Cybersecurity

Project 1 Technical Brief

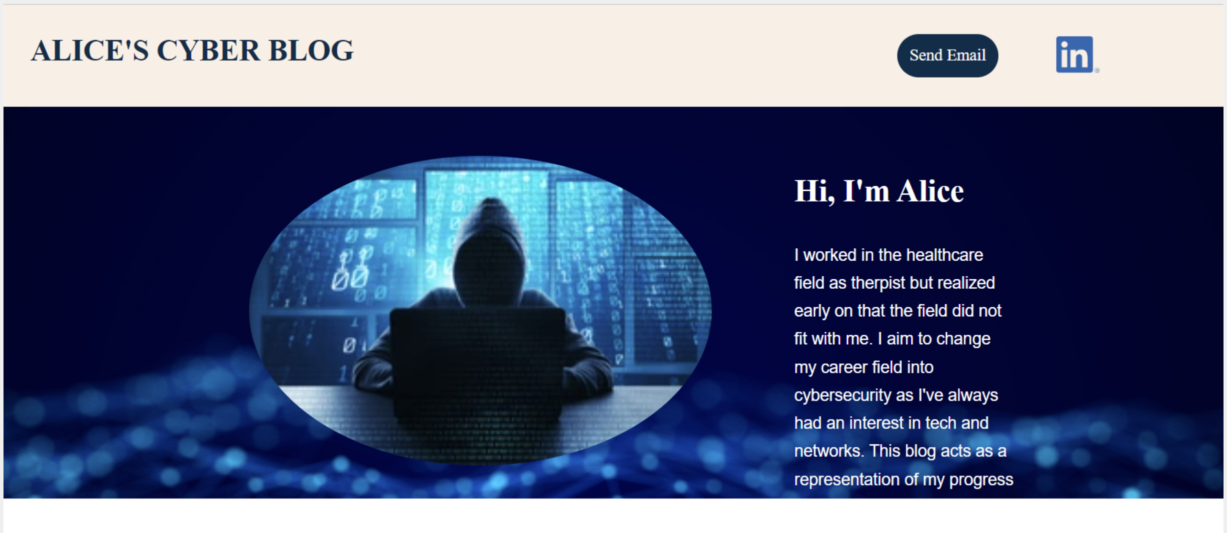
Make a copy of this document before you begin. Place your answers below each question. This completed document will be your deliverable for Project 1. Submit it through Canvas when you're finished with the project at the end of the week.

Your Web Application

Enter the URL for the web application that you created:

```
https://alicesecurityblog.azurewebsites.net
```

