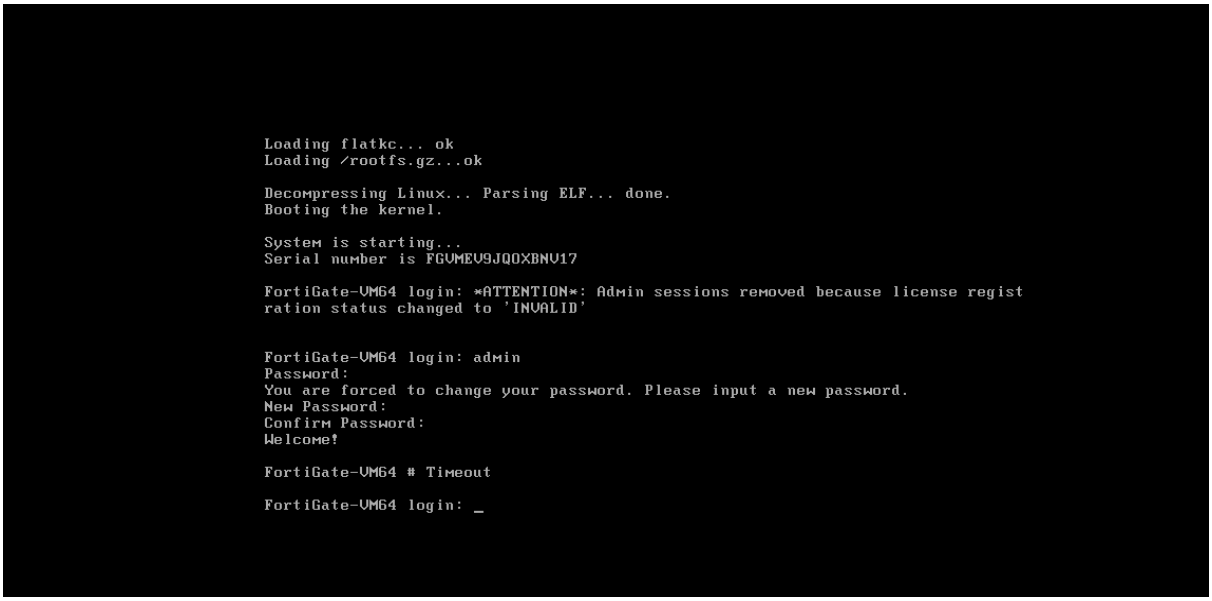
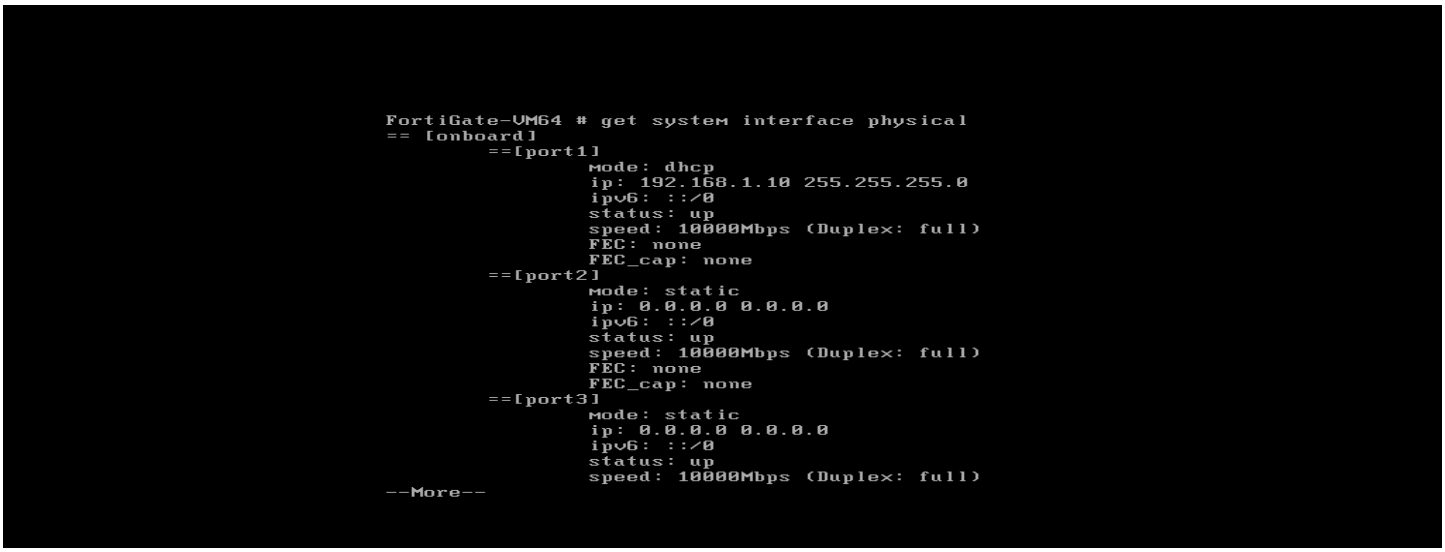
1.1. Initial Access and Password Security

