

# Healthcare Clinic Network

Supervisor: Elhosein Ahmed



# Team Members

- Ayad Zewail
- Hazem Ahmed
- Mohamed Khaled
- Mostafa Mahmoud
- Youssef Said
- Seif Samer



# Overview

- Healthcare clinic with different groups of users
  - Admins
  - Staff (Doctors, Nurses)
  - Guests (Visitors in waiting rooms)
- Data segregation importance for information privacy
- Network stability and security to ensure no delays/failures



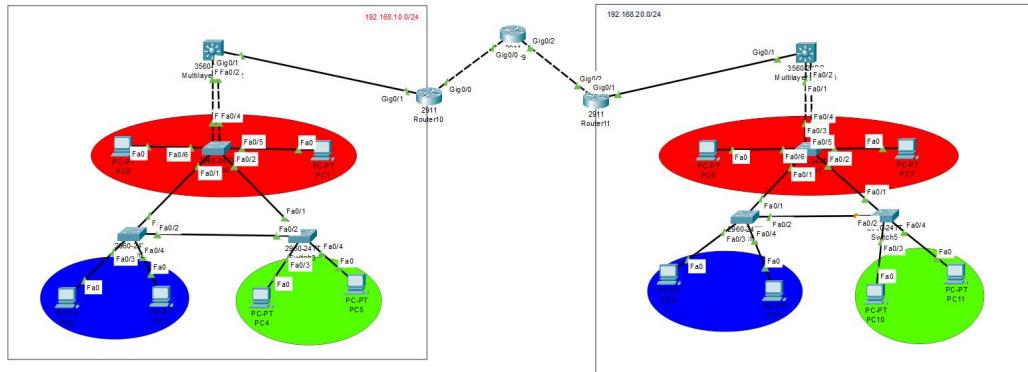
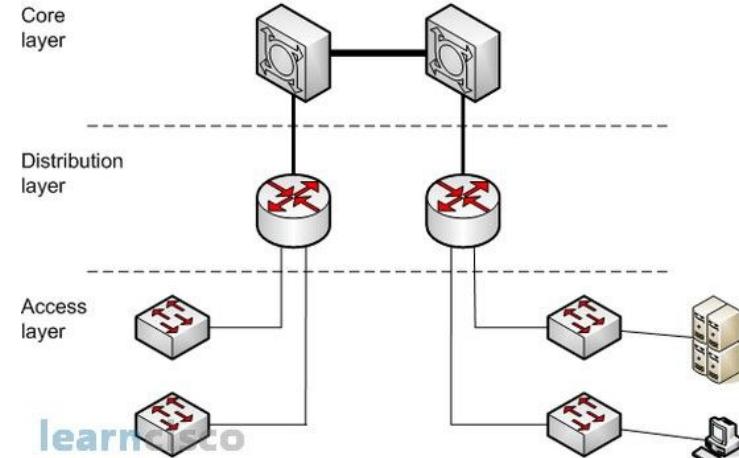
# Project Features

- CCNA:
  - Inter VLAN
  - DHCP
  - Routing
  - Port Channel
  - PVST
- FortiGate:
  - Objects
  - Firewall Policies
  - Web Filtering
  - Antivirus
  - Application Control



