Digital Egypt Pioneers Initiative (DEPI)

Final Project Report

Project 1:

Network Security Fundamentals and FortiGate Integration

Prepared by Team:

Abdullah Ashraf Saber

Marawan Mohamed Abdelfattah

Mazen Mohamed Fathy

Noor Hussain Mwafi

Omar Mohamed Abdelrahman El-Sayed Amer

Date:

November 25, 2025

1. Executive Summary

Document serves **Final Report** for **Project 1**"Network Security Fundamentals and FortiGate Integration."

The comprehensive project scope aimed to transform theoretical knowledge into a practical, resilient defense system, covering all required tasks from fundamental concepts to advanced firewall policy implementation.

The project successfully achieved its objectives across four phases, beginning with an in-depth analysis of the current threat landscape (e.g., RaaS, Phishing) and vital mitigation strategies (Zero Trust, Segmentation). This foundation was immediately utilized in the practical deployment of a **FortiGate Next-Generation Firewall (NGFW)** in a virtualized environment. The final phase successfully implemented and verified complex security measures, including **Network Address Translation (NAT)**, static routing, and granular security policies, resulting in a fully segmented and secured network environment prepared for production use.

---

2. Project Goals and Objectives

Goals (Strategic, Long-term Outcomes)	Objectives (Measurable, Achieved Actions)
Establish a Robust Security Posture: To master modern network defense mechanisms and effectively protect digital assets from evolving threats.	**Phase 1 (Fundamentals):** Conducted comprehensive research and delivered a presentation on current cyber threats (RaaS, Phishing) and implemented strategic mitigation models like Zero Trust and Network Segmentation.
Deploy and Validate NGFW Infrastructure: To build a fully operational, segmented, and secure virtualized network environment using industry-leading technology.	**Phase 2 (Configuration):** Successfully deployed the FortiGate VM, configured network interfaces (LAN/WAN segmentation), and established the default static route for external connectivity.
Implement Advanced Traffic Control: To manage inbound and outbound traffic flows securely, ensuring protected external access and adherence to defined security requirements.	**Phase 3 (Advanced Policies):** Configured and rigorously tested complex Firewall Policies, including Source NAT and Destination NAT rules, to facilitate secure and controlled internal and external communication.

---

3. Project Scope & Deliverables Status

Task	Core Subject	Deliverable (Output Documented)	Status
Task 1	Network Security Fundamentals	Submission of research and presentation materials covering vulnerabilities, attack methods, and mitigation strategies.	**Successfully Finalized** (Pages 4-5)
Task 2	FortiGate Initial Configuration	Documentation of VM deployment, interface segmentation, and the initial Internet-Access security policy.	**Successfully Finalized** (Pages 6-11)
Task 3	Advanced Policies and NAT Implementation	Verification and reporting on the configuration of complex Network Address Translation (NAT) rules and granular firewall access policies.	**Successfully Finalized** (pages 12-19)
Task 4	Final Project Report & Compilation	Final compilation of all phases, analysis, and conclusions into this comprehensive final document[8].	**Successfully Finalized** (This report itself)

Task 1: Network Security Fundamentals

The initial phase of the project focused on establishing a robust theoretical foundation by analyzing the contemporary cybersecurity threat landscape. This analysis was crucial for informing the subsequent design and implementation of the FortiGate solution.

4.1.1. Core Vulnerabilities: The Weakness Within Systems

A vulnerability is defined as an inherent flaw or weakness within a system, network, or process that, if exploited, can lead to unauthorized access or compromise. The research identified three primary vectors that malicious actors frequently exploit:

Vulnerability Type	Description & Impact	Mitigation Relevance
Unpatched Software	Outdated operating systems and applications with known security holes (CVEs). Attackers actively scan for systems missing critical updates.	Necessitates a strong patch management policy and the use of Next-Generation Firewalls (NGFWs) for virtual patching.
Misconfigurations	Oversight errors, such as using default passwords (e.g., admin/admin), leaving open ports (e.g., RDP 3389), or improperly configured firewall rules.	Requires stringent system auditing, immediate password changes post-deployment, and rule validation (addressed in Task 2).
The Human Factor	Employees lacking essential security awareness, often leading to policy bypass or accidental compromise.	Requires constant and engaging security awareness training (addressed in 4.1.3).

4.1.2. Strategic Defense Frameworks

The analysis highlighted that a simple perimeter defense is no longer sufficient. Modern cybersecurity requires layered strategies, specifically Zero Trust and Network Segmentation:

A. Zero Trust Architecture The core principle of Zero Trust is **"Never trust, always verify."** No user or device, whether inside or outside the network perimeter, is inherently trusted. This model strictly requires validation before access is granted to any resource.

B. Network Segmentation Segmentation involves creating virtual boundaries using technologies like VLANs and firewall rules to restrict access and limit the lateral movement of threats. Key applications :

- **Protect Critical Assets:** Placing mission-critical servers and sensitive data in highly restricted segments with stringent access controls.
- **Contain Guest Access:** Completely isolating guest Wi-Fi networks from internal corporate resources to prevent unauthorized access.
- **Reduced Attack Surface:** Significantly minimizes the potential impact and spread of a breach across the entire network.

4.1.3. Empowering the Human Firewall

Recognizing that the human element remains a critical component, **Security Awareness Training** is essential to transform employees from potential vulnerabilities into the first line of defense. Key training areas include:

Training Area	Objective
Phishing Recognition	Educating employees on how to identify, avoid, and report suspicious emails and malicious links.
Strong Passwords & MFA	Emphasizing the necessity of complex, unique passwords and the mandatory use of Multi-Factor Authentication (MFA).
Social Engineering	Training staff to recognize and resist psychological tactics used by attackers to manipulate individuals into divulging confidential information.
Data Handling	Establishing best practices for securely handling sensitive organizational data and understanding compliance requirements.

Task 2: FortiGate Deployment and Basic Configuration

4.2.1. Lab Environment Preparation and VM Deployment

Step	Detail	Rationale
1. Firmware Acquisition	Selected the specific **FGT_VM64-v7.4.x** image for the **VMware ESXi** platform, ensuring the full firewall functionality was acquired (avoiding the "FortiFirewall" variant).	Guaranteed compatibility with VMware Workstation and access to full NGFW feature set.
2. Virtual Machine Import	Utilized the VMware Workstation import process using the extracted .ovf template. The VM was named **FortiGate-DEPI** for project identification.	Established the necessary virtual hardware and network adapters within the lab environment.
3. Resource Optimization	The default virtual hardware was adjusted to meet evaluation license requirements: **1 Processor / 1 Core** and **2 GB RAM**.	Ensured the VM operates within legal license limits while providing adequate performance for the initial configuration.

