ANTONINE UNIVERSITY

Faculty of Engineering

Department of Informatics and Telecommunications

Baabda-Lebanon

Worker internship in the network sector of Cirrus

Labor internship report-STAP 301

Presented by: YOUSSEF Elie, 201720461, Telecommunications and networks

Host company: Cirrus

Baabda, 2022

THANKS

First of all, I would like to thank all my instructors and managers at Antonine University who guided me throughout my academic journey so that I could get there. Therefore, I would first like to thank the dean of the faculty of engineering, Dr Chady Abou Jaoude, but also Dr Talar Atechian who guided me and taught the course “Methodology and internship report” in order to introduce me little by little to the professional world and to derive the greatest possible benefit from it.

Next, I would like to thank the Head of Cloud Services Operations Mr. Tony Feghali who instructed and guided me during this internship so that I familiarized myself with the work sector of the company by offering his knowledge, his expertise and his continual support. Without forgetting to thank the entire Cirrus team as well as Mrs. Fatima Rhayel from the Human Management department who welcomed me and supported me in my daily tasks.

Finally, I would like to thank each member of my family and friends who inspired and supported me throughout my academic career and during this internship.

SUMMARY

This worker internship took place within the Cirrus company from June 20 to 31 August. During this period, as an intern in cloud networking, I was assigned the task of connecting, controlling and managing network resources in the cloud and more specifically: Creating virtual machines to implement and configure the various network components such as the Fortigate, FortiADC, FortiWEB as well as FortiMail and PCs playing the role of client and host. This internship allowed me to enrich the knowledge already acquired at university in the field of network and cloud computing while applying these new concepts with a serious and open to learning behavior.

ABSTRACT

This internship was rolled out at the company Cirrus from 20 June to 31 August 2022. During this period, as a cloud networking intern, I was assigned the task of connecting, controlling, and managing the networks' resources in the cloud and more precisely: Create virtual machines to implement the various network components such as the FortiGate, FortiADC, FortiWEB as well as FortiMail and PCs playing the role of client and host. This internship allowed me to enrich the knowledge already acquired at the university in the field of networking and Cloud computing while applying these concepts with a serious and open learning behavior.

TABLE OF CONTENTS

INTRODUCTION

As part of my fourth year of university in engineering telecommunications and networks, the procedure for the summer work placement is described in this report. Thanks to this internship, I was able to familiarize myself with the labor market as well as apply and develop my knowledge acquired during my university career in the professional world.

In this context, I was offered the opportunity to complete an internship of 11 weeks in the company "Cirrus" specialized in the field of cloud computing and part of the investment company "ITG Holding" in Beirut.

During this internship, various tasks were assigned to me in the field of cloud networking, most of these tasks were carried out in virtual environments using VMware Workstation while handling the various network components such as the FortiGate firewall, the FortiADC application delivery control, the FortiWeb web filter or the FortiMail mail filter which allowed me to control network traffic and grant or limit users' access to certain resources.

This introduction will be followed by three chapters: The first, which consists of present the company in detail as well as its sector of activity. The second, which consists of observations as well as tasks carried out during this internship. Finally, the last chapter, which covers a personal evaluation of the work carried out, adequate solutions to the obstacles encountered during the performance of the tasks as well as the working atmosphere. This report will finally end with a conclusion.

CHAPTER 1: PRESENTATION OF THE COMPANY

1.1. INTRODUCTION

This first chapter introduces the Cirrus hospitality business in which this internship took place from June 20 to August 31, 2022, for 7 hours a day with the option of working 2 days remotely (Work From Home) and 3 days at the company. In what follows, I will describe the mission as well as the vision of the company, its organization chart, its data sheet, its internal rules and finally my role within the team. This chapter will finally end with a summary.

1.2. COMPANY PRESENTATION

Assignment

Cirrus, an ITG company, founded in 2016 belonging to the ITG group and based in Lebanon, is a cloud service provider offering a complete directory of enterprise cloud services and catering to different infrastructure, platform and software service models.

The main mission of this company is to strengthen the capacities of its teams to work ethically and diligently to provide a wide range of superior technology products and services tailored to the exact needs of its customers.

Cirrus is recognized for its tier-IV Uptime certified data center Institute" which facilitates its disaster recovery and business continuity plans.

Vision

This company being one of the largest cloud service providers in the middle east, it therefore aspires to maintain its status and reputation while offering high quality services using its team of professionals and sophisticated and secure technologies in order to satisfy its customers and partners and thus grow even more.

Organizational chart

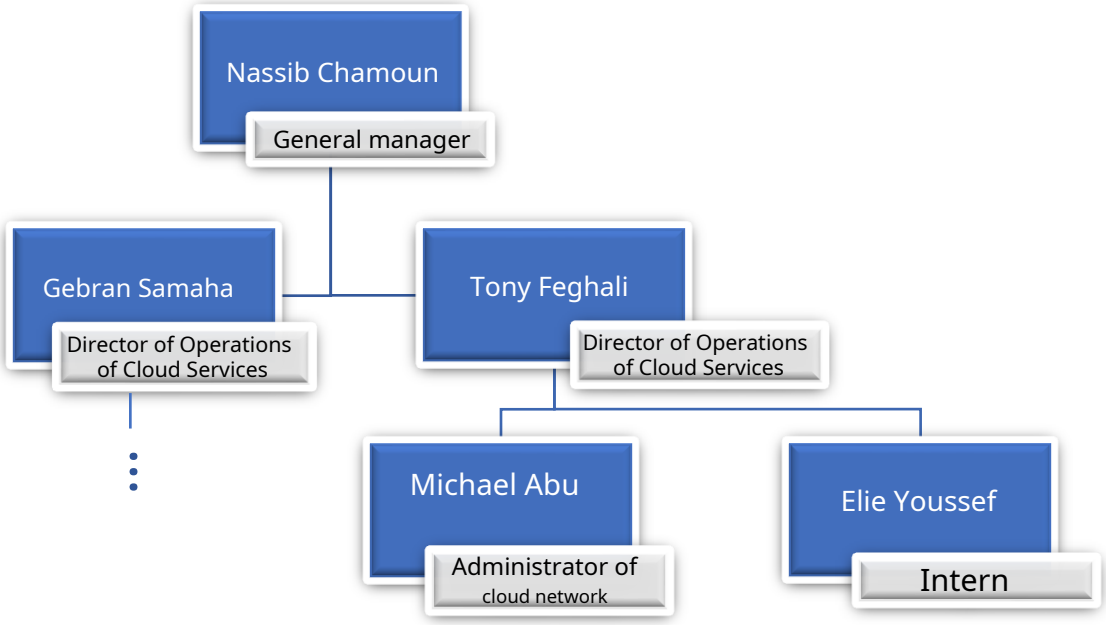


Figure 1:*The organization chart of the company*

Material Safety Data Sheet

Table 1:*MSDS*

Company Name	Cirrus
Creation date	2016
Kind	Private enterprise
Direction	Nassib Chamoun (General Manager)
Address	HOLCOM Bldg.,460 Corniche Al Nahr, Beirut, Lebanon
Activity area	Cloud Services
Phone	+ 961 1 595 570
Fax	+ 961 1 595 595
email address	info@itg.com.lb
Number of employees	12
Website	http://www.cirrus-me.com/#home
Logo	CIRRUS An ITG company

Internal rules

Discipline and seriousness are the main factors to achieve success in any prestigious company, and Cirrus is no exception. Indeed, in order to maintain the quality of the services offered, a series of internal regulations are applied. All employees must arrive and leave on time according to the schedule set by the company which is from 8 a.m. until 5 p.m. from Monday to Friday while registering their arrival and departure with the possibility of working remotely for some with the same schedule. . If unable to report to work on time, the employee in question must inform his superior of his delay and the cause. In the event of urgent problems, the employee in question will have to appeal to his superior to remedy them. All employees must dress appropriately in casual clothing while respecting the hygiene regulations imposed by wearing hygiene masks.

Role within the team

Within the Cirrus team and under the supervision of Mr. Tony Feghali, I been able to learn the work process within the company while contributing to this work through my skills and knowledge acquired during my university career.

My main task was to learn and apply all the instructions given by my internship supervisor, more specifically, by establishing virtual machines where I had to test the various security components by configuring them using network diagrams to be used later by the team

1.3. SUMMARY

This chapter has described the mission and vision of the hospitality company Cirrus, while presenting a simplified organization chart as well as its data sheet. The internal rules followed by each employee were covered and finally, the role I was assigned within the team as well as my main function were revealed. The following chapter will present the observations as well as the tasks accomplished during this internship.

CHAPTER 2: OBSERVATION AND TASKS PERFORMED

2.1. Introduction

This chapter discusses the observations made during this internship as well as the tools used to carry out the assigned tasks. In addition, it will contain in detail the tasks carried out throughout the internship period at Cirrus. And finally, a summary summary to close this chapter.

2.2. Comments

During the first two weeks of my internship, I was not given any practical tasks to perform, but rather I was assigned the objective of reading and researching about SDN and SD-WAN and their definition, advantages and respective top vendors, the difference between traditional network architecture and spine-leaf architecture as well as the difference between traditional MPLS and SD-WAN technology. Without forgetting to practice the different demos of the different components of Fortinet such as FortiGate, FortiADC, FortiWeb and FortiMail. This different research allowed me to immerse myself little by little in the field of cloud networking and to prepare myself for the manual tasks to be carried out.

During this period, my internship supervisor explained to me his role in the company as well as my assigned tasks by setting me a final objective and what I had to gain from this internship, I was also able to discuss with certain member of the Cirrus team about their role and their different tasks while observing their work, and it is through these discussions and observations that I better understood how this company works, and how I can contribute to the work done.

2.3. Tools used during the course

In order to carry out the work entrusted to me, I used different software and licenses. The following will consist of the different tools with a brief explanation of their role as well as their method of manipulation.

2.3.1. VMware Workstation Pro

Figure 2: *VMware Workstation Pro*

VMware Workstation Pro is defined as a hosted hypervisor responsible for implementation and virtualization on computers with a Microsoft Windows or Linux operating system. By creating an abstraction layer between software such as operating systems or applications, the latter ensures the administration of virtual representations of hardware (virtual processors, memory, network adapters, etc.). Using this software, I was able to implement the iso type files and configure them.

2.3.2. web-browser

Figure 3: *Mozilla Firefox*

Mozilla Firefox is an open-source web browser developed by the Mozilla Corporation foundation. This tool was mainly used to access the Web GUI of Fortinet components while entering the management ip address of the device.

2.3.3. Draw.io

Figure 4:*Draw.io*

Draw.io is an open source Windows application for creating diagrams offline or online. These charts can be saved or imported into other applications or programs, depending on the type of chart. This application was useful to me in the creation of network diagrams in order to better visualize it and plan the work process.

2.3.4. Apache HTTP server

Figure 5:*Apache http-server*

Apache http server is an open source web server that delivers web content over the internet. It is the web server that handles requests and serves web resources and content over http. Apache http server is implemented in Windows 10 virtual machine playing the role of HTTP Web server.

2.3.5. DVWA

Figure 6:*DVWA*

Damn Vulnerable Web Application is a PHP/MySQL web application, its main purpose is to help penetration testers and security professionals to test their tools which improves the security of their web applications. DVWA is implemented in Windows 10 virtual machine acting as DVWA Web server.

2.3.6. Microsoft Exchange Server

Picture 7:*Microsoft Exchange Server*

Microsoft Exchange is a collection of applications that enable digital messaging and collaboration in a corporate computing environment. It primarily allows an organization to set up and host messaging and collaboration services. This server is installed on Windows Server 2016 virtual machine to provide server side services and features.

2.3.7. Licence

The license file is a text file that automatically provides required information, such as product name, authorization number, and user contact information in order to use Fortinet components without restricted access.

2.3.8. Disk Image File

A disk image (.iso) is a file that is an exact copy of a disk volume or an entire physical disk drive. This file preserves all the properties of its source

as files, folders, etc. These files were imported into VMware Workstation pro in order to use Windows 10 and Windows Server 2016 virtual machines.

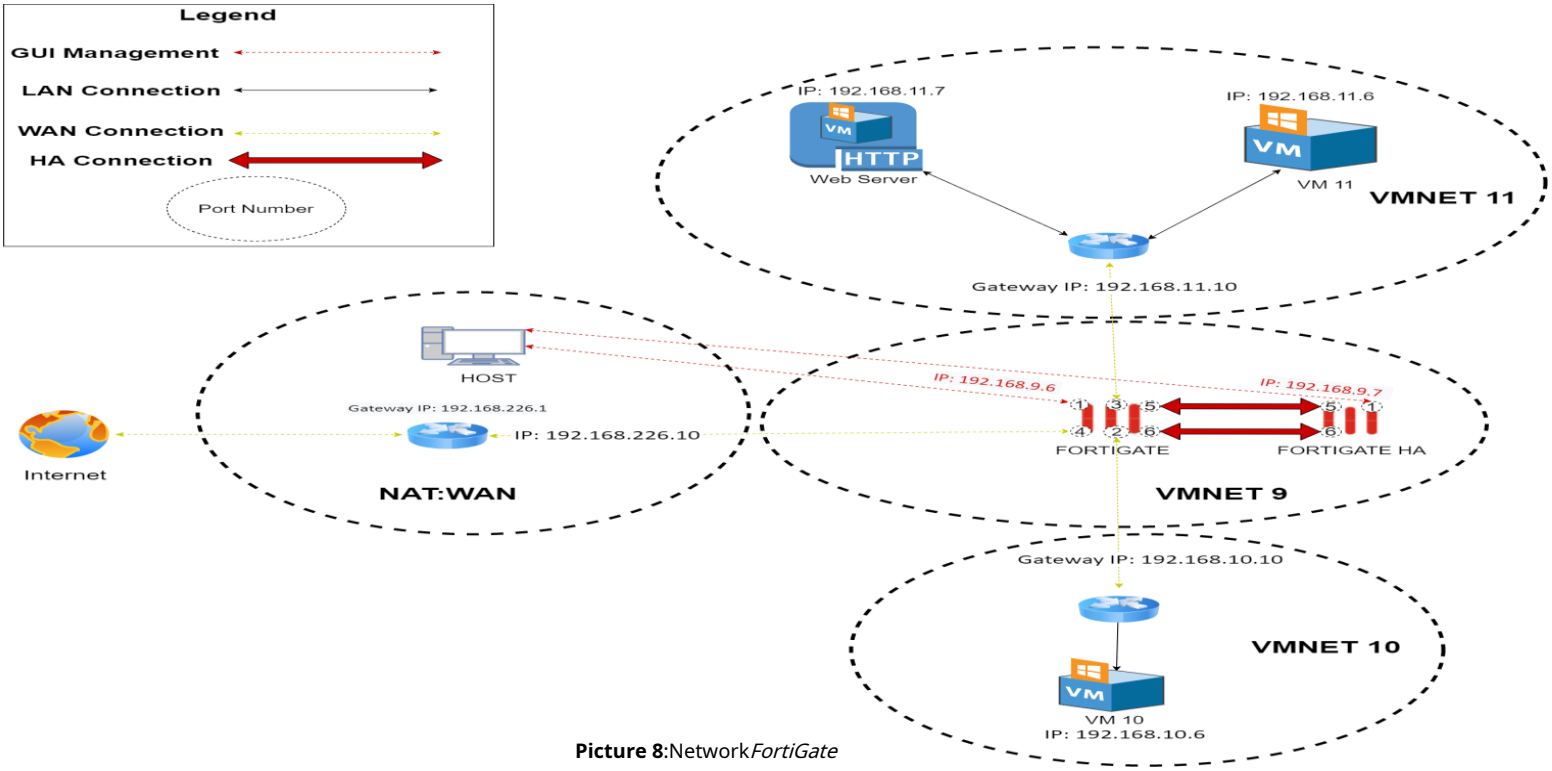
2.3.9. Open Virtualization Format Package

Open Virtualization Format (.ovf) is an open source standard for packaging and distributing software applications and services for virtual machines. These files have also been imported into VMware Workstation pro in order to use the virtual machines of Fortinet devices like FortiGate, FortiADC, FortiWeb and FortiMail, .

