

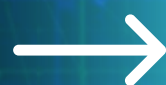


Network Security Fundamentals & FortiGate Integration

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



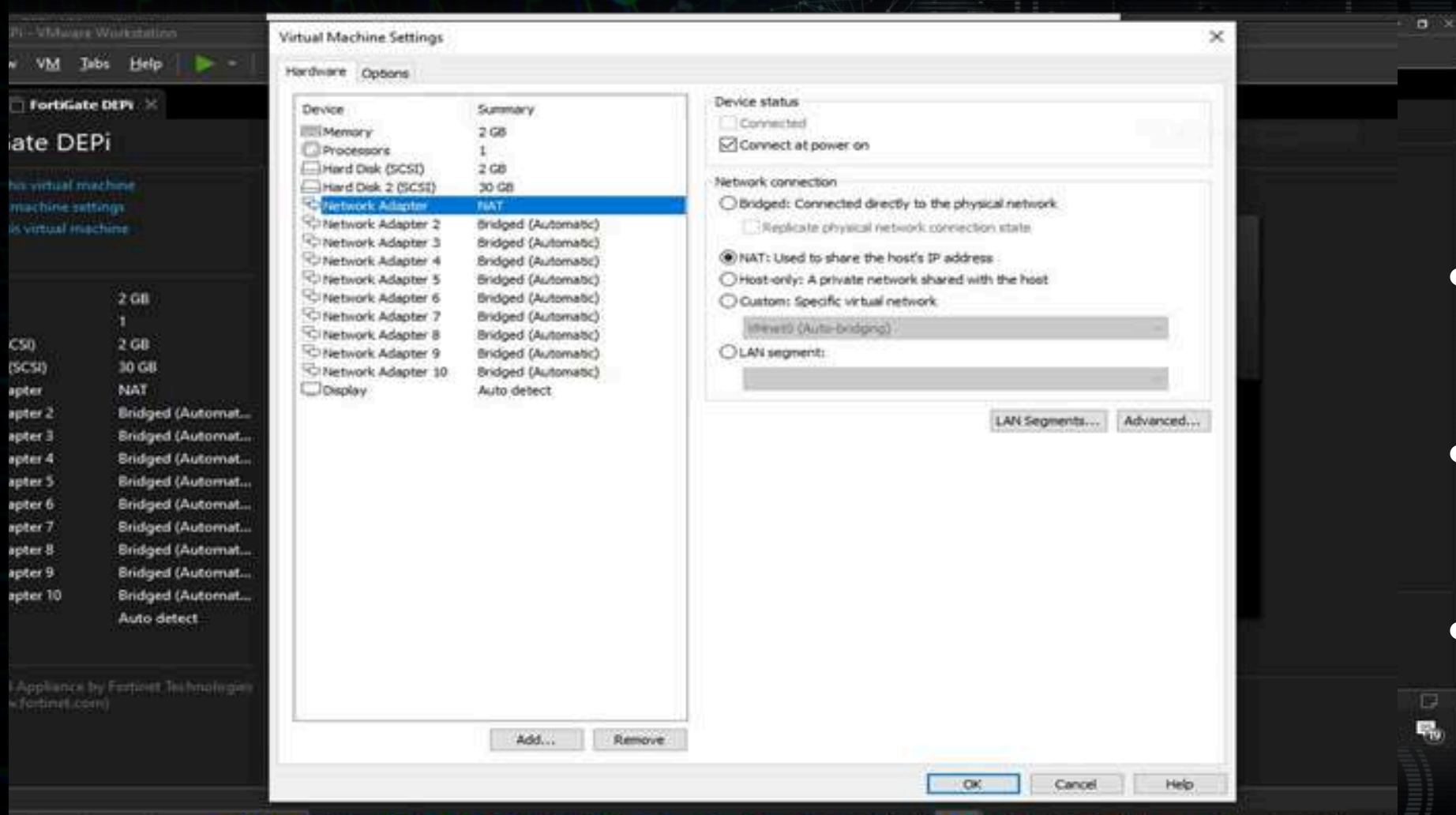
WEEK 2

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 port1
entry is not found in table
FortiGate-VM64 # show system interface port1
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
end
FortiGate-VM64 #
```

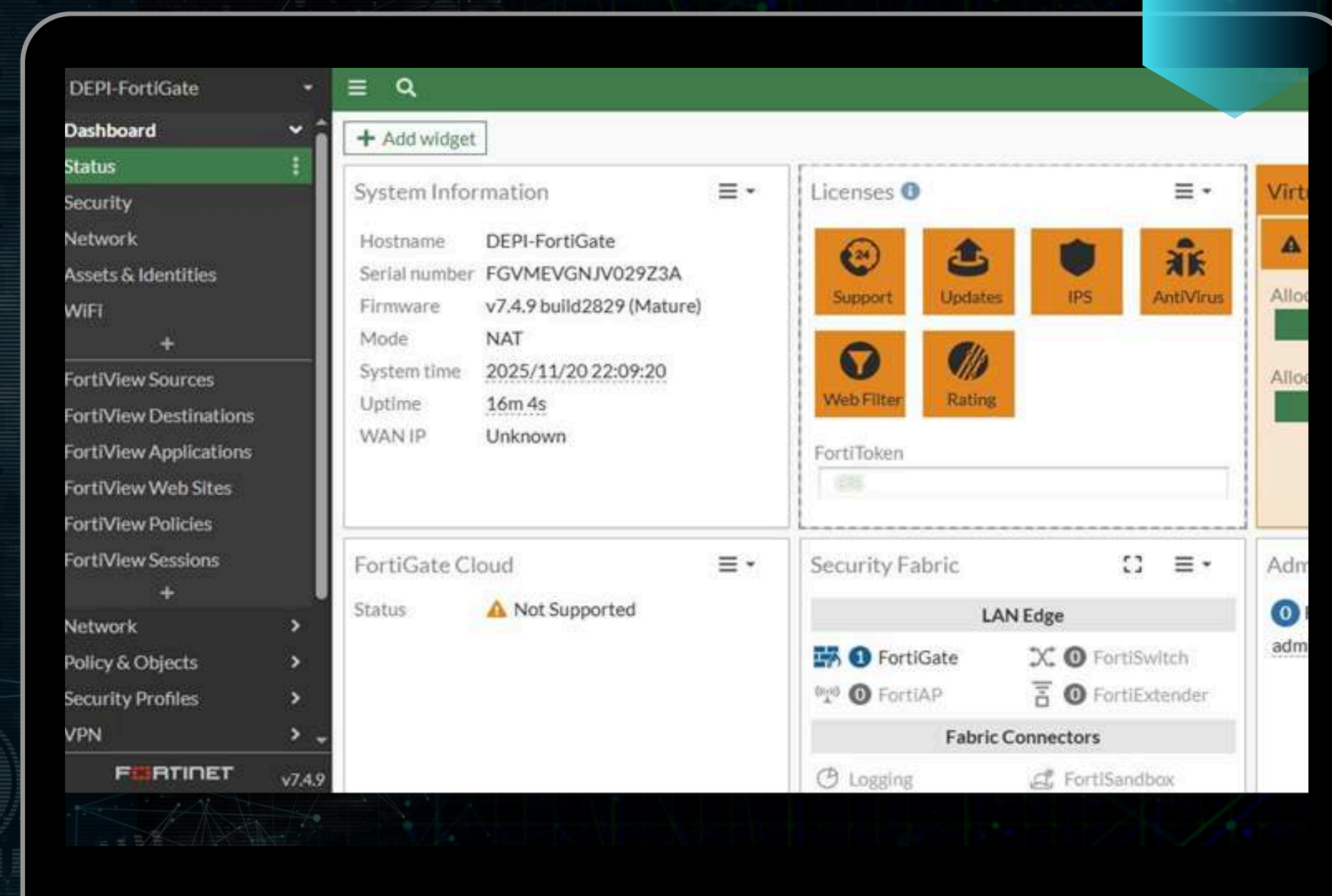
```
FortiGate-VM64 # get system interface physical
== (onboard)
==[port1]
mode: dhcp
