|  |
| --- |
| Cybersecurity |
| Project 1 Technical Brief |

Make a copy of this document before you begin. Place your answers below   
each question. This completed document will be your deliverable for Project 1. Submit it through Canvas when you’re finished with the project at the end of the week.

## Your Web Application

Enter the URL for the web application that you created:

|  |
| --- |
| https://rpwebapp.info/ |

## Day 1 Questions

### General Questions

1. What option did you select for your domain (Azure free domain, GoDaddy low-cost domain, Azure premium domain)?

|  |
| --- |
| GoDaddy low-cost domain |

1. What is your domain name?

|  |
| --- |
| rpwebapp.info |

### Networking Questions

1. What is the IP address of your webpage?

|  |
| --- |
| 20.48.202.160 |

1. What is the location (city, state, country) of your IP address?

|  |
| --- |
| Sudbury, ON, Canada Central |

1. Run a DNS lookup on your website. What does the NS record show?

|  |
| --- |
|  |

### Web Development Questions

1. When creating your web app, you selected a runtime stack. What was it? Does it work on the front end or the back end?

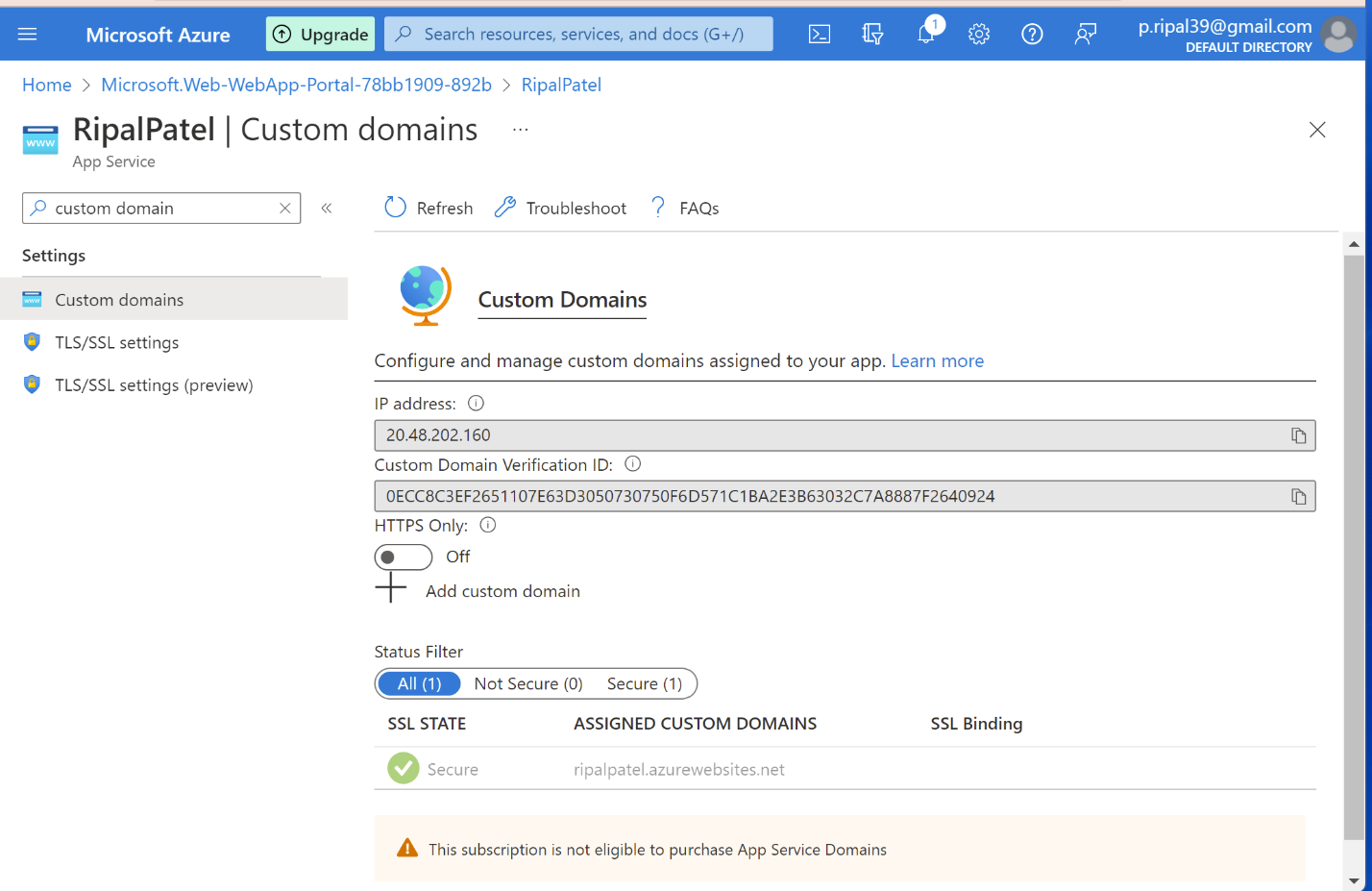
|  |
| --- |
| PHP 7.4 (LAMP STACK). It is the software stack responsible for installing your application code and its dependencies and running your application.  It works on back-end server. |

