



Network Security Fundamentals & FortiGate Integration

Building a Resilient, Segmented, and Secured Network Environment

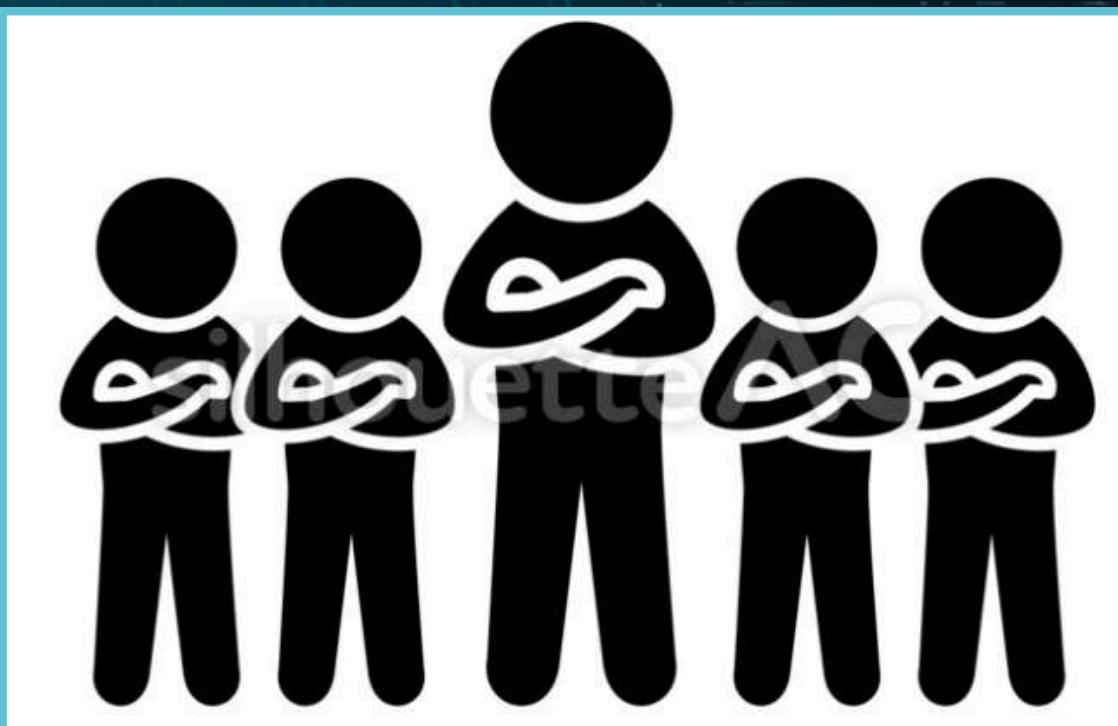
Date

November 25, 2025





Prepared By :



- **Abdullah Ashraf Saber**
- **Marawan Mohamed Abdelfattah**
- **Mazen Mohamed Fathy**
- **Noor Hussain Mwafi**
- **Omar Mohamed Abdelrahman El-Sayed Amer**



Project Overview



- **Project Name:** Network Security Fundamentals and FortiGate Integration
- **Goal:** Build a secure and segmented network using FortiGate Firewall
- **Focus Areas:**
 - Threat analysis
 - FortiGate deployment
 - NAT & Firewall policies
 - Web Filtering



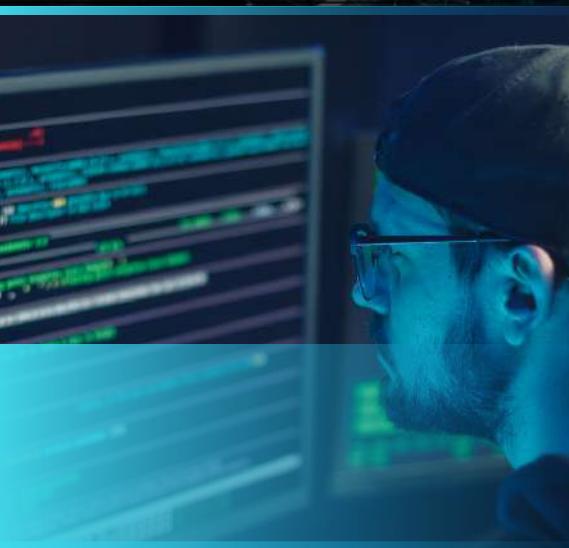
Project Goals & Objectives

1. GOALS:

- Establish a strong security posture
- Deploy a secure NGFW environment
- Control inbound and outbound traffic

2. OBJECTIVES:

- Analyze cyber threats
- Configure FortiGate VM
- Implement NAT & Firewall rules





WEEK 1

Network Security Fundamentals



Studied modern cyber threats:

- Ransomware (RaaS)
- Phishing Attacks
- Analyzed vulnerabilities:
- Unpatched systems
- Misconfigurations
- Human errors



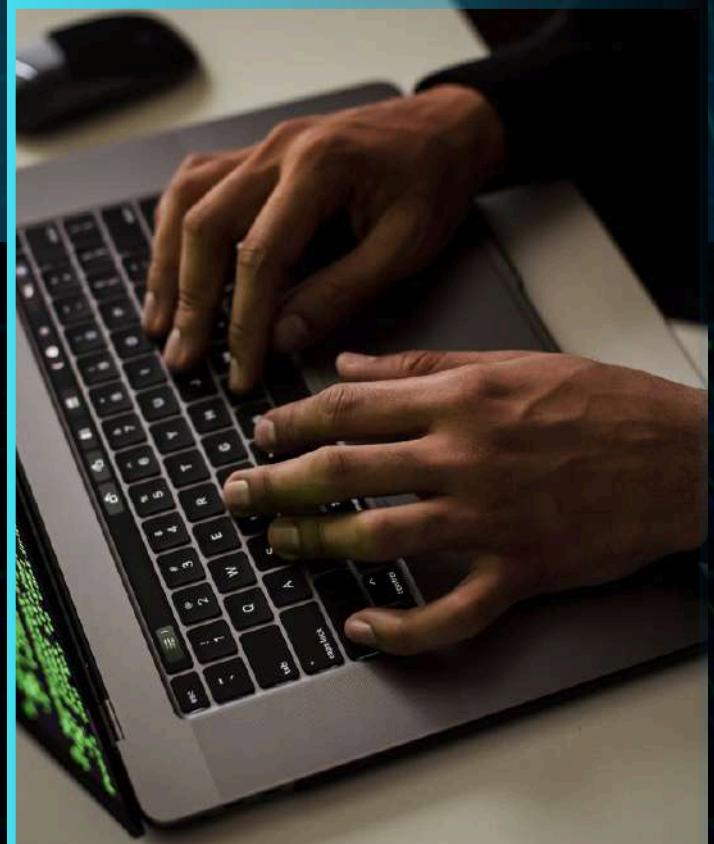
Security Models Used



- **Zero Trust Architecture**
- → “Never trust, always verify”
- **Network Segmentation**
- → Isolating critical systems using firewall rules and VLANs