2.4. COMPLETED TASKS

2.4.1. FortiGate firewall implementation

FortiGate next generation firewalls provide organizations with protection against web-based network threats, including known and unknown threats and intrusion strategies. Deployed on-premises using virtual hardware or the cloud. The primary use of this device is to scan incoming and outgoing traffic for viruses, malware, phishing attacks, spam, attempted network intrusions, and other cybersecurity threats. This component can also act as a router by implementing the appropriate firewall policies. The**Picture 8**below represents the network to implement and manipulate using VMware Workstation Pro and Mozilla Firefox.



Picture 8:Network*FortiGate*

According to**Figure 8,**the task assigned to me is to connect the virtual machine present in the VMNET 10 virtual network to the web server present in the VMNET 11 virtual network using the FortiGate and its implemented firewall policies. In order to better manipulate and configure the FortiGate, I needed to implement a Web GUI management interface on the virtual machine. From this, I imported the respective ovf file to this device on VMware Workstation and entered the following commands:

-**config sys int,**to configure the system interfaces.

-**editport1**, to configure the port 1 interface.

-**set mode static**, in order to enter an ip address manually.

-**set ip address 192.168.9.6/24**, enter the ip address and its subnet mask.

-**set allowaccess http https ping ssh telnet**, grant access to http and https requests, the ping command, and ssh and telnet connections.

The**figure 9**and**10**below shows the commands entered and the adapters suitable for the FortiGate, the Web GUI login page as well as the entry page.

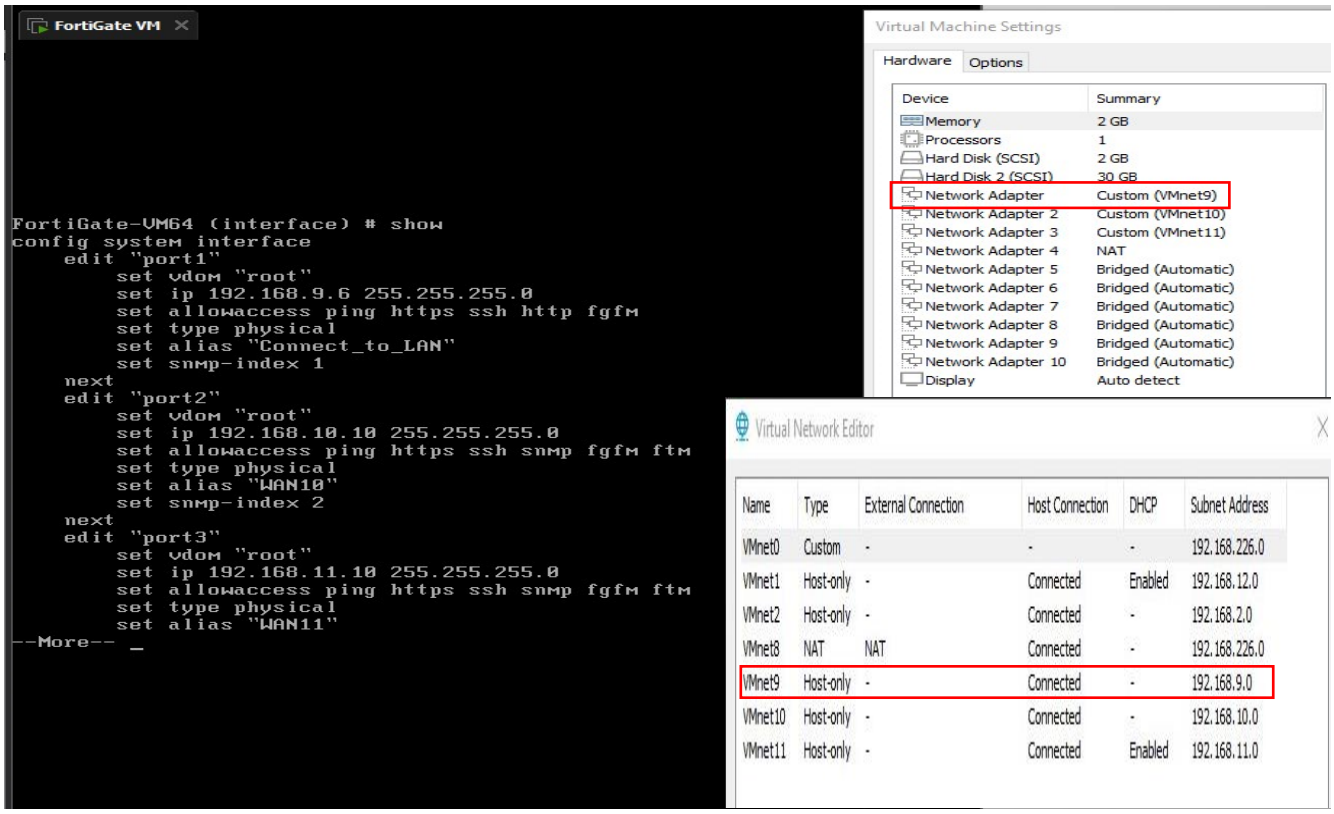
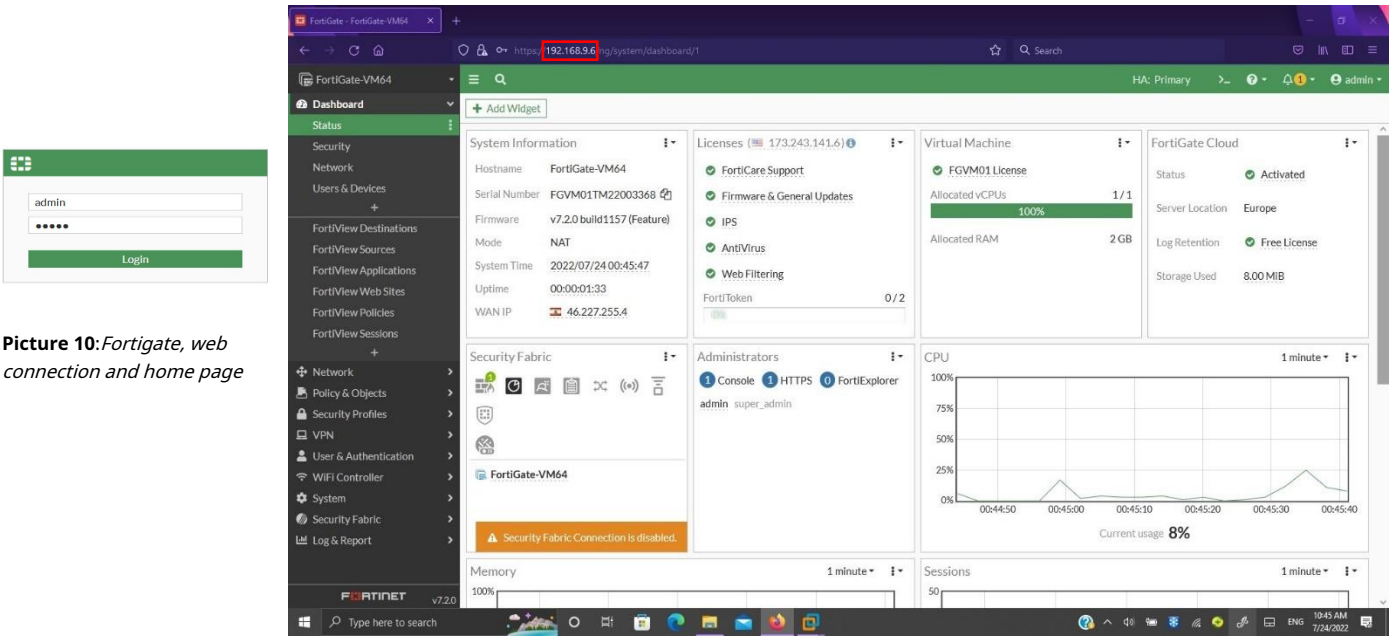
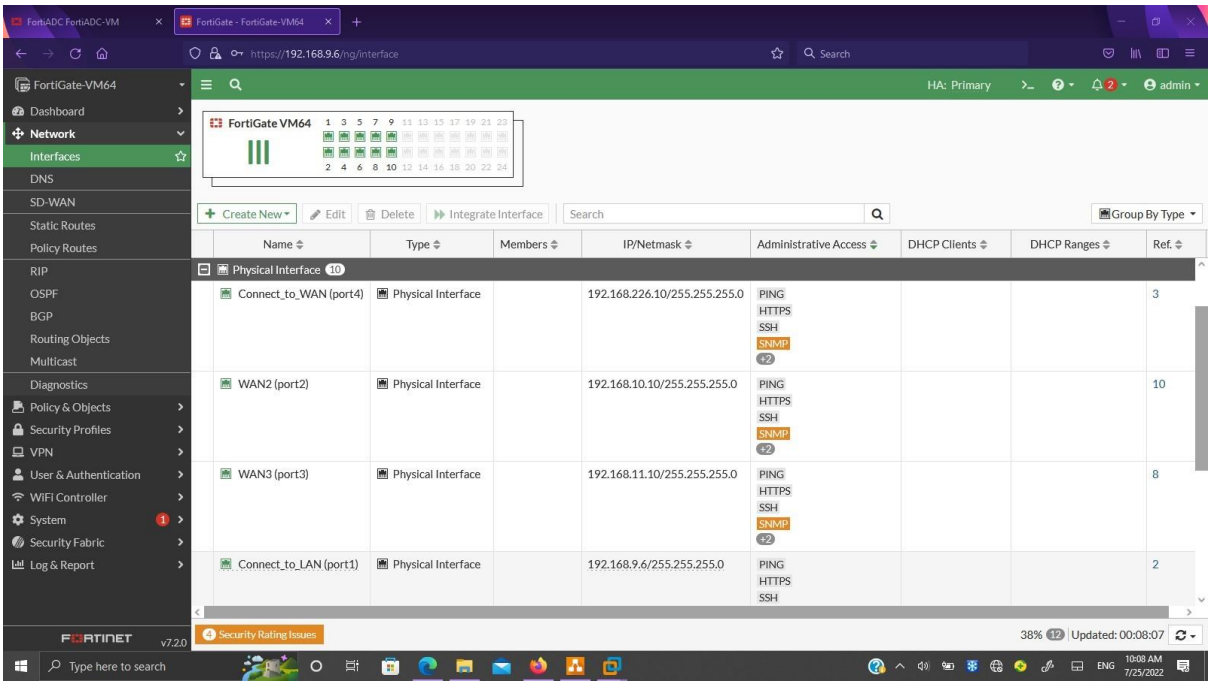


Figure 9:*FortiGate CLI, Virtual Machine and Network Settings*



Picture 10:*Fortigate, web connection and home page*

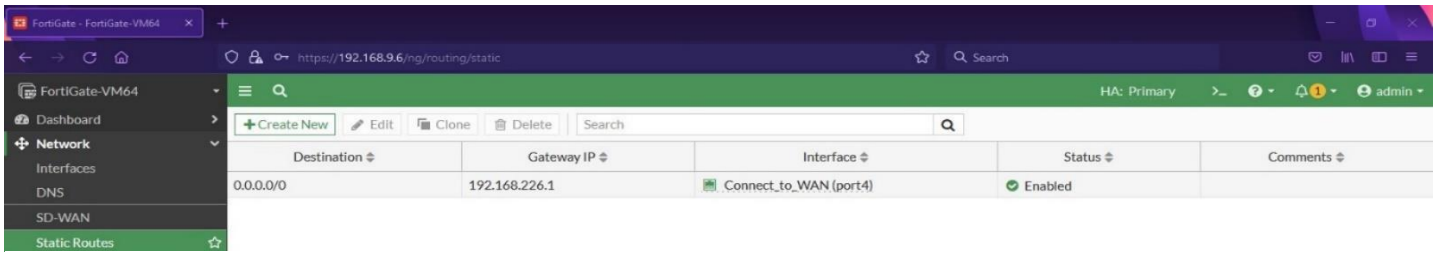
The same configurations were made for ports 2, 3 and 4 with respective IPs 192.168.10.10/24 (VMNET 10), 192.168.11.10/24 (VMNET11) and 192.169.226.10/24 (NAT which is present in the LAN from my PC in order to have access to the internet). The**figure 11**shows the different interfaces present on the FortiGate seen through the Web GUI.



