Documentation of Configuring FortiGate firewall

❖ INTRODUCTION

In the modern era of cybersecurity, firewalls are critical for securing internal networks from external threats. As cyberattacks become more sophisticated, network administrators rely on intelligent firewalls to monitor, filter, and allow or deny traffic. This project focuses on the deployment, configuration, and policy implementation of a FortiGate next-generation firewall using VMware Workstation Pro. FortiGate firewalls are widely used in enterprise networks for their advanced security features including deep packet inspection, intrusion prevention systems, antivirus scanning, and secure web filtering.

The configuration in this project is performed via the graphical user interface (GUI), making it easier to visualize and manage network policies. Internal LAN users and external WAN environments are simulated using virtual machines. Through this project, hands-on experience in designing secure network architectures and understanding how firewall policies control communication is achieved.

❖ OBJECTIVE

The main objectives of this project are:

- Deploy FortiGate Firewall as a virtual machine in VMware Workstation Pro.
- Configure interfaces with appropriate IP addressing schemes.
- Differentiate between external (WAN) and internal (LAN) zones.
- Create static routes to enable communication with the external internet.
- Enable DHCP services on the LAN interface to provide dynamic IP configuration to internal clients.
- Implement firewall policies that define how traffic is managed and filtered.
- Test and verify that the network setup meets the requirements for both security and connectivity.

❖ TOOLS & TECHNOLOGY USED

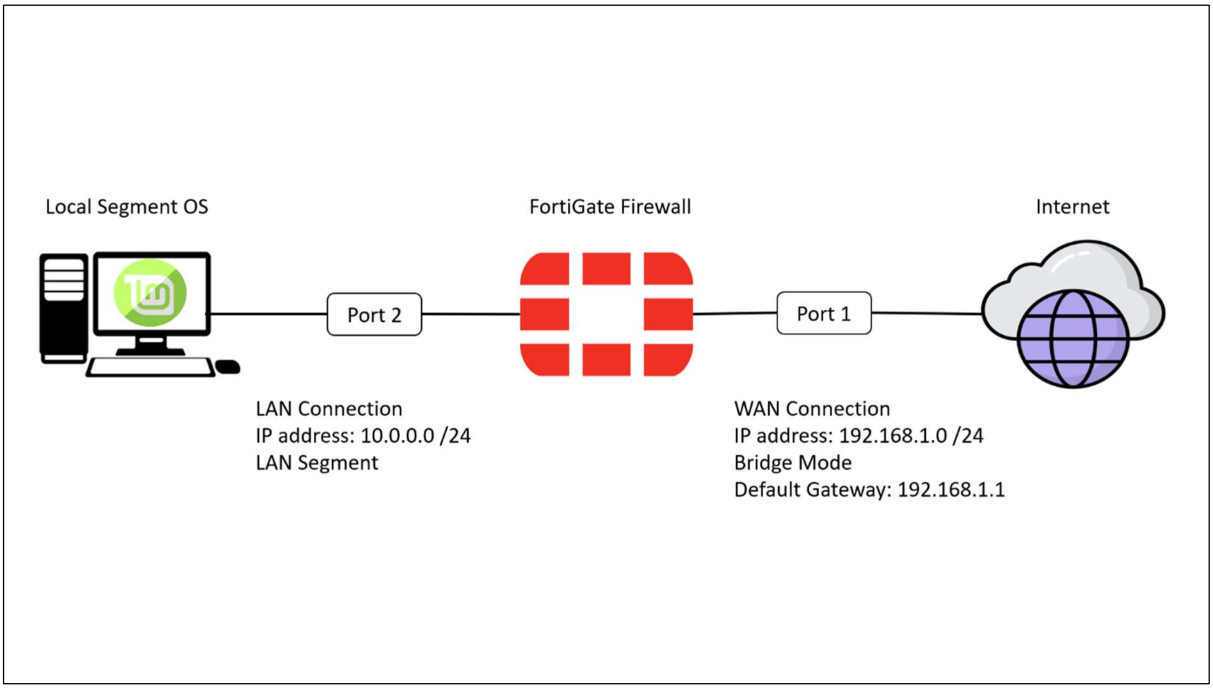
- **VMware Workstation Pro** – A powerful virtualization tool used to run multiple virtual machines. Version: 17.6.1 build-24319023
- **FortiGate Firewall VM** – A virtualized version of Fortinet's next-generation firewall. Version: FFW_VM64-v7.2.11.M-build1740-FORTINET.out.ovf
- **Windows/Linux Virtual Machines** – Used to simulate end-user systems in the internal LAN. Version: LinuxMint_21_VM
- **Web Browser** – Accessed via the FortiGate's management IP for GUI-based configuration.
- **Command Line Interface (CLI)** – Used for quick configuration and troubleshooting steps.

❖ TOPOLOGY

This project simulates a basic but secure enterprise network consisting of an internal LAN, a firewall, and access to the external internet.

Network Summary:

Component	Interface	IP Address	Mode	Role
FortiGate Firewall	port1	192.168.1.18	Bridged	WAN (Internet)
FortiGate Firewall	port2	10.0.0.1	LAN Segment	LAN Gateway
Admin Laptop	N/A	192.168.1.9	Bridged	Management
Internet Gateway	N/A	192.168.1.1	Default Router	External Access
Internal VM	N/A	10.0.0.10	LAN Segment	Client Device



The network topology used in this project is a hybrid architecture that demonstrates both WAN and LAN communications through a FortiGate firewall. The setup includes two main FortiGate interfaces:

- **Port 1 (WAN interface)** is configured with an IP address of 192.168.1.18/24 and placed in bridged mode. This interface communicates directly with the host laptop's physical network adapter, allowing access to the external router (192.168.1.1) and thus to the internet. The laptop used for administration has the IP 192.168.1.9 and is also on the same bridged network. This enables GUI-based access to the firewall from the host laptop.
- **Port 2 (LAN interface)** is configured with an IP address of 10.0.0.1/24 and connects to a virtual LAN segment inside VMware. This LAN segment acts as the internal secure

network where end-user virtual machines (e.g., a Linux Mint client) are deployed. These internal VMs receive their IP addresses (e.g., 10.0.0.10) dynamically via the DHCP service configured on port2. Their default gateway is 10.0.0.1, which is the FortiGate firewall.

