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

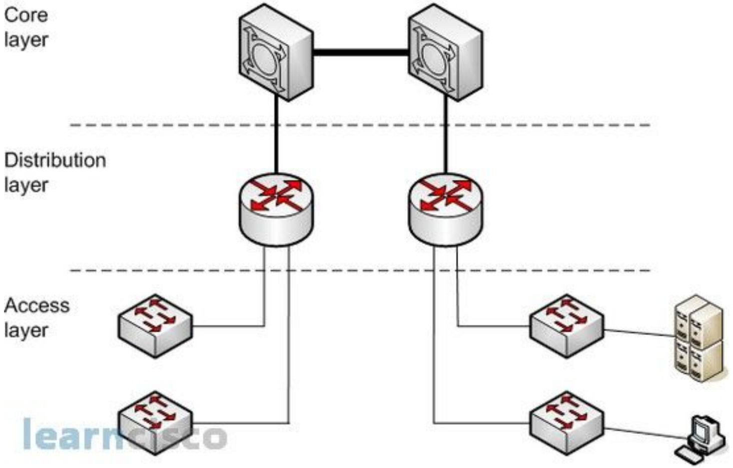
Project Features

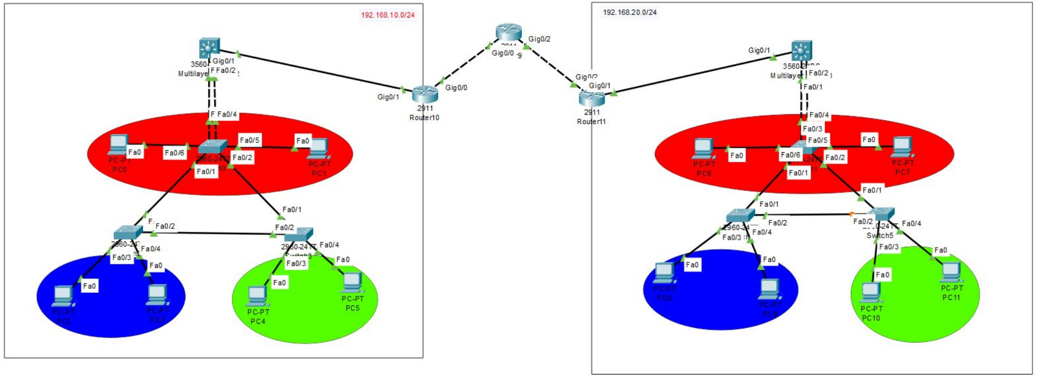
- CCNA:
    - Inter VLAN
    - DHCP
    - Routing
    - Port Channel
    - PVST

- FortiGate:
    - Objects
    - Firewall Policies
    - Web Filtering
    - Antivirus
    - Application Control
    - IPS
    - DNS Filter

Network Design

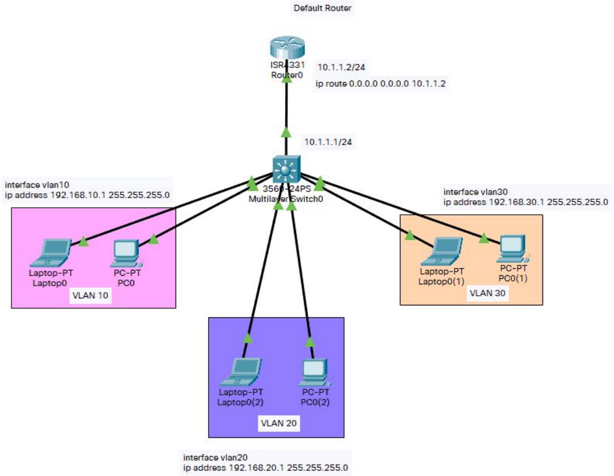
- Dual-Branch Clinic connected through a routed WAN backbone
- Each branch has a multilayer distribution switch
- Access switches serve multiple end devices
- Inter-VLAN routing at the distribution layer
- inter-site routing via the central routers





Inter VLAN

- Allows devices in different VLANs to communicate by routing traffic between segmented networks.
- Implemented using either a Layer 3 switch (SVIs) or a router-on-a-stick configuration.
- Enhances security and network organization by keeping VLANs isolated while still enabling controlled communication.



```
ip route 0.0.0.0 0.0.0.0 10.1.1.2
```

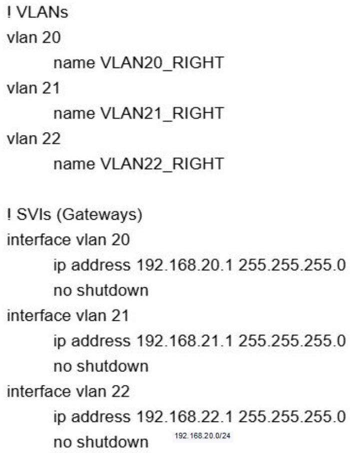
```
interface vlan10
ip address 192.168.10.1 255.255.255.0
```

```
interface vlan30
ip address 192.168.30.1 255.255.255.0
```

```
interface vlan20
ip address 192.168.20.1 255.255.255.0
```

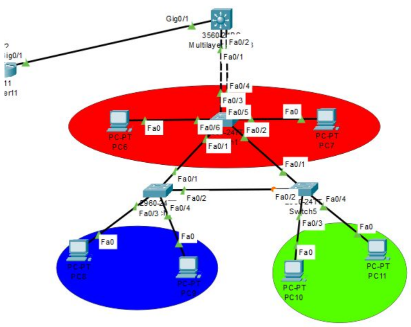
Inter VLAN Implementation

- 3 VLANs: 20 (Admins) - 21 (Staff) - 22 (Guests)
- Multilayer Switch (MLS) serves as the central router-on-a-stick, with SVIs defining default gateways
- All SVIs are configured "no shutdown" for immediate activation



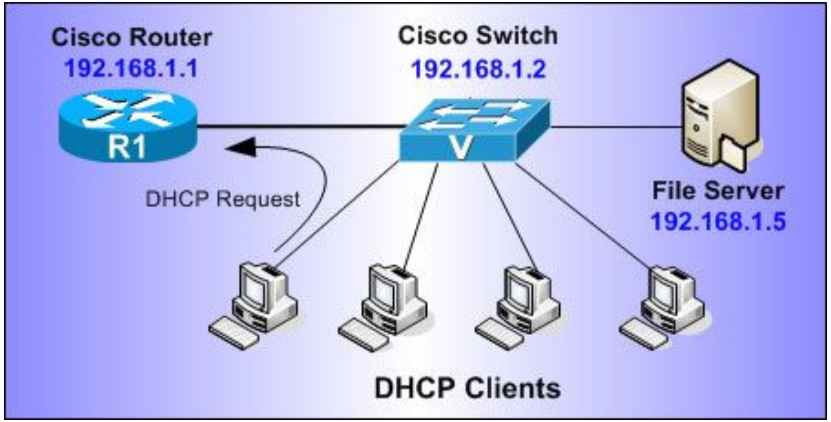
```
! VLANs
vlan 20
        name VLAN20_RIGHT
vlan 21
        name VLAN21_RIGHT
vlan 22
        name VLAN22_RIGHT

! SVIs (Gateways)
interface vlan 20
        ip address 192.168.20.1 255.255.255.0
        no shutdown
interface vlan 21
        ip address 192.168.21.1 255.255.255.0
        no shutdown
interface vlan 22
        ip address 192.168.22.1 255.255.255.0
        no shutdown
```



DHCP

- Automatically assigns IP addresses and network configuration to devices, reducing manual setup.
- Uses the DORA process (Discover, Offer, Request, Acknowledge) to provide clients with leases.
- Can be implemented on routers, servers, or switches, supporting options like default gateway and DNS distribution.

