FORTINET DEVICE MANAGEMENT WITH FORTIMANAGER

PROJECT 5

Topic

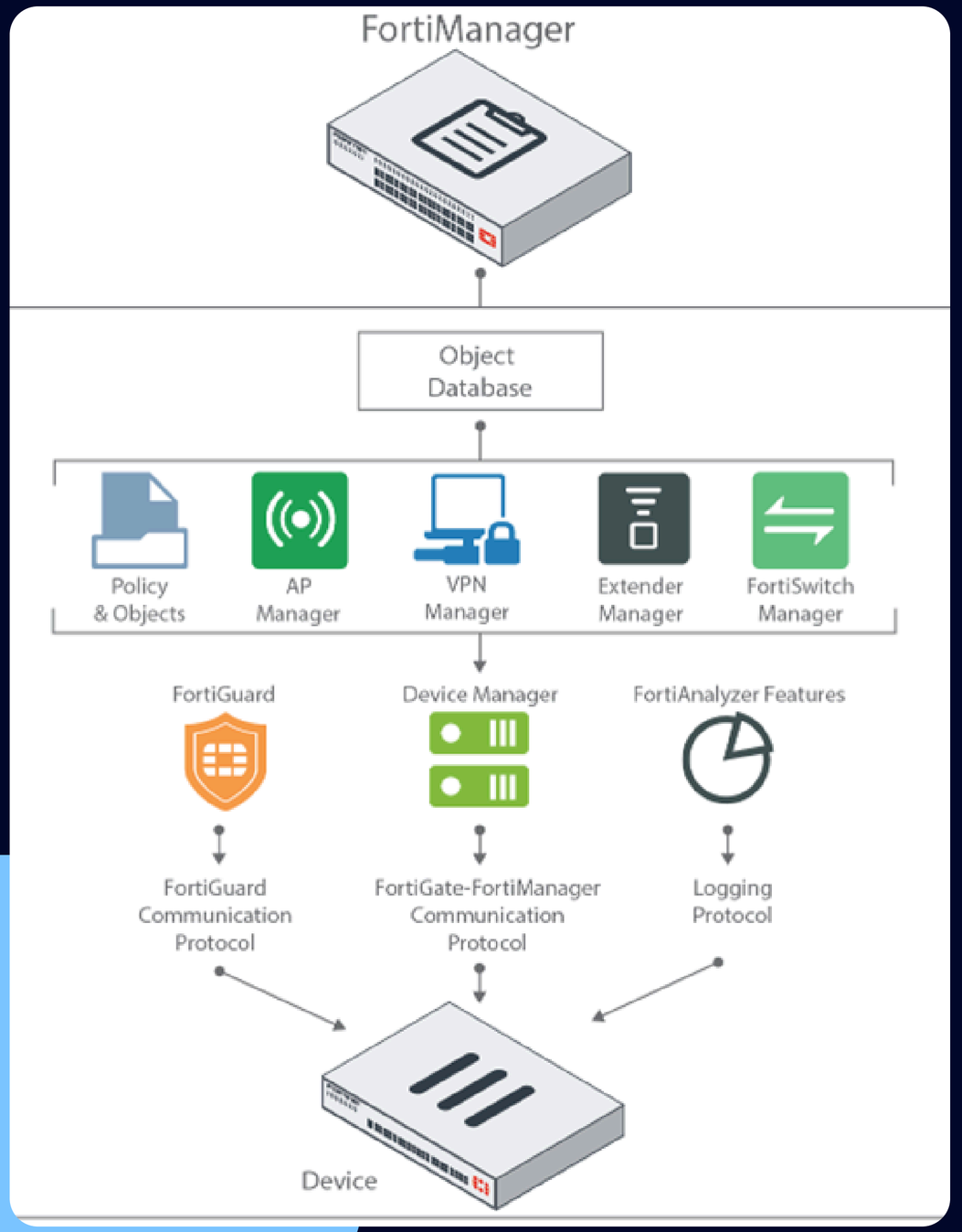
This project focused on implementing and configuring FortiManager to centralize and optimize the management of our Fortinet security infrastructure.