Picture 11:*FortiGate Interfaces*

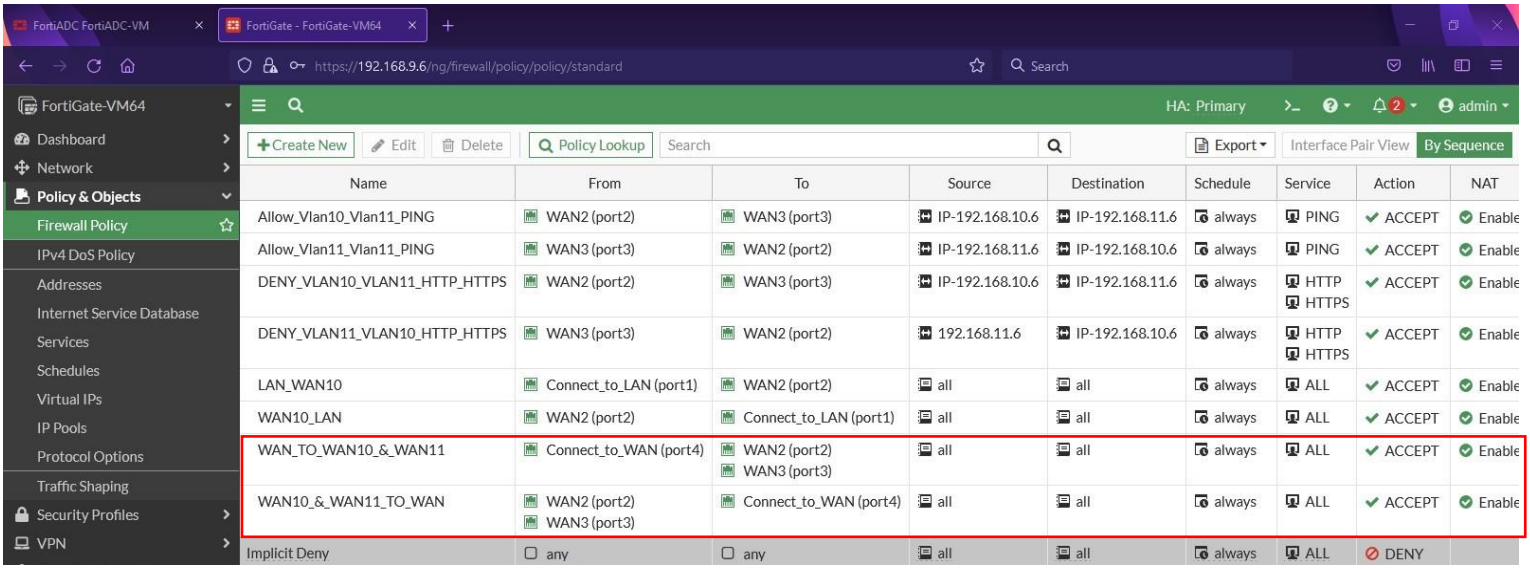
Trying the ping 8.8.8.8 command in the FortiGate CLI (to test connectivity to Google servers) to make sure it is connected to the internet, there was no response. After several searches, I realized that I had to

implemented a static route in the domain of the PC connected to the computer with a Gateway ip of 192.168.226.1 as listed in the**figure 12**.



Picture 12:*FortiGate Static road*

After this step, I had to create firewall policies in order to allocate connections across the entire network. As present in the**figure 13**containing all the policies used.



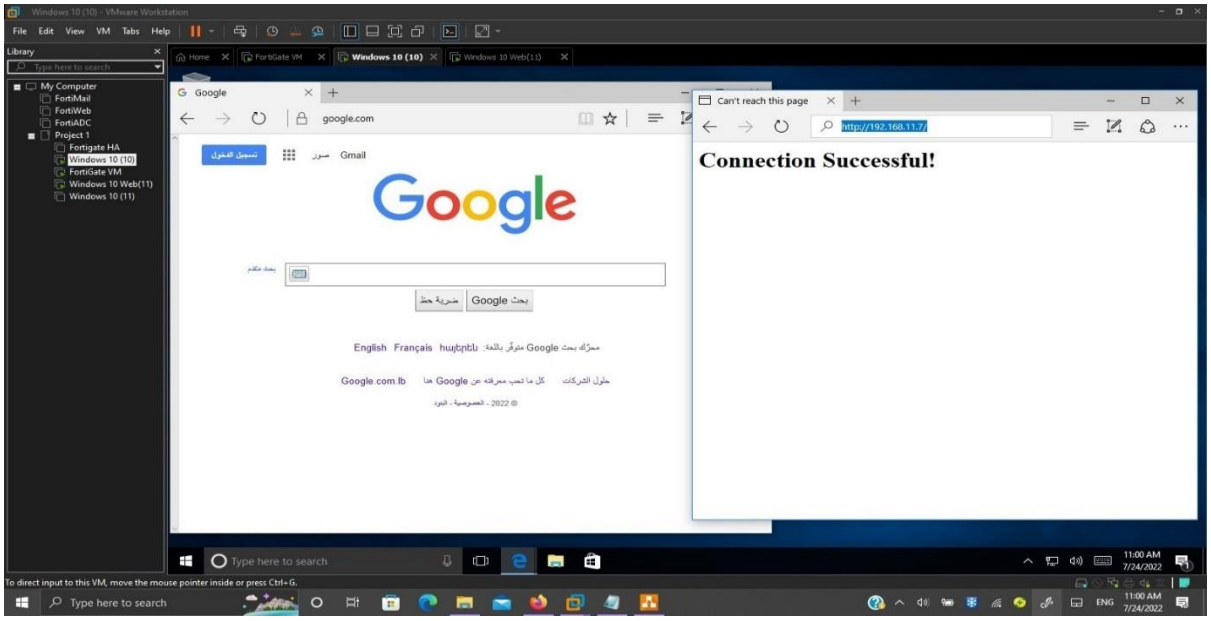
Picture 13:*FortiGate Firewall Policy*

The policies presented above framed have been implemented in order to ensure the connection of the NAT to VMNET 10 and VMNET 11 and vice versa. The other policies implemented were used to ensure connections to the different domains.

Then, we had to create the client and server virtual machines, first by creating the Windows 10 virtual machine with an ip address of 192.168.10.6/24 in VMNET 10 with a Gateway address of 192.168.10.10 and second, by creating the virtual machine Windows 10 with an ip address 192.168.11.6/24 as well as the Windows 10 virtual machine with an ip address 192.168.11.7/24 playing the role of http web server in VMNET 11 with a Gateway address of 192.168.11.10. In order for the Windows 10 vm to play the role of http Web server, it was necessary to install the Apache software and modify the ip address present in the httpd.conf file which listens to http requests so that it becomes 192.168.11.7 like that of the

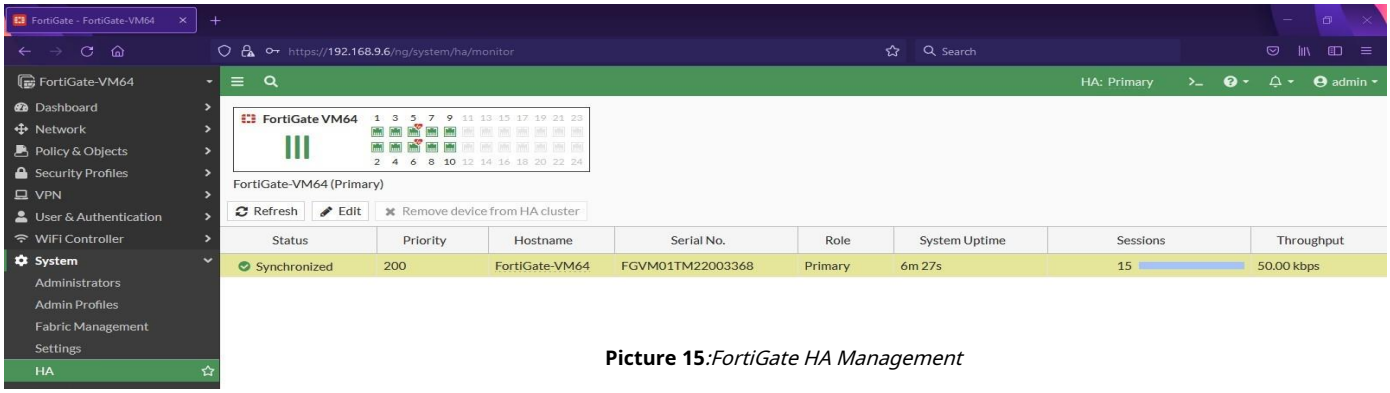
machine. I also had to modify the index.html file in order to display the message "Connection Successful!" to make sure the connection is established correctly.

Recently, we had to test all these configurations by starting the client virtual machine with a respective ip address 192.168.10.6 in VMNET 10 and trying to send an http request through the Web browser with a URLhttp://192.168.11.7 when the web server is started. According to**Picture 14**, the access to the web server was successful.



Picture 14:*Successful connection to web server and internet*

Eventually I needed to set up a second Fortigate, which would act as Active-Passive (the active device handles all traffic under normal circumstances, if something fails on the active device, the passive device becomes active and handles everything traffic instead) to ensure high-availability functionality. This functionality allows a device to act as a backup in the event of an incident such as a power failure to the first device. To achieve this, I had to perform the same configuration steps as the first FortiGate but this time assigning only ports 5 and 6 for HA management. I then had to authorize the HA mode in the two Fortigates by introducing the respective ip addresses to each device. The **figure 15**demonstrates the success of this operation.

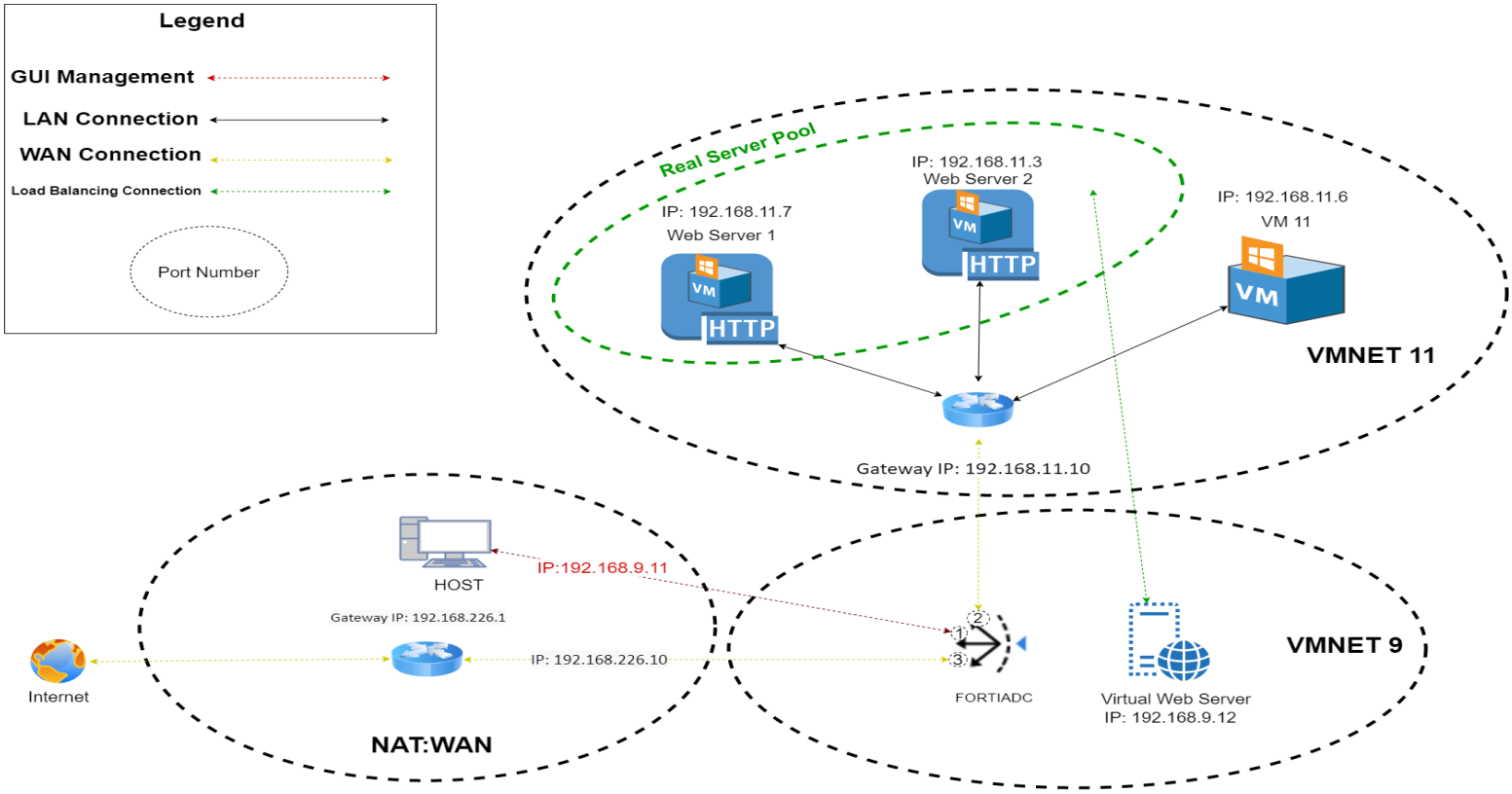


Picture 15:*FortiGate HA Management*

.

2.4.2. Implementing the FortiADC advanced Application Delivery Controller

The FortiADC is an advanced application delivery controller (ADC) that ensures the availability, security and optimization of applications. It offers advanced security features (WAF, DDoS and AV) and application connectors for total visibility into networks and applications. In this network, the role of the FortiADC was to offer the possibility of Load Balancing assigned to two real servers present in the VMNET 11 as indicated in the**figure 16**.



Picture 16*:FortiADC Network*

According to**figure 16**, it was necessary to group the two servers present in the VMNET 11 in the same real server pool and assign them to a virtual web server in the VMNET 9 in order to apply the server Load Balancing functionality which distributes the workload of the applications on the entire server pool by ensuring application availability by supporting back-end server health management.

At the beginning, it was necessary to create a virtual machine containing the FortiADC then to configure the various ports of this device as done previously with the FortiGate and as

indicated in the**figure 16**which I assigned the ip management address 192.168.9.11/24. After connecting to the Web GUI of the device and inserting the license, I had to start by adding the two real servers RS1 and RS2 with the respective ip addresses 192.168.11.7 and 192.168.11.3 and grouping them in the same real server pool named RSP as demonstrated in the**figure 17**.