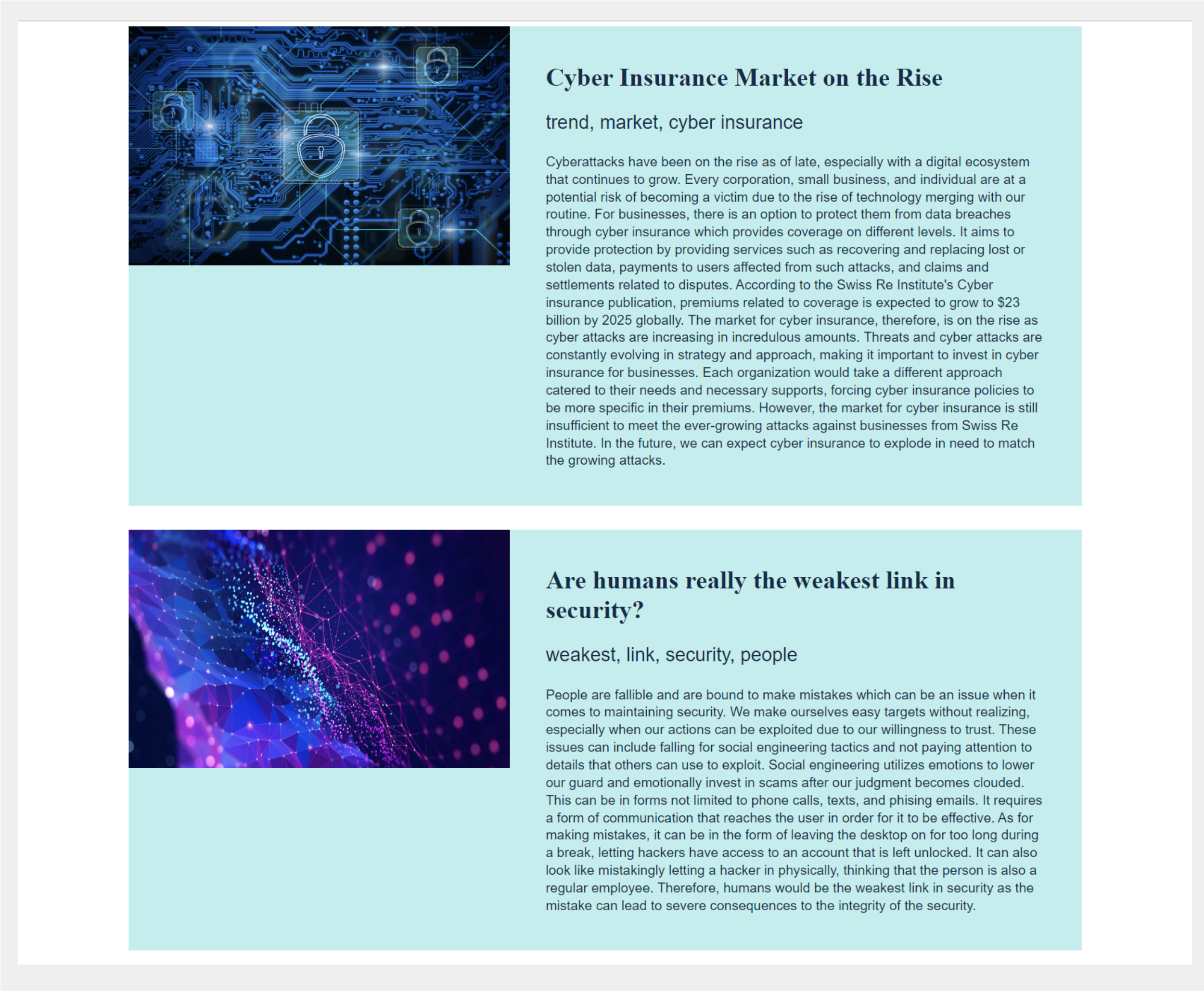
Paste screenshots of your website created (Be sure to include your blog posts):



ALICE'S CYBER BLOG

Hi, I'm Alice

I worked in the healthcare field as therpist but realized early on that the field did not fit with me. I aim to change my career field into cybersecurity as I've always had an interest in tech and networks. This blog acts as a representation of my progress



Cyber Insurance Market on the Rise

trend, market, cyber insurance

Cyberattacks have been on the rise as of late, especially with a digital ecosystem that continues to grow. Every corporation, small business, and individual are at a potential risk of becoming a victim due to the rise of technology merging with our routine. For businesses, there is an option to protect them from data breaches through cyber insurance which provides coverage on different levels. It aims to provide protection by providing services such as recovering and replacing lost or stolen data, payments to users affected from such attacks, and claims and settlements related to disputes. According to the Swiss Re Institute's Cyber insurance publication, premiums related to coverage is expected to grow to $23 billion by 2025 globally. The market for cyber insurance, therefore, is on the rise as cyber attacks are increasing in incredulous amounts. Threats and cyber attacks are constantly evolving in strategy and approach, making it important to invest in cyber insurance for businesses. Each organization would take a different approach catered to their needs and necessary supports, forcing cyber insurance policies to be more specific in their premiums. However, the market for cyber insurance is still insufficient to meet the ever-growing attacks against businesses from Swiss Re Institute. In the future, we can expect cyber insurance to explode in need to match the growing attacks.

Are humans really the weakest link in security?

weakest, link, security, people

People are fallible and are bound to make mistakes which can be an issue when it comes to maintaining security. We make ourselves easy targets without realizing, especially when our actions can be exploited due to our willingness to trust. These issues can include falling for social engineering tactics and not paying attention to details that others can use to exploit. Social engineering utilizes emotions to lower our guard and emotionally invest in scams after our judgment becomes clouded. This can be in forms not limited to phone calls, texts, and phising emails. It requires a form of communication that reaches the user in order for it to be effective. As for making mistakes, it can be in the form of leaving the desktop on for too long during a break, letting hackers have access to an account that is left unlocked. It can also look like mistakingly letting a hacker in physically, thinking that the person is also a regular employee. Therefore, humans would be the weakest link in security as the mistake can lead to severe consequences to the integrity of the security.

