

1.1. Initial Access and Password Security

```
>Loading flatkc... ok
>Loading /rootfs.gz...ok
Decompressing Linux... Parsing ELF... done.
Booting the kernel.

System is starting...
Serial number is FGUMEU9JQOXBNV17

FortiGate-UM64 login: *ATTENTION*: Admin sessions removed because license registration status changed to 'INVALID'

FortiGate-UM64 login: admin
Password:
You are forced to change your password. Please input a new password.
New Password:
Confirm Password:
Welcome!

FortiGate-UM64 # Timeout
FortiGate-UM64 login: _
```

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.

```
FortiGate-UM64 # get system interface physical
== [onboard]
--[port1]
    mode: dhcp
    ip: 192.168.1.10 255.255.255.0
    ipv6: ::/0
    status: up
    speed: 10000Mbps (Duplex: full)
    FEC: none
    FEC_cap: none
--[port2]
    mode: static
    ip: 0.0.0.0 0.0.0.0
    ipv6: ::/0
    status: up
    speed: 10000Mbps (Duplex: full)
    FEC: none
    FEC_cap: none
--[port3]
    mode: static
    ip: 0.0.0.0 0.0.0.0
    ipv6: ::/0
    status: up
    speed: 10000Mbps (Duplex: full)
--More--
```

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

The screenshot shows the FortiGate VM64 dashboard. The left sidebar includes sections for Status, Security, Network, Users & Devices, FortiView Sources, FortiView Destinations, FortiView Applications, FortiView Web Sites, FortiView Policies, and FortiView Sessions. Under Network, options like Policy & Objects, Security Profiles, VPN, User & Authentication, System, Security Fabric, and Log & Report are listed. 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), and Virtual Machine metrics (Allocated vCPUs: 1/1, Allocated RAM: 2 GB / 2 GB). A red warning box states 'Unable to connect to FortiGuard servers.' Below this is a 'Security Fabric' section showing FortiGate-VM64 and a message 'Security Fabric Connection is disabled.' On the right, the FortiGate Cloud status is shown as 'Not Supported'. A CPU usage chart shows current usage at 4% over a one-minute period.

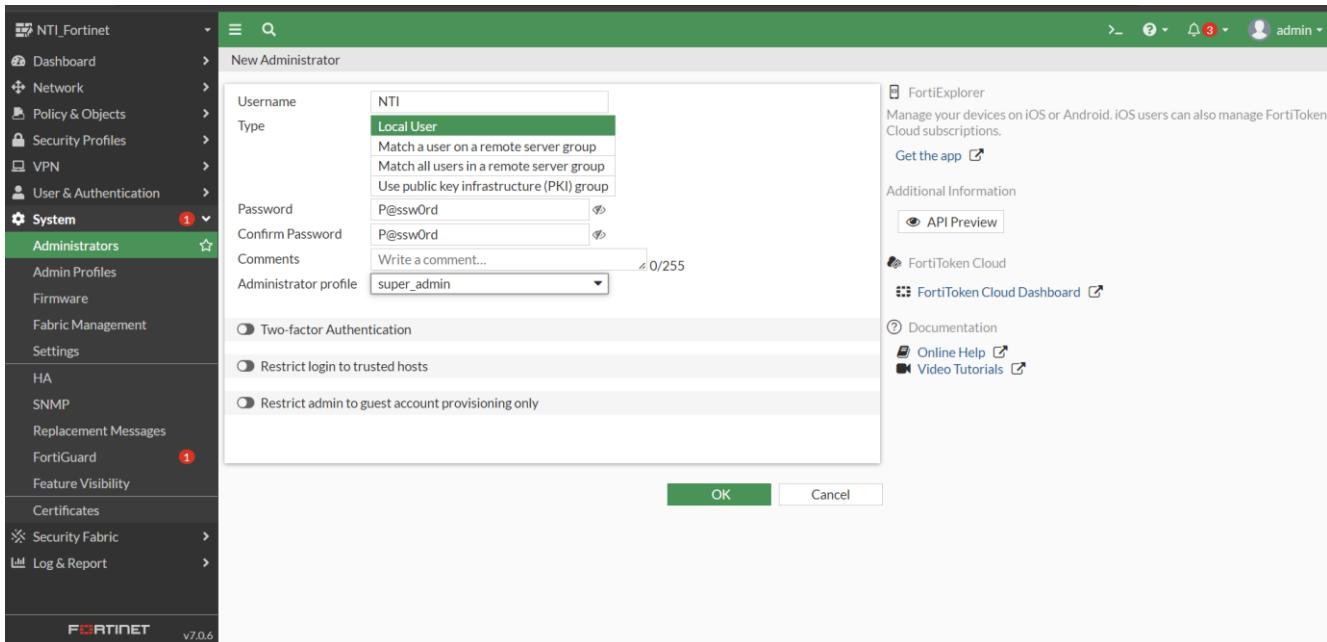
Port 1 (WAN) was assigned the address 192.168.1.10 in DHCP mode. This address was used to log in to the web interface (GUI), as shown in the main dashboard. This confirms that the device has a successful initial connection to the external network.