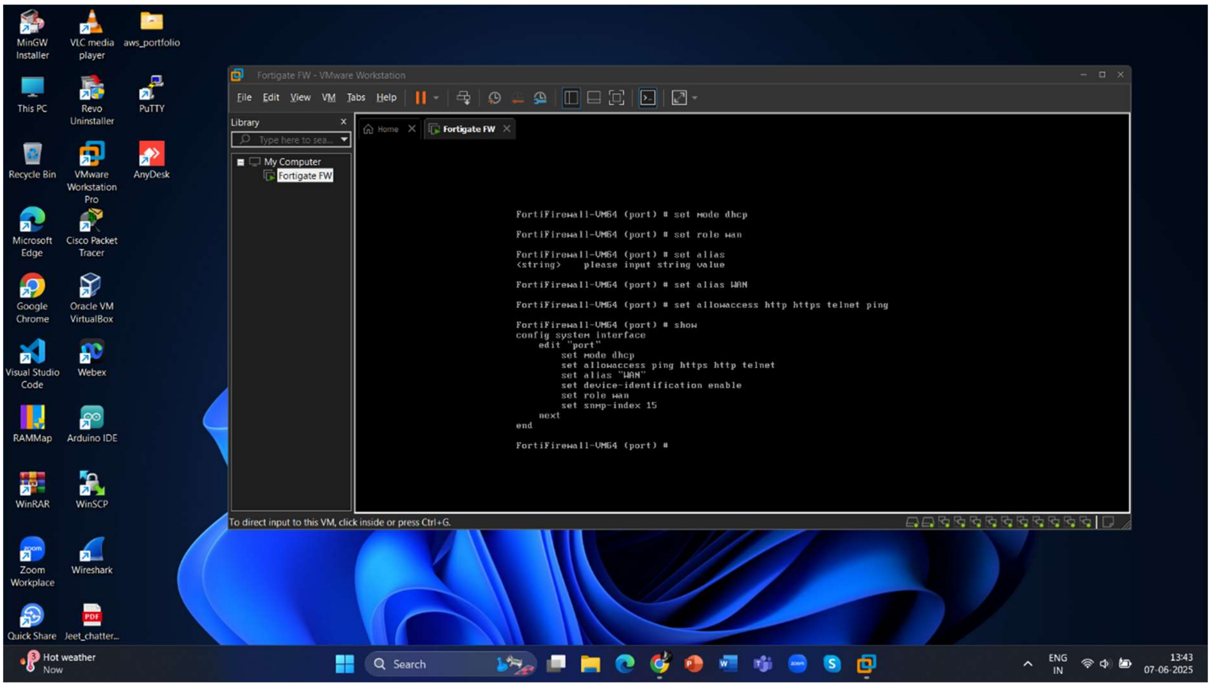
Traffic from internal systems destined for the internet must pass through port2 to port1. This design isolates internal traffic while providing centralized management and security enforcement through the FortiGate firewall. NAT is applied at the firewall, allowing internal private IPs to access public services securely.

This topology mirrors real-world enterprise deployments, where segmentation between internal LANs and external WANs is crucial for defence-in-depth.

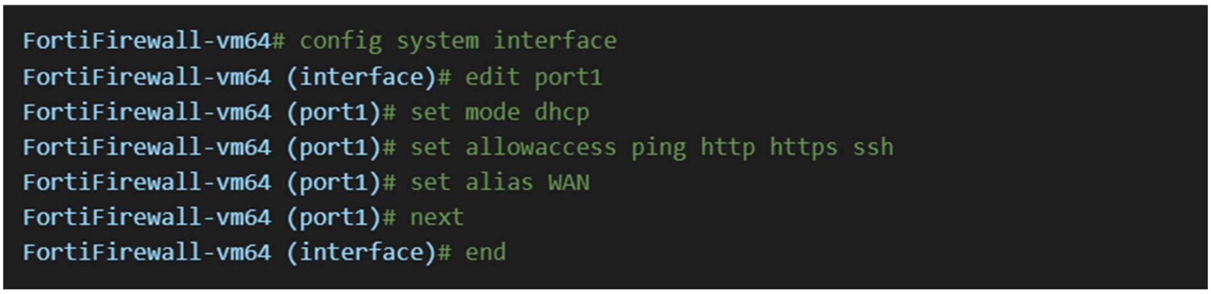
❖ IMPLEMENTATION

Step 1: Configure WAN Interface (port1)

This step configures the FortiGate's external-facing interface. By using bridged mode, the firewall is able to access the physical network through the host machine. The IP is dynamically obtained via DHCP.


Fortigate FW - VMware Workstation
File Edit View VM Tabs Help
Library
My Computer
Fortigate FW
Home
Fortigate FW
To direct input to this VM, click inside or press Ctrl+G.

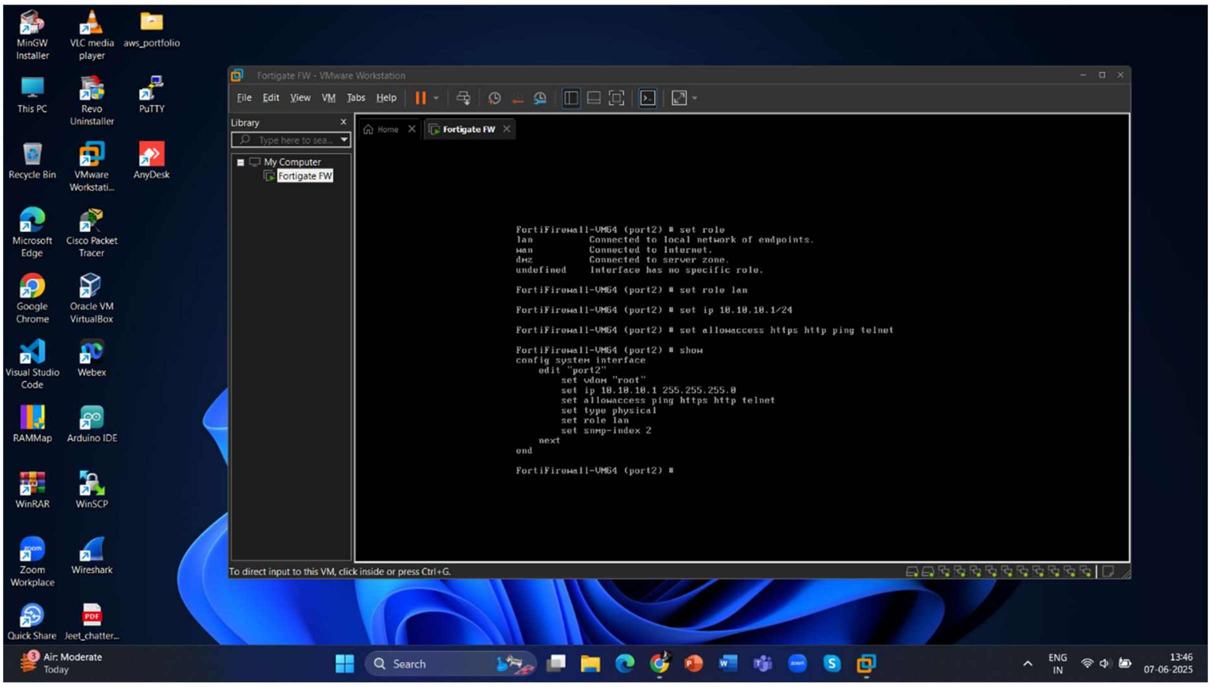
```
FortiFirewall-VM64 (port) # set mode dhcp

FortiFirewall-VM64 (port) # set role wan

FortiFirewall-VM64 (port) # set alias
<string>    please input string value

FortiFirewall-VM64 (port) # set alias WAN

FortiFirewall-VM64 (port) # set allowaccess http https telnet ping

FortiFirewall-VM64 (port) # show
config system interface
    edit "port"
        set mode dhcp
        set allowaccess ping https http telnet
        set alias "WAN"
        set device-identification enable
        set role wan
        set snmp-index 15
    next
end

FortiFirewall-VM64 (port) #
```



```
FortiFirewall-vm64# config system interface
FortiFirewall-vm64 (interface)# edit port1
FortiFirewall-vm64 (port1)# set mode dhcp
FortiFirewall-vm64 (port1)# set allowaccess ping http https ssh
FortiFirewall-vm64 (port1)# set alias WAN
FortiFirewall-vm64 (port1)# next
FortiFirewall-vm64 (interface)# end
```

