

FORTIGATE BASIC CONFIGURATION

Configure a basic FortiGate firewall from factory settings and set up

1-Amr Khaked Saad

2- Ahmed mahmoud Mohamed

3- Youssef Hosseny Mohamed

4- Youssef wageh Moawad

Initial Access and Password Security

1.2. Initial IP Discovery and WAN Configuration

The screenshot shows the FortiGate VM64 dashboard. The left sidebar includes sections for Dashboard, Status, Security, Network, Users & Devices, FortiView Sources, Destinations, Applications, Web Sites, Policies, and Sessions. Under Network, there are links for Network, Policy & Objects, Security Profiles, VPN, User & Authentication, System, Security Fabric, and Log & Report. The main content area displays System Information (Hostname: FortiGate-VM64, Serial Number: FGVMEV9JQOXBNV17, Firmware: v7.0.6 build0366 (Feature), Mode: NAT, System Time: 2025/11/11 03:03:14, Uptime: 00:00:22:52, WAN IP: Unknown), Licenses (FortiCare Support, Firmware & General Updates, IPS, AntiVirus, Web Filtering), Virtual Machine (FGVMEV License, Allocated vCPUs: 1/1, 100% usage, Allocated RAM: 2 GB / 2 GB, 98% usage), and FortiGate Cloud (Status: Not Supported). A red banner at the bottom left states 'Unable to connect to FortiGuard servers.' Below the main dashboard are three graphs: CPU (1 minute average at 4%), Memory (1 minute average at 1%), and Session (1 minute average at 1%).

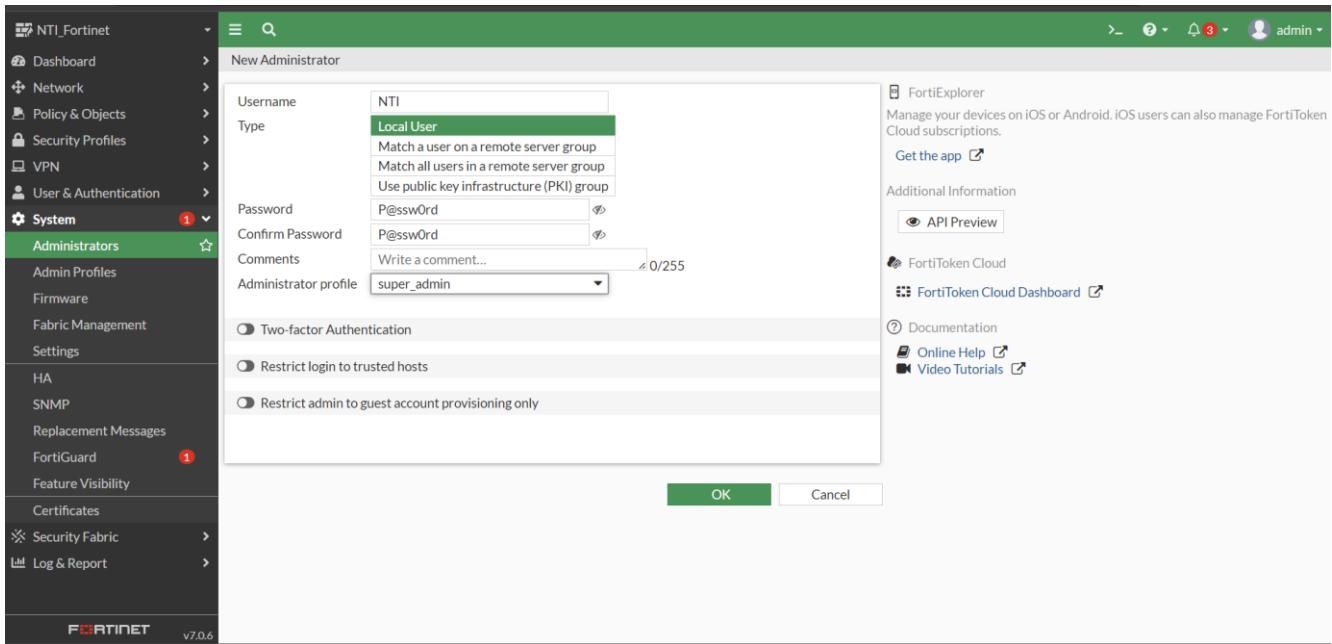
Port 1 (WAN) was assigned the address 192.168.1.10 in DHCP mode. This address was used to log in to the web interface (GUI), as shown in the main dashboard. This confirms that the device has a successful initial connection to the external network.

1.3. Assigning the hostname

The screenshot shows the System > Settings page. The left sidebar includes System, Settings, HA, SNMP, Replacement Messages, FortiGuard (with a red notification), Feature Visibility, Certificates, Security Fabric, and Log & Report. The main content area shows the Host name field set to 'NTL_Fortinet'. Other settings include System Time (Current system time: 2025/11/11 03:20:11, Time zone: (GMT-8:00) Pacific Time (US & Canada), Set Time: NTP, Select server: FortiGuard, Sync interval: 60 Minutes (1 - 1440), Listen on Interfaces: fortiflink), Administration Settings (HTTP port: 80, HTTPS port: 443, HTTPS server certificate: self-sign), and Additional Information (API Preview, Edit in CLI, Virtual Domain, Documentation, Online Help, Video Tutorials, Security Rating Issues, Show Dismissed). A yellow warning box notes a conflict between the SSL-VPN port setting (443) and the HTTPS port setting (443).