ip: 192.168.136.129 255.255.255.0
ipv6: ::/8
status: up
speed: 1000Mbps (Duplex: full)
FEC: none
FEC_cap: none
==[port2]
mode: static
ip: 0.0.0.0 0.0.0.0
ipv6: ::/8
status: up
speed: 1000Mbps (Duplex: full)
FEC: none
FEC_cap: none
==[port3]
mode: static
ip: 0.0.0.0 0.0.0.0
ipv6: ::/8
status: up
speed: 1000Mbps (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

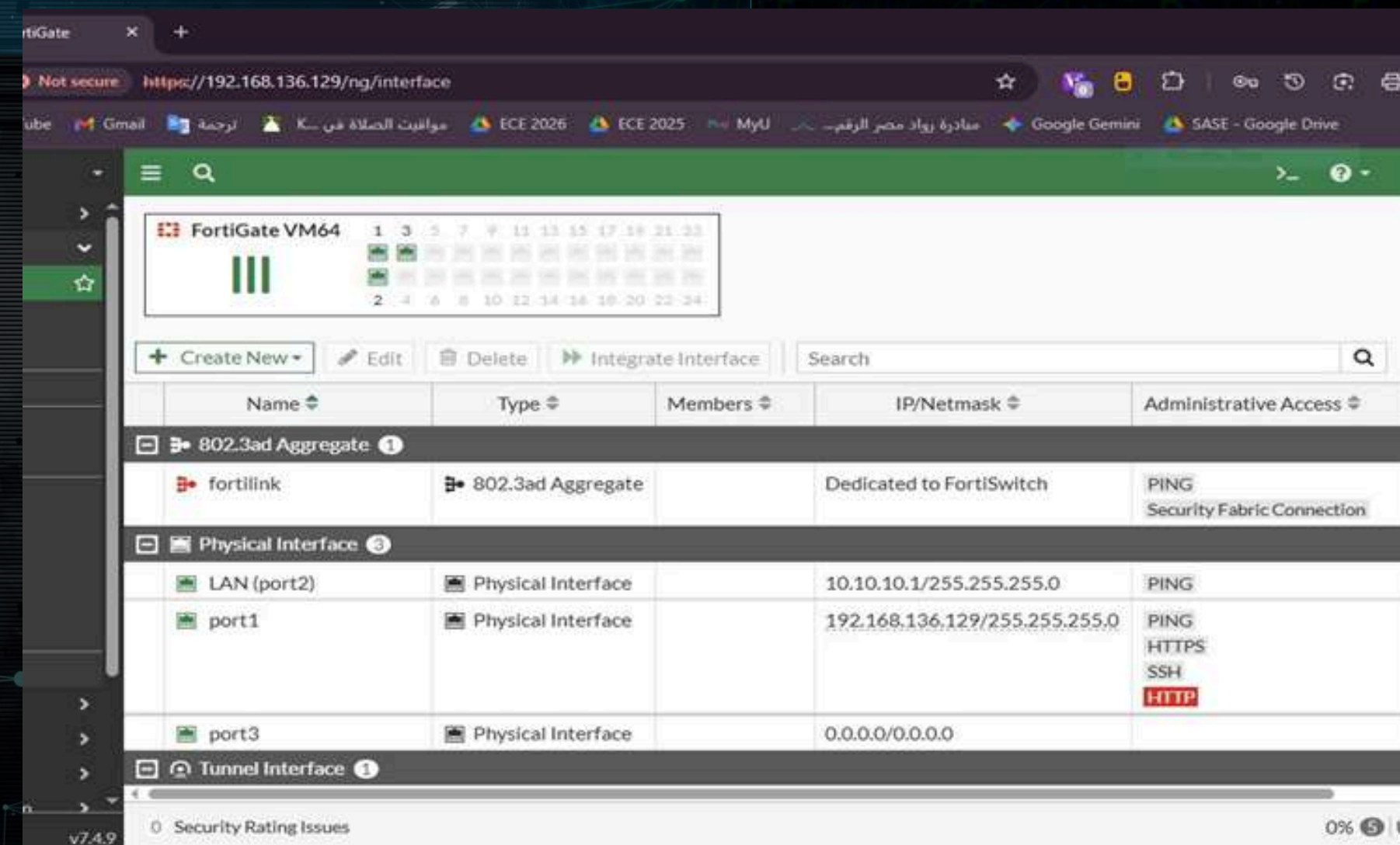
- Logged into GUI using assigned DHCP IP
- Changed hostname → DEPI-FortiGate
- Configured Time Zone “Cairo (GMT+2)”
- Synced NTP server for accurate logs





