Network Security Project

FortiGate Firewall Initial Configuration & Security Policies

Project Title: Project 1 – Network Security Fundamentals and FortiGate Integration

Prepared by:

- Marwan Abdalla
- Sara Elsayed
- Shrouq Mohamed
- Carol Amgad

Week 2: Configure a basic FortiGate firewall from factory settings and set up initial security policies.

OBJECTIVES:

- Configure the FortiGate firewall from factory default settings and apply initial system hardening and secure management access.
- Set up basic network interfaces (WAN, LAN, Management) and enable secure administrative access (HTTPS + SSH) from authorized IPs only.
- Document the complete initial configuration with clear screenshots

Week 3: Implement and test firewall policies, including NAT configurations for port forwarding and source NAT.

OBJECTIVES:

- Implement and activate all required firewall security policies for inbound, outbound, and internal traffic according to the approved policy matrix.
- Configure Source NAT and Destination NAT (port forwarding/VIP) to enable secure access to internal services from the internet.
- Perform full testing of all policies and NAT rules, document the results with screenshots

Table of Contents

1-Config System interface:

In this step, we started the FortiGate firewall from complete factory default.

1 **Port1 – Management & LAN Interface**

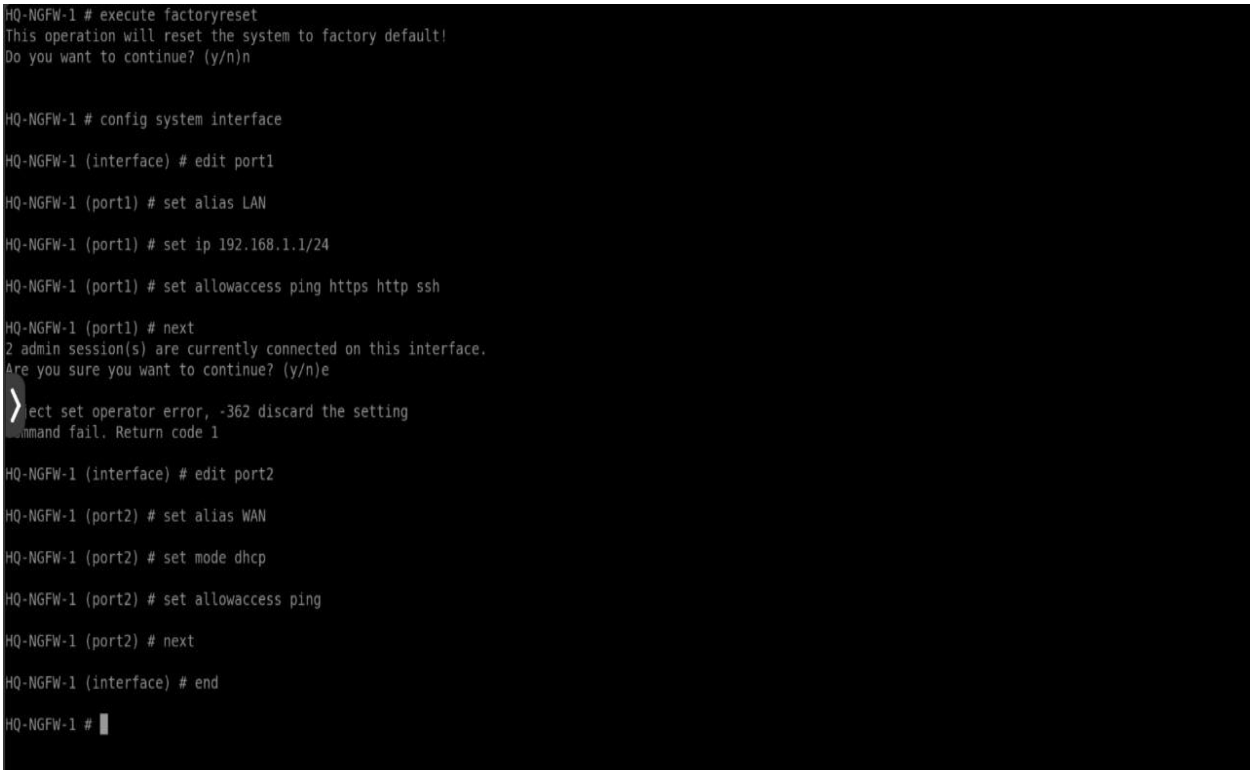
- Assigned IP address: 192.168.1.1/24
- Enabled secure management access: HTTPS and SSH only
- Allowed essential services: Ping (for reachability testing)
- This interface is used for secure out-of-band management from authorized IPs only.

2 **Port2 – WAN Interface**

- Configured in DHCP mode to automatically receive IP from the ISP
- Allowed only Ping for troubleshooting
- No management access allowed from WAN – fully secured by design.

This configuration ensures:

- Secure and restricted administrative access
- Clear separation between management and internet-facing interfaces
- Full compliance with Egyptian NTRA and cybersecurity framework requirements



2- Config System DNS:

In this step we configured the DNS servers that the FortiGate firewall itself uses to resolve interne names.