GOALS

01 Centralized Device Management

02 Improved Security Posture

03 Simplified Policy Administration



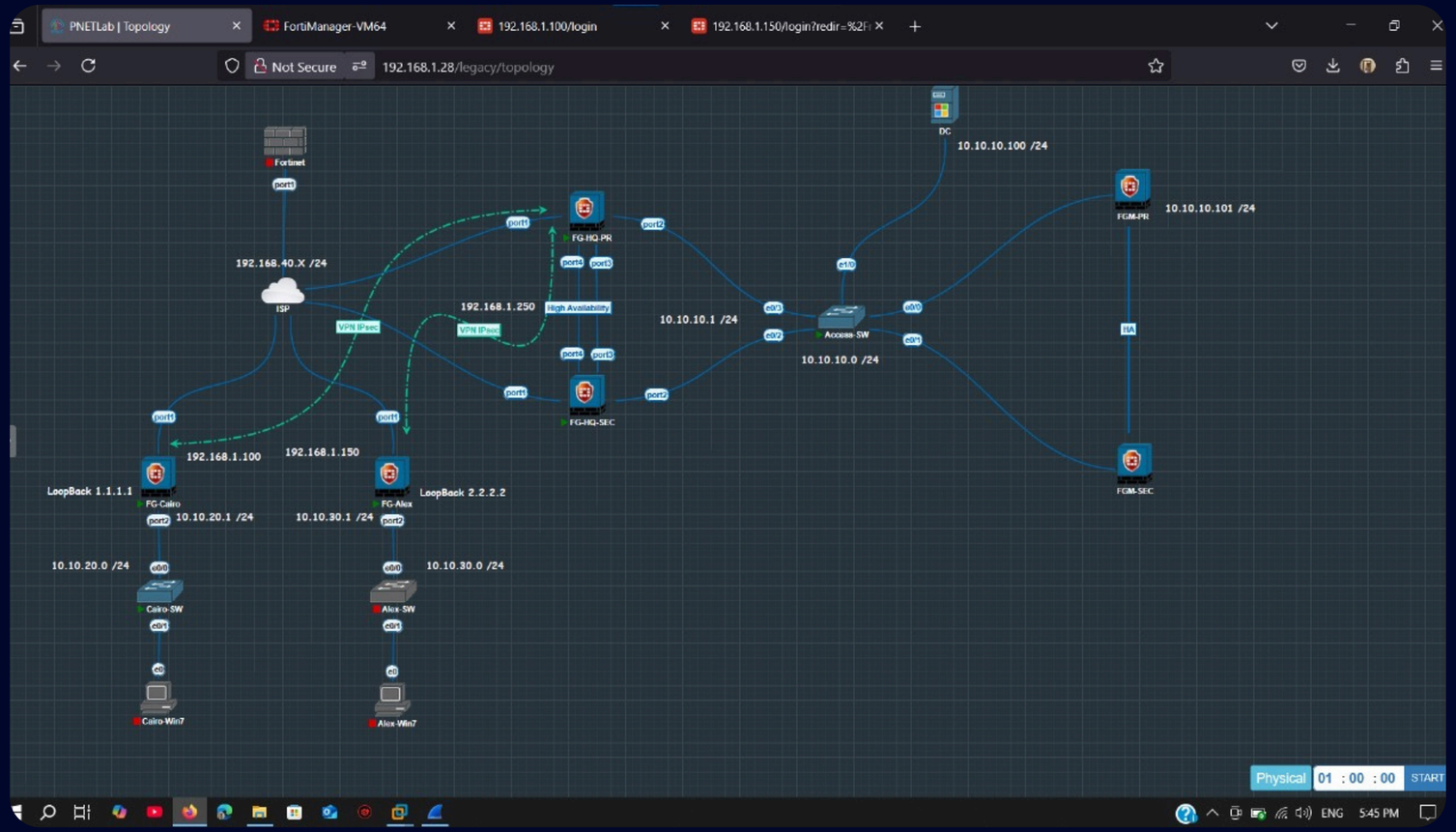
Why FortiManager

01
- Manual configuration of multiple devices is time-consuming and error-prone.