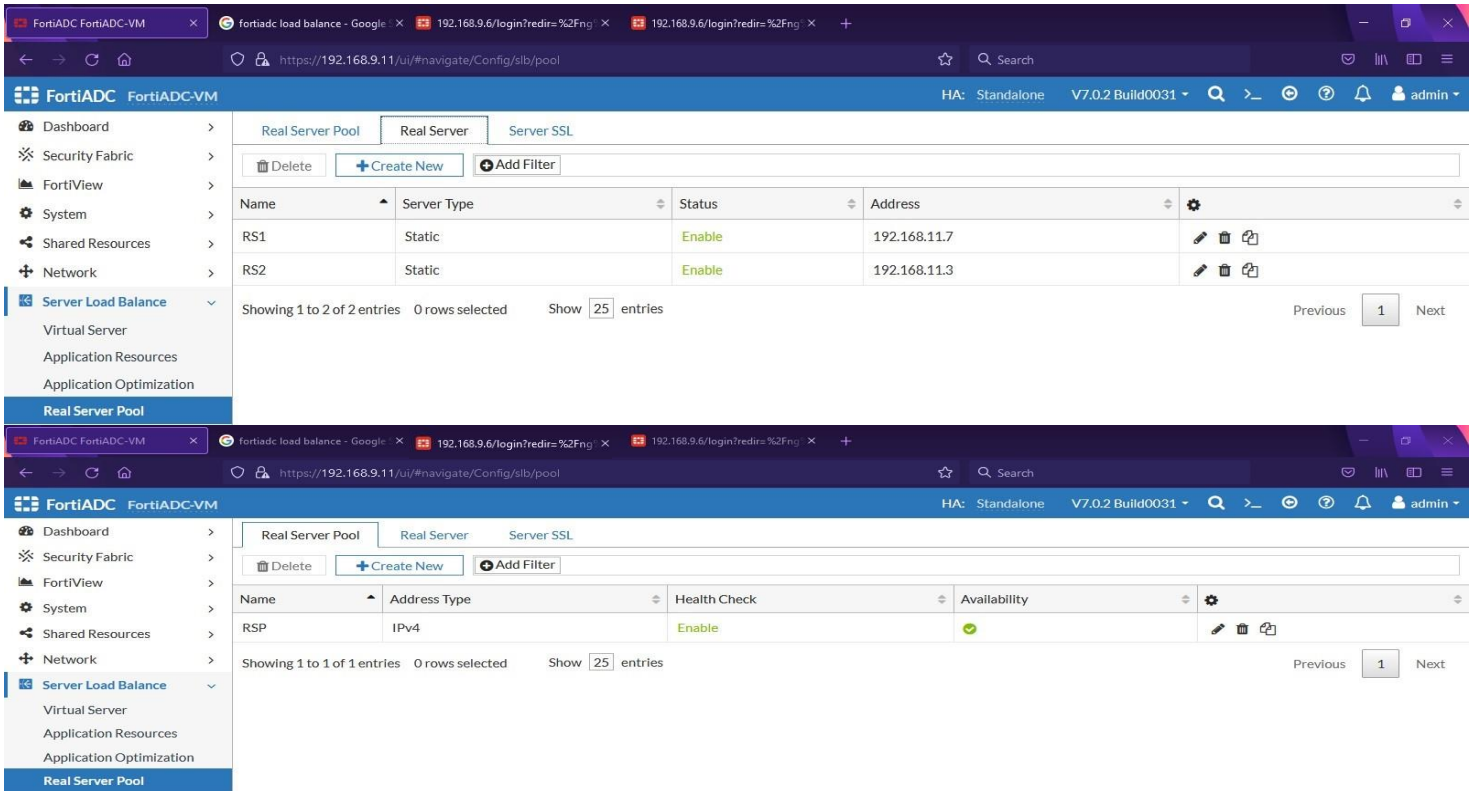
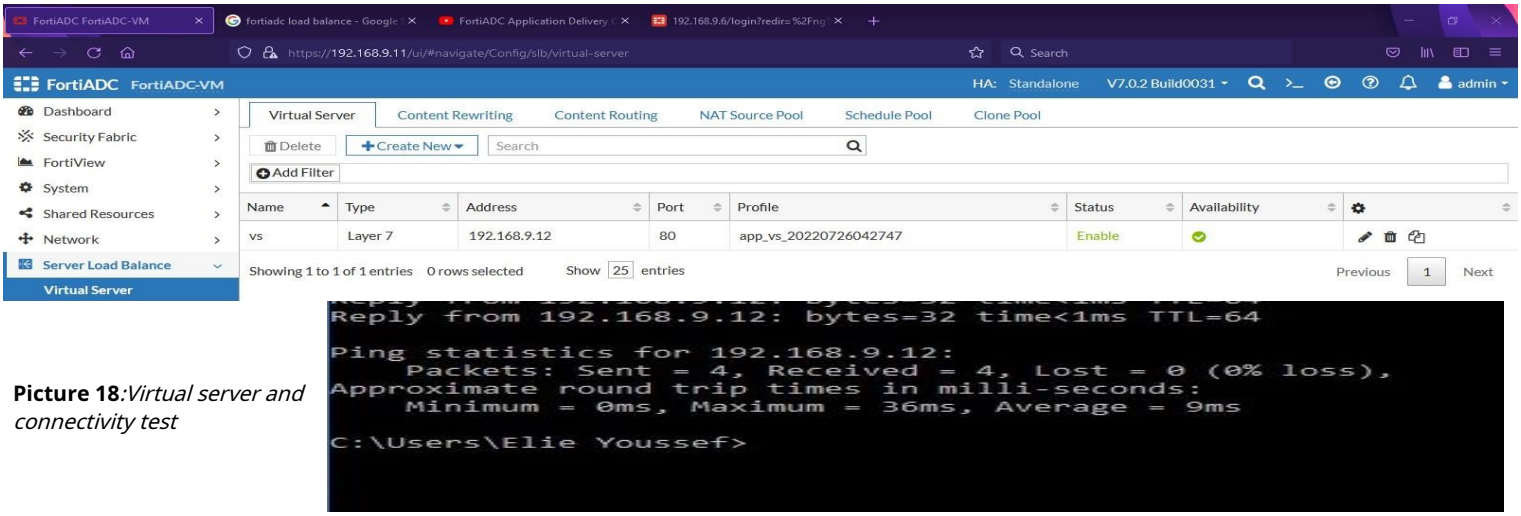


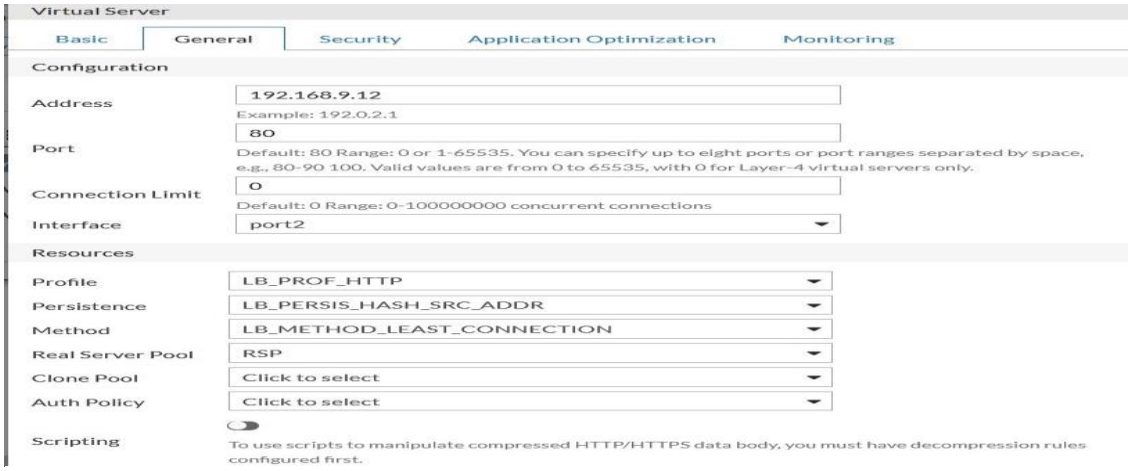
Figure 17*:Real server pool and its members*

After this step, the virtual server had to be created and since the two real servers were Web servers, the virtual server created had to be assigned port 80 and support Layer 7 (Application Layer). This same server was assigned the ip address 192.168.9.12 and connectivity to this server was tested from Web server 2 in VMNET 11 using the command**ping 192.168.9.12**on cmd as shown in the**figure 18**.



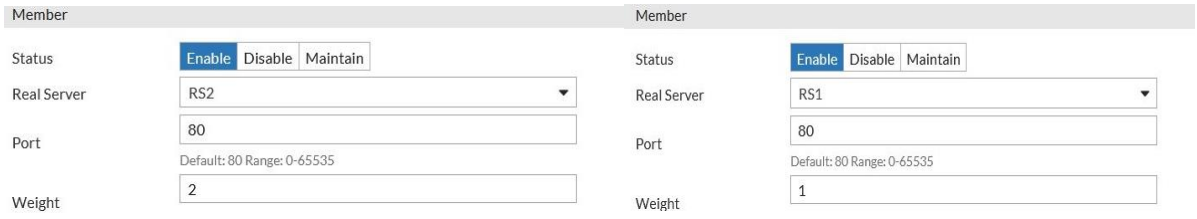
Picture 18*:Virtual server and connectivity test*

Additional configurations have been put in place to enforce server Load Balancing as the profile type**Load Balancing Profile http**since the two servers that are part of the server pool are http web servers, the persistence type**Load Balancing persistence hash source address**which uses the source and destination IP addresses of the client and server to generate a unique hash key which is used to allocate the client to a particular server and the method**Load Balancing method least connection**which uses the least consuming connection as demonstrated in the**figure 19**.



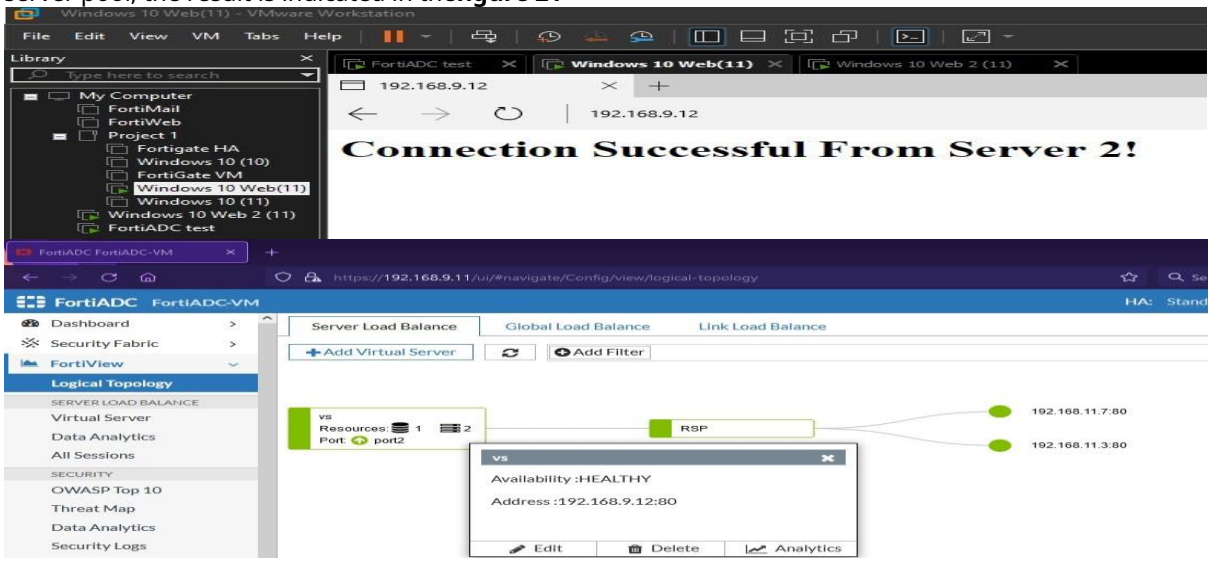
Picture 19:*Configuring virtual server resources*

A last step was to assign the weight of each of the real servers in order to determine which server the virtual server will connect to in priority, therefore, I therefore assigned server 2 the highest priority, the**figure 20**shows this configuration.



Picture 20:*Priority of real servers in the server pool*

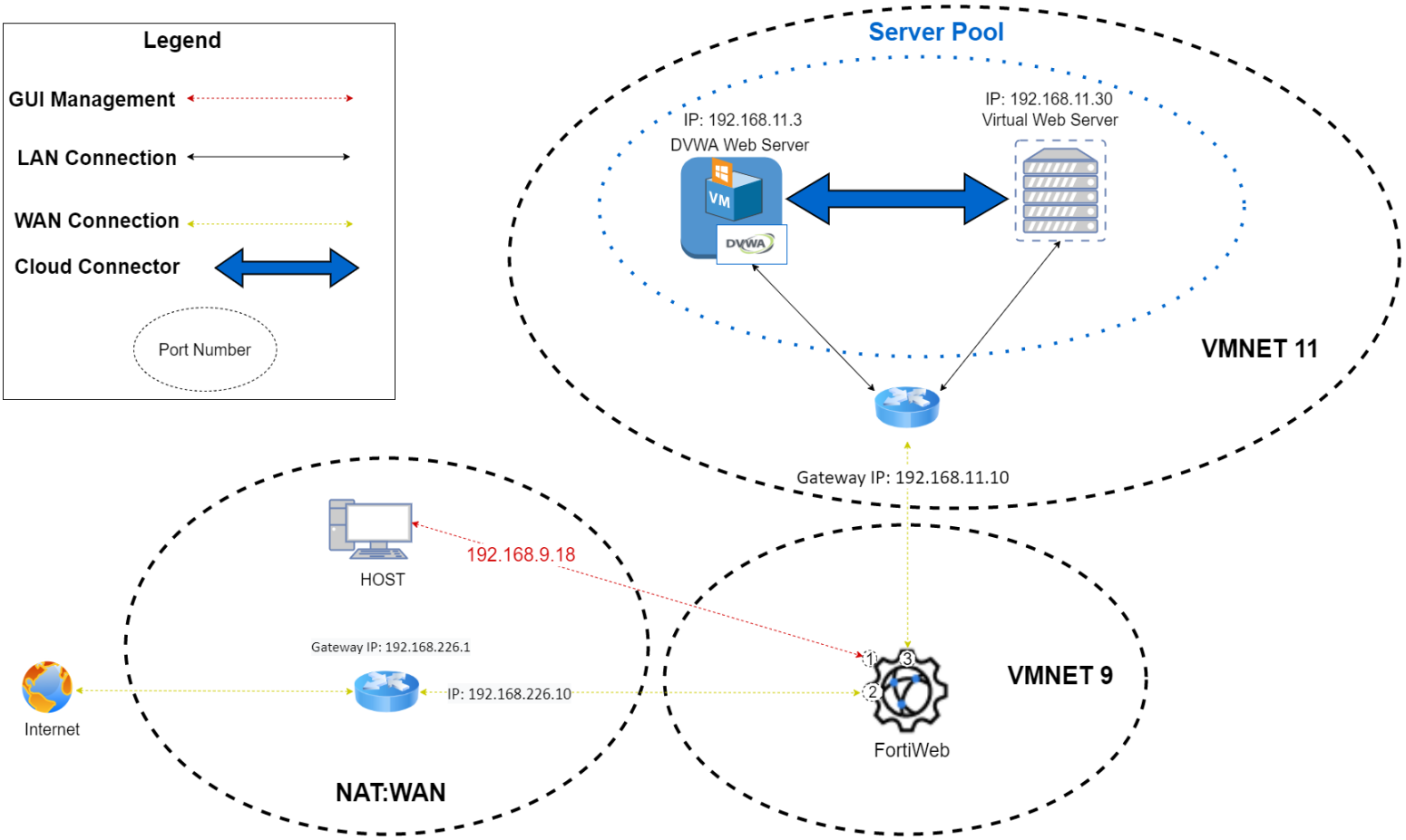
Finally it was necessary to test the connection to the virtual server of one of the real servers composing the server pool, the result is indicated in the**figure 21**



Picture 21:*Virtual network topology and successful connection*

2.4.3. FortiWeb Web Firewall Implementation

The FortiWeb is a web application firewall (WAF) that protects web applications and APIs from known target attacks and unknown exploits and helps maintain regulatory compliance. The network built to test the FortiWeb is presented in the**figure 22**.