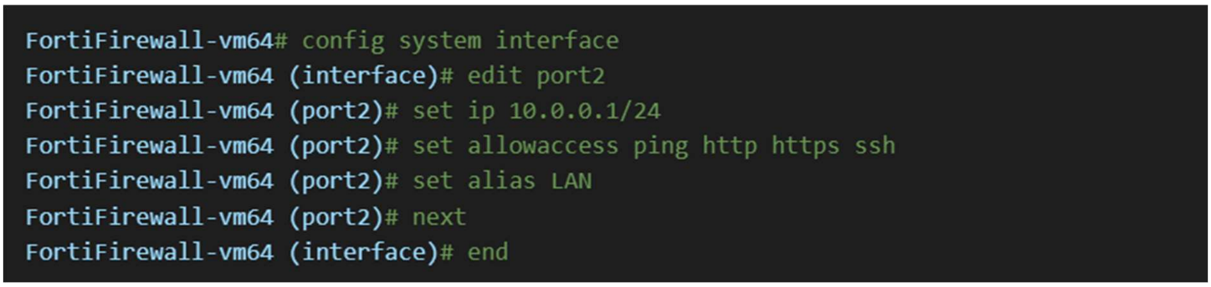
Step 2: Configure LAN Interface (port2)

Here, port2 acts as the LAN gateway. All internal devices route traffic through this IP. Allowing GUI and SSH access makes this interface manageable from internal systems.



```
FortiFirewall-VM64 (port2) # set role
lan           Connected to local network of endpoints.
wan           Connected to Internet.
dmz           Connected to server zone.
undefined     Interface has no specific role.

FortiFirewall-VM64 (port2) # set role lan

FortiFirewall-VM64 (port2) # set ip 10.10.10.1/24

FortiFirewall-VM64 (port2) # set allowaccess https http ping telnet

FortiFirewall-VM64 (port2) # show
config system interface
    edit "port2"
        set vdom "root"
        set ip 10.10.10.1 255.255.255.0
        set allowaccess ping https http telnet
        set type physical
        set role lan
        set snmp-index 2
    next
end

FortiFirewall-VM64 (port2) #
```

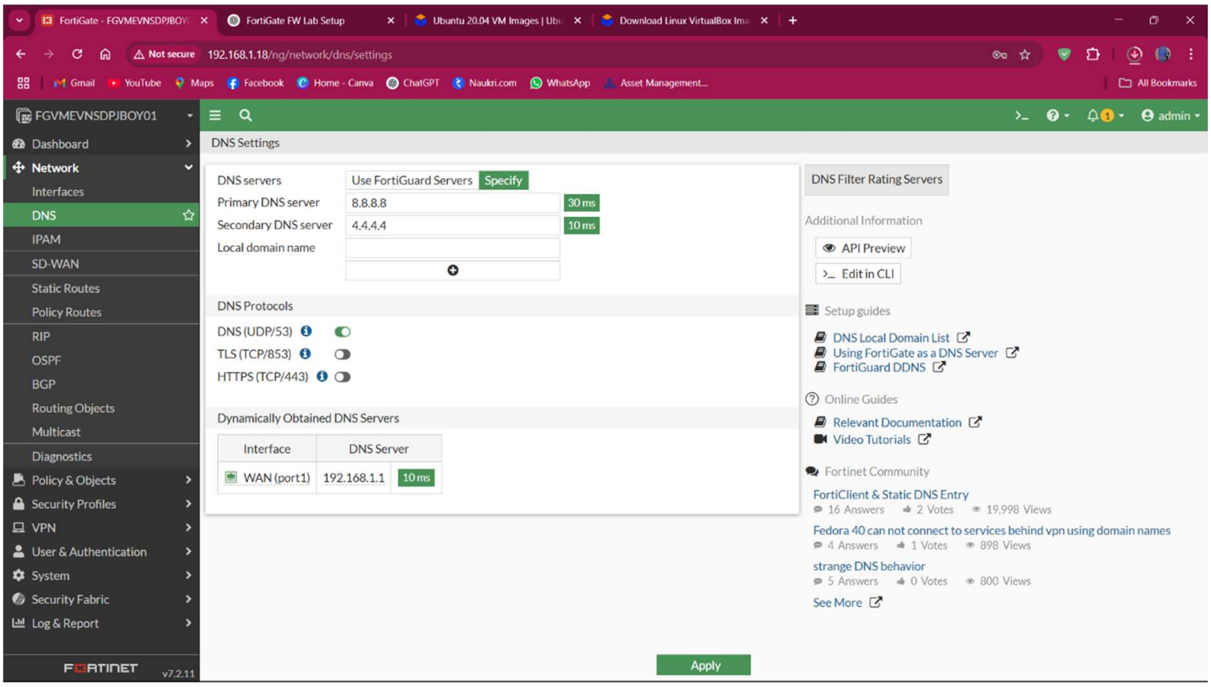
To direct input to this VM, click inside or press Ctrl+G.



```
FortiFirewall-vm64# config system interface
FortiFirewall-vm64 (interface)# edit port2
FortiFirewall-vm64 (port2)# set ip 10.0.0.1/24
FortiFirewall-vm64 (port2)# set allowaccess ping http https ssh
FortiFirewall-vm64 (port2)# set alias LAN
FortiFirewall-vm64 (port2)# next
FortiFirewall-vm64 (interface)# end
```

Step 3: Configure DNS

DNS was configured through the FortiGate GUI under Network → DNS. The configuration included setting the Primary DNS server to 8.8.8.8 and the Secondary DNS server to 4.4.4.4. This ensures that the firewall and internal LAN clients can resolve domain names to IP addresses, allowing access to external websites and services. Additionally, DNS caching was enabled to improve resolution performance. This GUI-based setup supports services like FortiGuard, Web Filtering, and policy-based domain controls essential for network operations and security.