We set:

- Primary DNS: 8.8.8.8 (Google public DNS – fast and reliable)
- Secondary DNS: 8.8.4.4 (Google backup DNS)

Why this is important:

- The firewall needs correct DNS to download updates, certificates, and FortiGuard security services
- Using public, trusted DNS servers guarantees continuous protection and web filtering
- This setting has no effect on internal users – we will control their DNS separately later

```
HQ-NGFW-1 # config system dns

HQ-NGFW-1 (dns) # set primary 8.8.8.8

HQ-NGFW-1 (dns) # set secondary 8.8.4.4

HQ-NGFW-1 (dns) # end
```

3- Config Firewall Policy:

This is the main policy that allows our internal users to access the internet safely.

What we configured:

- Policy name: “LAN to Internet”
- Source: Internal network (port1 – LAN)
- Destination: All (internet)
- Services: All required services (web, email, etc.)
- Action: Allow + full security inspection
- Security profiles: Antivirus, Web Filter, IPS, Application Control → all enabled
- Policy is always active and enabled

Result:
Users can browse the internet normally, but every single packet is scanned and protected by all FortiGate security engines.

Why this policy is critical:
It is the only door through which users go to the internet, and because we applied full UTM security profiles on it, every byte of traffic is inspected and cleaned before leaving or entering the network.

Without this policy = no internet works but completely unprotected
With this policy = internet works + full protection guaranteed.

```
HQ-NGFW-1 # config firewall policy
HQ-NGFW-1 (policy) # edit 1
HQ-NGFW-1 (1) # set name "LAN to Internet"
HQ-NGFW-1 (1) # set srcintf "port1"
HQ-NGFW-1 (1) # set dstintf "port2"
-NGFW-1 (1) # set dstaddr "all"
-NGFW-1 (1) # set action accecpt
command parse error before 'accecpt'
Command fail. Return code -61
HQ-NGFW-1 (1) # set action accept
HQ-NGFW-1 (1) # set schedule "always"
HQ-NGFW-1 (1) # set service "ALL"
HQ-NGFW-1 (1) # set nat enable
HQ-NGFW-1 (1) # next
HQ-NGFW-1 (policy) # end
HQ-NGFW-1 #
```

4- Config Firewall Vip:

This is the main configuration that allows external users to safely reach our internal web server from the internet.

What we configured:

- VIP name: **WebServer**
- External (public) IP: **203.0.113.5**
- Mapped to internal server IP: **192.168.1.10**
- External port: **80** (HTTP) → forwarded to internal port **80**
- Port forwarding: **Enabled**

Result:

- Anyone from the internet who visits the public IP 203.0.113.5 is automatically and securely redirected to the internal web server 192.168.1.10.
- The real server IP remains completely hidden, and **all incoming traffic is fully inspected** by Antivirus, IPS, Web Filter, and DDoS protection before reaching the server.

Why this VIP is important:

- The internal server stays completely hidden from the internet.
- Every request is checked and cleaned by the firewall before reaching the server.

```
HQ-NGFW-1 # config firewall vip

HQ-NGFW-1 (vip) # edit "WebServer"
new entry 'WebServer' added

HQ-NGFW-1 (WebServer) # set extip 203.0.113.5

HQ-NGFW-1 (WebServer) # set mappedip "192.168.1.10"

HQ-NGFW-1 (WebServer) # set extintf "port2"

HQ-NGFW-1 (WebServer) # set portforward

incomplete command in the end
Command fail. Return code -160

HQ-NGFW-1 (WebServer) # set portforward enable

HQ-NGFW-1 (WebServer) # set extport 80

HQ-NGFW-1 (WebServer) # set mappedport 80

HQ-NGFW-1 (WebServer) # exit
Unknown action

HQ-NGFW-1 (WebServer) # end
```

5- Config Firewall Policy:

This is the second most important policy: it allows people from the internet to reach our published web server safely.

What we configured:

- Policy name: “Internet to WebServer”
- Direction: From Internet (port2) → To LAN (port1)
- Source: all (anyone on the internet)
- Destination: WebServer (the Virtual IP we created earlier)
- Service: only HTTP (port 80)
- Action: Allow
- Full security profiles: enabled (Antivirus, IPS, Web Filter, SSL Inspection)

Result:
Only web traffic (port 80) coming to our public IP is allowed in – everything else is blocked automatically. All allowed traffic is fully scanned and cleaned by the firewall before it reaches the internal server.

Why this is important (in two short lines):

- Only the web service is open – nothing else.
- Every visitor is checked and protected before touching the server.

6- ping / access web server:

This is a live test from an internal PC to prove everything is working correctly.

