

FORTINET



FortiManager

FORTINET DEVICE MANAGEMENT WITH FORTIMANAGER

P R O J E C T 5

FORTINET.



FortiManager

Topic

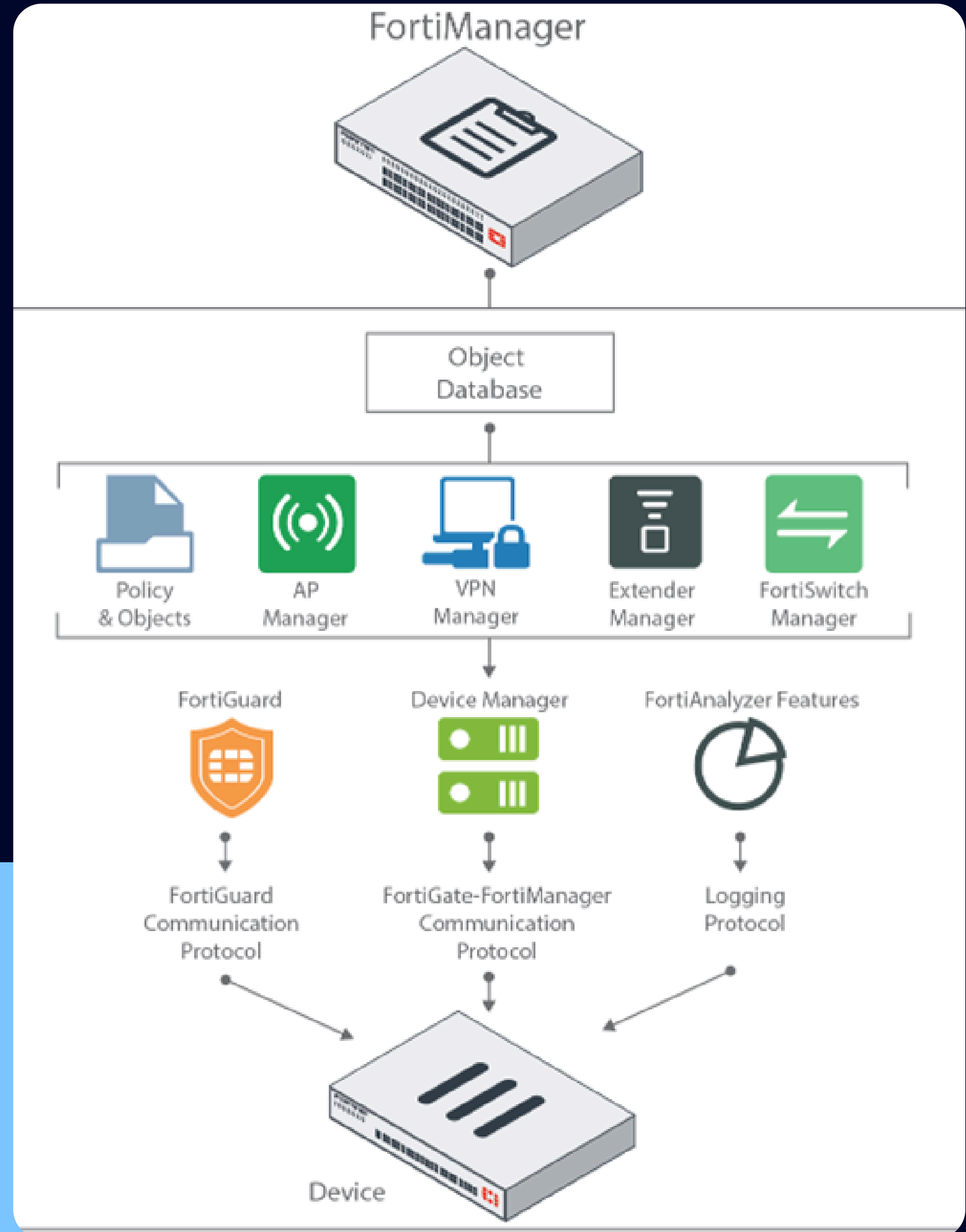
This project focused on implementing and configuring FortiManager to centralize and optimize the management of our Fortinet security infrastructure.