Day 1 Questions

General Questions

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

```
Azure free domain
```

2. What is your domain name?

```
alicesecurityblog.azurewebsites.net
```

Networking Questions

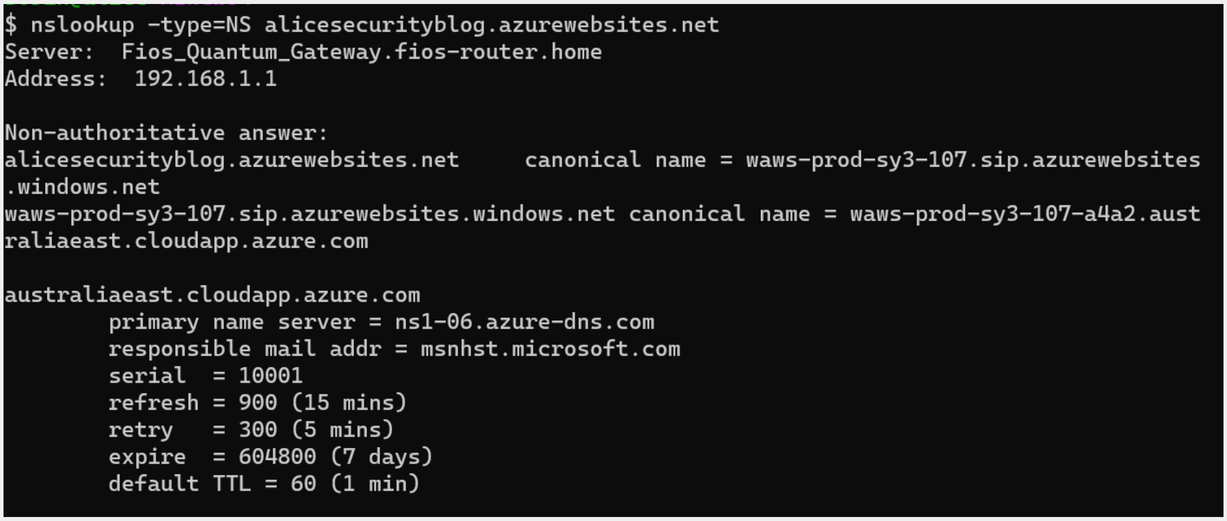
1. What is the IP address of your webpage?

```
20.211.64.21
```

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

```
Sydney, New South Wales, Australia
```

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



```
$ nslookup -type=NS alicesecurityblog.azurewebsites.net
Server:  Fios_Quantum_Gateway.fios-router.home
Address:  192.168.1.1

Non-authoritative answer:
alicesecurityblog.azurewebsites.net     canonical name = waws-prod-sy3-107.sip.azurewebsites
.windows.net
waws-prod-sy3-107.sip.azurewebsites.windows.net canonical name = waws-prod-sy3-107-a4a2.aust
raliaeast.cloudapp.azure.com

australiaeast.cloudapp.azure.com
        primary name server = ns1-06.azure-dns.com
        responsible mail addr = msnhst.microsoft.com
        serial  = 10001
        refresh = 900 (15 mins)
        retry   = 300 (5 mins)
        expire  = 604800 (7 days)
        default TTL = 60 (1 min)
```

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?

```
The runtime stack chosen for this site is PHP 8.2. PHP is an all-purpose
scripting language mainly used for web development for structure, data, and
logic. Therefore, it would work mainly on back-end development.
```

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

Inside the assets directory, there are two more directories called css and images. CSS is the file that shifts the objects of the html website to change of visual characteristics such as borders and font styles. The image folder contains images for the website.

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

This works with the front-end of the server as both files would be used to change the visuals of the html site.

Day 2 Questions

Cloud Questions

1. What is a cloud tenant?

A cloud tenant is a user or an organization utilizing resources and services offered by a cloud service to do various tasks such as storing data and installing software.

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

An access policy is important on a key vault because it determines permissions to a certain user, user group, or application for sensitive items such as secrets, keys, and certificates.

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

Keys, secrets, and certificates are indispensable objects that make up the key vault. Keys are cryptographic keys that are used to encrypt data. Secrets are anything, including certificates and keys, that the user would like to have tight access control over. A certificate creates an identifiable token tied to a public key so that any communication with a website or software would be secure.

Cryptography Questions

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

A self-signed certificate is a digital certificate issued independently with a private key by the user. The advantages of having a self-signed certificate is that they are quick and easy to setup and deploy, free to generate, useful for testing, able to customizable to the user’s preferences, and that it would not require waiting on a 3rd party to have it issued.

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

The disadvantages of a self-signed certificate is that they are not automatically trusted by other web browers or software, easier to compromise, have more vulnerabilities, and require maintenance from a short lifespan, and issues with compatibility. Therefore the best use for a self-signed certificate is for testing.

