Cybersecurity

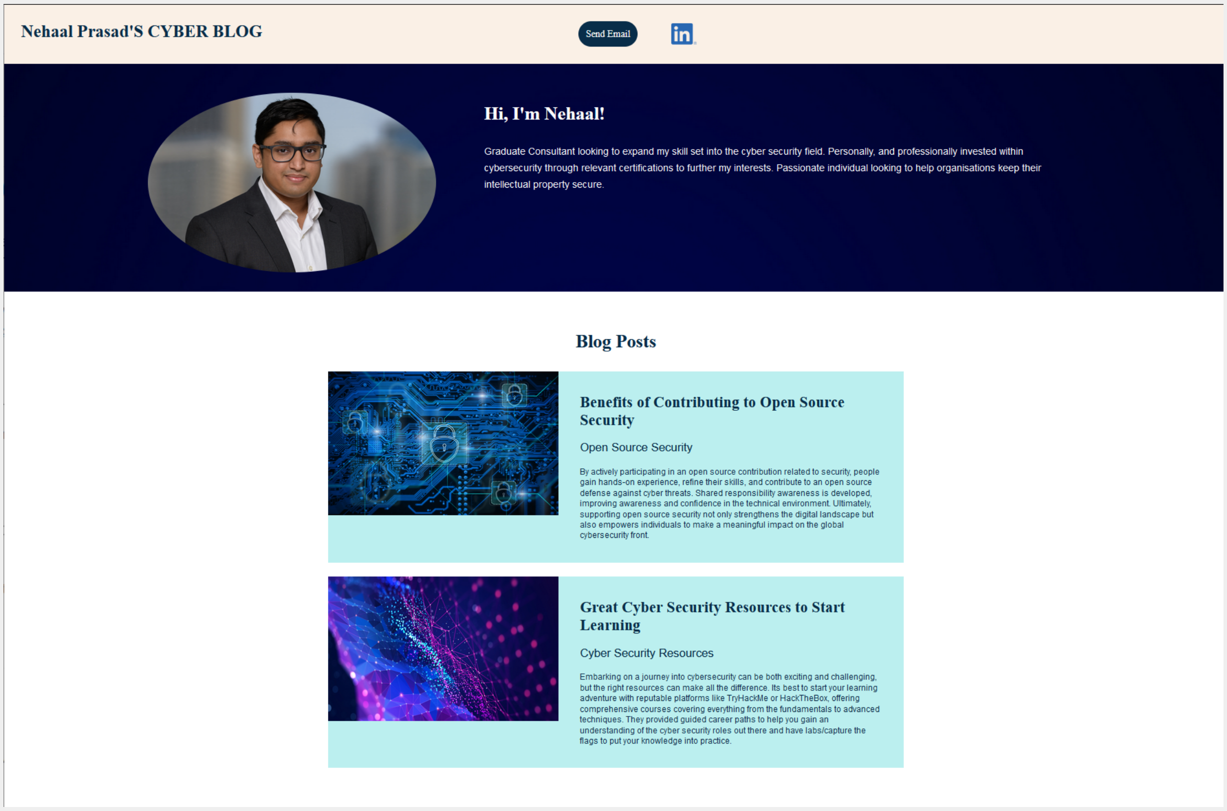
Project 1 Technical Brief

Your Web Application

Enter the URL for the web application that you created:

```
https://nehaalportfolio.azurewebsites.net/
```

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



Nehaal Prasad'S CYBER BLOG

Hi, I'm Nehaal!

Graduate Consultant looking to expand my skill set into the cyber security field. Personally, and professionally invested within cybersecurity through relevant certifications to further my interests. Passionate individual looking to help organisations keep their intellectual property secure.

Blog Posts

Benefits of Contributing to Open Source Security

Open Source Security

By actively participating in an open source contribution related to security, people gain hands-on experience, refine their skills, and contribute to an open source defense against cyber threats. Shared responsibility awareness is developed, improving awareness and confidence in the technical environment. Ultimately, supporting open source security not only strengthens the digital landscape but also empowers individuals to make a meaningful impact on the global cybersecurity front.