(Security Awareness) Human Firewall



1. Phishing Awareness
2. Strong Passwords & MFA
3. Social Engineering Protection
4. Secure Data Handling





WEEK 2

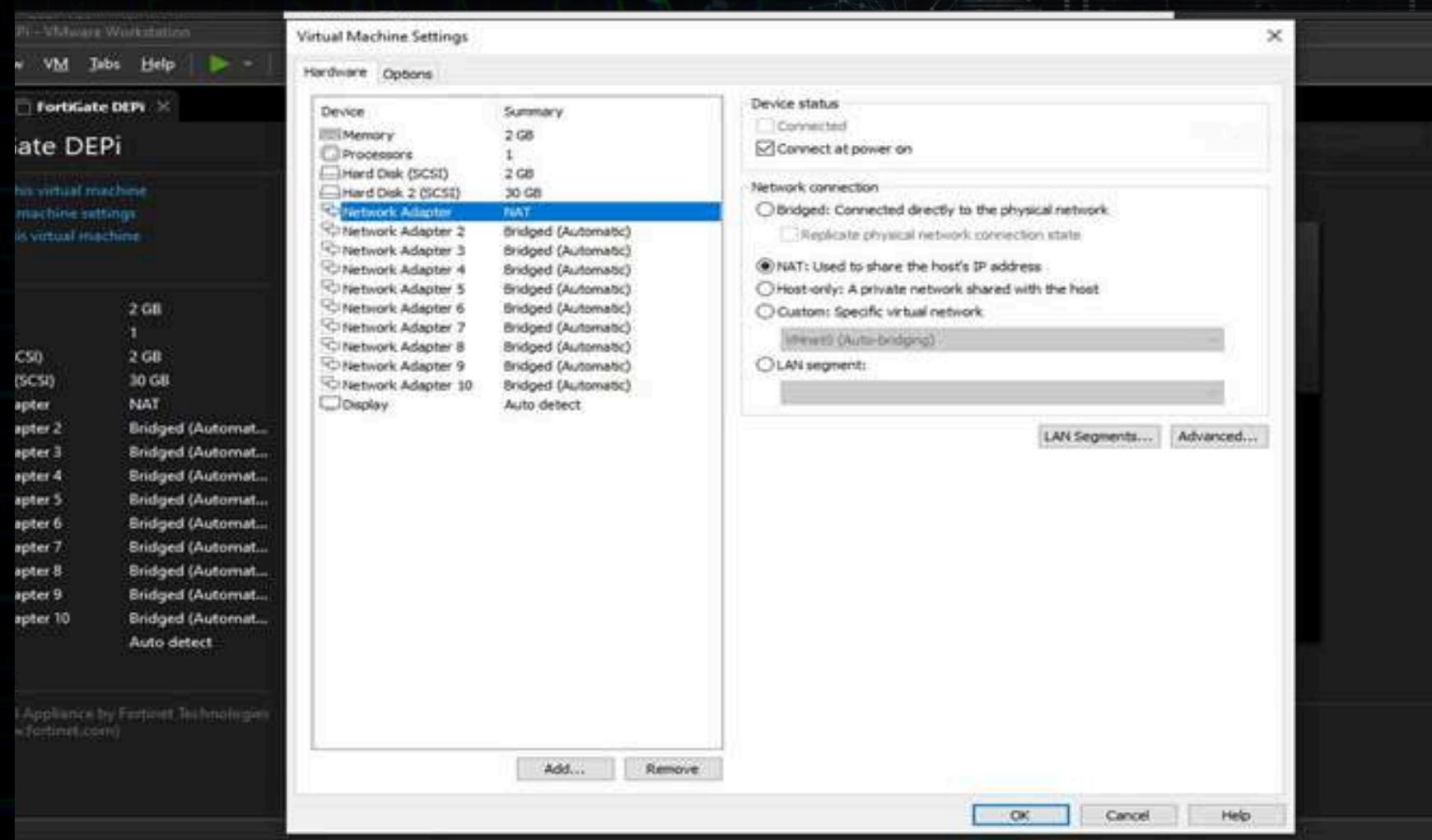
FortiGate Deployment & Initial Configuration

- Deploying FortiGate VM in lab environment
- Configuring management access (CLI & GUI)
- Setting up LAN/WAN interfaces
- Creating initial routing
- Building the first firewall policy





FortiGate VM Deployment



- Imported FortiGate .ovf template into VMware
- Allocated correct resources based on license
- Named VM: FortiGate-DEPI

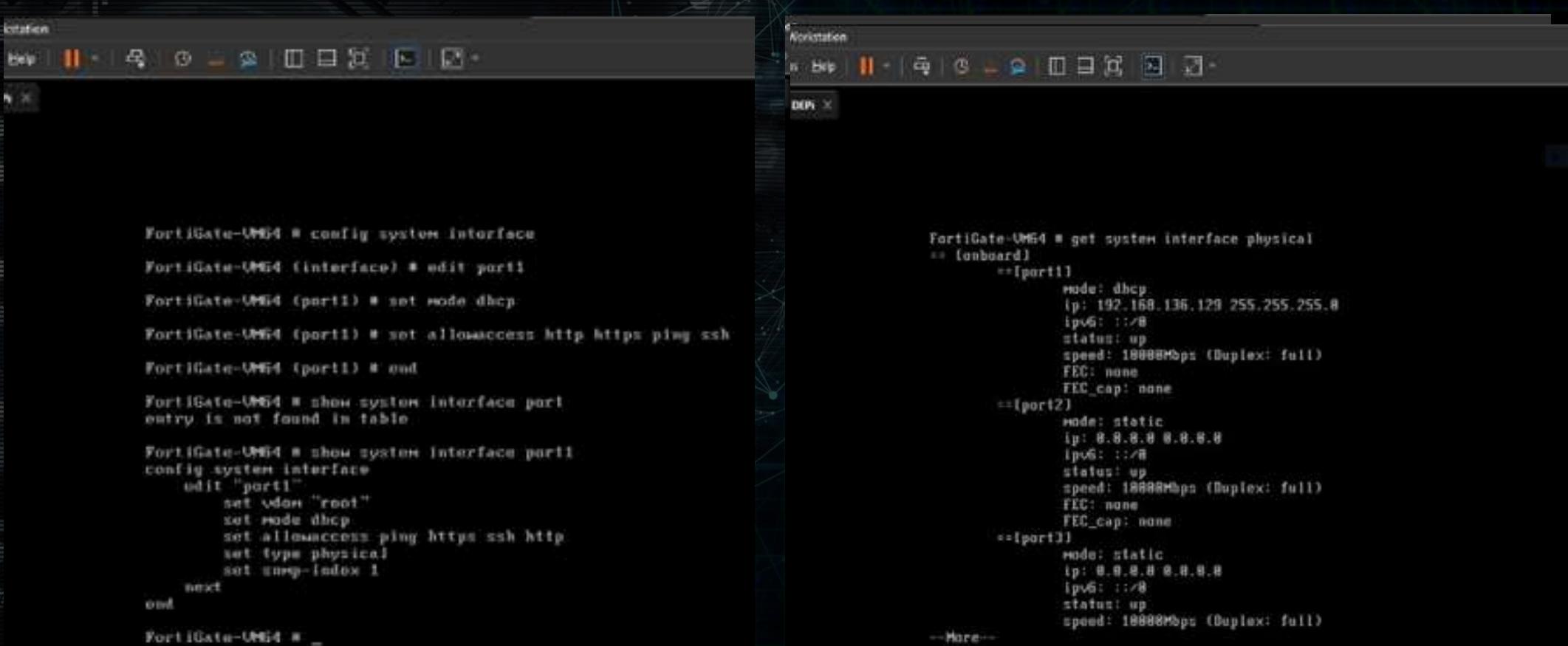
Screenshot verifying the CPU and RAM allocation within the VMware Workstation settings, confirming compliance with license restrictions.