# Network Design

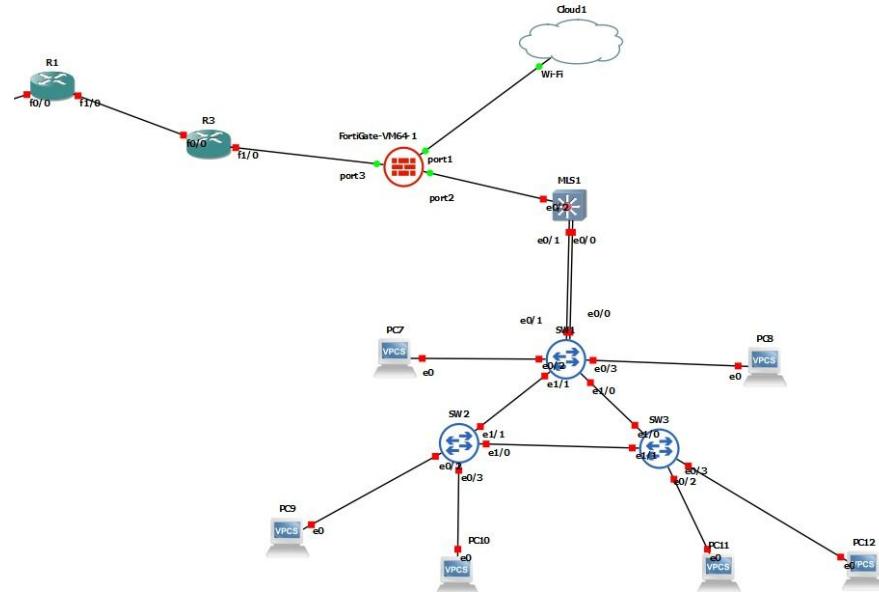
- Dual-Branch Clinic connected through a routed WAN backbone
- Each branch has a multilayer distribution switch
- Access switches serve multiple end devices
- Inter-VLAN routing at the distribution layer
- inter-site routing via the central routers





# FortiGate Integration

Interfaces	Role	IP Address
port1	WAN	192.168.107.128/24
port2	LAN	10.0.3.1/24
port3	WAN	10.0.4.1/24





# FortiGate Implementation

## Firewall Policies

- Admins -> Internet
  - (low restriction)
- Doctors -> Internet
  - (Medium filtering)
- Reception -> Internet
  - (Strict filtering)

FortiGate VM64 Project												
Dashboard		Firewall Policy										
Security Fabric		Policy Objects										
Network		Firewall Policy										
System		IPV4 DoS Policy										
Policy & Objects		IPV4 Policy										
Firewall Policy		IPV4 DoS Policy										
IPv4 DoS Policy		Addresses										
Security Fabric		Internet Service Database										
Network		Services										
System		Schedules										
Policy & Objects		Virtual IPs										
Firewall Policy		IP Pools										
IPv4 Policy		Protocol Options										
Firewall Policy		Traffic Shapers										
IPv4 Policy		Traffic Shaping Policy										
Firewall Policy		Traffic Shaping Profile										
IPv4 Policy		Security Profiles										
Firewall Policy		VPN										
IPv4 Policy		User & Authentication										
Firewall Policy		Log & Report										
		Right_to_Left										
		MLS_Conn (port2)										
		Router_conn (port3)										
		all										
		always										
		ALL										
		✓ ACCEPT										
		Disabled										
		SSL no-inspection										
		UTM										
		840 B										
		Left_To_Right										
		MLS_Conn (port2)										
		Router_conn (port3)										
		all										
		always										
		ALL										
		✓ ACCEPT										
		Enabled										
		SSL certificate-inspection										
		UTM										
		1.34 kB										
		Internet_Managers										
		MLS_Conn (port2)										
		port1										
		Managers_VLAN20										
		all										
		always										
		ALL										
		✓ ACCEPT										
		Enabled										
		SSL certificate-inspection										
		UTM										
		0 B										
		Internet_Doctors										
		MLS_Conn (port2)										
		port1										
		Doctors_VLAN21										
		all										
		always										
		ALL										
		✓ ACCEPT										
		Enabled										
		SSL certificate-inspection										
		UTM										
		0 B										
		Internet_Reception										
		MLS_Conn (port2)										
		port1										
		Reception_VLAN22										
		all										
		always										
		ALL										
		✓ ACCEPT										
		Enabled										
		SSL certificate-inspection										
		UTM										
		0 B										
		Implicit Deny										
		any										
		any										
		all										
		always										
		ALL										
		DENY										
		Disabled										