Great Cyber Security Resources to Start Learning

Cyber Security Resources

Embarking on a journey into cybersecurity can be both exciting and challenging, but the right resources can make all the difference. Its best to start your learning adventure with reputable platforms like TryHackMe or HackTheBox, offering comprehensive courses covering everything from the fundamentals to advanced techniques. They provided guided career paths to help you gain an understanding of the cyber security roles out there and have labs/capture the flags to put your knowledge into practice.

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?

```
nehaalportfolio.azurewebsites.net
```

Networking Questions

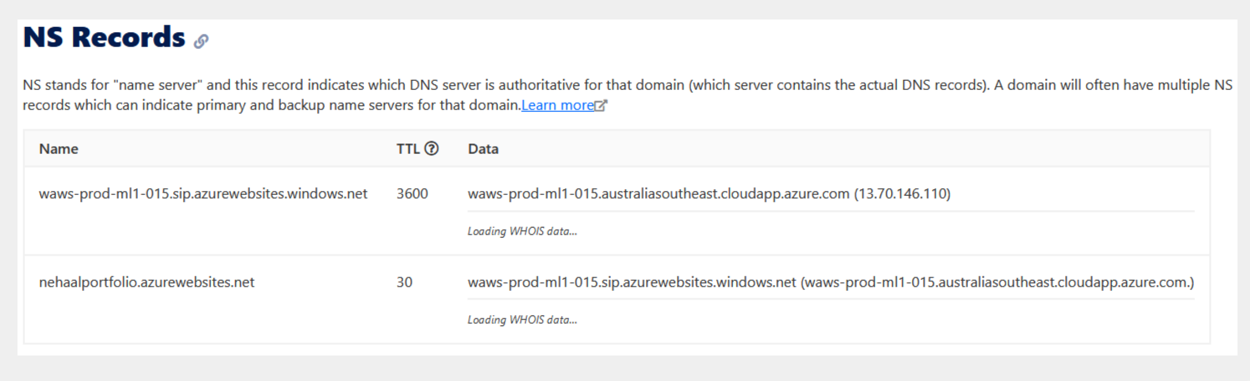
1. What is the IP address of your webpage?

```
13.70.146.110
```

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

```
Country: Australia
State/Region: Victoria
City: Melbourne
```

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



NS Records

NS stands for "name server" and this record indicates which DNS server is authoritative for that domain (which server contains the actual DNS records). A domain will often have multiple NS records which can indicate primary and backup name servers for that domain.Learn more

Name	TTL	Data
waws-prod-ml1-015.sip.azurewebsites.windows.net	3600	waws-prod-ml1-015.australiasoutheast.cloudapp.azure.com (13.70.146.110) *Loading WHOIS data...*
nehaalportfolio.azurewebsites.net	30	waws-prod-ml1-015.sip.azurewebsites.windows.net (waws-prod-ml1-015.australiasoutheast.cloudapp.azure.com.) *Loading WHOIS data...*

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 8.2
Back-End
```

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

```
There were two other sub directories. One was css and the other was images.
```

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

```
Front-End
```

Day 2 Questions

Cloud Questions

1. What is a cloud tenant?

```
A cloud tenant is a user that utilizes cloud computing services
```

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

An access key is important due to security reasons. It helps control and restrict who has access to key, secrets and certificates stored in the vault.

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

Keys are used to encrypt and decrypt data.

Certificates are used to establish trust between websites.

Secrets are stored away as they constrain sensitive information such as passwords.

Cryptography Questions

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

Self signed certificates are quick to set up, cheap and give their user full control which is great for testing or in development environments.

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

Self signed certificates have trust issues leading to websites warning users to not access the site and poses a security risk as users cannot verify the certificate leading to a man in the middle attack.

3. What is a wildcard certificate?

A wildcard makes it so a single certificate is able to also secure multiple domain hosts to the same main base domain.

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.

SSL 3.0 is not provided due to security vulnerabilities associated with the protocol.

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 since Azure set up a SSL certificate
```

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

```
Issued On    Sunday, 21 May 2023 at 15:09:05
Expires on    Wednesday, 15 May 2024 at 15:09:05
```

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

```
No, root certificate.
```

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

```
Yes, DigiCert Global Root G2
```

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

```
Yes
```

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

```
ACCV
```

Day 3 Questions

Cloud Security Questions

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

They are both load balancers.
Azure Front Door is non-regional.
Azure Application Gateway is regional.