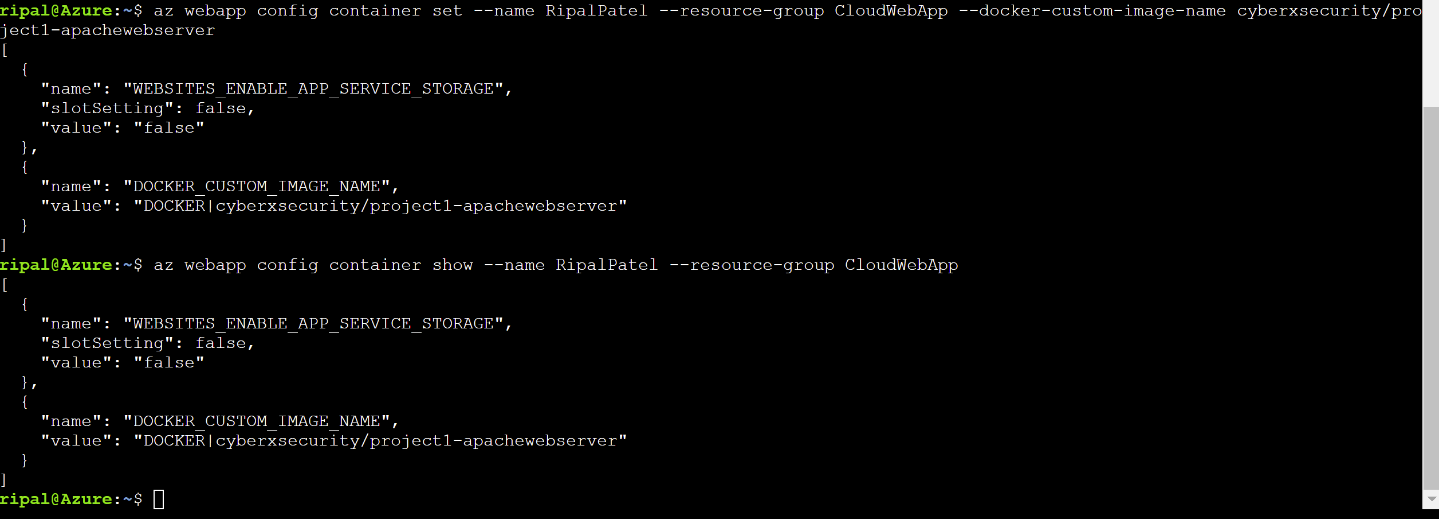
1. Inside the /var/www/html directory, there was another directory called assets. Explain what was inside that directory.

|  |
| --- |
| In assets directory there is another directory called css and inside it there is file called style.css. In this file there are properties for how to display HTML elements. It defines the size, color, font, line spacing, indentation, borders, and location of HTML elements. |

1. Consider your response to the above question. Does this work with the front end or back end?

|  |
| --- |
| It works with front-end. |





## 

## Day 2 Questions

### Cloud Questions

1. What is a cloud tenant?

|  |
| --- |
| A tenant is the organization that owns and manages a specific instance of Microsoft cloud services. It is most often used to refer to the set of Azure and Microsoft 365 services for an organization. |

1. Why would an access policy be important on a key vault?

|  |
| --- |
| A Key Vault access policy determines whether a given security principal, namely a user, application, or user group, can perform different operations on Key Vault secrets, keys and certificates. |

1. Within the key vault, what are the differences between keys, secrets, and certificates?

|  |
| --- |
| Keys: it involves cryptographic material imported into Key Vault or generated when a service requests the Key Vault to do so. An authorized cloud service can request the Key Vault perform one or more cryptographic operations with a key on its behalf.  Secrets: it is any sequence of bytes under 10 kb like connection strings, account keys, or the passwords for PFX. And authorized application can retrieve a secret for use in its operation.  Certificates: it is simply a managed X.509 certificate.  When Azure Key Vault creates the certificate, it creates a related private key and password. The password is stored as an Azure Secret while the private key is stored as an Azur Key. Expired certificates can roll over with notifications before these operations happen. |

### Cryptography Questions

1. What are the advantages of a self-signed certificate?

|  |
| --- |
| Self-signed certificates are free. They are suitable for internal network websites and development/testing environments. Encryption and Decryption of the data is done with the same ciphers used by paid SSL certificates. |

1. What are the disadvantages of a self-signed certificate?

|  |
| --- |
| Self-signed Certificates are risky because they have no validation from a third-party authority, which is usually a Trusted SSL Certificate Company. Developers and businesses try to save money by using or creating a free Self-Signed SSL Certificate. |