DNS Settings

DNS servers: Use FortiGuard Servers | **Specify**

Primary DNS server: 8.8.8.8 (30 ms)

Secondary DNS server: 4.4.4.4 (10 ms)

Local domain name:

DNS Protocols

DNS (UDP/53) ●

TLS (TCP/853) ○

HTTPS (TCP/443) ○

Dynamically Obtained DNS Servers

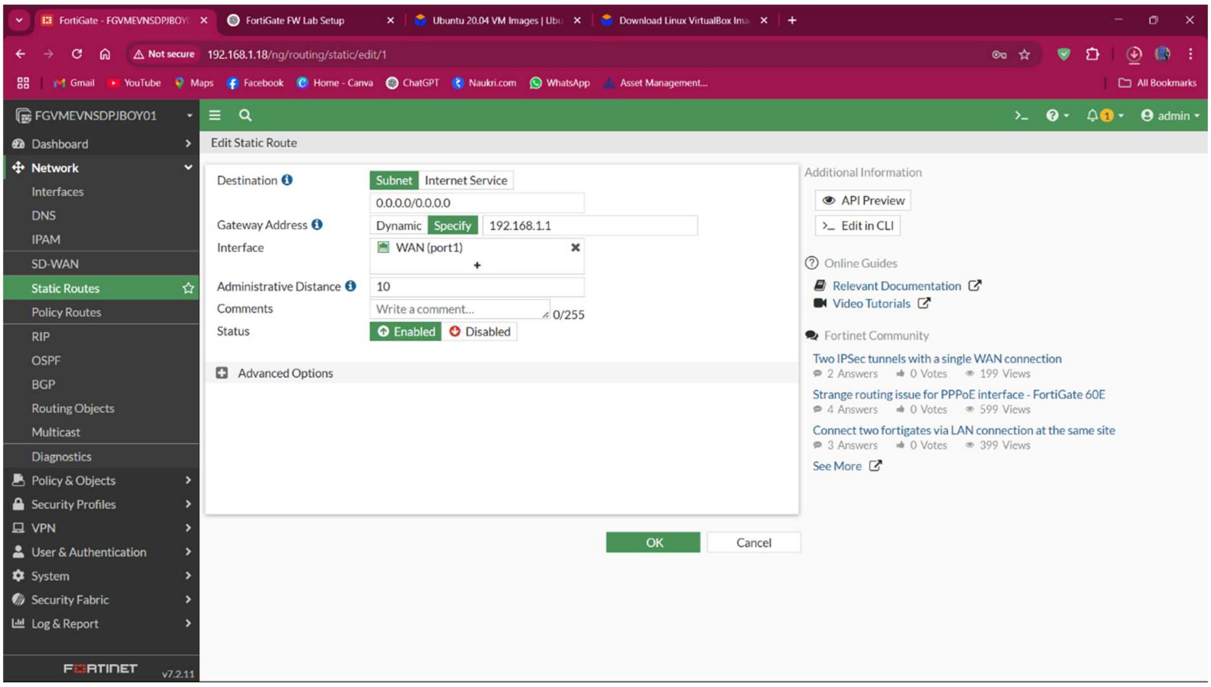
Interface	DNS Server	
WAN (port1)	192.168.1.1	10 ms

Step 4: Configure Static Route to Internet

To enable internet connectivity for internal clients, a static route is configured in GUI mode. This was done through the following steps:

- Navigate to **Network** > **Static Routes**.
- Click **Create New**.
- Set **Destination** as 0.0.0.0/0 to represent all external addresses.
- Set **Gateway** as the IP of your external router, for example 192.168.1.1.
- Set **Interface** to WAN port1.
- Save the configuration.

This static route tells the firewall to forward all non-local traffic from the LAN to the WAN router.



Edit Static Route

Destination: Subnet — 0.0.0.0/0.0.0.0

Gateway Address: Specify — 192.168.1.1

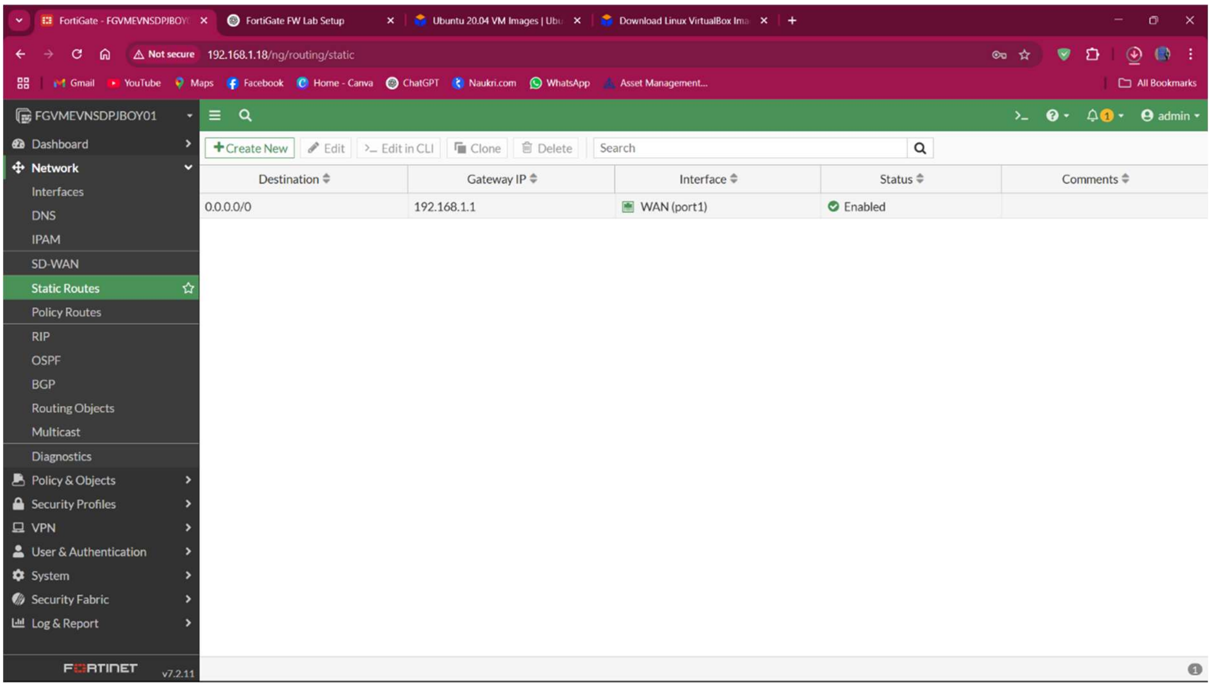
Interface: WAN (port1)