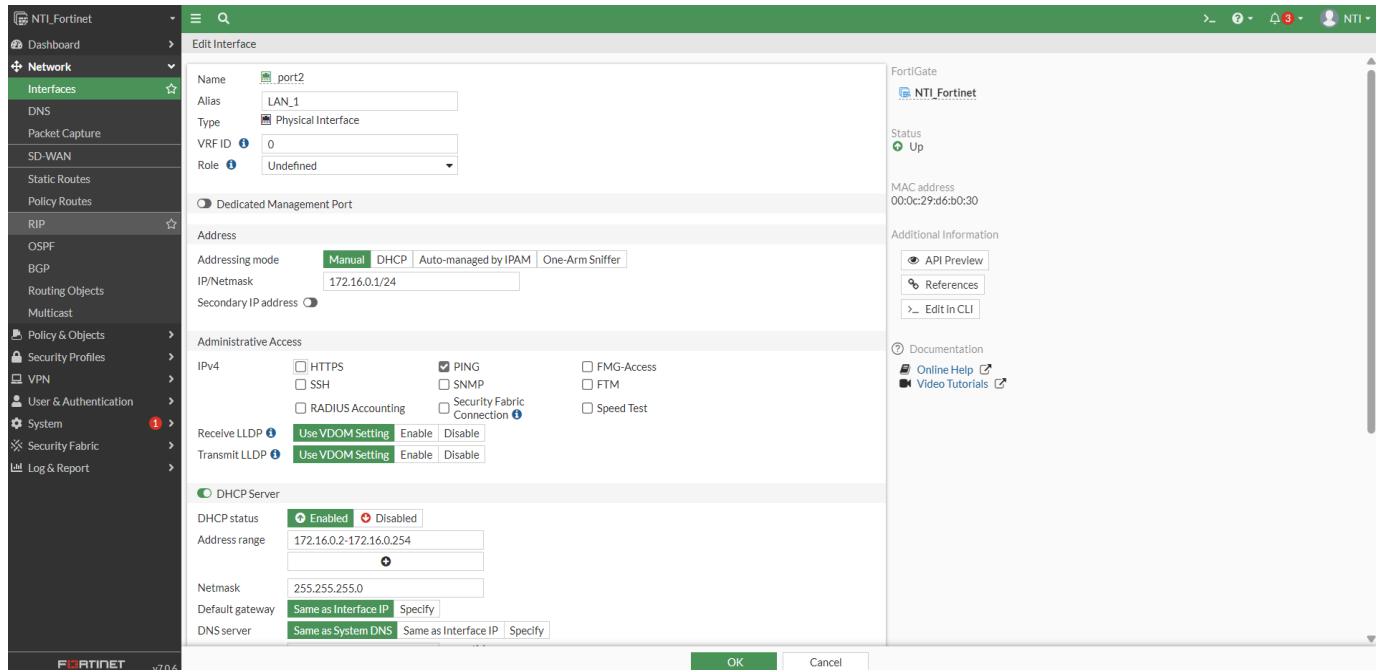
Within the *System > Settings* menu, the device's default hostname has been changed to **NTL_Fortinet**. This security measure aims to improve device identifiability in the operating environment and during log audits, and is a key component of system hardening.

1.4. Securing administrative access: Creating a new administrator account



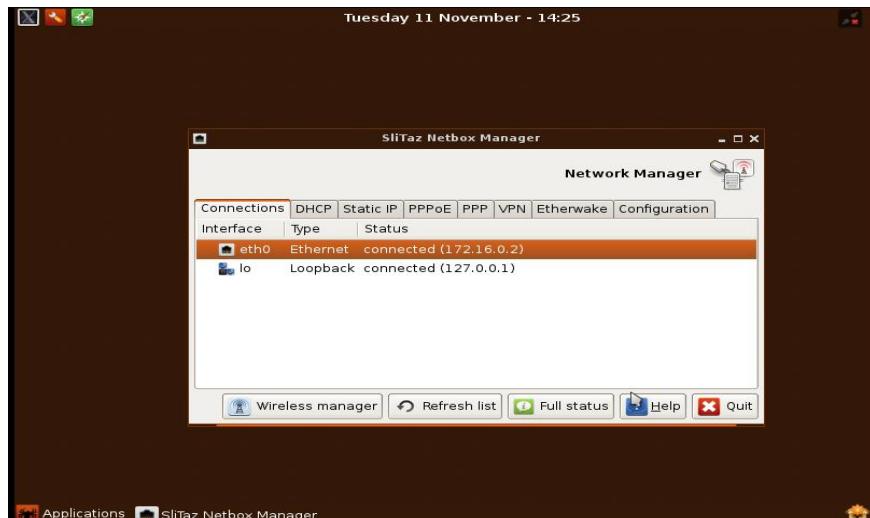
In the *System > Administrators* menu, a crucial security measure was taken by creating a new administrator account **named NTI**, assigning a strong password, and granting it **super_admin** privileges. This action is necessary to implement the principle of security hardening by avoiding the use of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

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.

2.1 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 172.16.0.2. This confirms the successful operation of the DHCP Server on FortiGate, demonstrating that the internal network is ready for communication.

