

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

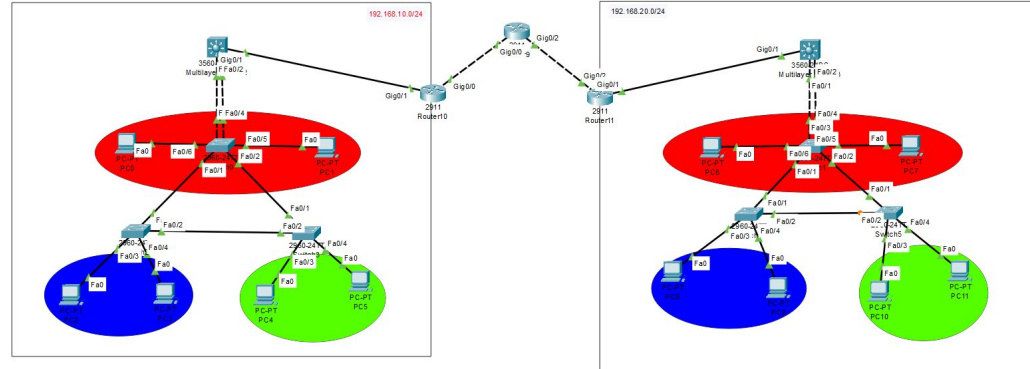
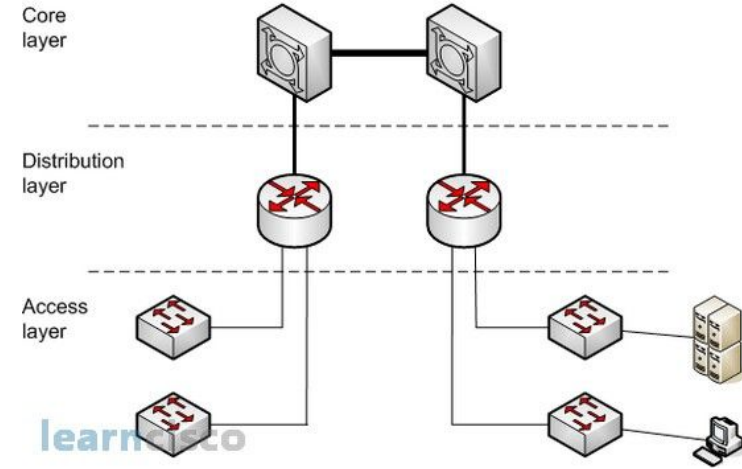


Project Features

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

Network Design

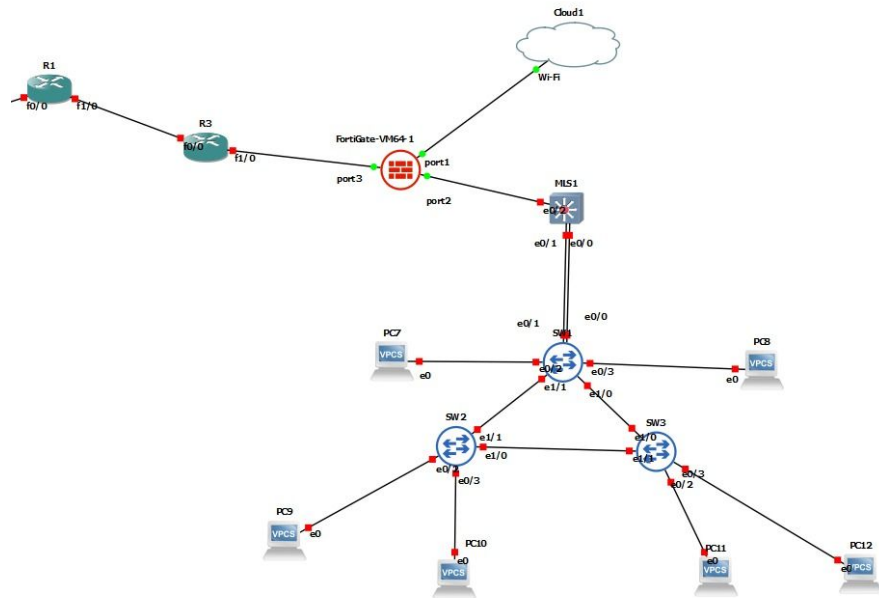
- Dual-Branch Clinic connected through a routed WAN backbone
- Each branch has a multilayer distribution switch
- Access switches serve multiple end devices
- Inter-VLAN routing at the distribution layer
- inter-site routing via the central routers