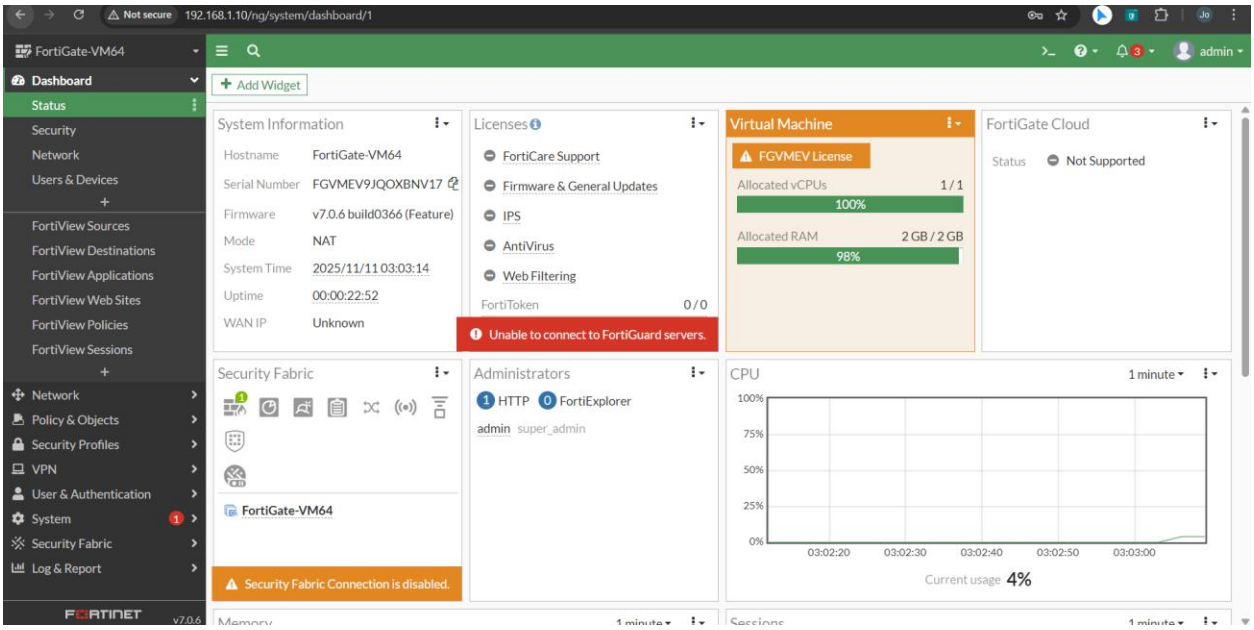


The initial login to FortiGate was via the command-line interface (CLI) using the default username (admin) and password (blank). The system forced a password change to secure the device directly from factory settings, and then a new, strong password was set.