02
- FortiManager allows centralized provisioning, monitoring, and management.

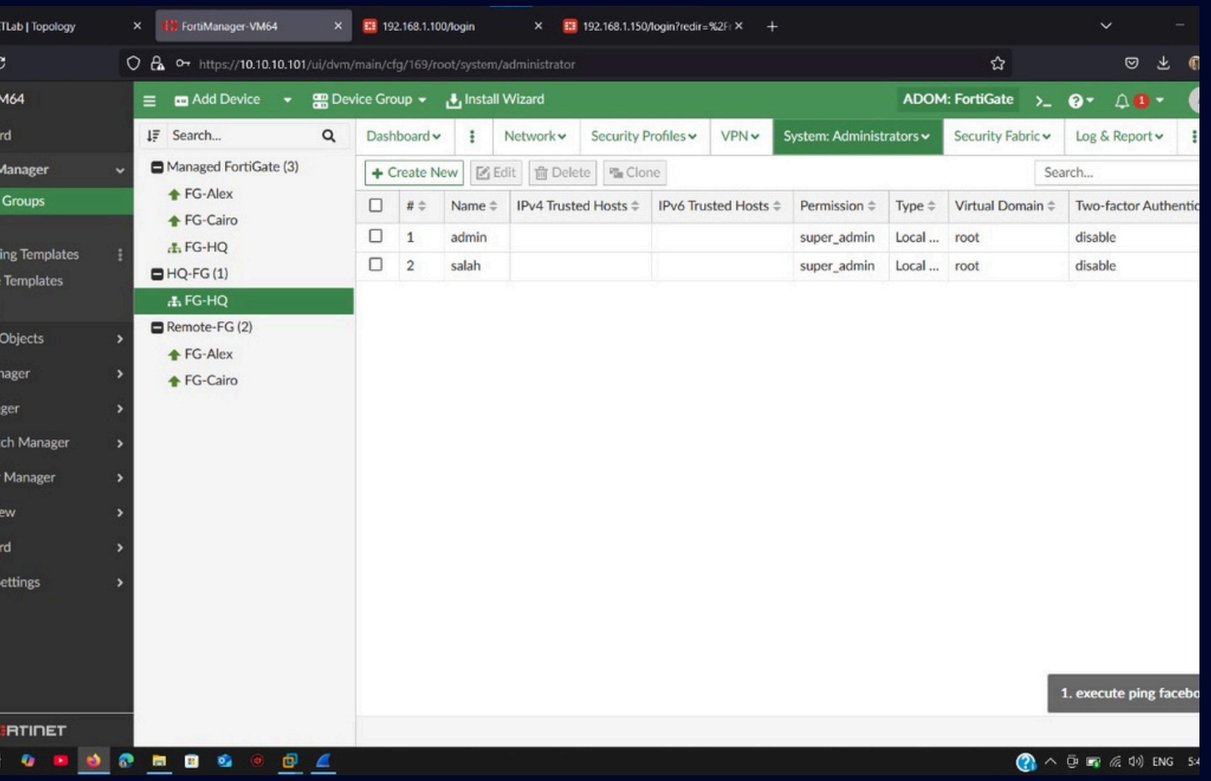
03
- It improves operational efficiency and strengthens network security posture.

