Yarmouk University
Hijjawi Faculty for Engineering Technology
Department of Computer Engineering

Graduation Project Report

Enhancing Network Connectivity for Yarmouk University using Fortinet products

Omar B. Talafhah - 2020980115

Zaid F. Salameh - 2020980118

Supervisor: Prof. Ola Taani

Semester: Summer 2023/2024

Date: July 20, 2024

Students' Property Right Declaration and Anti-Plagiarism Statement

We hereby declare that the work in this graduation project at Yarmouk University is our own except for quotations and summaries which have been duly acknowledged. This work has not been accepted for any degree and is not concurrently submitted for award of other degrees. It is the sole property of Yarmouk University and it is protected under the intellectual property right laws and conventions. We hereby declare that this report is our own work except from properly referenced quotations and contains no plagiarism. We have read and understood the school's rules on assessment offenses, which are available at Yarmouk University Handbook.

Name: Omar B. Talafhah	Signature:
Name: Zaid F. Salameh	Signature:

Contents

List of Tables

List of Figures

Abstract

Yarmouk University, like many other universities, has a large campus with many buildings and facilities. The university's network infrastructure is sort of outdated and does not provide adequate coverage for all areas, and connecting to the web servers in the university from outside can be a headache when more people are trying to access them. This project aims to enhance the network connectivity for Yarmouk University by using Fortinet products.

Fortinet is a network security company that provides relatively cheap, modern, and easy-to-use and maintain products that can also easily provide a great level of network security through different measures. Fortinet relies heavily on the use of **FortiGate** devices, which are firewalls that can be used to secure the network, as well as managing any Fortinet device connected to it. This project will implement a Hierarchical networking design for the main university building and another one for the South building, and connect them using **Site-To-Site VPN** to provide a secure connection between the two buildings. This project will also include a protection layer for the data center in the university using **DMZ** where the DMZ will include web servers and any service that is ok to be public. The project will also implement a Web Application Firewall to protect the web servers in the university from any attacks. One of the main focuses of this project is to provide redundancy and load balancing for the network using various technologies like **SD-WAN** and link monitoring for Internet connectivity and **High Availability (HA)** for FortiGate redundancy. FortiGates will also provide services like **Web Filtering** and **Application Control** to control the network traffic and prevent any unwanted traffic from entering the network. We will be using various Fortinet products like FortisSwitches, FortiAPs, FortiAnalyzer, and FortiManager to provide a complete solution for the university's network infrastructure.

1. Introduction

1.1 Problem Statement and Purpose

This Project aims to enhance university networking by making it more secure, reliable, easier and cheaper to obtain and maintain, and provide a better user experience for the students and staff.

1.2 Background

Yarmouk University holds more than 41,000 students and has many schools and departments [7] , yet, the network infrastructure is outdated and does not provide adequate coverage for all areas, and connecting to the web servers in the university from outside can be a nightmare during peak times. For example, system responsiveness during registration on the was not that great, especially that only those who are expected to graduate can register.

1.3 Aims and objectives

The main aim of this project is to enhance the network connectivity for Yarmouk University by using Fortinet products. The objectives of this project are:

- Implement a Hierarchical networking design for the main university campus and another one for the South campus.
- Connect the two campuses using Site-To-Site VPN to provide a secure connection between the two campuses.
- Implement a protection layer for the data center in the university using demilitarized zone (DMZ).
- Implement a Web Application Firewall to protect the web servers in the university from any attacks.

- Provide redundancy and load balancing for the network using various technologies like software-defined wide area network (SD-WAN) and link monitoring for Internet connectivity.
- Provide High Availability (HA) for FortiGate redundancy.
- Provide services like Web Filtering and Application Control to control the network traffic and prevent any unwanted traffic from entering the network.
- Use various Fortinet products like FortiSwitches, FortiAPs, FortiAnalyzer, and FortiManager to provide a complete solution for the university's network infrastructure.

1.4 Our solution

Figure 1.1: Fortinet Logo

Fortinet is a network security company, based in California, USA. It provides relatively cheap, modern, and easy-to-use and maintain products that can also easily provide a great level of network security through different measures. Fortinet relies heavily on the use of FortiGate devices, which are firewalls that can be used to secure the network, as well as managing any Fortinet device connected to it. Fortinet also provides other products like FortiSwitches, FortiAPs, FortiAnalyzer, and FortiManager to provide a complete solution for the network infrastructure [8]. We suggest converting to Fortinet products for its great security and ease of use and maintenance, as well as it being cheaper relative to Cisco and other competitors. [9] Our solution will include a full topology for the main university and the south campus, as well as the secure connection between them. It will also include many solutions that will provide redundancy and load balancing for the network. Our

solution will also include a protection layer for the data center in the university using DMZ, and a Web Application Firewall to protect the web servers in the university from any attack that may occur.

1.5 Key Technical Details

1.5.1 Network Topology

- Hierarchical design for main and south campuses.
- Core, distribution, and access layers.
- Layout of FortiGate firewalls, FortiSwitches, and FortiAPs.

1.5.2 FortiGate Firewalls

- Secure the network.
- Configure firewall rules, NAT, and security policies.
- High Availability (HA) for redundancy.

1.5.3 Site-to-Site VPN

- Secure connection between campuses.
- Encryption protocols and VPN policies.

1.5.4 Demilitarized Zone (DMZ)

- Protect the data center.
- Public services in the DMZ.
- Access control policies.

1.5.5 Web Application Firewall (WAF)

- Protect web servers from attacks.
- Configure WAF rules and profiles.

1.5.6 Software-Defined WAN (SD-WAN)

- Provide redundancy and optimize traffic.
- Link monitoring and failover.

1.5.7 Network Security Services

- **Web Filtering**: Block inappropriate/malicious websites.
- **Application Control**: Manage network applications.
- **Intrusion Prevention System (IPS)**: Detect and prevent intrusions.

1.5.8 Network Management and Monitoring

- FortiAnalyzer for logging and reporting.
- FortiManager for centralized management.
- Network monitoring tools.

1.5.9 Wireless Network

- FortiAPs for campus coverage.
- Configure SSIDs, security settings, and VLANs.

1.5.10 Load Balancing and Redundancy

- Load balancing for critical resources.
- Redundant links and devices for availability.

1.5.11 Network Access Control (NAC)

- Control device access to the network.
- Authentication and authorization policies.

1.5.12 Scalability and Future-proofing

- Future network expansion considerations.
- Flexible design for new technologies.

1.5.13 Example Configuration Details

FortiGate Firewall Configuration Example

```
config system interface
    edit "port1"
        set mode static
        set ip 192.168.1.1/24
    next
end


config firewall policy
    edit 1
        set srcintf "port1"
        set dstintf "port2"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "ALL"
        set logtraffic all
    next
```

```
end
```

Site-to-Site VPN Configuration Example

```
config vpn ipsec phase1-interface
    edit "VPN-to-SouthCampus"
        set interface "port1"
        set peertype any
        set net-device enable
        set proposal aes256-sha256
        set remote-gw 192.168.2.1
        set psksecret your_psk_secret
    next
end

config vpn ipsec phase2-interface
    edit "VPN-to-SouthCampus"
        set phase1name "VPN-to-SouthCampus"
        set proposal aes256-sha256
        set src-subnet 10.1.0.0 255.255.255.0
        set dst-subnet 10.2.0.0 255.255.255.0
    next
end
```

1.6 High-Level Design

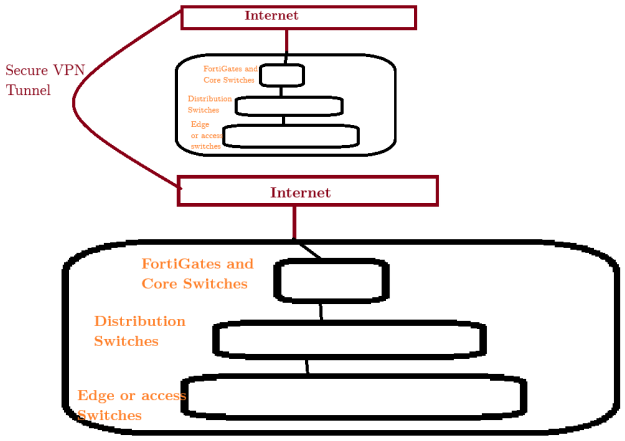


Figure 1.2: High Level Design

1.7 Report structure

The report is structured as follows:

- **Chapter 1: Introduction** - Provides an overview of the project, including the problem statement, aims and objectives, current solutions, our solution, key technical details, list of contributions, high-level design, and report structure.
- **Chapter 2: Background** - Provides background information on the project, including the current network infrastructure at Yarmouk University.
- **Chapter 3: Design** - Describes the design of the project, including the network topology, FortiGate firewalls, Site-to-Site VPN, DMZ, WAF, SD-WAN, network security services, network management and monitoring, wireless network, load balancing and redundancy, network access control, scalability and future-proofing, and example configuration details.
- **Chapter 4: Implementation** - Describes the implementation of the project, including the configuration of FortiGate firewalls, Site-to-Site VPN, DMZ, WAF, SD-WAN, network security services, network management and monitoring, wireless

network, load balancing and redundancy, network access control, and scalability and future-proofing.

- **Chapter 5: Results and Discussion** - Presents the results of the project and discusses the findings.
- **Chapter 6: Economical, Ethic, and Contemporary Issues** - Discusses the economical, ethical, and contemporary issues related to the project.
- **Chapter 7: Project Management** - Describes the project management process, including the project plan, timeline, and resources.
- **Chapter 8: Conclusion and Future Work** - Provides a conclusion to the project and suggests future work.
- **References** - Lists the references used in the report.
- **Appendices** - Includes any additional information related to the project, such as the user manual.

2. Background

2.1 Overview and context

Yarmouk University has outdated network infrastructure that struggles to serve the large student body and academic and technical staff over two large campuses. The network lacks redundancy and load balancing. The current network infrastructure is not suitable for the size and complexity of the university. In our modern interconnected world, a reliable and secure network is essential for the university to function effectively; a wide-spanning WiFi network is vital for students and staff to access the internet and university resources. Additionally, computer labs need a dependable backbone to function properly.

2.2 Target Market - Yarmouk University

Yarmouk University is a public university in Jordan, located in Irbid. It was established in 1976 and has grown to become one of the largest universities in Jordan. The university offers a wide range of undergraduate and postgraduate programs in various fields, including engineering, science, arts, and humanities. Yarmouk University has a large student body, with over 41,000 students enrolled in various programs. The university has multiple campuses, including the main campus and the south campus, which are located in different parts of Irbid. The university has a diverse student population, with students from different backgrounds and nationalities. The university is known for its high-quality education and research programs, and it has a strong reputation in the region. Yarmouk University is committed to providing its students with a supportive and inclusive learning environment, and it is constantly striving to improve its facilities and services to meet the needs of its students and staff. [7]

2.3 Potential Ethical and Environmental Issues

Yarmouk University use solar energy for its power needs, and the network infrastructure is not energy-intensive. The project will not have a significant environmental impact. The project will not have any ethical issues, as it aims to improve the network infrastructure for the benefit of the university community [10]. Figure 2.1 shows that Yarmouk University installed solar panels across the campus.

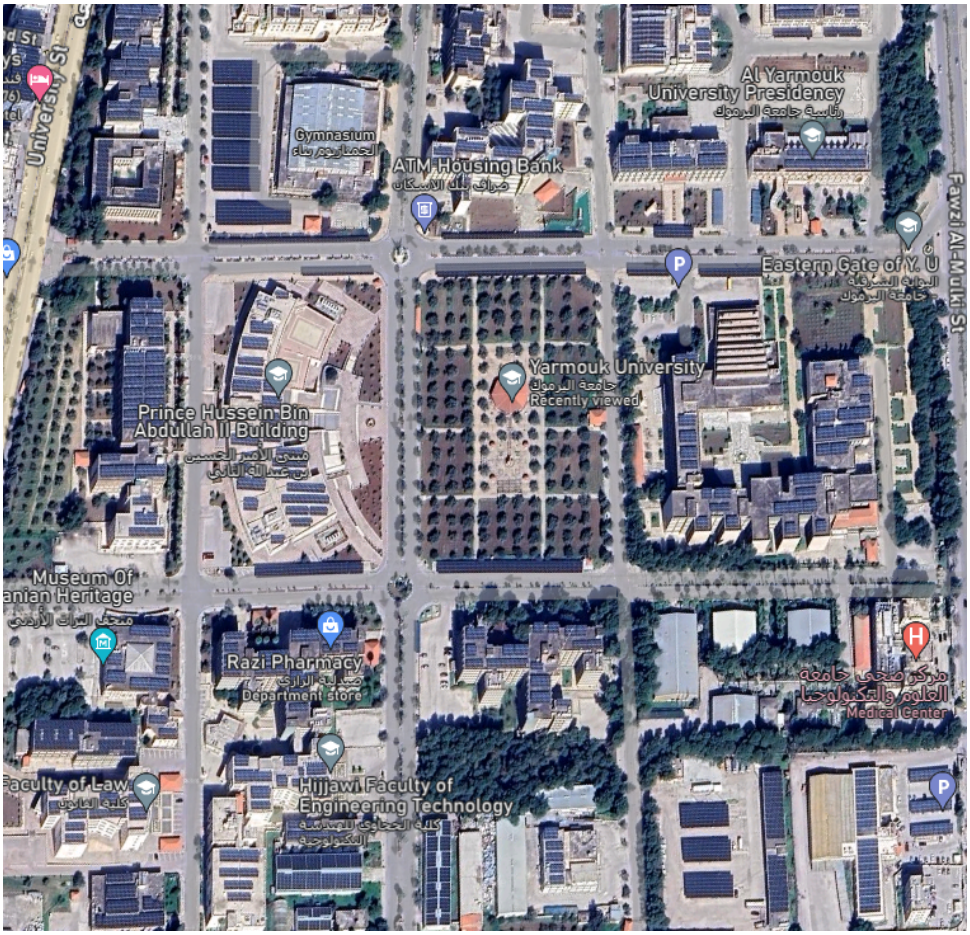


Figure 2.1: Solar Panels at Yarmouk University as seen on Google Maps

2.4 Other Approaches

Most organizations utilize CISCO systems since it was ubiquitous in the networking industry until mid 2010s. CISCO provided unmatched stability and consistency, but at the expense of cost and high level of expertise needed to setup and maintain, as it mainly relies on commands. CISCO's monopoly caused its innovation to stagnate, and prices to go up. They only offered basic systems, especially when it came to firewalls.[9] [11]