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

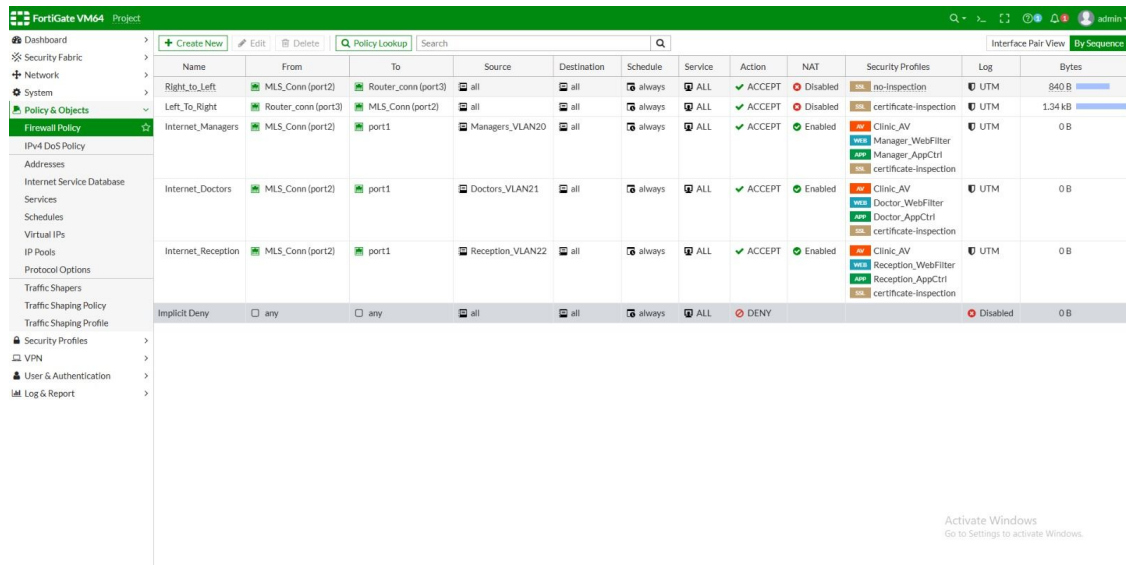




FortiGate Implementation

Firewall Policies

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



The screenshot shows the FortiGate VM64 Firewall Policy configuration page. The left sidebar contains navigation options: Dashboard, Security Fabric, Network, System, Policy & Objects (selected), Firewall Policy, IPv4 DoS Policy, Addresses, Internet Service Database, Services, Schedules, Virtual IPs, IP Pools, Protocol Options, Traffic Shapers, Traffic Shaping Policy, Traffic Shaping Profile, Security Profiles, VPN, User & Authentication, and Log & Report. The main table displays the following policies:

Name	From	To	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log	Bytes
Right_to_Left	MLS_Conn (port2)	Router_conn (port3)	all	all	always	ALL	ACCEPT	Disabled	no-inspection	UTM	\$40 B
Left_To_Right	Router_conn (port3)	MLS_Conn (port2)	all	all	always	ALL	ACCEPT	Disabled	certificate-inspection	UTM	1.34 kB
Internet_Managers	MLS_Conn (port2)	port1	Managers_VLAN20	all	always	ALL	ACCEPT	Enabled	Clinic_AV, Manager_AppCtrl, certificate-inspection	UTM	0 B
Internet_Doctors	MLS_Conn (port2)	port1	Doctors_VLAN21	all	always	ALL	ACCEPT	Enabled	Clinic_AV, Doctor_WebFilter, Doctor_AppCtrl, certificate-inspection	UTM	0 B
Internet_Reception	MLS_Conn (port2)	port1	Reception_VLAN22	all	always	ALL	ACCEPT	Enabled	Clinic_AV, Reception_WebFilter, Reception_AppCtrl, certificate-inspection	UTM	0 B
Implicit Deny	any	any	all	all	always	ALL	DENY			Disabled	0 B

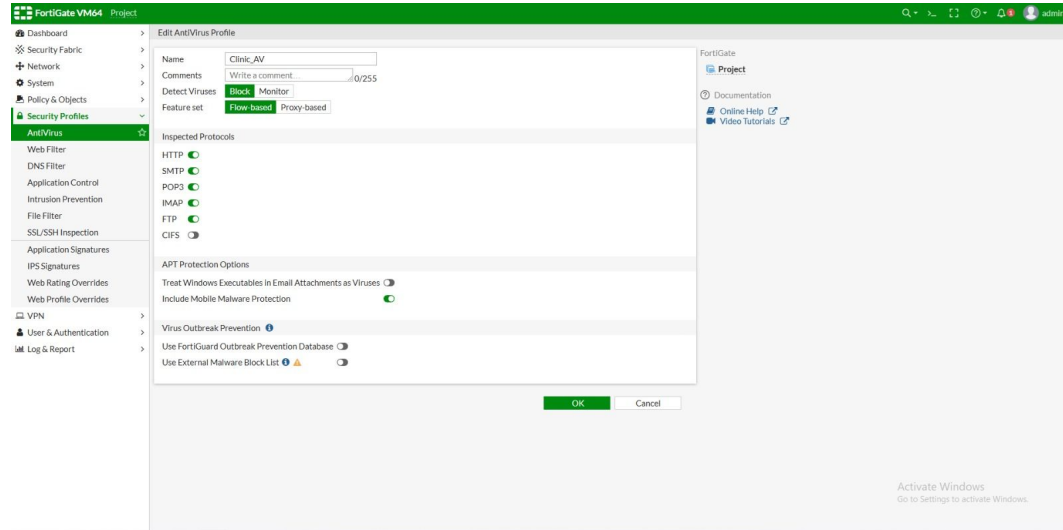
At the bottom right, there is a message: "Activate Windows Go to Settings to activate Windows."