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



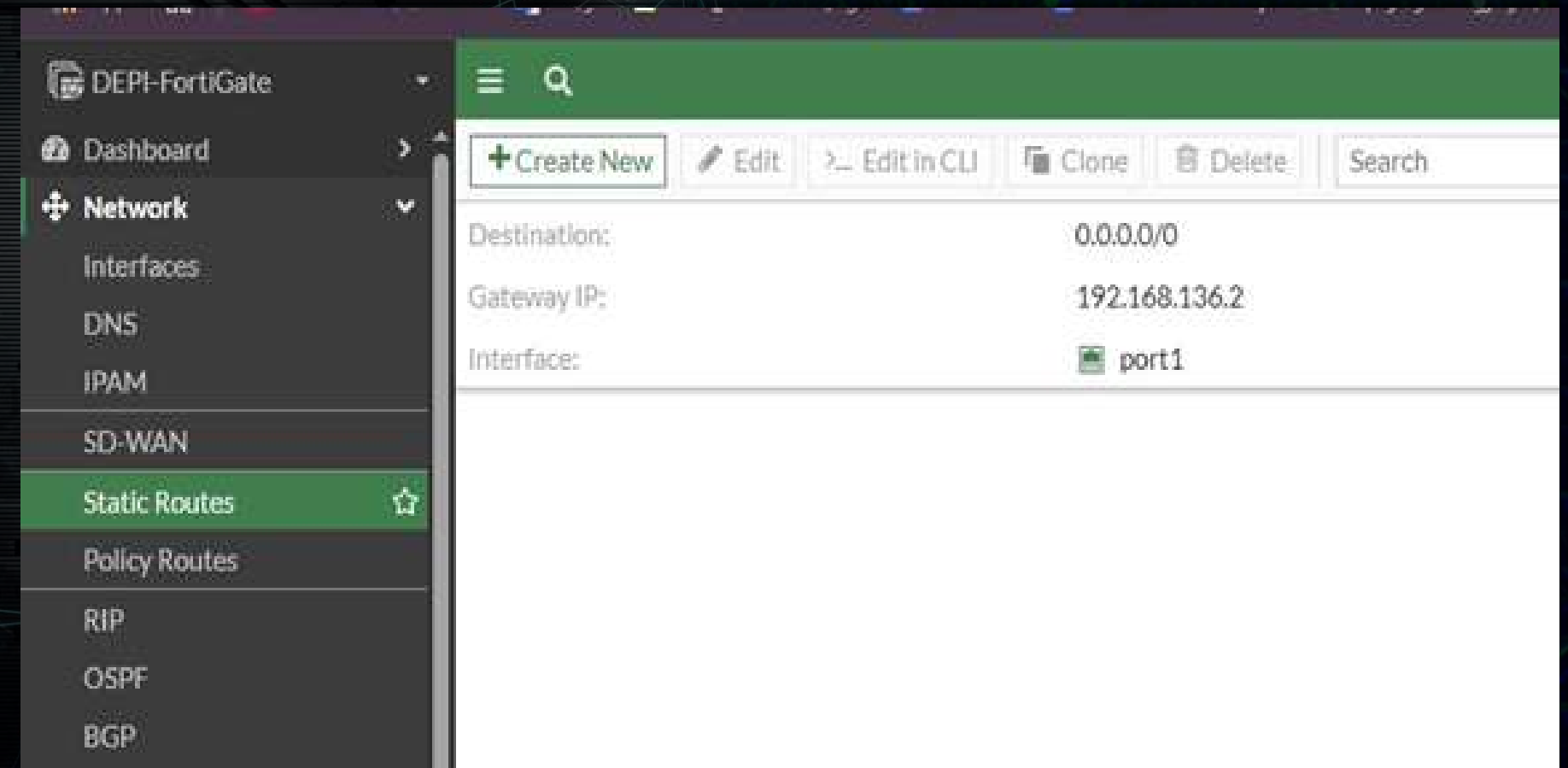
GUI screenshot displaying the configured roles and static IP assignment for the LAN interface (port2) and the DHCP scope





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)