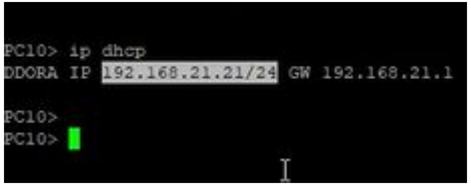


DHCP Implementation

- Excluded IPs that shouldn’t be given out to end devices
- Each VLAN has independent pool with network address, default-router, and dns-server defined
- Successful IP request on each end device

```
! DHCP for VLAN20/21/22
ip dhcp excluded-address 192.168.20.1 192.168.20.20
ip dhcp excluded-address 192.168.21.1 192.168.21.20
ip dhcp excluded-address 192.168.22.1 192.168.22.20

ip dhcp pool VLAN20_POOL
        network 192.168.20.0 255.255.255.0
        default-router 192.168.20.1
        dns-server 8.8.8.8
ip dhcp pool VLAN21_POOL
        network 192.168.21.0 255.255.255.0
        default-router 192.168.21.1
        dns-server 8.8.8.8
ip dhcp pool VLAN22_POOL
        network 192.168.22.0 255.255.255.0
        default-router 192.168.22.1
        dns-server 8.8.8.8
```

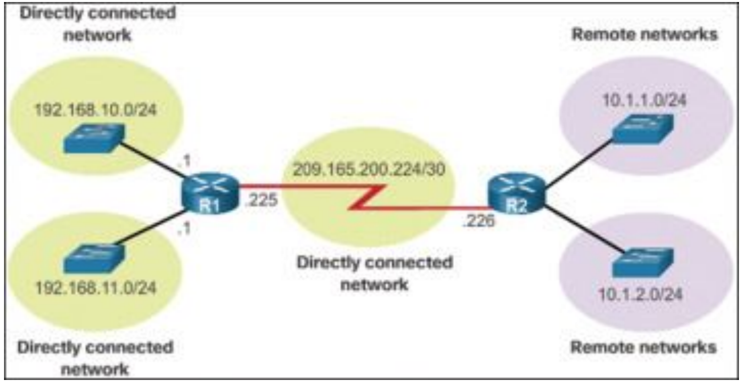


```
PC10> ip dhcp
DDORA IP 192.168.21.21/24 GW 192.168.21.1

PC10>
PC10>
```

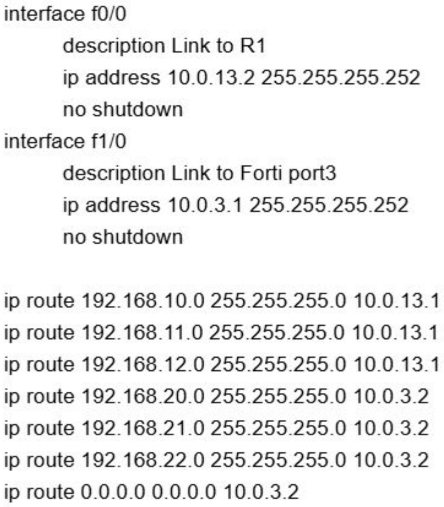
Routing

- Directs packets between different networks by selecting the best path based on routing tables.
- Can be configured manually with static routes or automatically using dynamic protocols like OSPF, EIGRP, and RIP.
- Ensures efficient, scalable communication across multi-network environments by adapting to topology changes.



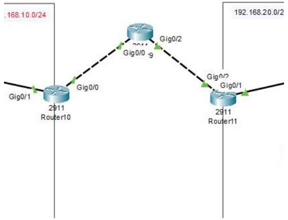
Routing Implementation

- Static routes between both sites for low overhead
- Routers have defined ip address ranges and destination address for them
- default route (0.0.0.0/0) moves all outbound traffic through gateway



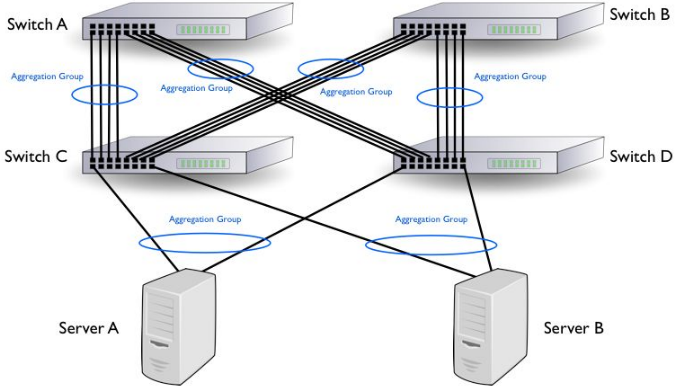
```
interface f0/0
        description Link to R1
        ip address 10.0.13.2 255.255.255.252
        no shutdown
interface f1/0
        description Link to Forti port3
        ip address 10.0.3.1 255.255.255.252
        no shutdown

ip route 192.168.10.0 255.255.255.0 10.0.13.1
ip route 192.168.11.0 255.255.255.0 10.0.13.1
ip route 192.168.12.0 255.255.255.0 10.0.13.1
ip route 192.168.20.0 255.255.255.0 10.0.3.2
ip route 192.168.21.0 255.255.255.0 10.0.3.2
ip route 192.168.22.0 255.255.255.0 10.0.3.2
ip route 0.0.0.0 0.0.0.0 10.0.3.2
```



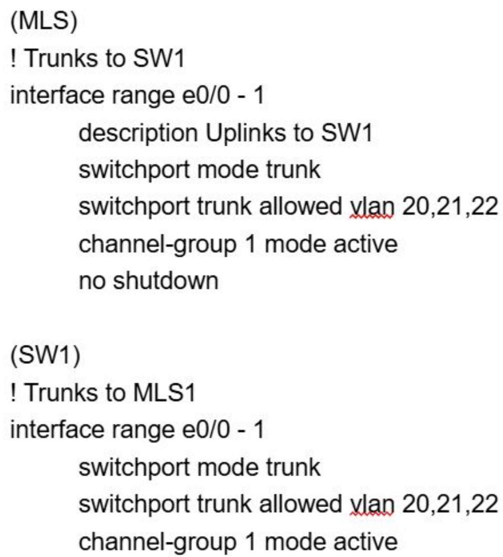
Port Channel

- Combines multiple physical links into a single logical link to increase bandwidth and provide redundancy.
- Supports load balancing and failover, ensuring traffic continues if one link fails.
- Commonly used between switches, routers, and servers for optimized throughput and link aggregation.



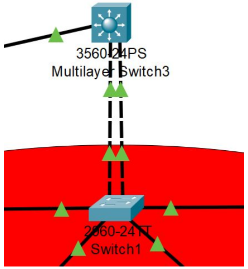
Port Channel Implementation

- Both MLS and SW1 interfaces are configured as trunks, allowing multiple VLANs to pass between switches.
- Interfaces are bundled using “channel-group 1 mode active” to form a LACP EtherChannel, increasing bandwidth and providing redundancy.
- no shutdown enables the links



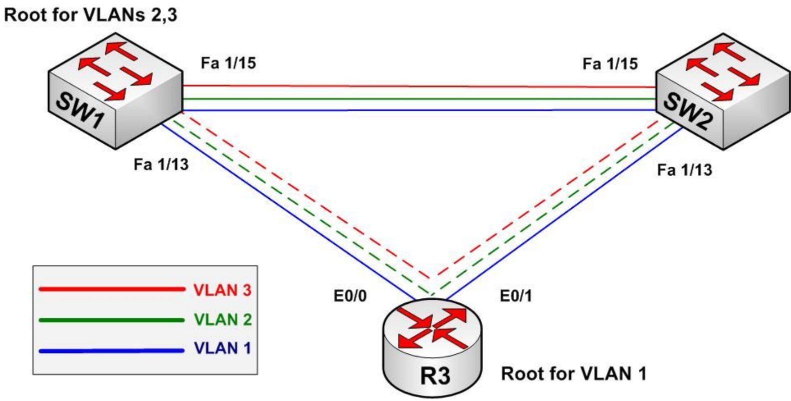
```
(MLS)
! Trunks to SW1
interface range e0/0 - 1
        description Uplinks to SW1
        switchport mode trunk
        switchport trunk allowed vlan 20,21,22
        channel-group 1 mode active
        no shutdown

(SW1)
! Trunks to MLS1
interface range e0/0 - 1
        switchport mode trunk
        switchport trunk allowed vlan 20,21,22
        channel-group 1 mode active
        no shutdown
```



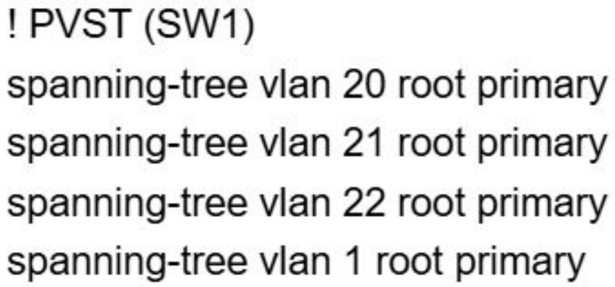
PVST

- VLAN-specific spanning trees: Creates a separate STP instance for each VLAN, allowing optimized path selection per VLAN.
- Redundancy & loop prevention: Prevents network loops while providing backup paths if the primary link fails.
- Better load balancing: Different VLANs can use different root bridges, distributing traffic more efficiently across links.