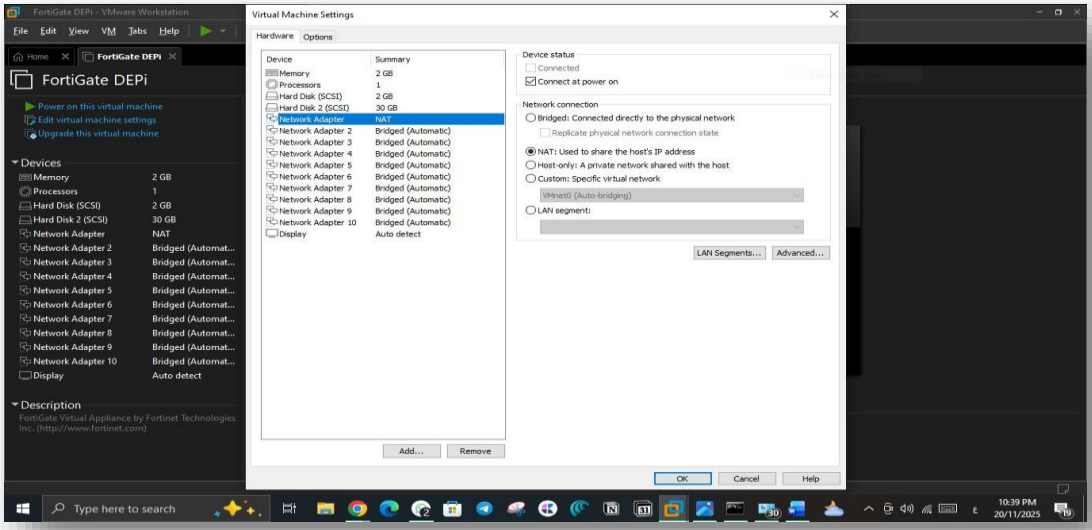
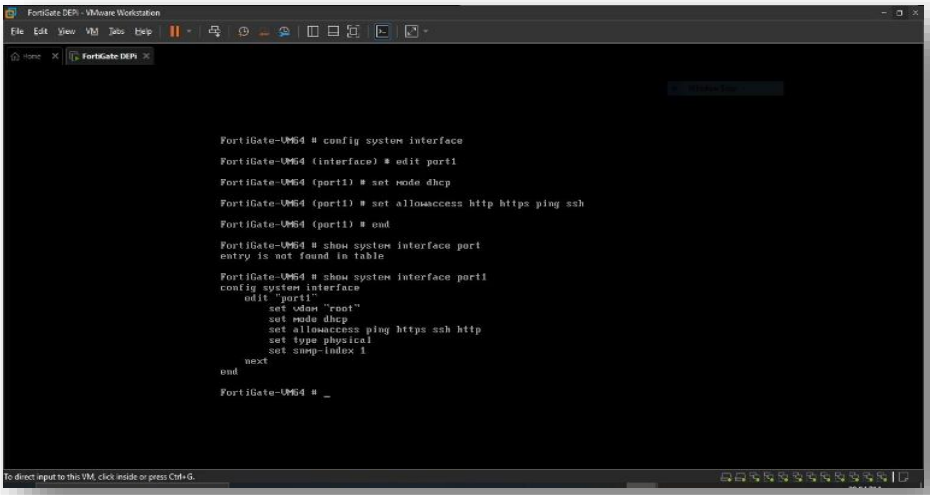


FIGURE 4.2.1

Figure 4.2.1: Virtual Machine Hardware Resource Allocation. Screenshot verifying the CPU and RAM allocation within the VMware Workstation settings, confirming compliance with license restrictions.

4.2.2. Initial Access and System Identification

4. CLI Configuration: The default login credentials were used to access the CLI, where the management interface (**port1**) was configured to utilize **DHCP** for quick IP acquisition. **HTTPS, SSH, PING, and HTTP** protocols were enabled for administrative access



.**FIGURE 4.2.2**

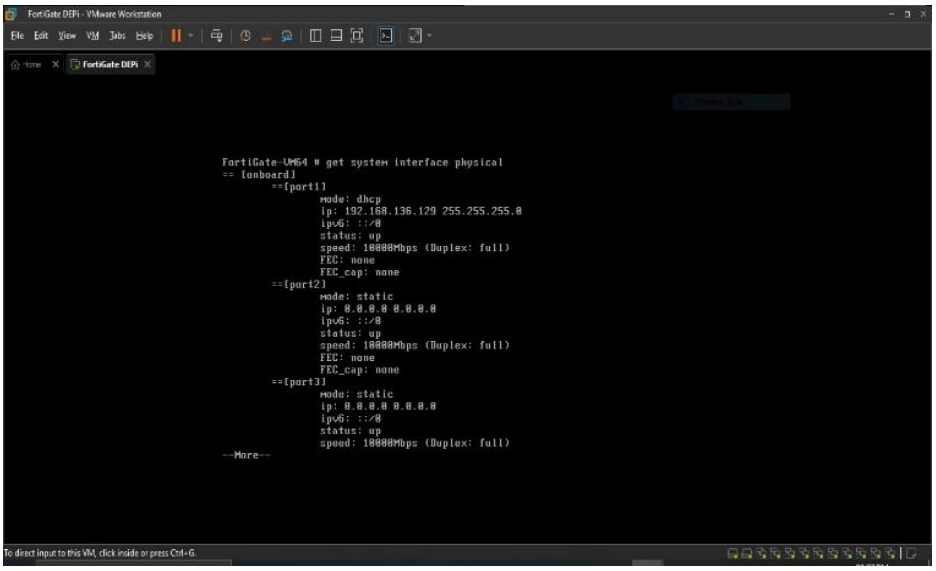


Figure 4.2.2: CLI Initialization and Management IP Verification. Command output showing the successful execution of configuration commands for port1 and the verification of the assigned DHCP IP address (e.g., `192.168.136.x`)

5. GUI Initialization: Access was confirmed via the assigned IP. Key system settings were immediately addressed:

- **Hostname:** Changed from the default serial number to **DEPI-FortiGate**.

- **Time Synchronization:** Time Zone was set to **(GMT+2:00) Cairo**, utilizing a public NTP server (`pool.ntp.org`) to guarantee accurate timestamps for log auditing.