1.3. Assigning the hostname

The screenshot shows the System > Settings page. The left sidebar includes System, Settings, HA, SNMP, Replacement Messages, FortiGuard (with 1 update), Feature Visibility, Certificates, Security Fabric, and Log & Report. The main content area shows the Host name field set to 'NTL_Fortinet'. Under System Time, the Current system time is 2025/11/11 03:20:11, Time zone is (GMT-8:00) Pacific Time (US & Canada), Set Time is NTP, Select server is FortiGuard, Sync interval is 60 minutes, and Listen on Interfaces is fortiflink. In Administration Settings, the HTTP port is 80 and the HTTPS port is 443. A warning message states 'Port conflicts with the SSL-VPN port setting'. Under HTTPS server certificate, it says 'self-sign' and provides a note: 'You are using a default built-in certificate, which will not be able to verify your server's domain name (your users will see a warning)'. A green 'Apply' button is at the bottom right.

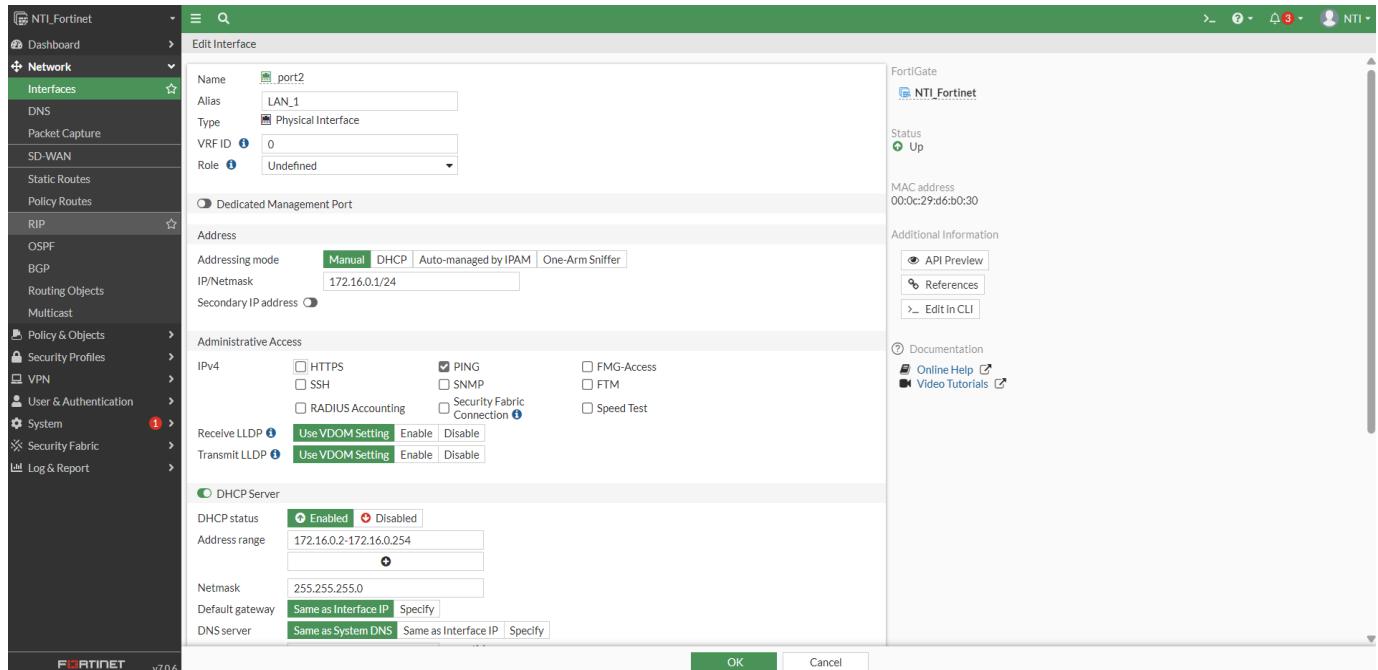
Within the *System > Settings* menu, the device's default hostname has been changed to **NTL_Fortinet**. This security measure aims to improve device identifiability in the operating environment and during log audits, and is a key component of system hardening.