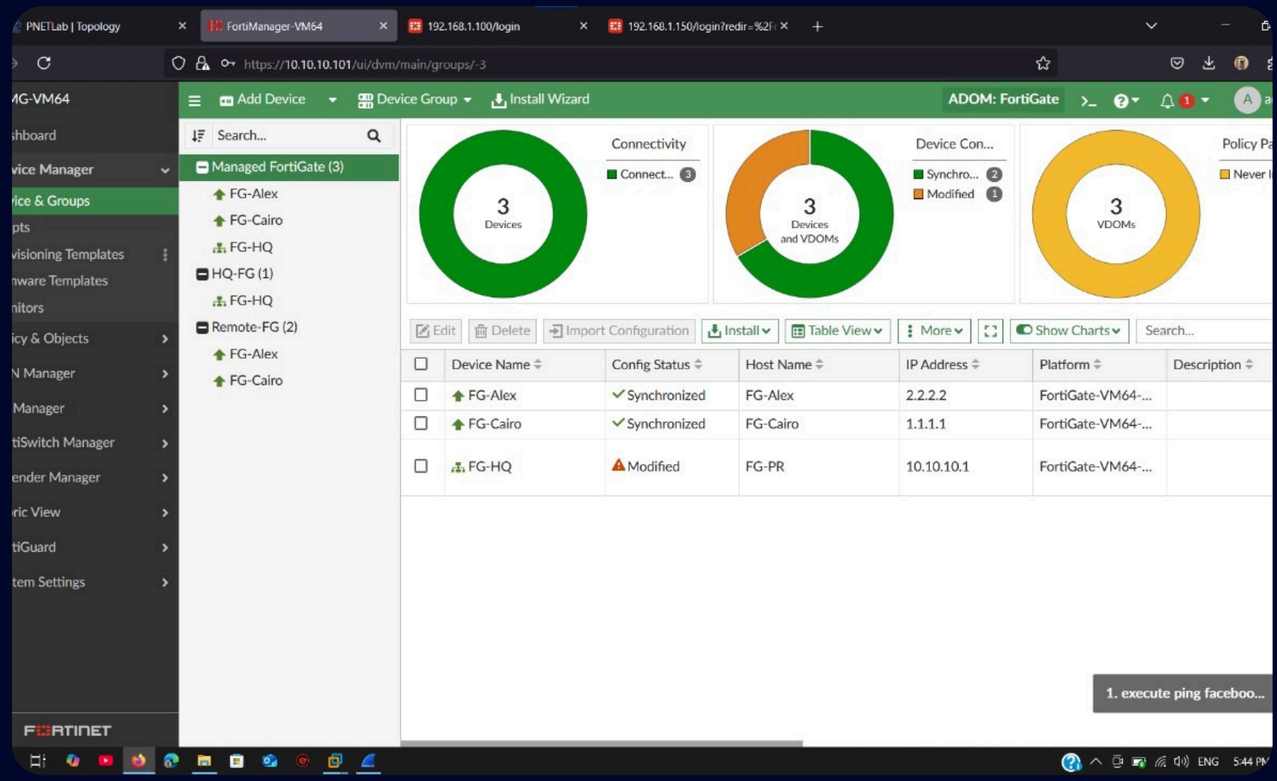
Our topology



- Three main sites: HQ, Cairo, and Alexandria
- Each site connected via IPsec VPN tunnels
- FortiManager deployed at HQ for centralized management
- All FortiGate devices managed under a single ADOM: “FortiGate”
- Implemented VDOMs for logical segmentation and isolation