1. What is a wildcard certificate?

|  |
| --- |
| The wildcard certificate is a public key certificate which can be used with multiple sub-domains of a domain. |

1. When binding a certificate to your website, Azure only provides TLS versions 1.0, 1.1, and 1.2. Explain why SSL 3.0 isn’t provided.

|  |
| --- |
| SSL 3.0 has a flaw that could allow an attacker to decrypt information, such as authentication cookies, according to Microsoft. It has security issues that is why it is not provided. |

1. After completing the Day 2 activities, view your SSL certificate and answer the following questions:
   1. Is your browser returning an error for your SSL certificate? Why or why not?

|  |
| --- |
| No. It because of the certificate is trusted. |

* 1. What is the validity of your certificate (date range)?

|  |
| --- |
| 2022-06-22 to 2022-12-23 |

* 1. Do you have an intermediate certificate? If so, what is it?

|  |
| --- |
| Yes. GeoTrust Global TLS RSA4096 SHA256 2022 CA1 |

* 1. Do you have a root certificate? If so, what is it?

|  |
| --- |
| Yes. DigiCert |

* 1. Does your browser have the root certificate in its root store?

|  |
| --- |
| Yes. |

* 1. List one other root CA in your browser’s root store.

|  |
| --- |
| Certum CA |

## 

## Day 3 Questions

### Cloud Security Questions

1. What are the similarities and differences between Azure Web Application Gateway and Azure Front Door?

|  |
| --- |
| Azure Front Door WAF and Azure Web App Gateway WAF are very similar in functionality. The main difference is Azure Front Door applies the WAF filters at edge locations, way before it gets to the datacenter. App Gateway applies the filter when it enters your VNET via the App Gateway. So basically, Front Door is a non-regional service whereas App Gateway is a regional service. |

1. A feature of the Web Application Gateway and Front Door is “SSL Offloading.” What is SSL offloading? What are its benefits?

|  |
| --- |
| SSL Offloading is the process of removing the ssl based encryption from incoming traffic that a web server receives to relives it from decryption of data. The device completes the hands shaking of SSL quicker than the web server. This results in smooth loading of the website and faster processing of requests at the end of the web application. |

1. What OSI layer does a WAF work on?

|  |
| --- |
| Layer 7 |

1. Select one of the WAF managed rules (e.g., directory traversal, SQL injection, etc.), and define it.

|  |
| --- |
| RCE (Remote Code Execution)  It is also known as Arbitrary Code Execution, is a concept that describes a form of a cyberattack in which the attacker can solely command the operation of another person’s computing device or computer. RCE takes place when malicious malware is downloaded by the host. It is a phenomenon that can affect a person regardless of the present location of his or her device. |

1. Consider the rule that you selected. Could your website (as it is currently designed) be impacted by this vulnerability if Front Door wasn’t enabled? Why or why not?

|  |
| --- |
| It would affect my website if this vulnerability was not enabled. Let’s say old apache version has some malicious codes injected in it and it has access to my website and my jumpbox. If I am not blocking RCE for that old apache server then someone can easily have access to my website through running the apache codes and it can damage my website. So, it is good practice to block unused servers through RCE. |

1. Hypothetically, say that you create a custom WAF rule to block all traffic from Canada. Does that mean that anyone who resides in Canada would not be able to access your website? Why or why not?