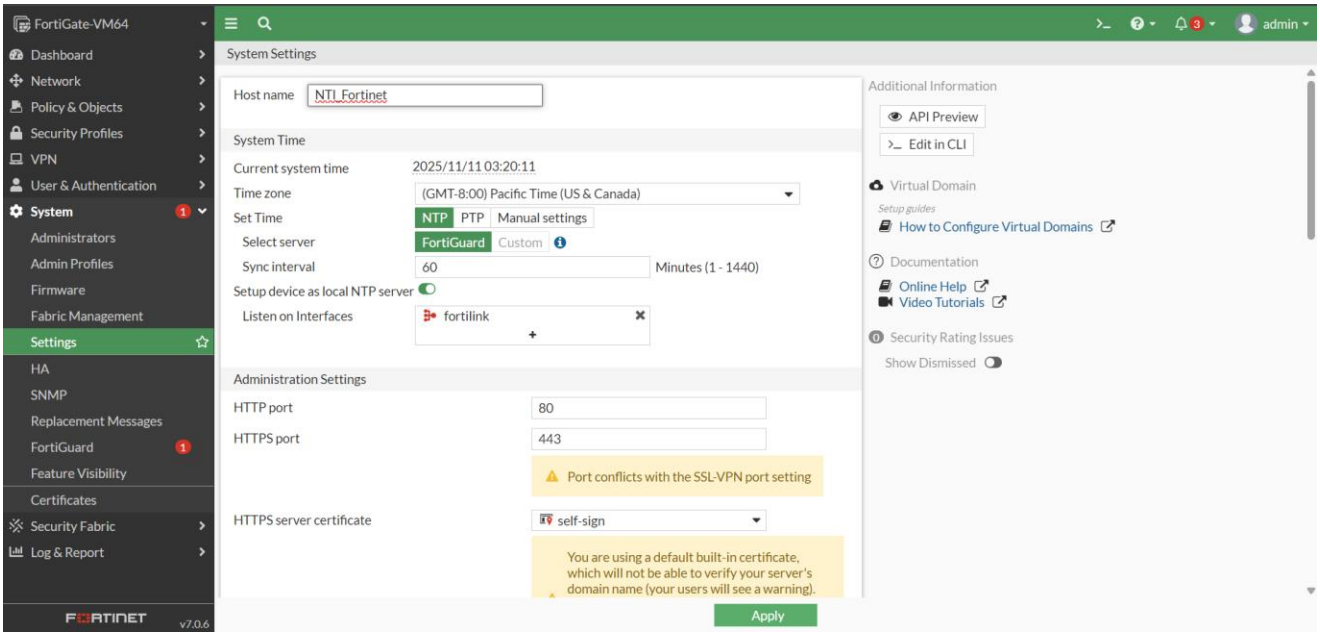
After securing the device, we switched to working via the graphical user interface (GUI). To determine the IP address that received the WAN port 1 interface from the VMware environment, the command was used to obtain the actual system interface in the CLI.

1.2. Initial IP Discovery and WAN Configuration



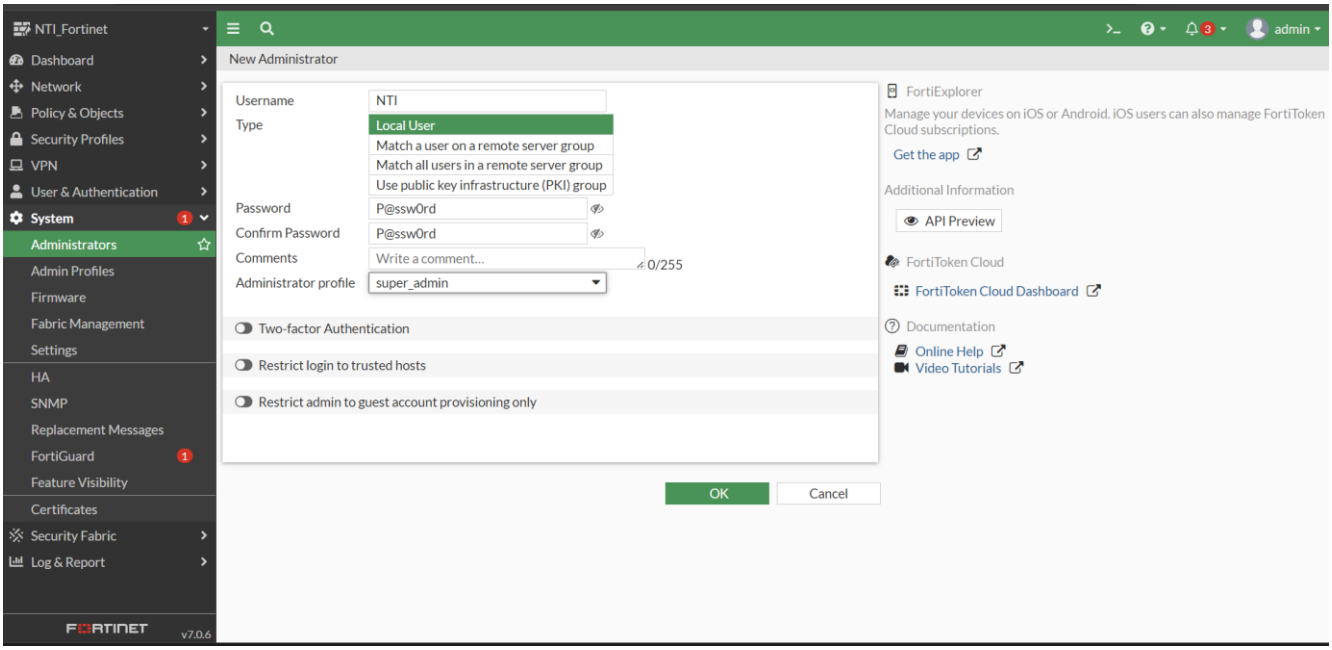
Port 1 (WAN) was assigned the address 192.168.1.10 in DHCP mode. This address was used to log in to the web interface (GUI), as shown in the main dashboard. This confirms that the device has a successful initial connection to the external network.