Initial CLI Configuration (Management Access)

- Used default credentials to access CLI
- Configured port1 (management interface)
- Enabled: HTTPS, HTTP, SSH, PING
- Set port1 to DHCP to get automatic IP



```
FortiGate-VM64 # config system interface
FortiGate-VM64 (interface) # edit port1
FortiGate-VM64 (port1) # set mode dhcp
FortiGate-VM64 (port1) # set allowaccess http https ping ssh
FortiGate-VM64 (port1) # end
FortiGate-VM64 # show system interface port
entry is not found in table
FortiGate-VM64 # show system interface port
config system interface
edit "port1"
set vdom "root"
set mode dhcp
set allowaccess ping https ssh http
set type physical
set unsg-index 1
next
end
FortiGate-VM64 # get system interface physical
=={port1}
node: dhcp
ip: 192.168.136.129 255.255.255.8
ipv6: ::/0
status: up
speed: 10000Mbps (Duplex: full)
FEC: none
FEC_cap: none
=={port2}
node: static
ip: 0.0.0.0 0.0.0.0
ipv6: ::/0
status: up
speed: 10000Mbps (Duplex: full)
FEC: none
FEC_cap: none
=={port3}
node: static
ip: 0.0.0.0 0.0.0.0
ipv6: ::/0
status: up
speed: 10000Mbps (Duplex: full)
More...
```

CLI Initialization and Management IP Verification. Command output showing the successful execution of configuration commands for port1 and the verification of the assigned DHCP IP address (e.g., 192.168.136.x)



Accessing the Web GUI

- Logged into GUI using assigned DHCP IP
- Changed hostname → DEPI-FortiGate
- Configured Time Zone “Cairo (GMT+2)”
- Synced NTP server for accurate logs

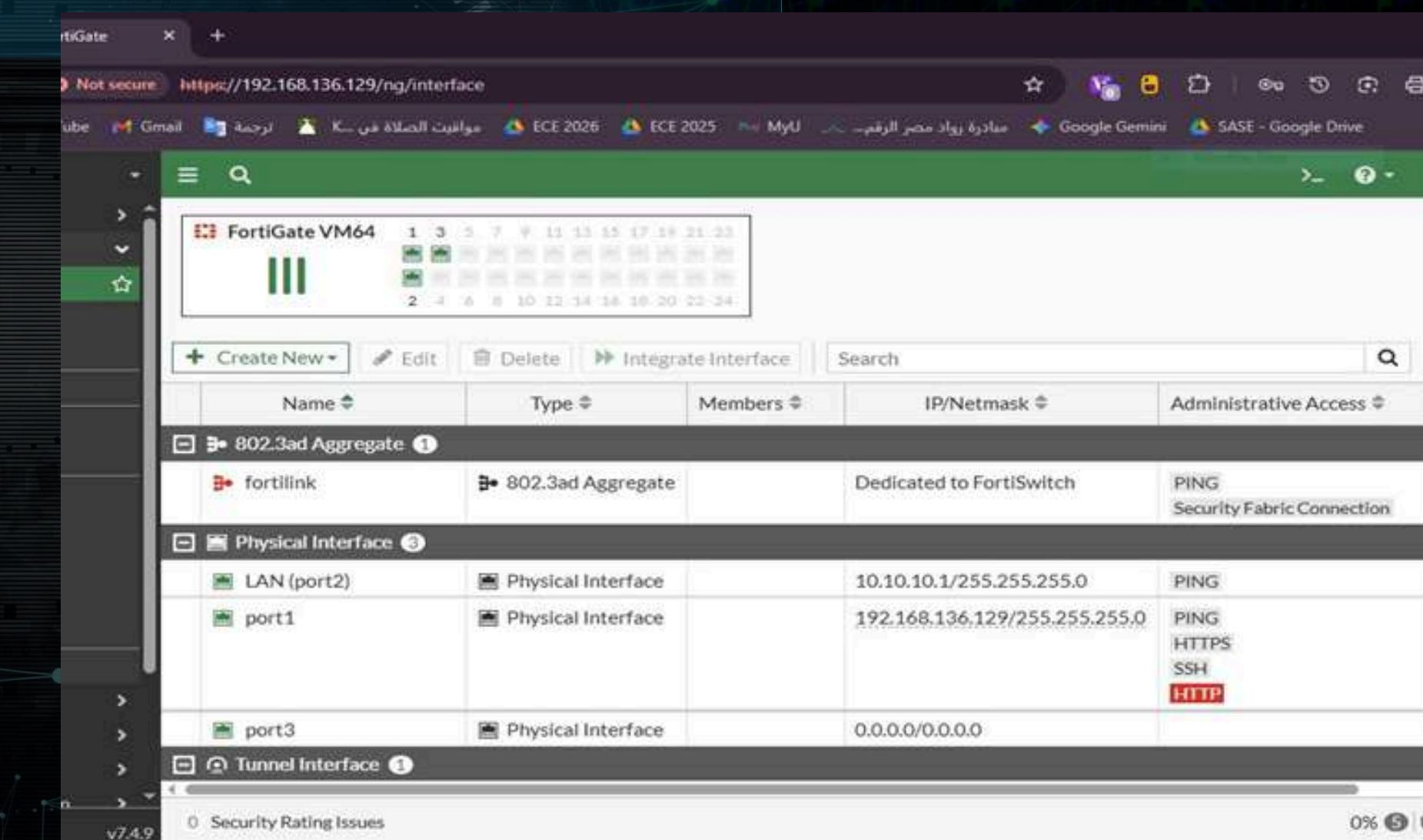
The screenshot shows the FortiGate Web GUI dashboard titled "DEPI-FortiGate". The left sidebar contains navigation links such as Dashboard, Status, Security, Network, Assets & Identities, WiFi, FortiView Sources, FortiView Destinations, FortiView Applications, FortiView Web Sites, FortiView Policies, FortiView Sessions, Network, Policy & Objects, Security Profiles, and VPN. The main content area displays "System Information" with details: Hostname: DEPI-FortiGate, Serial number: FGVMEVGNJV029Z3A, Firmware: v7.4.9 build2829 (Mature), Mode: NAT, System time: 2025/11/20 22:09:20, Uptime: 16m 4s, WAN IP: Unknown. Below this is the "FortiGate Cloud" section, which shows a status message: "Status: Not Supported". To the right, there are sections for "Licenses", "Security Fabric", "LAN Edge", and "Fabric Connectors". The "Security Fabric" section includes sub-sections for "Logging" and "FortiSandbox". The bottom of the screen shows the Fortinet logo and the version v7.4.9.