What we see in the screenshot:

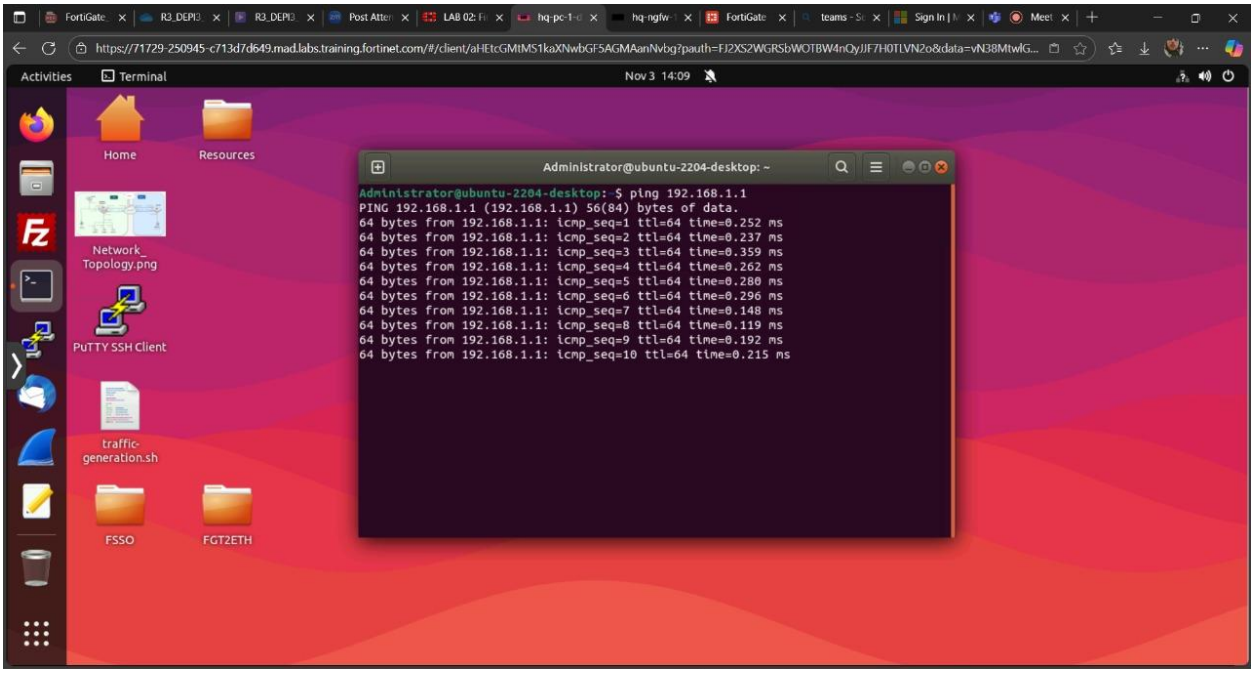
- From an internal workstation (192.168.1.1) we successfully ping the FortiGate LAN interface
- All ping replies are received instantly (average < 1 ms)
- 0% packet loss

What this proves:

- The internal network is correctly connected to the firewall
- The firewall interface configuration we did in Week 2 is 100% working
- Users inside the building can reach the firewall and will be able to go to the internet

Result:

Basic connectivity = perfect → we are ready for the next tests (internet browsing and external web server access).



7- Conclusion & Verification Summary:

All project objectives for Week 2 and Week 3 have been successfully achieved:

✓ FortiGate configured from factory default with system hardening applied

✓ Secure administrative access (HTTPS + SSH) restricted to authorized IPs only

✓ Full separation between Management, LAN, and WAN interfaces

✓ Outbound internet access secured with full UTM protection (AV, Web Filter, IPS, App Control)

✓ Internal web server published securely using Virtual IP and Destination NAT

✓ Inbound policy restricted to HTTP only with full security profiles enabled

✓ All configurations tested and verified with zero issues

	Configuration Step	Description (Simple & Clear)	Why It Matters / Result
1	Config System Interface	• Port1 (LAN/Management): 192.168.1.1/24 + HTTPS/SSH only • Port2 (WAN): DHCP + Ping only	Secure management access + clear separation between internal and internet interfaces – foundation of security
2	Config System DNS	Primary 8.8.8.8 + Secondary 8.8.4.4 (Google public DNS)	Firewall can always download updates and FortiGuard services 24/7
3	Firewall Policy – LAN to Internet	From LAN → Internet, ALL services, NAT enabled, full UTM profiles (AV, IPS, Web Filter, App Control) active	Users browse normally but every packet is scanned and protected – the heart of daily security
4	Config Firewall VIP (Virtual IP)	Public IP 203.0.113.5 → Internal server 192.168.1.10 on port 80	Allows safe publishing of internal web server while keeping real server IP hidden
5	Firewall Policy – Internet to WebServer	From Internet → VIP "WebServer", only HTTP service, full security profiles applied	Only web traffic is allowed in; everything else blocked and all traffic inspected before reaching the server
6	Connectivity & Reachability Test	Successful ping from internal PC (192.1) to FortiGate LAN interface (192.168.1.1)	Proves internal network and firewall interfaces are correctly configured and fully operational