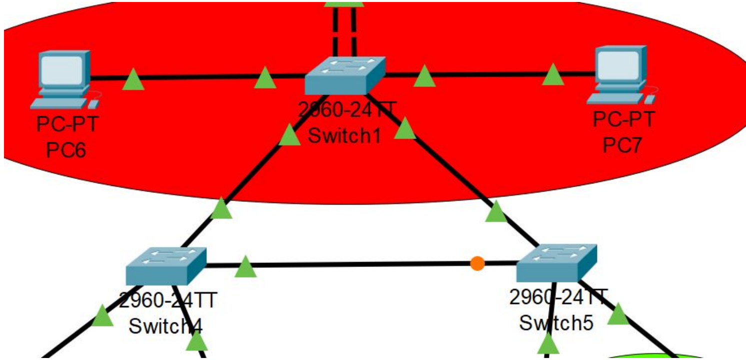


PVST Implementation

- Each of the three VLANs operates its own independent Spanning Tree instance.
- The administration’s switch (SW1) is configured as the root bridge for all VLANs.
- Centralizing the root bridge on SW1 ensures predictable path selection and reduces network loops.

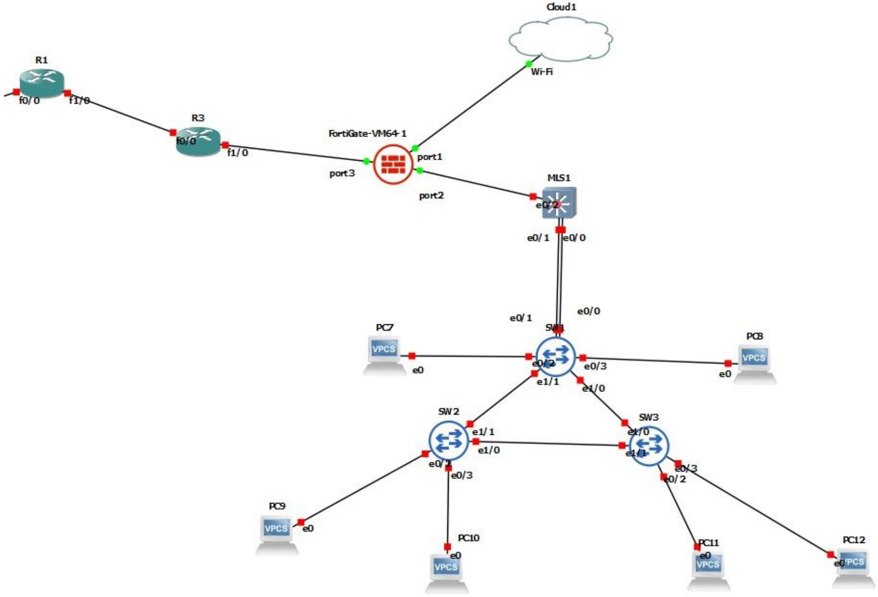


```
! PVST (SW1)
spanning-tree vlan 20 root primary
spanning-tree vlan 21 root primary
spanning-tree vlan 22 root primary
spanning-tree vlan 1 root primary
```

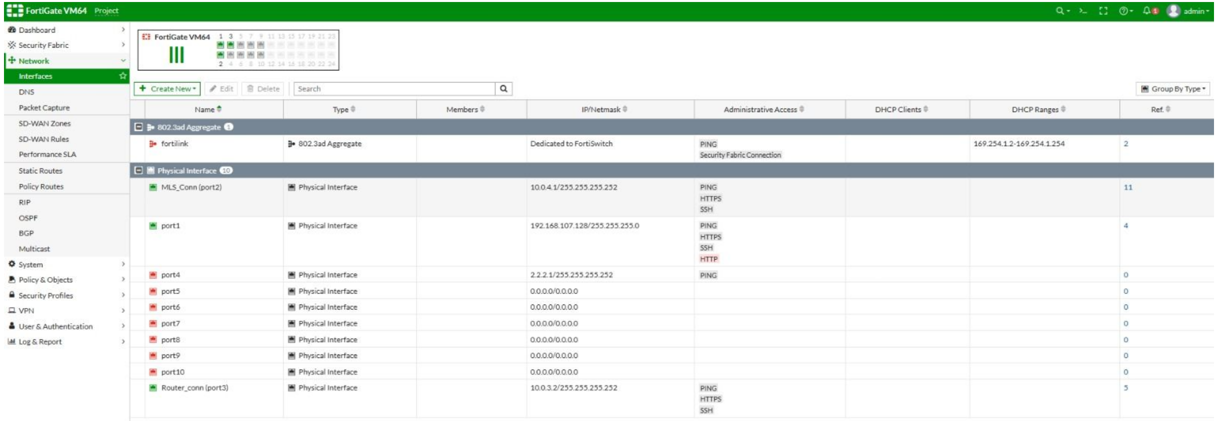


FortiGate Integration

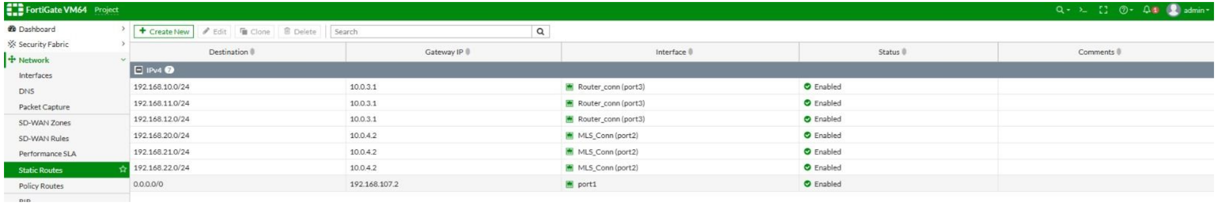
Interfaces	Role	IP Address
port1	WAN	192.168.107.128/24
port2	LAN	10.0.3.1/24
port3	WAN	10.0.4.1/24



FortiGate Interfaces & Static Routes



Name	Type	Members	IP/Netmask	Administrative Access	DHCP Clients	DHCP Ranges	Ref.
802.3ad Aggregate 1							
fortilink	802.3ad Aggregate		Dedicated to FortiSwitch	PING Security Fabric Connection		169.254.1.2-169.254.1.254	2
Physical Interface 10							
MLS_Conn (port2)	Physical Interface		10.0.4.1/255.255.255.252	PING HTTPS SSH			11
port1	Physical Interface		192.168.107.128/255.255.255.0	PING HTTPS SSH HTTP			4
port4	Physical Interface		2.2.2.1/255.255.255.252	PING			0
port5	Physical Interface		0.0.0.0/0.0.0.0				0
port6	Physical Interface		0.0.0.0/0.0.0.0				0
port7	Physical Interface		0.0.0.0/0.0.0.0				0
port8	Physical Interface		0.0.0.0/0.0.0.0				0
port9	Physical Interface		0.0.0.0/0.0.0.0				0
port10	Physical Interface		0.0.0.0/0.0.0.0				0
Router_conn (port3)	Physical Interface		10.0.3.2/255.255.255.252	PING HTTPS SSH			5

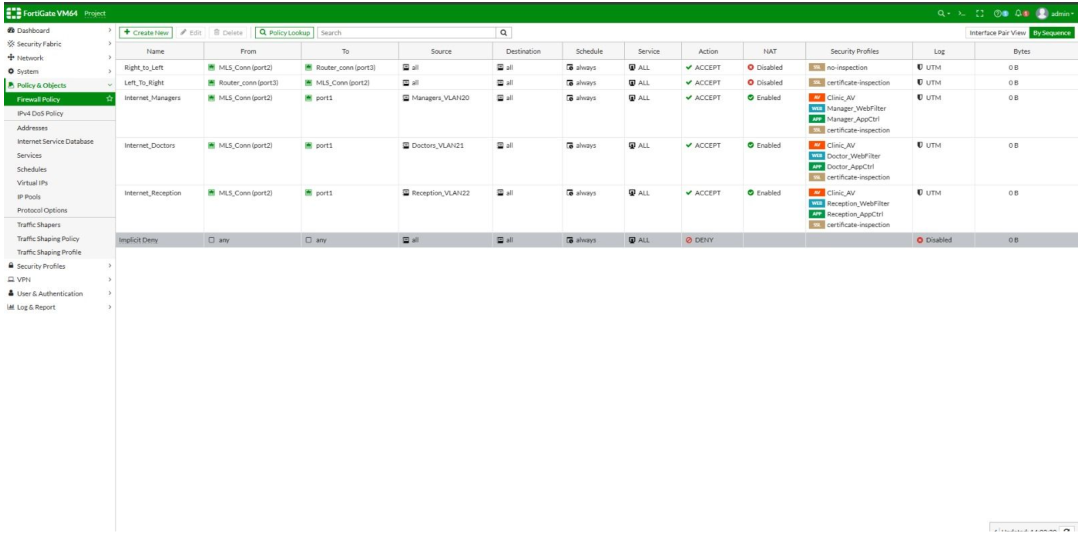


Destination	Gateway IP	Interface	Status	Comments
IPv4 7				
192.168.10.0/24	10.0.3.1	Router_conn (port3)	✓ Enabled	
192.168.11.0/24	10.0.3.1	Router_conn (port3)	✓ Enabled	
192.168.12.0/24	10.0.3.1	Router_conn (port3)	✓ Enabled	
192.168.20.0/24	10.0.4.2	MLS_Conn (port2)	✓ Enabled	
192.168.21.0/24	10.0.4.2	MLS_Conn (port2)	✓ Enabled	
192.168.22.0/24	10.0.4.2	MLS_Conn (port2)	✓ Enabled	
0.0.0.0/0	192.168.107.2	port1	✓ Enabled	