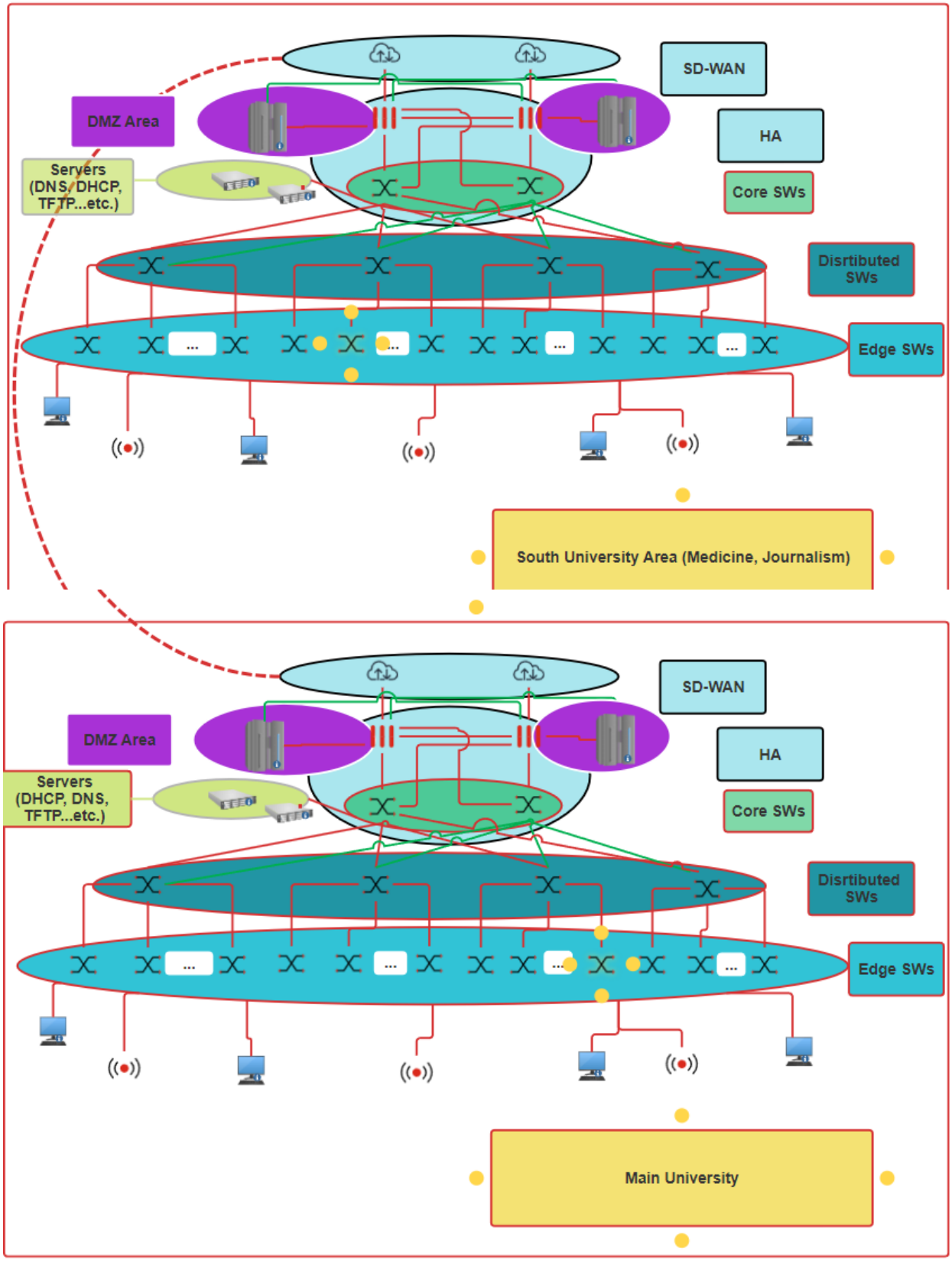
3. Design

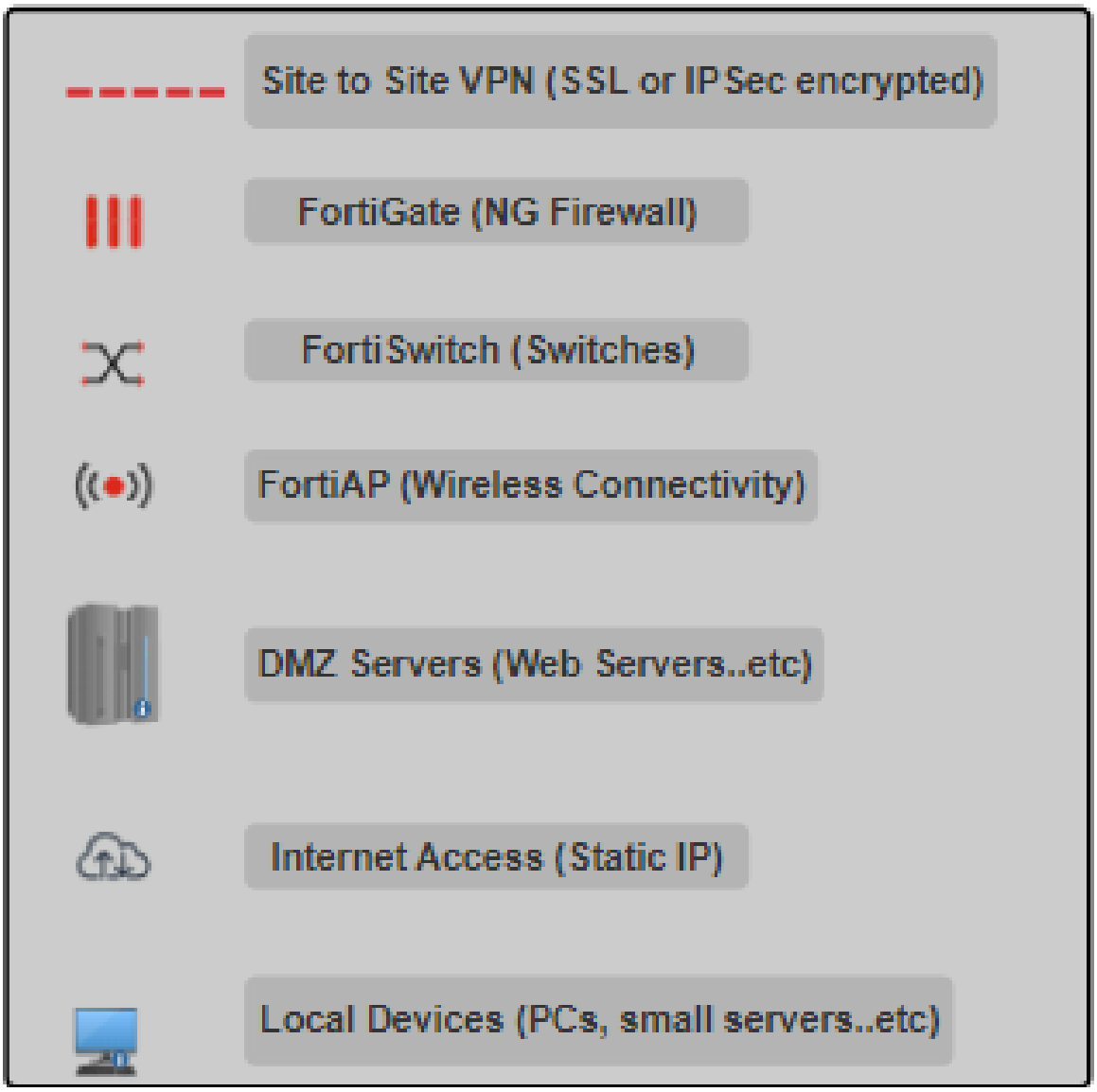
3.1 Design Overview

3.1.1 Design Description

The design of the project will focus on enhancing the network connectivity for Yarmouk University by using Fortinet products. The project will implement a Hierarchical networking design for the main university campus and another one for the South campus, and connect them using Site-To-Site VPN to provide a secure connection between the two buildings. The project will also include a protection layer for the data center in the university using DMZ where the DMZ will include web servers and any service that is ok to be public. The project will also implement a Web Application Firewall to protect the web servers in the university from any attacks. One of the main focuses of this project is to provide redundancy and load balancing for the network using various technologies like SD-WAN and link monitoring for Internet connectivity and High Availability (HA) for FortiGate redundancy. FortiGates will also provide services like Web Filtering and Application Control to control the network traffic and prevent any unwanted traffic from entering the network We will be using various Fortinet products like FortiSwitches, FortiAPs, FortiAnalyzer, and FortiManager to provide a complete solution for the university's network infrastructure.

3.1.2 Detailed figure


SD-WAN
DMZ Area
HA
Servers
(DNS, DHCP,
TFTP...etc.)
Core SWs
Disrtibuted
SWs
Edge SWs
South University Area (Medicine, Journalism)
SD-WAN
DMZ Area
HA
Servers
(DHCP, DNS,
TFTP...etc.)
Core SWs
Disrtibuted
SWs
Edge SWs
Main University


Site to Site VPN (SSL or IPSec encrypted)
FortiGate (NG Firewall)
FortiSwitch (Switches)
FortiAP (Wireless Connectivity)
DMZ Servers (Web Servers..etc)
Internet Access (Static IP)
Local Devices (PCs, small servers..etc)

3.2 Design Details

3.2.1 Design Specifications

This project requires:

1. Two server rooms (which may already exist), equipped with heavy-duty cooling, uninterruptible power supplies, and a backup generator.

2. A large number of Fortinet devices, including FortiGate firewalls, FortiSwitches, and FortiAPs (both indoor and outdoor for enhanced WiFi coverage).

3. Extra server racks for redundant devices.

4. A team of network engineers and security experts for regular maintenance and vulnerability testing of the network infrastructure.

5. At least two high-speed internet connections from different ISPs to minimize internet outage time.

6. Cabling: fiber connections for high-speed links between core devices (e.g., FortiGates to core FortiSwitches or servers) and CAT6A for inter-switch connectivity and access points. CAT6 cabling will be used for end-users and terminal devices.

3.3 Design Process

This project will include countless technologies that will enhance networking around Yarmouk University, many of which is provided by Fortinet.

3.3.1 Hierarchical Networking Design

The project will implement a Hierarchical networking design for the main university campus and another one for the South campus. The Hierarchical design will include Core, Distribution, and Access layers. The Core layer will be responsible for high-speed switching and routing between different parts of the network. The Distribution layer will be responsible for routing between different VLANs and providing access to the core layer. The Access layer will be responsible for connecting end-user devices to the network. The Hierarchical design will provide scalability, redundancy, and security for the network infrastructure. It will also allow for modularity as any future changes is easier to manage through the separation of the network into different layers.[12]

3.3.2 FortiGate, a Next-Generation Firewall

Firewall vs Router

In the past, the main device that allowed for inter-network and inter-VLAN routing was a router, a router would usually observe the destination IP of a packet, and based on a routing table, a router would decide where to send the packet. On-premise firewalls where introduced as a replacement for routers as they provide additional security features, such as what traffic to allow, what IPs or ports to block, posing limitations on end devices as to who they can communicate with and so on. Firewalls are usually used to protect the network from the outside world, while routers are used to connect different networks together. Firewalls started replacing routers especially since the internet expanded for more people, more hackers where found where they imposed new ways to access networks and devices that they should not be accessing. Table 3.1 shows the difference between routers and firewalls. [13]

Feature	Router	Firewall
Layer	3	4
Routing	Yes	Yes
Security	Limited features	Yes

Table 3.1: Router vs Firewall

Legacy vs Next-Generation Firewalls

Legacy firewalls are firewalls that operate at the network layer (Layer 4) of the OSI model and provide basic packet filtering based on source ports and IPs and stateful inspection, which tracks the packets state to determine if a suspicious activity such as a DOS attack is occurring or not. Next-Generation Firewalls (NGFWs) are firewalls that operate at the application layer (Layer 7) of the OSI model and provide advanced features like web filtering, which determines what website a certain user is blocked from visiting, intrusion prevention systems, which would block any suspicious activity that is trying to access any valuable devices, servers or data for stealing or damaging them, anti-malware, which detects any malware through behaviors and any signature that would point out that this packet is a malware, and managing external services, for example, forcing safe-search on google such that no inappropriate search results appear, and track what users do on the web. NGFWs are more advanced and provide better security than legacy firewalls. Table 3.2 shows the difference between legacy and next-generation firewalls. [14] Figures 3.1 and 3.2 show an example of both a legacy firewall from CISCO and a next-generation firewall from Fortinet.

