Cources Center Network(HQ + 1BR)

Supervisores:

Dr. Hussen Harb

Eng. Elhosein Ahmed

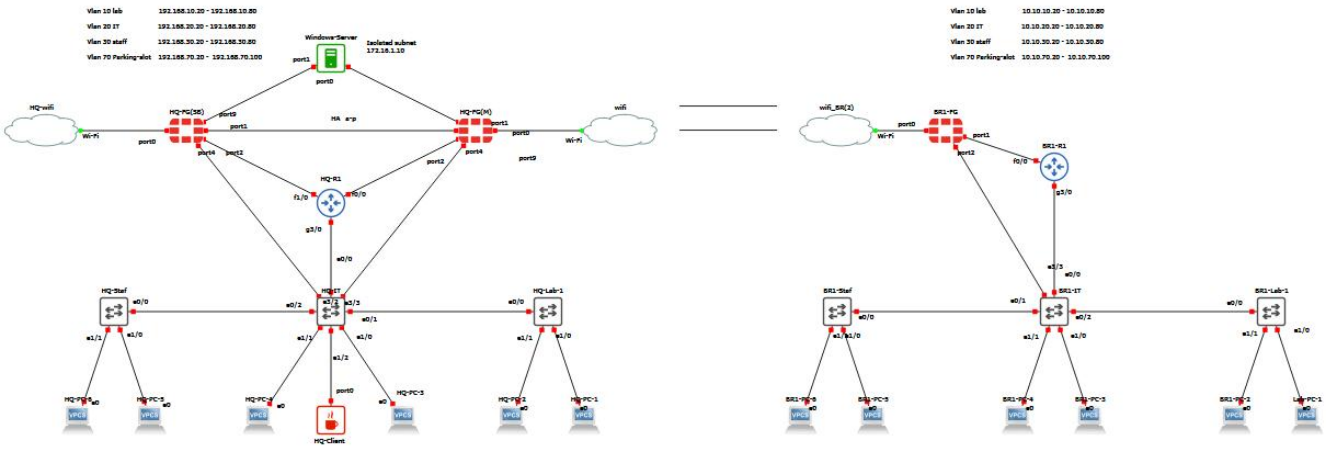
Group ID: R3_DEPI3_CAI3_ISS8_S2 Fortinet Cybersecurity Engineer

Name	ID
Mina Romany Shawky	21038827
Hossam Mohamed Jamal	21063285
Youssef Ahmed Hassan	21065584
Youssef Usama Mohamed	21043953
Abdalla Alaa Eldyn Atya	21054375
Yousef Elsayed Fakhry	21088058

Table of Content

1. Introduction

1.1 Cources Center (HQ + 1BR) Topology:



1.2 Device Inventory:

Site	Device type	Quantity	Host Name	Role
HQ	FortiGate	2	HQ-FG-1, HQ-FG-2	Security
HQ	Router	1	HQ-R1	Core routing
HQ	L2 Switch	3	HQ-Lab1, HQ-IT, HQ-STAF	Core switching
HQ	Server	1	DC-1	AD
BR-1	FortiGate	1	BR1-FG-1	Security
BR-1	Router	1	BR1-R1	Core routing
BR-1	L2 Switch	3	BR1-Lab1, BR1-IT, BR1-STAF	Core switching

1.3 IP Addressing Schema:

1.3.1 HQ Subnets

Name	Network	Getway	VLAN ID	Purpose
Servers	172.16.1.0	172.16.1.10	80	Core servers
Lab-1	192.168.10.0	192.168.10.1	10	Trainees and Instructors
IT	192.168.20.0	192.168.20.1	20	IT staf
Staf	192.168.30.0	192.168.30.1	30	Remain workers

1.3.1 HQ Subnets

Name	Network	Getway	VLAN ID	Purpose
Lab-1	10.10.10.0	10.10.10.1	10	Trainees and Instructors
IT	10.10.20.0	10.10.20.1	20	IT staf
Staf	10.10.30.0	10.10.30.1	30	Remain workers

1.4 Project Overview :Secure Multi-Site Enterprise Network with Fortinet Security Fabric:

1.4.1 Cources Center Network:

Secure Enterprise Network with Fortinet Security Fabric – HQ + Branch Office Deployment.

1.4.2 Business Objectives

- Provide secure, highly available network services for HQ and Branch users
- Centralize authentication on a single Windows Server (Active Directory)
- Deliver full remote worker support via IPsec-VPN
- Securely connect HQ and Branch with IPsec site-to-site VPN
- Implement Zero-Trust segmentation using Fortinet Security Fabric

1.5 Core Components & Architecture:

1.5.1 High-Availability FortiGate Cluster (HQ)

- 2 × FortiGate firewalls in Active/Passive HA cluster
- All interfaces and policies synchronized
- Single virtual IP for all zones used by clients and routers

1.5.2 FortiGate (Branch)

- Single FortiGate for cost optimization (can be upgraded to HA later)
- Site-to-site IPsec VPN tunnel to HQ HA cluster

1.5.3 Fortinet Security Fabric

- Root FortiGate = HQ HA cluster
- Windows Server authorized and added into Security Fabric
- Fabric telemetry, FortiClient EMS integration, and automatic quarantine possible

1.5.4 Windows Server 2016 (HQ – placed in DMZ)

1.5.4.1 Roles installed:

– Active Directory Domain Controller

– LDAP server (used for FortiGate user authentication – SSL-VPN & administrative logins).

1.5.4.2 Machine is joined to Security Fabric for visibility and automatic IOC sharing

1.5.5 Remote Access

- FortiGate IPsec-VPN (GlobalProtect-style portal & tunnel mode)
- Authentication against Active Directory via LDAP
- Full-tunnel options configured per group

1.5.6 Site-to-Site Connectivity

- Permanent IPsec VPN tunnel between HQ HA cluster and Branch FortiGate
- Full reachability for all VLANs in both directions
- Encrypted traffic with DES (the only available method for our version)

1.5.7 Inter-VLAN Routing

- HQ & BR: Router-on-a-Stick on the HQ FortiGate cluster
- Sub-interfaces for VLAN 10, 20, 30, on the internal port

1.5.8 DHCP Strategy

- HQ: DHCP scopes served directly from Relay (ip-helper) from the main router (HQ-R1)
- Branch: DHCP Relay (ip-helper) configured on the main router (BR1-R10) as HQ.

1.5.9 Security Profiles (Applied on all FortiGates)

- Deep packet inspection (Application Control, IPS, AntiVirus, Web Filter)
- SSL/SSH inspection enabled
- All policies logged to FortiAnalyzer (or FortiGate Cloud)

1.6 Key Benefits

- Single Active Directory for authentication everywhere (VPN, Wi-Fi, admins)
- Full high availability at headquarters
- Centralized logging, policy, and visibility via Security Fabric
- Consistent security policy enforcement at both sites
- Easy future scaling (add more branches or upgrade Branch to HA)

1.7 Challenges:

- We don’t have enough resources to expand our project
- We don’t have FortiGuard licence
- We couldn’t test the security profiles because of licence
- Don’t have FrtiAnaluzer to put in security fabric for the logs

2. FortiGate Rules and Configurations:

2.1 FortiGate Firewall Deployment & Network Segmentation:

2.1.1 VLAN and IP Addressing Schema:

- VLANs were implemented to securely segment departments and apply different network access levels.
- The Windows Server VLAN remained isolated, while IT, Staff, and LAB networks were routed only through controlled firewall rules.

VLAN Name	Subnet Range	Assigned Purpose
VLAN 10 – LAB	192.168.10.20– 192.168.10.80	Student & training zone
VLAN 20 – IT	192.168.20.20– 192.168.20.80	IT department access
VLAN 30 – STAFF	192.168.30.20– 192.168.30.80	General employee usage
VLAN 70 – Parking/Guest	192.168.70.20– 192.168.70.100	Visitor network
Windows Server VLAN	172.16.1.0/24	AD server

2.1.2 Firewall Interface Configuration:

- The FortiGate appliance operated with four main interfaces.
- Port0 obtained its IP via DHCP from the ISP router.
- Port1 hosted the isolated Windows Server VLAN.
- Port4 served as the LAN trunk, carrying all user VLANs and supporting DHCP relay.
- Port3 linked the firewall to the router for outbound internet traffic.