Administrative Distance: 10

Comments: Write a comment... 0/255

Status: Enabled

192.168.1.18/ng/routing/static/edit/1
Advanced Options
Additional Information
API Preview
Edit in CLI
Online Guides
Relevant Documentation
Video Tutorials
Fortinet Community
Two IPSec tunnels with a single WAN connection
Strange routing issue for PPPoE interface - FortiGate 60E
Connect two fortigates via LAN connection at the same site
See More
OK
Cancel



Destination	Gateway IP	Interface	Status	Comments
0.0.0.0/0	192.168.1.1	WAN (port1)	Enabled	

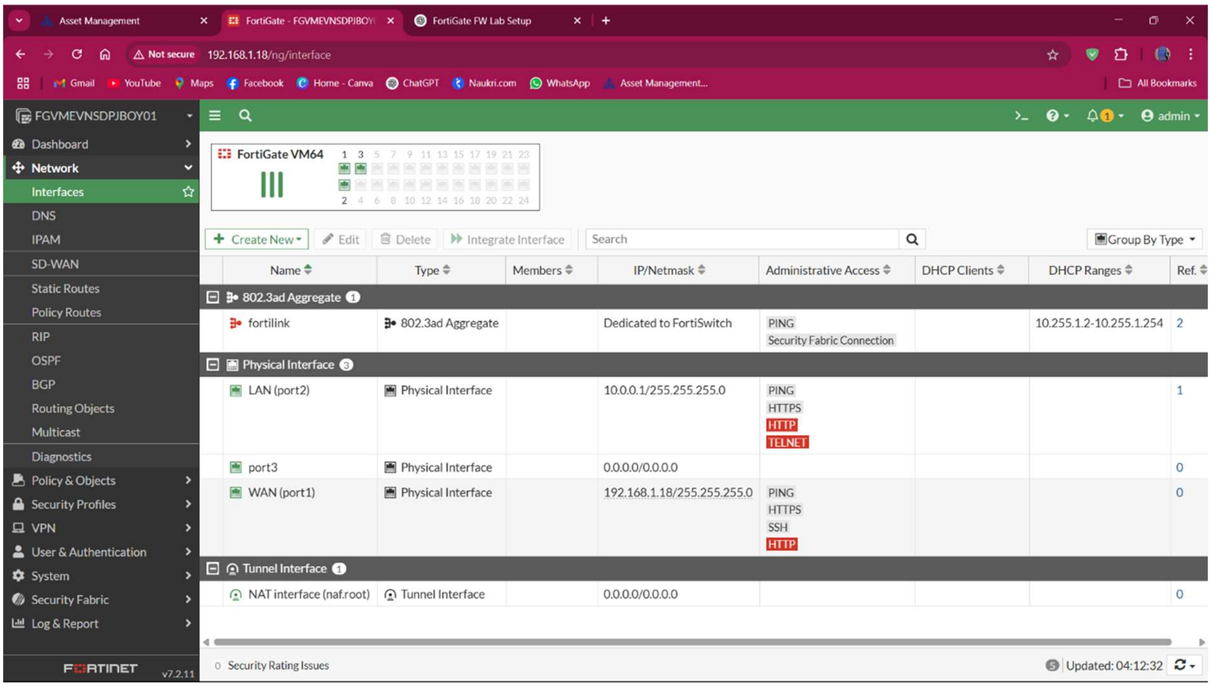
Step 5: Create Firewall Policy for Internet Access (GUI Mode)

A firewall policy allows internal traffic to reach the internet while applying NAT.

- Navigate to Policy & Objects > Firewall Policy.
- Click Create New.
- Name: allow-internet
- Incoming Interface: port2

- Outgoing Interface: port1
- Source: all
- Destination: all
- Schedule: always
- Service: ALL_ICMP
- Action: ACCEPT
- NAT: Enabled
- Save and apply the policy.

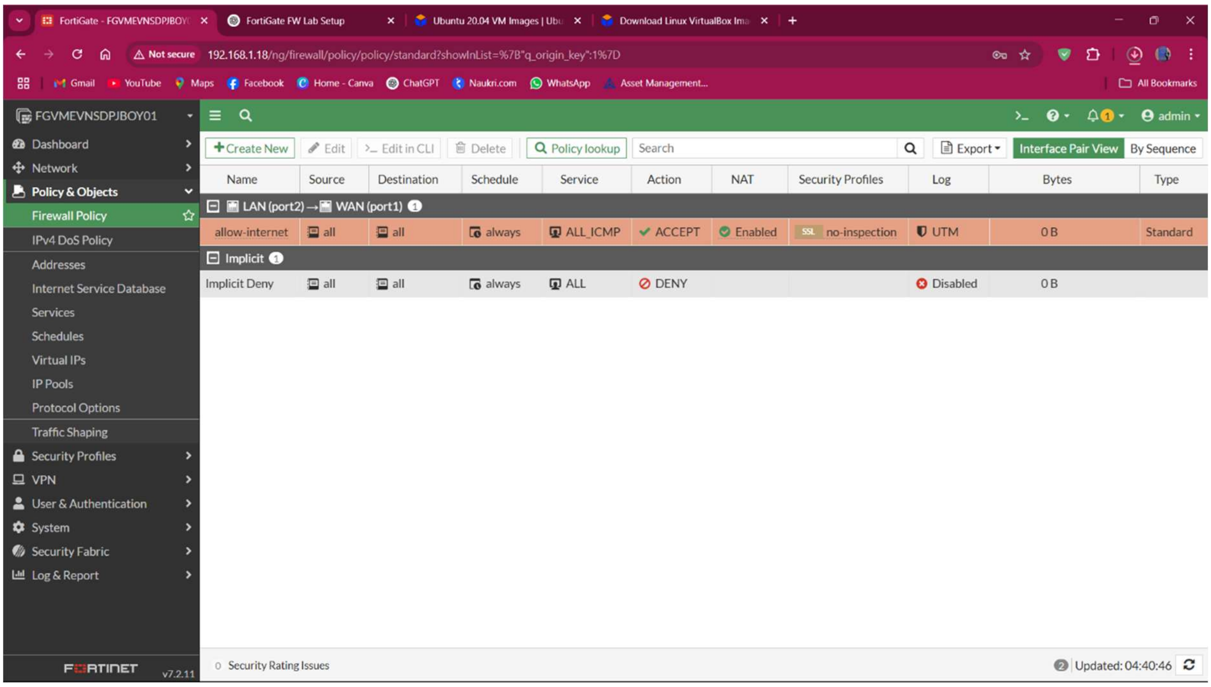
This policy allows outbound traffic from the internal LAN segment to the internet via NAT, ensuring internal IPs remain hidden from the external network.