1.3. Assigning the hostname



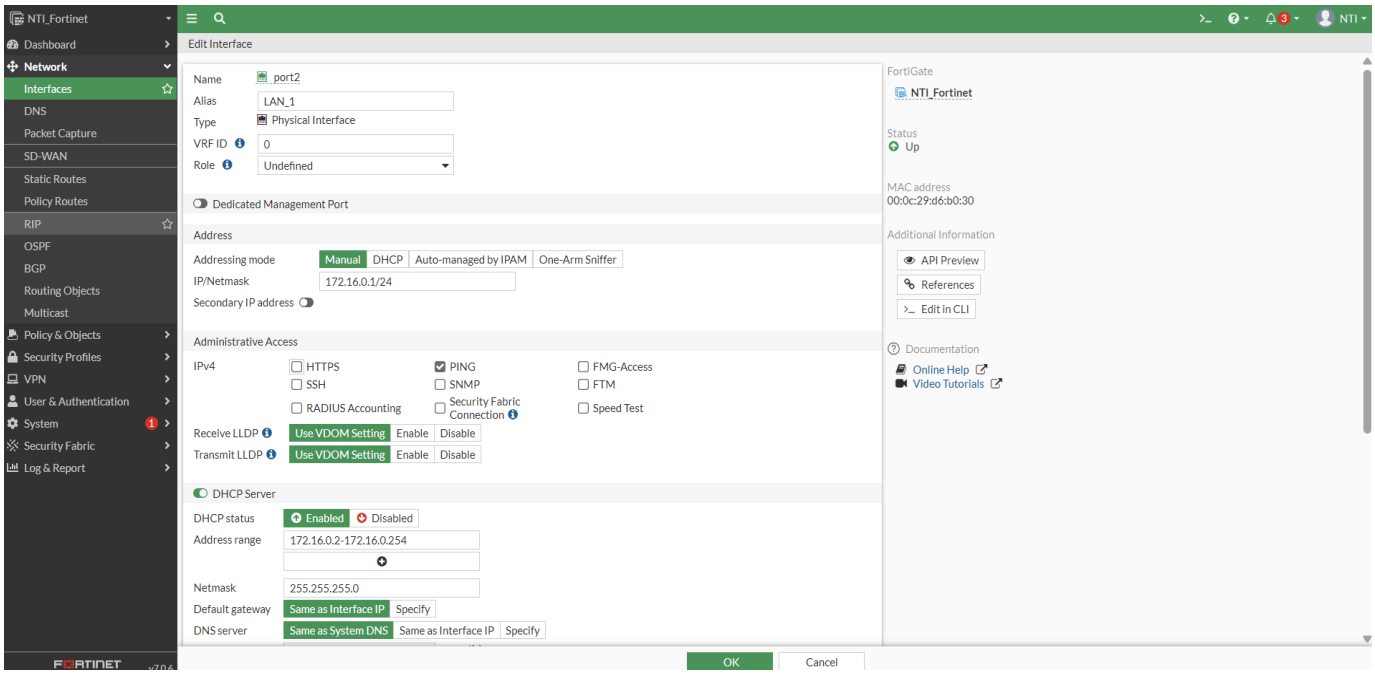
Within the *System > Settings* menu, the device's default hostname has been changed to **NTL_Fortinet** . This security measure aims to improve device identifiability in the operating environment and during log audits, and is a key component of system hardening.