Network Interface Configuration

- port1 = WAN (DHCP)
- port2 = LAN (Static: 10.10.10.1/24)
- Enabled DHCP on port2 for internal hosts
- Segmentation established for internal network



GUI screenshot displaying the configured roles and static IP assignment for the LAN interface (port2) and the DHCP scope



Static Routing Configuration

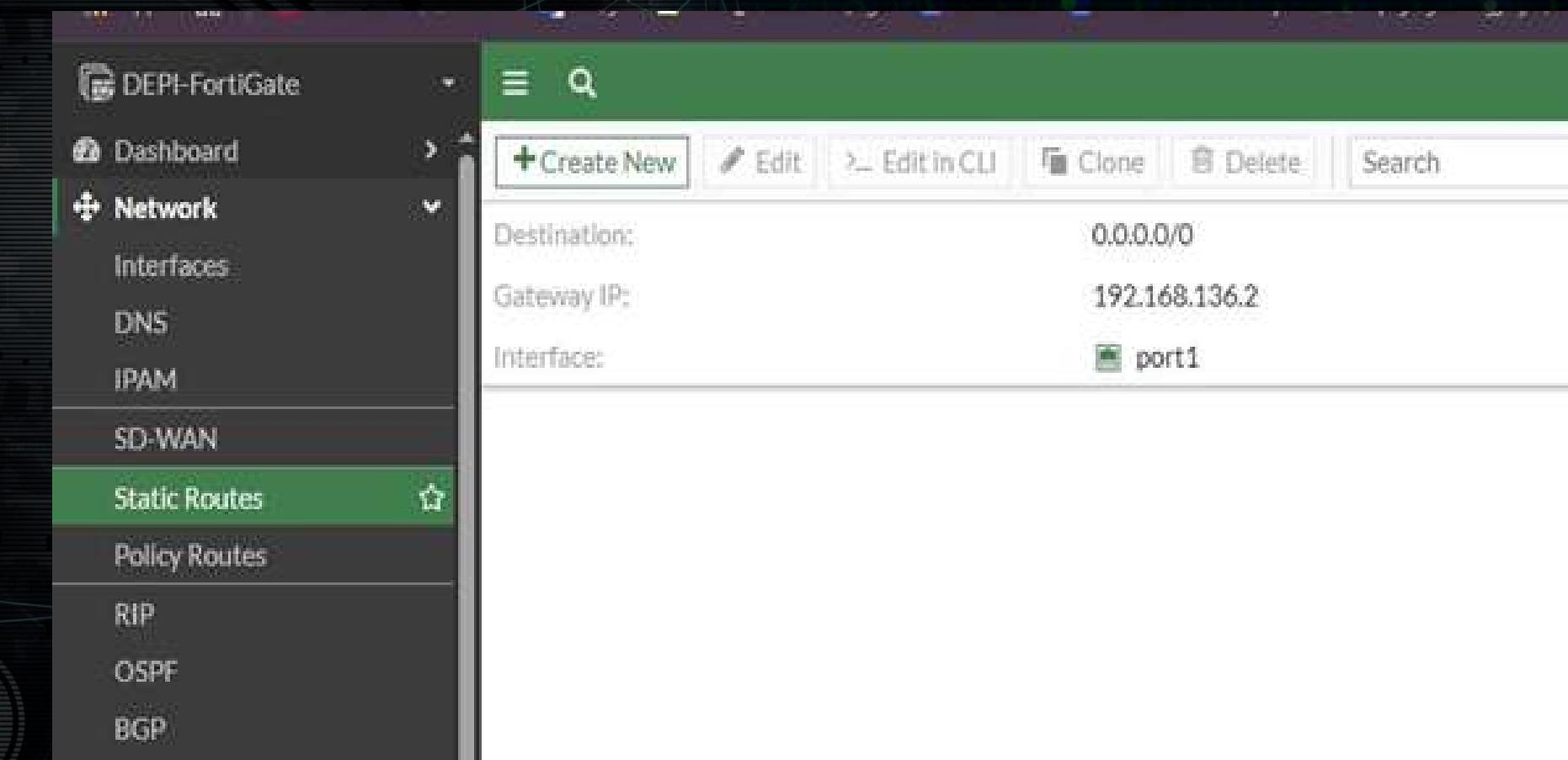
- Added default route for internet access