192.168.1.18/ng/interface

Name	Type	Members	IP/Netmask	Administrative Access	DHCP Clients	DHCP Ranges	Ref.
802.3ad Aggregate 1							
fortilink	802.3ad Aggregate		Dedicated to FortiSwitch	PING Security Fabric Connection		10.255.1.2-10.255.1.254	2
Physical Interface 3							
LAN (port2)	Physical Interface		10.0.0.1/255.255.255.0	PING HTTPS HTTP TELNET			1
port3	Physical Interface		0.0.0.0/0.0.0.0				0
WAN (port1)	Physical Interface		192.168.1.18/255.255.255.0	PING HTTPS SSH HTTP			0
Tunnel Interface 1							
NAT interface (naf.root)	Tunnel Interface		0.0.0.0/0.0.0.0				0

0 Security Rating Issues   5 Updated: 04:12:32



192.168.1.18/ng/firewall/policy/policy/standard?showInList=%7B"q_origin_key":1%7D

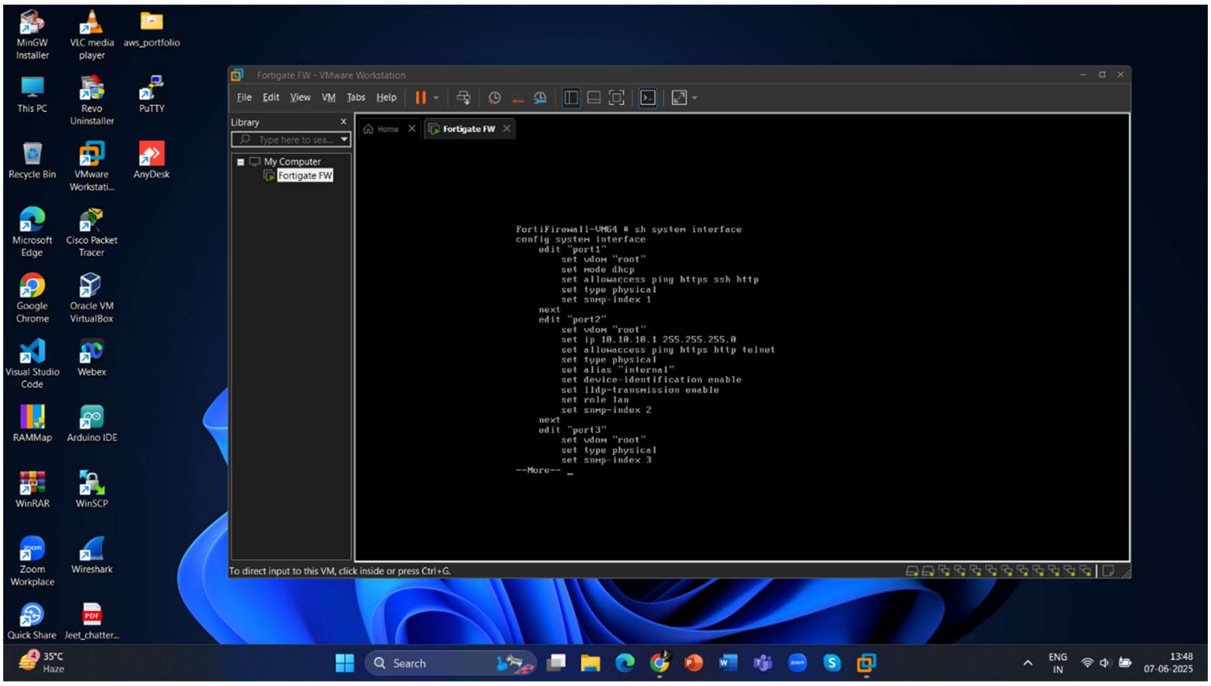
Name	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log	Bytes	Type
LAN (port2) → WAN (port1) 1										
allow-internet	all	all	always	ALL_ICMP	✓ ACCEPT	Enabled	SSL no-inspection	UTM	0 B	Standard
Implicit 1										
Implicit Deny	all	all	always	ALL	DENY			Disabled	0 B	

