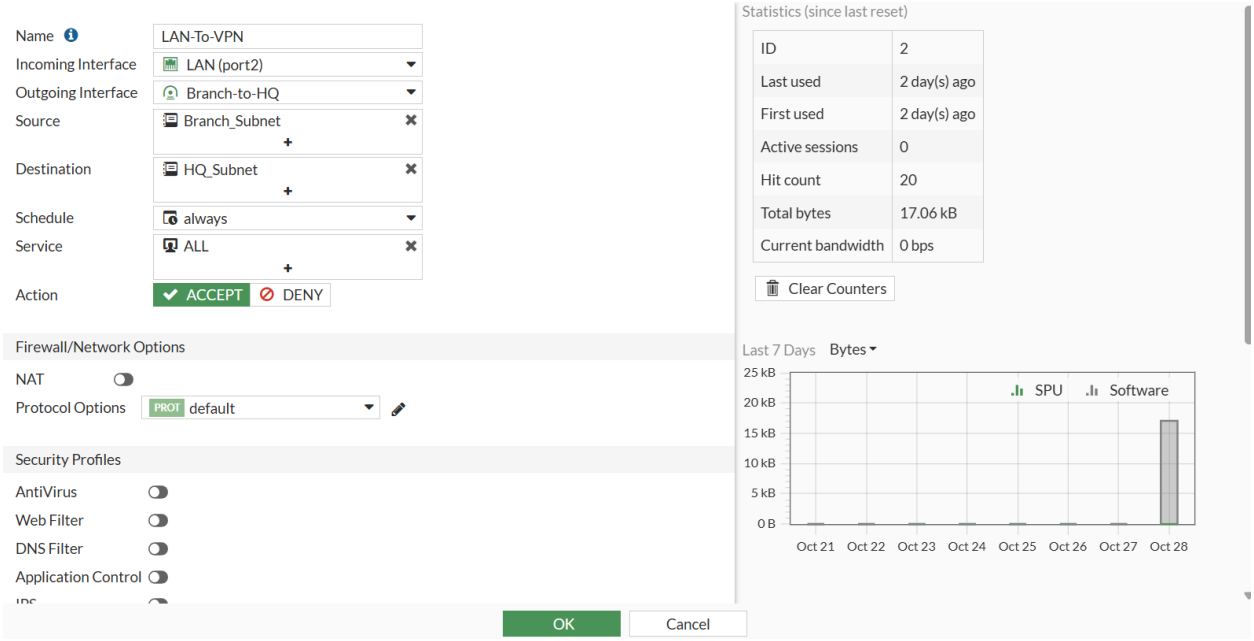


Step 3: Firewall Policies

1- LAN-To-VPN

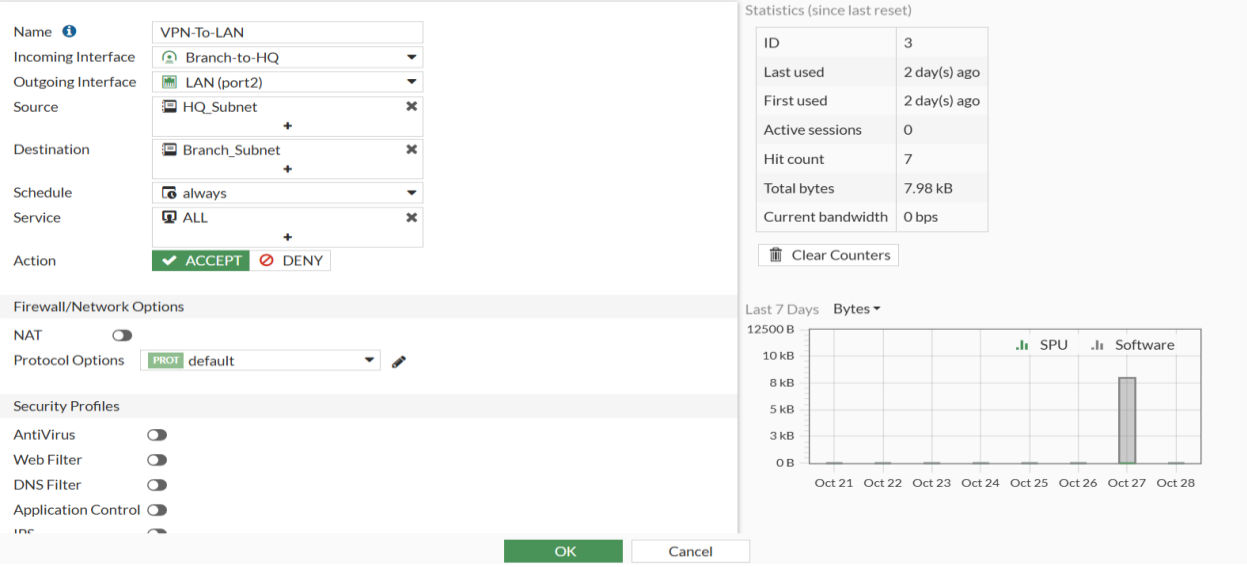
- **Incoming Interface: LAN (port2)**
- **Outgoing Interface: Branch-to-HQ**
- **Action: Accept**
- **NAT: Disabled**