Feature	Legacy Firewall	Next-Generation Firewall
Layer	4	7
Packet Filtering	Yes	Yes
Stateful Inspection	Yes	Yes
Application Awareness	No	Yes
Intrusion Prevention	No	Yes
Web Filtering	No	Yes
Anti-Malware	No	Yes
SSL Inspection	No	Yes

Table 3.2: Legacy vs Next-Generation Firewalls

Next-generation firewalls (NGFWs), particularly FortiGate devices, emphasize the im-

Figure 3.1: Legacy Firewall from CISCO [1]

Figure 3.2: Next-Generation Firewall from Fortinet [2]

portance of comprehensive policy management to enhance security. In FortiGate NGFWs, virtually all configurations, including routing and advanced security features, are implemented through security policies. This approach centralizes control, allowing administrators to define, enforce, and monitor rules within a single, cohesive framework. By managing routing within policies, FortiGate ensures that traffic is scrutinized and controlled based on security parameters before it is allowed to proceed, reducing the risk of unauthorized access and potential breaches. This method of embedding most functionalities within a policy framework enhances security by maintaining consistent and granular control over network traffic, ensuring that all actions align with the organization's secu-

rity posture and compliance requirements [15]. Figure 3.3 shows an example of FortiGate Policy Management page on the FortiOS configuration page.

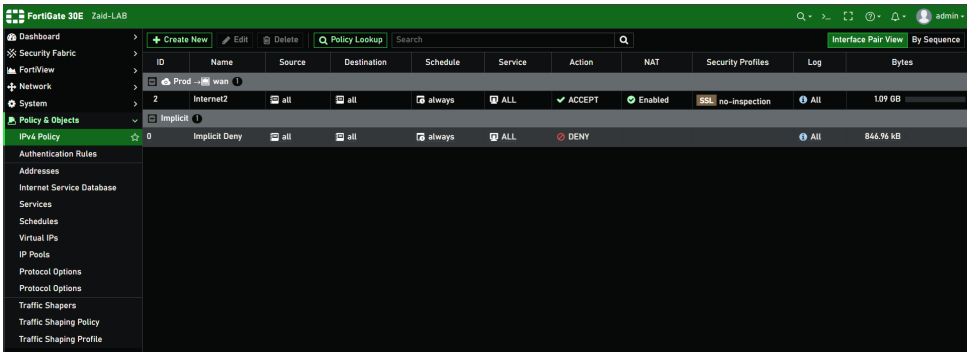


Figure 3.3: FortiGate Policy Management

3.3.3 Switches

Switches are devices that connect devices together in a network, they operate at either layer 2 or layer 3 of the OSI model, and they use MAC addresses to determine where to send packets. Layer 2 switches are used to connect devices together in a network, while Layer 3 can switch between different VLANs. Layer 3 switches can also perform routing functions, and they are used to connect different VLANs together. Switches are used to provide high-speed connectivity between devices in a network and to reduce network congestion. They are used to create a network that is fast, reliable, and secure. This project will utilize the use of layer 2 switching services as any routing must be done at the firewall to ensure security [16]. Figure 3.4 shows an example of a FortiSwitch device from Fortinet.

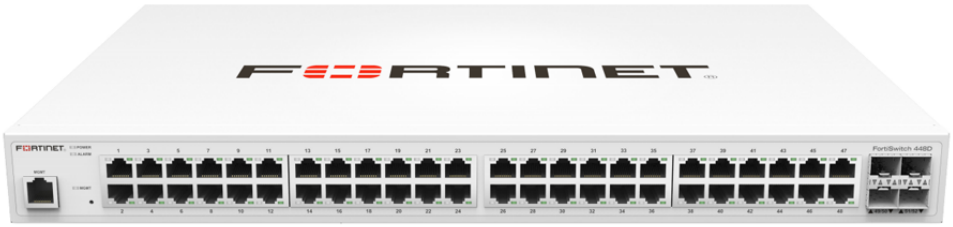


Figure 3.4: FortiSwitch from Fortinet [3]

3.3.4 VLANs

VLANs are Virtual Local Area Networks, they are used to separate different parts of a network into different segments, they are used to provide security, scalability, and flexibility to a network. VLANs are used to separate different departments in an organization, different floors in a building, or different parts of a campus. VLANs are used to reduce network congestion and improve network performance. VLANs are used to provide flexibility by allowing devices to be moved between different parts of a network without changing their IP addresses. This project will use VLANs to separate different parts of the network, however, VLAN managment is one of the main things that is discussed with the upper management like CEOs, presidents or who can represent them, since they are the ones who envision how the splitting should be. [17]

3.3.5 Wireless Access Points

Wireless Access Points (WAPs) are devices that allow devices to connect to a network wirelessly. They are used to provide WiFi coverage in a network. WAPs are used to provide wireless connectivity to devices that do not have a wired connection, such as mobile phones. WAPs are used to provide mobility to users by allowing them to connect to the network from anywhere in the coverage area. WAPs can be used indoors or outdoors, depending on the coverage area required. Indoor WAPs are used to provide WiFi coverage inside buildings, while outdoor WAPs are used to provide WiFi coverage outside buildings. This project heavily aims to improve WiFi quality thus will use both indoor and outdoor WAPs to provide WiFi coverage to the main university campus and the South campus [18]. Figure 3.5 shows an example of a FortiAP device from Fortinet.

3.3.6 NATting

Network Address Translation (NAT) is a process that allows devices on a private network to communicate with devices on a public network. NAT is used to translate the private IP addresses of devices on a private network to a public IP. NAT is used to conserve public IP addresses by allowing multiple devices on a private network to share a

Figure 3.5: FortiAP from Fortinet [4]

single public IP address. NAT is used to provide security by hiding the internal network structure from the outside world. There are three types of NAT: Static NAT, Dynamic NAT, and Port Address Translation (PAT). Static NAT maps a private IP address to a public IP address on a one-to-one basis. Dynamic NAT maps a private IP address to a public IP address from a pool of public IP addresses. PAT maps multiple private IP addresses to a single public IP address utilizing different port numbers. This project will use PAT to allow devices on the private network to communicate with the public network [19]. Figure 3.6 shows an example of NAT configuration on a FortiGate device.

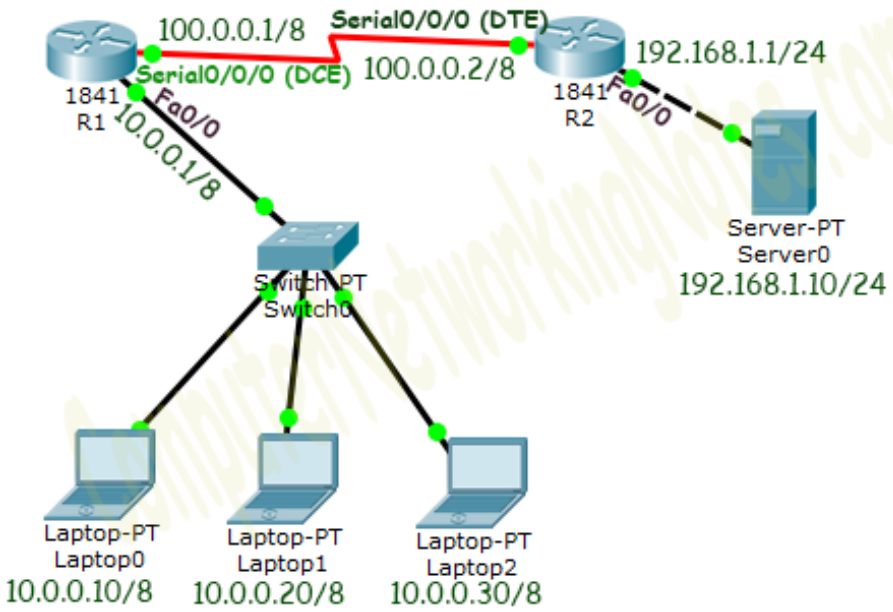


Figure 3.6: FortiGate NAT Configuration [5]

3.3.7 SD-WAN & Link Monitoring

The project will use Software-Defined Wide Area Network (SD-WAN) technology to provide redundancy and load balancing for the network. SD-WAN technology allows for the dynamic routing of traffic over multiple links based on the quality of the link and the traffic type. This will ensure that critical traffic is always routed over the best link and that the network is always available. SD-WAN technology will also allow for link monitoring and failover, so that if one link fails, traffic is automatically rerouted over another link. This will provide a high level of availability for the network and ensure that users always have access to the resources they need. SD-WAN is mainly used when connecting to the internet, so what sites usually do is to subscribe to more than one ISP, for example, a company would subscribe to both Zain and Umniah, and apply SD-WAN in a way that allows for a device in the network to connect to the outside world through Zain, and another device to be connected through Umniah, thus load balancing session-wise is applied. [20] Link monitoring is a feature that allows the network administrator to monitor the quality of the links in the network. Link monitoring can be used to monitor the latency, packet loss, and jitter of the links. This information can be used to determine the best link for routing traffic and to ensure that the network is always available. Link

monitoring can also be used to detect link failures and automatically reroute traffic over another link. This will provide a high level of availability for the network and ensure that users always have access to the resources they need. Link monitoring is used in conjunction with SD-WAN technology to provide redundancy and load balancing for the network. [21]

3.3.8 High Availability (HA)

High Availability (HA) is a feature that allows the network administrator to ensure that the network is always available. HA can be used to provide redundancy for critical devices in the network, such as firewalls and switches. HA can be used to ensure that if one device fails, another device takes over automatically. This will provide a high level of availability for the network and ensure that users always have access to the resources they need. HA can also be used to provide load balancing for the network, so that traffic is distributed evenly across multiple devices. This will ensure that the network is always available and that users always have access to the resources they need. HA is used in conjunction with SD-WAN technology to provide redundancy and load balancing for the network. Figure 3.7 shows an example of HA configuration on a FortiGate device.

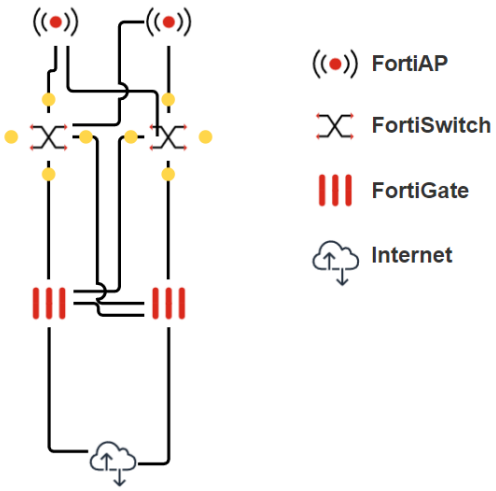


Figure 3.7: FortiGate HA Configuration

As the above topology shows, a link between the 2 HA devices known as the heartbeat is required to ensure that the slave knows when to takeover when the master fails. Devices in HA mode ping each other in regular intervals and wait for a response from the other device. If the other device replies, things proceed as is, if there is no reply to the ping, another ping is sent to check if the device really failed or not, if still there is no reply, and the slave is being problematic, the master just operates normally and warns the administration that slave might have failed, if the master is the one that is not responding, slave takes over, advertises itself as the gateway to the switches until the issue is fixed, then the master will take over again and advertise itself as the gateway. It is recommended to have a redundant heartbeat, in an active-passive mode; if we had only 1 link and it failed, the slave will assume that the master failed, advertising itself as the gateway, meaning that 2 FortiGates assume that they are the the active gateway, causing confusion for the core switches and thus the site goes down. This project will utilize HA for the FortiGates in an active-passive mode, as this will increase the life-span of the overall topology, lowering costs in the long run, and minimizing down-time. [22] [23]

3.3.9 DMZ

A Demilitarized Zone (DMZ) is a network segment that is used to provide a layer of security between the internal network and the external network. The DMZ is used to host public-facing services, such as web servers and email servers. Any storage servers is located in the internal network and is accessed through the DMZ. The DMZ is isolated from the internal network and the external network, and traffic is only allowed to flow between the DMZ and the internal network through specific security policies. The DMZ is used to protect the internal network from attacks that originate from the external network. The DMZ is also used to provide a layer of security for public-facing services, so that if an attacker compromises a public-facing service, they cannot gain access to the internal network. When an external traffic enters the FortiGate, it is routed immediately to the service it needs in the DMZ, and any access needed to the storage servers or a device inside the network is done by the servers themselves requesting access to the

required device in the network, ensuring that only the permitted requests are allowed, thus protecting any sensitive data or device that shouldnt be accessed or have limited access. This process is also known as port fowarding, since the request by the DMZ servers to access the internal network uses different port number from that of the request done by the user using the web servers from outside (he would usually access the web server with number 80 for HTTP or 443 for HTTPS). This project will implement a DMZ for parts of the data center in the university, where the DMZ will host web servers and any other public-facing services. [24]

3.3.10 Site-to-Site VPN

A Site-to-Site Virtual Private Network (VPN) is a method used to connect two or more networks over the internet securely. It allows different locations of an organization to communicate with each other as if they were on the same local network, ensuring data integrity and confidentiality over the public internet. In a network, a Site-to-Site VPN is typically used to connect branch offices to a central office, creating a cohesive internal network. This setup is essential for organizations with multiple geographic locations, enabling secure and efficient communication between sites. For instance, a company with a head office and remote branch offices can use a Site-to-Site VPN to connect all locations into a single network, ensuring seamless access to shared resources. A Site-to-Site VPN establishes a secure and encrypted connection between VPN gateways at each site. The process involves the following steps [25]:

- Encryption: Data is encrypted before it is transmitted over the internet to ensure confidentiality.
- Tunneling: Data packets are encapsulated within another packet to create a secure tunnel between the sites.
- Authentication: Both endpoints authenticate each other to establish a trusted connection.

- Decryption: Once the data reaches the destination, it is decrypted for use within the local network.