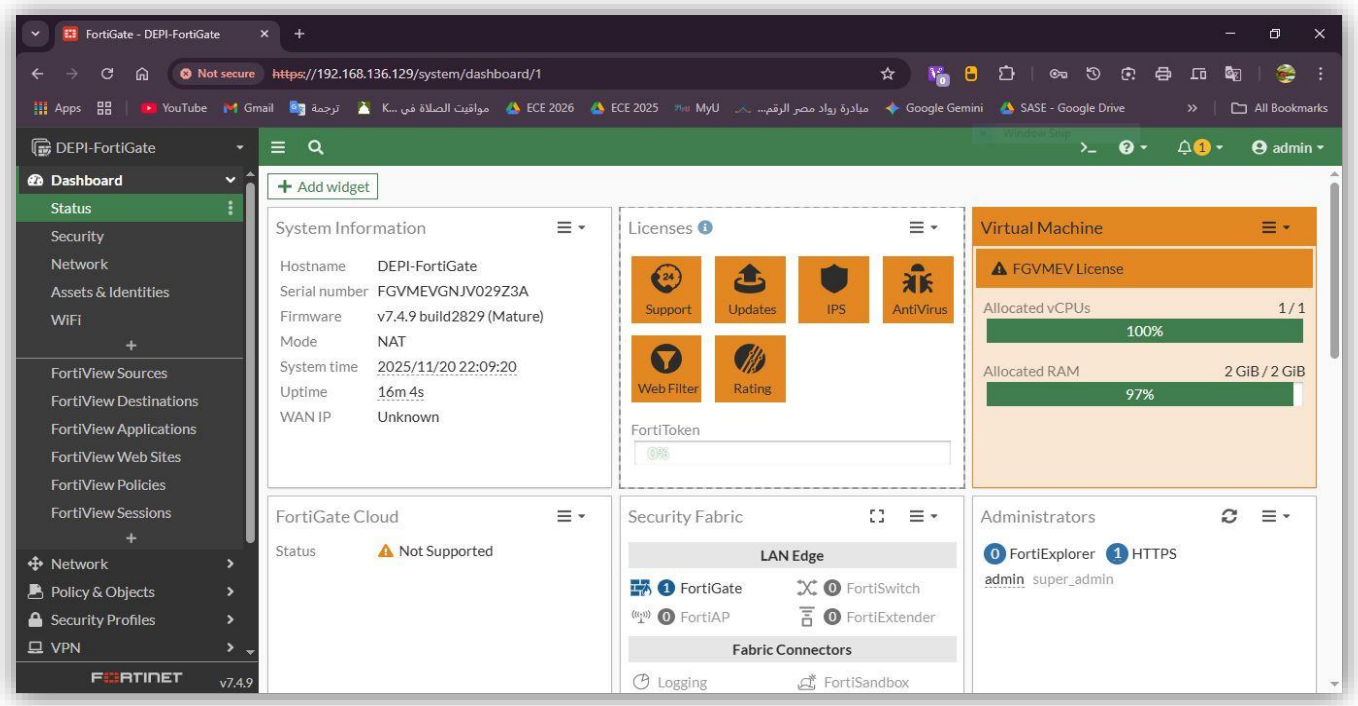


FIGURE 4.2.3

Figure 4.2.3: System Dashboard and Time Synchronization. Screenshot of the FortiGate Web GUI dashboard confirming the updated Hostname and the successful NTP synchronization status.

4.2.3. Network Interface Segmentation and Routing

Network segmentation was executed by assigning distinct roles and static IP addressing to the internal interface (LAN) and configuring the default outbound route.

Interface	Role	IP Addressing & Access	DHCP Scope
port1	**WAN (External)**	DHCP (Dynamic IP assignment)	N/A
port2	**LAN (Internal)**	Static IP: **10.10.10.1/24**	Enabled (Range: **10.10.10.2 - 10.10.10.254**)

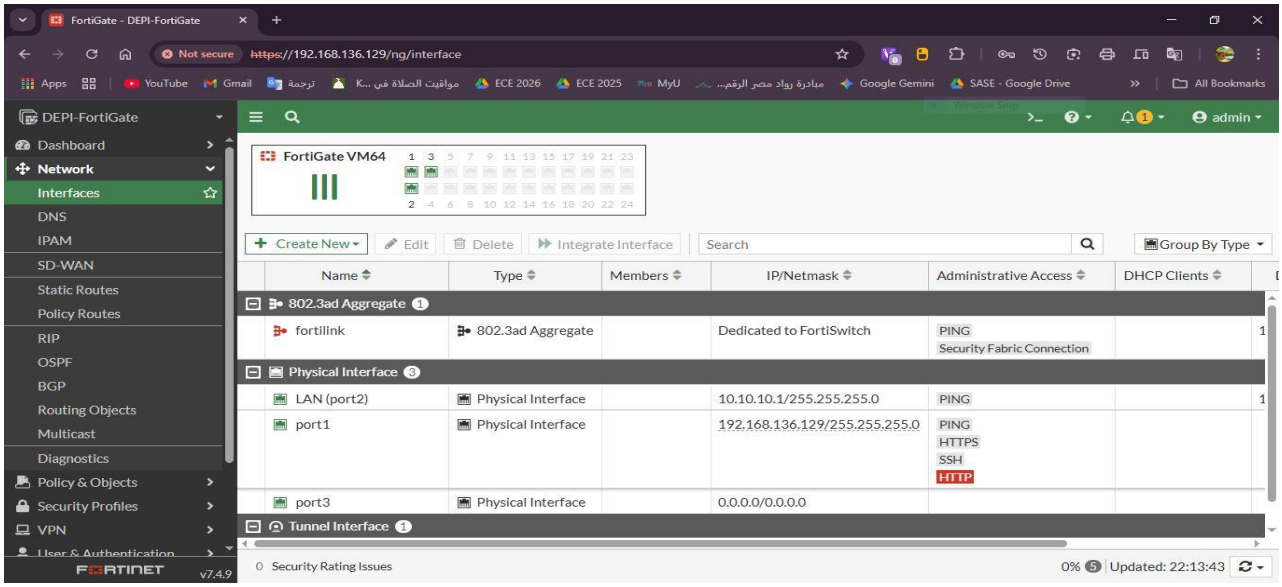


FIGURE 4.2.4

Figure 4.2.4: Interface Configuration Summary. GUI screenshot displaying the configured roles and static IP assignment for the LAN interface (port2) and the DHCP scope.

6. Routing Configuration: A **Static Default Route** was verified and implemented to direct all internet-bound traffic:

- **Destination:** 0.0.0.0/0 (All traffic)
- **Gateway:** 192.168.136.2 (The VMware NAT Gateway IP)
- **Interface:** port1 (WAN)
- Rationale*:* This ensures proper forwarding of outgoing packets through the external interface.

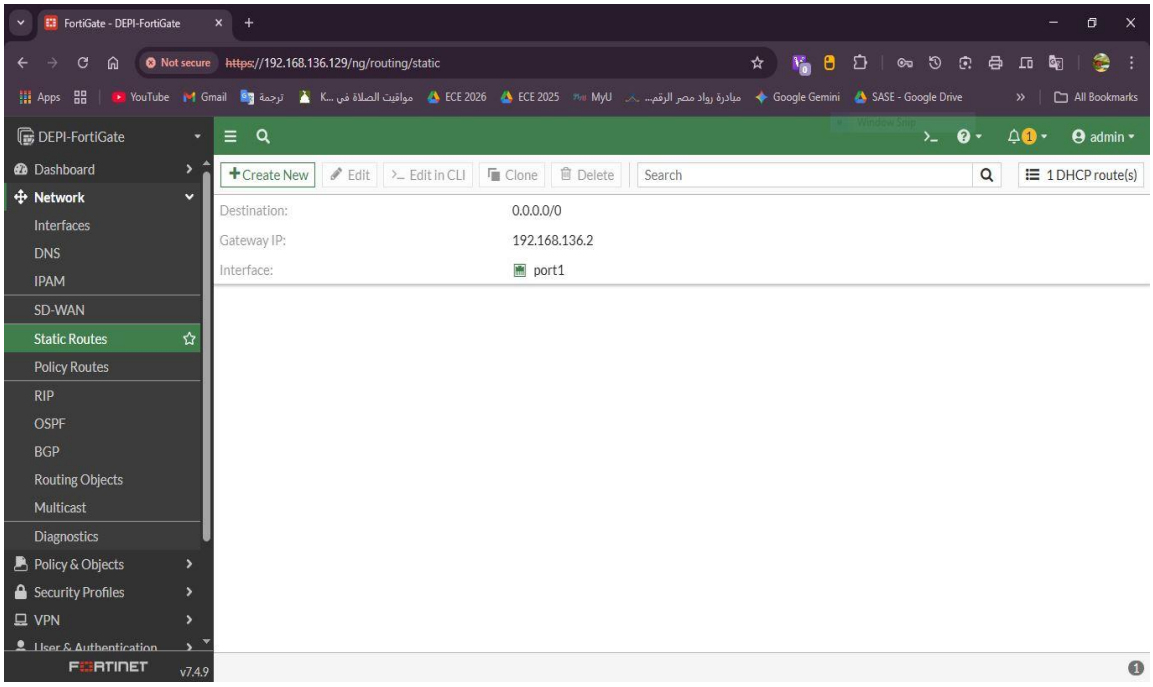


FIGURE 4.2.5

Figure 4.2.5: Static Default Route Configuration. Screenshot from the Network -> Static Routes menu, confirming the 0.0.0.0/0 route pointing towards the correct Gateway via port1