Device Registration and Configuration



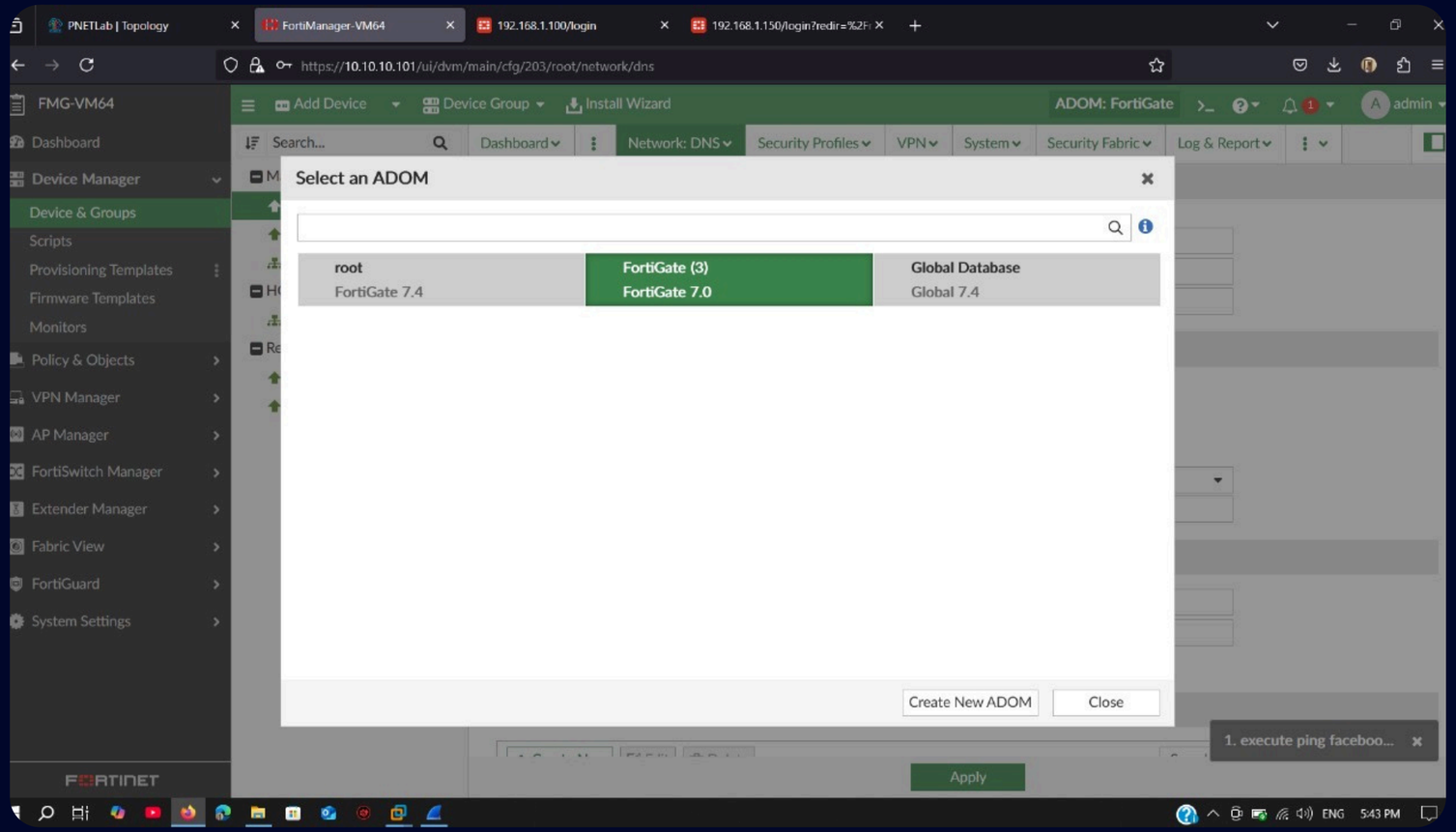


- Devices grouped and monitored from FortiManager dashboard
- 2 administrator accounts created for role-based access control:
- Super Admin (full access)
- Read-Only Admin (full access)
- Supports secure and structured management across all devices

What is ADOM?