The VPN gateway at each site handles the encryption, tunneling, and decryption processes, ensuring secure communication between the networks. There are two primary types of VPN protocols used in Site-to-Site VPNs: SSL VPN and IPsec VPN. SSL VPN operates at the application layer, using SSL/TLS for encryption and authentication, while IPsec VPN operates at the network layer, using the IPsec protocol suite for security features. Table 3.3 provides a comparison of SSL VPN and IPsec VPN [26] [27] For our

Feature	**SSL VPN**	**IPsec VPN**
Layer of Operation	Application Layer	Network Layer
Security	Uses SSL/TLS for encryption and authentication	Uses IPsec protocol suite for encryption, integrity, and authentication
Setup Complexity	Easier to set up, often requires just a web browser	More complex, requires configuration on both client and server
Performance	Generally slower due to higher overheads	Typically faster due to lower overheads
Usage Scenarios	Remote access for individual users	Site-to-Site connections and remote access
Firewall Traversal	Better at traversing firewalls and NAT	May have issues with firewalls and NAT

Table 3.3: Comparison of SSL VPN and IPsec VPN

project, which involves connecting the main campus and the south campus, IPsec is the preferred choice due to several reasons:

- Security: IPsec provides robust security features, including strong encryption and comprehensive authentication mechanisms.

- Performance: IPsec typically offers better performance and lower latency, which is crucial for maintaining efficient communication between campuses.

- Compatibility: IPsec is widely supported across various devices and platforms, ensuring seamless integration with existing network infrastructure.

The primary purpose of using IPsec in this project is to establish a secure, reliable, and high-performance connection between the main campus and the south campus. This connection will enable both campuses to share resources, access centralized services, and communicate effectively, thereby enhancing the overall operational efficiency of the organization.

3.3.11 VRRP in Core Switches

Virtual Router Redundancy Protocol (VRRP) is a network protocol that provides high availability for core switches on a LAN. VRRP allows multiple switches to work together as a single virtual router, providing redundancy and failover in case one switch fails. VRRP works by electing a master switch that handles all traffic, while the other routers act as backups. If the master switch fails, one of the backup switches takes over as the master, ensuring continuous network operation. VRRP is commonly used in core switches to provide redundancy and failover in case of failure of one of the switches. In this project, VRRP will be used in the core switches to provide redundancy for the network. Half of the VLANs will be VRRP'd to one of the core switches, and the other half will be VRRP'd to the other core switch. This will ensure loadbalancing and parallelism. If one core switch fails, the other core switch can take over and handle the traffic for all VLANs. This will provide a high level of availability for the network and ensure that users always have access to the resources they need. [28]

3.3.12 Internal Servers

DNS

Domain Name System (DNS) is a hierarchical decentralized naming system for computers, services, or any resource connected to the internet or a private network. It translates domain names into IP addresses, which are required for locating and identifying computer services and devices with the underlying network protocols. DNS is used to map human-readable domain names to IP addresses, allowing users to access websites, send emails, and connect to other network resources using easy-to-remember names. DNS

servers store and manage domain name records, including IP addresses, aliases, and other information necessary for routing network traffic. In this project, internal DNS servers will be deployed to resolve domain names within the university's network, ensuring seamless communication between devices and services. The DNS servers will be configured to handle internal domain names and provide name resolution for local resources, enhancing network connectivity and accessibility. [29] Figure 3.8 shows an example of DNS configuration on a FortiGate device.

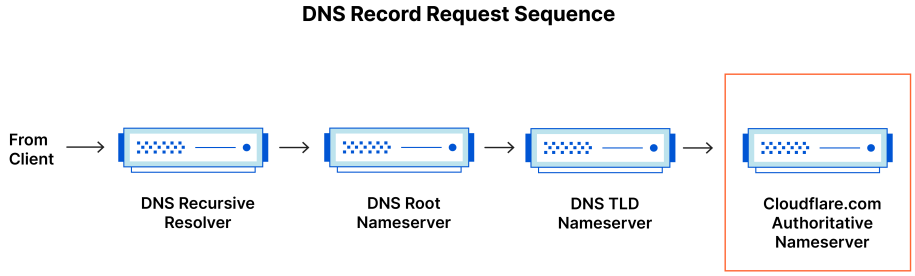


Figure 3.8: FortiGate DNS Configuration [6]

DHCP

Dynamic Host Configuration Protocol (DHCP) is a network management protocol used to automatically assign IP addresses and other network configuration parameters to devices on a network. DHCP eliminates the need for manual IP address configuration, making it easier to manage and scale large networks. DHCP servers dynamically allocate IP addresses from a predefined range, along with subnet masks, default gateways, and other network settings, to devices that request network connectivity. DHCP simplifies network administration by centralizing IP address management and ensuring efficient resource utilization. In this project, internal DHCP servers will be deployed to automate the assignment of IP addresses to devices within the university's network, streamlining network configuration and ensuring seamless connectivity for users and devices. The DHCP servers will be configured to provide IP addresses, subnet masks, and other network parameters to devices, enabling plug-and-play connectivity and efficient network

resource allocation. [30]

TFTP Servers

Trivial File Transfer Protocol (TFTP) is a simple file transfer protocol that allows devices to transfer files over a network. TFTP is commonly used for transferring configuration files, firmware updates, and other small files between devices. TFTP servers store files that can be accessed and downloaded by devices on the network. In this project, TFTP servers will be deployed to store configuration files and backups for network devices. The TFTP servers will provide a centralized repository for storing device configurations, enabling network administrators to perform automated, timely backups, updates, and restores as needed. By using TFTP servers, the project will ensure efficient management of network configurations and enhance network reliability and security. [31]

Storage

Storage servers are used to store data and files for users and applications within the network. Storage servers provide centralized storage resources that can be accessed by multiple devices and users. In this project, storage servers will be deployed to store user data, application files, and other critical information within the university's network. The storage servers will be configured to provide secure, reliable, and scalable storage solutions, ensuring data availability, integrity, and accessibility for users and applications. By using storage servers, the project will enhance data management, collaboration, and productivity within the university's network.

3.3.13 Fortinet services

Fortilink

FortiLink is a technology developed by Fortinet that enables the integration and management of FortiSwitches and FortiAPs within a FortiGate. FortiLink allows network administrators to configure, monitor, and manage FortiSwitches directly from the FortiGate interface, providing centralized control and visibility over the entire network

infrastructure, it also deploys any VLAN created to the switches automatically, emaking configuration easier and take less time. FortiLink simplifies network deployment and management by streamlining switch configuration, monitoring, and troubleshooting processes. In this project, FortiLink will be used to integrate FortiSwitches and FortiAPs with FortiGate firewalls, enabling seamless communication and coordination between network devices. FortiLink will provide a unified management interface for configuring and monitoring switches, enhancing network visibility, control, and security. [32]

Web Filter & DNS Filter

Web filtering is a security feature that allows network administrators to control and monitor user access to websites and online content. Web filters can block or allow specific websites, categories of websites, or types of content based on predefined policies and rules. DNS filtering is a security feature that blocks access to malicious or inappropriate websites by filtering DNS requests and responses. DNS filters can prevent users from accessing known malicious domains, phishing sites, or inappropriate content by redirecting or blocking DNS queries. In this project, web filtering and DNS filtering will be implemented to enhance network security and control user access to the internet. The web filter and DNS filter will be configured to block malicious websites, inappropriate content, and other security threats, ensuring a safe and secure browsing experience for users within the university's network. [33] [34]

Application Control

Application control is a security feature that allows network administrators to monitor and control the use of applications and services within the network. Application control can block or allow specific applications, protocols, or services based on predefined policies and rules. Application control provides visibility into network traffic, identifies unauthorized applications, and enforces security policies to prevent data breaches and security incidents. In this project, application control will be implemented to monitor and control the use of applications and services within the university's network. The

application control feature will be configured to block unauthorized applications, restrict access to high-risk services, and enforce security policies to protect network resources and data. By using application control, the project will enhance network security, compliance, and performance, ensuring a safe and productive network environment. [35]

Intrusion Prevention System (IPS)

Intrusion Prevention System (IPS) is a security feature that monitors network traffic for malicious activities, vulnerabilities, and security threats. IPS inspects packets, identifies suspicious behavior, and blocks or alerts on potential threats to prevent unauthorized access, data breaches, and cyber attacks. IPS uses signature-based detection, anomaly-based detection, and other advanced techniques to analyze network traffic and detect security incidents in real-time. In this project, IPS will be implemented to protect the university's network from cyber threats, malware, and other security risks. The IPS feature will be configured to monitor and block malicious traffic, detect and prevent security breaches, and ensure the integrity and availability of network resources. By using IPS, the project will enhance network security, compliance, and resilience, safeguarding critical assets and data from cyber threats. [36]

Antivirus

Antivirus is a security feature that detects, blocks, and removes malware, viruses, and other malicious software from devices and networks. Antivirus software scans files, applications, and network traffic for known malware signatures, suspicious behavior, and security threats to prevent infections and data breaches. Antivirus uses signature-based detection, heuristic analysis, and other methods to identify and eliminate malware from systems and networks. In this project, antivirus will be implemented to protect the university's network from malware, viruses, and other cyber threats. The antivirus feature will be configured to scan and block malicious files, applications, and network traffic, ensuring the security and integrity of network resources. By using antivirus, the project will enhance network security, protect against cyber threats, and maintain the confidentiality

and availability of data within the network. [37]

SSL Inspection

SSL inspection is a security feature that decrypts and inspects encrypted SSL/TLS traffic to detect and prevent security threats, malware, and data leaks. SSL inspection intercepts SSL/TLS connections, decrypts the traffic, and scans the content for malicious activity, vulnerabilities, and security risks. SSL inspection uses SSL certificates, key pairs, and other cryptographic mechanisms to decrypt and analyze encrypted traffic without compromising security or privacy. In this project, SSL inspection will be implemented to protect the university's network from encrypted threats, malware, and data breaches. The SSL inspection feature will be configured to decrypt and inspect SSL/TLS traffic, detect and block malicious content, and ensure the security and compliance of network communications. By using SSL inspection, the project will enhance network security, visibility, and control, safeguarding sensitive data and resources from cyber threats. [38]

Traffic Shaping

Traffic shaping (also called Quality of Service in CISCO) is a feature that allows the network administrator to control the flow of traffic in the network. Traffic shaping can be used to prioritize certain types of traffic over others and to limit the bandwidth of certain types of traffic. This can be used to ensure that critical traffic, such as voice and video traffic, always has enough bandwidth and that non-critical traffic, such as file downloads, does not consume all the available bandwidth. Traffic shaping can also be used to control the flow of traffic between different parts of the network and to ensure that the network is always available. Traffic Shaping can also limit internet speed for a certain user/VLAN, meaning that for example, you can limit any traffic for a certain source IP to get a max speed of 12Mbps. This project will use traffic shaping to allow for a smoother experience when connecting to the internet in the university, as well as give more bandwidth to the Computer Engineering department as we deserve it. There are two types of traffic shaping: Per-IP traffic shaping and Shared traffic shaping. Per-IP

traffic shaping limits the bandwidth for each individual IP address, while Shared traffic shaping limits the bandwidth for all IP addresses in a group. Per-IP traffic shaping is used to limit the bandwidth for specific users or devices, while Shared traffic shaping is used to limit the bandwidth for a group of users or devices. This project will use both types of traffic shaping to control the flow of traffic in the network and ensure that critical traffic always has enough bandwidth. [39] [40]

3.3.14 Exam Configuration

Fortinet devices features such as easy scripting, fortilink and being able to access all switches from one device could allow great ideas like this to be implemented.

3.3.15 Examination VLAN Implementation

The Examination VLAN is a critical component designed to enhance security and manageability during university exams. This VLAN segregates exam-related network traffic from the university's main network, ensuring a controlled environment for exam takers. Below are the key steps and configurations for setting up and managing the Examination VLAN.

- Define the VLAN ID unique to the Examination VLAN.
- Allocate a dedicated IP subnet (e.g., 172.16.0.0/16) to the VLAN to prevent IP address conflicts.
- Configure DHCP on FortiGate to dynamically assign IP addresses within this subnet to exam takers' devices, ensuring that each device gets a unique IP address.

Role-Based Access Control

- Implement FortiAuthenticator for centralized authentication management. It will handle different roles including students, invigilators, and administrative staff.
- Configure authentication policies to ensure users are granted access based on their roles:

  - Students can only access exam materials.
  - Invigilators can monitor exam sessions.
  - Teachers have permissions to manage and oversee the examination content.
  - Administrators manage the VLAN and network configurations.

Security Policies

- Use FortiGate firewalls to enforce strict access control policies that restrict internet access during exams.
- Set up application control policies to prevent access to non-exam related websites and services.

Monitoring and Reporting

- Deploy FortiAnalyzer for real-time monitoring and logging of network traffic within the Examination VLAN.
- Configure alerts for any suspicious activities that could indicate cheating or other security incidents.

Testing and Validation

- Conduct pre-exam tests to validate the functionality of the DHCP, role-based access controls, and internet restrictions.
- Perform failover tests to ensure the Examination VLAN remains operational even if primary systems fail.

This setup not only enhances the integrity and security of the examination process but also aligns with the university's commitment to providing a fair and technologically advanced assessment environment, especially after the new technologies involved in cheating in exams.

3.4 Legal Aspects

Fortinet products require licensing to enable certain features and services. The project will need to purchase the necessary licenses for the Fortinet devices to ensure that all security features, updates, and support services are available. The project will also need to comply with licensing agreements and terms of use for the Fortinet products to avoid any legal issues. The project will work with Fortinet representatives to ensure that all licensing requirements are met and that the network infrastructure is properly licensed and supported. This project will comply with all regulation and laws by the Jordanian government to ensure data security, privacy, and compliance with legal requirements. The project will also ensure that all network configurations and security policies adhere to industry best practices and standards to protect the university's network and data. The project will also follow Fortinet's guidelines and recommendations for configuring and managing Fortinet devices to ensure that the network infrastructure is secure, reliable, and efficient.