GOALS

01 Centralized Device Management

02 Improved Security Posture

03 Simplified Policy Administration

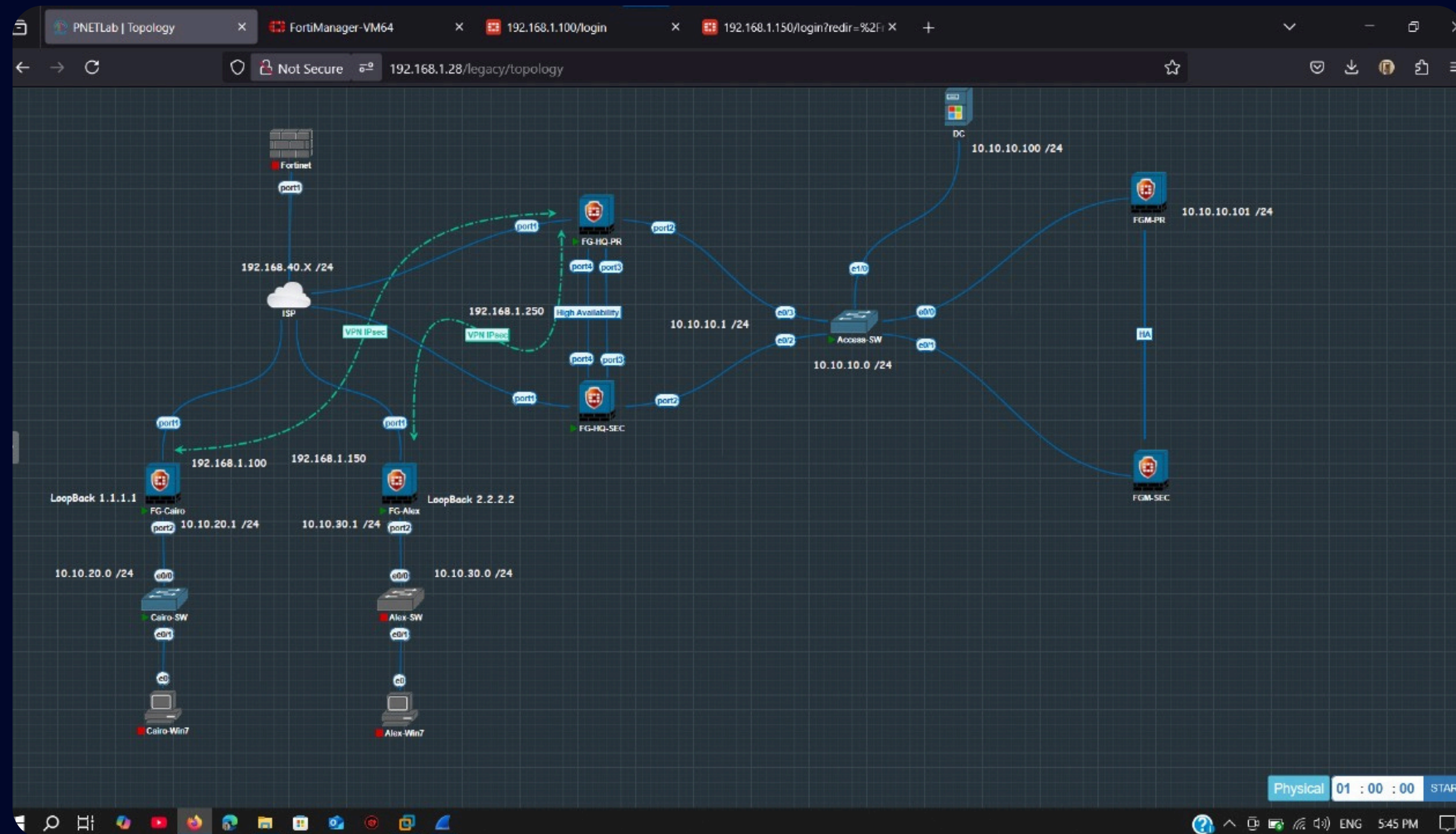


Why FortiManager