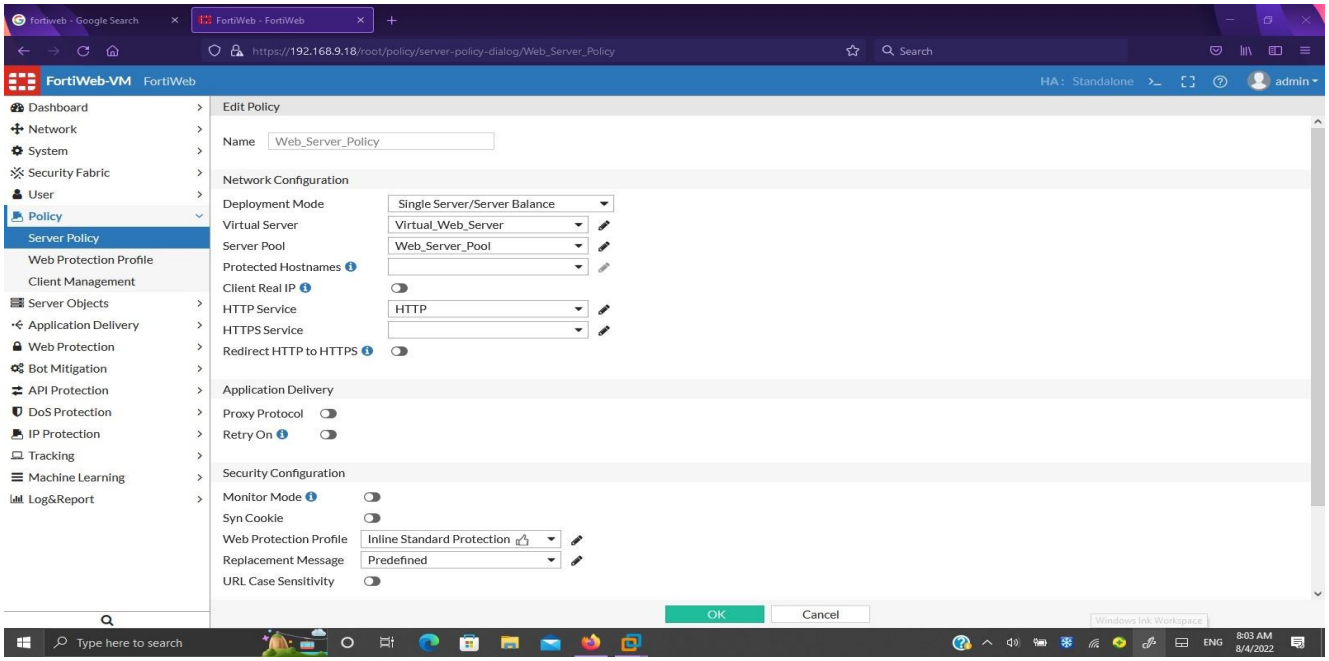


Picture 22*: FortiWeb Network*

In this diagram, I had to assign a virtual server with a respective ip address 192.168.11.30/24 connected to the DVWA web server with an ip address 192.168.11.3/24 in the VMNET 11.

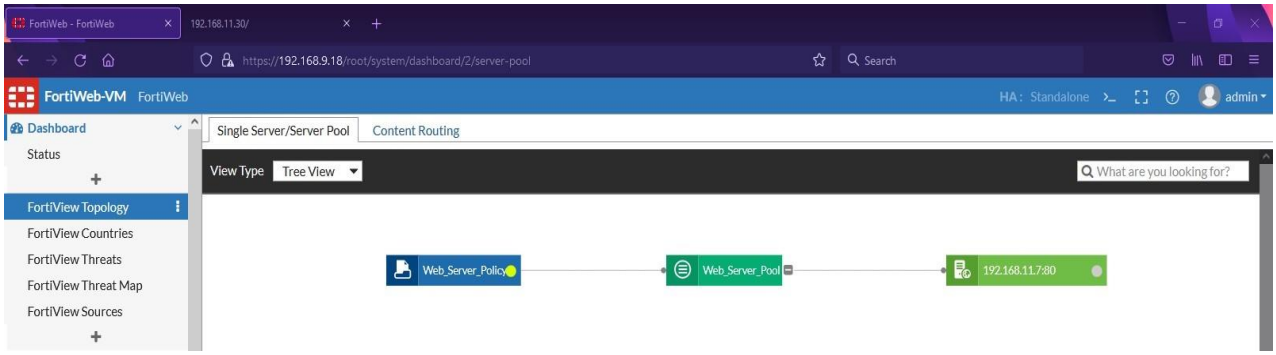
As done previously with other Fortinet devices, you must first create a FortiWeb virtual machine and configure its ports as indicated in the**figure 22**by assigning the ip management address 192.168.9.18/24. After accessing the web GUI and inserting the license, I created the server pool containing the DVWA server and assigned it to the virtual server to which I had to connect to test the protection efficiency. The fortiWeb contains by default security policies configured as the**figure 23**confirms against the OWASP top 10 which is a standard awareness document for developers and

Web Application Security representing a broad consensus on the most critical security risks for web applications.



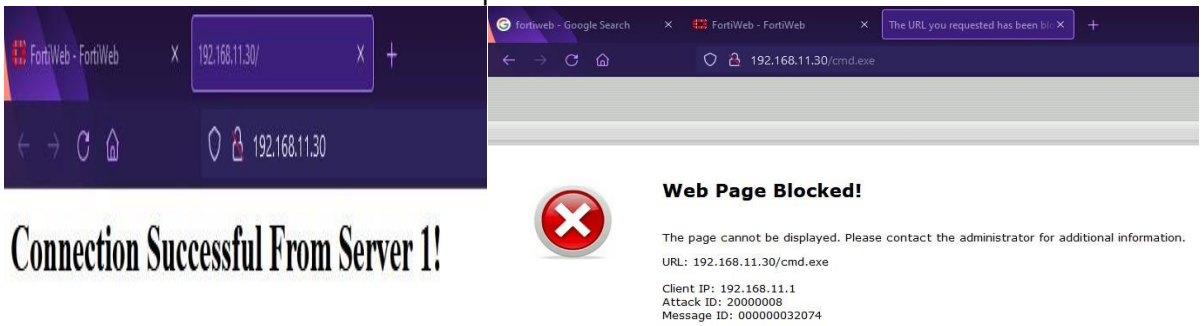
Picture 23*:Virtual server policies*

The**figure 24**shows the virtual server topology.



Picture 24*:Virtual server topology*

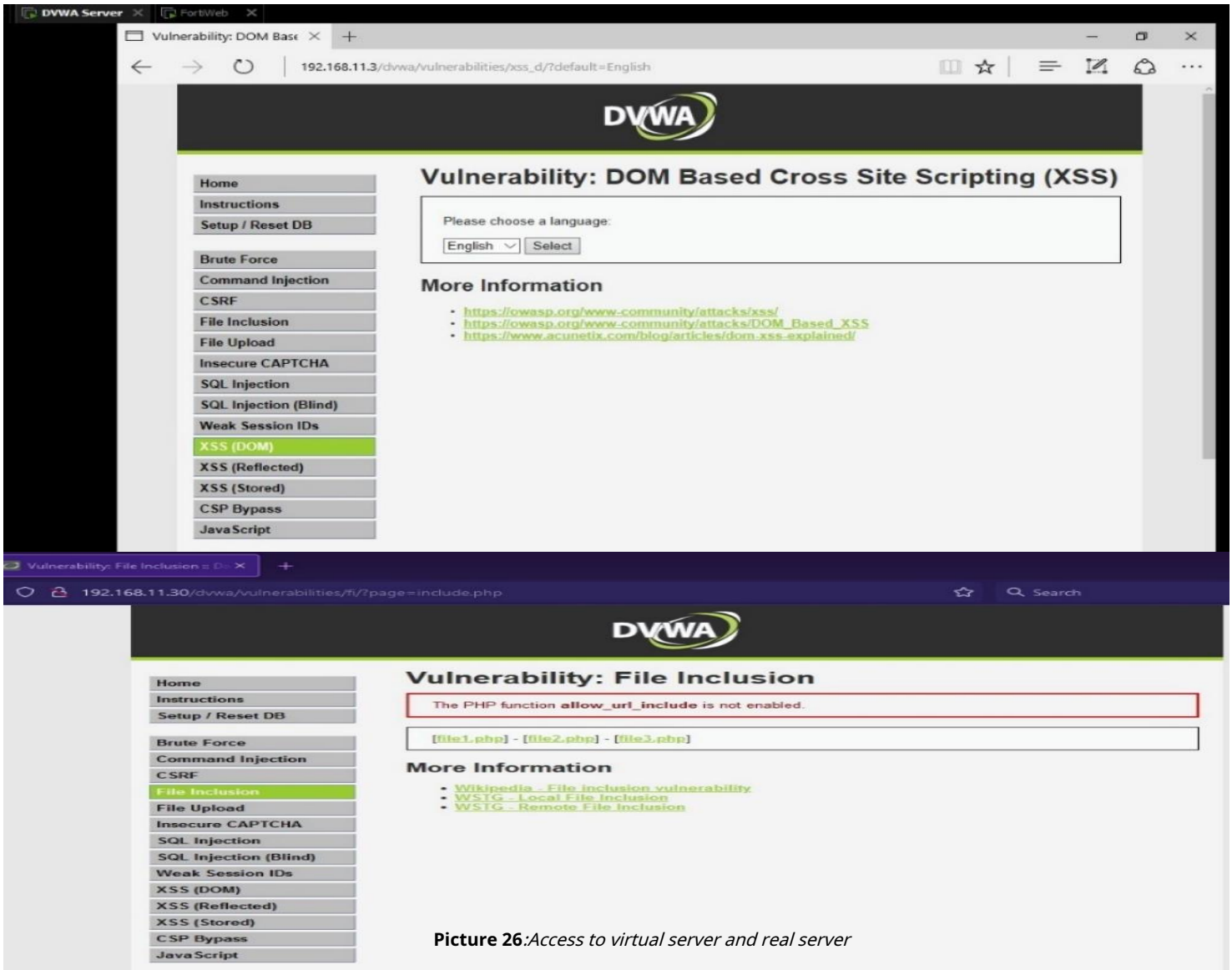
In what follows and as presented in the**figure 25**, I tried to connect to the virtual server using the web browser. In the first case, no alert or access denied occurred. But by inserting the extension /cmd.exe, the web page was blocked by the administrator since the user does not have access to this request.



Picture 25*:Virtual server connection test*

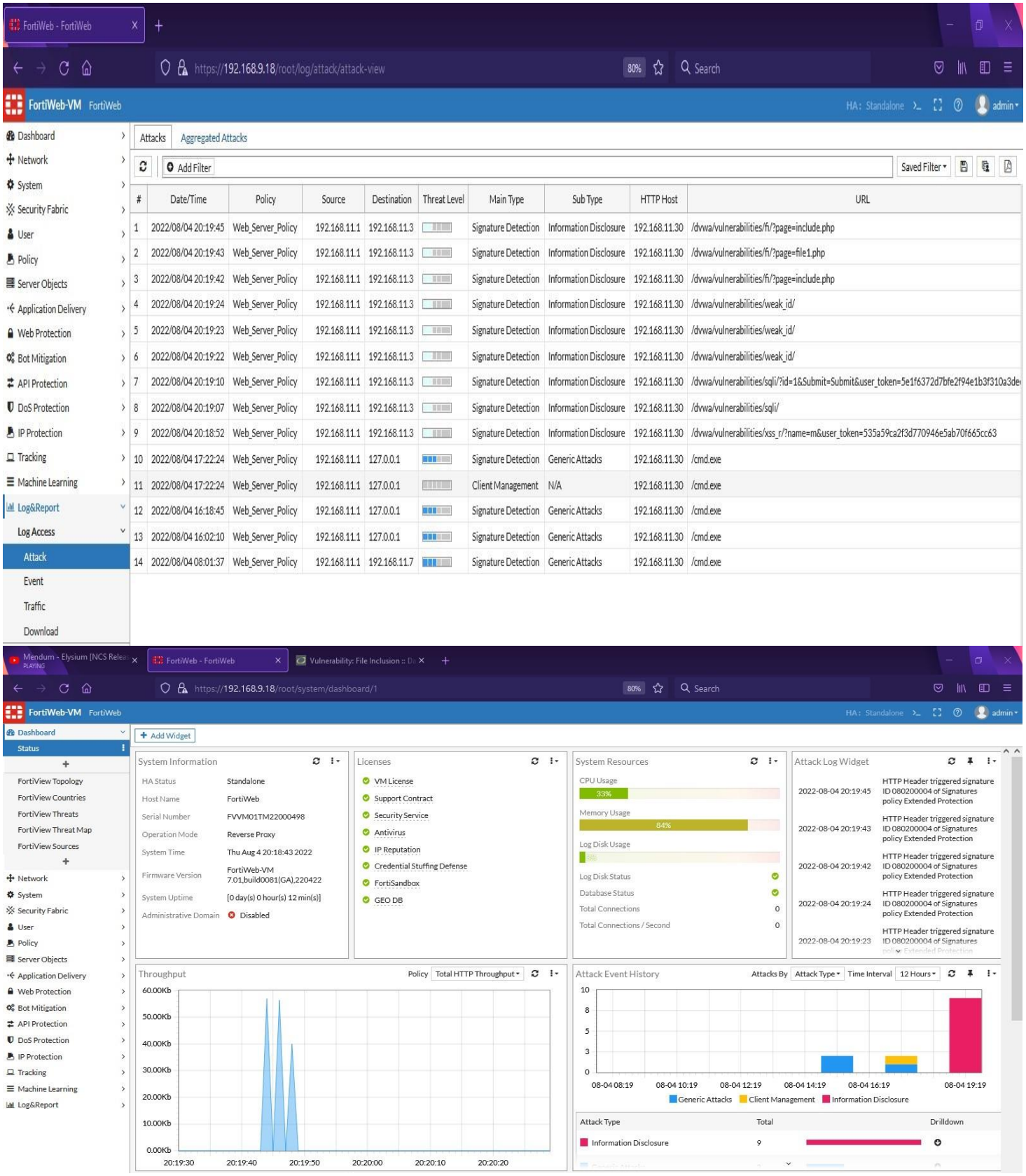
The second step was to install the DVWA software on the Windows 10 virtual machine and configure it so that this machine acts as a web server to test the various attacks. To start I had to install the apache http server software and start it then install the DVWA software and modify the ip address of the server in the "config.inc" file so that I can access this server from this address, I also had to change the username and password.

Now that everything was configured, I had to test access to the virtual server from my PC. The **figure 26**presents access to the virtual server as well as access to the DVWA server from the virtual machine.