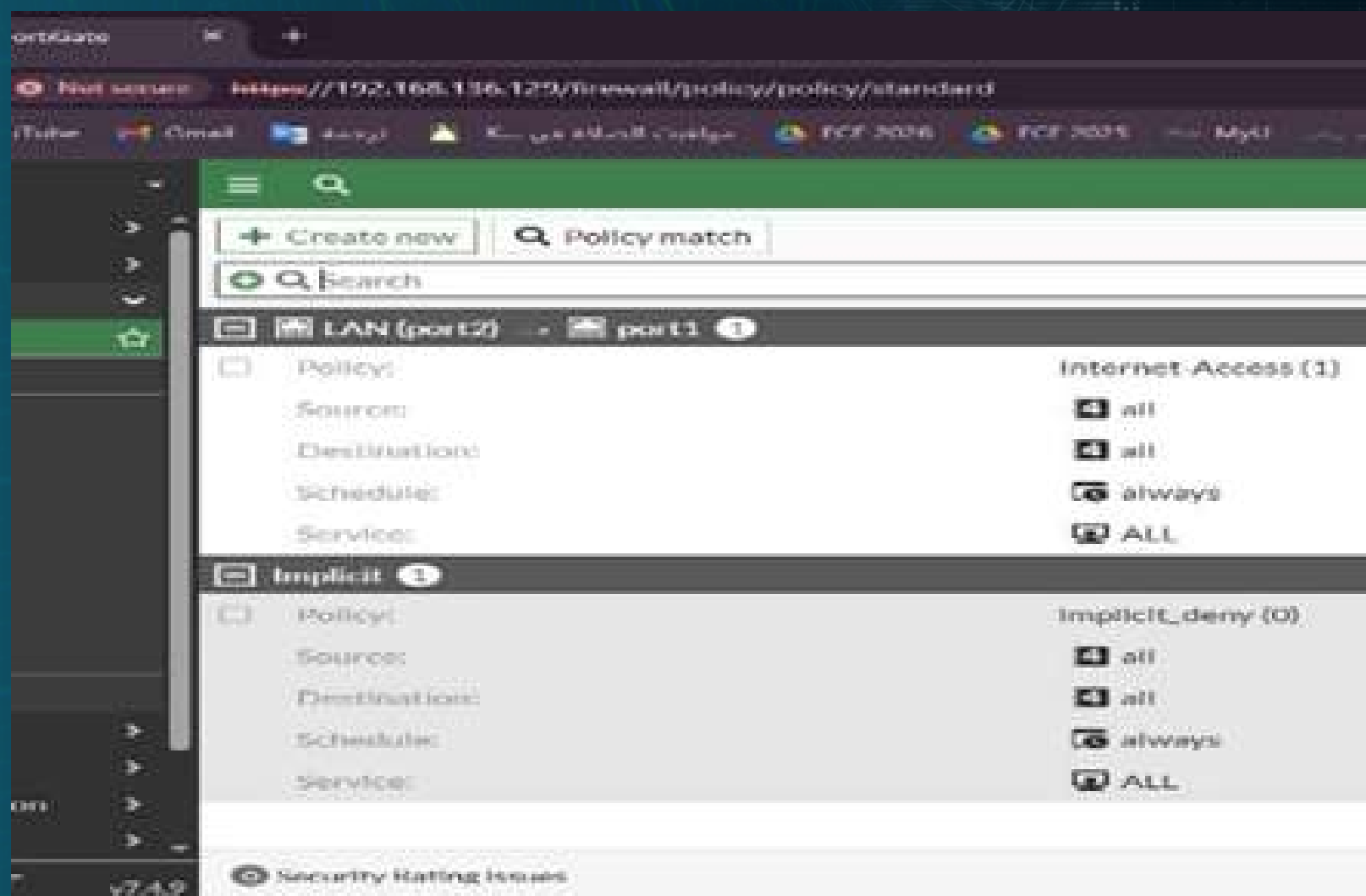
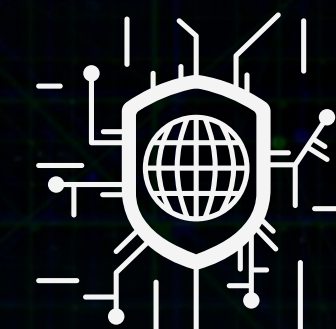


Screenshot from the Network -> Static Routes menu, confirming the 0.0.0.0/0 route pointing towards the correct Gateway via port1





Initial Firewall Policy Internet-Access



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

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





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 FortiGate Firewall Policy configuration interface. The left sidebar lists various configuration sections, with 'Policy & Objects' and 'Firewall Policy' highlighted. The main area displays the 'Edit Policy' window for a policy named 'LAN-to-WAN'.

Policy Configuration:

- Name:** LAN-to-WAN
- Incoming interface:** LAN (port2)
- Outgoing interface:** port1
- Source:** all
- Destination:** all
- Schedule:** always
- Service:** ALL
- Action:** ACCEPT (checked), DENY (unchecked)

Firewall/Network Options:

- NAT:** Enabled
- IP pool configuration:** Use Outgoing Interface Address (selected), Use Dynamic IP Pool (unchecked)
- Manage source port:** Fixed port (selected), Preserve source port (unchecked)
- Protocol options:** default

Security Profiles:

- AntiVirus:** Disabled
- Web filter:** Enabled, Block-Social (selected)
- DNS filter:** Disabled

Statistics (since last reset):

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

Current bandwidth: 0 bps

Last 7 Days Bytes: A bar chart showing traffic volume over the last 7 days, with a peak around 22 days ago.