- Destination: 0.0.0.0/0

- Gateway: 192.168.136.2

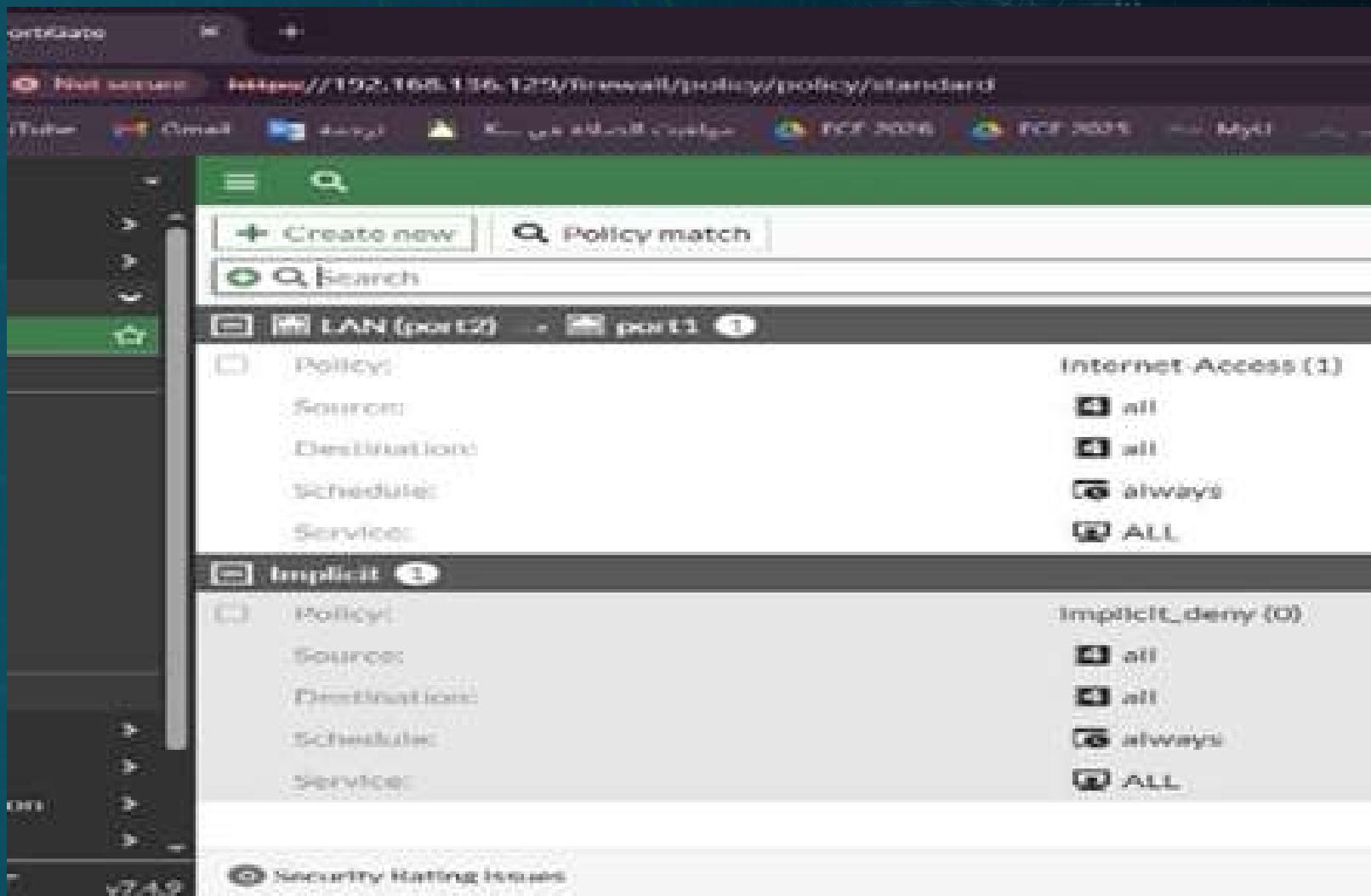
(VMware NAT gateway)

- Interface: port1 (WAN)

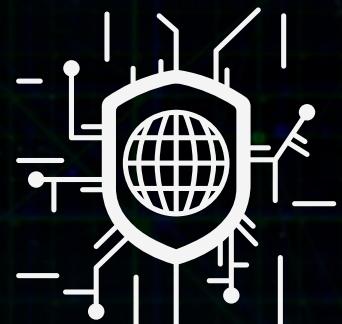


Screenshot from the Network -> Static Routes menu, confirming the 0.0.0.0/0 route pointing towards the correct Gateway via port1





Initial Firewall Policy Internet-Access



- Policy Name: Internet-Access
- Incoming: port2 (LAN)
- Outgoing: port1 (WAN)
- Action: Accept
- NAT Enabled (Source NAT)
- Logging: All Sessions

Initial Firewall Policy (Internet-Access) Details. Screenshot displaying the policy configuration, highlighting the enabled NAT feature and "All Sessions" logging setting.



Week 2 Summary

- Successfully deployed FortiGate VM
- Configured initial management & GUI settings
- Set up LAN/WAN segmentation
- Added default route
- Created first security policy enabling internet access





WEEK 3

Advanced Policies & NAT Implementation

1

Implemented
advanced NAT
rules
(SNAT & DNAT)

2

Applied
granular access
policies

3

Configured
Web
Filtering

4

Performed
full testing &
verification





Source NAT (SNAT) Outbound Traffic

- To allow LAN devices to access the internet
- SNAT is enabled within the "Internet-Access" policy
- To make all devices use a WAN IP address instead of a private IP address





SNAT Verification

- Checked Traffic Logs
- Source IP: 10.10.10.2
- Translated to WAN IP of port1
- Outbound browsing successful

The screenshot shows the Fortinet DEPI-FortiGate interface. The left sidebar menu includes: Dashboard, Network, Policy & Objects (selected), Firewall Policy, DoS Policy, Addresses, Internet Service Database, Services, Schedules, Virtual IPs, IP Pools, Protocol Options, Traffic Shaping, Security Profiles, VPN, User & Authentication, WiFi Controller, System, Security Fabric, and Log & Report. The main window displays the 'Edit Policy' dialog for a policy named 'LAN-to-WAN'. The policy details are as follows:

Setting	Value
Name	LAN-to-WAN
Incoming interface	LAN (port2)
Outgoing interface	port1
Source	all
Destination	all
Schedule	always
Service	ALL
Action	✓ ACCEPT ✘ DENY

Under 'Firewall/Network Options', the NAT settings are configured to use the outgoing interface address. Other options include:

- IP pool configuration: Use Outgoing Interface Address (selected) or Use Dynamic IP Pool
- Manage source port: Fixed port (selected) or Preserve source port
- Protocol options: PROT: default
- Security Profiles:
 - AntiVirus: Enabled
 - Web filter: WEB (selected) or Block-Social
 - DNS filter: Enabled

On the right side of the interface, there is a 'Statistics (since last reset)' section showing the following data:

ID	2
Last used	19m 26s ago
First used	2h 47m 1s ago
Active sessions	3
Hit count	983
Total bytes	597.69 MB

Below the statistics is a 'Current bandwidth 0 bps' message and a 'Clear Counters' button. A chart titled 'Last 7 Days Bytes' shows traffic distribution by protocol: nTurbo (green), SPU (orange), and Software (purple). The chart indicates a significant peak in Software traffic around the 22nd day of the month.