1.4. Securing administrative access: Creating a new administrator account



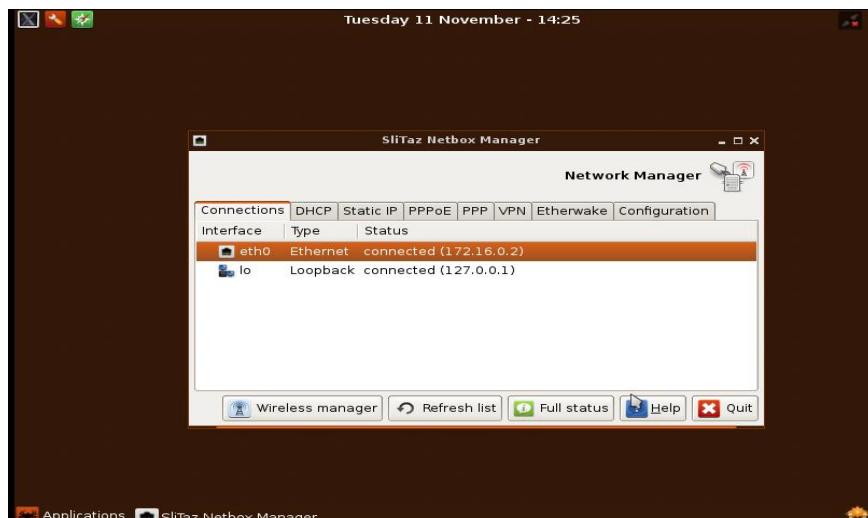
In the *System > Administrators* menu, a crucial security measure was taken by creating a new administrator account **named NTI**, assigning a strong password, and granting it super_admin privileges. This action is necessary to implement the principle of security hardening by avoiding the use of the 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



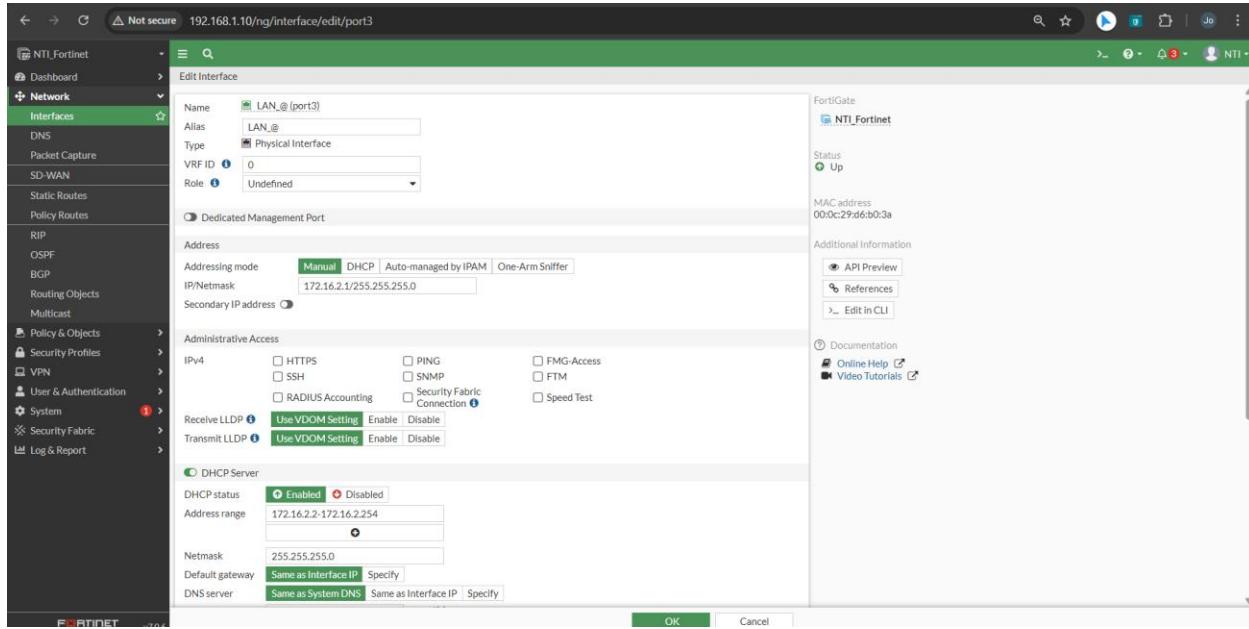
Configuring the Local Area Network (LAN) and Enabling Administrative Access: In the **Network > Interfaces** menu, the LAN interface (Port 2) was configured. It was assigned the alias LAN_1, and its address was manually set to 172.16.0.1/24, making it the gateway for the local network. To ensure the 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.