Firewall Policies

Firewall Policies

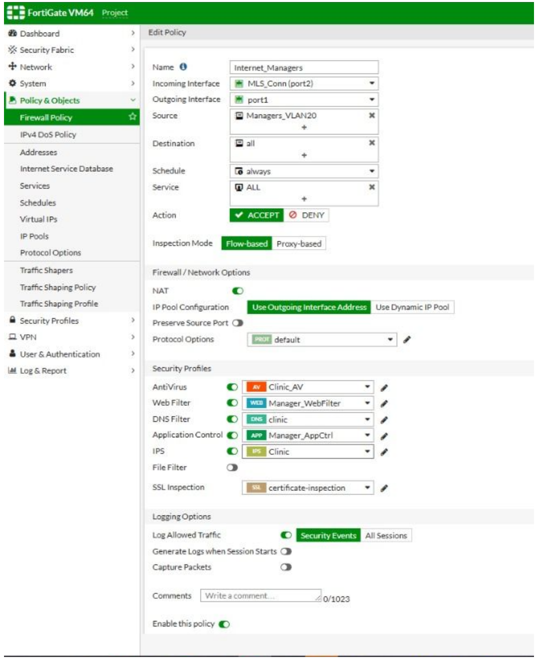
- Admins -> Internet
  - (low restriction)
- Doctors -> Internet
  - (Medium filtering)
- Reception -> Internet
  - (Strict filtering)



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	SSL no-inspection	UTM	0 B
Left_To_Right	Router_conn (port3)	MLS_Conn (port2)	all	all	always	ALL	✓ ACCEPT	Disabled	SSL certificate-inspection	UTM	0 B
Internet_Managers	MLS_Conn (port2)	port1	Managers_VLAN20	all	always	ALL	✓ ACCEPT	Enabled	AV Clinic_AV WEB Manager_WebFilter APP Manager_AppCtrl SSL certificate-inspection	UTM	0 B
Internet_Doctors	MLS_Conn (port2)	port1	Doctors_VLAN21	all	always	ALL	✓ ACCEPT	Enabled	AV Clinic_AV WEB Doctor_WebFilter APP Doctor_AppCtrl SSL certificate-inspection	UTM	0 B
Internet_Reception	MLS_Conn (port2)	port1	Reception_VLAN22	all	always	ALL	✓ ACCEPT	Enabled	AV Clinic_AV WEB Reception_WebFilter APP Reception_AppCtrl SSL certificate-inspection	UTM	0 B
Implicit Deny	□ any	□ any	all	all	always	ALL	DENY			Disabled	0 B

Firewall Policies

Admins



Edit Policy

Name: Internet_Managers
Incoming Interface: MLS_Conn (port2)
Outgoing Interface: port1
Source: Managers_VLAN20
Destination: all
Schedule: always
Service: ALL
Action: [✓ ACCEPT] DENY
Inspection Mode: [✓ Flow-based] Proxy-based

Firewall / Network Options

NAT ●
IP Pool Configuration: [✓ Use Outgoing Interface Address] Use Dynamic IP Pool
Preserve Source Port ○
Protocol Options: PROT default

Security Profiles

AntiVirus ● AV Clinic_AV
Web Filter ● WEB Manager_WebFilter
DNS Filter ● DNS clinic
Application Control ● APP Manager_AppCtrl
IPS ● IPS Clinic
File Filter ○
SSL Inspection: SSL certificate-inspection

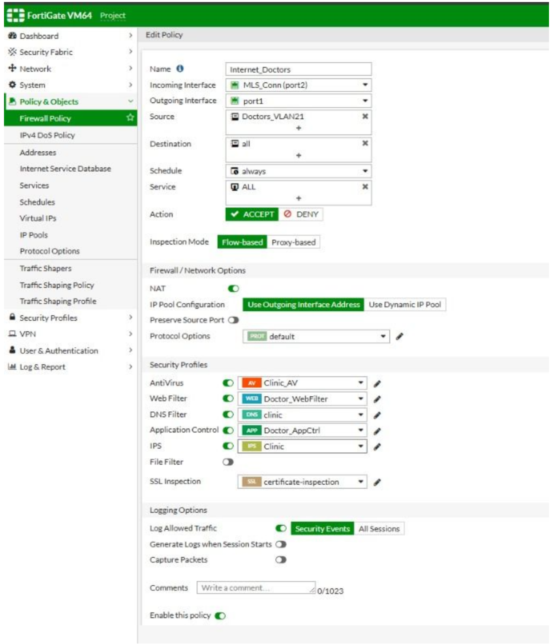
Logging Options

Log Allowed Traffic ● [✓ Security Events] All Sessions
Generate Logs when Session Starts ○
Capture Packets ○

Comments: Write a comment... 0/1023

Enable this policy ●

Staff



Edit Policy

Name: Internet_Doctors
Incoming Interface: MLS_Conn (port2)
Outgoing Interface: port1
Source: Doctors_VLAN21
Destination: all
Schedule: always
Service: ALL
Action: [✓ ACCEPT] DENY
Inspection Mode: [✓ Flow-based] Proxy-based

Firewall / Network Options

NAT ●
IP Pool Configuration: [✓ Use Outgoing Interface Address] Use Dynamic IP Pool
Preserve Source Port ○
Protocol Options: PROT default

Security Profiles

AntiVirus ● AV Clinic_AV
Web Filter ● WEB Doctor_WebFilter
DNS Filter ● DNS clinic
Application Control ● APP Doctor_AppCtrl
IPS ● IPS Clinic
File Filter ○
SSL Inspection: SSL certificate-inspection

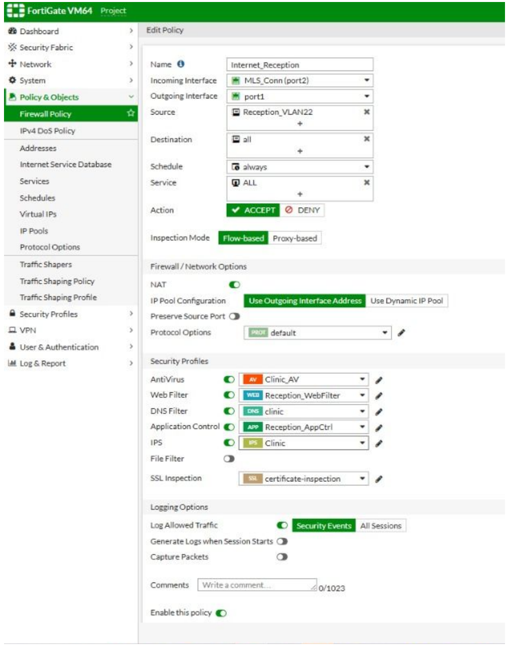
Logging Options

Log Allowed Traffic ● [✓ Security Events] All Sessions
Generate Logs when Session Starts ○
Capture Packets ○

Comments: Write a comment... 0/1023

Enable this policy ●

Guests



Edit Policy

Name: Internet_Reception
Incoming Interface: MLS_Conn (port2)
Outgoing Interface: port1
Source: Reception_VLAN22
Destination: all
Schedule: always
Service: ALL
Action: [✓ ACCEPT] DENY
Inspection Mode: [✓ Flow-based] Proxy-based

Firewall / Network Options

NAT ●
IP Pool Configuration: [✓ Use Outgoing Interface Address] Use Dynamic IP Pool
Preserve Source Port ○
Protocol Options: PROT default

Security Profiles

AntiVirus ● AV Clinic_AV
Web Filter ● WEB Reception_WebFilter
DNS Filter ● DNS clinic
Application Control ● APP Reception_AppCtrl
IPS ● IPS Clinic
File Filter ○
SSL Inspection: SSL certificate-inspection