- **Source: Branch Subnet (10.20.20.0/24)**
- **Destination: HQ Subnet (10.10.10.0/24)**



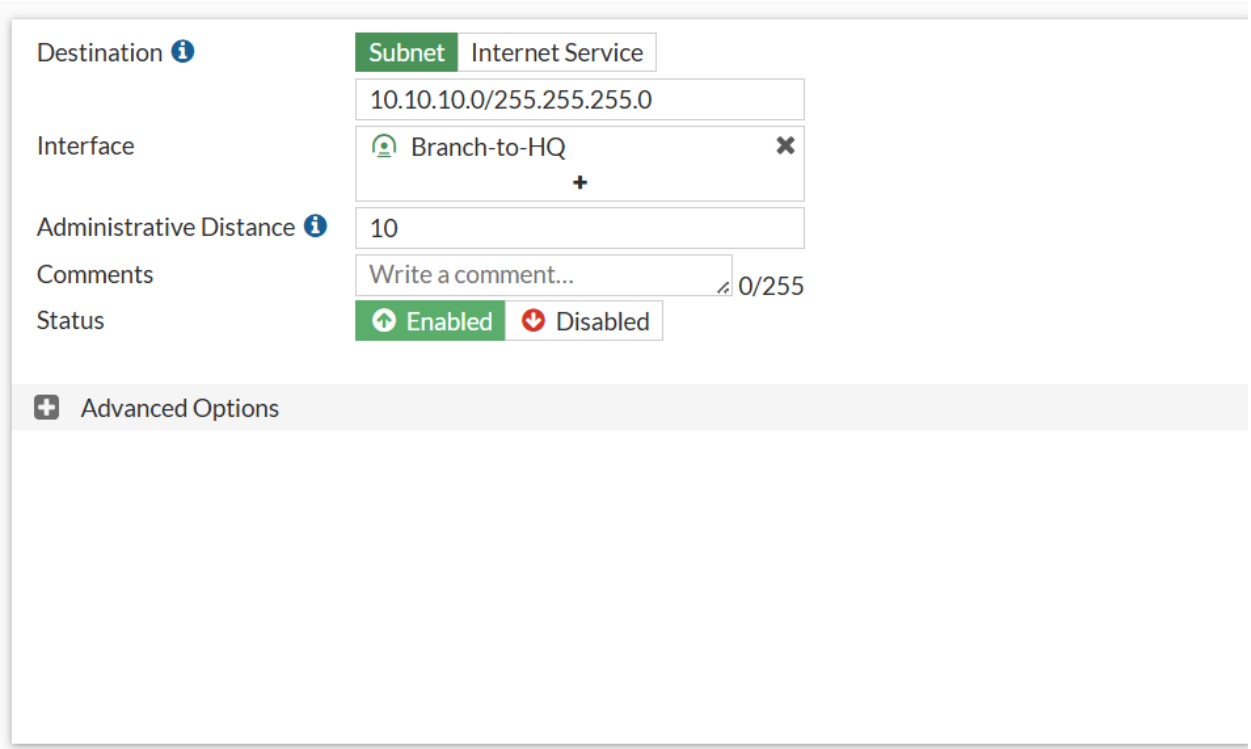
2- VPN-To-LAN

- **Incoming Interface: Branch-to-HQ**
- **Outgoing Interface: LAN (port2)**
- **Action: Accept**
- **NAT: Disabled**
- **Source: HQ Subnet (10.10.10.0/24)**
- **Destination: Branch Subnet (10.20.20.0/24)**