3.5 Design Constraints

Yarmouk University is usually tight on money, so this project will try to be as cost-effective as possible. The project will also try to minimize downtime during the implementation phase to avoid disrupting the university's operations. Different models of switches and APs will be used to ensure minimum budget needed, for example, no need for high end switches for all layers, access layer switches can be a lower model than that of the core switches, and no need for high-end outdoor APs in a small room or building. Distribution of APs need to be done in a way to ensure coverage in all areas of the university, but still consider using the least number of APs possible. [41]

3.6 Design Standards

The project will adhere to industry standards and best practices for network design and security. The project will follow IEEE 802 standards for networking, including Ether-

net, WiFi, and other protocols. The project will also follow ISO/IEC 27001 standards for information security management to ensure that the university's network infrastructure is secure and compliant with international security standards. The project will also follow Fortinet's best practices and guidelines for configuring and managing Fortinet devices to ensure that the network is secure, reliable, and efficient. The project will also follow ITIL best practices for network management and service delivery to ensure that the network infrastructure meets the university's requirements and objectives. The project will also follow local regulations and laws to ensure that the network infrastructure complies with legal requirements and data protection regulations. The project will also follow industry standards for network design, security, and management to ensure that the network infrastructure is robust, scalable, and secure. [42] [43] [44]

3.7 Design Alternatives

MPLS is a great solution for connecting multiple sites, but it is expensive and requires a high level of expertise to set up and maintain. Site-to-Site VPN is a more cost-effective solution that provides a secure connection between two sites over the internet. It is easier to set up and maintain and provides a good level of security for most applications. For this project, we chose to use Site-to-Site VPN to connect the main campus and the south campus, as it provides a good balance between cost, security, and ease of use.

3.8 Design Considerations Table

Design Consideration	**Project Application**	**Relevant Location in Report**
Performance	High	Ch4
Serviceability	Easy to service	Idr
Economic	Cost-effective	Ch6
Environmental	No significant impact	2.ethical

Table 3.4: Design Considerations

4. Implementation

4.1 Methods and Procedures

First thing, after topology gets approved and an accurate devices list required is obtained, the devices will be ordered and delivered to the university, along with the licenses required. The FortiGates will be installed and configured first, then switches are connected and each deivce and port will be named through the FortiGate, then the FortiAPs will be installed and configured.

4.1.1 FortiGate Configuration

The FortiGates will be configured to provide security, routing, and VPN services for the university's network. The FortiGates will be configured with the following features:

- Firewall policies to control traffic between different parts of the network.
- VPN configurations to connect the main campus and the south campus.
- NAT configurations to allow devices on the private network to access the internet.
- SD-WAN configurations to provide redundancy and load balancing for the network.
- HA configurations to provide high availability for the network.
- DMZ configurations to host public-facing services.
- SSL inspection configurations to decrypt and inspect encrypted traffic.
- Traffic shaping configurations to control the flow of traffic in the network.
- Web filtering, DNS filtering, application control, IPS, and antivirus configurations to protect the network from security threats.

FortiGate Configuration Steps

We will first view the ports on the Fortigate, then setup the ports that will connect to the internet and any other ports needed. Figure 4.1 and 4.2 show an example of port

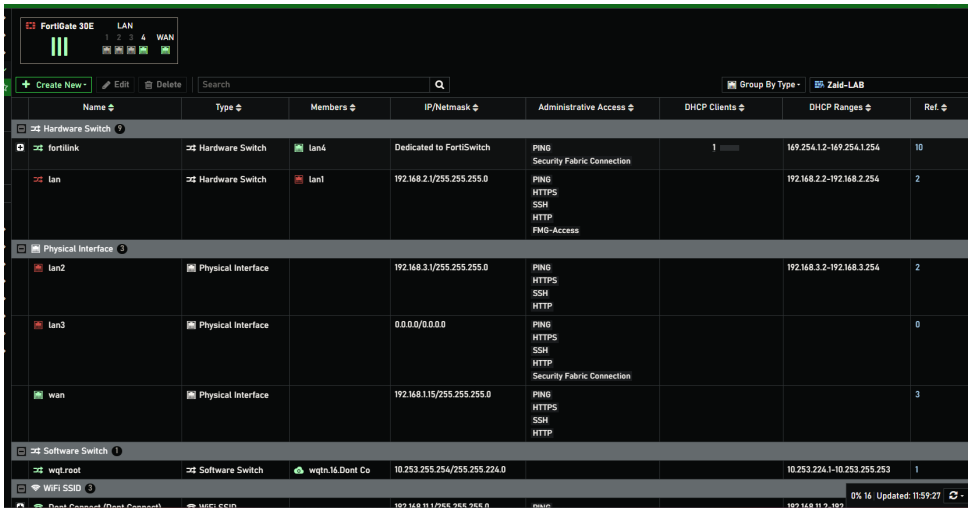


Figure 4.1: FortiGate Ports Page

configuration on a FortiGate device. As we can see in the images, we can see the ports on the FortiGate, and we can configure the ports to be used for different purposes, such as WAN, LAN, DMZ, etc, as seen in 4.3. We also need to configure the DNS for the FortiGate, as shown in Figure 4.4. Then we go to add the routes based on what we need, as shown in Figure 4.5. Then we configure the firewall policies, as shown in Figure 4.6. This figure shows a simple allow all IPs to go to the internet policy, but we can configure it to allow only certain IPs to go to the internet, or block certain IPs from going to the internet, or even block certain IPs from accessing the network, etc. When adding a policy, as shown in Figure 4.7, we need to specify the source and destination interfaces, the source and destination addresses, the services, and the action to be taken, and whether this port will deal with NATing or not. Now, we can test the connectivity from and to the FortiGate, and ensure it is connected to the internet. We can also test the firewall policies to ensure that traffic is being allowed or blocked as expected.

Next, we need to Application layer services (which require a license) such as Web Filtering, DNS Filtering, Application Control, IPS, and Antivirus. First, we start with Antivirus, as shown in Figure 4.8. We can configure the antivirus to what protocols to inspect, how should it handle mobile malware, and to determine which database to use for the antivirus detection. Next, we configure the Web Filtering, as shown in Figures 4.9, 4.10, & 4.11. We can configure the web filter to block certain categories of websites, or