Logging Options

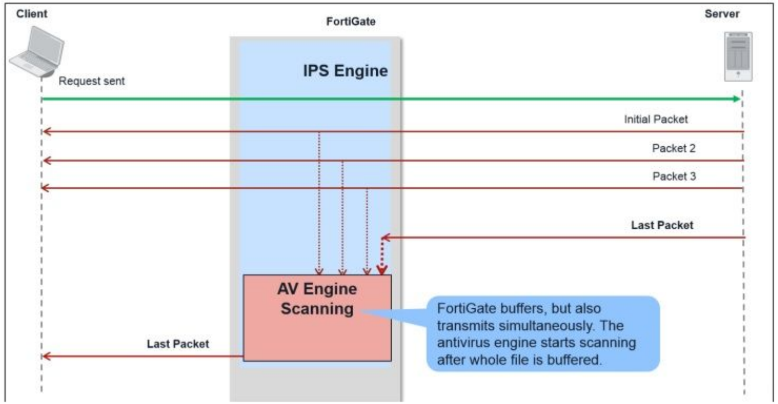
Log Allowed Traffic ● [✓ Security Events] All Sessions
Generate Logs when Session Starts ○
Capture Packets ○

Comments: Write a comment... 0/1023

Enable this policy ●

Antivirus

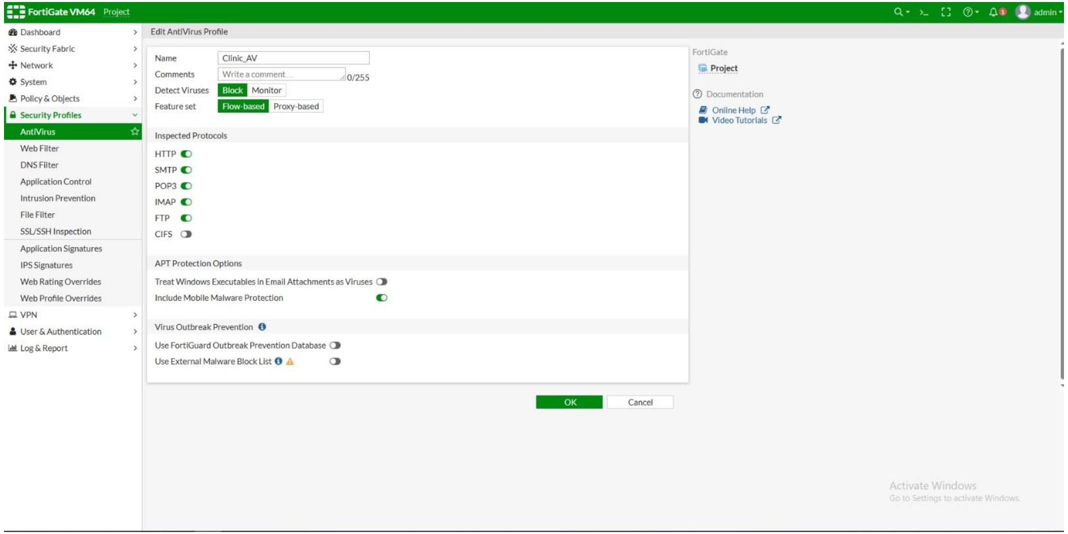
- Provides real-time malware detection by scanning files, web traffic, and email content passing through the firewall.
- Uses signature-based, heuristic, and AI-driven analysis to detect known and emerging threats.
- Supports both flow-based and proxy-based inspection modes to balance performance and security needs.



FortiGate buffers, but also transmits simultaneously. The antivirus engine starts scanning after whole file is buffered.

Antivirus Implementation

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



Edit AntiVirus Profile

Name: Clinic_AV
Comments: Write a comment... 0/255
Detect Viruses: [✓ Block] Monitor
Feature set: [✓ Flow-based] Proxy-based

Inspected Protocols
HTTP ●
SMTP ●
POP3 ●
IMAP ●
FTP ●
CIFS ○

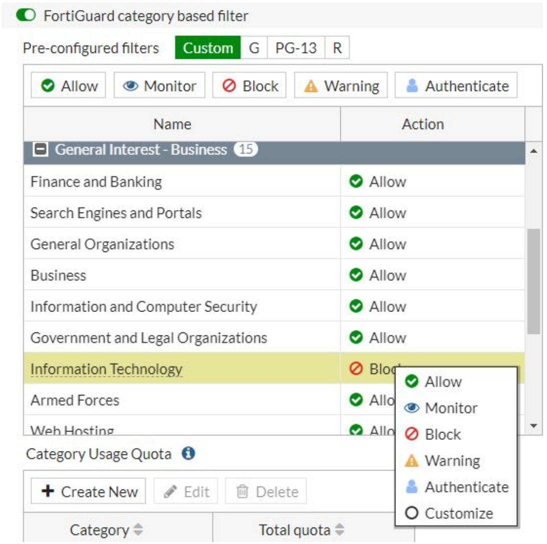
APT Protection Options
Treat Windows Executables in Email Attachments as Viruses ○
Include Mobile Malware Protection ●

Virus Outbreak Prevention
Use FortiGuard Outbreak Prevention Database ○
Use External Malware Block List ○

OK Cancel

Web Filtering

- Controls and monitors user access to websites based on categories, reputation, or custom URL rules.
- Uses FortiGuard Web Filtering database for real-time categorization and threat intelligence.
- Provides granular controls such as allow/block/exempt, quotas, and user/group-based policies.
- Generates detailed logs and reports to track browsing behavior and security events.



FortiGuard category based filter

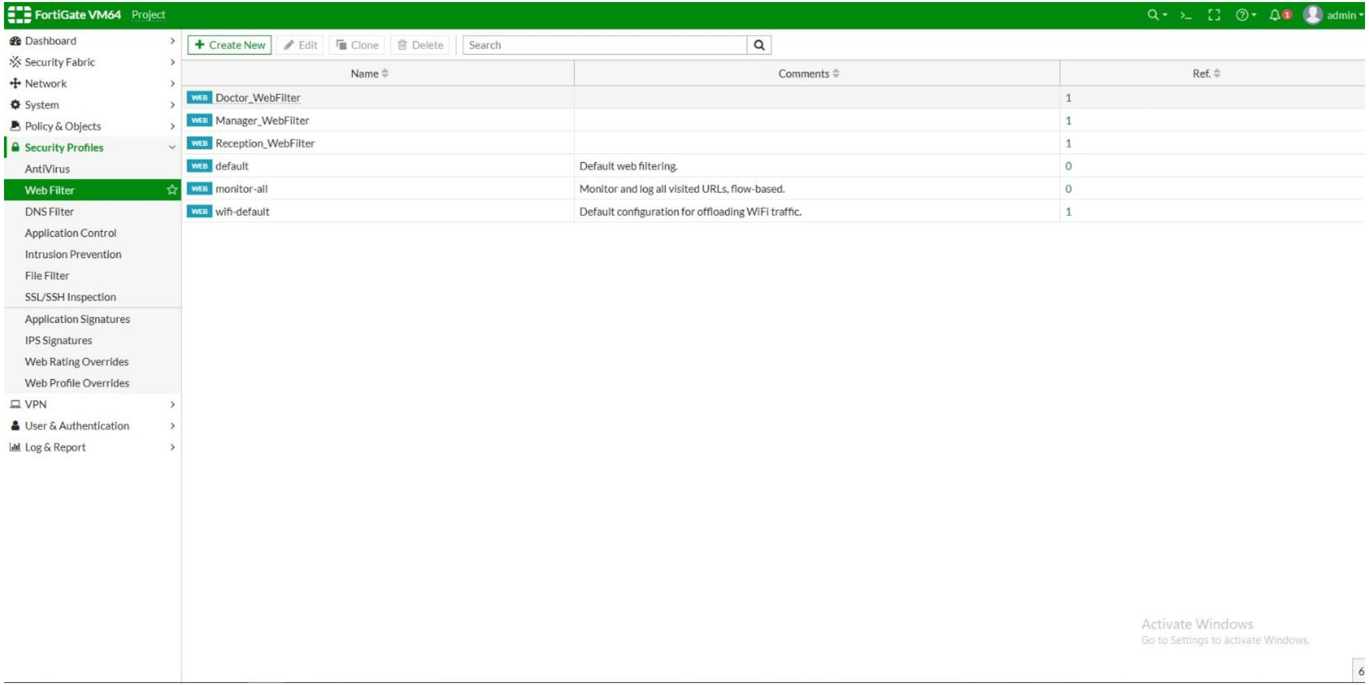
Pre-configured filters: Custom | G | PG-13 | R

Name	Action
General Interest - Business 15	
Finance and Banking	Allow
Search Engines and Portals	Allow
General Organizations	Allow
Business	Allow
Information and Computer Security	Allow
Government and Legal Organizations	Allow
Information Technology	Bloc
Armed Forces	Allo
Web Hosting	Allo