0 Security Rating Issues   2 Updated: 04:40:46

❖ RESULT & DISCUSSION

Step 1: Verify Configuration

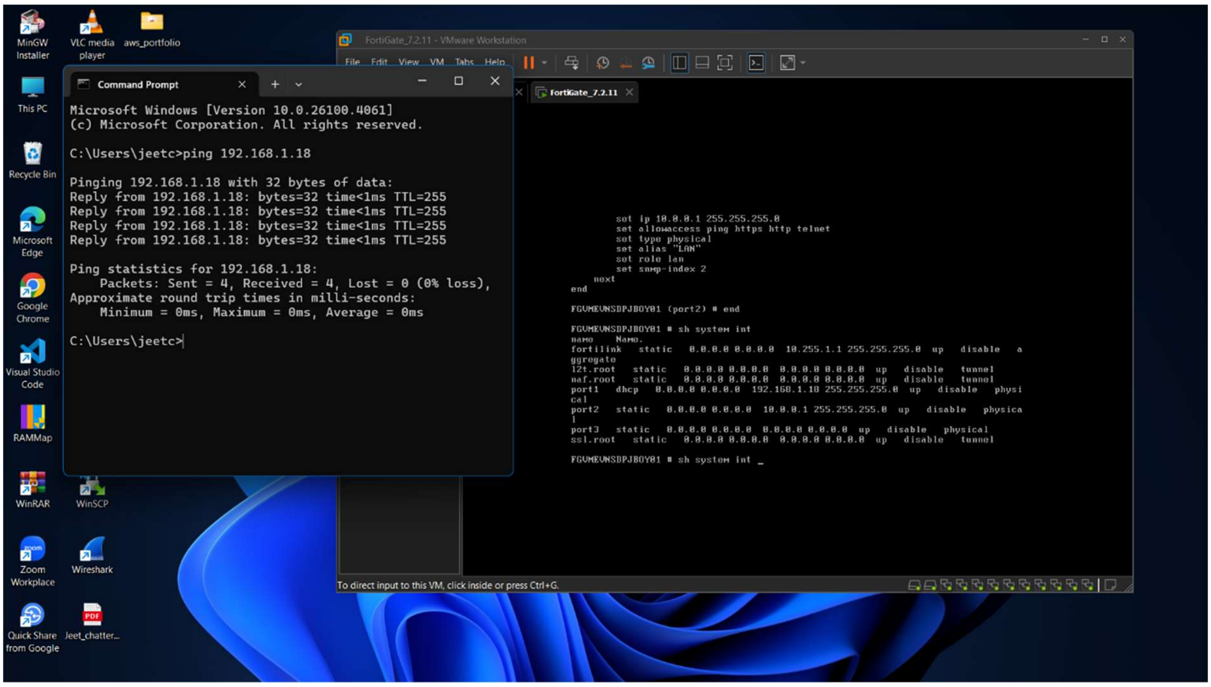
The “show system interface” command shows the configuration of interfaces.



```
FortiFirewall-VM64 # sh system interface
config system interface
    edit "port1"
        set vdom "root"
        set mode dhcp
        set allowaccess ping https ssh http
        set type physical
        set snmp-index 1
    next
    edit "port2"
        set vdom "root"
        set ip 10.10.10.1 255.255.255.0
        set allowaccess ping https http telnet
        set type physical
        set alias "internal"
        set device-identification enable
        set lldp-transmission enable
        set role lan
        set snmp-index 2
    next
    edit "port3"
        set vdom "root"
        set type physical
        set snmp-index 3
--More-- _
```

Step 2: Verify Connectivity with Internet

We have verified connectivity by executing the ping command. From the firewall interface we have pinged the gateway using the command “execute ping 192.168.1.1. and the connectivity with bridge is verified by pinging the firewall from Admin Laptop.

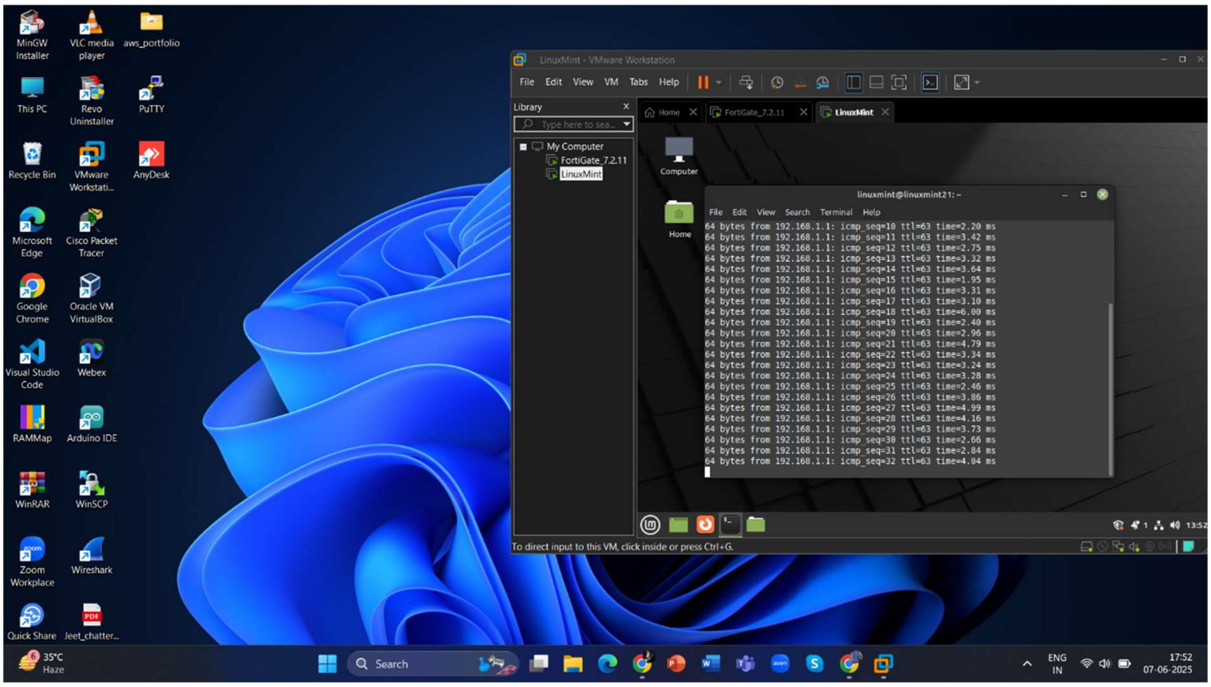


```
Microsoft Windows [Version 10.0.26100.4061]
(c) Microsoft Corporation. All rights reserved.

C:\Users\jeetc>ping 192.168.1.18

Pinging 192.168.1.18 with 32 bytes of data:
Reply from 192.168.1.18: bytes=32 time<1ms TTL=255
Reply from 192.168.1.18: bytes=32 time<1ms TTL=255
Reply from 192.168.1.18: bytes=32 time<1ms TTL=255
Reply from 192.168.1.18: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.1.18:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\jeetc>
```

```
        set ip 10.0.0.1 255.255.255.0
        set allowaccess ping https http telnet
        set type physical
        set alias "LAN"
        set role lan
        set snmp-index 2
    next
end

FGVMEVNSDPJBOY01 (port2) # end

FGVMEVNSDPJBOY01 # sh system int
name    Name.
fortilink   static   0.0.0.0 0.0.0.0  10.255.1.1 255.255.255.0  up   disable   a
ggregate
l2t.root   static   0.0.0.0 0.0.0.0  0.0.0.0 0.0.0.0  up   disable   tunnel
naf.root   static   0.0.0.0 0.0.0.0  0.0.0.0 0.0.0.0  up   disable   tunnel
port1   dhcp   0.0.0.0 0.0.0.0  192.168.1.18 255.255.255.0  up   disable   physi
cal
port2   static   0.0.0.0 0.0.0.0  10.0.0.1 255.255.255.0  up   disable   physica
l
port3   static   0.0.0.0 0.0.0.0  0.0.0.0 0.0.0.0  up   disable   physical
ssl.root   static   0.0.0.0 0.0.0.0  0.0.0.0 0.0.0.0  up   disable   tunnel

FGVMEVNSDPJBOY01 # sh system int _
```