Step 4: Static Routes

- **Destination: 10.10.10.0 / 255.255.255.0**
- **Interface: Branch-to-HQ**

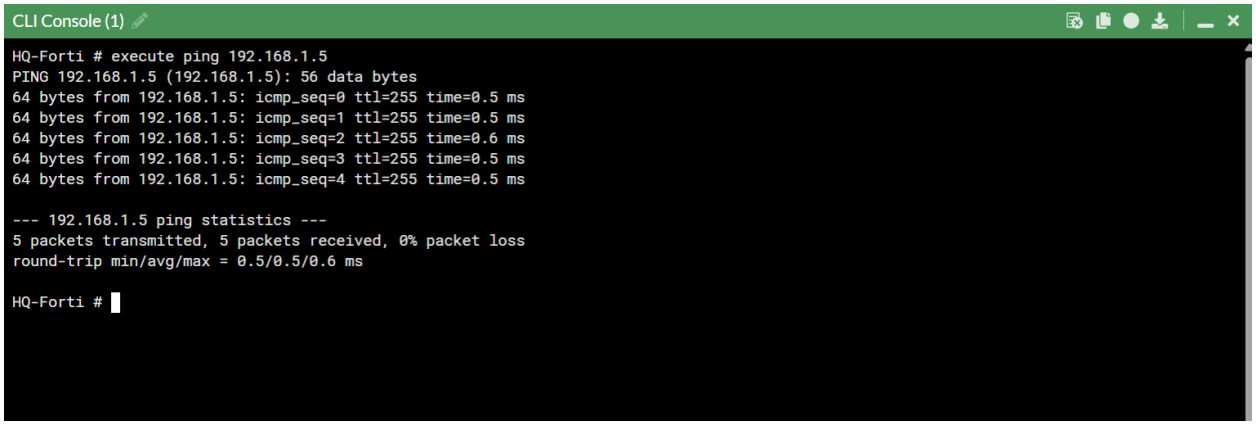


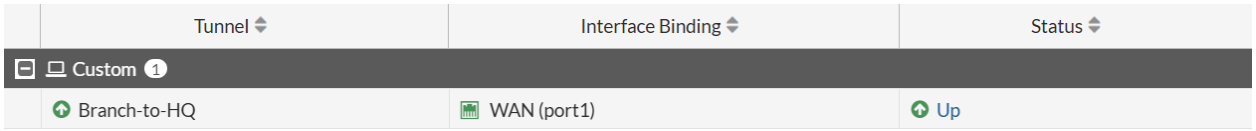
5. Connectivity Test Results

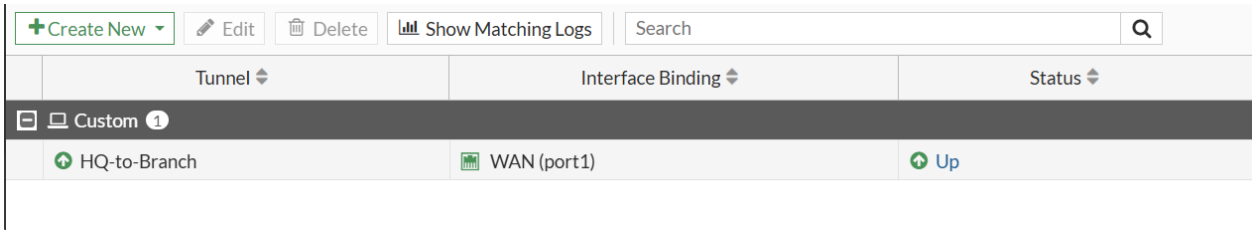
Test 1: Ping Test Between Branches

- **From: HQ Forti 192.168.1.8**
- **To: Branch Forti 192.168.1.5**

✅ **Result: Successful ping replies received, indicating that both LAN networks are reachable through the IPsec VPN tunnel.**