2.2 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.

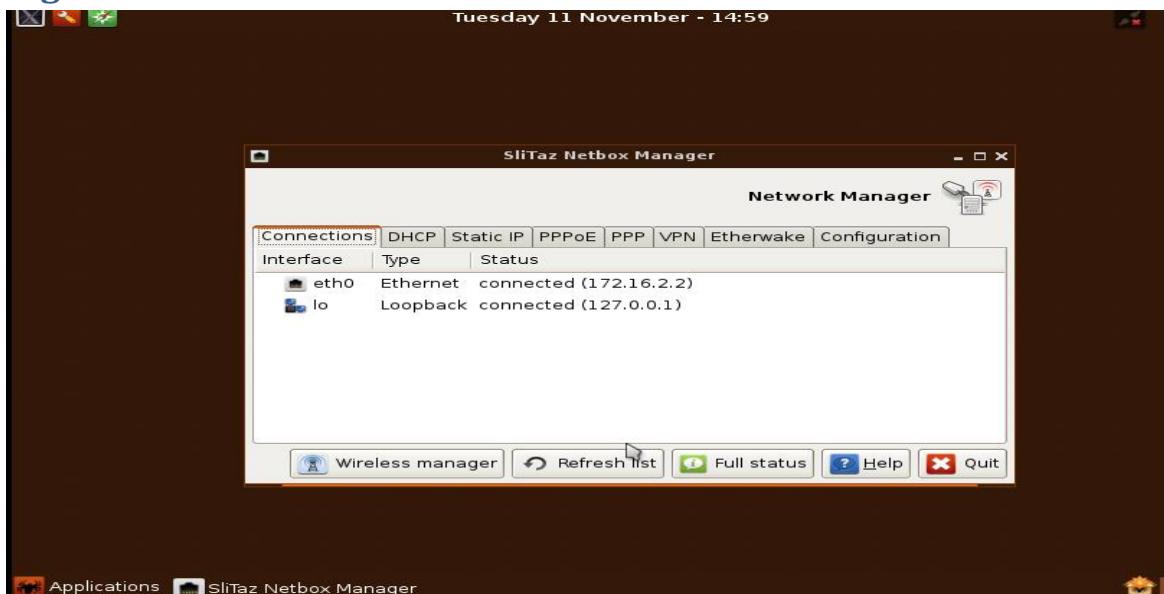
2.3Configuring the Local Area Interface (LAN2) and enabling administrative access



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.

2.4 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

The image consists of two vertically stacked screenshots of the Fortinet FortiManager web interface, specifically under the 'Policy & Objects' > 'Firewall Policy' menu.

Screenshot 1: New Policy - PC1_Ping_PC2

This screenshot shows the configuration of a new firewall policy named 'PC1_Ping_PC2'. The policy details are as follows:

- Name:** PC1_Ping_PC2
- Incoming Interface:** LAN_1 (port2)
- Outgoing Interface:** LAN_3 (port3)
- Source:** all
- Destination:** all
- Schedule:** always
- Service:** PING
- Action:** ACCEPT

Below the policy details, the 'Inspection Mode' is set to 'Flow-based'. Under 'Protocol Options', 'PROT default' is selected. The 'SSL Inspection' dropdown is set to 'no-inspection'. On the right side, there is an 'Additional Information' panel with links to API Preview, Documentation, Online Help, Video Tutorials, and Consolidated Policy Configuration.