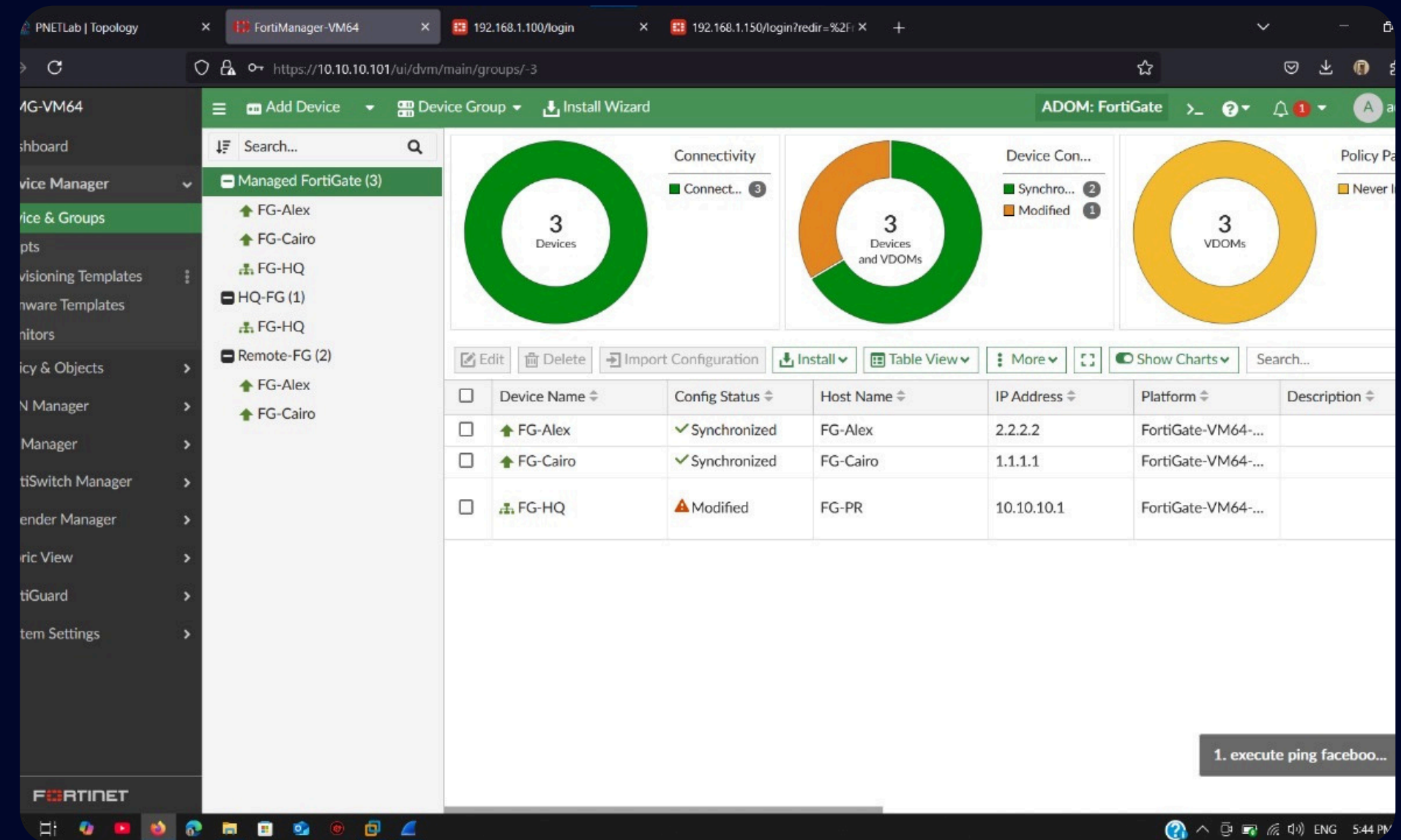
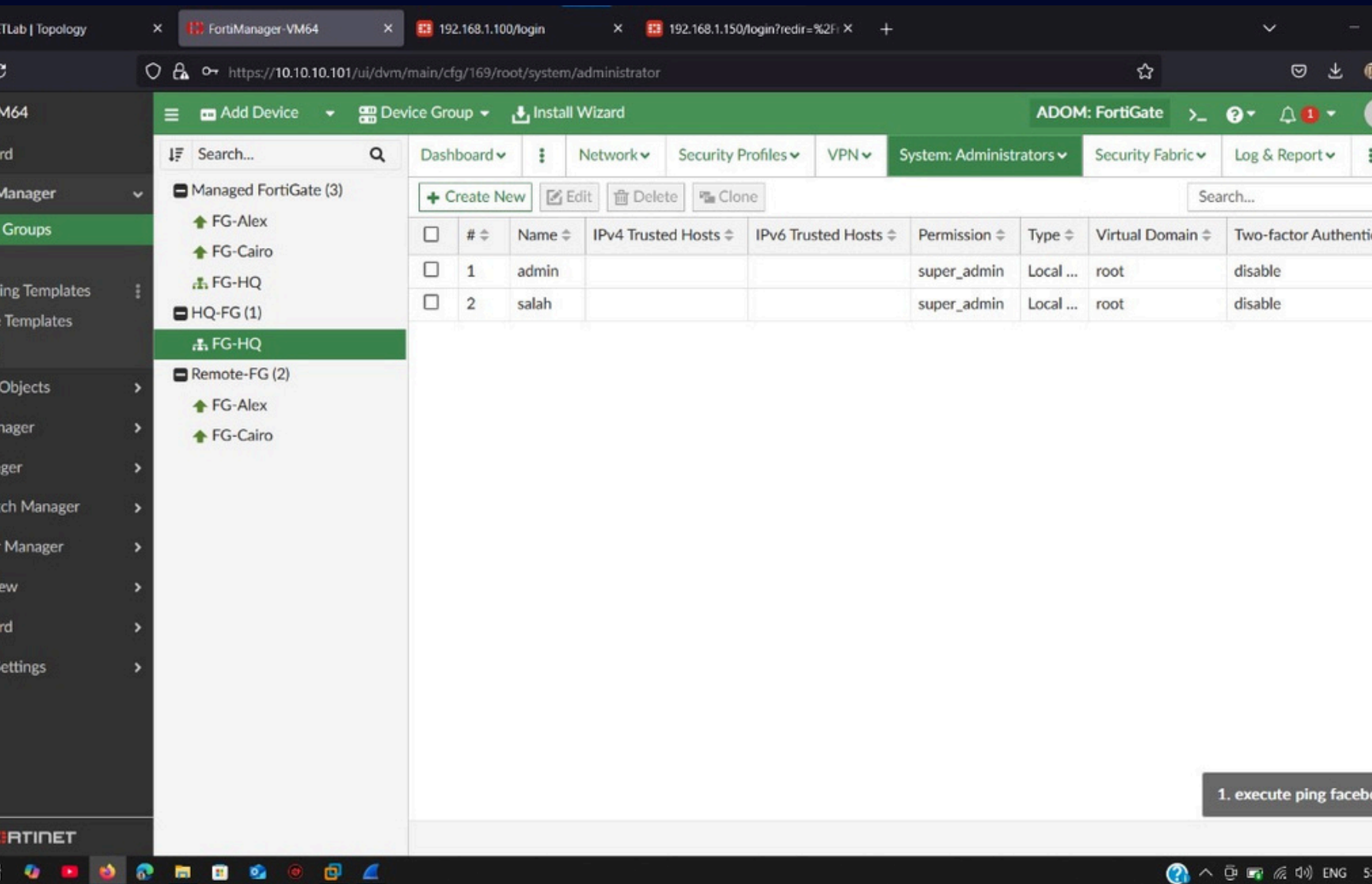
- 01 • Manual configuration of multiple devices is time-consuming and error-prone.
- 02 • FortiManager allows centralized provisioning, monitoring, and management.
- 03 • It improves operational efficiency and strengthens network security posture.