Additional Information: API Preview, Edit in CLI





Destination NAT (DNAT) Inbound Access

- To allow SSH access to the internal server



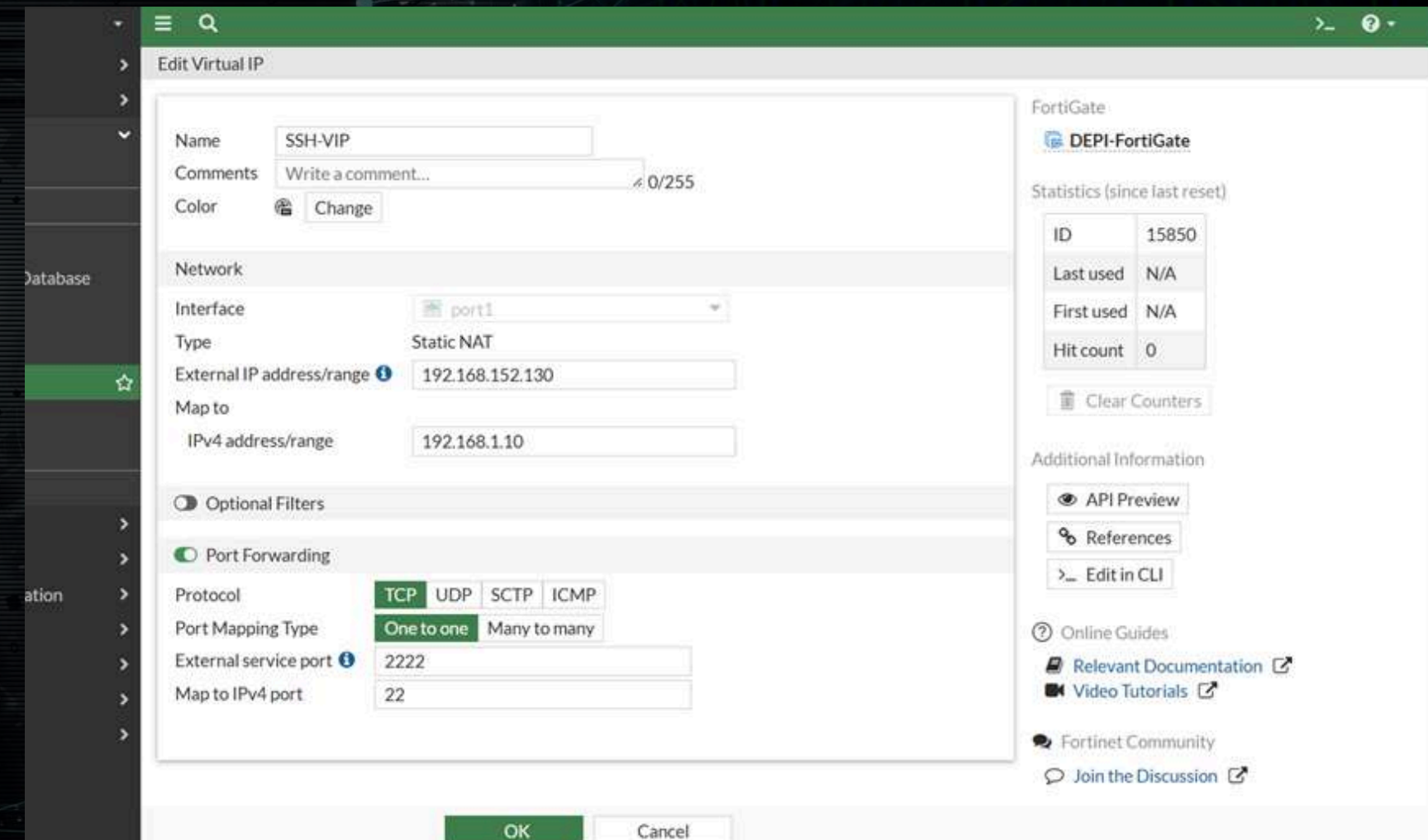
- Used Virtual IP (VIP) mapping

- 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)