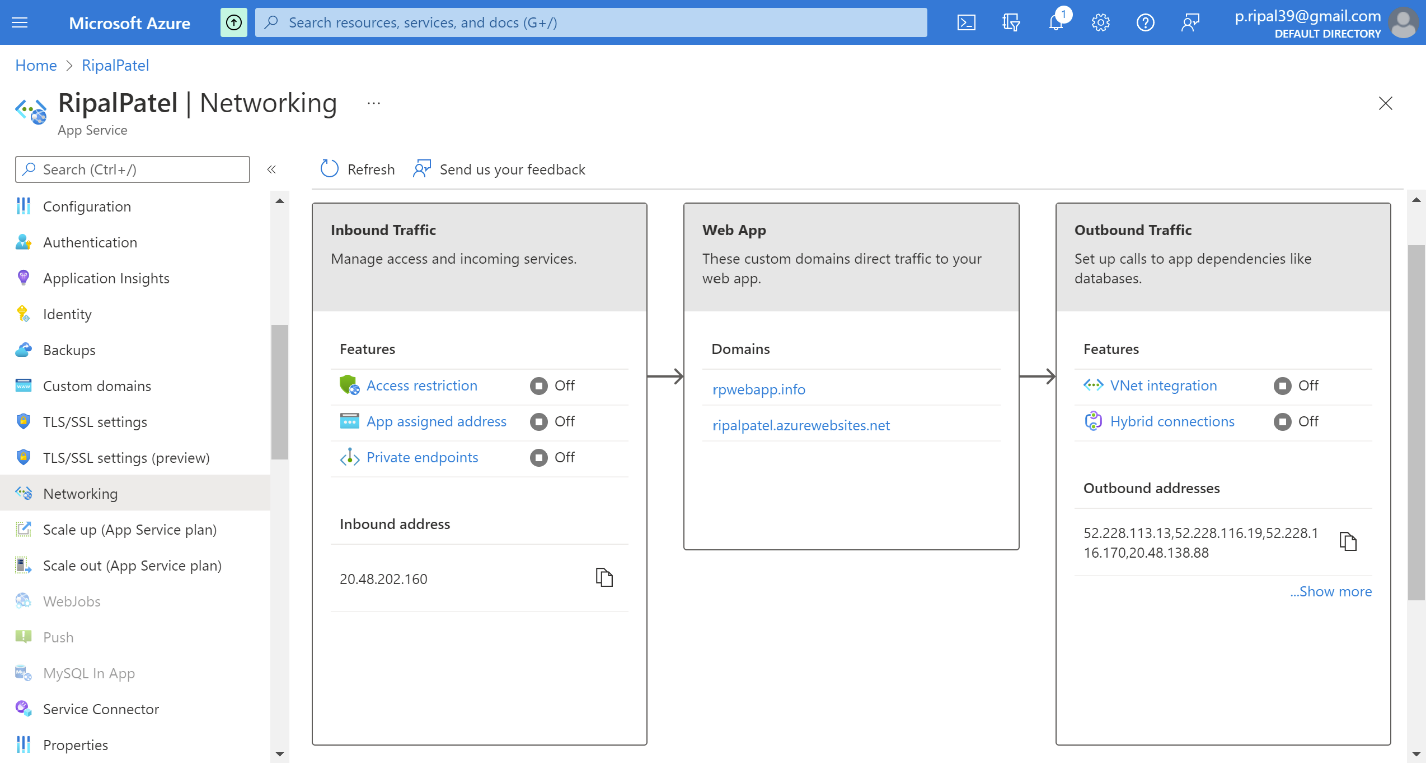
|  |
| --- |
| True. Because I am blocking all the incoming traffic from Canada with custom created WAF rule, no one can access my website from Canada. |

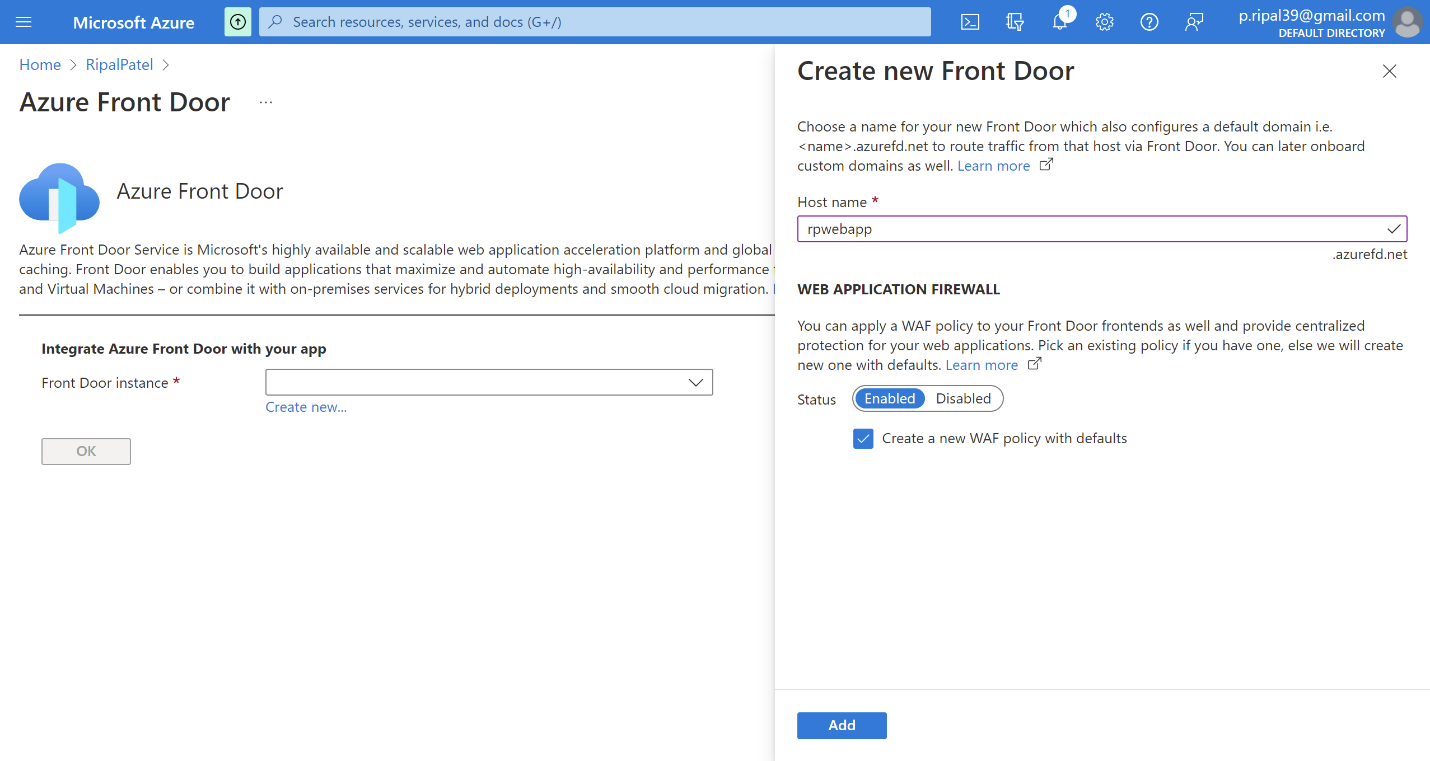
1. Include screenshots below to demonstrate that your web app has the following:
   1. Azure Front Door enabled