Category Usage Quota

Category	Total quota

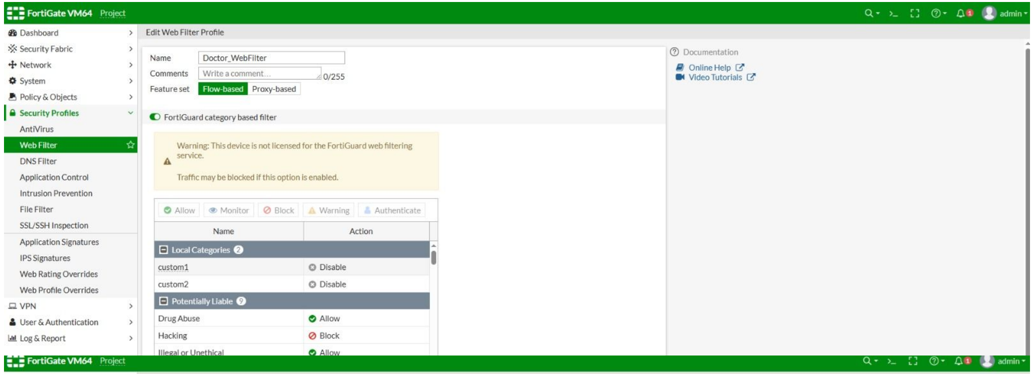
Web Filtering



Name	Comments	Ref.
WEB Doctor_WebFilter		1
WEB Manager_WebFilter		1
WEB Reception_WebFilter		1
WEB default	Default web filtering.	0
WEB monitor-all	Monitor and log all visited URLs, flow-based.	0
WEB wifi-default	Default configuration for offloading WiFi traffic.	1

Web Filtering

- Profiles based on group
  - Doctors have medium filtering (can view drug-related content for example but not hacking
  - Waiting room more strict (anything potentially liable blocked for example)



Edit Web Filter Profile

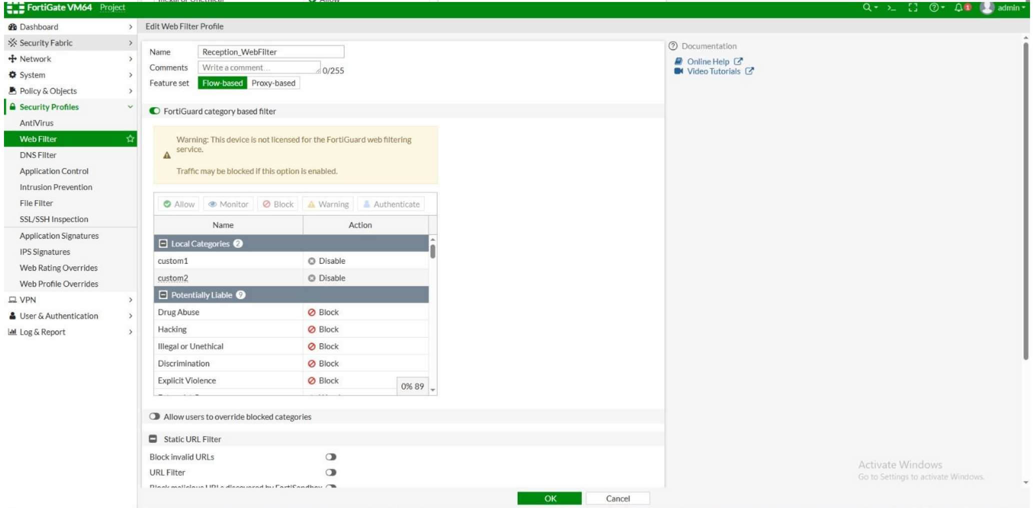
Name: Doctor_WebFilter
Comments: Write a comment... 0/255
Feature set: Flow-based | Proxy-based

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.

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



Edit Web Filter Profile

Name: Reception_WebFilter
Comments: Write a comment... 0/255
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.

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

Allow users to override blocked categories

Static URL Filter

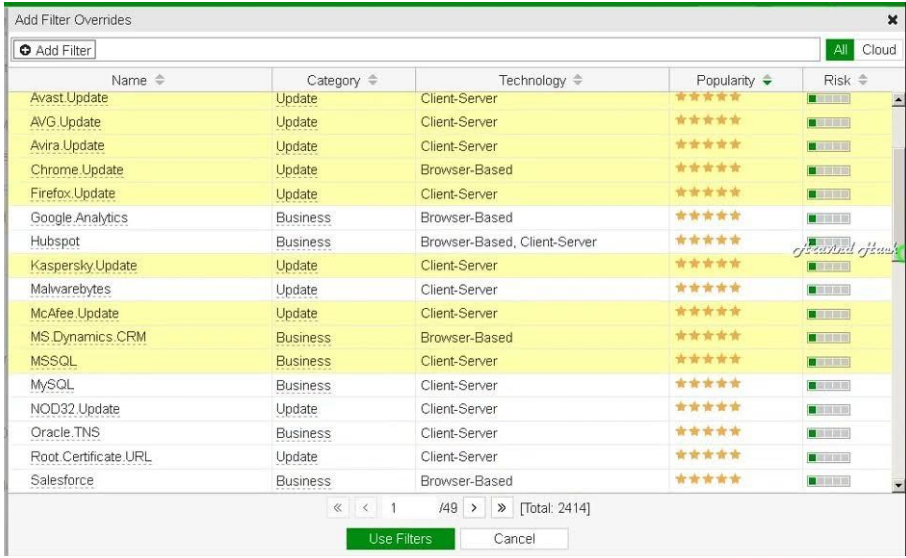
Block invalid URLs

URL Filter

Block malicious URLs discovered by FortiSandbox

Application Control

- Identifies and controls applications running on the network, even with non-standard ports or encryption.
- Uses a large, continuously updated signature database from FortiGuard to detect thousands of applications.
- Allows administrators to allow, block, throttle, or monitor specific applications or application categories.