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

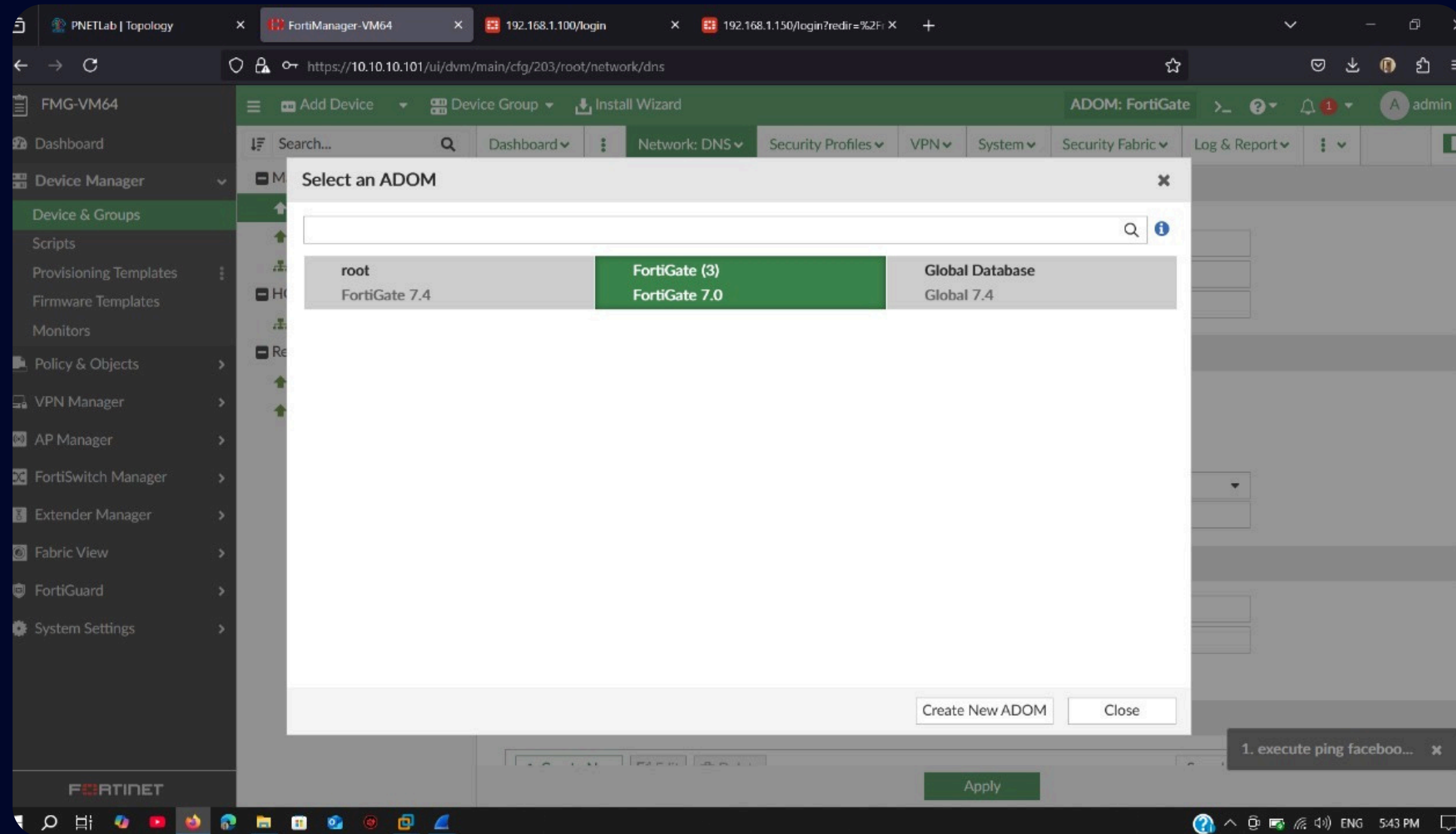


- Devices grouped and monitored from FortiManager dashboard
- 2 administrator accounts created for role-based access control:
 - Super Admin (full access)
 - Read-Only Admin (full access)
- Supports secure and structured management across all devices

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

The screenshot shows the FortiManager web interface for managing firewall policies. The left sidebar contains navigation options: Dashboard, Device Manager, Policy & Objects (selected), VPN Manager, AP Manager, FortiSwitch Manager, Extender Manager, Fabric View, FortiGuard, and System Settings. The main content area is titled 'Firewall Policy' and shows a table of policies. The table has columns for #, Name, From, To, Source, Destination, and Schedule. Policies 1 through 5 are explicitly defined, and Policy 6 is the Implicit Deny rule.

#	Name	From	To	Source	Destination	Schedule
1	internet	LAN	WAN	all	all	always
2	vpn_To_HQ_Alex_local...	L0	To_HQ_Alex	To_HQ_Alex_lo...	To_HQ_Alex_r...	always
3	vpn_To_HQ_Alex_local...	LAN	To_HQ_Alex	To_HQ_Alex_lo...	To_HQ_Alex_r...	always
4	vpn_To_HQ_Alex_remo...	To_HQ_Alex	L0	To_HQ_Alex_r...	To_HQ_Alex_lo...	always
5	vpn_To_HQ_Alex_remo...	To_HQ_Alex	LAN	To_HQ_Alex_r...	To_HQ_Alex_lo...	always
Implicit (6/6 Total:1)						
6	Implicit Deny	any	any	all	all	always

- 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 Elsayah

Ahmed Hanafy

Fatma Abdelfatah

Mohamed Salah

Shahd Haitham