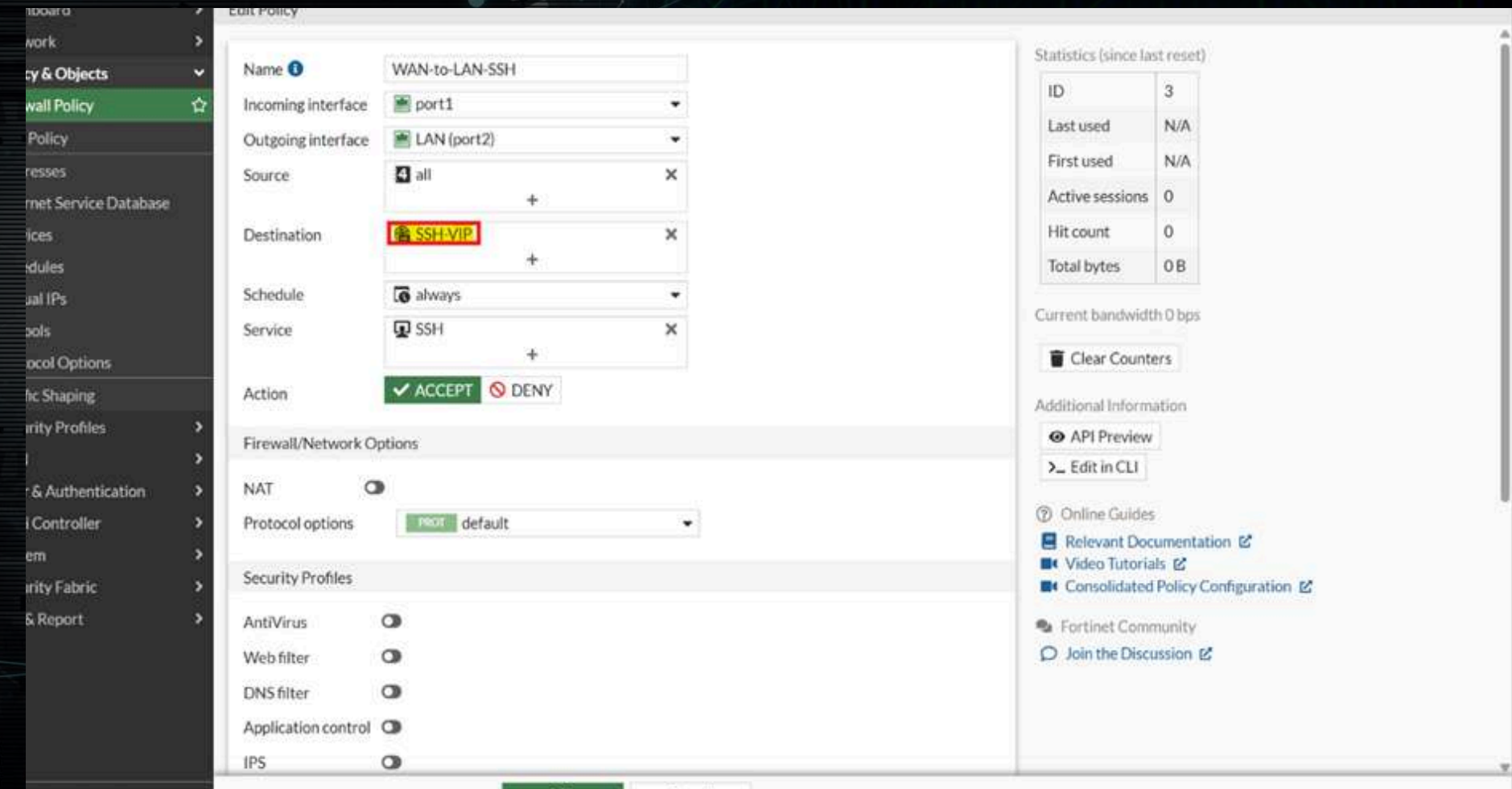


The screenshot displays the 'Edit Virtual IP' configuration window in the FortiGate WebUI. The configuration is for a Virtual IP named 'SSH-VIP'. The 'Network' section shows the 'Interface' set to 'port1', 'Type' as 'Static NAT', 'External IP address/range' as '192.168.152.130', and 'Map to IPv4 address/range' as '192.168.1.10'. The 'Optional Filters' section has 'Port Forwarding' enabled. Under 'Port Forwarding', the 'Protocol' is set to 'TCP', 'Port Mapping Type' is 'One to one', 'External service port' is '2222', and 'Map to IPv4 port' is '22'. The right sidebar shows statistics for the Virtual IP (ID 15850, Last used N/A, First used N/A, Hit count 0) and additional information links like 'API Preview', 'References', 'Edit in CLI', 'Online Guides', 'Relevant Documentation', 'Video Tutorials', and 'Fortinet Community'.

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)

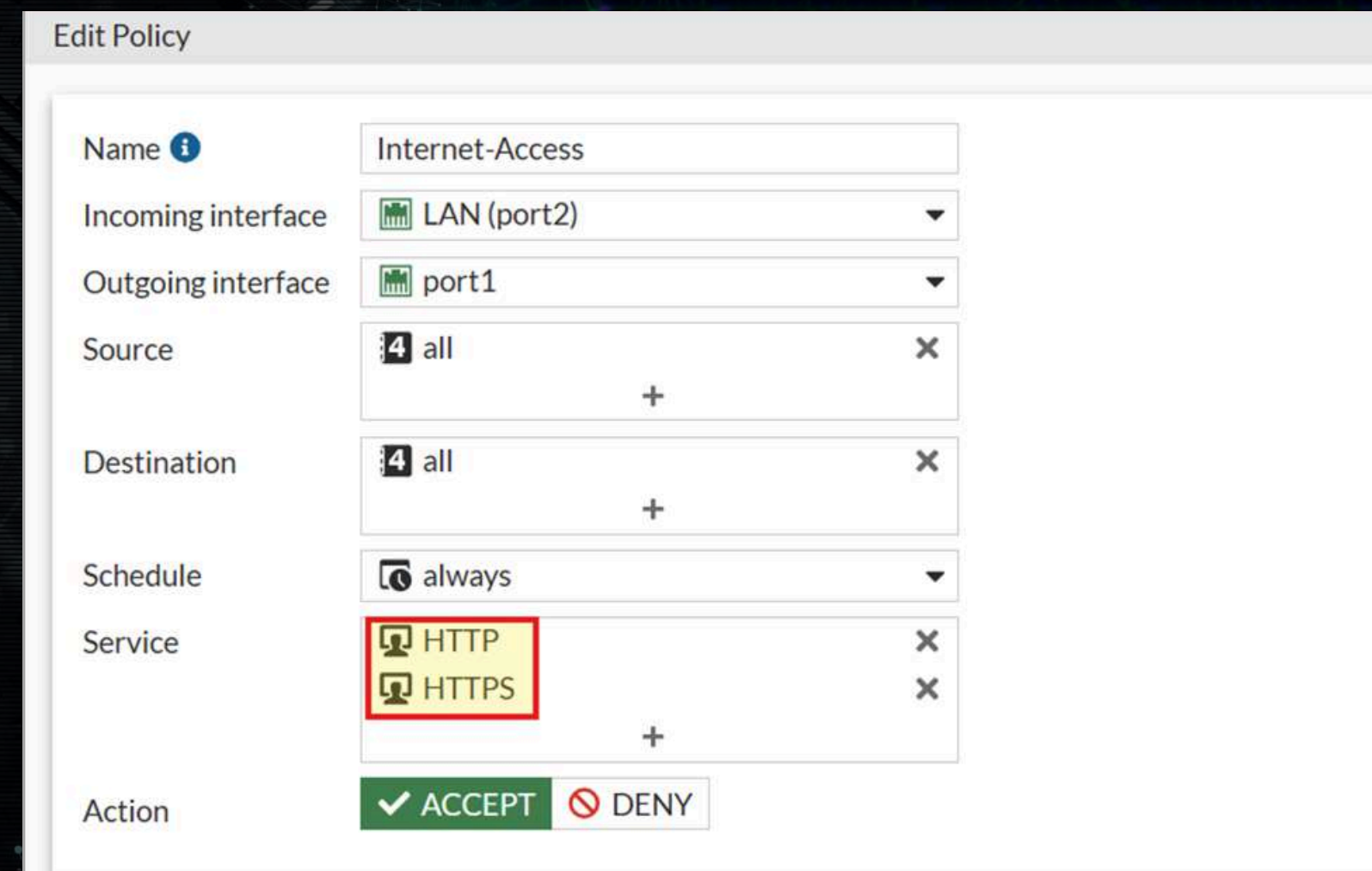


Inbound Service Access Policy. Firewall policy (WAN-to-LAN-SSH) allowing WAN-to-LAN traffic using the SSH-Server-VIP as the destination object.



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



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

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



LICERIA & CO.