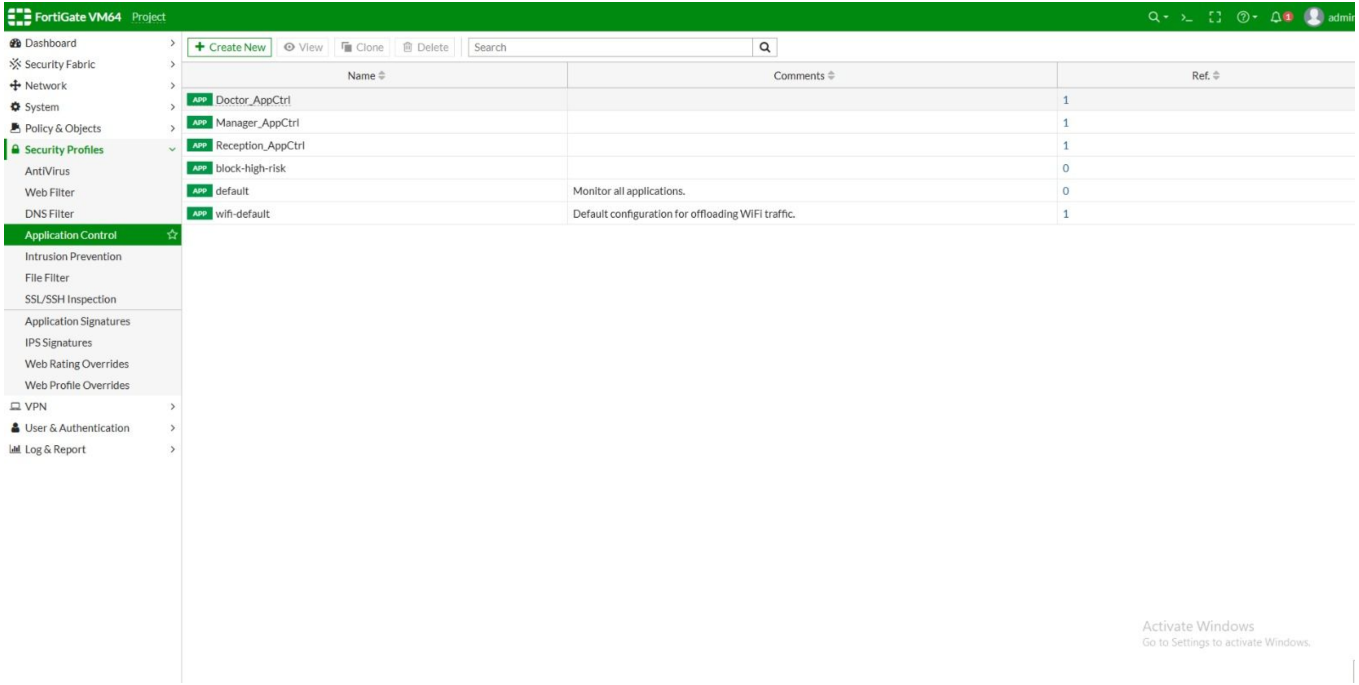


Add Filter Overrides

Name	Category	Technology	Popularity	Risk
Avast.Update	Update	Client-Server	★★★★★	■□□□□
AVG.Update	Update	Client-Server	★★★★★	■□□□□
Avira.Update	Update	Client-Server	★★★★★	■□□□□
Chrome.Update	Update	Browser-Based	★★★★★	■□□□□
Firefox.Update	Update	Client-Server	★★★★★	■□□□□
Google.Analytics	Business	Browser-Based	★★★★★	■□□□□
Hubspot	Business	Browser-Based, Client-Server	★★★★★	■□□□□
Kaspersky.Update	Update	Client-Server	★★★★★	■□□□□
Malwarebytes	Update	Client-Server	★★★★★	■□□□□
McAfee.Update	Update	Client-Server	★★★★★	■□□□□
MS.Dynamics.CRM	Business	Browser-Based	★★★★★	■□□□□
MSSQL	Business	Client-Server	★★★★★	■□□□□
MySQL	Business	Client-Server	★★★★★	■□□□□
NOD32.Update	Update	Client-Server	★★★★★	■□□□□
Oracle.TNS	Business	Client-Server	★★★★★	■□□□□
Root.Certificate.URL	Update	Client-Server	★★★★★	■□□□□
Salesforce	Business	Browser-Based	★★★★★	■□□□□

1 /49 [Total: 2414]

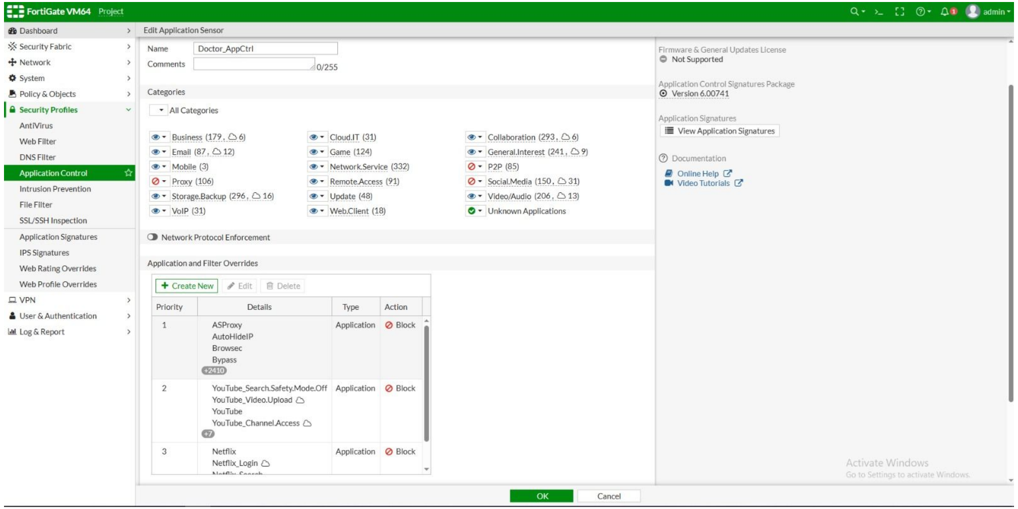
Application Control



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

Application Control

- Control who accesses what to avoid abuse of network
- Limit non-essential applications for staff—e.g., doctors cannot access Netflix during shifts.
- Restrict high-bandwidth applications for guests to maintain network performance.



Edit Application Sensor

Name: Doctor_AppCtrl

Comments: 0/255

Categories

All Categories

👁 Business (179, ☁ 6)	👁 Cloud.IT (31)	👁 Collaboration (293, ☁ 6)
👁 Email (87, ☁ 12)	👁 Game (124)	👁 General.Interest (241, ☁ 9)
👁 Mobile (3)	👁 Network.Service (332)	⊘ P2P (85)
⊘ Proxy (106)	👁 Remote.Access (91)	⊘ Social.Media (150, ☁ 31)
👁 Storage.Backup (296, ☁ 16)	👁 Update (48)	👁 Video/Audio (206, ☁ 13)
👁 VoIP (31)	👁 Web.Client (18)	✓ Unknown Applications

○ Network Protocol Enforcement

Application and Filter Overrides

Priority	Details	Type	Action
1	ASProxy AutoHideIP Browsec Bypass +2410	Application	⊘ Block
2	YouTube_Search.Safety.Mode.Off YouTube_Video.Upload ☁ YouTube YouTube_Channel.Access ☁ +7	Application	⊘ Block
3	Netflix Netflix_Login ☁ Netflix_Search	Application	⊘ Block

Firmware & General Updates License
Not Supported

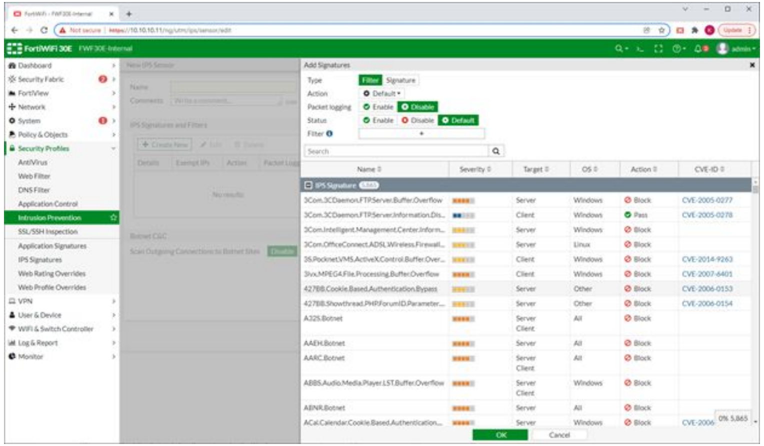
Application Control Signatures Package
Version 6.00741

Application Signatures

Documentation

IPS

- Detects and blocks network attacks by inspecting traffic for malicious patterns and exploits.
- Uses FortiGuard signature updates to identify known and emerging vulnerabilities.
- Protects systems from threats like buffer overflows, port scans, evasion attempts, and protocol violations.



Add Signatures

Type	[✓ Filter] Signature
Action	Default ▾
Packet logging	Enable [✓ Disable]
Status	Enable Disable [✓ Default]
Filter	+

Search

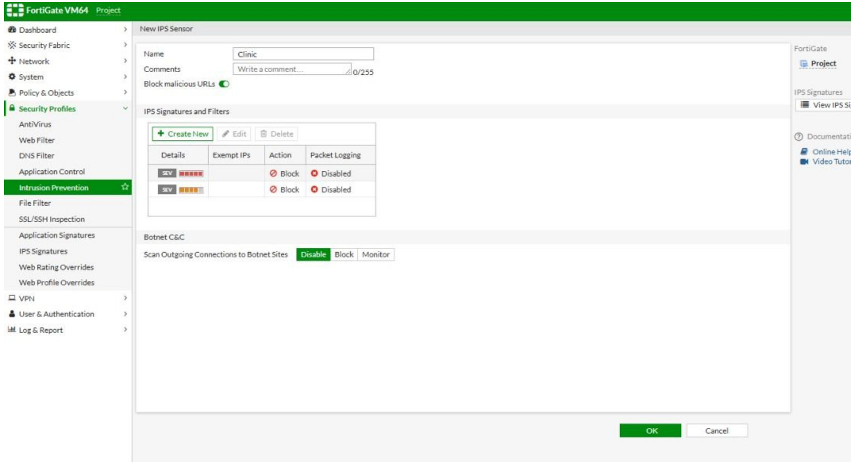
Name	Severity	Target	OS	Action	CVE-ID
IPS Signature 5,865					
3Com.3CDaemon.FTP.Server.Buffer.Overflow	■■■■□	Server	Windows	Block	CVE-2005-0277
3Com.3CDaemon.FTP.Server.Information.Dis...	■■□□□	Client	Windows	Pass	CVE-2005-0278
3Com.Intelligent.Management.Center.Inform...	■■■□□	Server	Windows	Block	
3Com.OfficeConnect.ADSL.Wireless.Firewall...	■■■□□	Server	Linux	Block	
35.Pocknet.VMS.ActiveX.Control.Buffer.Over...	■■■□□	Client	Windows	Block	CVE-2014-9263
3ivx.MPEG4.File.Processing.Buffer.Overflow	■■■■□	Client	Windows	Block	CVE-2007-6401
427BB.Cookie.Based.Authentication.Bypass	■■■□□	Server	Other	Block	CVE-2006-0153
427BB.Showthread.PHP.ForumID.Parameter...	■■■□□	Server	Other	Block	CVE-2006-0154
A325.Botnet	■■■■□	Server Client	All	Block	
AAEH.Botnet	■■■■□	Server	All	Block	
AARC.Botnet	■■■■□	Server Client	All	Block	
ABBS.Audio.Media.Player.LST.Buffer.Overflow	■■■■□	Server Client	Windows	Block	
ABNR.Botnet	■■■■□	Server	All	Block	
ACal.Calendar.Cookie.Based.Authentication...	■■■■□	Server	Windows	Block	CVE-2006

0% 5,865

OK Cancel

IPS Implementation

- Implemented an IPS sensor to actively monitor and protect the clinic’s network.
- Automatically block signatures classified as highly critical to prevent severe security incidents.
- Block access to known malicious URLs to reduce exposure to web-based threats.