1.4. Securing administrative access: Creating a new administrator account



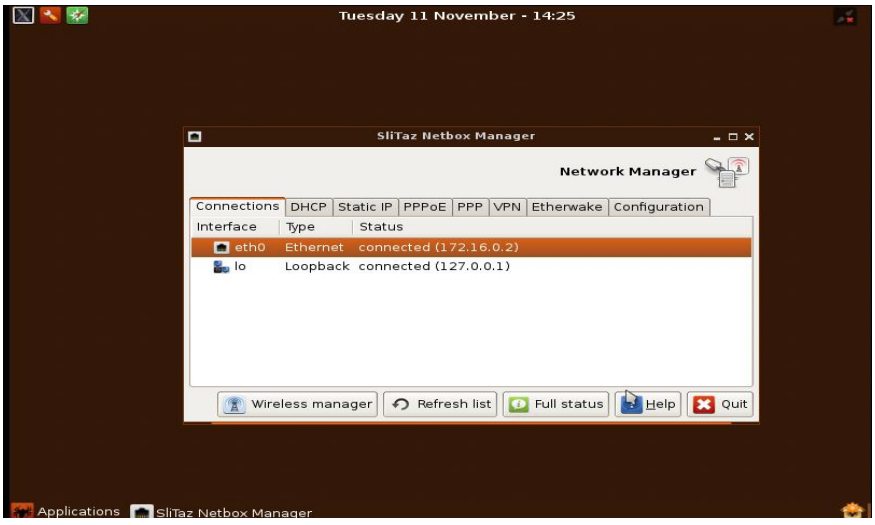
In the *System > Administrators* menu, a crucial security measure was taken by creating a new administrator account **named NTI**, assigning a strong password, and granting it super_admin privileges. This action is necessary to implement the principle of security hardening by avoiding the use of the default username (admin), which significantly reduces the likelihood of successful guessing attacks targeting common usernames.

2.1 Configuring the Local Area Interface (LAN) and enabling administrative access



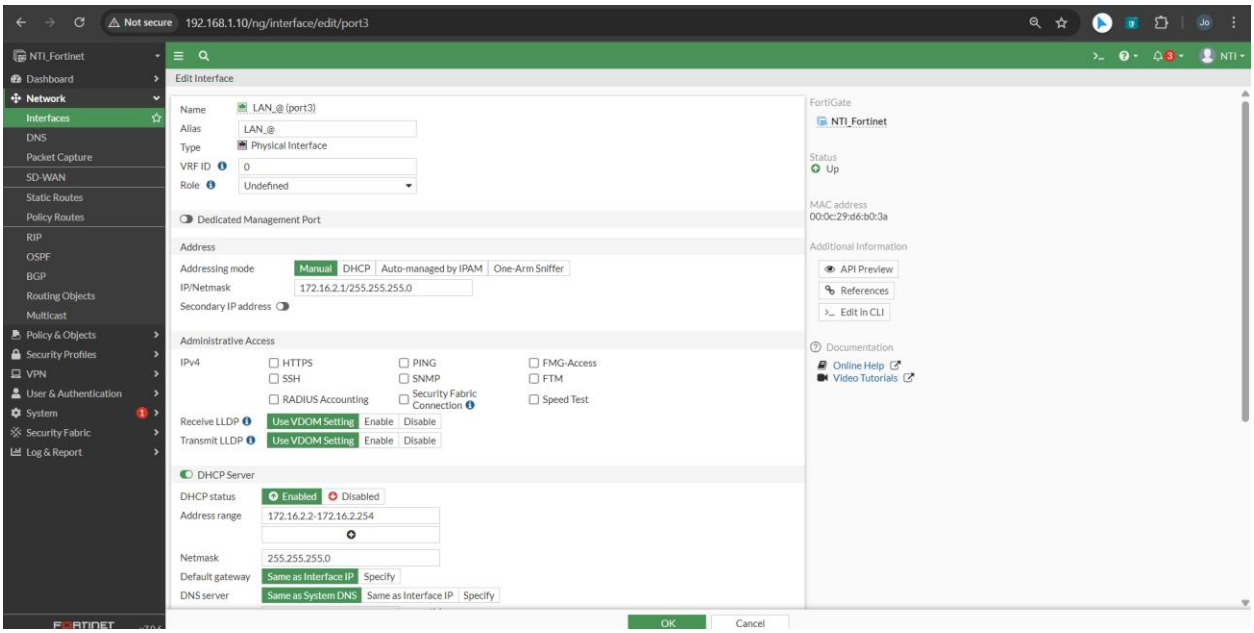
Configuring the Local Area Network (LAN) and Enabling Administrative Access: In the **Network > Interfaces** menu, the LAN interface (Port 2) was configured. It was assigned the alias LAN_1, and its address was manually set to *172.16.0.1/24*, making it the gateway for the local network. To ensure the device can be managed from the internal network, HTTPS and PING administrative access options were enabled. A DHCP server was also enabled on the same interface to automatically distribute IP addresses to internal devices within the range 172.16.0.2 to 172.16.0.254, thus completing the basic internal network configuration.

.22Testing the effectiveness of the DHCP server for the internal network



As shown in the screenshot, the client device was automatically assigned the IP address 172.16.0.2. This confirms the successful operation of the DHCP Server on FortiGate , demonstrating that the internal network is ready for communication.