Web Filtering

Block Social Media

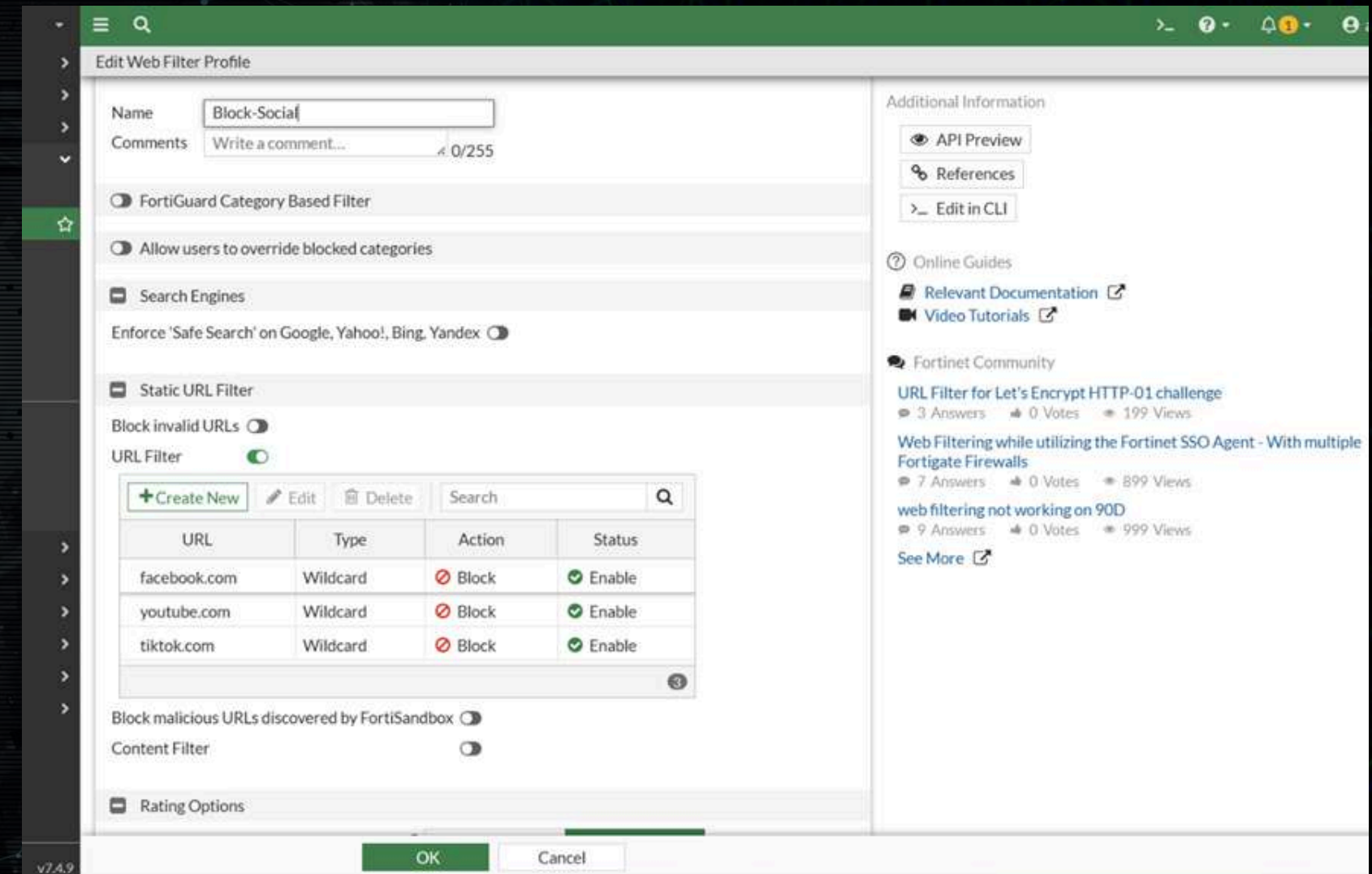
HOME

ABOUT

CONTENT

OTHERS

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



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	Service	Action	IP Pool	NAT	Type	Security Profiles	Log
LAN (port2) → port1 2										
LAN-to-WAN (2)	all	all	always	ALL	✓ ACCEPT		✓ NAT	Standard	<div> <div>Web Filter</div> <div>Block-Social</div> <div>SSL</div> <div>certificate-inspection</div> </div>	✓ All
Internet-Access (1)	all	all	always	ALL	✓ ACCEPT		✓ NAT	Standard	<div> <div>SSL</div> <div>no-inspection</div> </div>	✓ 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