4.2.4. Initial Security Policy Implementation

To enable controlled network communication, the first security policy was created to permit traffic that would otherwise be blocked by the 'Implicit Deny' rule :

Policy Parameter	Configuration	Technical Rationale
Name	Internet-Access	Clear identification of the policy function.
Incoming Interface	port2 (LAN)	Source of permitted traffic.
Outgoing Interface	port1 (WAN)	Destination of permitted traffic.
Source/Destination	All / All	Allows access for all internal devices to all external destinations.
Action	ACCEPT	Permits the traffic flow.
NAT	Enabled (Source NAT)	Essential for translating internal private IPs to the firewall's public-facing IP.
Logging	All Sessions	Mandatory setting for complete auditing and troubleshooting capabilities.

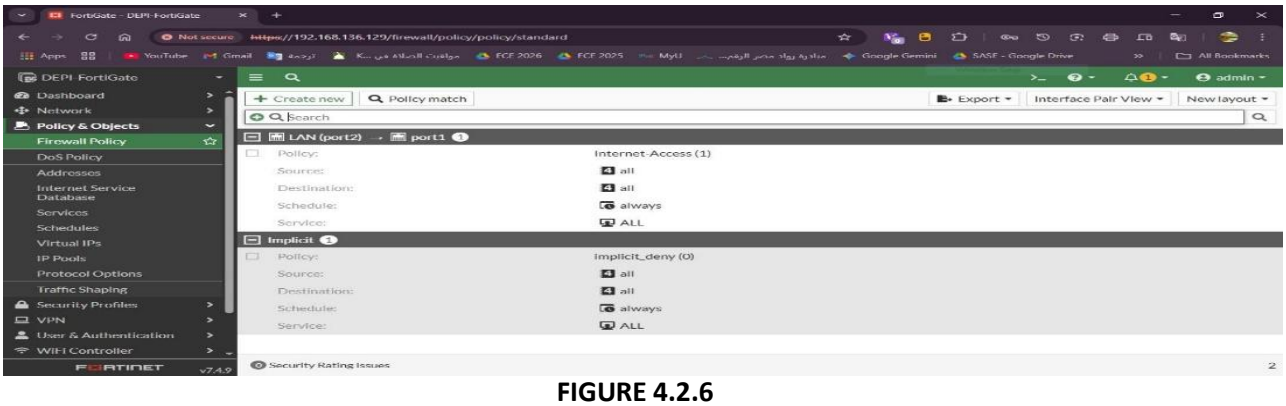


FIGURE 4.2.6

Figure 4.2.6: Initial Firewall Policy (Internet-Access) Details. Screenshot displaying the policy configuration, highlighting the enabled NAT feature and "All Sessions" logging setting.

Task 3: FortiGate Policies and NAT

This section of the report documents the third phase of the project, which focused on building an advanced perimeter defense by implementing comprehensive Network Address Translation (NAT) and granular Access Control Policies. This ensured a fully secure and operational network environment ready for advanced integration.

4.3.1. Network Address Translation (NAT) Implementation

The objective was to implement SNAT for internal-to-external communication and configure DNAT for secure inbound service exposure

A. Source NAT (SNAT) Verification

Goal	Procedure	Verification
Ensure all internal traffic (10.10.10.0/24) is translated to the firewall's WAN IP upon exit[8].	The existing `Internet-Access` policy (LAN to WAN) was verified to have the NAT option enabled and set to **"Use Outgoing Interface Address"**.	Outbound traffic from the LAN Host (10.10.10.2) was confirmed to reach the internet[10]. Logs confirmed the original source IP (10.10.10.2) was translated to the port1 IP (e.g., 192.168.152.130).

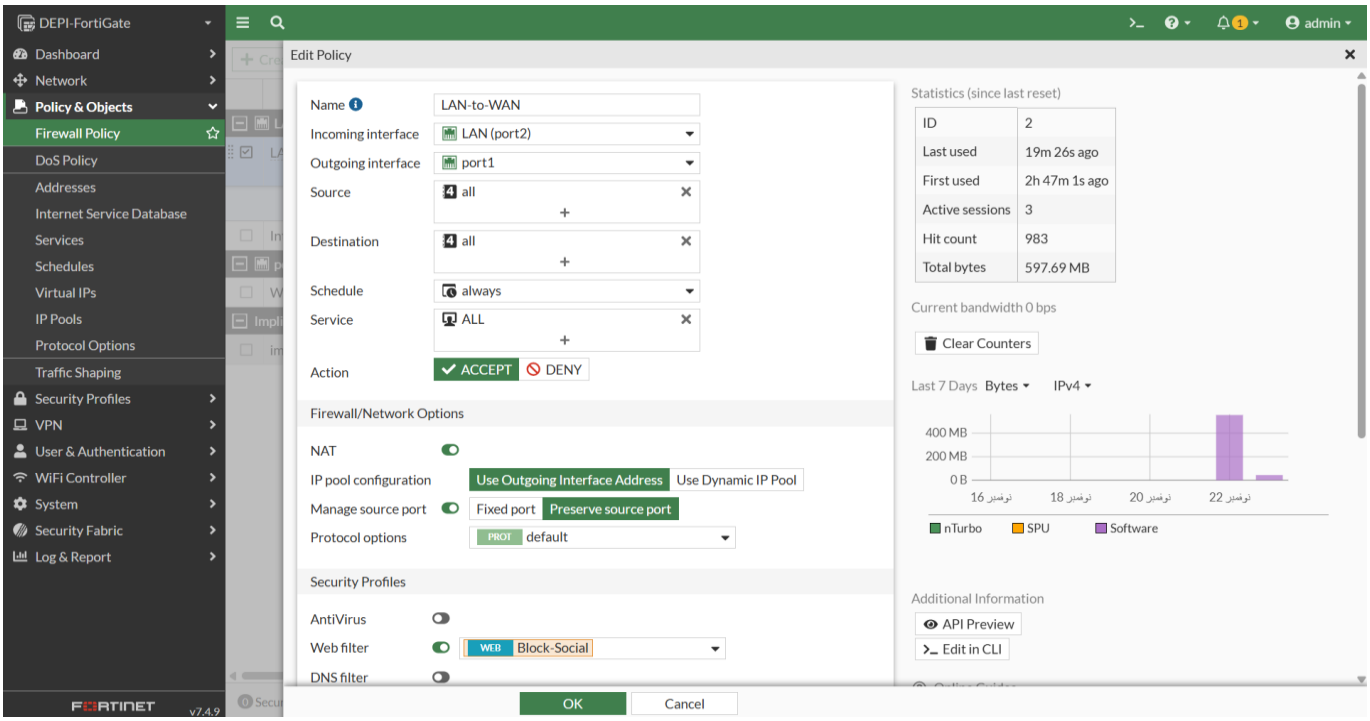


FIGURE 4.3.1

B. Destination NAT (DNAT) / Virtual IP Configuration

The goal was to **allow secure external access to the internal server (10.10.10.2) for SSH**