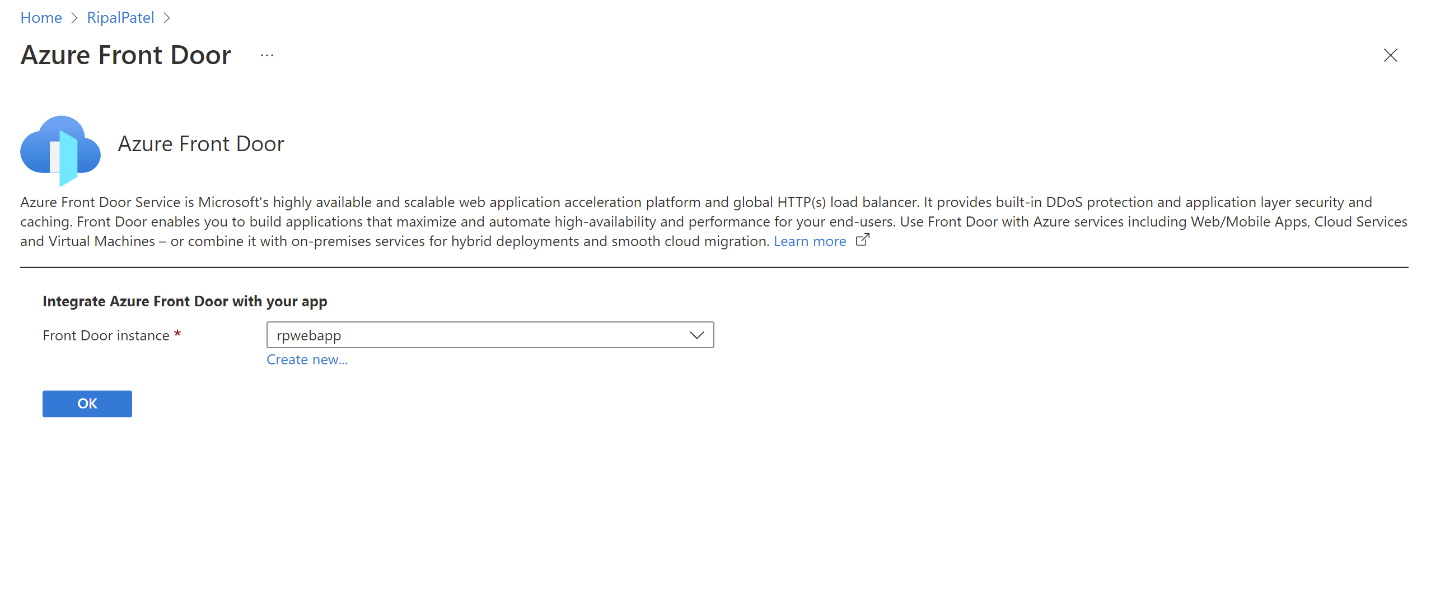
|  |
| --- |
|  |

* 1. A WAF custom rule

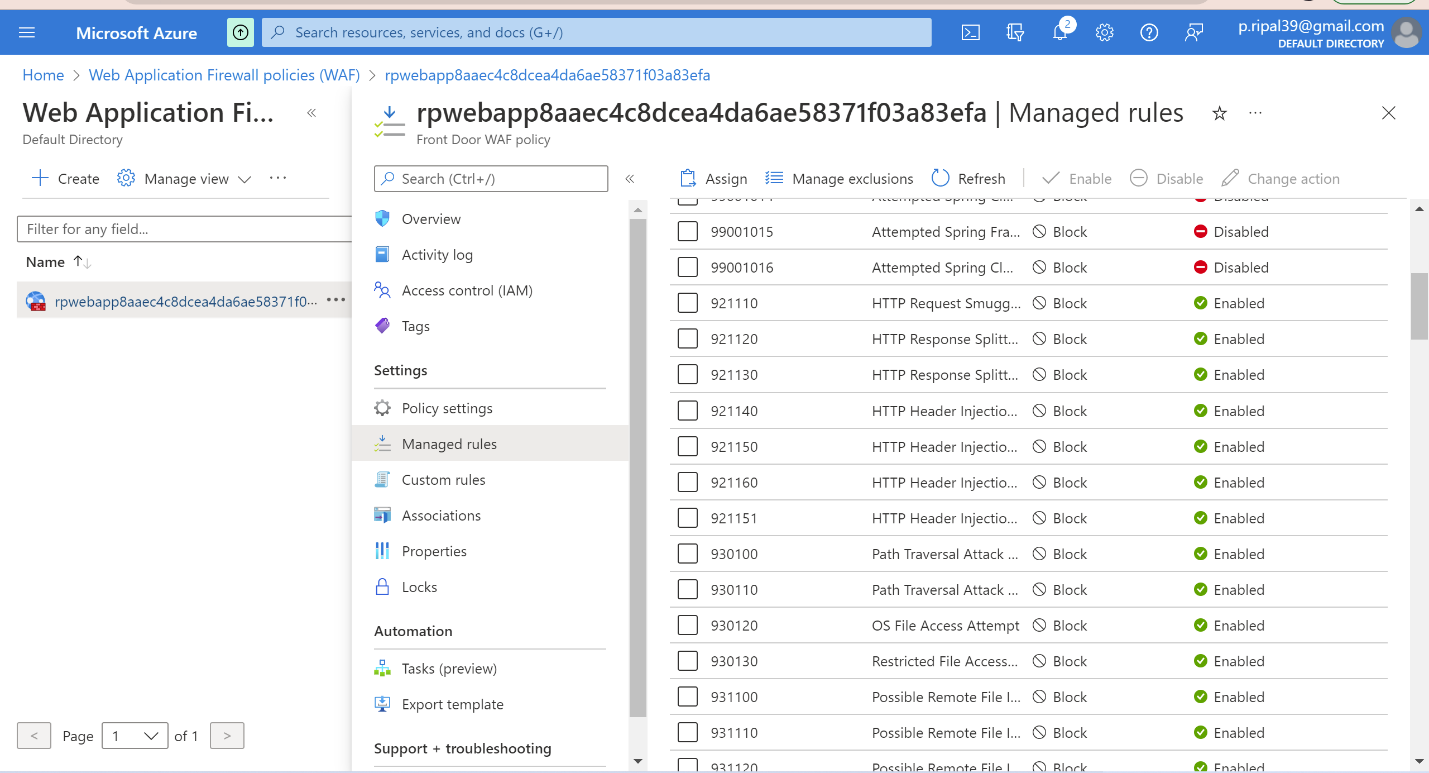
|  |
| --- |
|  |

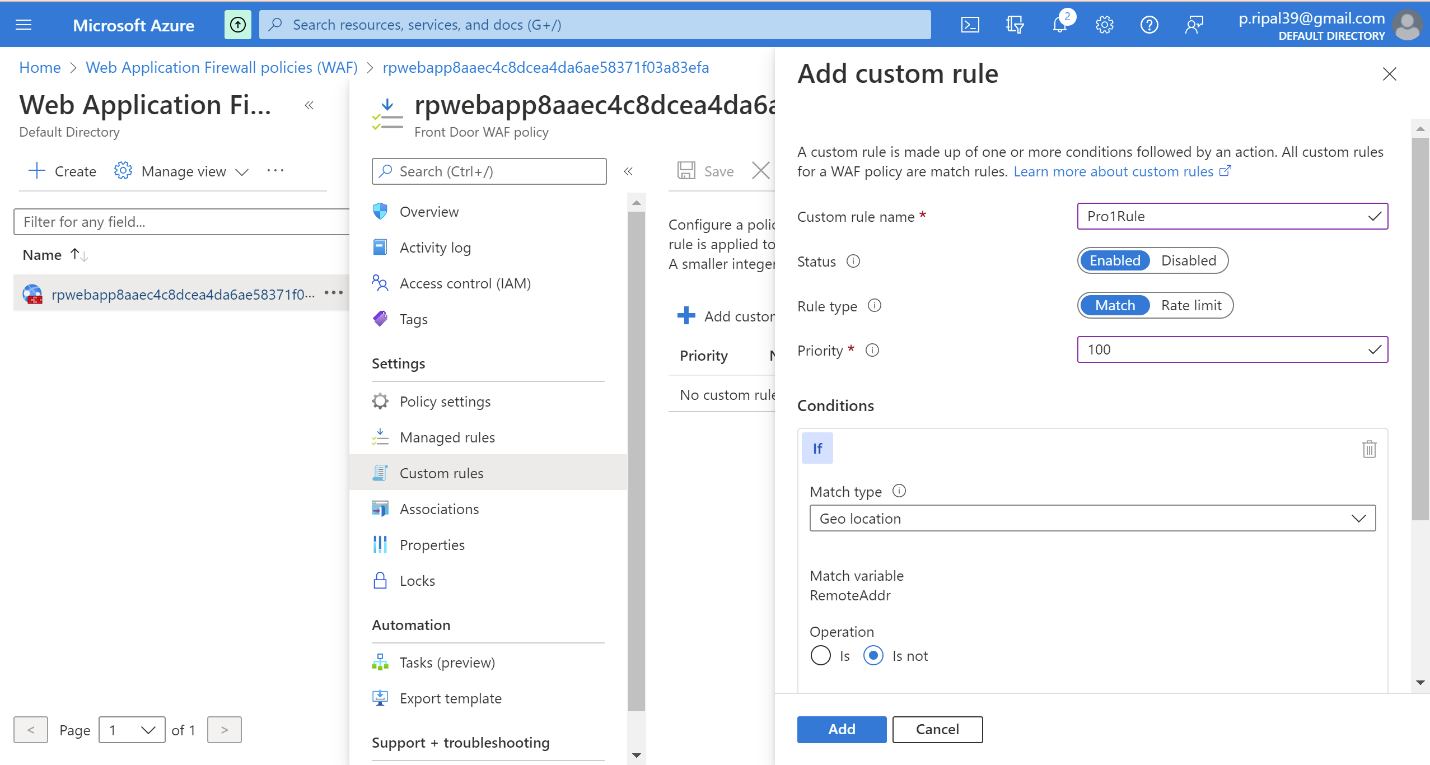


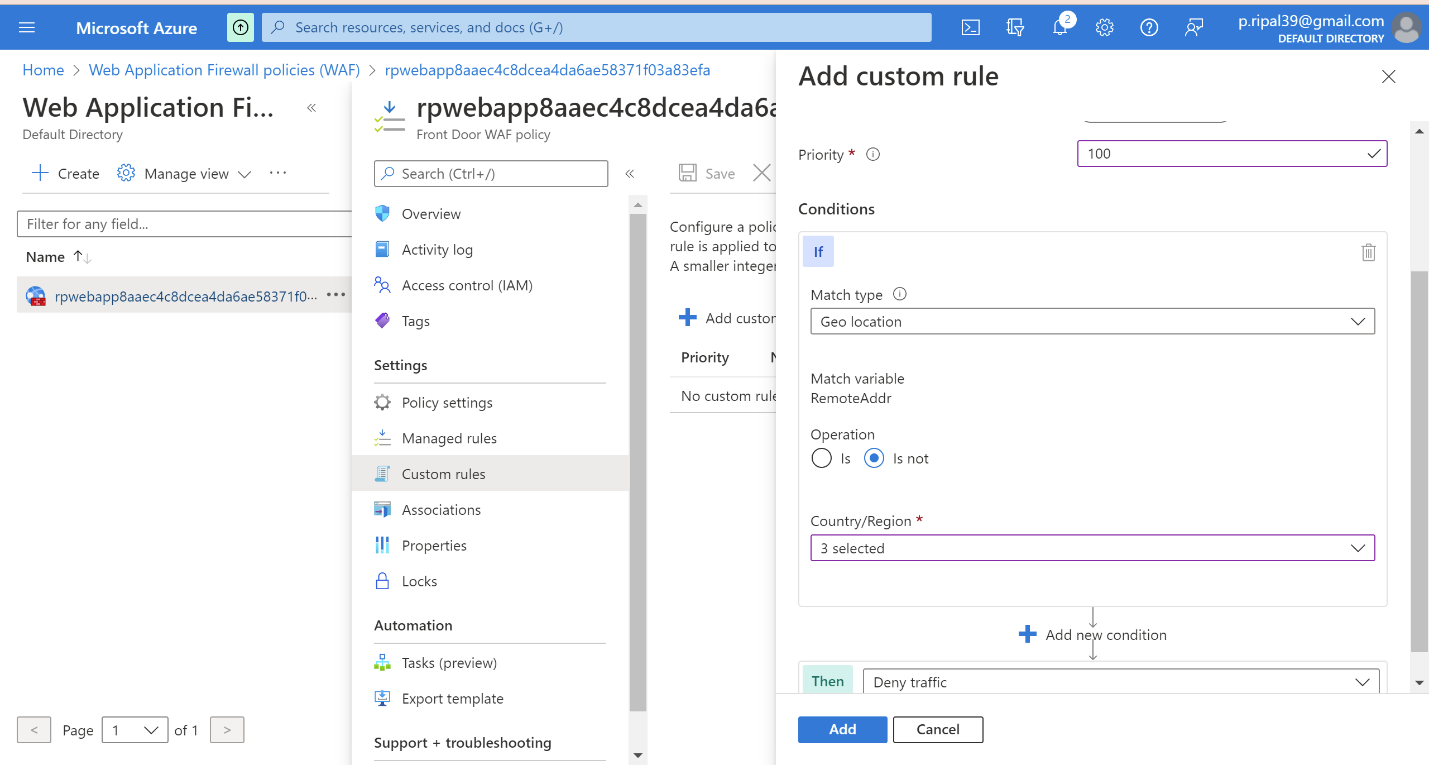