DNAT Test — Result

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

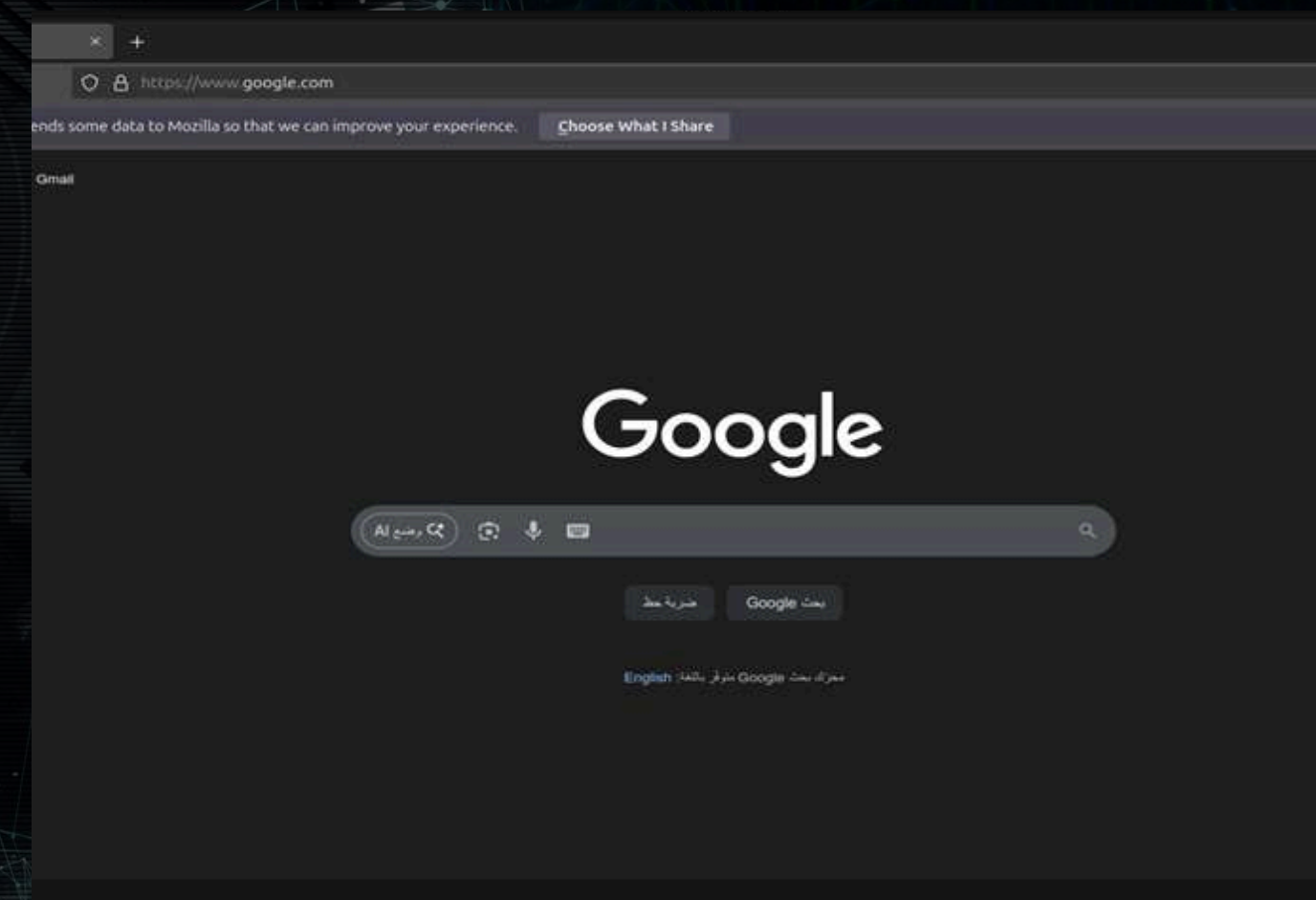
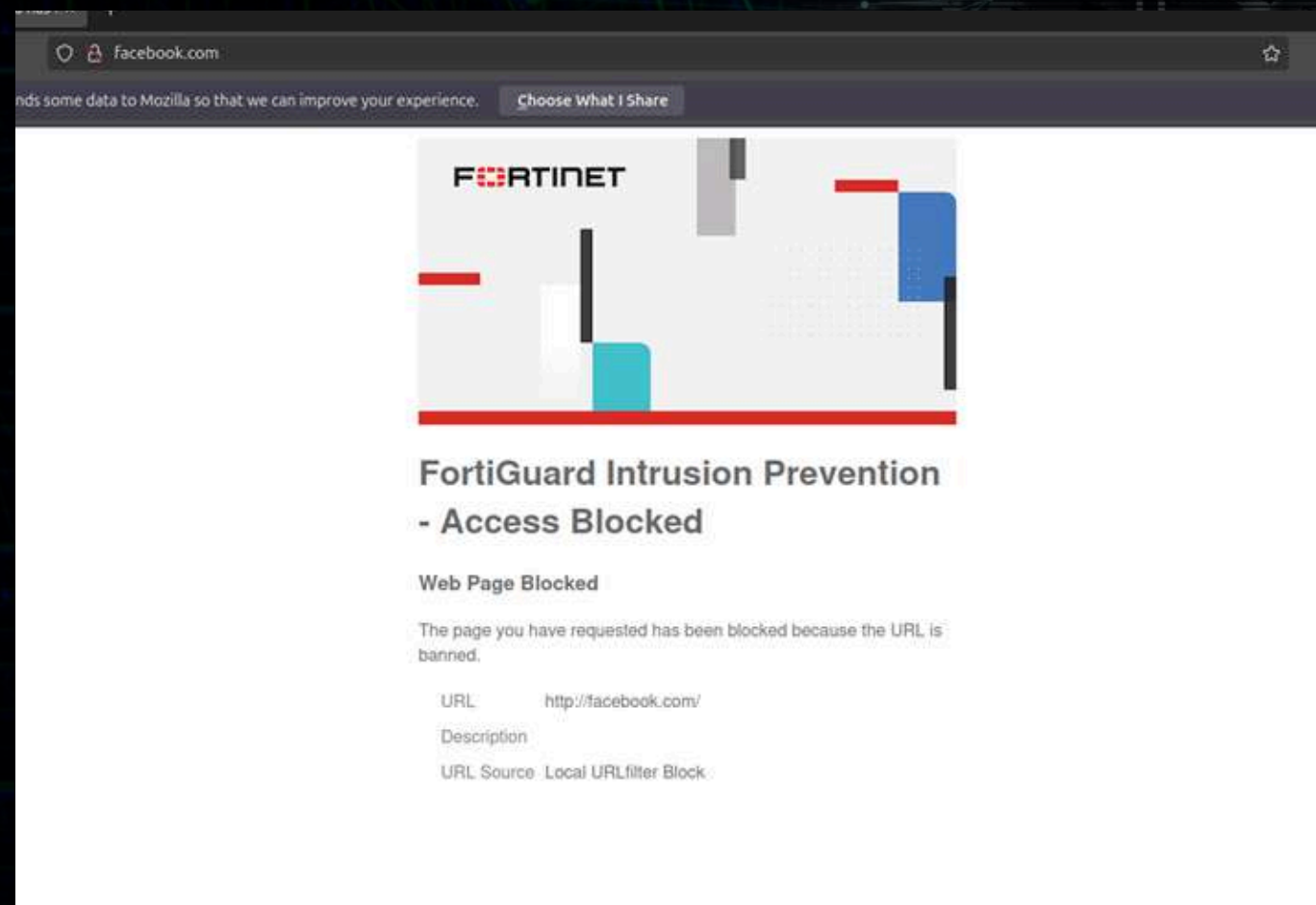




Web Filtering Test Result

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.