Picture 26:*Access to virtual server and real server*

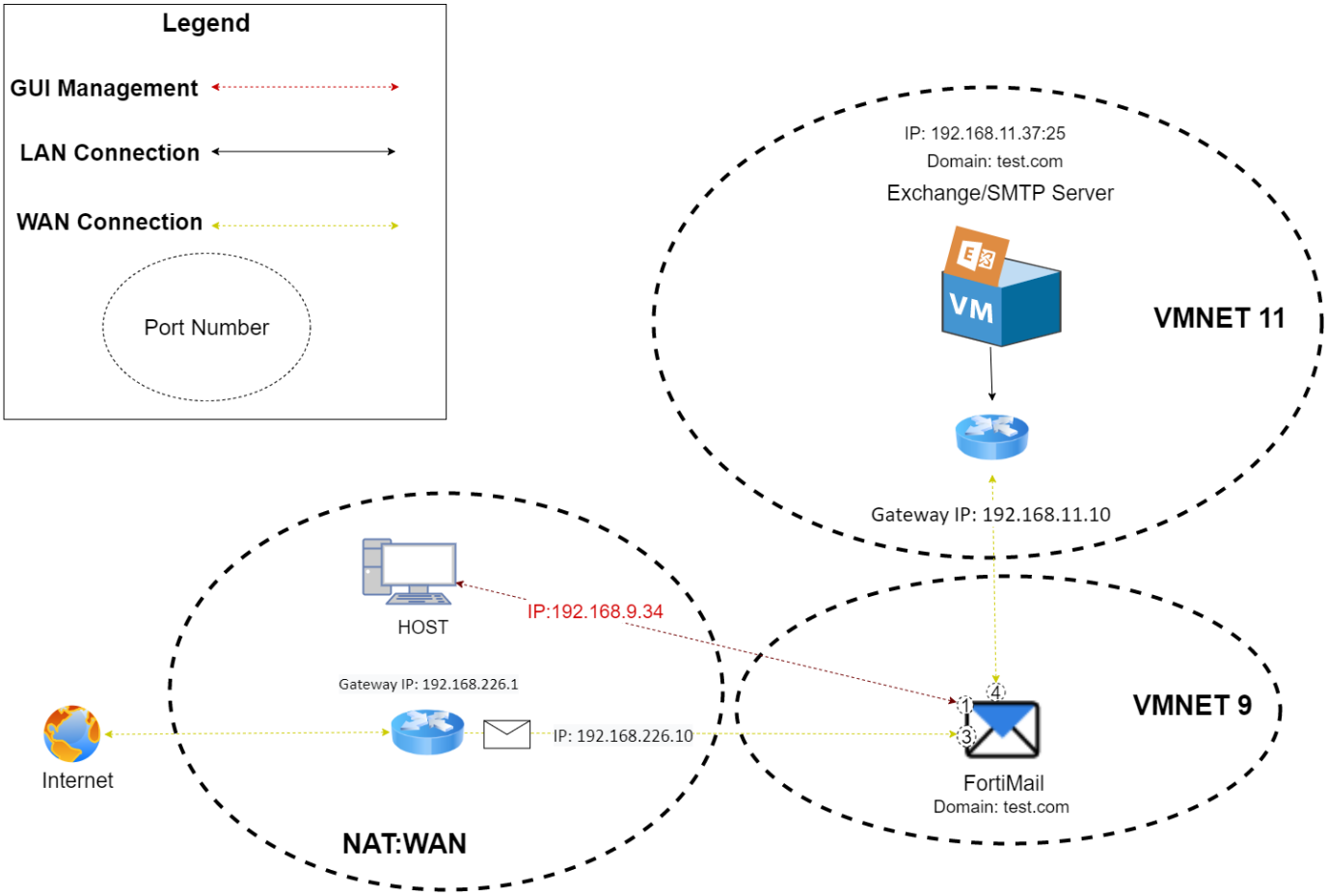
In order to test the effectiveness of FortiWeb, I applied several intrusions like cross-site Scripting (XSS) which allows an attacker to compromise user interactions with a vulnerable application, sql injection which can destroy the database, file inclusion that affects web applications relying on script runtime, weak session IDs that expose users to session hijacking. The**figure 27**confirms the safety test by the results obtained.



Picture 27:*Attack results*

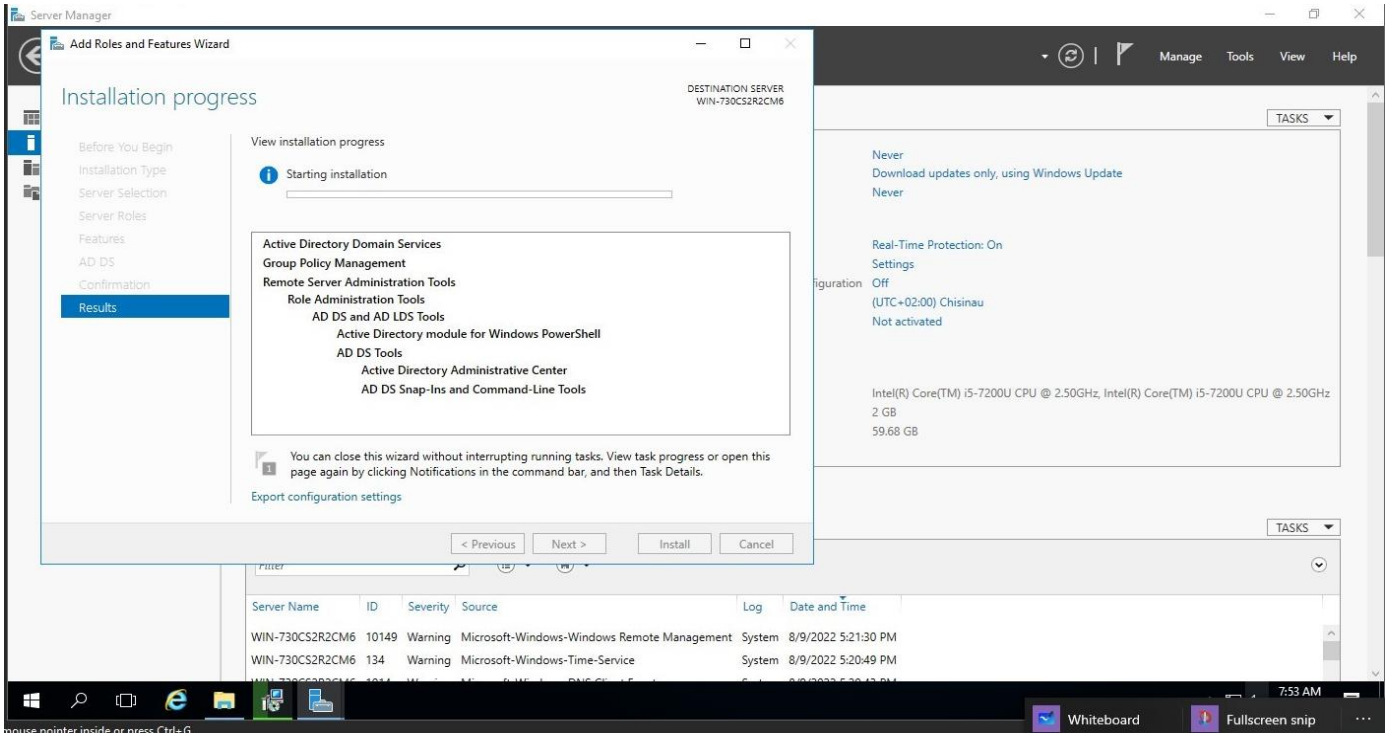
2.4.4. Implementation of the FortiMail mail firewall

FortiMail offers advanced multi-layered protection against email-borne threats. It prevents, detects and responds to email threats, including spam, phishing, malware and zero-day threats. In this network according to the**figure 28**, the fortiMail has the role of filtering emails and blocking certain emails according to different parameters.



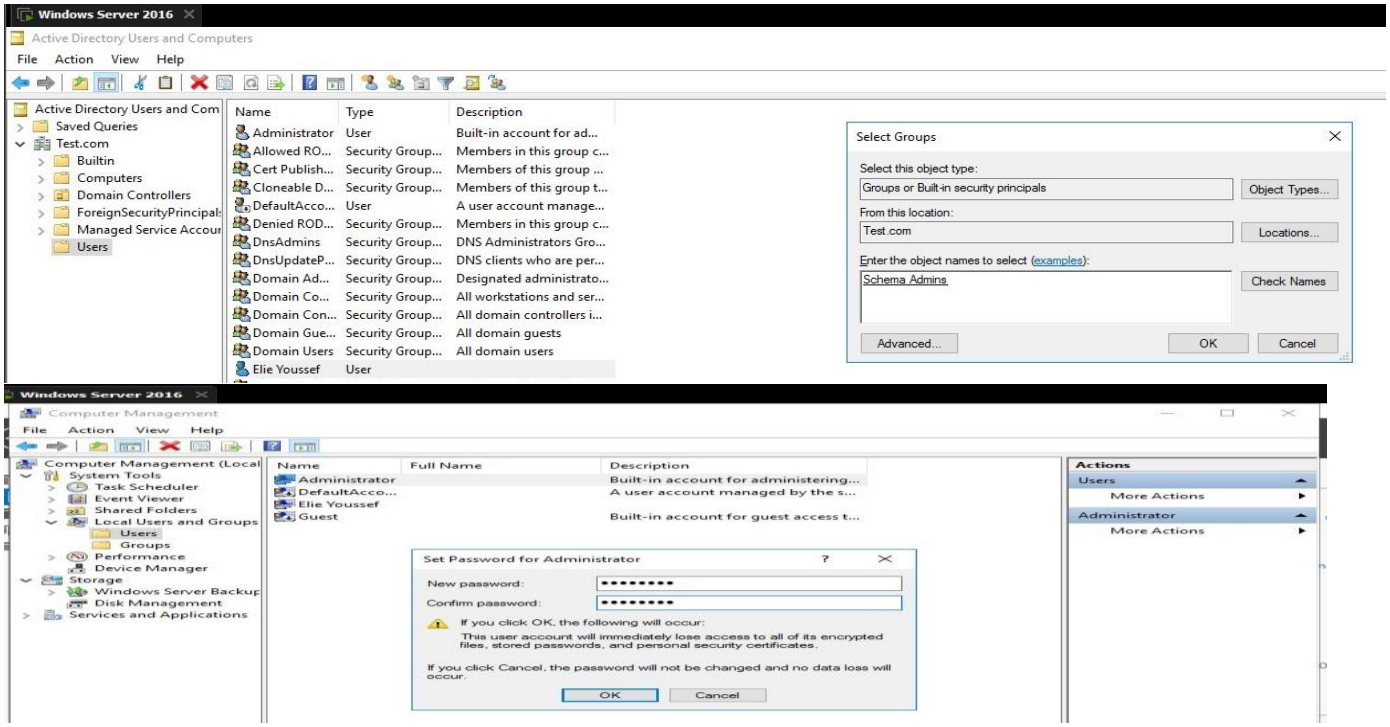
Picture 28*:FortiMail Network*

To achieve this task, it was necessary to implement a Microsoft exchange server in the Microsoft server 2016 virtual machine to provide the services and functionalities relating to server-side emails. According to this diagram, I had to send an email from my PC to the Exchange/SMTP server through the FortiMail which was to block this operation. Thus, and as done previously with all Fortinet virtual machines, I had to configure the device interfaces as indicated in the **figure 28**, with an ip management address of 192.168.9.34/24. The first step was to configure the Exchange server on the Windows Server 2016 virtual machine, this step consisted of several sub-steps. First of all, it was necessary to add the roles and the characteristics of the active directory domain as displayed in the**figure 29**.



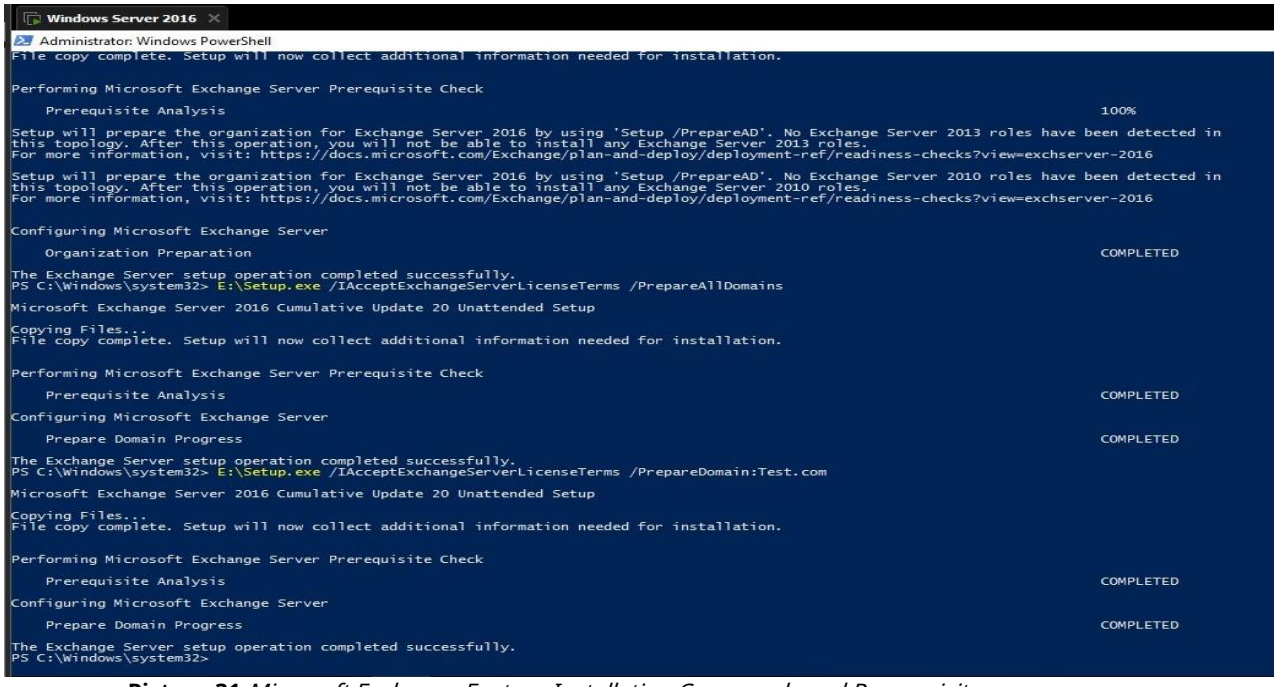
Picture 29:*Roles and Characteristics of the active directory domain*

It was necessary to add a root domain “Test.com” by adding a new forest in order to deploy this server. But an error occurred indicating that the user did not have the necessary privileges and that this same user was not part of the group allocated to this domain. To remedy this, I had to add a password to the user for more security and also add this same user to the "Schema Admins" and "Enterprise Admins" group as shown in the**figure 30**.