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.

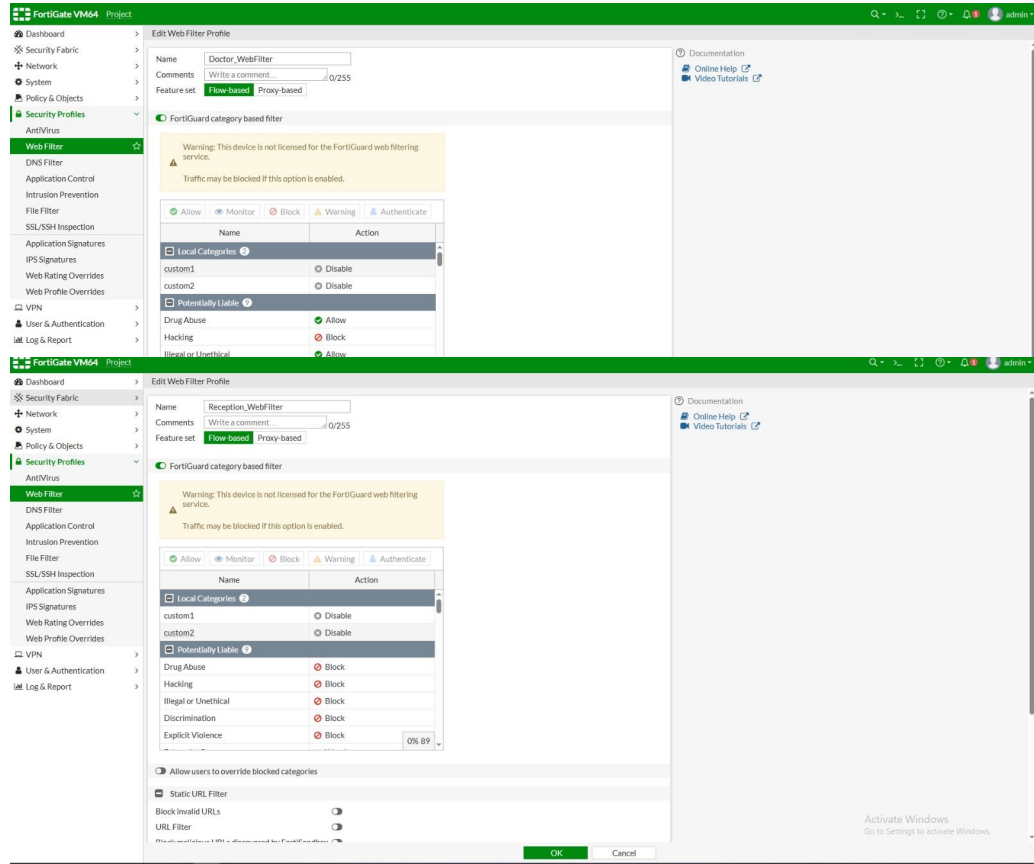




FortiGate Implementation

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





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 displays the FortiGate VM64 web interface. The left sidebar shows the navigation menu with 'Security Profiles' expanded and 'Application Control' selected. The main content area is divided into two sections: 'Edit Application Sensor' and 'Application and Filter Overrides'.

Edit Application Sensor:

- Name: Doctor_AppCtrl
- Comments: 0/255
- Categories: All Categories
 - Business (179, 6)
 - Email (87, 12)
 - Mobile (3)
 - Proxy (106)
 - Storage.Backup (276, 16)
 - VoIP (31)
 - Cloud.IT (31)
 - Game (124)
 - Network.Service (332)
 - Remote.Access (91)
 - Update (48)
 - Web.Client (18)
 - Collaboration (293, 6)
 - GeneralInterest (241, 9)
 - P2P (85)
 - Social.Media (150, 31)
 - Video.Audio (206, 13)
 - Unknown Applications

Application and Filter Overrides:

Priority	Details	Type	Action
1	ASProxy AutoHideP Browsesec Bypass (2510)	Application	Block
2	YouTube_SearchSafetyModeOff YouTube_VideoUpload YouTube YouTube_ChannelAccess (17)	Application	Block
3	Netflix Netflix_Login Netflix_Forum	Application	Block

The right sidebar shows the 'Firmware & General Updates License' section, indicating 'Not Supported' and 'Application Control Signatures Package Version 6.00741'.



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	https://filegen.fortinet.com/v1/sandbox-file?file_name=windows.exe&s=ftnt
Quarantined File Name	b0693ac0.windows.exe
Reference URL	http://www.fortinet.com/ve?vn=FSA%2FRISK_MEDIUM

Web Filtering

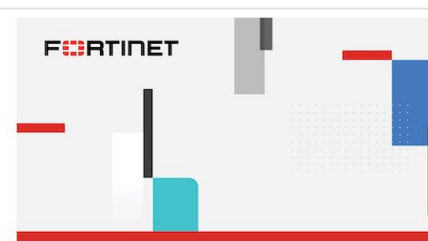


Web Page Blocked

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.NT.6.3.Web.Surfing
Category	Web.Client
URL	http://nhl.com/
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