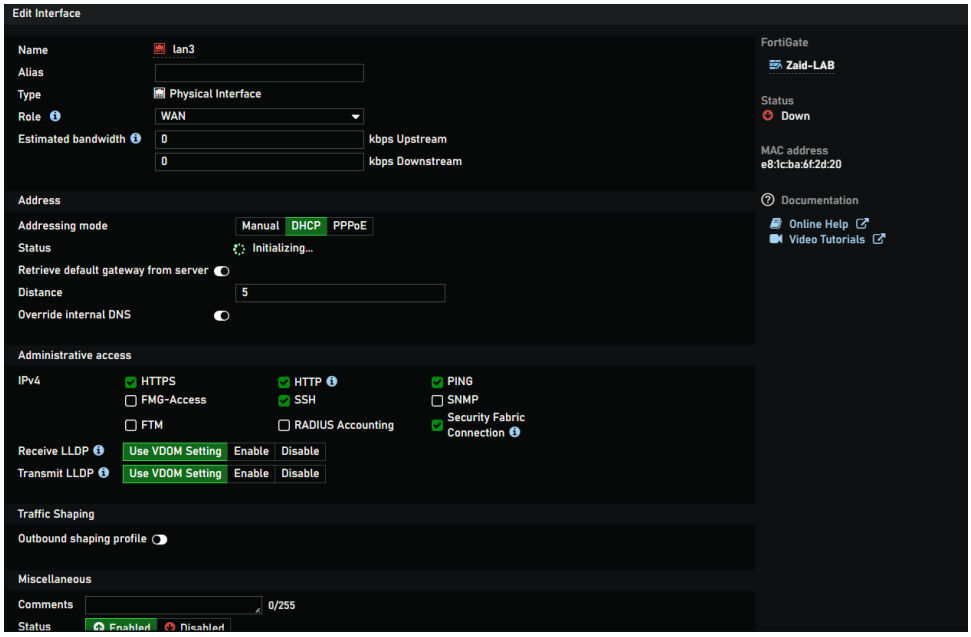


Figure 4.2: FortiGate Port Configuration

Figure 4.3: FortiGate Interface Role Configuration

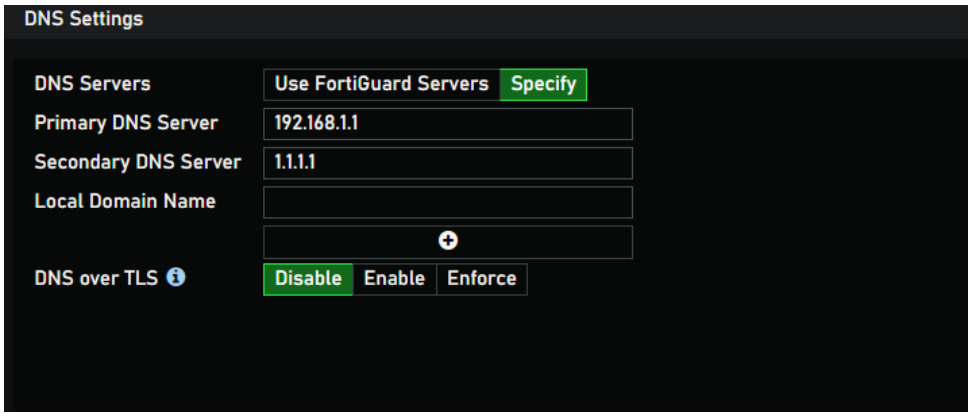


Figure 4.4: FortiGate DNS Configuration

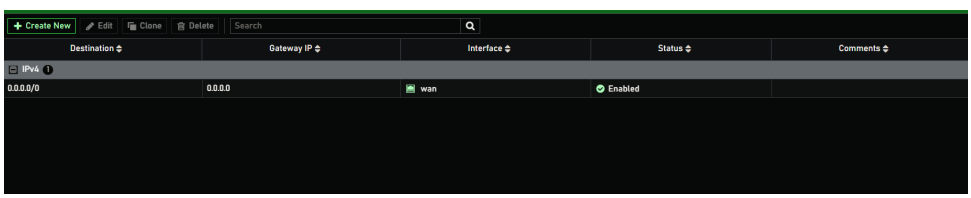


Figure 4.5: FortiGate Routes Configuration

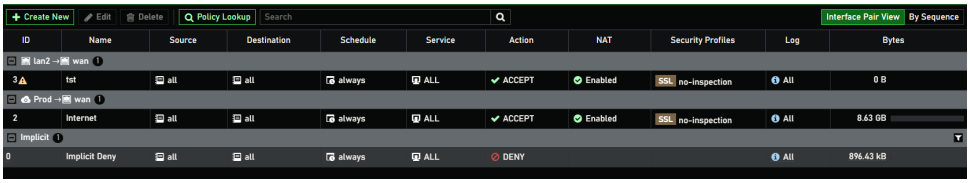


Figure 4.6: FortiGate IP Policy Configuration

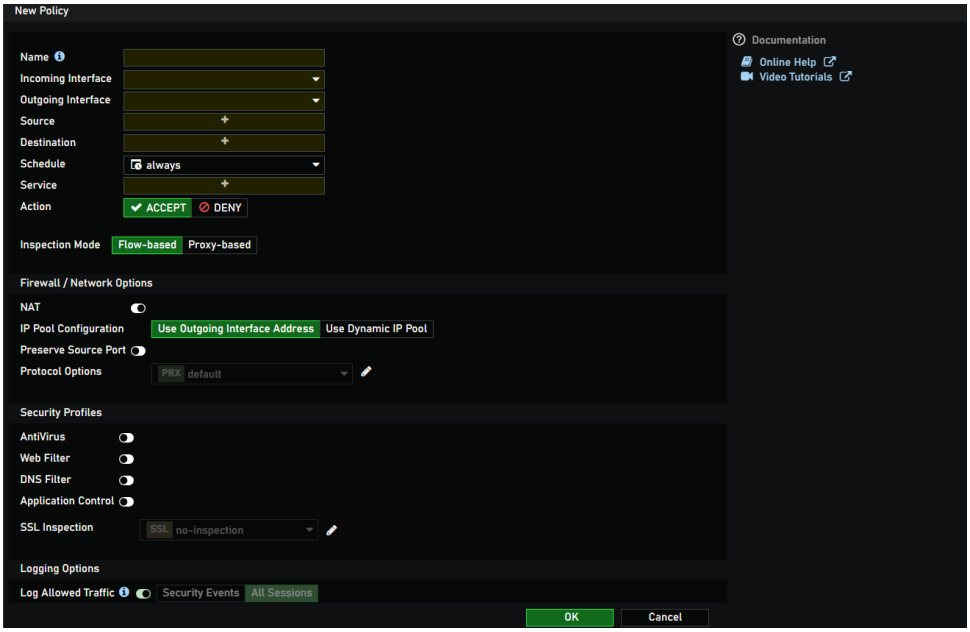


Figure 4.7: FortiGate IP Policy Configuration Options

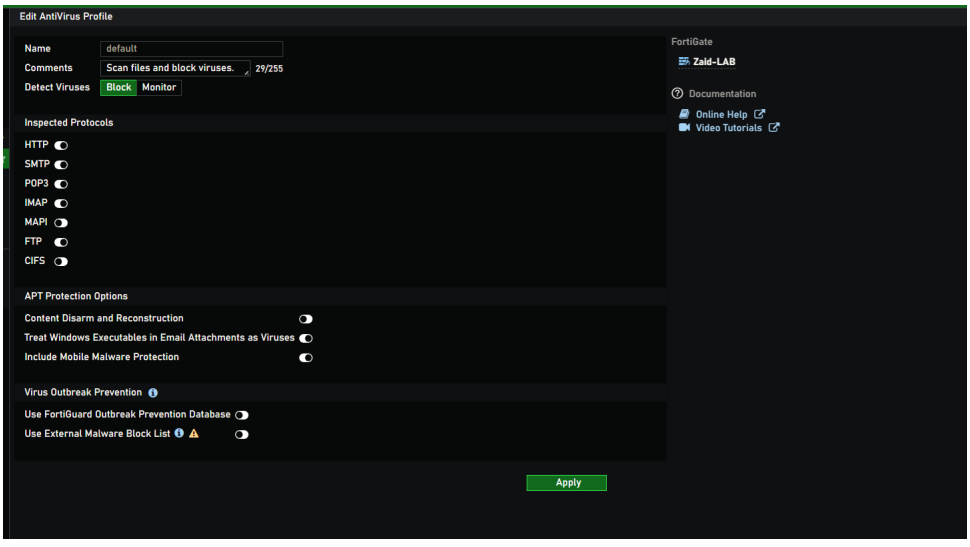


Figure 4.8: FortiGate Antivirus Configuration

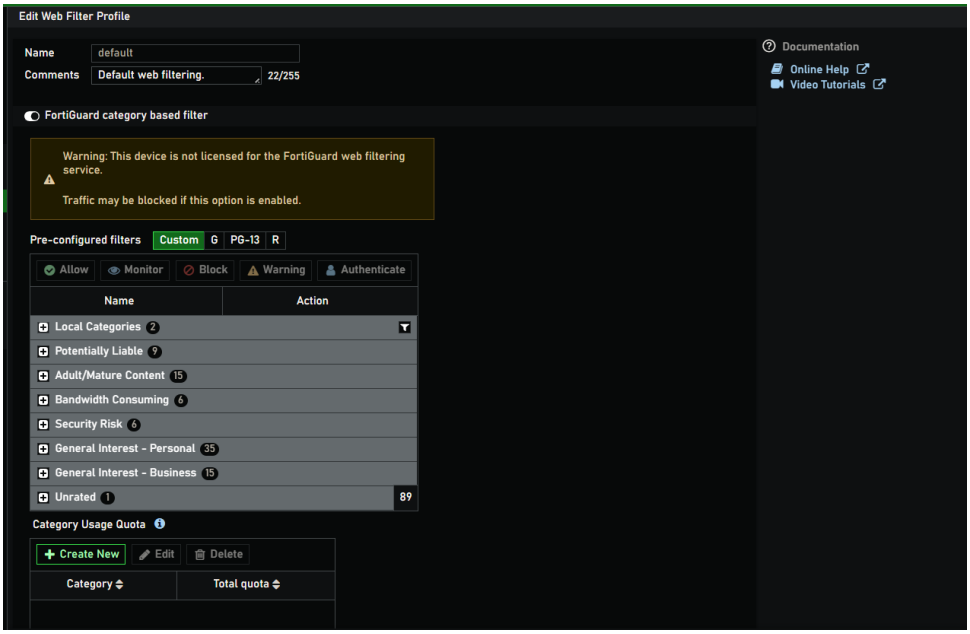


Figure 4.9: FortiGate Web Filtering Configuration

to allow only certain categories of websites, or to block certain websites, or to allow only certain websites, etc. We can also impose what limitations we want on a website, such as forcing safe search and limiting youtube access. We can also allow for logging all searches and websites visited by each user. Next, we configure the DNS Filtering, as shown in Figure 4.12. We can configure the DNS filter not only to block certain websites, but to redirect the user to a page that indicate that the website is blocked. We can also use dns filter to redirect the user from a website he wants to access to a more local or limited version of the website, in a university setting, we can redirect the user from youtube to the university's youtube channel, or from facebook to the university's facebook page, we can also redirect the user to a page that shows the university's rules and regulations, etc. DNS Filter could also be set to use the local IP address to access the website, wh9ich nwould increase dependency on the local network and reduce the load on the internet. Now, we configure the Application Control, as shown in Figure 4.13. We can configure the application control to block certain applications, or to allow only certain applications, or to mintor traffic related to certain applications. This can be catrgorized too like apps related to gaming, emails, cloud..etc. Now, we can set up the site to site VPN between campuses. We can do this by going to the VPN section in the FortiGate, and then to the IPsec VPN section, and then to the Create New section, as shown in Figure 4.14. We

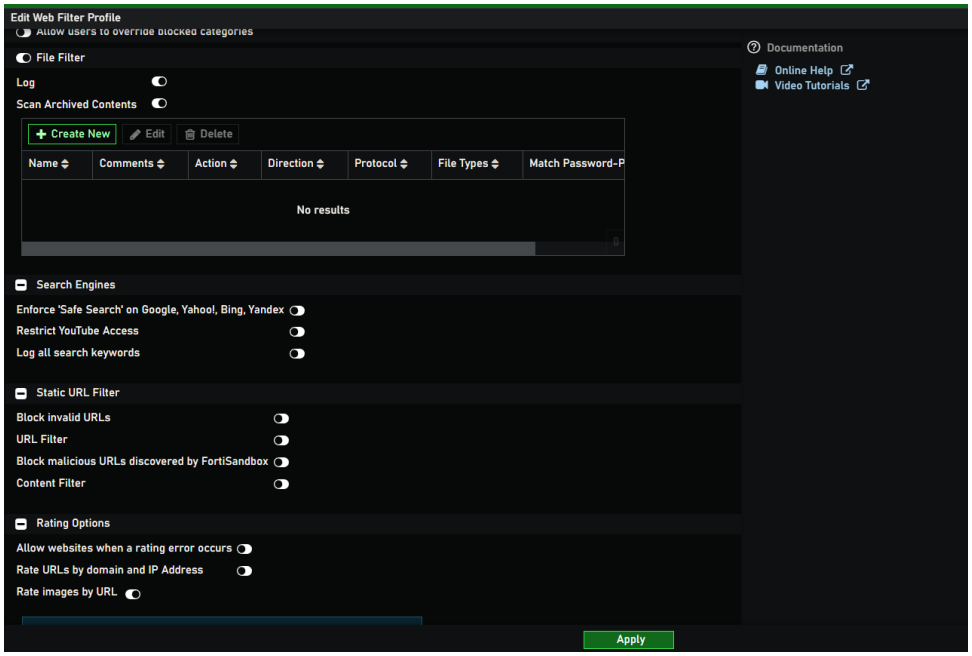


Figure 4.10: FortiGate Web Filtering Configuration

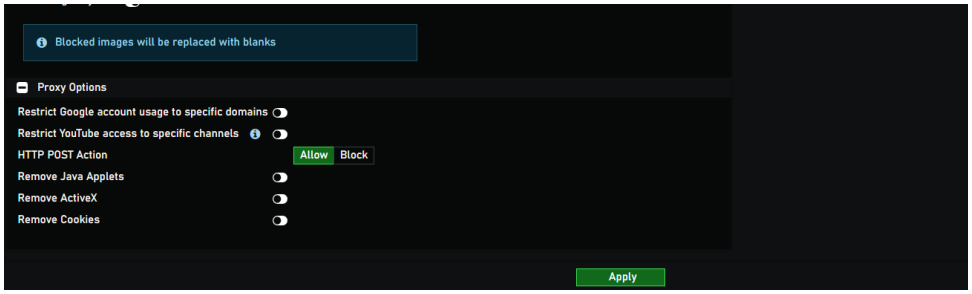


Figure 4.11: FortiGate Web Filtering Configuration

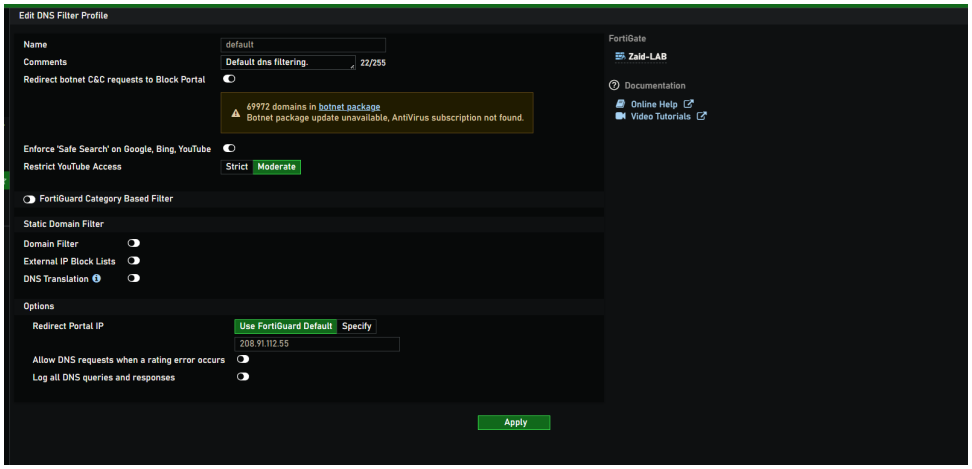


Figure 4.12: FortiGate DNS Filtering Configuration

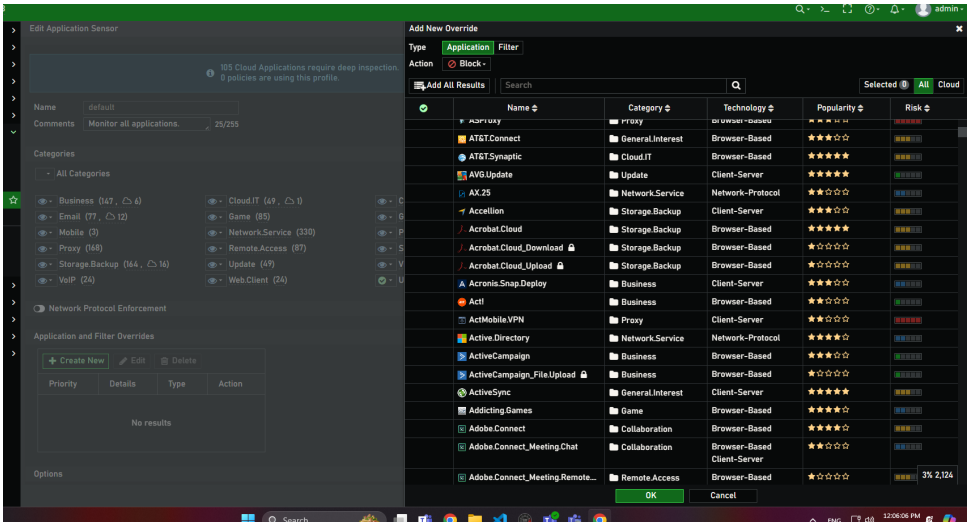


Figure 4.13: FortiGate Application Control Configuration

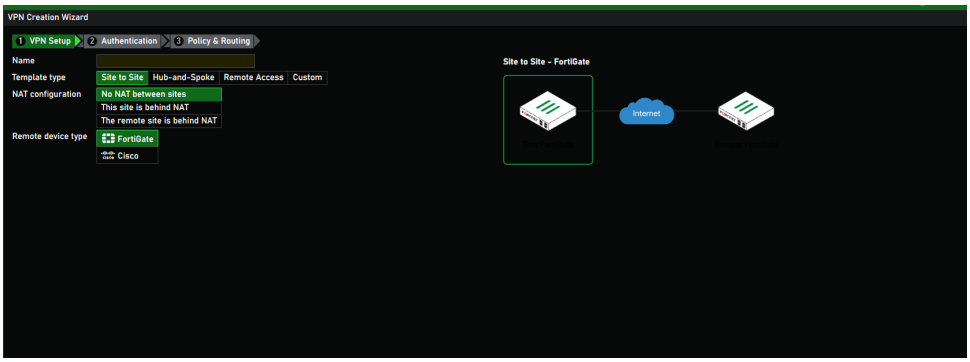


Figure 4.14: FortiGate VPN Setup

choose to where we are connecting (whether it is Fortinet device or CISCO), and whether there should be NATting between the sites or not. We then set the IPs and the PSKs for the connection as shown in Figure 4.15. Now we can start adding our switches and APs and view and access them through our FortiGate as shown in figures 4.16, 4.17, and 4.18. Topology can be seen in Figure 4.19. Now, we add the required VLANs to our setup as shown in Figure 4.20. We can add the VLANs and assign them to the required ports in fortiswitches, as shown in figure 4.21 and then we can configure the VLANs to have the required IP addresses and subnets. We also need to setup the APs. We first ensure that our APs are connected to the FortiGate, Then we set up the SSID as shown in Figure 4.22, and then we can configure the APs to have the required VLANs and IP addresses. We can set up SSIDs to be either tunnels or bridges,difference between them is shown in Table 4.1. Note: all ports carrying AP traffic should allow Security Fabric