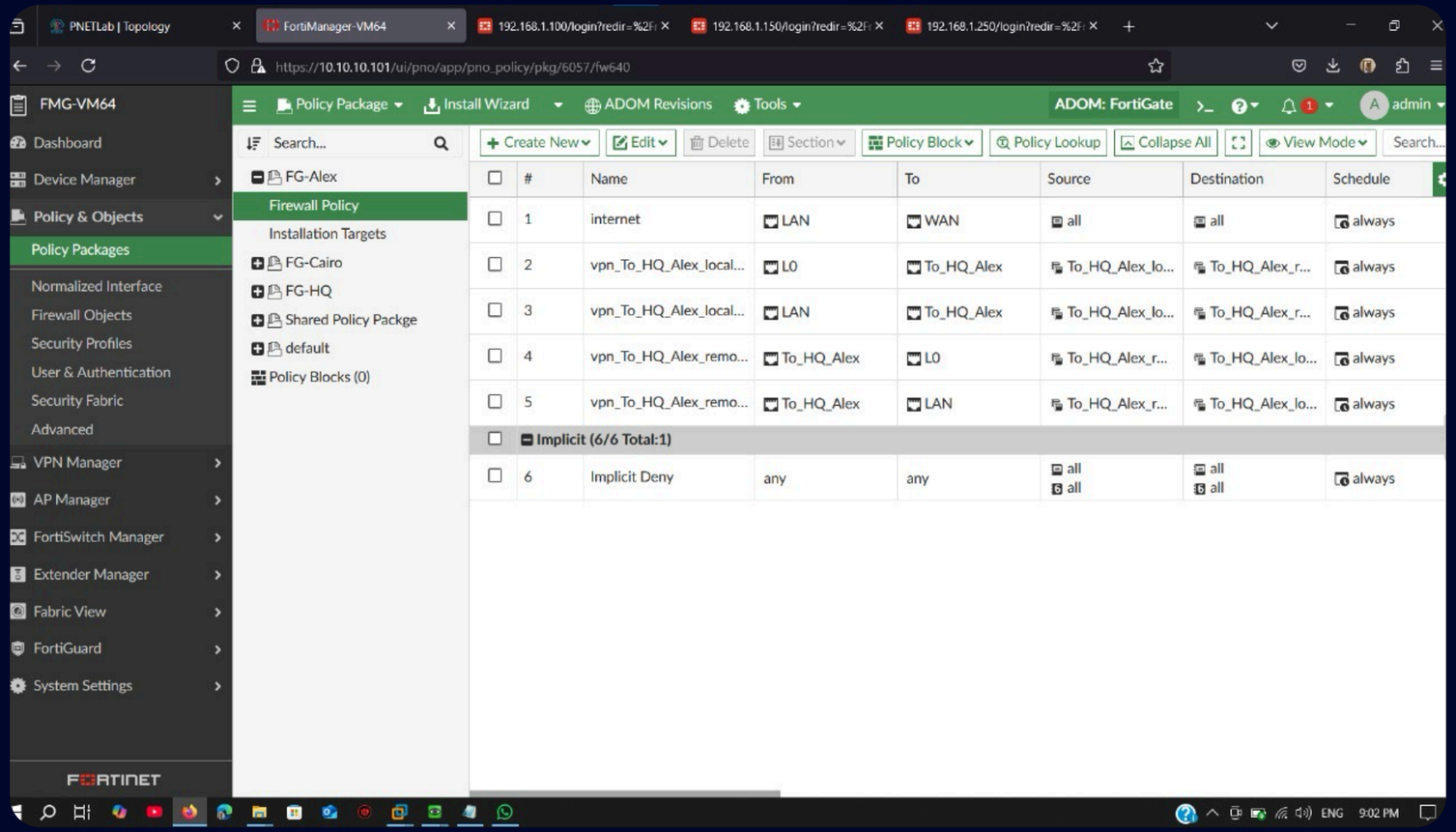
- ADOM stands for Administrative Domain. It is a logical partition within FortiManager that allows you to separate configurations and management tasks for different sets of devices, policies, and configurations.
- It provides an additional layer of security, scalability, and manageability by organizing the FortiManager system.
- Why is it used?!
- Multi-Tenant Environments
- Separation of Configuration and Administration:
- Simplified Device and Policy Management

ADOM



- ADOMs allow logical separation of devices and configurations
- Suitable for managing multiple devices under one administrative scope
- Simplifies policy management and monitoring for all devices
- All FortiGate devices (HQ, Cairo, Alexandria) assigned to this ADOM

Policy management



- Policy #1 allows internet access from the LAN to the WAN.
- Policies #2 to #5 handle VPN traffic between the local site and headquarters, specifying directions and interfaces like LAN, L0, and To_HQ_Alex.
- Policy #6 is the default Implicit Deny rule, which blocks any traffic that doesn’t match a defined policy — a crucial security measure to ensure only explicitly allowed traffic is permitted.

Thank You

Team members:

Salah Zedan
Ahmed Elsawah
Ahmed Hanafy
Fatma Abdelfatah
Mohamed Salah
Shahd Haitham