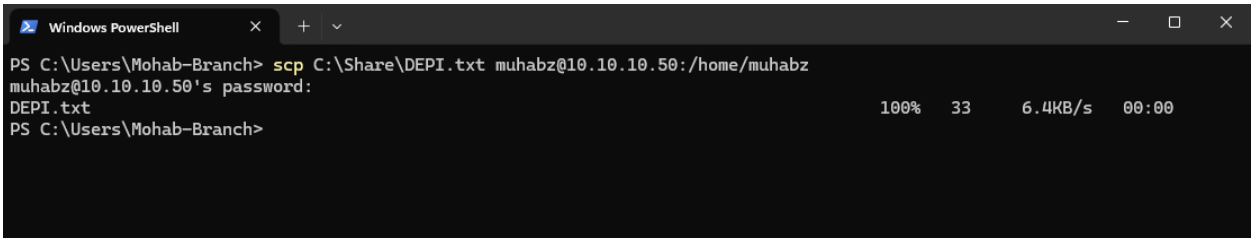


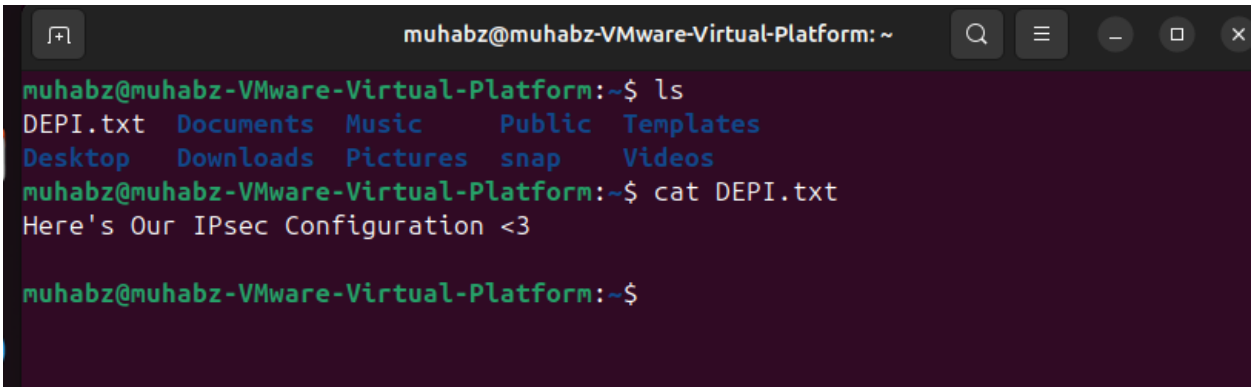


Test 2: File Transfer Test (SCP Protocol)

- **Objective: Verify real data transfer through the IPsec tunnel.**
- **Setup:**
    - **A Windows machine connected to HQ LAN (10.10.10.50).**
      (From DHCP Of LAN)
    - **A Kali Linux machine connected to Branch LAN (10.20.20.50).**
      (From DHCP Of LAN)

- **Method:**
    - **From the Windows PC, access the Kali shared folder using SSH protocol (\\10.20.20.50\share).**
    - **Attempt to copy a test file (e.g., test.txt) between both devices.**
- **Command:**
    - **From Windows PC Open The PowerShell and Type :**
    - **scp C:\Share\DEPI.txt muhabz@10.10.10.50:/home/muhabz**
- **Result:**
  ✅ **File transfer completed successfully with stable throughput and no packet loss. This confirms that the IPsec tunnel securely transmits not only ICMP packets but also application-layer data traffic.**





---

6. Conclusion

The IPsec VPN tunnel between the HQ FortiGate and the Branch FortiGate was successfully established and tested.
Connectivity between the two LANs was confirmed through ICMP ping tests and SSH file transfer verification.
This demonstrates that encrypted communication and secure data exchange between both networks are fully operational.
The configuration followed standard security best practices, ensuring data integrity and confidentiality across the VPN connection.