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 where the SSL/TLS encryption and decryption tasks are offloaded from the web services to a service or a dedicated device such as a load balancer like Azure Web Application Gateway (WAG) and Azure Front Door (AFD). The benefits are that due to SSL offloading, your website will load faster.

3. What OSI layer does a WAF work on?

Layer 7 Defense

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

Directory Traversal is one vulnerability when an attacker is able to traverse directories that users are not supposed to have access to. An example is a user is able to find a password file via directory traversal.

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?

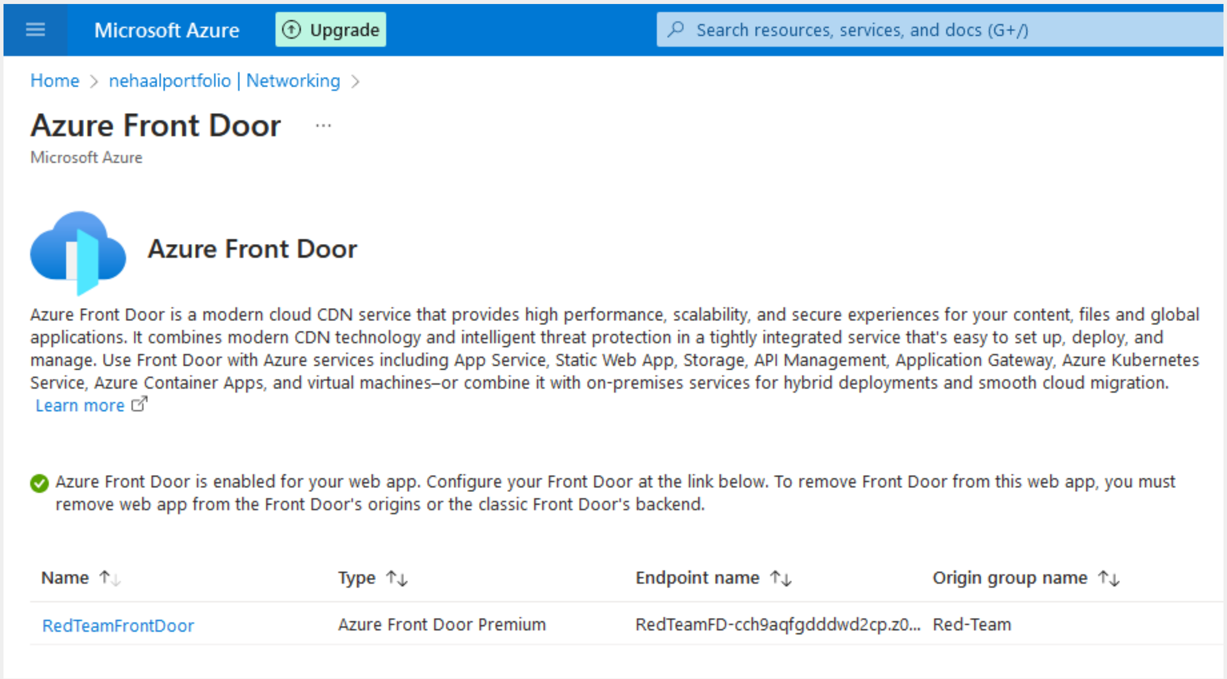
No, since my Web Application Firewall (WAF) with its rulesets are designed to detect and prevent directory traversal attempts.

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, since the Web Application Firewall (WAF) is only targeting IP’s coming from Canada. A user in Canada can use a VPN to mask their IP and origin to access my site.