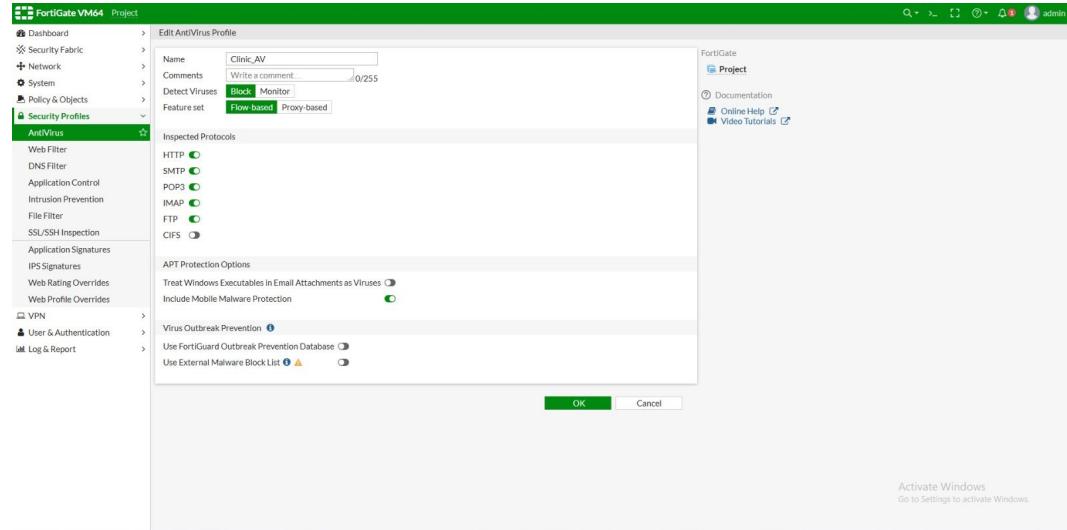
Activate Windows  
Go to Settings to activate Windows.



# FortiGate Implementation

## Security Profile: Antivirus

- Malware Detection Mode
  - Block: prevents infected files from passing through the firewall.
- Flow-Based Scanning
  - Inspects traffic in real time with minimal latency.





# FortiGate Implementation

## Security Profile: Web Filtering

- Category-based filter
  - allow or block etc. for all websites belonging to specific category to make configuration easy
- Profiles based on group
  - doctors have medium filtering (can view drug-related content for example but not hacking)
  - waiting room more strict

The screenshot shows the FortiGate VM64 Project interface with two 'Edit Web Filter Profile' windows open.

**Top Window (Doctor.WebFilter):**

- Name: Doctor.WebFilter
- Comments: Write a comment... 0/255
- Feature set: Flow-based Proxy-based
- FortGuard category based filter:**
  - Warning: This device is not licensed for the FortGuard web filtering service.  
Traffic may be blocked if this option is enabled.
  - Table:

Name	Action
custom1	Disable
custom2	Disable
Potentially Liable	
Drug Abuse	Allow
Hacking	Block
Illegal or Unethical	Allow

**Bottom Window (Reception\_WebFilter):**

- Name: Reception\_WebFilter
- Comments: Write a comment... 0/255
- Feature set: Flow-based Proxy-based
- FortGuard category based filter:**
  - Warning: This device is not licensed for the FortGuard web filtering service.  
Traffic may be blocked if this option is enabled.
  - Table:

Name	Action
custom1	Disable
custom2	Disable
Potentially Liable	
Drug Abuse	Block
Hacking	Block
Illegal or Unethical	Block
Discrimination	Block
Explicit Violence	Block

Both windows include sections for 'Allow users to override blocked categories', 'Static URL Filter', 'Block Invalid URLs', and 'URL Filter'. At the bottom right of each window are 'OK' and 'Cancel' buttons.