Step	Configuration/Menu Path	Details
1. Create Virtual IP (VIP)	Policy & Objects \to Virtual IPs	**Name:** `SSH-Server-VIP` **Interface:** `port1` **External IP:** `192.168.152.130` (FortiGate WAN IP) **Mapped IP:** `10.10.10.2` **Port Forwarding:** Enabled (TCP/2222 to 22)
2. Create DNAT Policy	Policy & Objects to Firewall Policy	**Incoming:** `port1` **Outgoing:** `port2` **Source:** `all` **Destination:** `SSH-Server-VIP` **Service:** `SSH` **Action:** `ACCEPT` **NAT:** Disabled

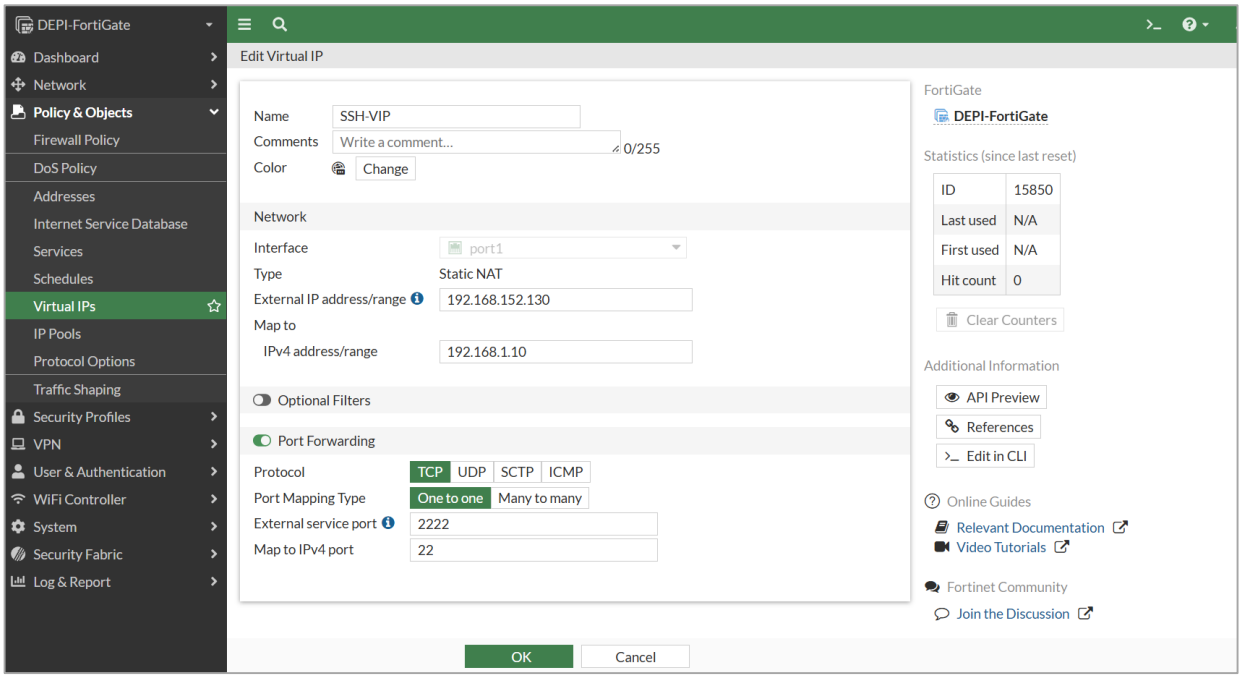


FIGURE 4.3.2

FIGURE 4.3.2: 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.

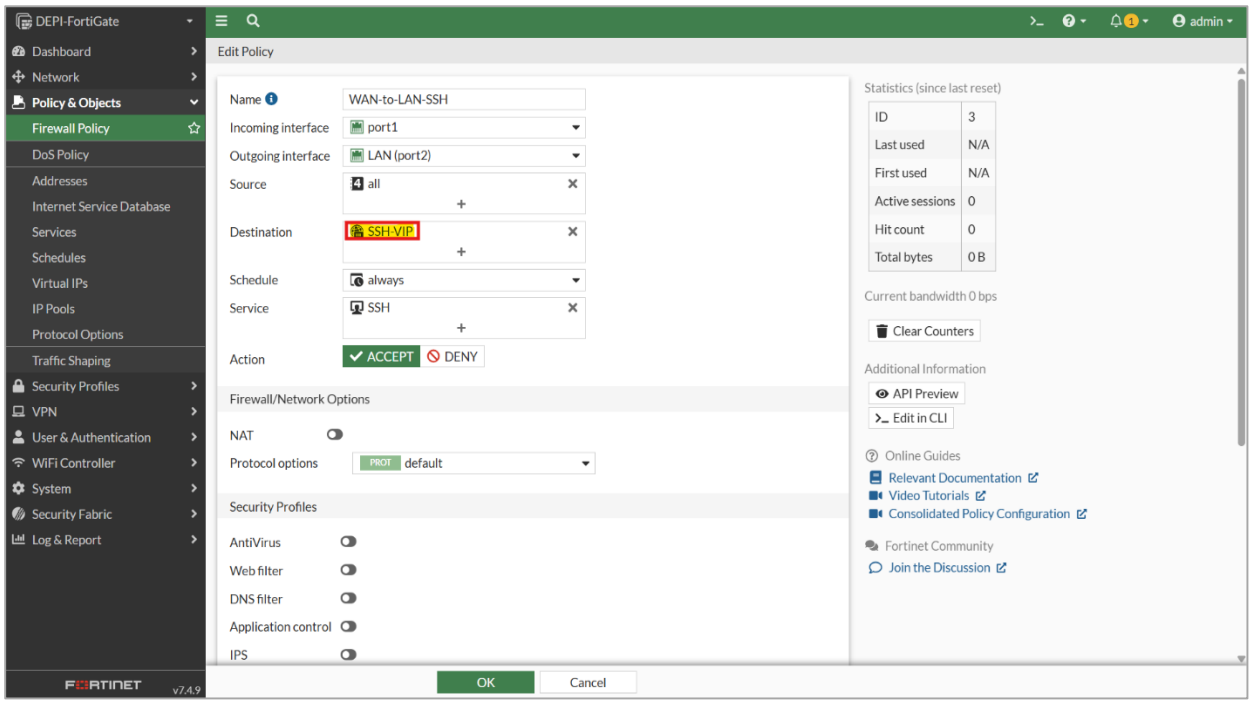


FIGURE 4.3.3

FIGURE 4.3.3: Inbound Service Access Policy. Firewall policy (`WAN-to-LAN-SSH`) allowing WAN-to-LAN traffic using the `SSH-Server-VIP` as the destination object.

4.3.2. Policy-Based Access Control

The objective was to implement a specific access policy to demonstrate granular traffic control and security filtering**.**

A. Granular Internet Access Policy

Goal	Procedure	Verification
Restrict general internet access to specific services (e.g., only HTTP/HTTPS) to enforce the principle of least privilege.	A new policy, `LAN-Web-Only`, was created (LAN to WAN, Source: All, Destination: All) but the **Service** field was restricted to include only `HTTP` and `HTTPS`	The LAN host could browse the web but was prevented from using services like FTP or Telnet via this specific policy.