Interface	Role	IP Address / Assignment
Port0	WAN - Internet uplink	DHCP from ISP
Port1	Windows Server VLAN	Static 172.16.1.10
Port4	LAN Trunk / VLAN access	192.168.x.x subnets
Port3	Firewall → Router Link	WAN handoff, router NAT

2.1.3 Firewall Rules & Security Policies:

- Firewall policies were configured to strictly control flows between VLANs and to the internet.
- Security profiles (App Control, IPS, Web Filter, SSL Deep Inspection) were applied based on department sensitivity.

Policy Target	Source	Destination	Security Profile Applied
Internet access for IT	IT VLAN	WAN	Deep Inspection + AV + IPS
Internet access for Staff	STAFF VLAN	WAN	Web Filter + IPS
Student/Lab Permission	LAB VLAN	WAN	Restricted access + filtering
Server outbound	Server VLAN	WAN	Certificate & DPI inspection
Inbound Response Handling	WAN	Internal VLANs	State-based return traffic

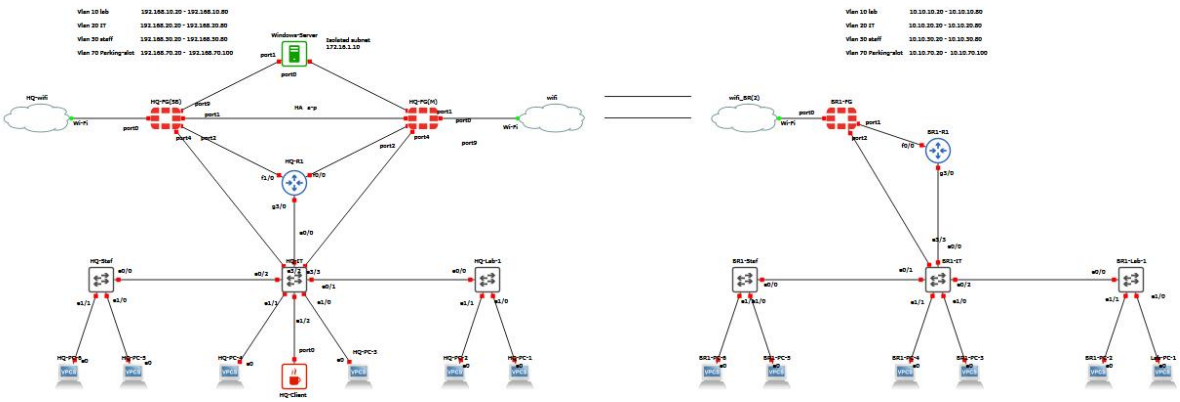
2.1.4 Results & Validation:

Validation tests confirmed the following:

- Successful inter-VLAN routing through the FortiGate
- DHCP leases correctly served from the Router
- Internet access functioning for all departments according to applied rules
- Security profiles enforced correctly
- Logs verified policy hits and traffic patterns

2.1.5 Configuration Pictures:

2.1.5.1 Network Topology:



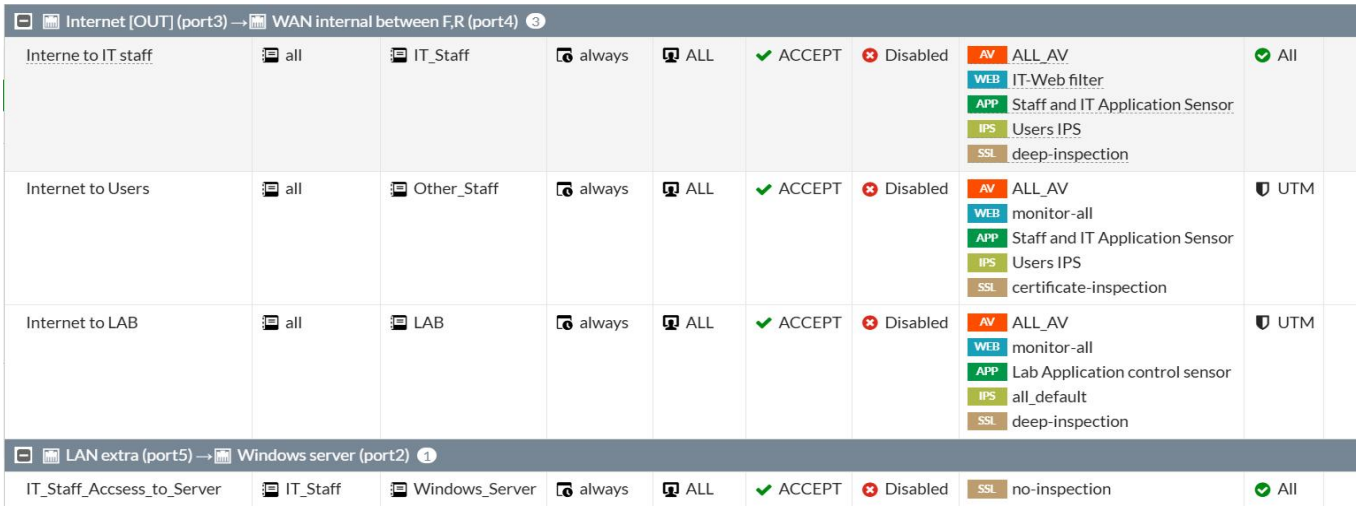
2.1.5.2 Address Objects:

LAB	192.168.10.0/26	WAN internal between F,R (port4)	Address	3
Other_Staff	192.168.30.0/26	WAN internal between F,R (port4)	Address	3
SSLVPN_TUNNEL_ADDR1	10.212.134.200 - 10.212.134.210	SSL-VPN tunnel interface (ssl.root)	Address	1
Windows_Server	172.16.1.10/32	Windows server (port2)	Address	2
all	0.0.0.0/0		Address	9
none	0.0.0.0/32		Address	0
FQDN 6				
Address Group 3				
ALL_Internet_Acsses	LAB Other_Staff IT_Staff	WAN internal between F,R (port4)	Address Group	0

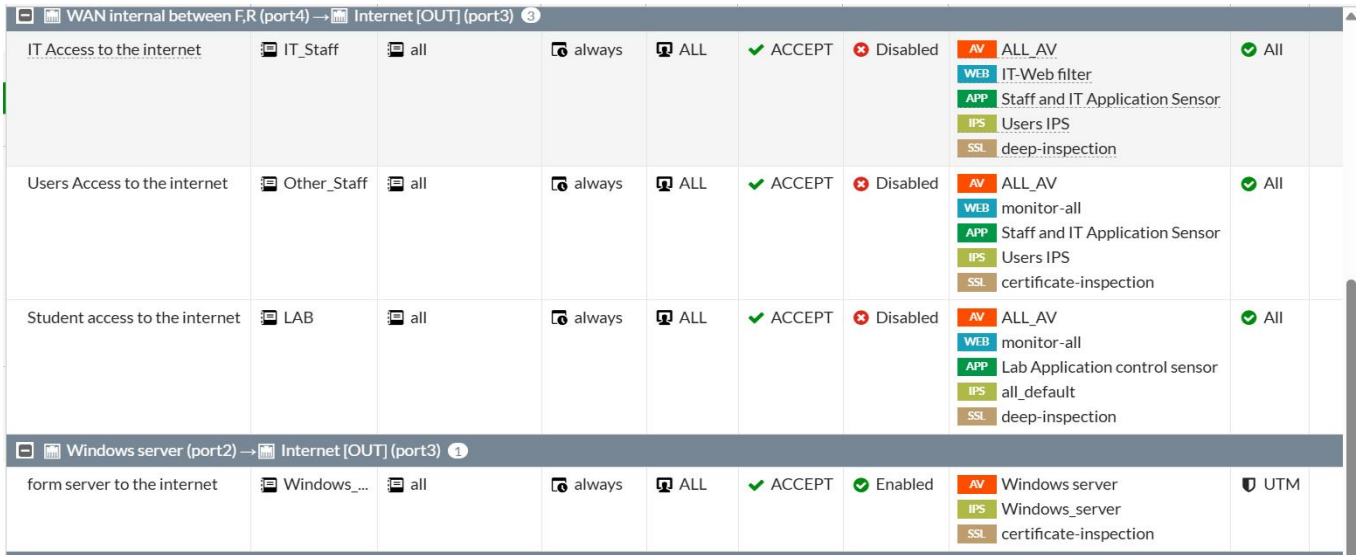
2.1.5.3 Interfaces:

Physical Interface 10							
Internet [OUT] (port3)	Physical Interface		192.168.1.7/255.255.255.0	PING HTTPS SSH FTM			8
LAN extra (port5)	Physical Interface		192.168.40.1/255.255.255.0	PING HTTPS SSH SNMP +2			1
WAN internal between F,R (port4)	Physical Interface		192.168.100.1/255.255.255.252	PING HTTPS SSH SNMP +3		Relay: 172.168.1.10	8
Windows server (port2)	Physical Interface		172.16.1.1/255.255.255.0	PING HTTPS SSH			3

2.1.5.4 Policies:



Internet [OUT] (port3) → WAN internal between F,R (port4) 3								
Interne to IT staff	all	IT_Staff	always	ALL	ACCEPT	Disabled	AV ALL_AV WEB IT-Web filter APP Staff and IT Application Sensor IPS Users IPS SSL deep-inspection	All
Internet to Users	all	Other_Staff	always	ALL	ACCEPT	Disabled	AV ALL_AV WEB monitor-all APP Staff and IT Application Sensor IPS Users IPS SSL certificate-inspection	UTM
Internet to LAB	all	LAB	always	ALL	ACCEPT	Disabled	AV ALL_AV WEB monitor-all APP Lab Application control sensor IPS all_default SSL deep-inspection	UTM
LAN extra (port5) → Windows server (port2) 1								
IT_Staff_Accsess_to_Server	IT_Staff	Windows_Server	always	ALL	ACCEPT	Disabled	SSL no-inspection	All



WAN internal between F,R (port4) → Internet [OUT] (port3) 3								
IT Access to the internet	IT_Staff	all	always	ALL	ACCEPT	Disabled	AV ALL_AV WEB IT-Web filter APP Staff and IT Application Sensor IPS Users IPS SSL deep-inspection	All
Users Access to the internet	Other_Staff	all	always	ALL	ACCEPT	Disabled	AV ALL_AV WEB monitor-all APP Staff and IT Application Sensor IPS Users IPS SSL certificate-inspection	All
Student access to the internet	LAB	all	always	ALL	ACCEPT	Disabled	AV ALL_AV WEB monitor-all APP Lab Application control sensor IPS all_default SSL deep-inspection	All
Windows server (port2) → Internet [OUT] (port3) 1								
form server to the internet	Windows_...	all	always	ALL	ACCEPT	Enabled	AV Windows server IPS Windows_server SSL certificate-inspection	UTM

2.2 LDAP Integration and User Management:

2.2.1 Overview:

In this phase, the FortiGate firewall was integrated with an external **Windows Server 2016 Active Directory Domain** to centralize and unify all user authentication.
This integration allowed the firewall to authenticate and authorize users using their **AD usernames and passwords**, eliminating the need for managing separate local accounts on the FortiGate.

The LDAP server was added to FortiGate using the following parameters:

- **Server Type:** Regular LDAP
- **Authentication Method:** Simple Bind
- **Server IP:** *Windows Server IP (172.16.1.10)*
- **Common Name Identifier:** sAMAccountName
- **Distinguished Name Base:** DC=fortidomain,DC=local
- **Bind DN:** Administrator account

2.2.2 Active Directory Structure:

Inside Active Directory, users were organized into **organizational groups** representing different departments:

AD Group	**Description**
LAB	Students + Instructor
IT	IT Engineers
STAFF	Employees + Manager
SOC	SOC Engineer
RED	RED Team Engineer

These groups were imported into FortiGate and mapped into corresponding firewall groups to support **policy-based access control**, web filters, IPS, and application control mappings

2.2.3 FortiGate User Group Mapping:

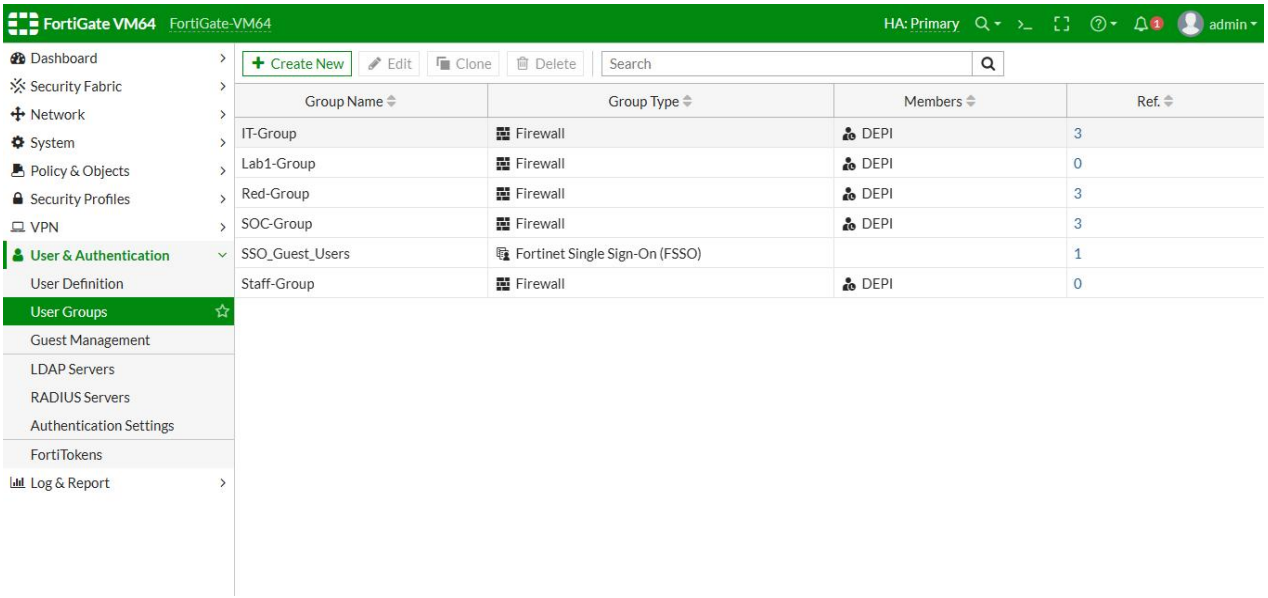
Each AD group was mapped to a **Firewall User Group** so it can be referenced in:

- Security Policies
- VPN Policies
- Web Filter Profiles
- Application Control
- IPS Rules

Examples:

- LAB → LAB_Users
- STAFF → Staff_Users
- IT → IT_Users
- SOC → SOC_Users
- RED → RedTeam_Users

This ensures each department receives the correct network permissions and security profiles.