# FortiGate Implementation

## Security Profile: Application Control

- Regulate Network Usage
  - control who accesses what to avoid abuse of network
  - doctors can't open netflix while on shift for example

The screenshot shows the FortiGate VM64 Project interface with the 'Application Control' tab selected. The left sidebar includes options like Dashboard, Security Fabric, Network, System, Policy & Objects, Security Profiles, and Application Control. The main pane displays a table of application profiles:

Name	Comments	Ref.
Doctor_AppCtrl		1
Manager_AppCtrl		1
Reception_AppCtrl		1
block-high-risk		0
default	Monitor all applications.	0
wifi-default	Default configuration for offloading WiFi traffic.	1

Below this, there's a detailed view of the 'Doctor\_AppCtrl' profile, showing categories like Business, Email, Mobile, Cloud, Game, Network, P2P, Remote Access, Social Media, Update, Video/Audio, and Web Client. A 'Network Protocol Enforcement' section is also visible. At the bottom, a 'Create New' dialog is open for a new application profile.

# Expected Outcomes

## Antivirus



### High Security Alert

You are not permitted to download the file "windows.exe" because it is infected with the virus "FSA/RISK\_MEDIUM".

URL	<a href="https://filegen.fortinet.com/v1/sandbox-file?file_name=windows.exe&amp;s=fnt">https://filegen.fortinet.com/v1/sandbox-file?file_name=windows.exe&amp;s=fnt</a>
Quarantined File Name	b0693ac0.windows.exe
Reference URL	<a href="http://www.fortinet.com/ve/?vn=FSA%2FRISK_MEDIUM">http://www.fortinet.com/ve/?vn=FSA%2FRISK_MEDIUM</a>

## Web Filtering

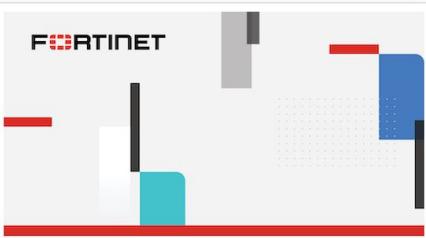


### Web Page Blocked

An error occurred while trying to rate the website using the webfiltering service.

Web Filter Service Error N/A

## Application Control



### FortiGate Application Control

#### Application Blocked

You have attempted to use an application that violates your Internet usage policy.

Application	Windows NT6.3 Web Surfing
Category	Web.Client
URL	<a href="http://nhl.com/">http://nhl.com/</a>
Policy	645f5f78-57db-51ee-9b3a-ea49bd1203ab



# Project Achievements

- Scalability
  - Inter-VLAN design supports adding departments and subnets easily.
  - Port Channels increase uplink capacity as traffic grows.
  - FortiGate objects simplify scaling security policies.
- Centralized Manageability
  - DHCP automates IP assignment across all VLANs.
  - PVST improves L2 control and speeds up troubleshooting.
  - FortiGate policies centralize all firewall and security management.
- High Availability & Redundancy
  - PVST maintains loop-free L2 operation with optimized paths.
  - Port Channels keep traffic running even if a link fails.



# Project Achievements

- Security Enhancement
  - Firewall policies segment traffic and enforce access control.
  - Web Filtering, Antivirus, and App Control protect against malicious sites, malware, risky apps, and exploits.
  - Inter-VLAN segmentation reduces lateral movement.



# Project Beneficiaries

- Network Administrators / IT Team
  - Easier management, faster troubleshooting, better visibility, and reduced manual workload.
- Security Operations Personnel
  - Stronger threat prevention, clearer logs, and more centralized policy control.
- End Users (Employees/Students/Staff)
  - Faster network performance, safer browsing, and fewer outages or disruptions.
- Organization / Management
  - Improved security posture, reduced risk, better compliance, and long-term scalability.
- Business Services / Applications
  - Benefit from stable routing, reliable connectivity, and less downtime caused by network issues.



# What We Learned

- Network design
- Routing & switching
- Firewall & security policy management
- Troubleshooting & monitoring
- Real world infrastructure skills
- Documentation & presentation