Screenshot 2: Edit Policy - PC2-PING_PC1

This screenshot shows the configuration of an existing firewall policy named 'PC2-PING_PC1'. The policy details are as follows:

- Name:** PC2-PING_PC1
- Incoming Interface:** LAN_3 (port3)
- Outgoing Interface:** LAN_1 (port2)
- Source:** all
- Destination:** all
- Schedule:** always
- Service:** ALL
- Action:** ACCEPT

Below the policy details, the 'Inspection Mode' is set to 'Flow-based'. Under 'Protocol Options', 'PROT default' is selected. The 'SSL Inspection' dropdown is set to 'no-inspection'. On the right side, there is an 'Additional Information' panel with links to API Preview, Documentation, Online Help, Video Tutorials, and Consolidated Policy Configuration. A 'Statistics (since last reset)' table is also displayed, showing the following data:

ID	2
Last used	N/A
First used	N/A
Active sessions	0
Hit count	0
Total bytes	0 B
Current bandwidth	0 bps

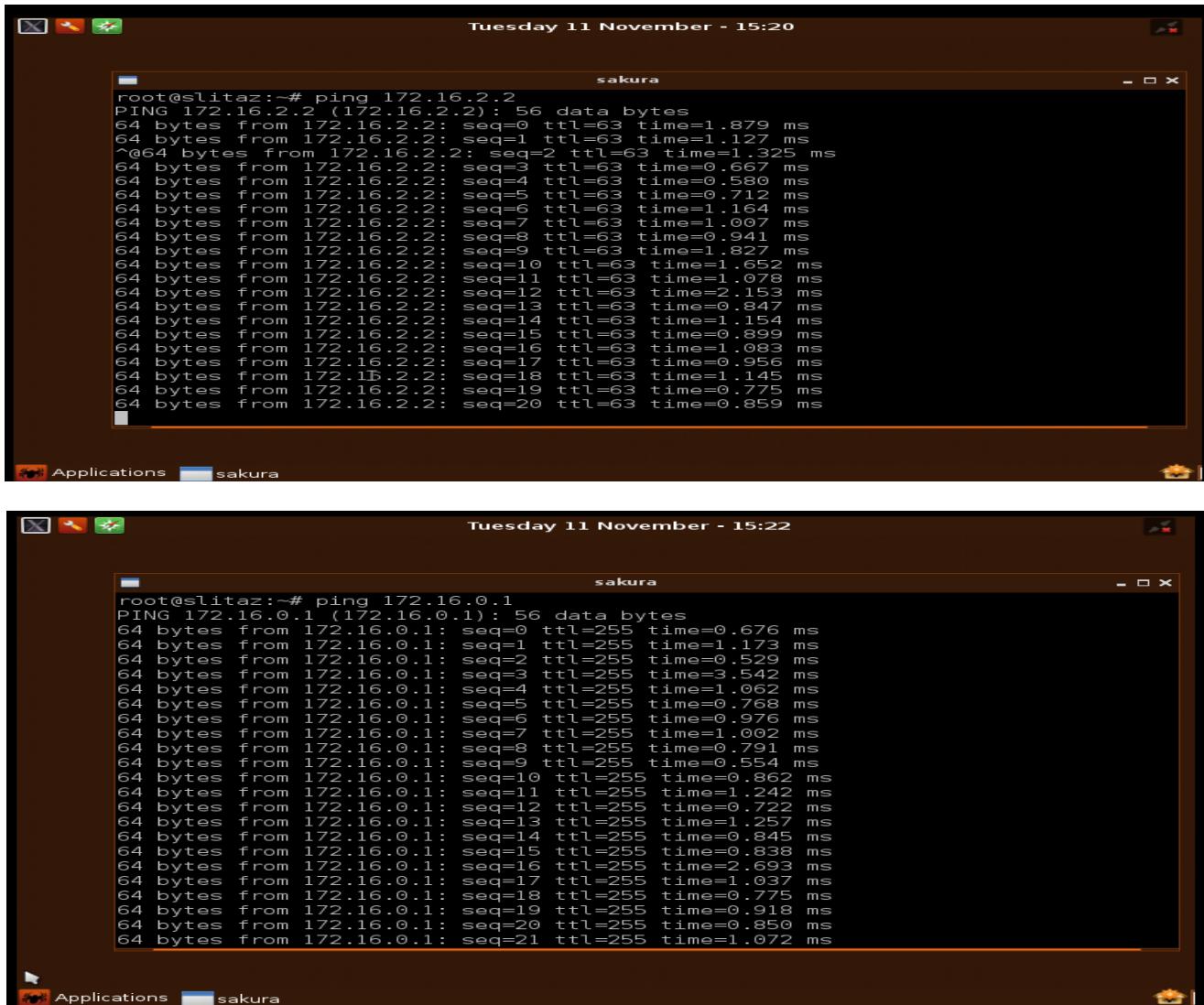
In the Policy & Objects > Firewall Policy menu, two policy sets were created to enable bidirectional communication between multiple LANs:

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



The image shows two terminal windows side-by-side, both titled "sakura". The top window is from "Tuesday 11 November - 15:20" and the bottom window is from "Tuesday 11 November - 15:22". Both windows show the output of the "ping" command.