Destination NAT (DNAT) Inbound Access

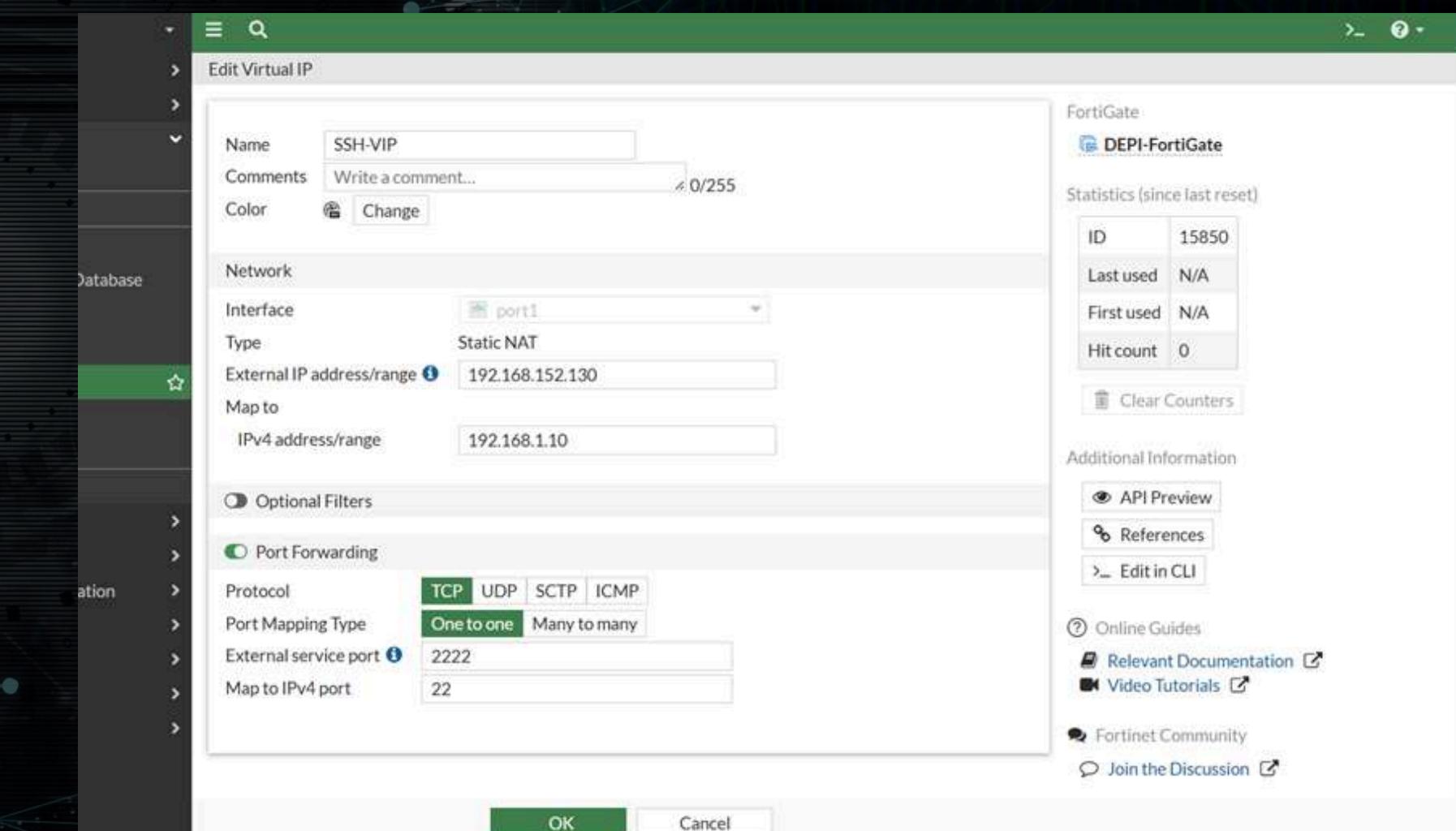
- To allow SSH access to the internal server
- Used Virtual IP (VIP) mapping
- External Port: 2222
Internal Port: 22





Virtual IP Configuration (DNAT)

- VIP Name: SSH-Server-VIP
- Interface: port1
- External IP → Internal IP mapping
- Port Forwarding Enabled (2222 → 22)

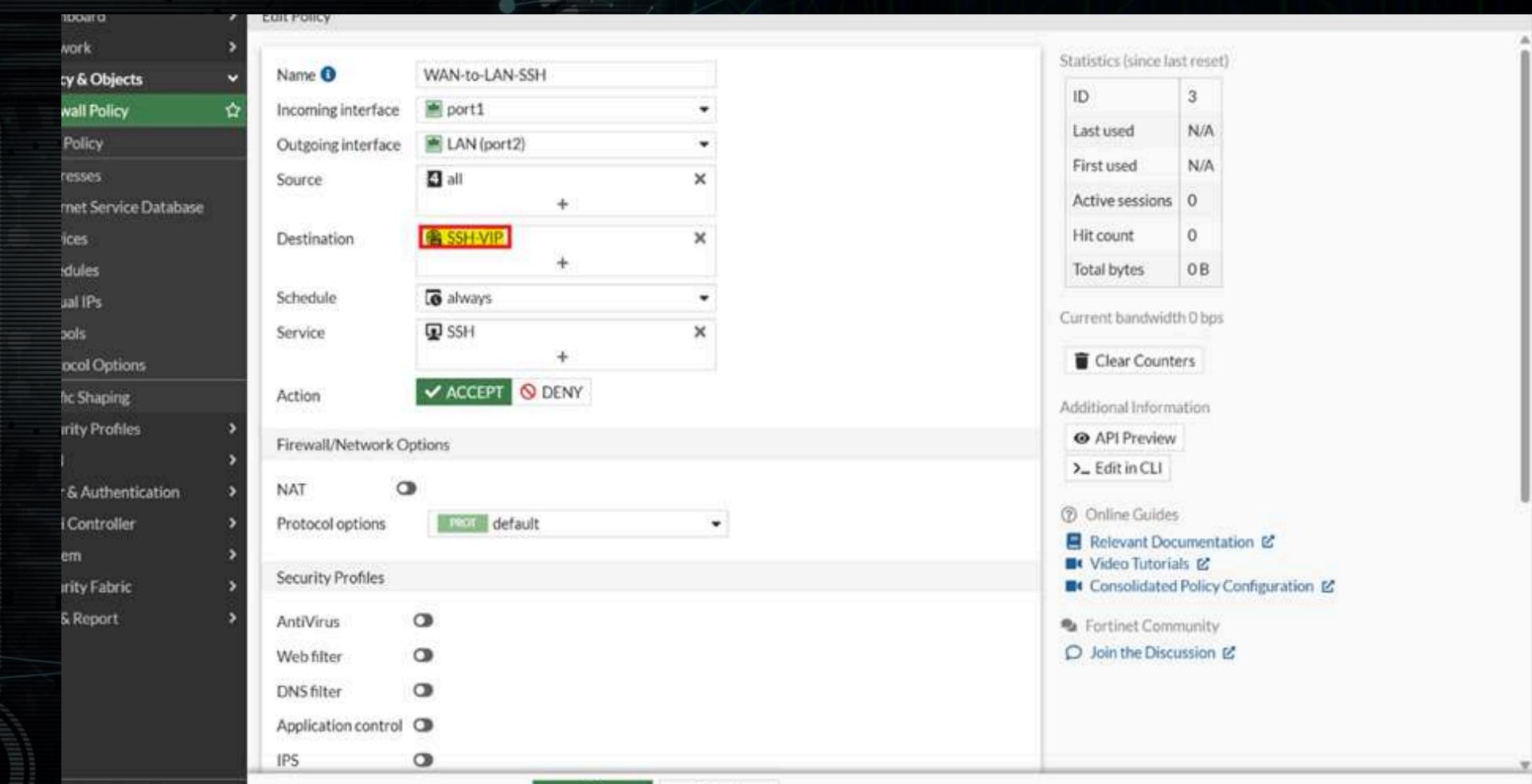


Destination NAT (DNAT) Virtual IP Creation. Configuration of the SSH-Server-VIP, mapping the External IP to the Mapped IP with port forwarding for TCP 2222 to 22.