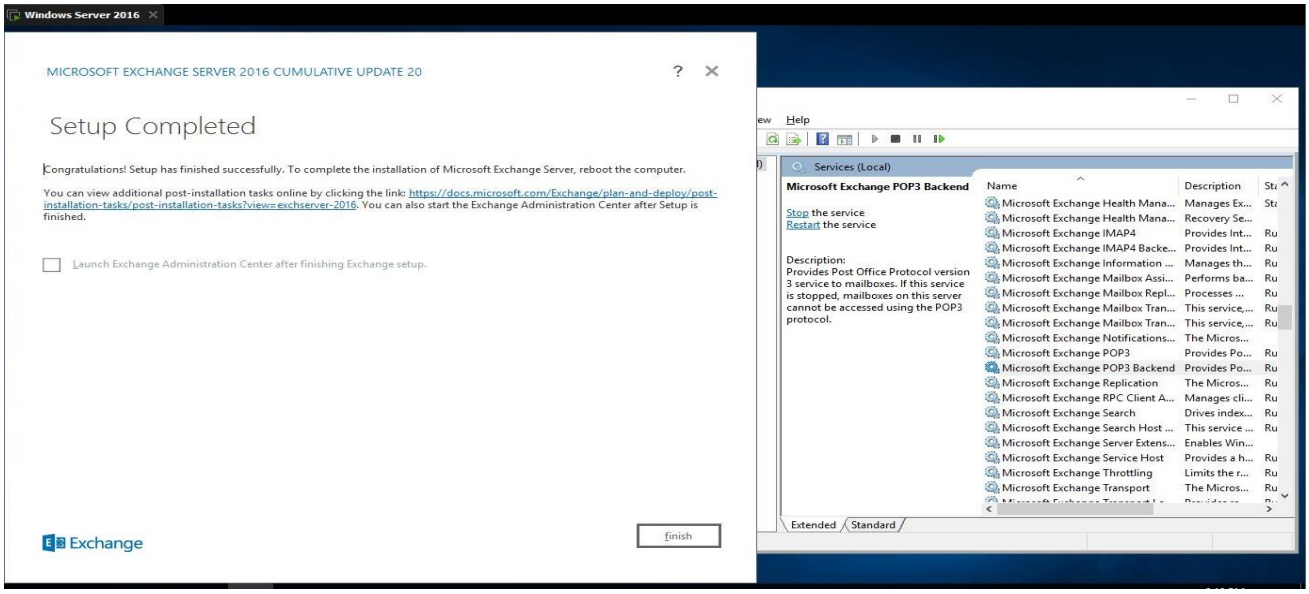
Picture 30:*Password and group configuration*

After creating this domain, one had to install the features and prerequisites of Microsoft Exchange server and assign it to this domain by installing the server prerequisites like "Microsoft .NET framework" and "Unified Communications Managed API Runtime" and entering the commands following on Windows PowerShell:
-**Install-WindowsFeature RSAT-ADDS:**install the remote server administration tools
-**Install-WindowsFeature AS-HTTP-Activation, Desktop-Experience, NET-Framework-45-Features, RPC-over-HTTP-proxy, RSAT-Clustering, RSAT-Clustering-CmdInterface, RSAT-Clustering-Mgmt, RSAT-Clustering-PowerShell , Web-Mgmt-Console, WAS-Process-Model, Web-Asp-Net45, Web-Basic-Auth, Web-Client-Auth, Web-Digest-Auth, Web-Dir-Browsing, Web-Dyn-Compression, Web -Http-Errors, Web-Http-Logging, Web-Http-Redirect, Web-Http-Tracing, Web-ISAPI-Ext, Web-ISAPI-Filter, Web-Lgcy-Mgmt-Console, Web-Metabase, Web-Mgmt -Console, Web-Mgmt-Service, Web-Net-Ext45, Web-Request-Monitor, Web-Server, Web-Stat-Compression, Web-Static-Content, Web-Windows-Auth, Web-WMI, Windows-Identity -Foundation:** install the various server features.
- E:\Setup.exe /IAcceptExchangeServerLicenseTerms /PrepareAllDomains: Prepare all areas
As observed in the**figure 31**.



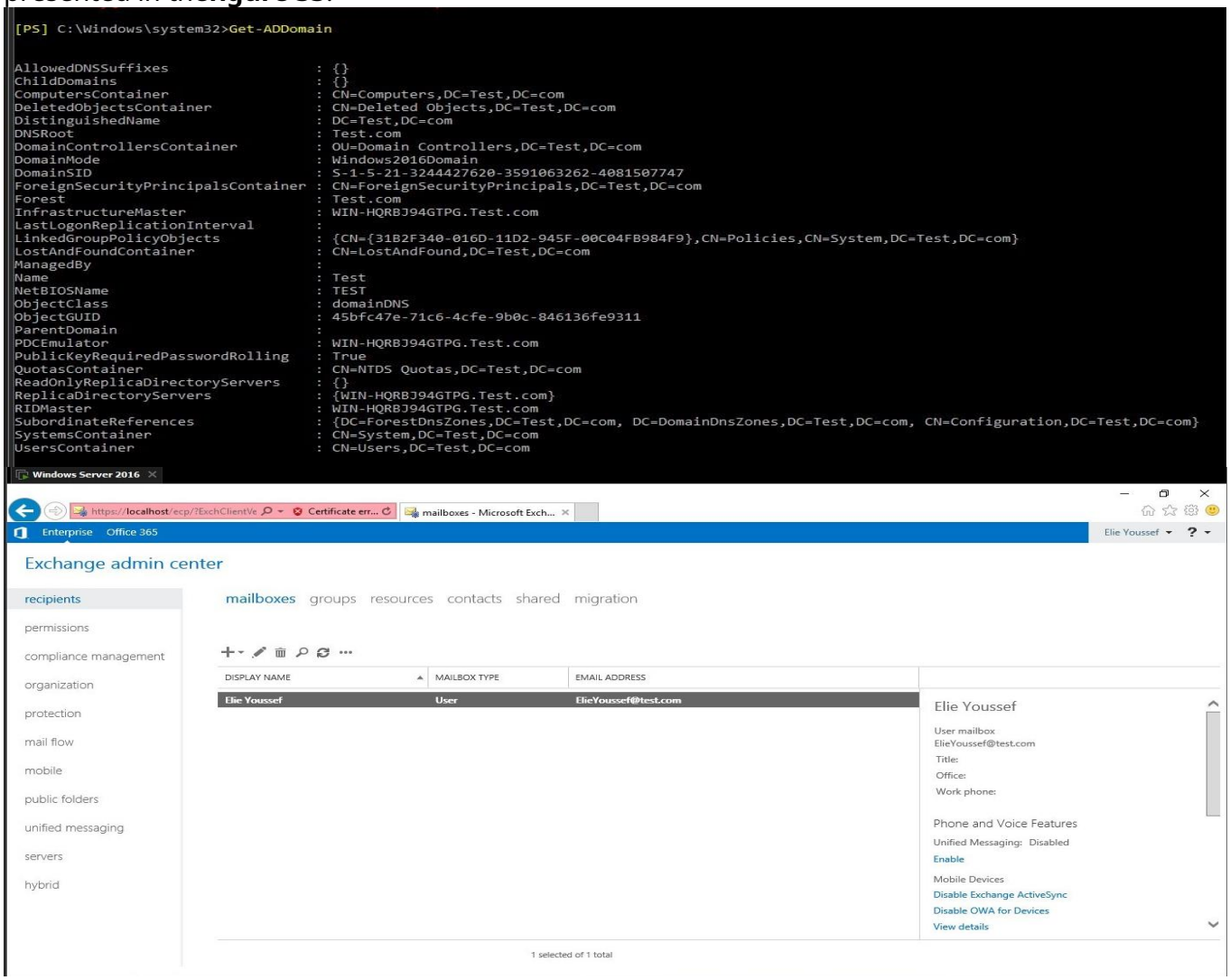
Picture 31*:Microsoft Exchange Feature Installation Commands and Prerequisites*

Now that all the prerequisites were installed and ready, it was time to install the Microsoft Exchange Server and assign it to this domain. But during this installation, a common problem occurred at the last step, when it was time to start this server an error occurred and forced me to redo all these configurations from the beginning. This problem was caused by the automatic stop of all services related to this server during the last step which caused the installation to not finish. To remedy this, I had to start the services concerning the Exchange Server with the last installation step which resulted in the successful installation of the server according to the**figure 32**.



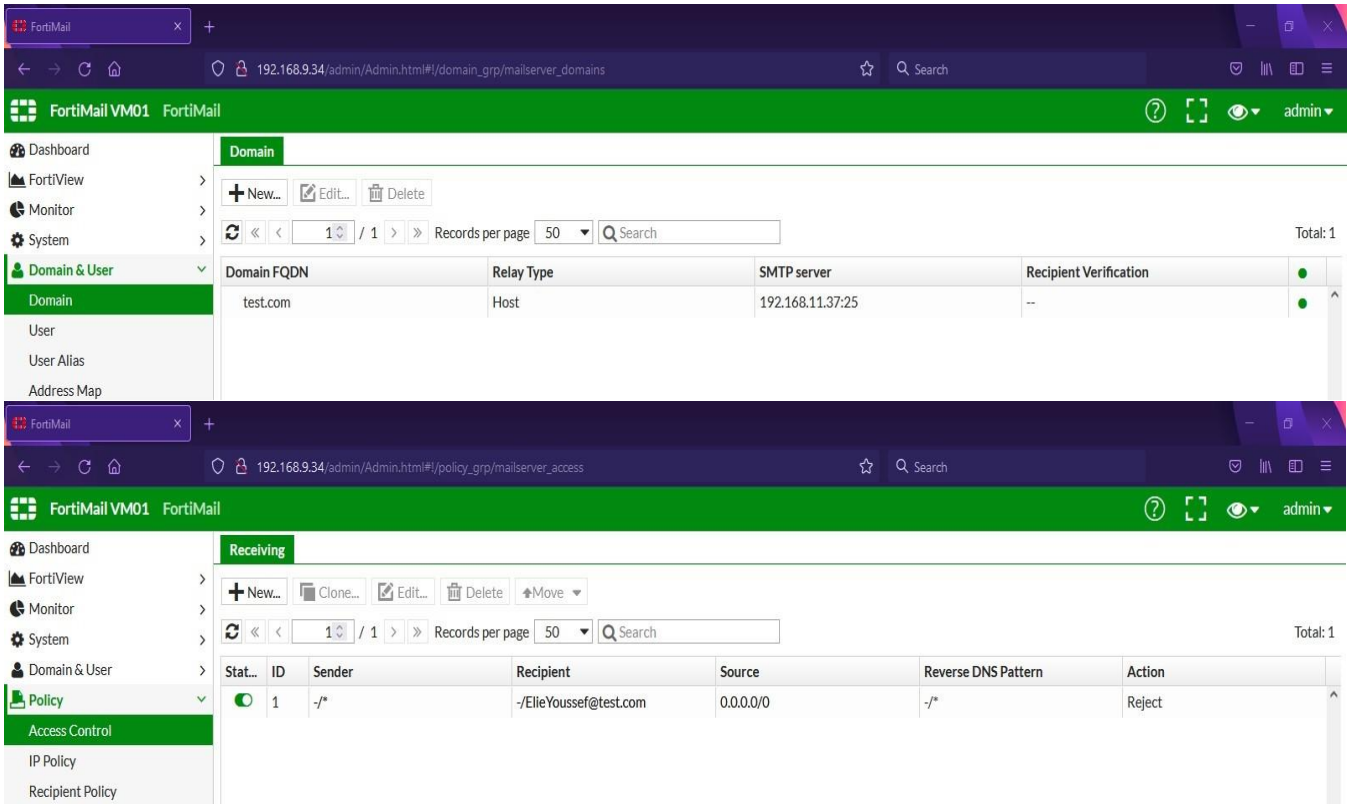
Picture 32*:Successful installation of the Exchange server as well as the start of the services connected to this server*

The domain information as well as the user account created on Microsoft Exchange are presented in the**figure 33**.



Picture 33*:Domain information as well as the user account created on Microsoft Exchange*

On the FortiMail side, it was necessary to configure the "test.com" domain so that it corresponded to the same domain as the server with an ip address 192.168.11.37 (port 25 ->email) and applied an access control policy which rejects any email from any source with a recipient " ElieYoussef@test.com " corresponding to the SMTP/Exchange server as indicated in the**figure 34**.



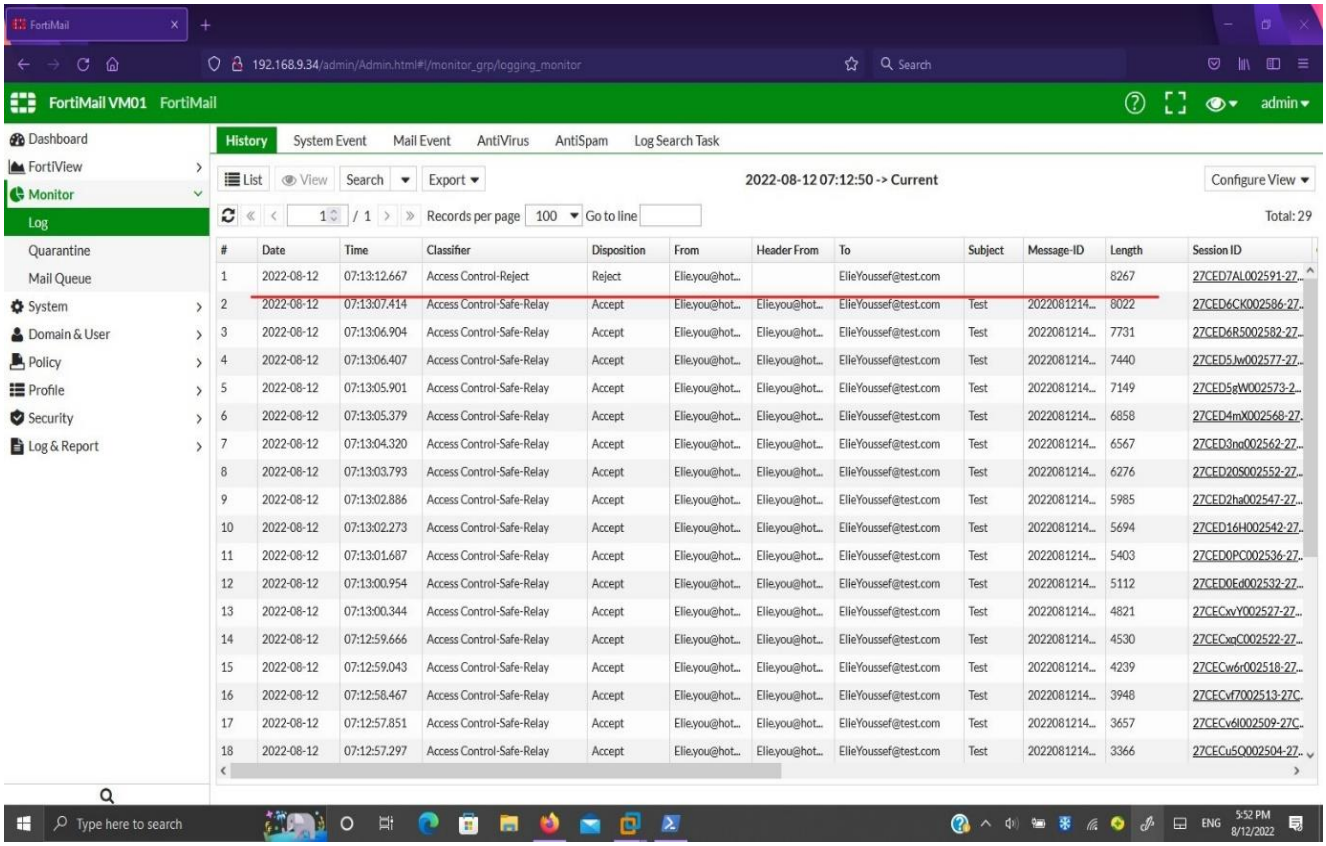
Picture 34*:Configuring the domain on FortiMail and the access control policy*

Finally, the FortiMail had to be tested by sending an email to the server user to ensure that the email would not be sent. To achieve this, it was necessary to send on PowerShell the command **Send-MailMessage -SmtpServer 192.168.11.37**from the address Elie.you@hotmail.com to ElieYoussef@test.com . According to the message received in PowerShell and the logs present on FortiMail shown in the**figures 35, 36 and 37**, the email rejection operation is successful.