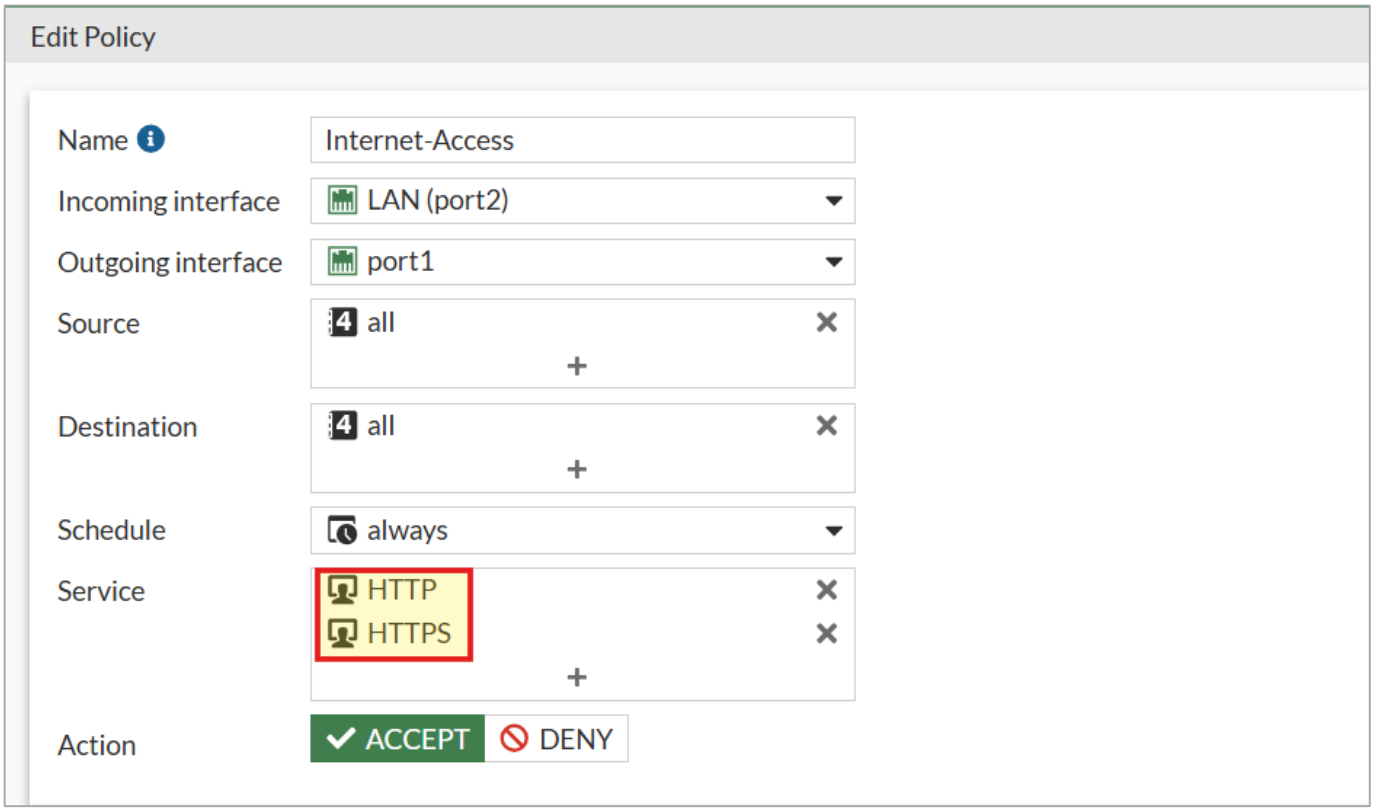


FIGURE 4.3.4

FIGURE 4.3.4: Granular Access Control Policy. Firewall policy (`Internet-Access`) restricting internal outbound traffic to only `HTTP` and `HTTPS` services.

B. Web Filtering Implementation

Goal	Procedure	Verification
Apply a security profile to block access to specific content categories (e.g., Social Media).	1. A **Web Filter Profile** (`Block-Social`) was created, enforcing a block on the "Social Networking" category. 2. The existing policy was edited to enable the **Web Filter** security profile and assign `Block-Social`.	Browsing a social media site (e.g., facebook.com) from the LAN Host (10.10.10.2) resulted in a successful FortiGate block page appearing.

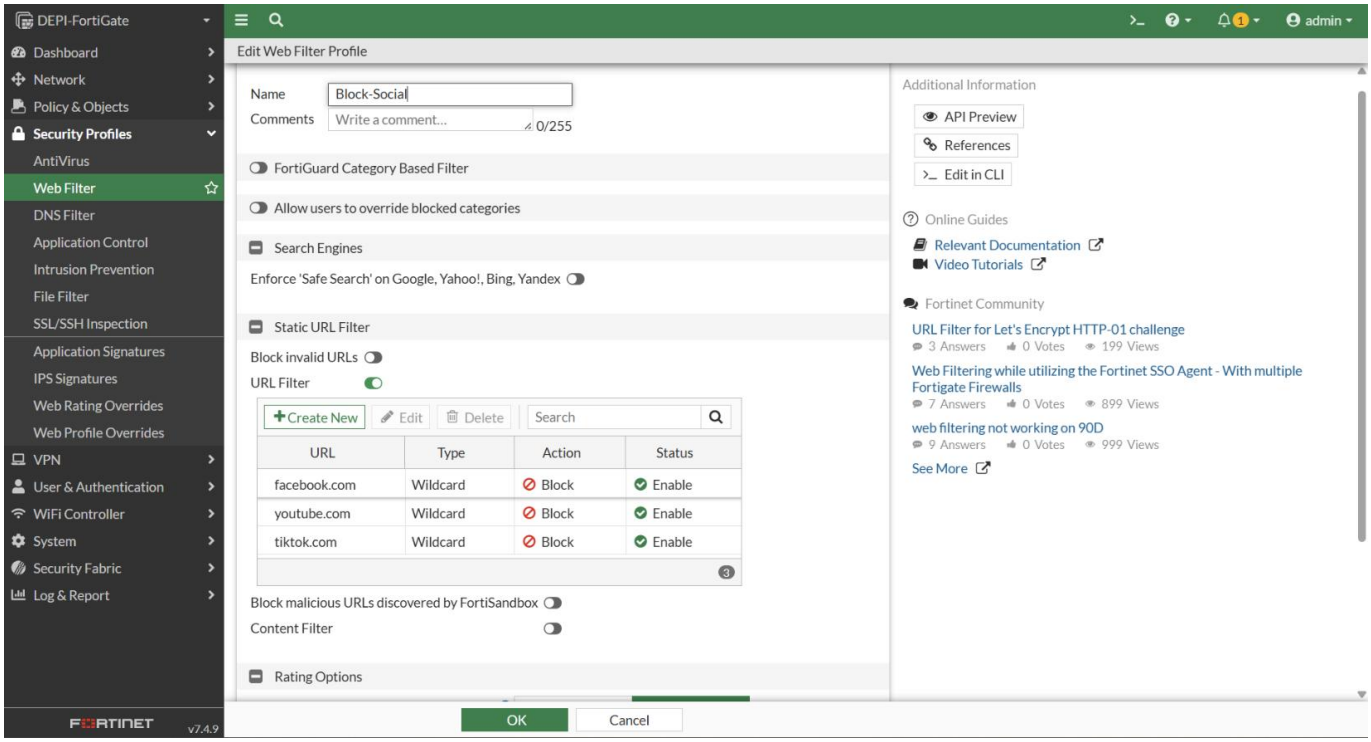


FIGURE 4.3.5

FIGURE 4.3.5: Web Filtering Profile Configuration. Details of the `Block-Social` profile enforcing a block on specific static URLs and the Social Networking category