2.2.4 FortiGate Administrative Access Using LDAP:

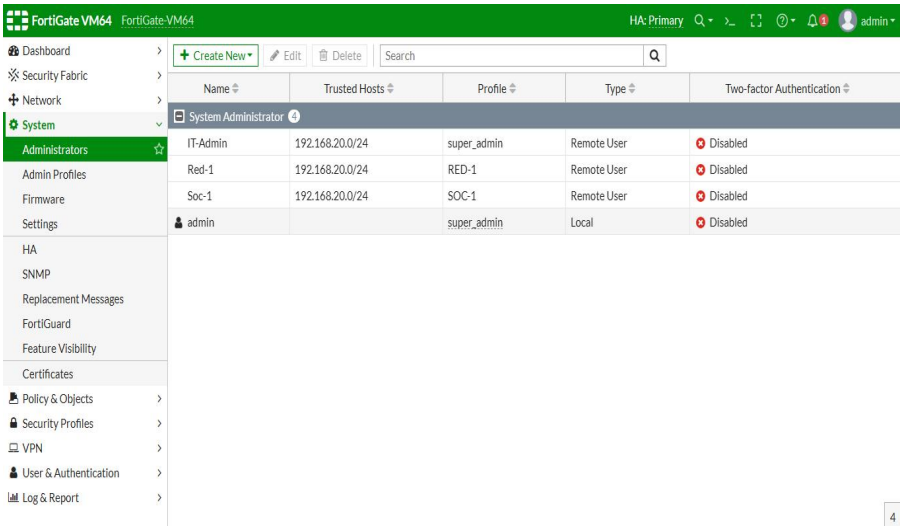
Specific AD users were granted administrative access on the FortiGate.
Each admin user was linked to a dedicated **Admin Profile** providing role-based permissions.

Admin Roles Implemented:

- **super_admin** – Full access
- **RED-1** – Red Team administrative scope
- **SOC-1** – SOC monitoring + incident roles
- **Helpdesk/Admin** – Limited operational control

This structure ensures:

- Controlled access
- Role-based permissions
- Auditability and tracking
- Preventing privilege misuse



2.2.5 Final Results

- LDAP authentication working successfully
- AD groups synchronized correctly
- Users authenticated based on AD credentials
- Security policies matching according to AD group
- Administrator roles functioning properly
- Clear separation of privileges between SOC, RED, IT, and STAFF

2.3 DHCP Configuration:

DHCP services were deployed on the routers at both the Headquarters (R1) and Branch-2 (R2) sites to automate IP address assignment and maintain consistent segmentation across all VLANs. Each router provides dedicated DHCP scopes for its local VLANs, ensuring dynamic and conflict-free address distribution.

2.3.1 HQ Router (R1):

Separate DHCP pools were configured for each VLAN as follows:

- **VLAN 10 – LAB-1**
  Range: **192.168.10.20 – 192.168.10.80**
- **VLAN 20 – IT**
  Range: **192.168.20.20 – 192.168.20.80**
- **VLAN 30 – STAFF**
  Range: **192.168.30.20 – 192.168.30.80**
- **VLAN 70 – ParkingLot**
  Range: **192.168.70.20 – 192.168.70.80**

2.3.2 Branch-2 Router (R2):

Equivalent DHCP pools were configured using Branch-2's internal subnet ranges:

- **VLAN 10 – LAB-1**
  Range: **10.10.10.20 – 10.10.10.80**
- **VLAN 20 – IT**
  Range: **10.10.20.20 – 10.10.20.80**
- **VLAN 30 – STAFF**
  Range: **10.10.30.20 – 10.10.30.80**
- **VLAN 70 – ParkingLot**
  Range: **10.10.70.20 – 10.10.70.80**

2.4 Fortinet Security Fabric:

The **Fortinet Security Fabric** was deployed to provide **centralized visibility, monitoring, and coordination** across the security infrastructure.

As part of this implementation, **Windows Server 2016 Active Directory** was integrated into the Security Fabric. This integration enables the FortiGate firewalls to:

- Identify users and devices across the network
- Correlate activity and events
- Apply **identity-based security policies** with improved accuracy

2.4.1 Active Directory as Fabric Connector:

Including Active Directory as a **Fabric connector** allows:

- Enhanced **user awareness**
- Centralized **device inventory**
- Improved **event correlation**

This setup ensures that:

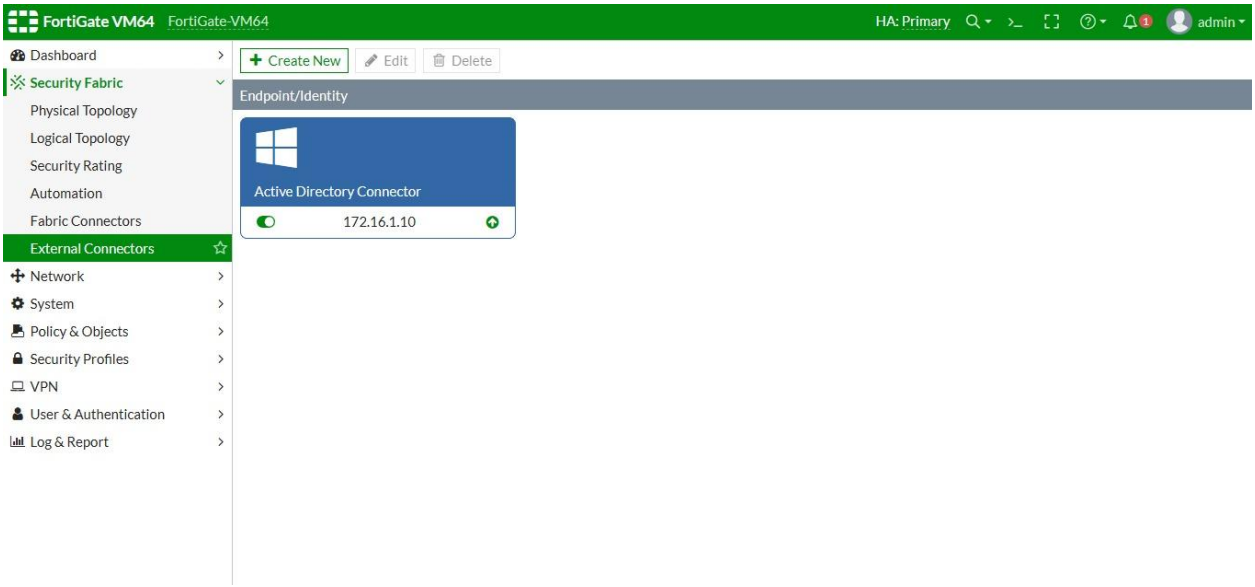
- Authenticated users are detected
- Users are mapped to organizational groups
- Appropriate access controls are enforced across the network

2.4.2 FortiAnalyzer Integration:

- A **FortiAnalyzer** appliance was planned for advanced logging, analytics, and reporting. Its intended capabilities included:
    - Centralized log storage
    - Incident correlation
    - Security reporting and alerts

- **Limitation:**
  Due to **resource constraints**, the FortiAnalyzer could not be deployed in this project environment.

- **Despite this**, the Security Fabric remains **fully functional** with AD integration, providing **centralized visibility** across all FortiGate units.



2.5 Implementation of Security Profiles:

2.5.1 Advanced FortiGate Security Profile Overview:

Objective:

The objective of this project is to implement and monitor FortiGate security profiles Web Filter, Antivirus (AV), IPS, and Application Control to protect lab and corporate networks from malware, inappropriate content, and risky applications, while maintaining access to productivity and developer resources.

2.5.2 Security Profiles Overview:

Profile Type	Purpose	Notes
Web Filter	Controls website access based on FortiGuard categories and URL filtering	Unique one for lab Staff and IT users.
Antivirus	Scans HTTP , SMTP, POP3, IMAP ,FTP ,CIFS (for all users) / And HTTP , FTP , CIFS (for windows server).	Windows server gets its own antivirus profile because it doesn't need email protocols as it doesn't act as an email server.
IPS	Detects and blocks network-based attacks, exploits, and vulnerabilities.	IPS sensors for Windows server and one for windows end devices.
Application Control	Monitors or blocks applications based on type or category.	Controls high-risk applications (P2P, remote access) and allows productivity/development apps One for employees and one for lab students.