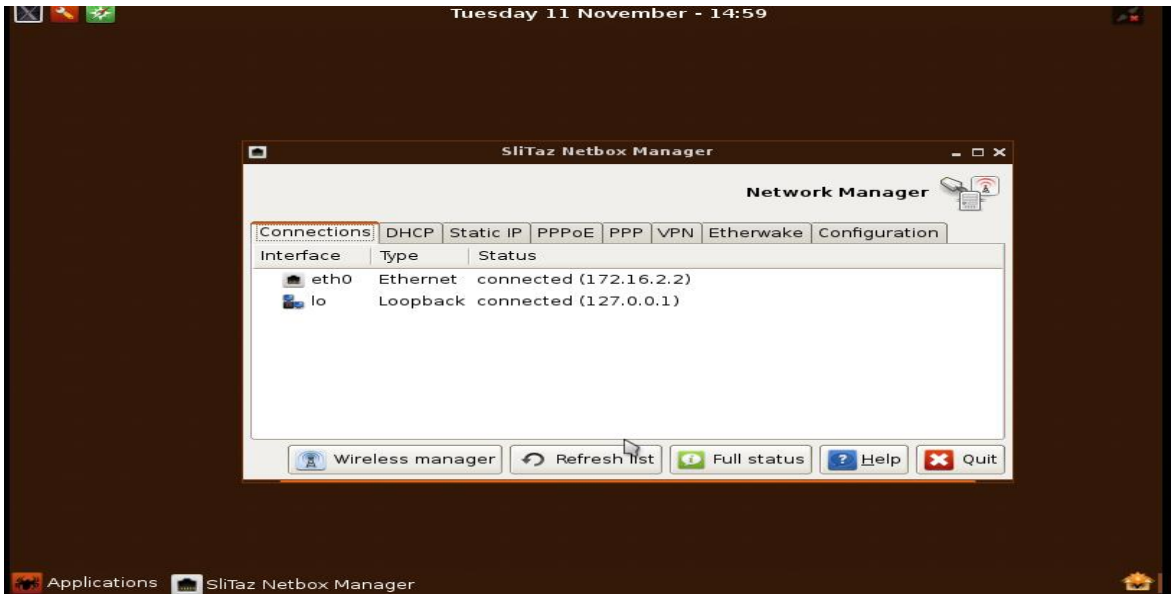
2.3Configuring the Local Area Interface (LAN2) and enabling administrative access



Configuring the Local Area Network (LAN2) and Enabling Administrative Access: In the

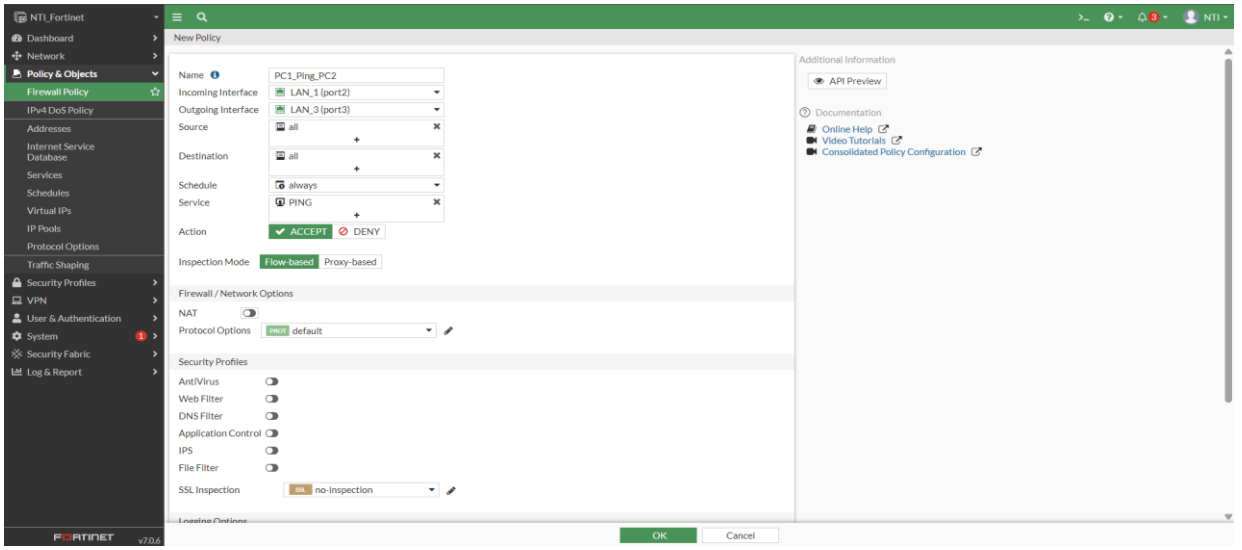
Network > Interfaces menu, the LAN interface (Port3) was configured. It was assigned the alias LAN_2, and its address was manually set to *172.16.2.1/24*, making it the gateway for the local network. To ensure the device can be managed from the internal network, HTTPS and PING administrative access options were enabled. A DHCP server was also enabled on the same interface to automatically distribute IP addresses to internal devices within the range 172.16.2.2 to 172.16.2.254, thus completing the basic internal network configuration.