New IPS Sensor

Name: Clinic

Comments: Write a comment... 0/255

Block malicious URLs ●

IPS Signatures and Filters

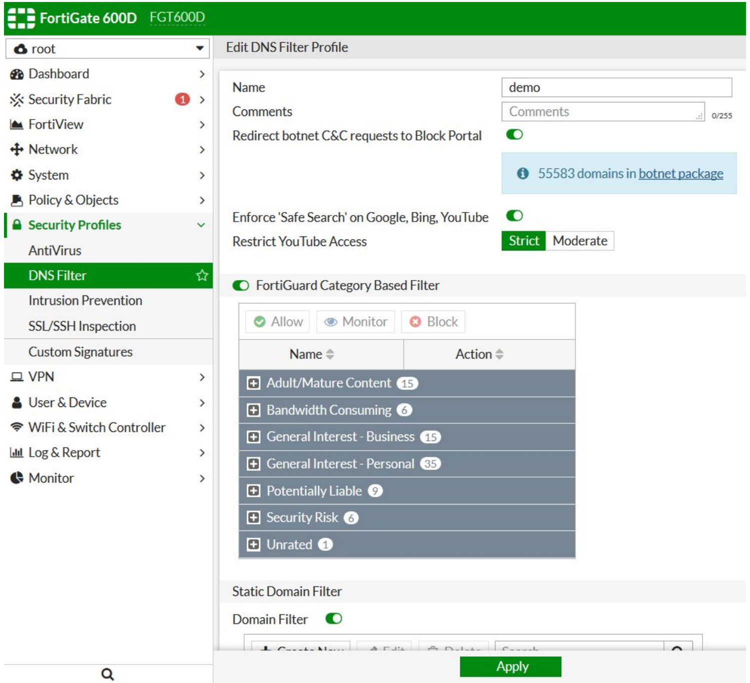
Details	Exempt IPs	Action	Packet Logging
SEV		Block	Disabled
SEV		Block	Disabled

Botnet C&C

Scan Outgoing Connections to Botnet Sites: [✓ Disable] Block Monitor

DNS Filtering

- Blocks malicious or unwanted domains at the DNS lookup stage, before any web connection is made.
- Uses FortiGuard DNS intelligence to stop phishing, botnet, and malware-related domains.
- DNS Filtering blocks threats earlier at the domain-lookup level with lower overhead than Web Filtering which inspects full web traffic.



Edit DNS Filter Profile

Name: demo

Comments: Comments 0/255

Redirect botnet C&C requests to Block Portal ●

55583 domains in botnet package

Enforce 'Safe Search' on Google, Bing, YouTube ●

Restrict YouTube Access: Strict | Moderate

● FortiGuard Category Based Filter

Allow | Monitor | Block

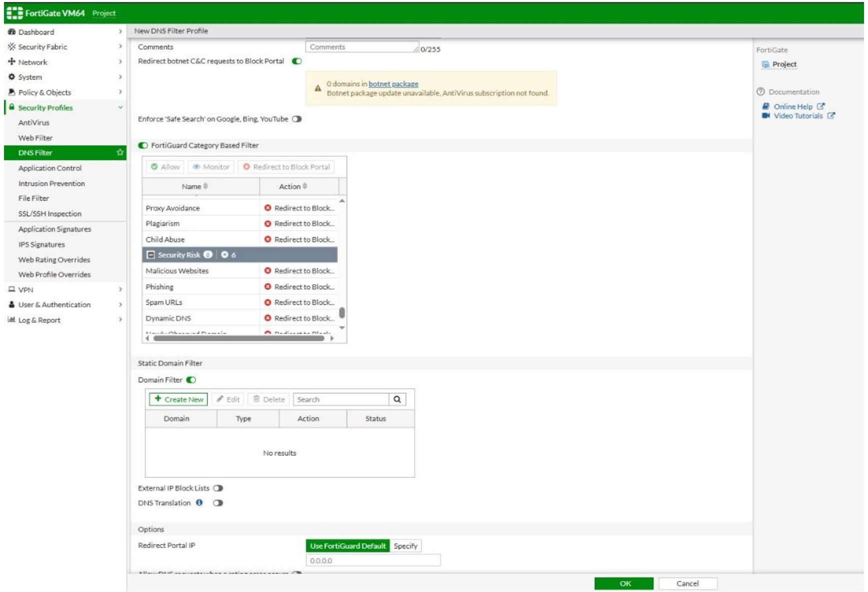
Name	Action
⊞ Adult/Mature Content 15	
⊞ Bandwidth Consuming 6	
⊞ General Interest - Business 15	
⊞ General Interest - Personal 35	
⊞ Potentially Liable 9	
⊞ Security Risk 6	
⊞ Unrated 1	

Static Domain Filter

Domain Filter ●

DNS Filtering

- Enabled filtering to control access based on website categories.
- Block sites that present security risks, contain inappropriate content, etc.



New DNS Filter Profile

Comments: Comments 0/255

Redirect botnet C&C requests to Block Portal ●

0 domains in botnet package
Botnet package update unavailable, AntiVirus subscription not found.

Enforce 'Safe Search' on Google, Bing, YouTube ○

● FortiGuard Category Based Filter

Allow | Monitor | Redirect to Block Portal

Name	Action
Proxy Avoidance	Redirect to Block...
Plagiarism	Redirect to Block...
Child Abuse	Redirect to Block...
Security Risk 6	6
Malicious Websites	Redirect to Block...
Phishing	Redirect to Block...
Spam URLs	Redirect to Block...
Dynamic DNS	Redirect to Block...

Static Domain Filter

Domain Filter ●

Create New | Edit | Delete | Search

Domain	Type	Action	Status
No results			

External IP Block Lists ○

DNS Translation ○

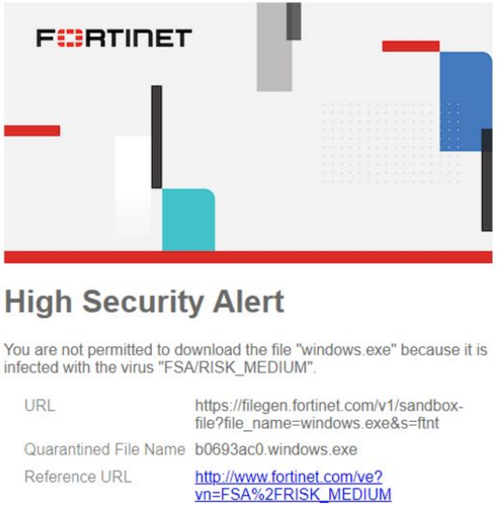
Options

Redirect Portal IP: Use FortiGuard Default | Specify
0.0.0.0

OK | Cancel

Expected Outcomes

Antivirus

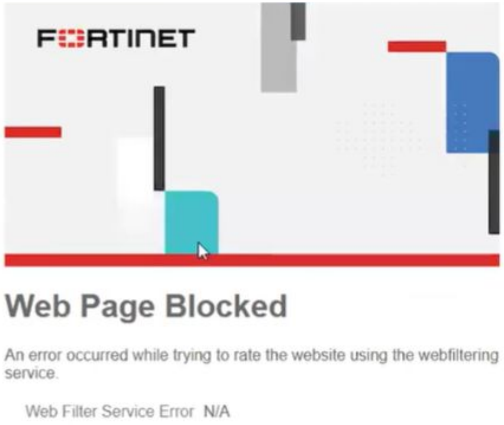


High Security Alert

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

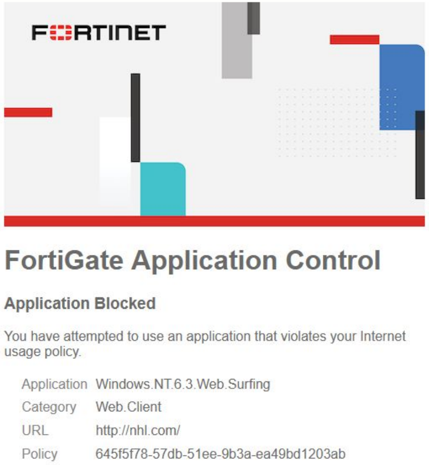


Web Page Blocked

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