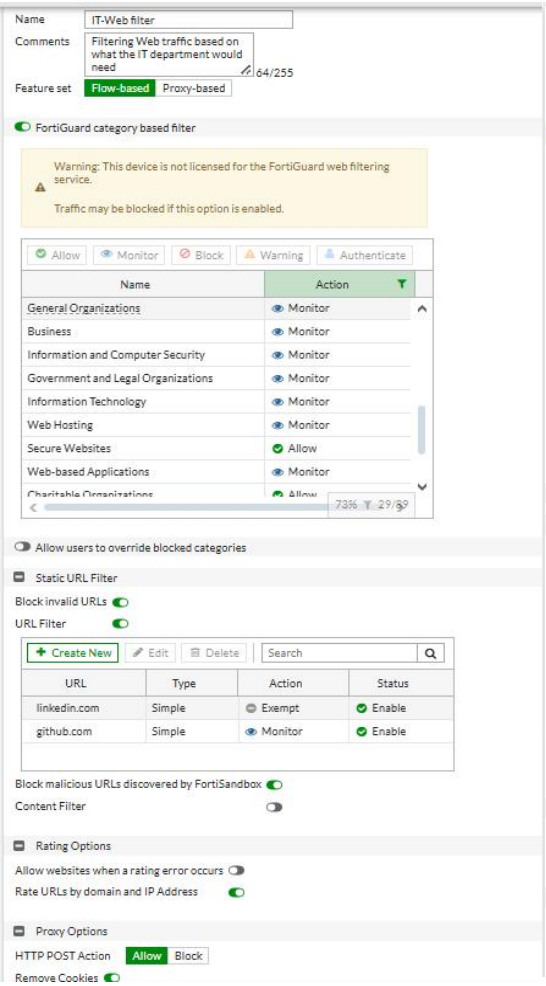
2.5.3 User Groups and Security Profile Mapping:

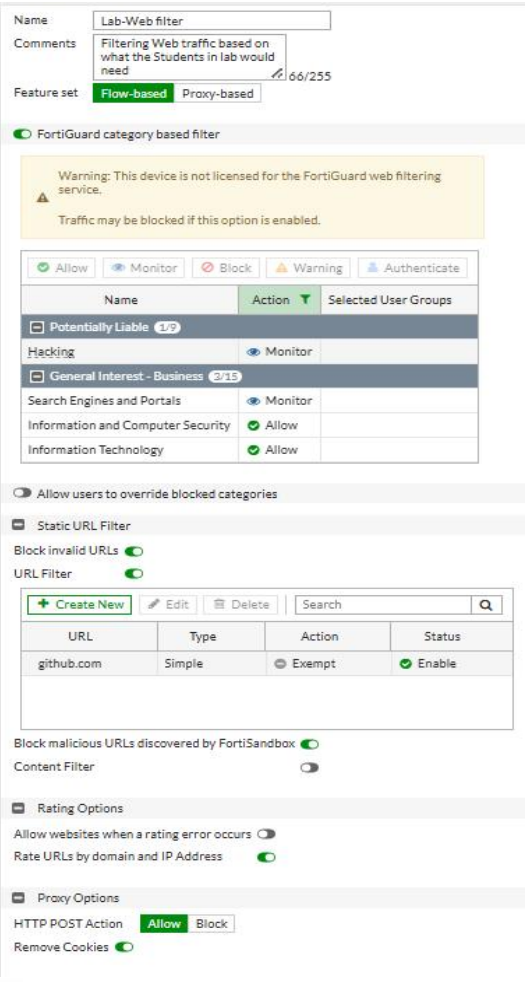
User Group	Applied Security Profiles	Notes
Lab Users	Web Filter (Lab-Web filter), AV (ALL_AV), IPS (Users IPS), Application Control (Lab Application control sensor)	Limiting access for lab students to only needed features, blocking all things unrelated to lab use.
IT Users	Web Filter (IT-Web filter), AV (ALL_AV), IPS (Users IPS), Application Control (Employee Application Sensor)	Gets broader access; GitHub, LinkedIn and development tools and other necessities monitored or allowed, downloads monitored.
Staff Users	Web Filter (Staff-Web filter), AV (ALL_AV), IPS (Users IPS), Application Control (Employee Application Sensor)	Gets broad access but less than IT user group, access limited to productivity related functions and allowing LinkedIn override.

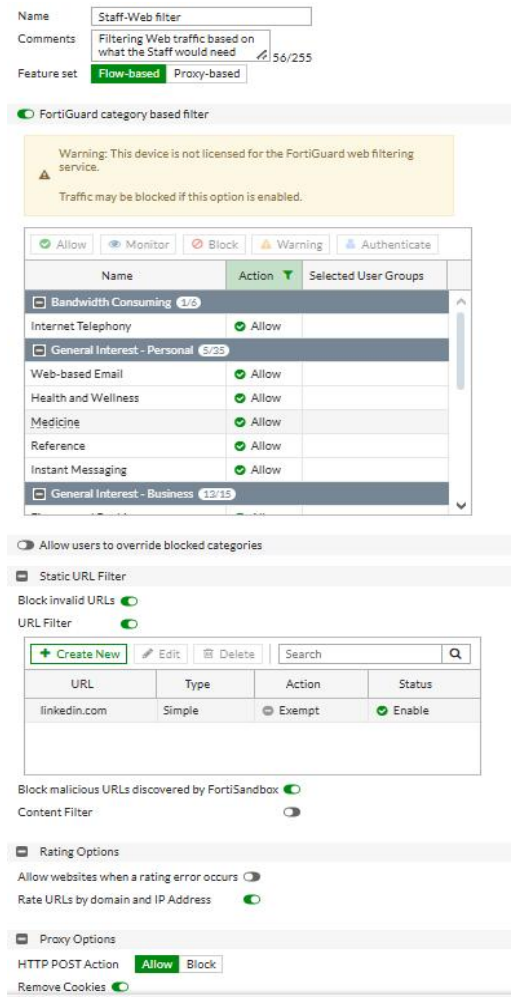
2.5.4 Web Filter Configuration:

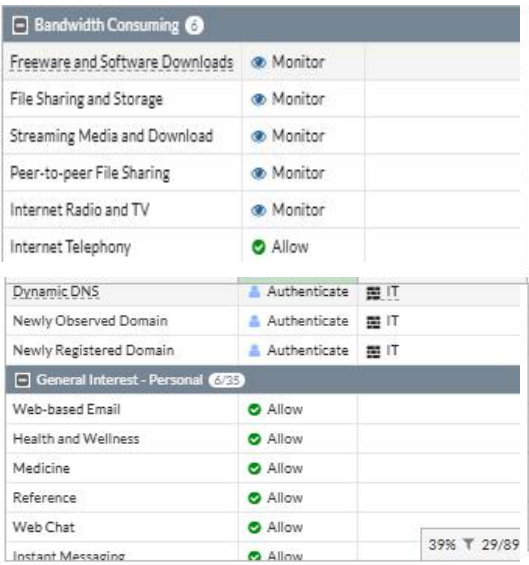
Each Web Filter profile is configured based on the needs of each user group:

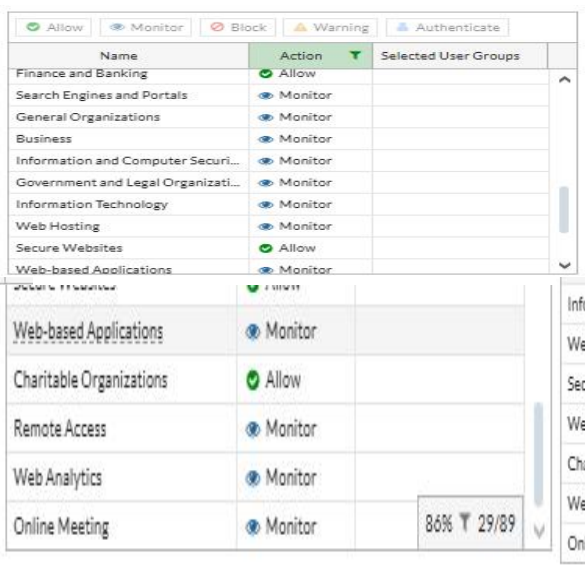
- IT users allowed developer and productivity categories.
- Staff profile restricted to work-related content only.
- Lab profile heavily restricted, allowing only learning-related sites.
- Category overrides configured per group where necessary.