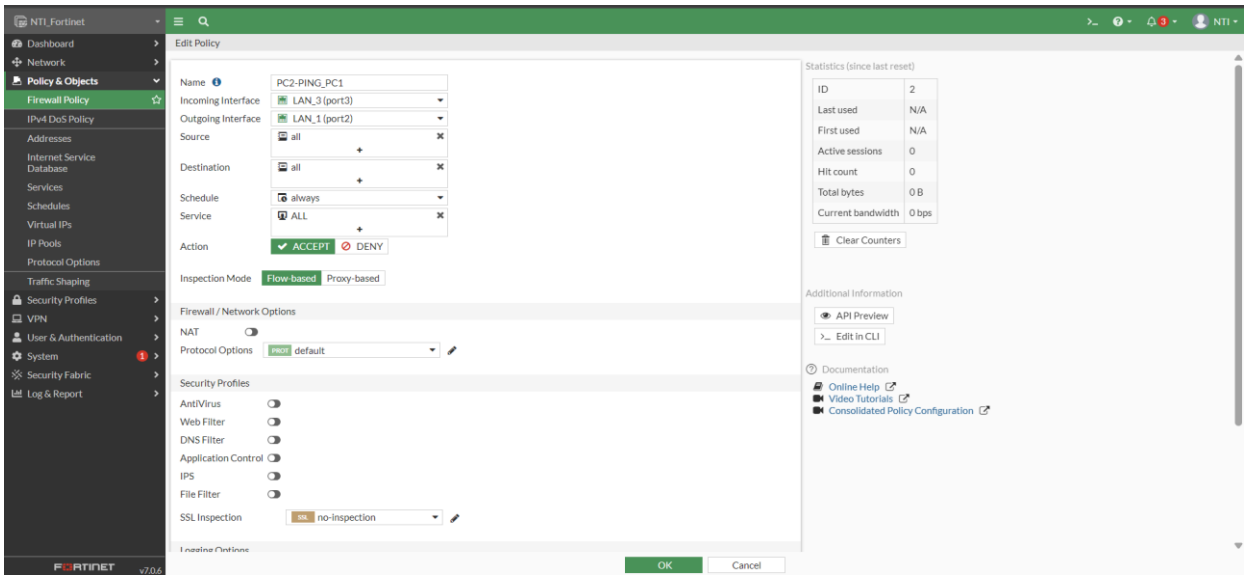
.24 Testing the effectiveness of the DHCP server for the internal network



As shown in the screenshot, the client device was automatically assigned the IP address 172.16.2.2. This confirms the successful operation of the DHCP Server on FortiGate , demonstrating that the internal network is ready for communication

2.5. Establishing two-way (LAN-to-LAN) internal communication policies





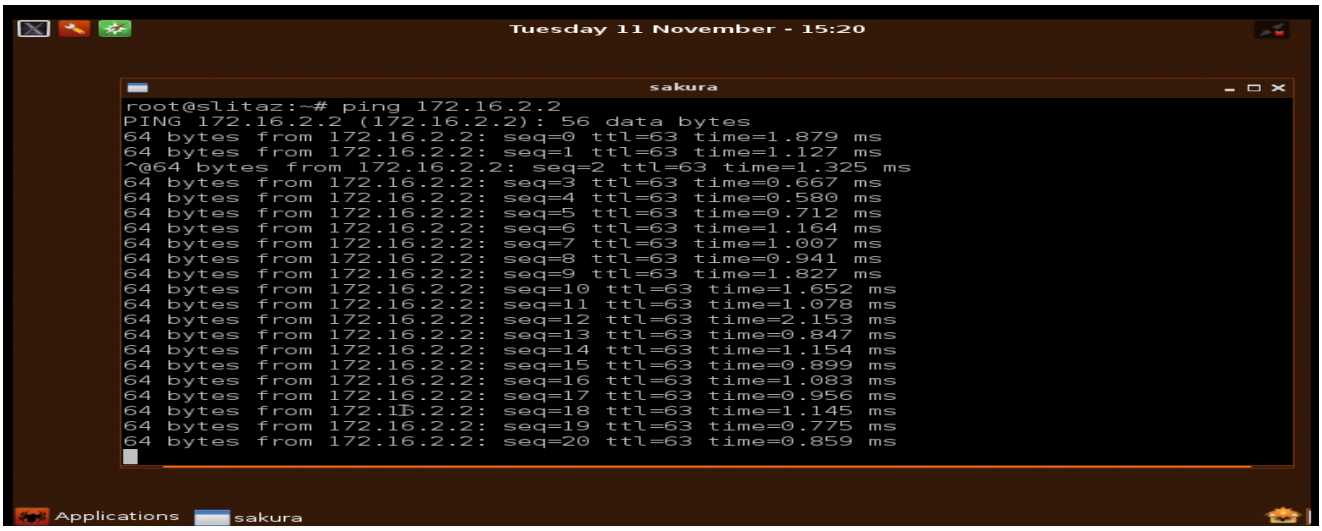
In the Policy & Objects > Firewall Policy menu, two policy sets were created to enable bidirectional communication between multiple LANs:

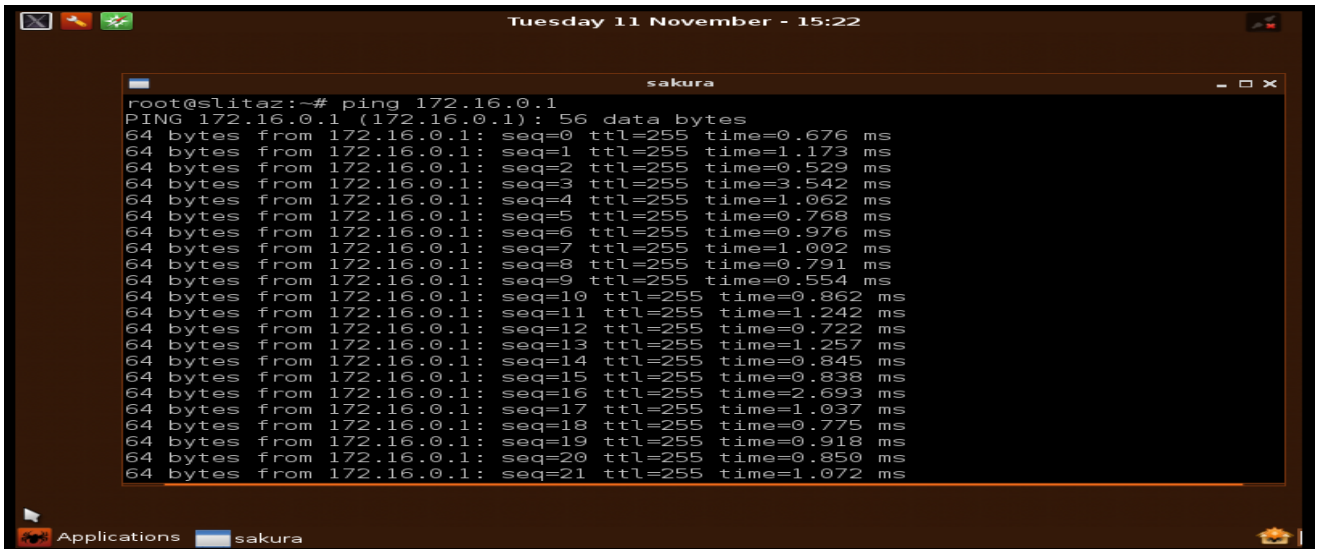
PC1_Ping_PC2: Allows access from LAN_1 to LAN_3.

PC2_PING_PC1: Allows access from LAN_3 to LAN_1.

These policies were implemented to regulate communication between internal networks. In both policies, the service is restricted to PING only, allowing basic connection inspection traffic without enabling other unnecessary services. This ensures that communication between internal networks is tightly controlled, in accordance with best security practices.

2.6. Testing the effectiveness of internal communication (LAN-to-LAN) policies





An effectiveness test of the internal communication policies (PC1_Ping_PC2 and PC2_PING_PC1) was performed from a client device connected to the LAN. The PING command was used to verify connectivity:

Connection to the Gateway: A successful PING was sent to 172.16.0.1 (the FortiGate address of LAN_1), confirming effective communication between the client and the network gateway.

Connection to the Other Network: A successful PING was sent to 172.16.2.2 (the address of another client device on LAN_3).

Results: The results confirm the effectiveness of the defined internal communication policies and that FortiGate efficiently routes traffic and forwards ICMP packets between the two internal networks.