Step 3: Verify Connectivity of LAN to internet

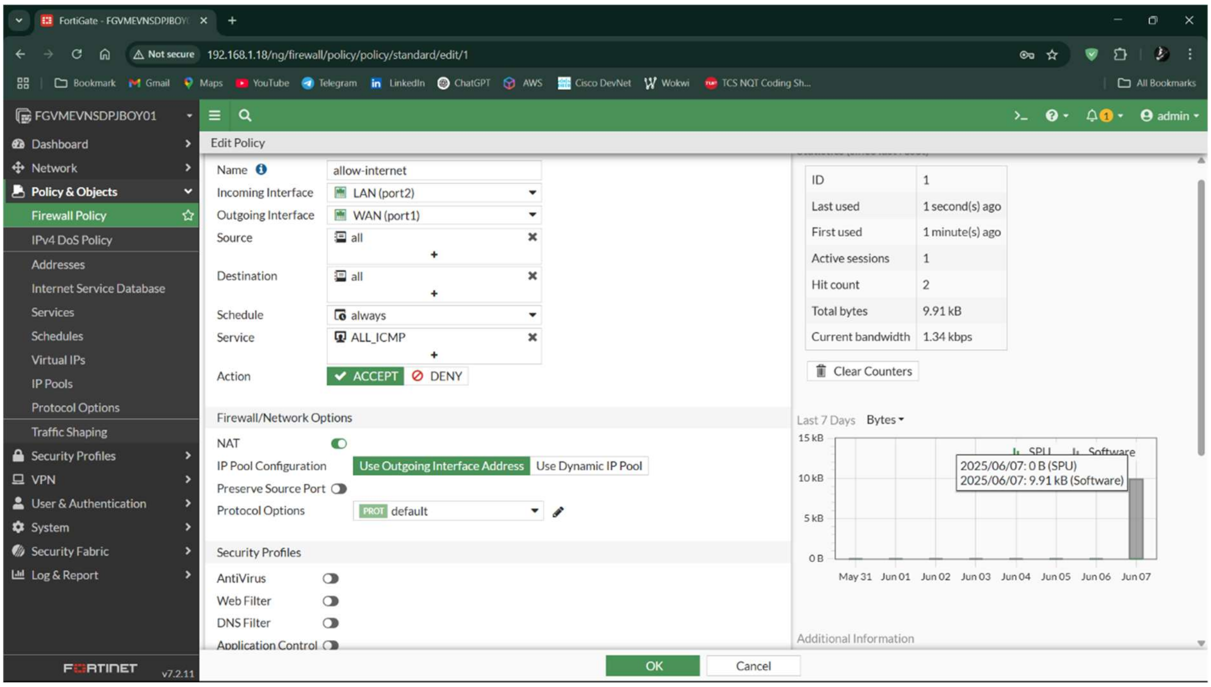
The firewall blocks the ping until the firewall policy is assigned. After assigning the policy Local PC from the LAN can ping the gateway.



linuxmint@linuxmint21: ~

```
64 bytes from 192.168.1.1: icmp_seq=10 ttl=63 time=2.20 ms
64 bytes from 192.168.1.1: icmp_seq=11 ttl=63 time=3.42 ms
64 bytes from 192.168.1.1: icmp_seq=12 ttl=63 time=2.75 ms
64 bytes from 192.168.1.1: icmp_seq=13 ttl=63 time=3.32 ms
64 bytes from 192.168.1.1: icmp_seq=14 ttl=63 time=3.64 ms
64 bytes from 192.168.1.1: icmp_seq=15 ttl=63 time=1.95 ms
64 bytes from 192.168.1.1: icmp_seq=16 ttl=63 time=3.31 ms
64 bytes from 192.168.1.1: icmp_seq=17 ttl=63 time=3.10 ms
64 bytes from 192.168.1.1: icmp_seq=18 ttl=63 time=6.00 ms
64 bytes from 192.168.1.1: icmp_seq=19 ttl=63 time=2.40 ms
64 bytes from 192.168.1.1: icmp_seq=20 ttl=63 time=2.96 ms
64 bytes from 192.168.1.1: icmp_seq=21 ttl=63 time=4.79 ms
64 bytes from 192.168.1.1: icmp_seq=22 ttl=63 time=3.34 ms
64 bytes from 192.168.1.1: icmp_seq=23 ttl=63 time=3.24 ms
64 bytes from 192.168.1.1: icmp_seq=24 ttl=63 time=3.28 ms
64 bytes from 192.168.1.1: icmp_seq=25 ttl=63 time=2.46 ms
64 bytes from 192.168.1.1: icmp_seq=26 ttl=63 time=3.86 ms
64 bytes from 192.168.1.1: icmp_seq=27 ttl=63 time=4.99 ms
64 bytes from 192.168.1.1: icmp_seq=28 ttl=63 time=4.16 ms
64 bytes from 192.168.1.1: icmp_seq=29 ttl=63 time=3.73 ms
64 bytes from 192.168.1.1: icmp_seq=30 ttl=63 time=2.66 ms
64 bytes from 192.168.1.1: icmp_seq=31 ttl=63 time=2.84 ms
64 bytes from 192.168.1.1: icmp_seq=32 ttl=63 time=4.04 ms
```

To direct input to this VM, click inside or press Ctrl+G.



192.168.1.18/ng/firewall/policy/policy/standard/edit/1

Edit Policy

Name	allow-internet
Incoming Interface	LAN (port2)
Outgoing Interface	WAN (port1)
Source	all
Destination	all
Schedule	always
Service	ALL_ICMP
Action	✓ ACCEPT ⊘ DENY

Firewall/Network Options

NAT	●
IP Pool Configuration	Use Outgoing Interface Address / Use Dynamic IP Pool
Preserve Source Port	○
Protocol Options	PROT default

Security Profiles

AntiVirus	○
Web Filter	○
DNS Filter	○
Application Control	○

ID	1
Last used	1 second(s) ago
First used	1 minute(s) ago
Active sessions	1
Hit count	2
Total bytes	9.91 kB
Current bandwidth	1.34 kbps

2025/06/07: 0 B (SPU)
2025/06/07: 9.91 kB (Software)

❖ CONCLUSION

The firewall configuration was completed successfully. The LAN users were able to obtain IP addresses automatically, and all policy rules enforced the intended traffic behavior. Internet access was confirmed, and NAT worked flawlessly. The GUI proved effective for visualizing traffic and debugging any issues.