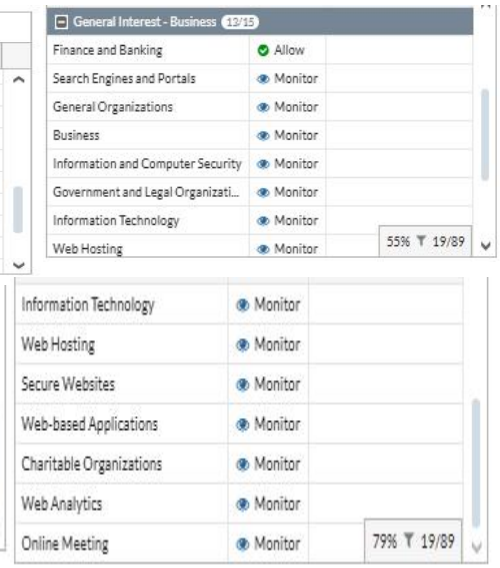

Name
IT-Web filter
Comments
Filtering Web traffic based on what the IT department would need
64/255
Feature set
Flow-based
Proxy-based
FortiGuard category based filter
Warning: This device is not licensed for the FortiGuard web filtering service.
Traffic may be blocked if this option is enabled.
Allow
Monitor
Block
Warning
Authenticate
Name
Action
General Organizations
Monitor
Business
Monitor
Information and Computer Security
Monitor
Government and Legal Organizations
Monitor
Information Technology
Monitor
Web Hosting
Monitor
Secure Websites
Allow
Web-based Applications
Monitor
Allow users to override blocked categories
Static URL Filter
Block invalid URLs
URL Filter
Create New
Edit
Delete
Search
URL
Type
Action
Status
linkedin.com
Simple
Exempt
Enable
github.com
Simple
Monitor
Enable
Block malicious URLs discovered by FortiSandbox
Content Filter
Rating Options
Allow websites when a rating error occurs
Rate URLs by domain and IP Address
Proxy Options
HTTP POST Action
Allow
Block
Remove Cookies


Name
Lab-Web filter
Comments
Filtering Web traffic based on what the Students in lab would need
66/255
Feature set
Flow-based
Proxy-based
FortiGuard category based filter
Warning: This device is not licensed for the FortiGuard web filtering service.
Traffic may be blocked if this option is enabled.
Allow
Monitor
Block
Warning
Authenticate
Name
Action
Selected User Groups
Potentially Liable 1/9
Hacking
Monitor
General Interest - Business 3/15
Search Engines and Portals
Monitor
Information and Computer Security
Allow
Information Technology
Allow
Allow users to override blocked categories
Static URL Filter
Block invalid URLs
URL Filter
Create New
Edit
Delete
Search
URL
Type
Action
Status
github.com
Simple
Exempt
Enable
Block malicious URLs discovered by FortiSandbox
Content Filter
Rating Options
Allow websites when a rating error occurs
Rate URLs by domain and IP Address
Proxy Options
HTTP POST Action
Allow
Block
Remove Cookies


Name
Staff-Web filter
Comments
Filtering Web traffic based on what the Staff would need
56/255
Feature set
Flow-based
Proxy-based
FortiGuard category based filter
Warning: This device is not licensed for the FortiGuard web filtering service.
Traffic may be blocked if this option is enabled.
Allow
Monitor
Block
Warning
Authenticate
Name
Action
Selected User Groups
Bandwidth Consuming 1/6
Internet Telephony
Allow
General Interest - Personal 5/25
Web-based Email
Allow
Health and Wellness
Allow
Medicine
Allow
Reference
Allow
Instant Messaging
Allow
General Interest - Business 12/15
Allow users to override blocked categories
Static URL Filter
Block invalid URLs
URL Filter
Create New
Edit
Delete
Search
URL
Type
Action
Status
linkedin.com
Simple
Exempt
Enable
Block malicious URLs discovered by FortiSandbox
Content Filter
Rating Options
Allow websites when a rating error occurs
Rate URLs by domain and IP Address
Proxy Options
HTTP POST Action
Allow
Block
Remove Cookies


Bandwidth Consuming 6
Freeware and Software Downloads
Monitor
File Sharing and Storage
Monitor
Streaming Media and Download
Monitor
Peer-to-peer File Sharing
Monitor
Internet Radio and TV
Monitor
Internet Telephony
Allow
Dynamic DNS
Authenticate
IT
Newly Observed Domain
Authenticate
IT
Newly Registered Domain
Authenticate
IT
General Interest - Personal 6/25
Web-based Email
Allow
Health and Wellness
Allow
Medicine
Allow
Reference
Allow
Web Chat
Allow
Instant Messaging
Allow
39% 29/89

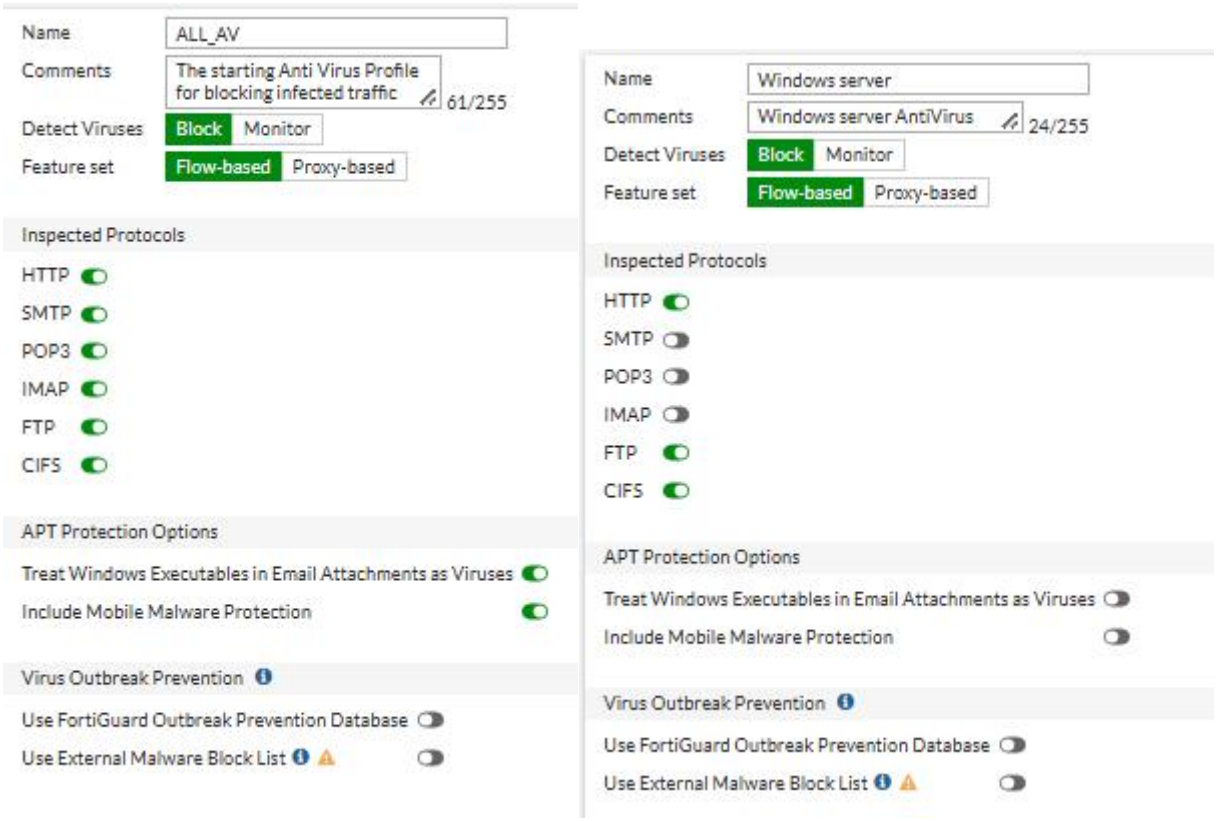

Allow
Monitor
Block
Warning
Authenticate
Name
Action
Selected User Groups
Finance and Banking
Allow
Search Engines and Portals
Monitor
General Organizations
Monitor
Business
Monitor
Information and Computer Securi...
Monitor
Government and Legal Organizati...
Monitor
Information Technology
Monitor
Web Hosting
Monitor
Secure Websites
Allow
Web-based Applications
Monitor
Charitable Organizations
Allow
Remote Access
Monitor
Web Analytics
Monitor
Online Meeting
Monitor
86% 29/89


General Interest - Business 12/15
Finance and Banking
Allow
Search Engines and Portals
Monitor
General Organizations
Monitor
Business
Monitor
Information and Computer Security
Monitor
Government and Legal Organizati...
Monitor
Information Technology
Monitor
Web Hosting
Monitor
55% 19/89
Information Technology
Monitor
Web Hosting
Monitor
Secure Websites
Monitor
Web-based Applications
Monitor
Charitable Organizations
Monitor
Web Analytics
Monitor
Online Meeting
Monitor
79% 19/89

2.5.5 Antivirus (AV) Configuration:

VOS could not be enabled due to licensing requirements.