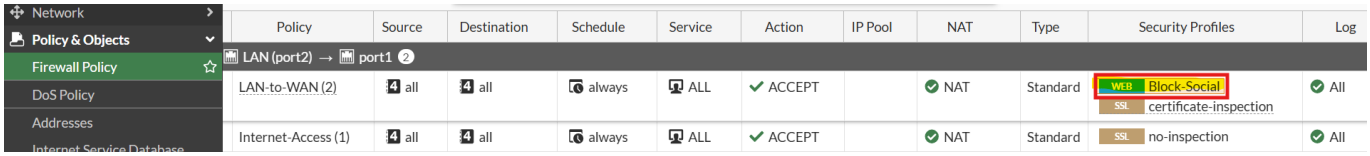


FIGURE 4.3.6

FIGURE 4.3.6: Applying Security Profiles. Firewall policy list showing the `Block-Social` security profile successfully applied to the LAN-to-WAN traffic

4.3.3. Verification and Testing

This section documents the essential functional tests performed to verify the correct implementation of the Network Address Translation (NAT) rules and the Web Filtering Security Profile, concluding the configuration for Task 3

A. Source NAT (SNAT) Test

The tests ensured that outbound traffic from the internal network (LAN) was correctly translated to the FortiGate's public-facing IP address.

Test Case	Procedure	Expected Result	Actual Result
Outbound Connectivity	Browse any website from the LAN Host (10.10.10.2).	Successful web page load.	Successful.
Log Validation	Check FortiGate Traffic Logs for the corresponding session.	The original Source IP (10.10.10.2) is confirmed to be translated to the WAN IP (e.g., 192.168.152.130).	Confirmed.

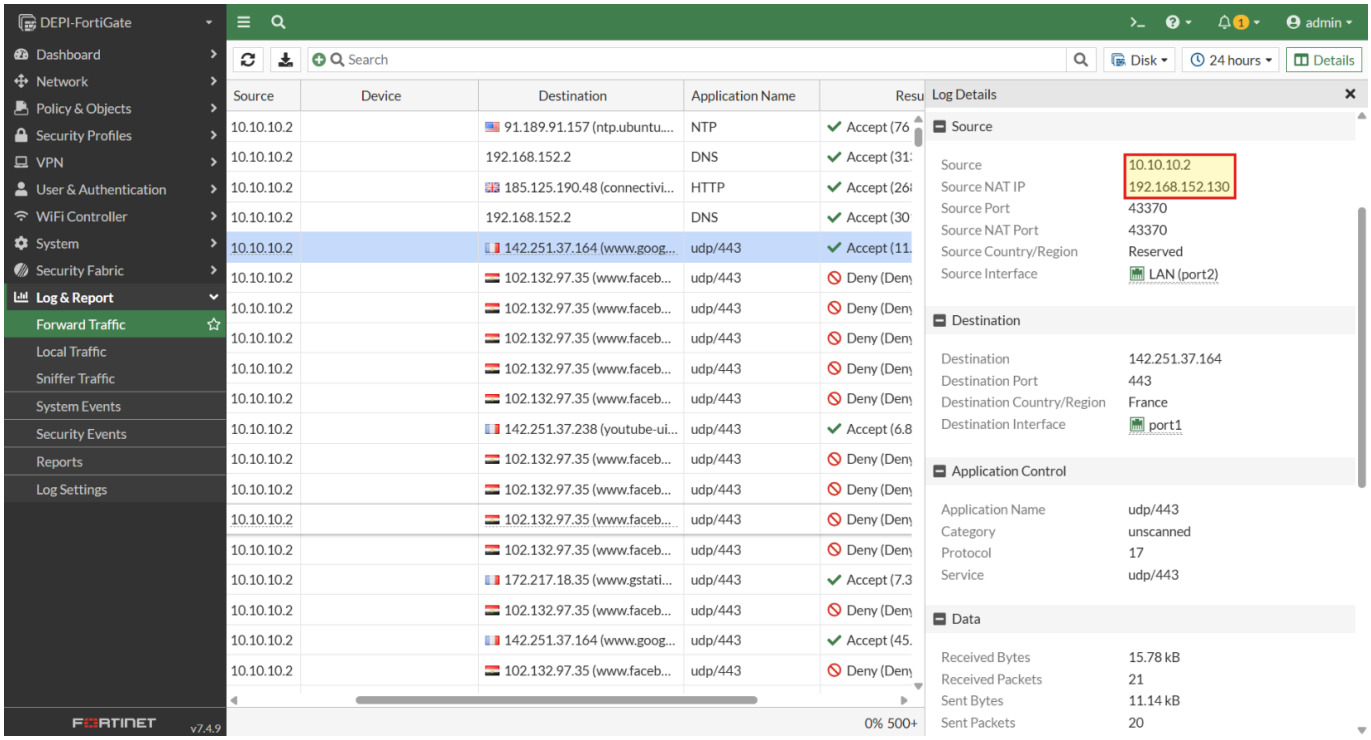


FIGURE4.3.7

FIGURE4.3.7 Source NAT Test Log Validation. Screenshot of the FortiGate Traffic Logs confirming the translation (SNAT) of the internal IP to the WAN interface IP

B. Destination NAT (DNAT) Test

These tests confirmed that the configured Virtual IP (VIP) and corresponding DNAT policy successfully allowed external access to the internal server.