Top Window (15:20):

```
root@slitaz:~# ping 172.16.2.2
PING 172.16.2.2 (172.16.2.2) 56 data bytes
64 bytes from 172.16.2.2: seq=0 ttl=63 time=1.879 ms
64 bytes from 172.16.2.2: seq=1 ttl=63 time=1.127 ms
^@64 bytes from 172.16.2.2: seq=2 ttl=63 time=1.325 ms
64 bytes from 172.16.2.2: seq=3 ttl=63 time=0.667 ms
64 bytes from 172.16.2.2: seq=4 ttl=63 time=0.580 ms
64 bytes from 172.16.2.2: seq=5 ttl=63 time=0.712 ms
64 bytes from 172.16.2.2: seq=6 ttl=63 time=1.164 ms
64 bytes from 172.16.2.2: seq=7 ttl=63 time=1.007 ms
64 bytes from 172.16.2.2: seq=8 ttl=63 time=0.941 ms
64 bytes from 172.16.2.2: seq=9 ttl=63 time=1.827 ms
64 bytes from 172.16.2.2: seq=10 ttl=63 time=1.652 ms
64 bytes from 172.16.2.2: seq=11 ttl=63 time=1.078 ms
64 bytes from 172.16.2.2: seq=12 ttl=63 time=2.153 ms
64 bytes from 172.16.2.2: seq=13 ttl=63 time=0.847 ms
64 bytes from 172.16.2.2: seq=14 ttl=63 time=1.154 ms
64 bytes from 172.16.2.2: seq=15 ttl=63 time=0.899 ms
64 bytes from 172.16.2.2: seq=16 ttl=63 time=1.083 ms
64 bytes from 172.16.2.2: seq=17 ttl=63 time=0.956 ms
64 bytes from 172.16.2.2: seq=18 ttl=63 time=1.145 ms
64 bytes from 172.16.2.2: seq=19 ttl=63 time=0.775 ms
64 bytes from 172.16.2.2: seq=20 ttl=63 time=0.859 ms
```

Bottom Window (15:22):

```
root@slitaz:~# ping 172.16.0.1
PING 172.16.0.1 (172.16.0.1) 56 data bytes
64 bytes from 172.16.0.1: seq=0 ttl=255 time=0.676 ms
64 bytes from 172.16.0.1: seq=1 ttl=255 time=1.173 ms
64 bytes from 172.16.0.1: seq=2 ttl=255 time=0.529 ms
64 bytes from 172.16.0.1: seq=3 ttl=255 time=3.542 ms
64 bytes from 172.16.0.1: seq=4 ttl=255 time=1.062 ms
64 bytes from 172.16.0.1: seq=5 ttl=255 time=0.768 ms
64 bytes from 172.16.0.1: seq=6 ttl=255 time=0.976 ms
64 bytes from 172.16.0.1: seq=7 ttl=255 time=1.002 ms
64 bytes from 172.16.0.1: seq=8 ttl=255 time=0.791 ms
64 bytes from 172.16.0.1: seq=9 ttl=255 time=0.554 ms
64 bytes from 172.16.0.1: seq=10 ttl=255 time=0.862 ms
64 bytes from 172.16.0.1: seq=11 ttl=255 time=1.242 ms
64 bytes from 172.16.0.1: seq=12 ttl=255 time=0.722 ms
64 bytes from 172.16.0.1: seq=13 ttl=255 time=1.257 ms
64 bytes from 172.16.0.1: seq=14 ttl=255 time=0.845 ms
64 bytes from 172.16.0.1: seq=15 ttl=255 time=0.838 ms
64 bytes from 172.16.0.1: seq=16 ttl=255 time=2.693 ms
64 bytes from 172.16.0.1: seq=17 ttl=255 time=1.037 ms
64 bytes from 172.16.0.1: seq=18 ttl=255 time=0.775 ms
64 bytes from 172.16.0.1: seq=19 ttl=255 time=0.918 ms
64 bytes from 172.16.0.1: seq=20 ttl=255 time=0.850 ms
64 bytes from 172.16.0.1: seq=21 ttl=255 time=1.072 ms
```

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.