- CDR (Content Disarm & Reconstruction) was not used because enabling it under proxy-based scanning conflicted with SMTP “splice” mode.
- Windows Server AV profile has all mail protocol inspection disabled since the server is not acting as an email server.
- AV profiles for client devices perform full protocol inspection.

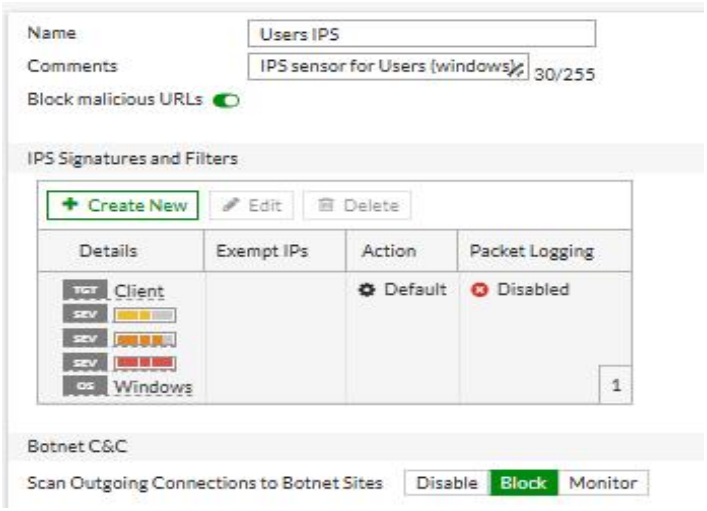


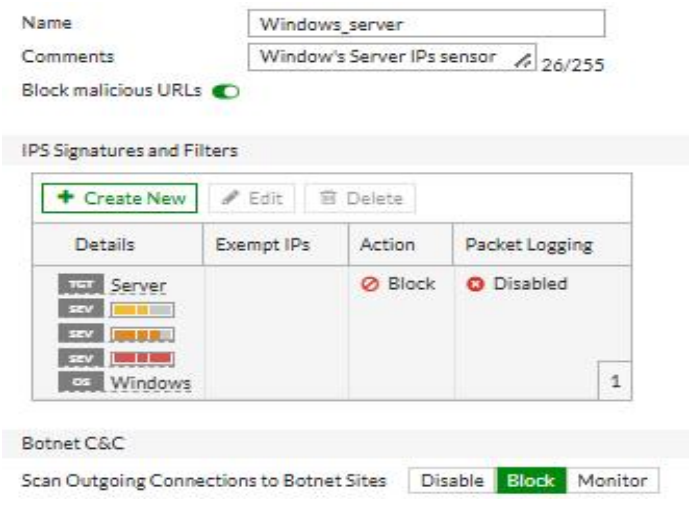
2.5.6 IPS Configuration:

Two IPS sensors were implemented:

- **Users IPS Sensor:** covers client-side vulnerabilities and workstation exploits.
- **Windows Server IPS Sensor:** tailored for server-side vulnerabilities.

These IPS profiles were then applied inside the firewall policies for the corresponding VLANs.

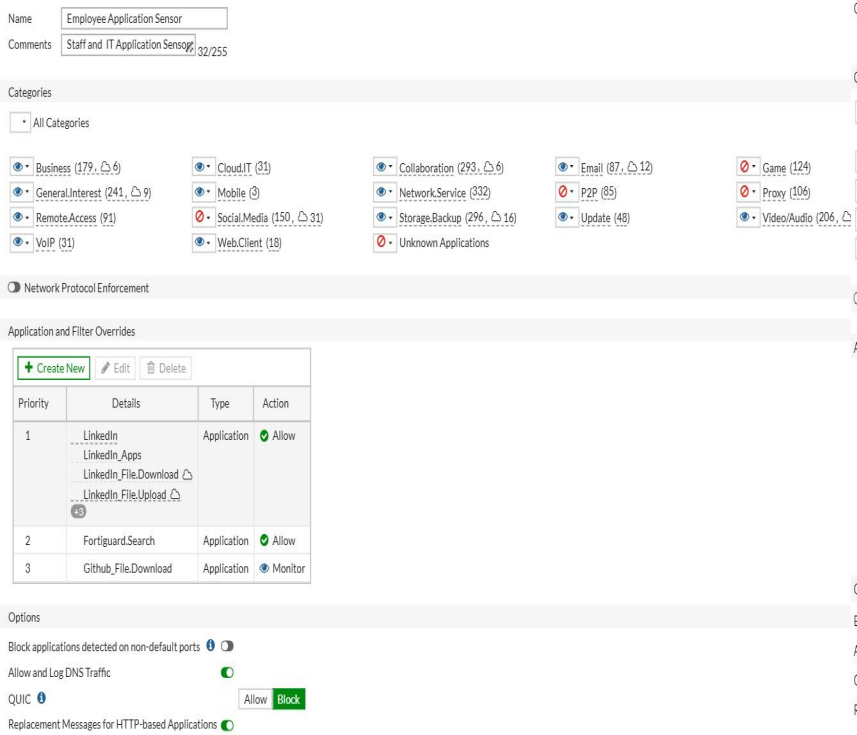


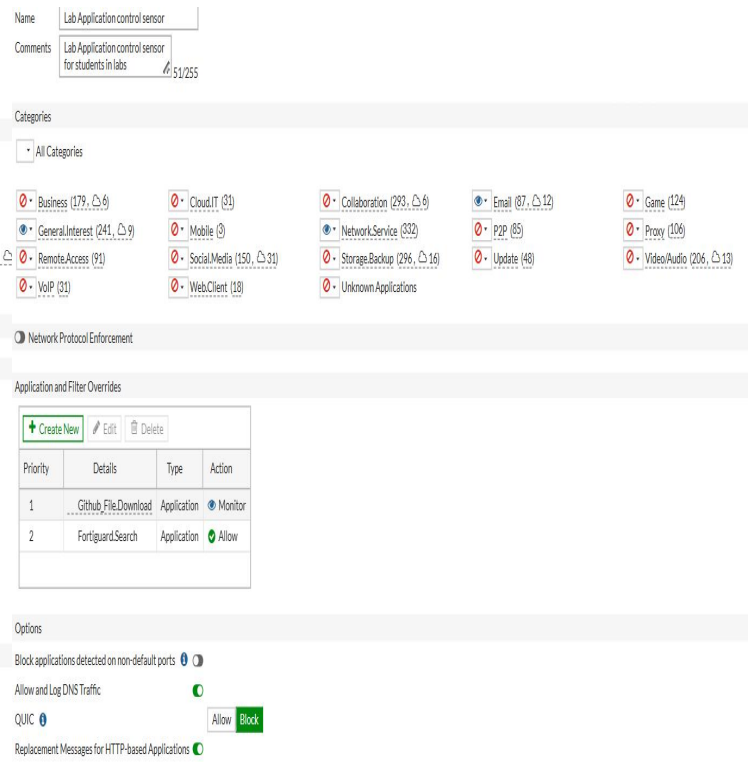


2.5.7 Application Control Configurations:

Application Control rules were designed depending on the user group:

- **IT & Staff** → monitored productivity apps, blocked risky categories (P2P, remote access, torrents).
- **Lab students** → heavily restricted; exceptions were added for:
  - GitHub downloads
  - FortiGuard_Search
  - Development tools required for lab work





2.6 FortiGate IPsec VPN Implementation:

(Site-to-Site + Remote-Access Dial-Up VPN)

2.6.1 Overview:

This stage of the project involved deploying **two types of VPNs** across two FortiGate firewalls running in VMware:

1. **Site-to-Site IPsec VPN** (FG1 ↔ FG2)
2. **Remote-Access IPsec Dial-Up VPN** for Windows laptops and Android devices

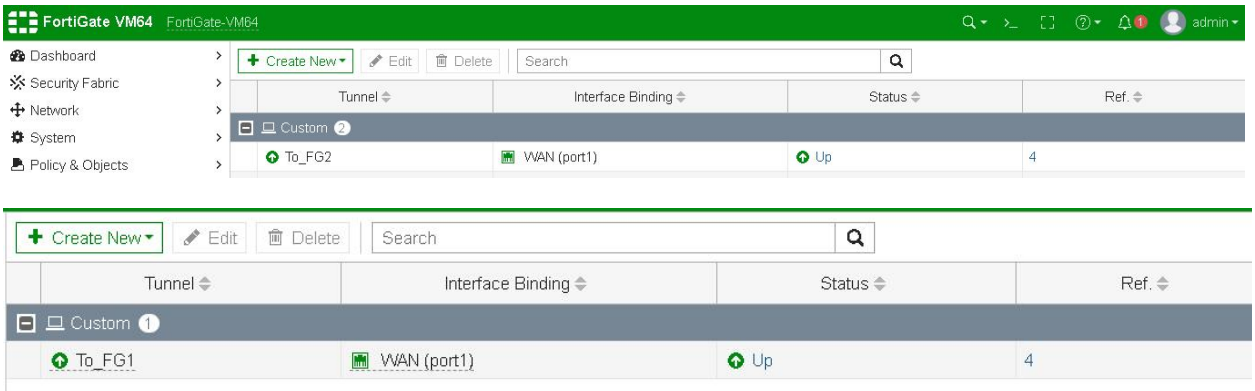
Multiple configuration issues occurred due to legacy encryption limitations, aggressive-mode client behavior, and mismatch of Phase 2 proposals.

2.6.2 Site-to-Site IPsec VPN Configuration:

Both FortiGate appliances were placed on separate virtual LANs inside VMware and were connected using a routed IPsec tunnel.

2.6.2.1 FG1 Configuration (FG1 → FG2):

- NAT-T enabled
- IKEv2 chosen for stability and faster SA negotiation
- Improved mobility handling and better rekey performance



2.6.2.2 FG2 Configuration (FG2 → FG1):

Configuration was mirrored on FG2:

- Same IKE version
- Same DES/SHA512
- Same pre-shared key
- Same NAT-Traversal settings

#Because only **DES** was available, it was used for both Phase 1 and Phase 2.

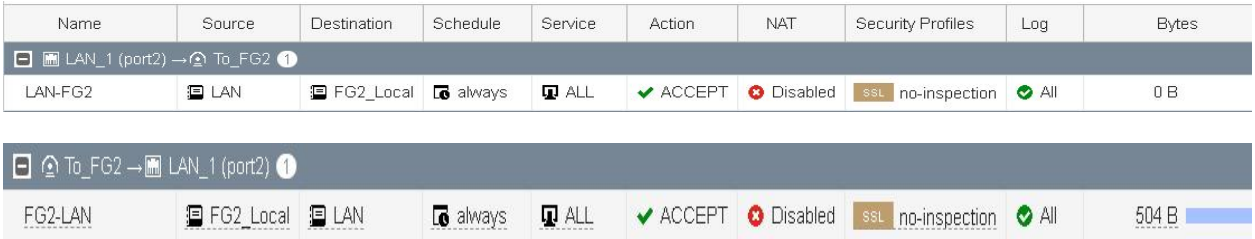
2.6.2.3 Firewall Policies (FG1 & FG2):

FG1:

- Allow FG1 LAN → FG2 LAN
- Allow FG2 LAN → FG1 LAN
- NAT disabled (VPN must route, not NAT)

FG2:

- Same mirrored structure



2.6.2.4 Static Routes:

Each firewall contained a static route pointing to the other LAN through the IPsec tunnel:

- FG1 → FG2 LAN via tunnel
- FG2 → FG1 LAN via tunnel

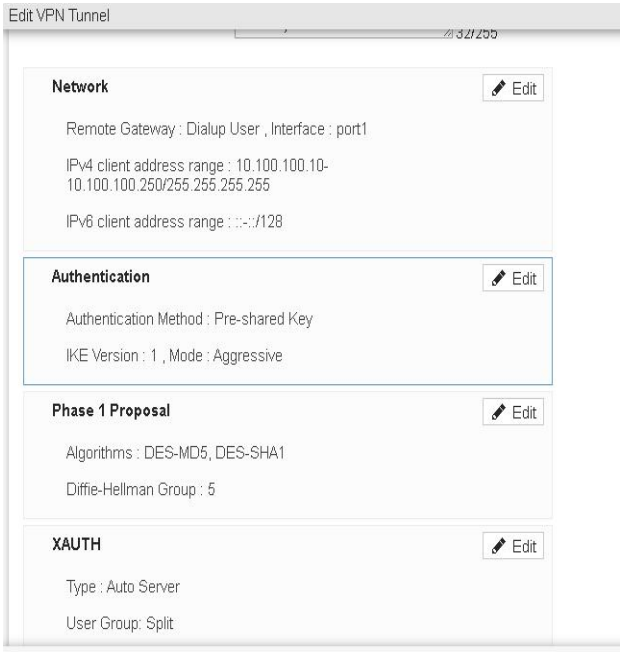
A **lower route distance** ensured tunnel routing takes priority over default internet routes.

Destination	Gateway IP	Interface	Status	Comments	Distance	Priority
IPv4 2						
0.0.0.0/0	192.168.1.1	WAN (port1)	Enabled		10	0
FG2_Local	0.0.0.0	To_FG2	Enabled		9	0

2.6.3 Remote-Access Dial-Up IPsec VPN (FG1):

This VPN enables external laptops and mobile devices to reach FG1's LAN securely.

2.6.3.1 VPN Configuration:



Aggressive Mode selected because:

- Faster negotiation (3-message exchange)
- Works better when client IP is unstable
- Required for certain legacy Android/Windows clients

Authentication:

- XAUTH enabled
- Mode: auto-server
- Group: split
- User: *boudy*
- Peer ID: any

2.6.3.2 Phase 1 & Phase 2 Proposals:

A major limitation was discovered:

Clients only supported outdated ciphers.

Mutually compatible ciphers were:

- **DES + MD5**
- **DES + SHA-1**

Both were selected to ensure cross-device compatibility.

2.6.3.3 Remote-Access Firewall Policy

A policy was added on FG1 to allow authenticated VPN clients to access internal resources.

2.7 High Availability (HA) Configuration:

A **High Availability (HA) cluster** was deployed on the FortiGate firewalls to guarantee **continuous network operation** and **minimize downtime** in case of device failure.

Two **FortiGate VM64 units** were configured in an **Active-Passive HA cluster** using **FGCP (FortiGate Clustering Protocol)**. The HA setup allows:

- Configuration synchronization
- Session information sharing
- Routing table replication

2.7.1 HA Priorities

- **Primary Unit:** Priority **250** → Preferred master
- **Secondary Unit:** Priority **128** → Backup for failover

Both devices reported a **synchronized status**, confirming:

- Proper alignment of configuration data
- Runtime session and routing synchronization
- Seamless failover capability

2.7.2 Benefits of HA Setup

- Provides redundancy and **improves network reliability**
- Ensures **uninterrupted connectivity** during hardware or system failures
- Enables maintenance without downtime