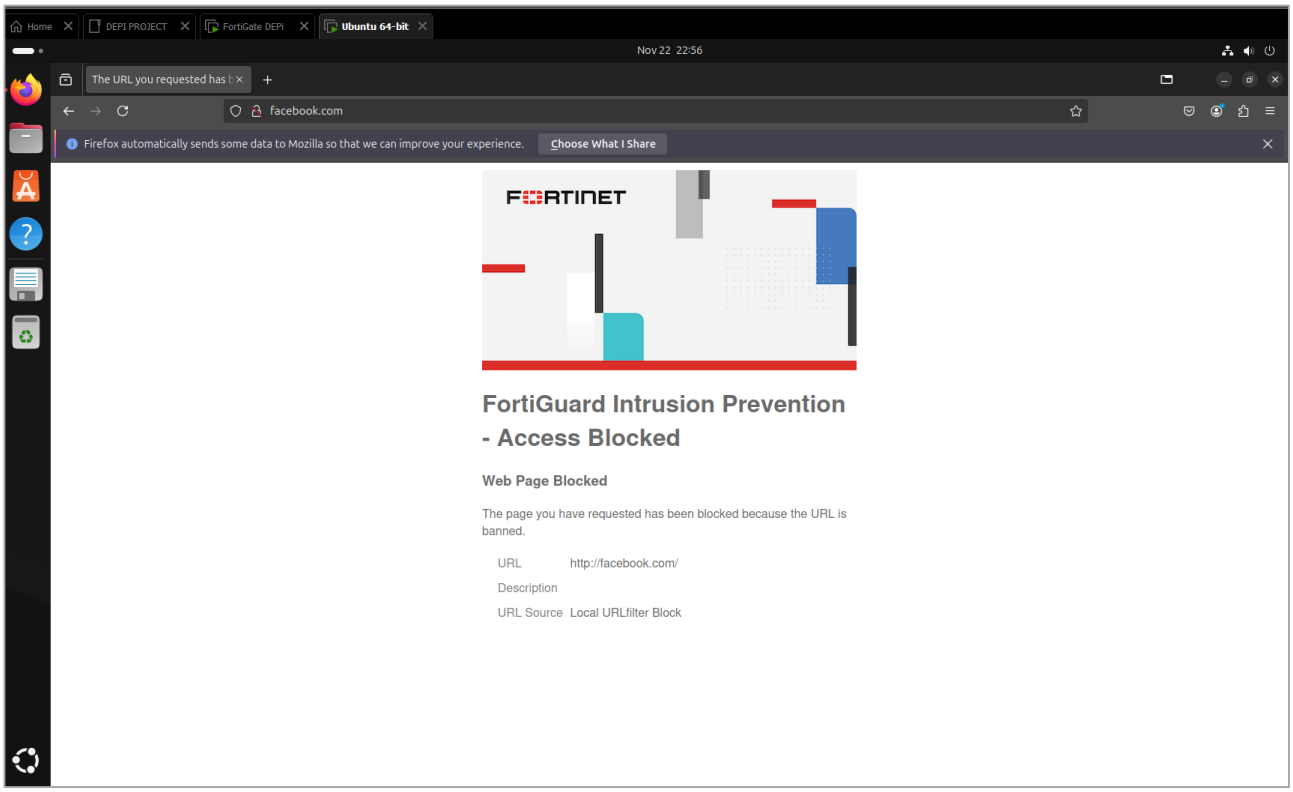
Test Case	Procedure	Expected Result	Actual Result
Inbound Service Access (SSH)	Attempt an SSH connection from the Host PC (external network) to the WAN IP (192.168.152.130) using the mapped port (TCP/2222).	The SSH client successfully connects and displays the login prompt for the internal server (10.10.10.2).	Successful.
Log Validation	Check FortiGate Traffic Logs for the inbound session.	The original Destination IP (192.168.152.130) is translated to the internal server IP (10.10.10.2).	Confirmed.

C .Web Filtering Test

This test validated the function of the `Block-Social` security profile to restrict access to prohibited content categories

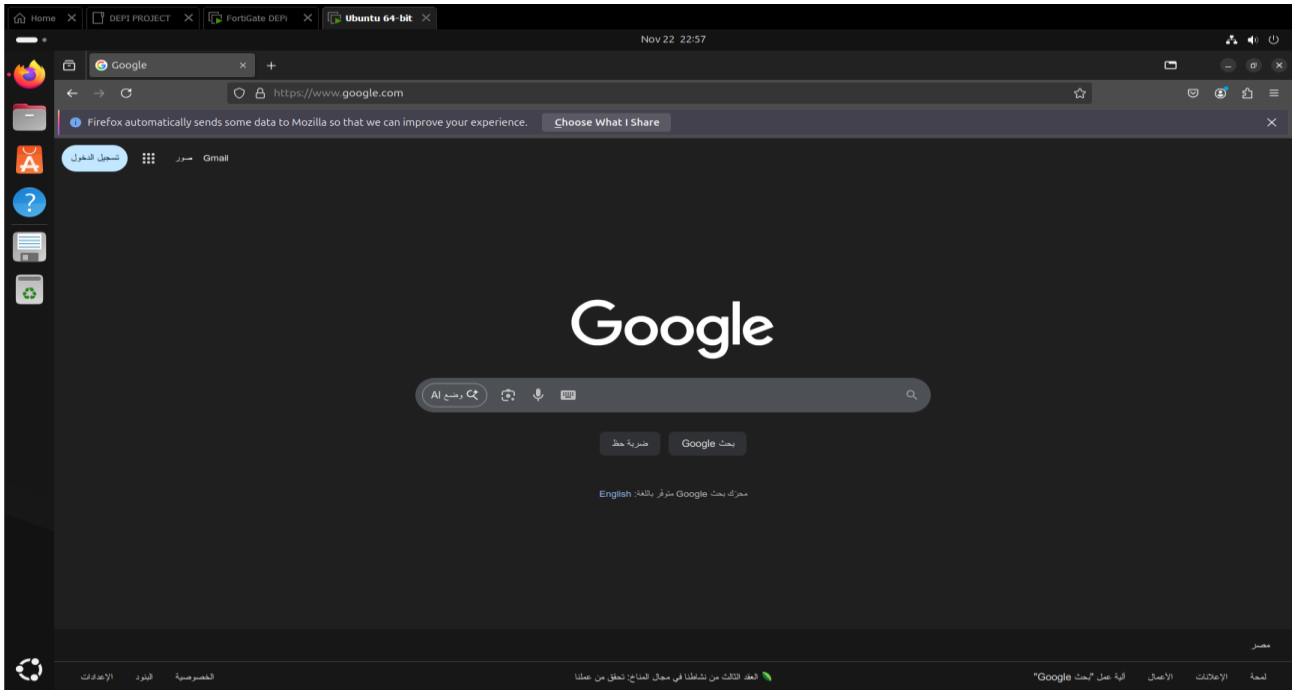
Test Case	Procedure	Expected Result	Actual Result
Content Block	Attempt to browse a social media site (e.g., facebook.com) from the LAN Host (10.10.10.2).	The FortiGate block page (Web Filter Block) appears in the browser.	Successful.
Allowed Access	Attempt to browse a normally allowed website (e.g., https://www.google.com/search?q=google.com) from the LAN Host.	The website loads successfully without intervention.	Successful.

Blocked websites like Facebook:



102.132.97.35 (www.faceb...	udp/443	Deny (Deny: UTM Blocked)	LAN-To-WAN (4)

Other websites are normally allowed like Google:



Final Conclusion and Future Recommendations

Project Summary

This Final Report serves as the comprehensive documentation for the **"Network Security Fundamentals and FortiGate Integration"** project, successfully transforming theoretical knowledge into a robust, resilient practical implementation. The defined objectives were achieved across four key phases, ranging from the deep analysis of contemporary cyber threats (e.g., RaaS and Phishing) and vital mitigation strategies (Zero Trust, Segmentation), to the advanced deployment and configuration of the FortiGate Next-Generation Firewall.

Key successes include the deployment of a functionally segmented virtual environment, the implementation and documentation of Network Address Translation (NAT) policies for secure internal/external connectivity, and the creation of granular Access Control Policies with verified Security Profiles (such as Web Filtering). The project has successfully demonstrated the technical competency required to build a fully secured network environment prepared for production use.

Recommendations and Future Enhancements

To further enhance the resilience of the built security architecture, the team strongly recommends focusing on the following future steps:

- **Activate Advanced NGFW Features:** Implement and test remaining Security Profiles, specifically **Application Control** and the **Intrusion Prevention System (IPS)**, to provide a deeper layer of protection against sophisticated, targeted threats.
- **Implement Remote Access VPN:** Establish either an **IPSec VPN** or **SSL VPN** connection to allow authorized users secure, encrypted access to the internal network resources, ensuring both business continuity and data confidentiality during remote operations.
- **Apply Multi-Factor Authentication (MFA):** A critical recommendation for all administrative access accounts to reinforce the defense layer against unauthorized access attempts utilizing compromised credentials.
- **Logging and Auditing Management:** Integrate the FortiGate with a centralized logging system (e.g., FortiAnalyzer or SIEM) to enable continuous monitoring and real-time security analysis of all traffic and events.

رواد مصر الرقمية