3. What is a wildcard certificate?

A wildcard certificate is a type of certificate that secures multiple subdomains under a main domain with a single certificate.

4. 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.

TLS versions were built upon SSL with better security and stronger encryption. SSL is considered outdated in design and have vulnerabilities that are easier to exploit. Therefore, SSL 3.0 is not provided as TLS is the safer and stronger option.

5. After completing the Day 2 activities, view your SSL certificate and answer the following questions:

a. Is your browser returning an error for your SSL certificate? Why or why not?

No, my brower is not returning an error for my SSL certificate as a third-party certificate authority is running on my website (azure free domain). However, if the self-signed certificate was applied, it would have returned an error as it wouldn’t be automatically trusted by the browser.

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

from 07/29/20 until 06/27/24

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

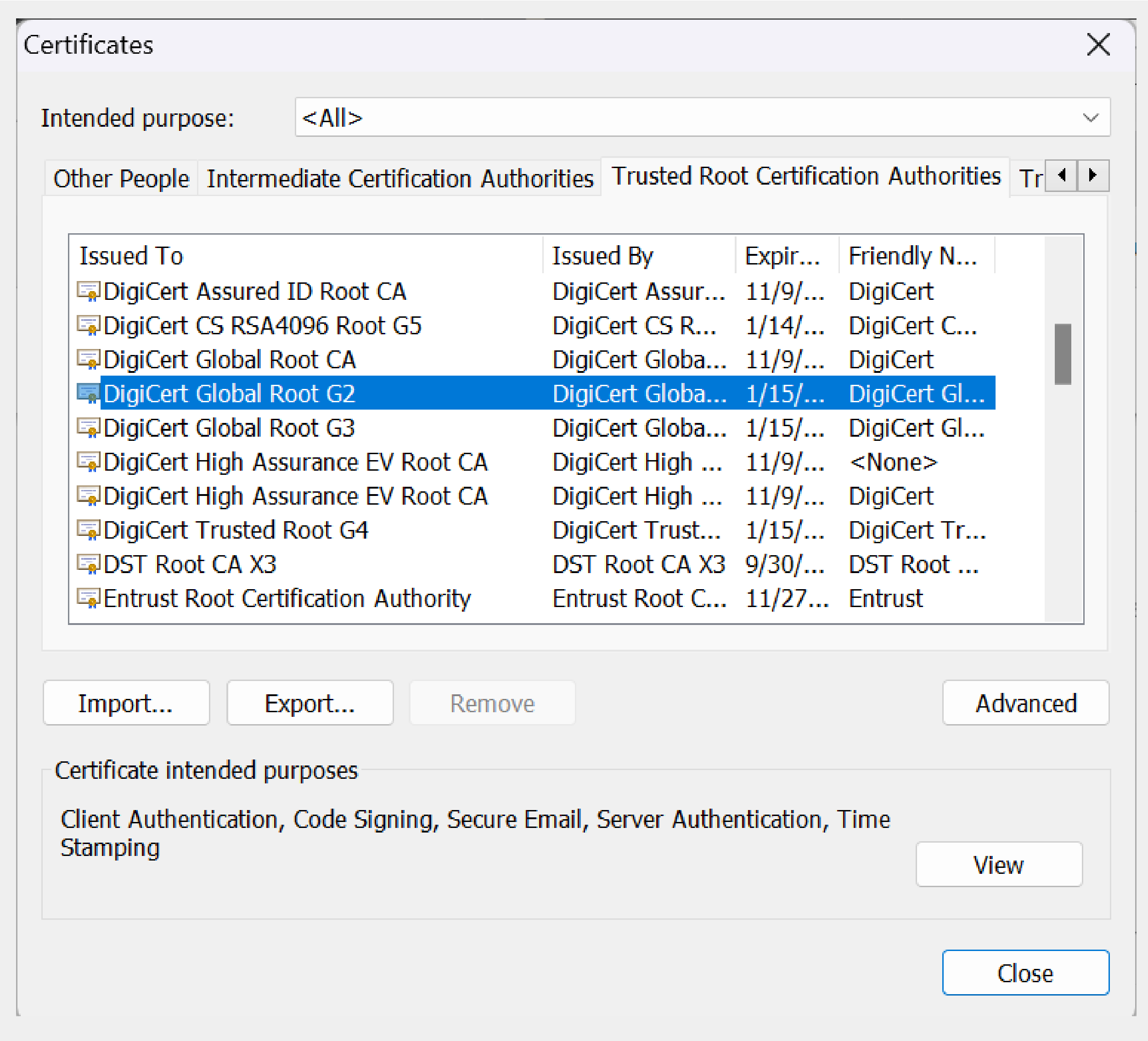
Yes, the intermediate certificate is Microsoft Azure TLS Issuing CA 01.