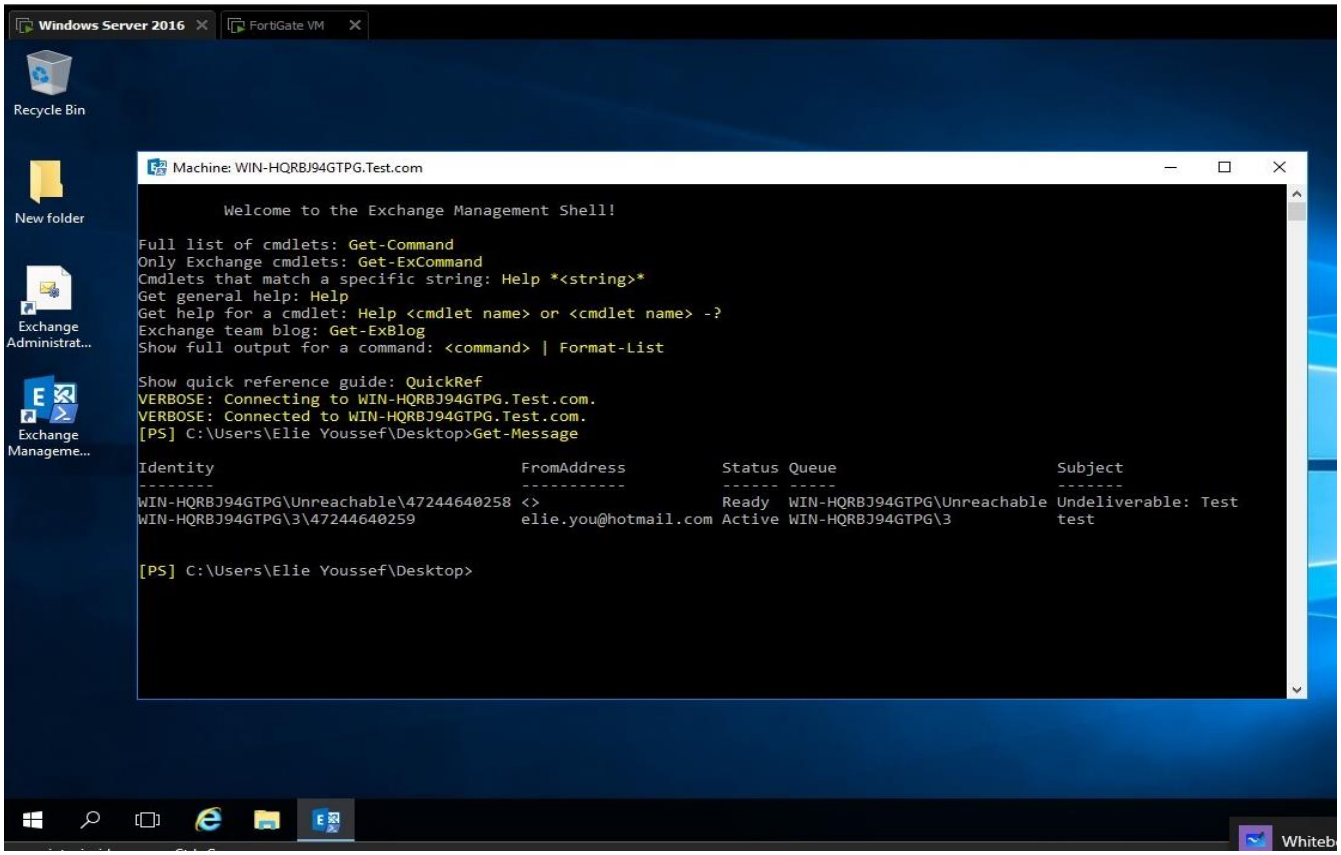
```
PS C:\Users\Elie Youssef> Send-MailMessage -SmtpServer 192.168.11.37

cmdlet Send-MailMessage at command pipeline position 1
Supply values for the following parameters:
From: Elie.you@hotmail.com
Subject: test
To[0]: ElieYoussef@test.com
To[1]:
Send-MailMessage : Unable to read data from the transport connection: net_io_connectionclosed.
At line:1 char:1
+ Send-MailMessage -SmtpServer 192.168.11.37
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : InvalidOperation: (System.Net.Mail.SmtpClient:SmtpClient) [Send-MailMessage], SmtpExcept
   ion
    + FullyQualifiedErrorId : SmtpException,Microsoft.PowerShell.Commands.SendMailMessage
```

Picture 35*:Send email and message of failure of this operation*



Picture 36:*Logs of emails traversed on FortiMail*



Picture 37:*Exchange Server Email Inbox*

As noted from the**figure 37,**the Exchange Server email inbox does not contain the rejected email. For information, the other emails present in the FortiMail logs are test emails that have been accepted.

SUMMARY

This chapter presented an overview of the observations made as well as the tools used at Cirrus. In addition, he discussed the multiple tasks performed to which I was assigned, including the manipulation of the various Fortinet components such as FortiGate, FortiADC, FortiWeb and FortiMail which all provide network protection and security. The following chapter will describe the evaluation of the course performed.

CHAPTER 3: INTERNSHIP EVALUATION

3.1 INTRODUCTION

The last chapter of this report presents the personal evaluation of this course. The following consists of the evaluation of the tasks carried out during the internship, the technical difficulties encountered and the solutions proposed to remedy them. Likewise, the new notions learned as well as the applied knowledge and the evaluation of the working atmosphere within the company. Finally, I will end this chapter with a summary.

3.2 ASSESSMENT

Evaluation of the work done during the internship

As an intern at Cirrus, my expectations were to apply my knowledge acquired during my university career in the professional world and to increase it even more. Indeed, from the first days, all the work done before my eyes aroused my attention and my curiosity, which led me to ask lots of questions in order to immerse myself more and more in this new environment as well as to strengthen professional relationships with employees. By carrying out the tasks requested by my internship supervisor and where it required a conversation with him to clarify a few points, I kept a humble attitude and remained open to any instructions or recommendations that would improve my performance. In addition, I was able to work in partnership with the Cloud network administrator in order to accomplish a few tasks, an opportunity that allowed me to learn from his expertise and his advice in order to carry out my work, on the other hand I was also able to share with him my knowledge and my experience in the concepts and applications used that I had already acquired and mastered thanks to the university. Moreover, I knew how to keep my cool during the problems covered while keeping a critical thought by applying the objectives set in order to demonstrate that I am able to become a real engineer. Thus, all the work done during this internship brought me closer and closer to the professional world and prepared me to face future on the other hand I was also able to share with him my knowledge and my experience in the concepts and applications used that I had already acquired and mastered thanks to the university. Moreover, I knew how to keep my cool during the problems covered while keeping a critical thought by applying the objectives set in order to demonstrate that I am able to become a real engineer. Thus, all the work done during this internship brought me closer and closer to the professional world and prepared me to face future on the other hand I was also able to share with him my knowledge and my experience in the concepts and applications used that I had already acquired and mastered thanks to the university. Moreover, I knew how to keep my cool during the problems covered while keeping a critical thought by applying the objectives set in order to demonstrate that I am able to become a real engineer. Thus, all the work done during this internship brought me closer and closer to the professional world and prepared me to face future

obstacles, not to mention the discovery of a new work environment filled with regulations and new work approaches.

Possible proposed improvements

Before starting this internship, I had set myself objectives that I had to achieve in terms of knowledge and technical skills acquired during this new experience. Indeed, and thanks to the tasks carried out, I was able to further develop my technical skills and therefore achieve the objectives set by myself and by my internship supervisor. However, there are some possible improvements that I would have liked to propose to the tasks performed, such as working on physical models such as switches or routers and configuring them manually and not only working with virtual components and machines.

Technical difficulties encountered and proposed solutions

During this internship, I was certainly confronted with several difficulties techniques when carrying out the required tasks. These difficulties are due to the lack of practice and experience with cloud networking components such as FortiGate, FortiADC, FortiWeb or FortiMail... Indeed, during the first weeks I had to familiarize myself with these components and configure them using virtual machine configured on VMWare Workstation, Despite reading the instructive documents and searching the web, I was finding difficulty in connecting the network components together. After consultation with my tutor who first advised me to make the network diagrams in order to see the problem from another angle and after several tries, I managed to connect all the network components together. One of the technical difficulties I encountered the most was the slowness of the virtual machines since I had to start 3 or 4 machines at the same time with 2-3 GB of memory each, which made the work difficult and stressful at times and in order to to fix it I either had to turn off one or two machines or turn my computer back on and start over again. Despite these technical difficulties that I had to face, I

I always kept my cool and a never-give-up attitude because I knew I could overcome them with the help of my knowledge.

Evaluation of the working atmosphere and degree of integration

From the first day, the Cirrus team welcomed me very well and considered me like a member of the team. Despite a stressful first period where I found it difficult to adapt, the team members supported me by using humor and motivation, something that allowed me to form professional and friendly relationships with some and which allowed me to move forward. I noticed that the team is really united and that when a problem arose, they did not hesitate to help each other. Same thing for me, in case of absence of my internship supervisor and in case of difficulty and even if they had different technical backgrounds and specializations, they always came to help me with their experience in the field. Regarding my degree of integration, I had set myself the objective from the first day of the course to improve myself and to benefit as much as possible from this experience. This is why I always kept smiling with a serious and friendly attitude in order to get closer to the members of the team and carry out the various tasks requested. Moreover, with each task accomplished, I motivated myself more and more to give the best of myself and after seeing the seriousness of the employees in their work, I felt like a duty towards my internship supervisor and the team of Cirrus to work seriously.

Assessment of applied knowledge and new learning

During my university career, I had the opportunity to learn several notions and concepts acquired thanks to the courses of Cisco, Networks Architecture, Theory of operating systems, Proprietary systems... which proved useful during my internship. As a network trainee, I was able to apply all the notions relating to networks that I learned using the VMWare Workstation software, which I learned to use thanks to the Theory of operating systems course. I configured IP addresses, interfaces and other attributes of network components while running commands like ping or tracert on cmd to test connections. But also, thanks to this internship, I was able to learn new notions in a field that is not very familiar to me, which is Cyber Security. I was introduced to Fortinet which is a company that develops solutions in this area such as firewalls,

It is worth mentioning the different components I was able to work on such as FortiGate which is a Next Generation Firewall, FortiADC which is an Advanced Delivery Controller, FortiWeb being a firewall designed for Web pages and finally FortiMail being a firewall that filters emails. On a personal level, I improved my communication skills while being responsible, persevering, autonomous and never giving up before completing the tasks requested.

SUMMARY

This chapter presented the improvements to the proposed tasks, the solutions to the difficulties encountered during the performance of the work, as well as the evaluation of the internship performed. Thanks to this experience, I was able to increase my technical skills and personal traits while applying the knowledge already acquired during my academic training.

CONCLUSION

This internship as a network intern took place from June 20 until August 31, 2022 equivalent to 11 weeks within the Cirrus company and this at the rate of 7 hours a day. The purpose of this internship was to familiarize myself with the professional and practical world and apply my already acquired knowledge while improving it and learning new concepts.

During this internship, I was able to immerse myself in the world of cloud networking and discover its multiple services. And this, while observing the work team and applying the tasks assigned to me in relation to cyber security and Fortinet firewall components.

Not only was I able to further develop my networking skills, I also improved my interrelationship and professional skills with team members. I also had the chance to have a taste of the job market and to live this new experience which will surely help me in my future professional stage.

Finally, I was able to realize that no member of the team can work alone, it takes full cooperation with all members in order to aspire to achieve the expected results.

BIBLIOGRAPHIC REFERENCES

[1] Cirrus | Cloud Services [online]. Available on :https://www.cirrus-me.com/ (07/25/2022).

[2] FortiGate Administrative Guide [in line]. Available on : https://docs.fortinet.com/document/fortigate/7.0.3/administration-guide/777334 (25/06/2022).

[3] FortiADC Administrative Guide [in line]. Available on : https://docs.fortinet.com/document/fortiadc/7.0.1/handbook/105358/introduction (04/07/2022).

[4] FortiWeb Administrative Guide [in line]. Available on : https://docs.fortinet.com/document/fortiweb/7.0.0/administration-guide (23/07/2022).

[5] FortiMail Administrative Guide [in line]. Available on : https://docs.fortinet.com/document/fortimail/7.2.0/administration-guide (02/08/2022).

[6] Microsoft Exchange Server Prerequisites [online]. Available on: https://docs.microsoft.com/en-us/exchange/plan-and-deploy/prerequisites?view=exchserver-2016 (04/08/2022).

LIST OF FIGURES

LIST OF PAINTINGS

ABREVIATIONS LIST

APIs	Application Programming Interface
AV	Anti-virus
CLI	Command Line Interface
DDoS	Distributed Denial of Service
MISTLETOE	Graphical User Interface
HA	High Availability
HTTP	Hypertext Transfer Protocol
IPs	Internet-Protocol
MPLS	Multiprotocol Label Switching
FVO	Open Virtualization Format
OWASP	Open Web Application Security Project
PHP	Hypertext Preprocessor
SDN	Software-Defined Networking
SD-WAN	Software-Defined Networking Wide Area Network
SMTP	Simple Mail Transfer Protocol
SQL	Structured Query Language
VMNET	Virtual Machine Network
WAF	Web Application Firewall