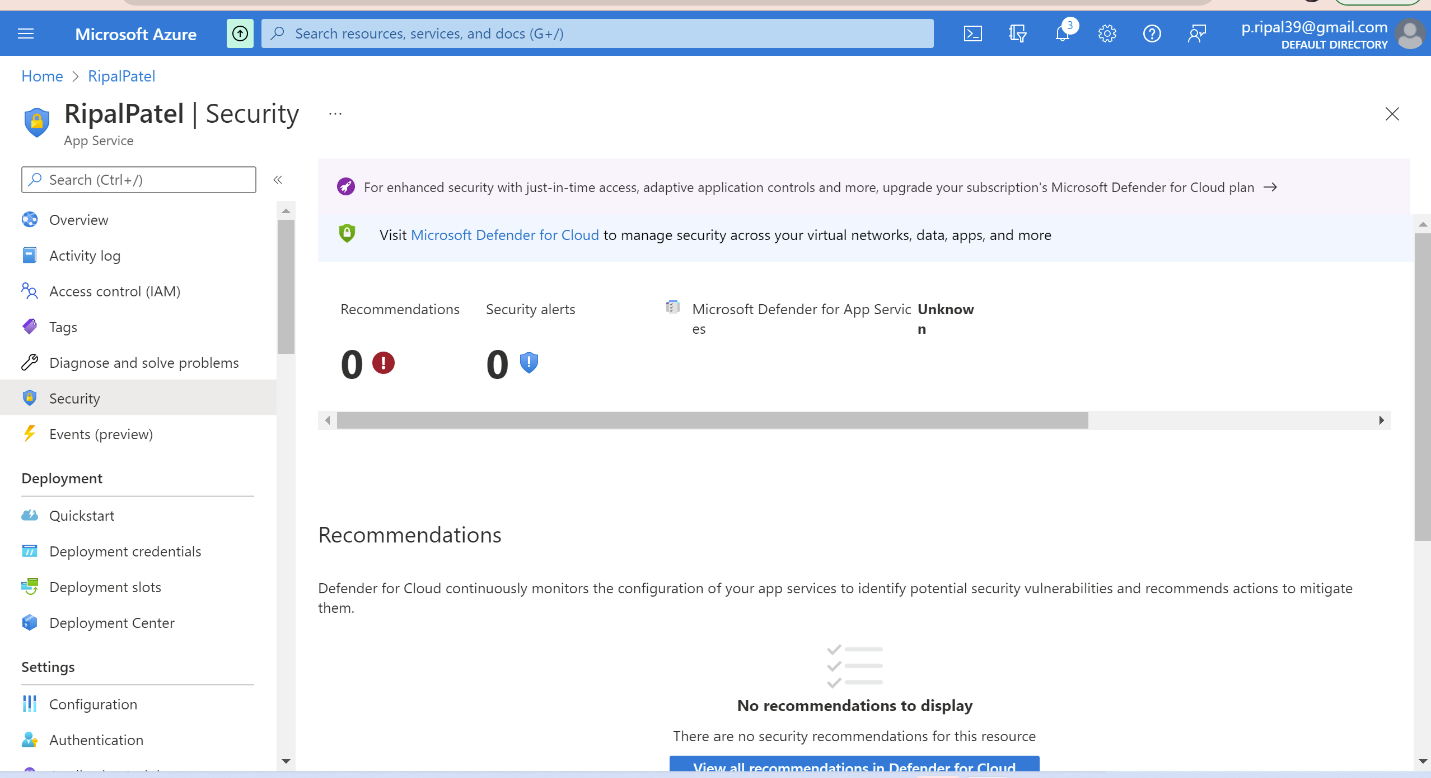


Graphical user interface, text, application, Word

Description automatically generated







## Disclaimer on Future Charges

Please type “**YES**” after one of the following options:

* ***Maintaining website after project conclusion****: I am aware that I am responsible for any charges that I incur by maintaining my website. I have reviewed the guidance for minimizing costs and monitoring Azure charges.*

***YES***

* ***Disabling website after project conclusion****: I am aware that I am responsible for deleting all my project resources as soon as the project has been graded.*

© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.