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

Yes, the root certificate is DigiCert Global Root G2

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

Yes.


Certificates
Other People
Intermediate Certification Authorities
Trusted Root Certification Authorities
Tr
Import...
Export...
Remove
Advanced
View
Close

Intended purpose: <All>

Issued To	Issued By	Expir...	Friendly N...
DigiCert Assured ID Root CA	DigiCert Assur...	11/9/...	DigiCert
DigiCert CS RSA4096 Root G5	DigiCert CS R...	1/14/...	DigiCert C...
DigiCert Global Root CA	DigiCert Globa...	11/9/...	DigiCert
DigiCert Global Root G2	DigiCert Globa...	1/15/...	DigiCert Gl...
DigiCert Global Root G3	DigiCert Globa...	1/15/...	DigiCert Gl...
DigiCert High Assurance EV Root CA	DigiCert High ...	11/9/...	<None>
DigiCert High Assurance EV Root CA	DigiCert High ...	11/9/...	DigiCert
DigiCert Trusted Root G4	DigiCert Trust...	1/15/...	DigiCert Tr...
DST Root CA X3	DST Root CA X3	9/30/...	DST Root ...
Entrust Root Certification Authority	Entrust Root C...	11/27...	Entrust

Certificate intended purposes

Client Authentication, Code Signing, Secure Email, Server Authentication, Time Stamping

f. List one other root CA in your browser's root store.

```
GlobalSign Root CA
```

Day 3 Questions

Cloud Security Questions

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

The similarity between Azure Web Application Gateway and Azure Front Door is that they are both load balancers that reside in the front of the web app to protect it.The main difference in these services is geographical applicability - The Azure Web Application works regionally while the Azure Front Door works globally.

2. 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 removal of SSL encryption from incoming traffic to reduce the workload involved in processing encryptions when sending and receiving web page traffic. The benefits of it are smoother and faster page load times, better performance, and enhanced stability of the website.

3. What OSI layer does a WAF work on?

WAF works on the Application Layer (7th layer).

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

One rule that is managed by WAF is the HTTP Response Splitting Attack. This rule would block malicious input that has CRLF (Carriage Return, Line Feed) characters before it can reach the application.

5. 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?

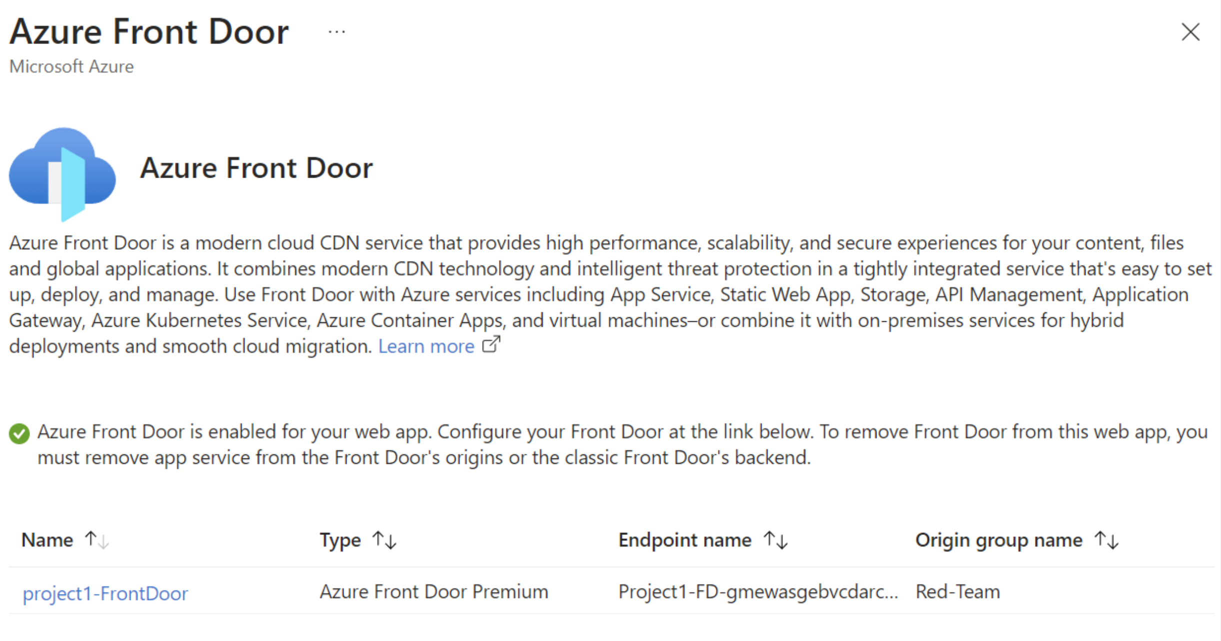
Yes, my website would be impacted by this vulnerability because it would no longer have a secure rule that would prevent the attack from happening.