Inbound SSH Access Policy

- Direction: WAN → LAN
- Destination: SSH-Server-VIP
- Service: SSH
- Action: ACCEPT
- NAT: Disabled
- (because DNAT already handled by VIP)



Inbound Service Access Policy. Firewall policy (WAN-to-LAN-SSH) allowing WAN-to-LAN traffic using the SSH-Server-VIP as the destination object.





Granular Access Control (Web-Only Policy)

- Created policy “LAN-Web-Only”
- Allows only: HTTP + HTTPS
- Blocks all other protocols (FTP / Telnet etc.)
- Demonstrates principle of Least Privilege

Edit Policy

Name	Internet-Access
Incoming interface	LAN (port2)
Outgoing interface	port1
Source	all
Destination	all
Schedule	always
Service	HTTP HTTPS
Action	ACCEPT DENY

Granular Access Control Policy. Firewall policy (Internet-Access) restricting internal outbound traffic to only HTTP and HTTPS services.





LICERIA & CO.

HOME

ABOUT

CONTENT

OTHERS

Web Filtering

Block Social Media

- Created profile “Block-Social”
- Blocked category: Social Networking
- Added Static URL Filters
- Protects users from risky content

The screenshot shows the 'Edit Web Filter Profile' dialog box. The profile is named 'Block-Social'. Under the 'Category Based Filter' section, the 'Allow users to override blocked categories' option is selected. In the 'Search Engines' section, 'Safe Search' is enforced on Google, Yahoo!, Bing, and Yandex. Under 'Static URL Filter', 'Block invalid URLs' is selected. The 'URL Filter' section is active, showing a table of static URL filters:

URL	Type	Action	Status
facebook.com	Wildcard	Block	Enable
youtube.com	Wildcard	Block	Enable
tiktok.com	Wildcard	Block	Enable

Below the table, there are sections for 'Block malicious URLs discovered by FortiSandbox' and 'Content Filter'. At the bottom right are 'OK' and 'Cancel' buttons. The version 'v7.4.9' is visible at the bottom left of the dialog.

Web Filtering Profile Configuration. Details of the Block-Social profile enforcing a block on specific static URLs and the Social Networking category





Applying Security Profile to Policy

Policy	Source	Destination	Schedule	Action	IP Pool	NAT	Type	Security Profiles	Log
LAN (port2) → port1 ②									
LAN-to-WAN (2)	4 all	4 all	⌚ always	ALL	✓ ACCEPT	✓ NAT	Standard	WEB Block-Social SSL certificate-inspection	All
Internet-Access (1)	4 all	4 all	⌚ always	ALL	✓ ACCEPT	✓ NAT	Standard	SSL no-inspection	All

- Added Web Filter to the outbound policy
- Ensures filtered browsing for LAN users
- Verified policy is applied correctly





SNAT Test — Result

- Browsed internet from LAN host
- Logs confirm IP translation
- SNAT is working correctly

Log Details				
Source	Device	Destination	Application Name	Result
10.10.10.2		91.189.91.157 (ntp.ubuntu...)	NTP	✓ Accept (76)
10.10.10.2		192.168.152.2	DNS	✓ Accept (31)
10.10.10.2		185.125.190.48 (connectivi...	HTTP	✓ Accept (26)
10.10.10.2		192.168.152.2	DNS	✓ Accept (30)
10.10.10.2		142.251.37.164 (www.goog...	udp/443	✓ Accept (11)
10.10.10.2		102.132.97.35 (www.faceb...	udp/443	✗ Deny (Deny)
10.10.10.2		102.132.97.35 (www.faceb...	udp/443	✗ Deny (Deny)
10.10.10.2		102.132.97.35 (www.faceb...	udp/443	✗ Deny (Deny)
10.10.10.2		102.132.97.35 (www.faceb...	udp/443	✗ Deny (Deny)
10.10.10.2		142.251.37.238 (youtube-ui...	udp/443	✓ Accept (6.8)
10.10.10.2		102.132.97.35 (www.faceb...	udp/443	✗ Deny (Deny)
10.10.10.2		102.132.97.35 (www.faceb...	udp/443	✗ Deny (Deny)
10.10.10.2		102.132.97.35 (www.faceb...	udp/443	✗ Deny (Deny)
10.10.10.2		172.217.18.35 (www.gstati...	udp/443	✓ Accept (7.3)
10.10.10.2		102.132.97.35 (www.faceb...	udp/443	✗ Deny (Deny)
10.10.10.2		142.251.37.164 (www.goog...	udp/443	✓ Accept (45)
10.10.10.2		102.132.97.35 (www.faceb...	udp/443	✗ Deny (Deny)