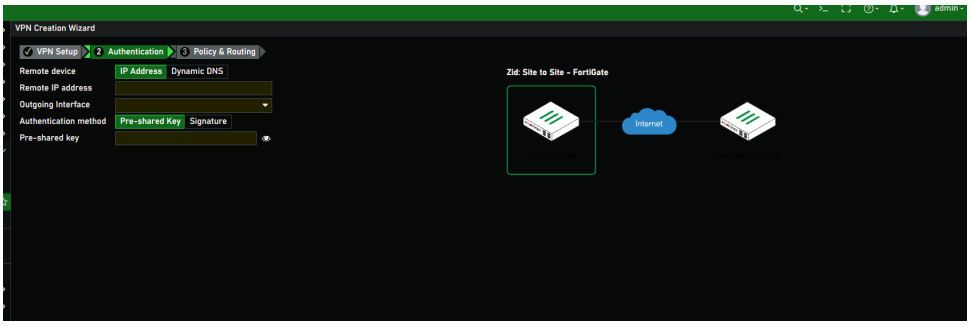


Figure 4.15: FortiGate VPN Setup

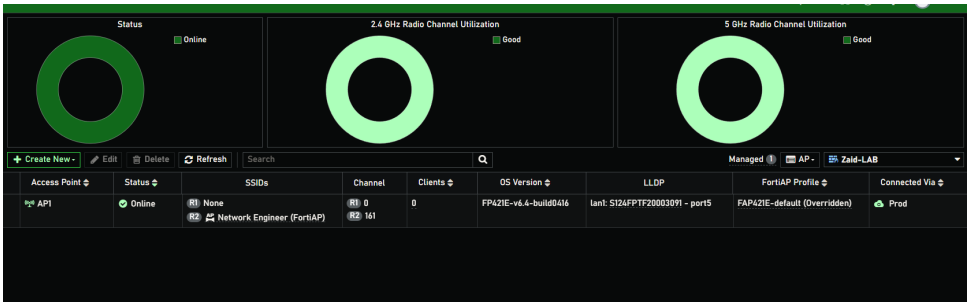


Figure 4.16: FortiGate Access Points

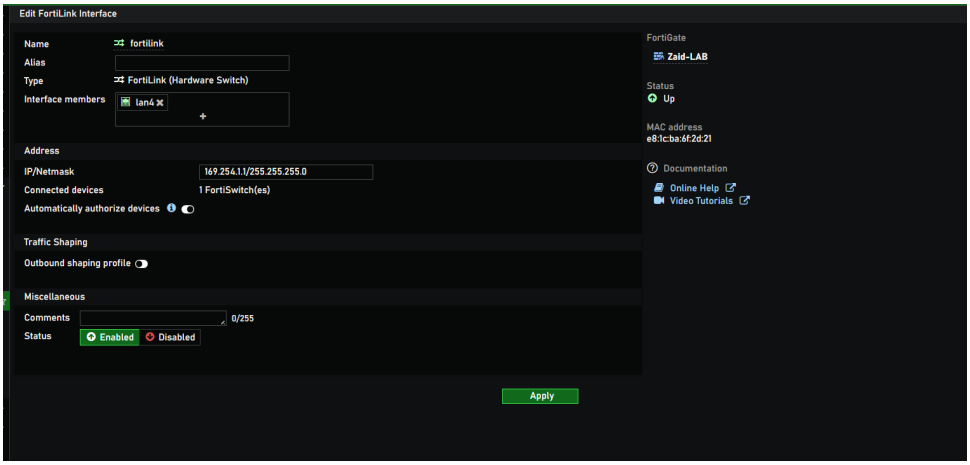


Figure 4.17: FortiGate FortiLink

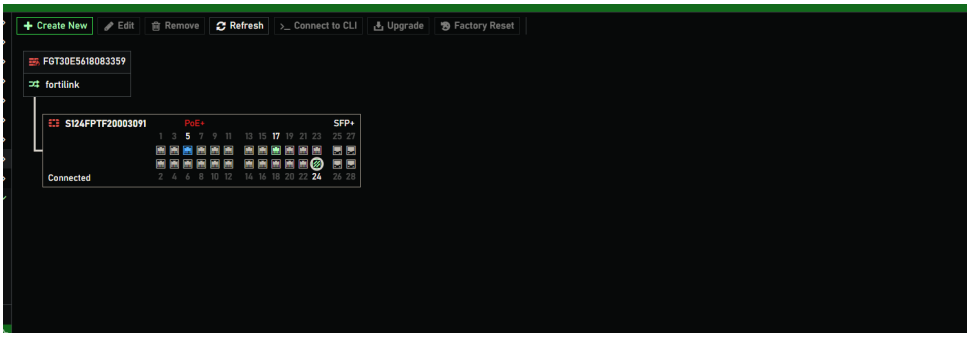


Figure 4.18: FortiGate FortiLink Ports

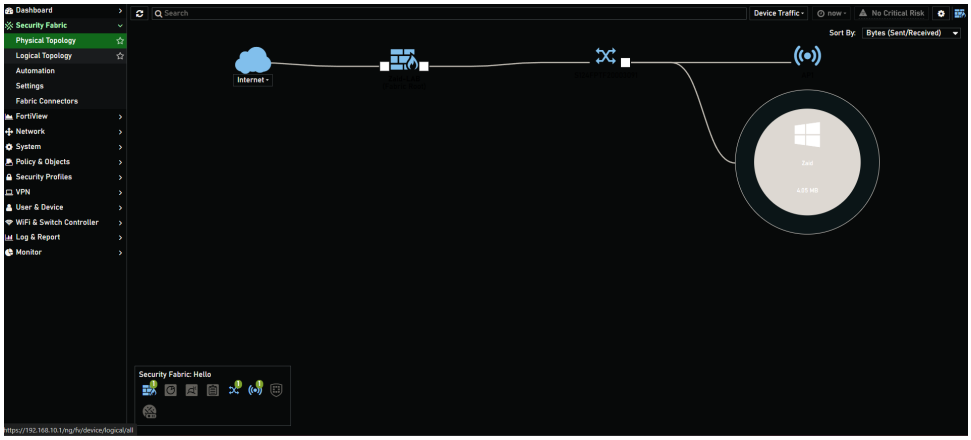


Figure 4.19: FortiGate Topology

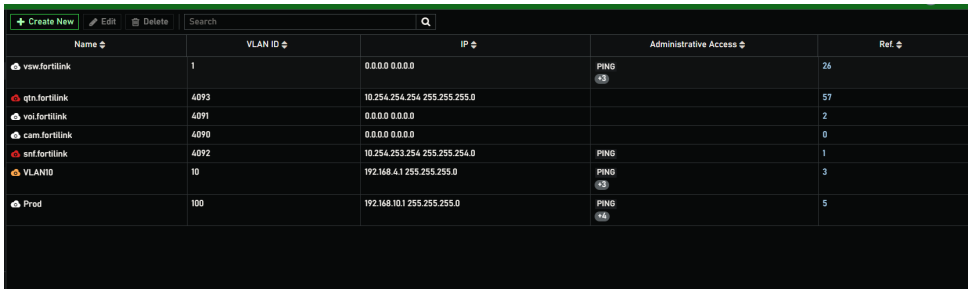


Figure 4.20: FortiGate VLANs

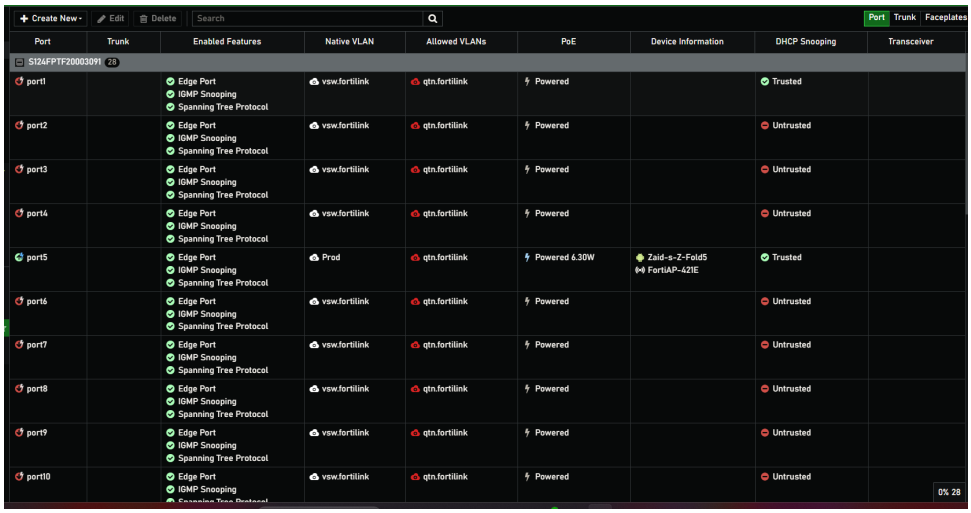


Figure 4.21: FortiGate FortiLink Ports

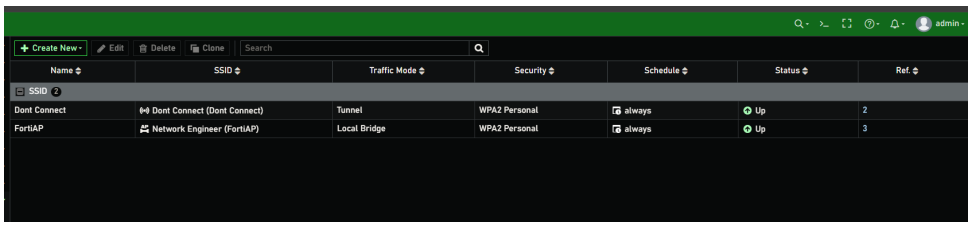


Figure 4.22: FortiGate SSID Configuration

Bridge Mode	Tunnel Mode
APs act as a bridge between wireless and wired networks	APs act as a tunnel between wireless and wired networks
APs forward traffic between wireless and wired networks	APs encapsulate wireless traffic and send it to the FortiGate
APs do not encrypt wireless traffic	APs encrypt wireless traffic before sending it to the FortiGate
VLANs are configured on the FortiGate	VLANs are configured on the APs

Table 4.1: Bridge Mode vs Tunnel Mode

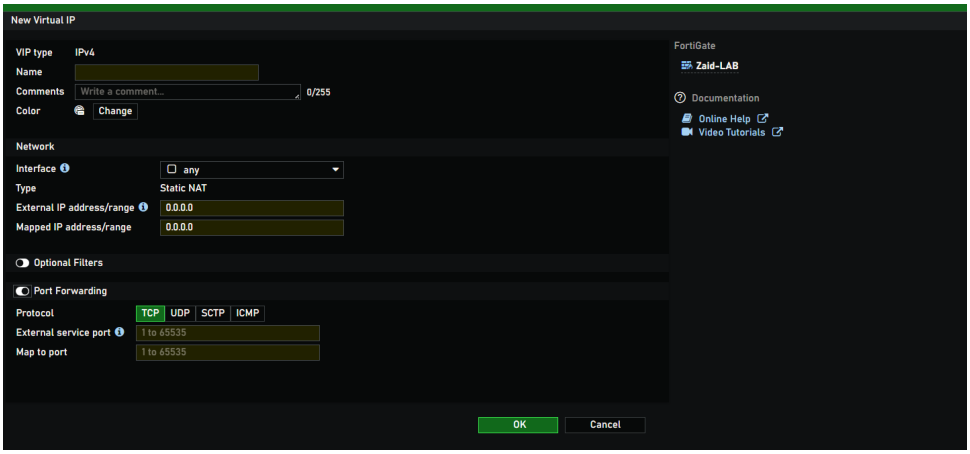


Figure 4.23: FortiGate VIP Configuration

Connection in the interface settings.

For the DMZ configuration, we need to configure the DMZ interface on the FortiGate, as shown in the previously shown Figure 4.2. We can then configure the VIP for the DMZ, as shown in Figure 4.23. VIP, also known as port forwarding, is used to forward traffic from a public IP address to a private IP address on a specific port. This is useful for hosting services such as web servers, email servers, or FTP servers behind a firewall.

Now we will set up the HA. To be able to achieve HA between two routers, we need to make sure that:

- Both routers have the same firmware version.
- Both routers have the same configuration.
- Both routers have the same hardware.

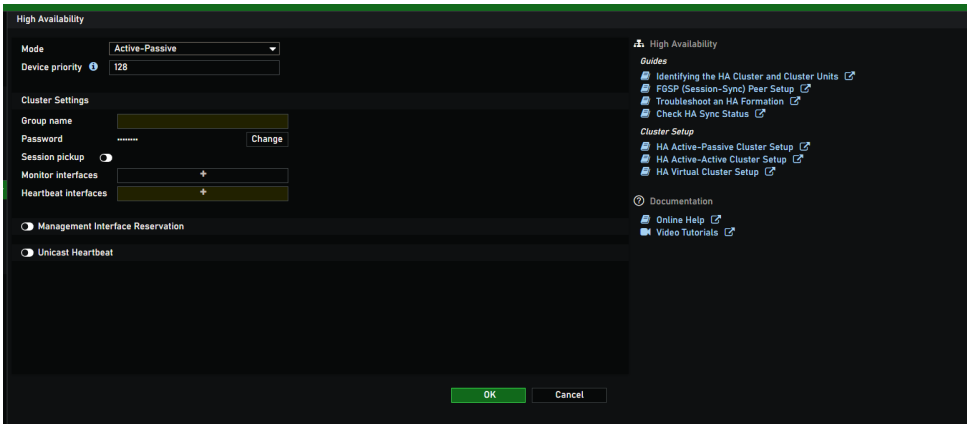


Figure 4.24: FortiGate HA Configuration

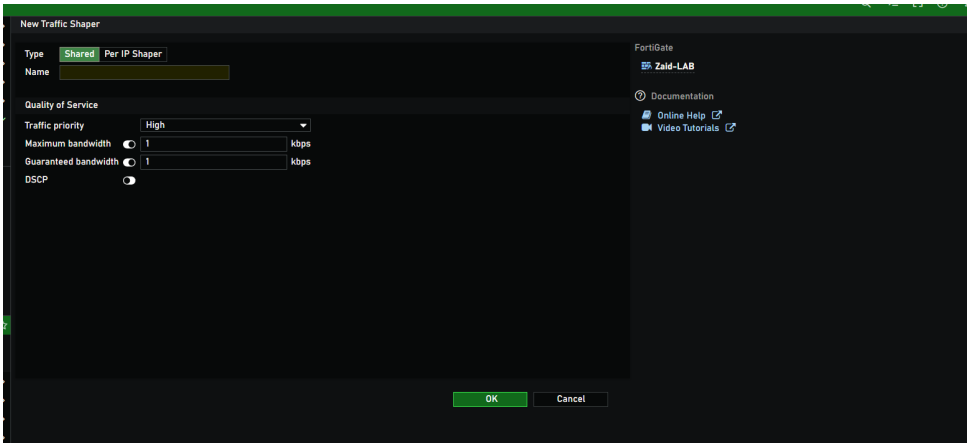


Figure 4.25: FortiGate Traffic Shaping Configuration

- Both routers have the same licenses.
- Both routers have the same interfaces.
- Both routers have the same VLANs.