6. 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?

No, anyone who resides in Canada would not be able to access my website because the rule is restricting traffic from a specific location. The WAF would read the IP address that is trying to communicate and if it’s in range of an IP address from Canada, it will apply the block.

7. Include screenshots below to demonstrate that your web app has the following:

    a. Azure Front Door enabled

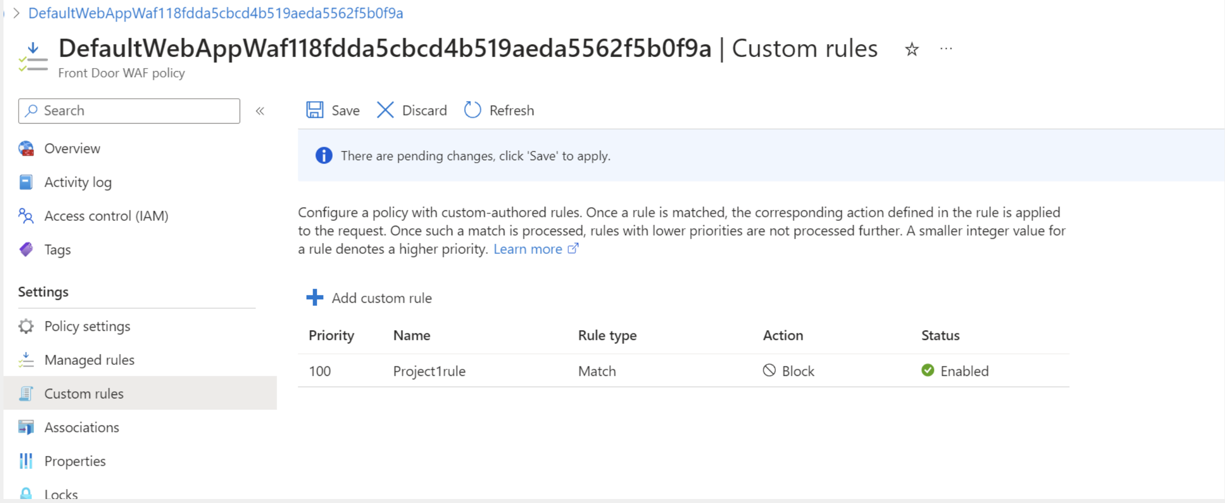


Azure Front Door is a modern cloud CDN service that provides high performance, scalability, and secure experiences for your content, files and global applications. It combines modern CDN technology and intelligent threat protection in a tightly integrated service that's easy to set up, deploy, and manage. Use Front Door with Azure services including App Service, Static Web App, Storage, API Management, Application Gateway, Azure Kubernetes Service, Azure Container Apps, and virtual machines–or combine it with on-premises services for hybrid deployments and smooth cloud migration. Learn more

✓ Azure Front Door is enabled for your web app. Configure your Front Door at the link below. To remove Front Door from this web app, you must remove app service from the Front Door's origins or the classic Front Door's backend.

Name ↑↓	Type ↑↓	Endpoint name ↑↓	Origin group name ↑↓
project1-FrontDoor	Azure Front Door Premium	Project1-FD-gmewasgebvcdarc...	Red-Team

    b. A WAF custom rule



There are pending changes, click 'Save' to apply.

Configure a policy with custom-authored rules. Once a rule is matched, the corresponding action defined in the rule is applied to the request. Once such a match is processed, rules with lower priorities are not processed further. A smaller integer value for a rule denotes a higher priority. Learn more

Priority	Name	Rule type	Action	Status
100	Project1rule	Match	⊘ Block	✓ Enabled

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 of my project resources as soon as I have gathered all of my web application screen shots and completed this document.*
  YES