DNAT Test — Result

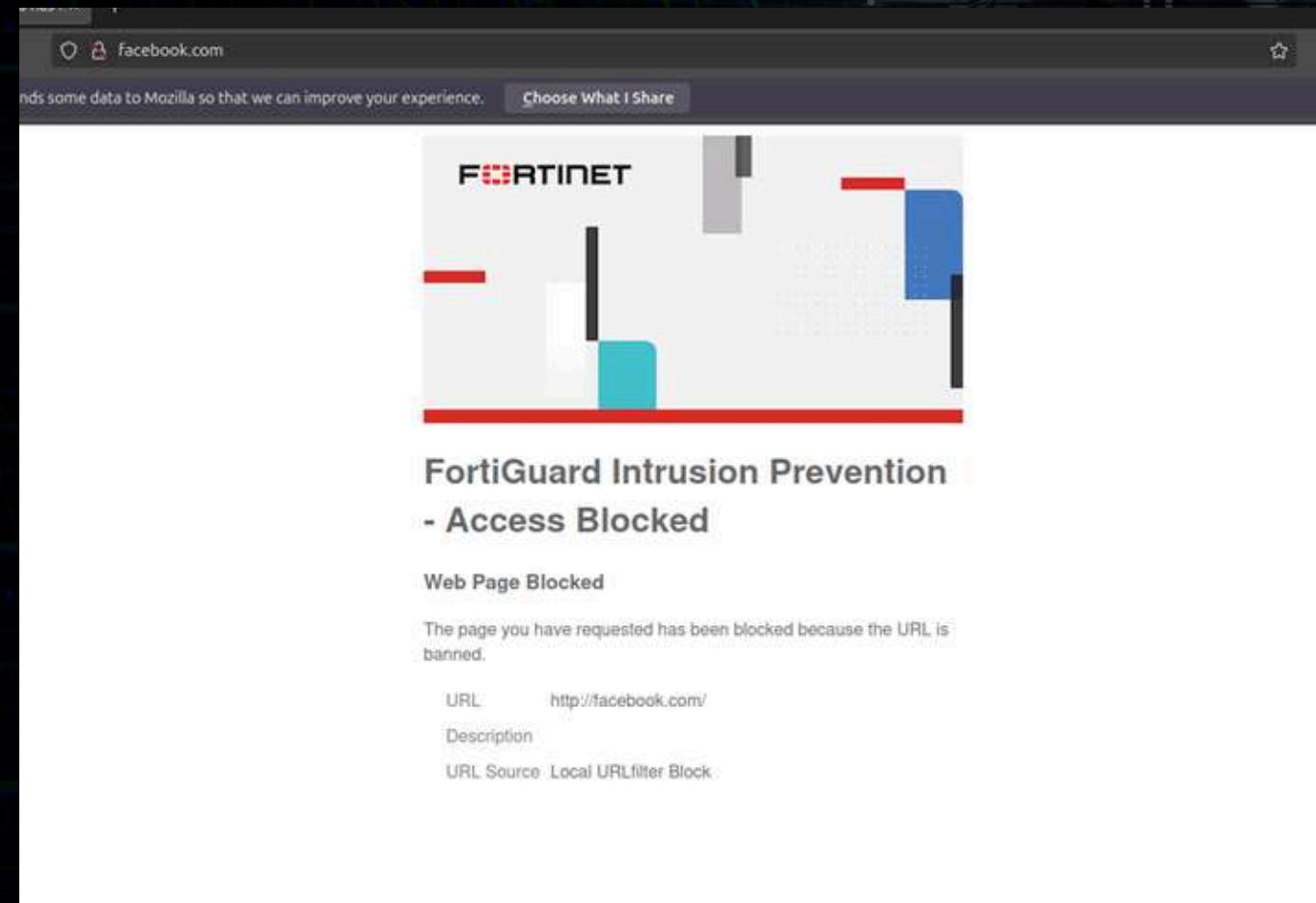
- Attempted SSH on port TCP/2222
- Successfully mapped to internal server
- Logs confirm correct DNAT translation



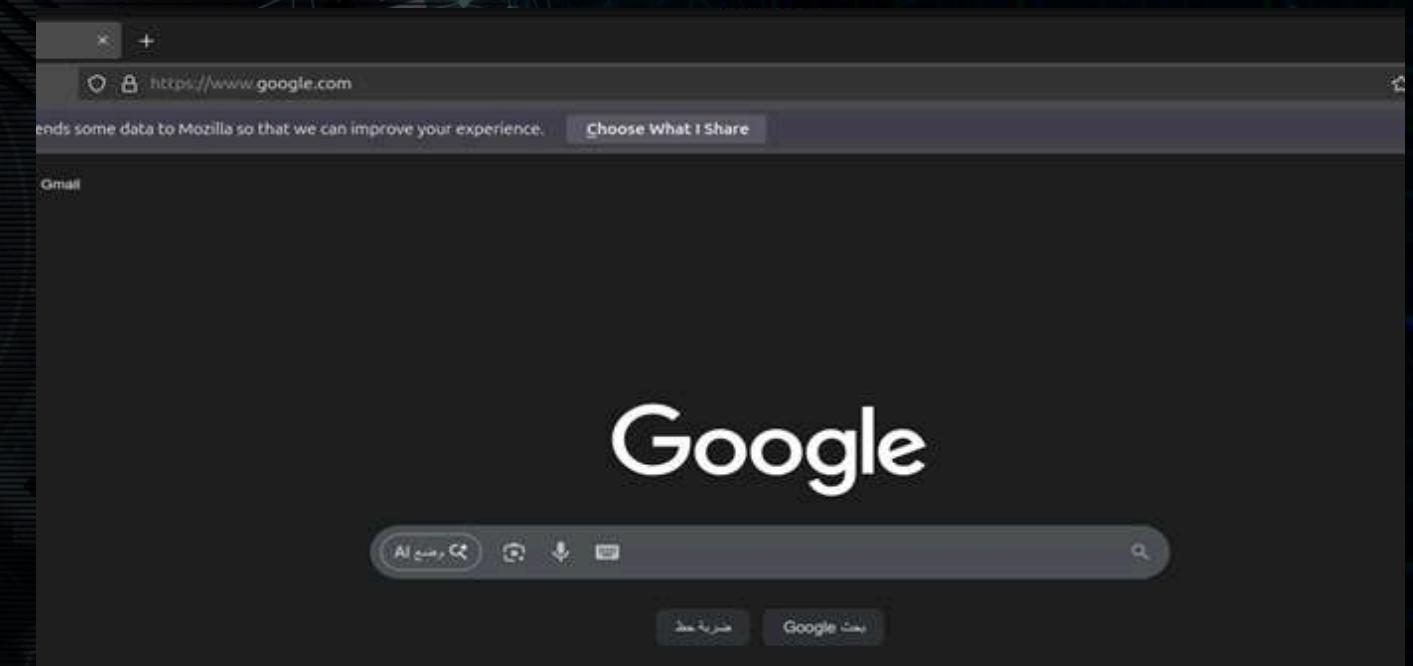


Web Filtering Test Result

Block page appears (Successful)



Allowed websites: Loaded normally





Week 3 Summary

- Implemented SNAT and DNAT
- Built granular firewall policies
- Applied Web Filtering
- Fully validated with testing
- Network is secure and operational





Week 4

Presentation & Final Report

- Compiled all project findings from Week 1 to Week 3
- Organized configuration steps, policies, NAT rules, and screenshots
- Documented all testing procedures and validation results in the final report
- Structured a professional presentation summarizing:
 - Threat analysis
 - FortiGate configuration
 - Policies & NAT
 - Testing and verification
- Ensured all tasks meet the project requirements and learning objectives





Thank You

We truly appreciate your time and the opportunity to present our work.

This project helped us grow technically and professionally as future security engineers.

Thank you for your guidance — and we're ready for your questions.