We can then configure the HA as shown in Figure 4.24.

Next we configure the Traffic shaping as shown in Figure 4.25. We can configure the traffic shaping to prioritize certain types of traffic over others, and to limit the bandwidth of certain types of traffic. This can be used to ensure that critical traffic, such as voice and video traffic, always has enough bandwidth and that non-critical traffic, such as file downloads, does not consume all the available bandwidth. The ww configure the traffic shaping policy as shown in Figure 4.26.

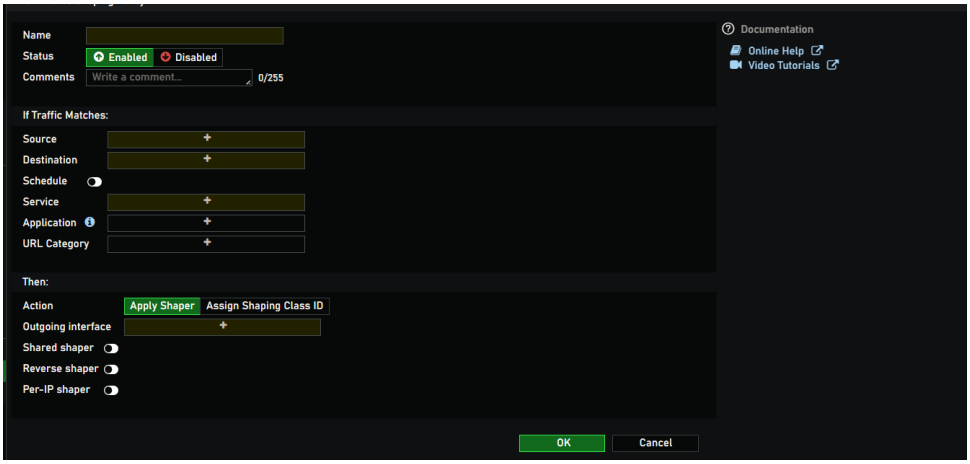


Figure 4.26: FortiGate Traffic Shaping Policy Configuration

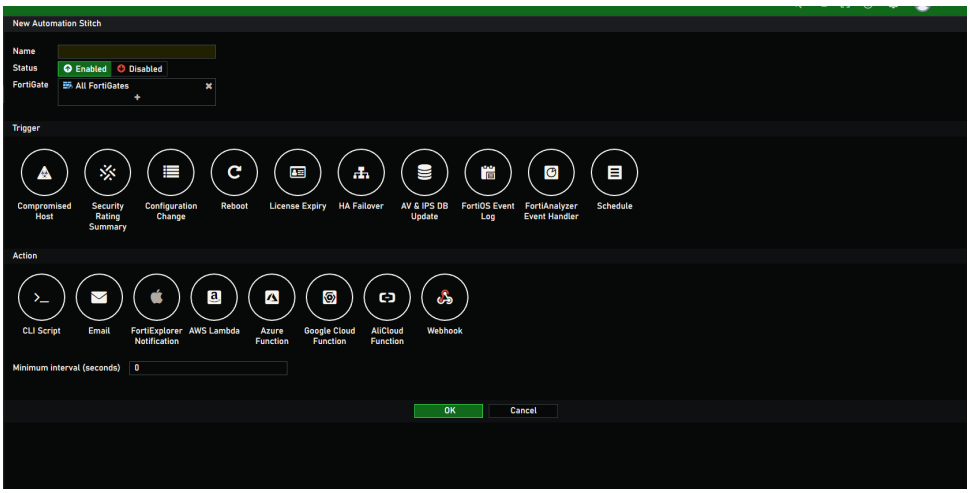


Figure 4.27: FortiGate Automation Configuration

4.1.2 Automation

As shown in figure 4.27, we can set up a trigger and an action to be taken when the trigger is activated. This can be used to automate certain tasks, such as sending an email when a certain event occurs, or blocking a user when a certain condition is met, etc. This can be used for our Exam VLAN, for example, we can set up a trigger to block a user when he tries to access a certain website, or to block a user when he tries to access the internet during an exam, etc. Unfortuantely, this feature is hard to apply on a small scale, thus it will only be presented as part of the design, but not implemented.

5. Results and Discussion

6. Economical, Ethic, and Contemporary Issues

6.1 Preliminary Cost Estimation

6.2 Relevant Codes of Ethics and Moral Frameworks

The project will adhere to the following codes of ethics and moral frameworks:

- **ACM Code of Ethics and Professional Conduct**: The project will follow the ACM Code of Ethics and Professional Conduct, which outlines the ethical responsibilities of computing professionals. The project team will ensure that all decisions and actions are in line with the principles of the ACM Code of Ethics. [45]
- **IEEE Code of Ethics**: The project will also follow the IEEE Code of Ethics, which provides guidelines for ethical behavior in the engineering profession. The project team will adhere to the principles of the IEEE Code of Ethics in all aspects of the project. [46]
- **Fortinet Code of Business Conduct**: The project will also adhere to the Fortinet Code of Business Conduct, which outlines the ethical standards and principles that Fortinet employees and partners are expected to follow. The project team will ensure that all interactions with Fortinet and the use of Fortinet products are in line with the Fortinet Code of Business Conduct. [47]

6.3 Relevant Environmental Considerations

6.4 Relevance to Jordan and Region

One of the things we aim to achieve is to standardize network infrastructure in Jordanian universities, and produce a standard that any institution can follow when installing/renewing their network infrastructure. This project can be used as a template for other universities in Jordan and the region to enhance their network connectivity and security using Fortinet products.

7. Project Management

7.1 Schedule and Time Management

If this project to be implemented, it will take around 2 months to complete. The project will be divided into several phases, including the design phase, implementation phase, testing phase, and deployment phase. The project team will work closely with the collaborate IT department to ensure that the project is completed on time and within budget. The project team will also provide regular updates to the university's management team to keep them informed of the project's progress.

7.2 Resource and Cost Management

Resource and cost management will be handled by the university's presidential council, which will allocate the necessary resources and funds for the project. The project team will collaborate with the university's finance department to ensure that the project is completed within budget.

7.3 Quality Management

The project team will follow a strict quality management process to ensure that the project meets the university's requirements and standards. The project team will conduct regular testing and quality assurance checks to identify and resolve any issues that may arise during the project. The project team will also provide training to the university's IT staff to ensure that they are familiar with the new network infrastructure and can effectively manage and maintain it.

7.4 Risk Management

The project team is committed to minimizing downtime by strategically utilizing breaks, nights, and weekends. This approach includes broadcasting scheduled downtimes to users to ensure they are informed and can plan accordingly. As a precautionary mea-

sure, the team will regularly backup data to safeguard against unexpected incidents. The hardware installation will follow a top-down approach, starting from the FortiGates and moving to the FortiAPs as per the roadmap. This method is designed to minimize downtime and ensure a smooth transition. In addition, the team will conduct a comprehensive risk assessment to pinpoint potential risks. These risks could range from hardware failures and software bugs to network outages. Once identified, a risk management plan will be developed to mitigate these risks. The team will devise strategies aimed at minimizing the impact of these risks on the project. Furthermore, the team will create a contingency plan to address any unforeseen issues that may arise during the project's lifecycle. This plan will provide a roadmap for dealing with potential problems and ensure the project stays on track.

7.5 Project Procurement

Once approved, YU project manager will contact a networking services company (e.g. Specialized Technical Services, or FutureTech) who will handle the procurement of the necessary hardware and software. The company will be responsible for sourcing the Fortinet products, as well as any additional equipment required for the project. The company will also be responsible for the installation and configuration of the network infrastructure, as well as providing training to the university's IT staff. The project manager will work closely with the company to ensure that the project is completed on time and within budget.

8. Conclusion and Future Work

References

[1] https://www.cisco.com/c/en_uk/products/security/firewalls/index-1b.html#~products. Accessed: 2024-06-11.

[2] https://www.avfirewalls.com/FortiGate-1200D.asp. Accessed: 2024-06-11.

[3] https://www.avfirewalls.com/FortiSwitch-448D.asp. Accessed: 2024-06-11.

[4] https://www.enbitcon.com/shop/fortinet/promo/fortinet-promo/fortinet-fortiap-231g-fap-231g-e. Accessed: 2024-06-11.

[5] https://www.computernetworkingnotes.com/ccna-study-guide/how-to-configure-dynamic-nat-in-cisco-router.html. Accessed: 2024-06-11.

[6] https://www.cloudflare.com/learning/dns/what-is-dns/. Accessed: 2024-06-11.

[7] https://www.yu.edu.jo. Accessed: 2024-06-01.

[8] https://www.fortinet.com/corporate/about-us/about-us. Accessed: 2024-06-05.

[9] https://www.netgate.com/blog/cisco-vs.-fortinet. Accessed: 2024-06-01.

[10] https://www.ammonnews.net/article/617705. Accessed: 2024-06-10.

[11] https://www.ineteconomics.org/research/research-papers/the-pursuit-of-shareholder-value-ciscos-transformation-from-innovation-to-financi Accessed: 2024-06-10.

[12] https://www.auvik.com/franklyit/blog/hierarchical-network-design. Accessed: 2024-06-11.

[13] https://www.checkpoint.com/cyber-hub/network-security/what-is-firewall/router-vs-firewall/. Accessed: 2024-06-09.

[14] https://luminisindia.com/it-networking-blog/153-journey-from-legacy-to-next-gener Accessed: 2024-06-09.

[15] https://docs.fortinet.com/document/fortigate/7.4.4/administration-guide/118003/policies#:~:text=These%20policies%20are%20essentially%20discrete,to%20pass%20through%20the%20FortiGate. Accessed: 2024-06-09.

[16] https://www.cloudflare.com/learning/network-layer/what-is-a-network-switch/. Accessed: 2024-06-01.

[17] https://www.solarwinds.com/resources/it-glossary/vlan. Accessed: 2024-06-01.

[18] https://www.fortinet.com/products/wireless-access-points. Accessed: 2024-06-01.

[19] https://docs.fortinet.com/document/fortigate/5.6.0/cookbook/335151/installing-a-fortigate-in-nat-mode. Accessed: 2024-06-02.

[20] https://www.fortinet.com/products/sd-wan. Accessed: 2024-06-02.

[21] https://docs.fortinet.com/document/fortigate/7.4.4/administration-guide/76624/link-monitor. Accessed: 2024-06-02.

[22] https://docs.fortinet.com/document/fortigate/7.4.4/administration-guide/900885/ha-active-passive-cluster-setup. Accessed: 2024-06-04.

[23] https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/high-availability/ha-overview. Accessed: 2024-06-04.

[24] https://docs.fortinet.com/document/fortigate/5.4.0/cookbook/361386/protecting-a-web-server-with-dmz. Accessed: 2024-06-04.

[25] https://www.fortinet.com/resources/cyberglossary/what-is-site-to-site-vpn. Accessed: 2024-06-02.

[26] https://www.cloudflare.com/learning/network-layer/what-is-ipsec/. Accessed: 2024-06-11.

[27] https://www.cloudflare.com/learning/network-layer/ipsec-vs-ssl-vpn/. Accessed: 2024-06-11.

[28] https://docs.fortinet.com/document/fortigate/7.4.4/administration-guide/850547/vrrp. Accessed: 2024-06-05.

[29] https://www.fortinet.com/resources/cyberglossary/what-is-dns. Accessed: 2024-06-05.

[30] https://www.fortinet.com/resources/cyberglossary/dynamic-host-configuration-protocol-dhcp. Accessed: 2024-06-05.

[31] https://www.ibm.com/docs/en/i/7.3?topic=services-trivial-file-transfer-protocol. Accessed: 2024-06-05.

[32] https://docs.fortinet.com/document/fortigate/6.4.0/ports-and-protocols/899996/fortilink. Accessed: 2024-06-04.

[33] https://docs.fortinet.com/document/fortigate/7.4.4/administration-guide/833698/web-filter. Accessed: 2024-06-04.

[34] https://docs.fortinet.com/document/fortigate/6.2.16/cookbook/605868/dns-filter. Accessed: 2024-06-04.

[35] https://docs.fortinet.com/document/fortigate/6.2.16/cookbook/302748/application-control. Accessed: 2024-06-07.

[36] https://docs.fortinet.com/document/fortigate/6.2.16/cookbook/565562/intrusion-prevention. Accessed: 2024-06-09.

[37] https://docs.fortinet.com/document/fortigate/6.2.16/cookbook/836396/antivirus. Accessed: 2024-06-09.

[38] https://docs.fortinet.com/document/fortigate/6.2.16/cookbook/929997/ssl-inspection. Accessed: 2024-06-09.

[39] https://docs.fortinet.com/document/fortigate/6.2.16/cookbook/933502/shared-traffic-shaper. Accessed: 2024-06-10.

[40] https://docs.fortinet.com/document/fortigate/6.2.16/cookbook/885253/per-ip-traffic-shaper. Accessed: 2024-06-10.

[41] https://www.petra.gov.jo/Include/InnerPage.jsp?ID=267484&lang=ar&name=news, note = Accessed: 2024-06-11.

[42] https://ieee802.org/. Accessed: 2024-06-11.

[43] https://www.iso.org/standard/27001. Accessed: 2024-06-11.

[44] https://www.ibm.com/topics/it-infrastructure-library. Accessed: 2024-06-11.

[45] https://www.acm.org/code-of-ethics. Accessed: 2024-06-11.

[46] https://www.ieee.org/about/corporate/governance/p7-8.html. Accessed: 2024-06-11.

[47] https://investor.fortinet.com/committee-details/code-business-conduct-and-ethics. Accessed: 2024-06-11.

A. User Manual