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

   a. Azure Front Door enabled


Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Home > nehaalportfolio | Networking >

Azure Front Door

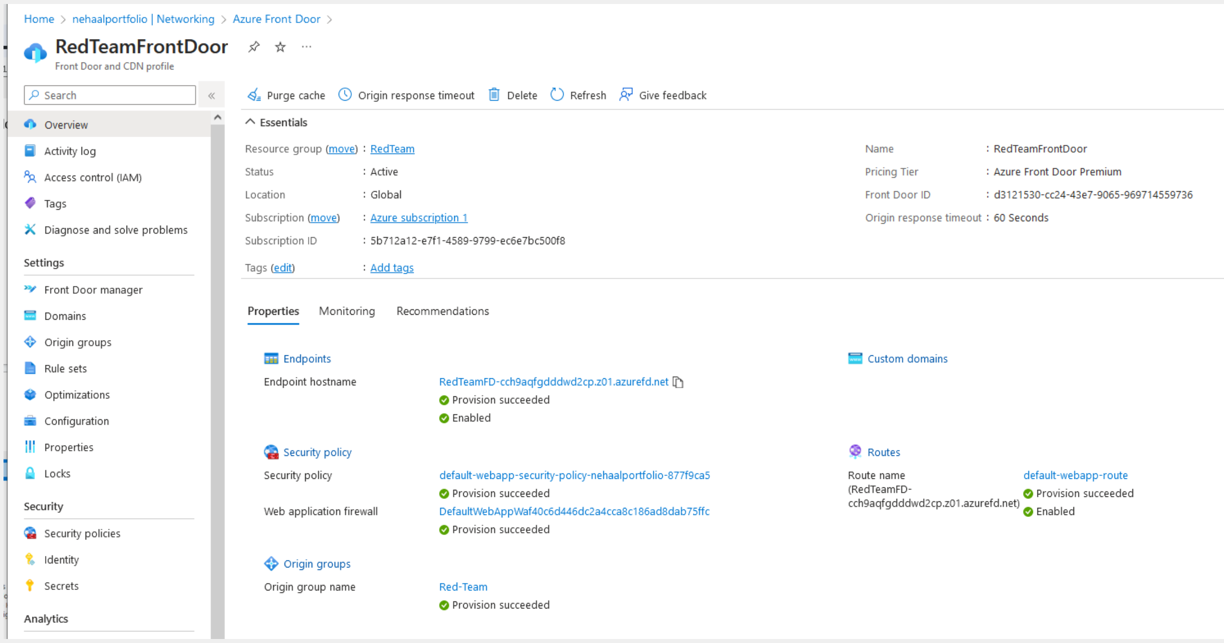
Microsoft Azure

Azure Front Door

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 web app from the Front Door's origins or the classic Front Door's backend.

Name ↑↓	Type ↑↓	Endpoint name ↑↓	Origin group name ↑↓
RedTeamFrontDoor	Azure Front Door Premium	RedTeamFD-cch9aqfgdddwd2cp.z0...	Red-Team



RedTeamFrontDoor

Front Door and CDN profile

Essentials

Resource group (move)	: RedTeam	Name	: RedTeamFrontDoor
Status	: Active	Pricing Tier	: Azure Front Door Premium
Location	: Global	Front Door ID	: d3121530-cc24-43e7-9065-969714559736
Subscription (move)	: Azure subscription 1	Origin response timeout	: 60 Seconds
Subscription ID	: 5b712a12-e7f1-4589-9799-ec6e7bc500f8		
Tags (edit)	: Add tags		

Endpoints

Endpoint hostname: RedTeamFD-cch9aqfgdddwd2cp.z01.azurefd.net
✓ Provision succeeded
✓ Enabled

Custom domains

Security policy

Security policy: default-webapp-security-policy-nehaalportfolio-877f9ca5
✓ Provision succeeded

Web application firewall: DefaultWebAppWaf40c6d446dc2a4cca8c186ad8dab75ffc
✓ Provision succeeded

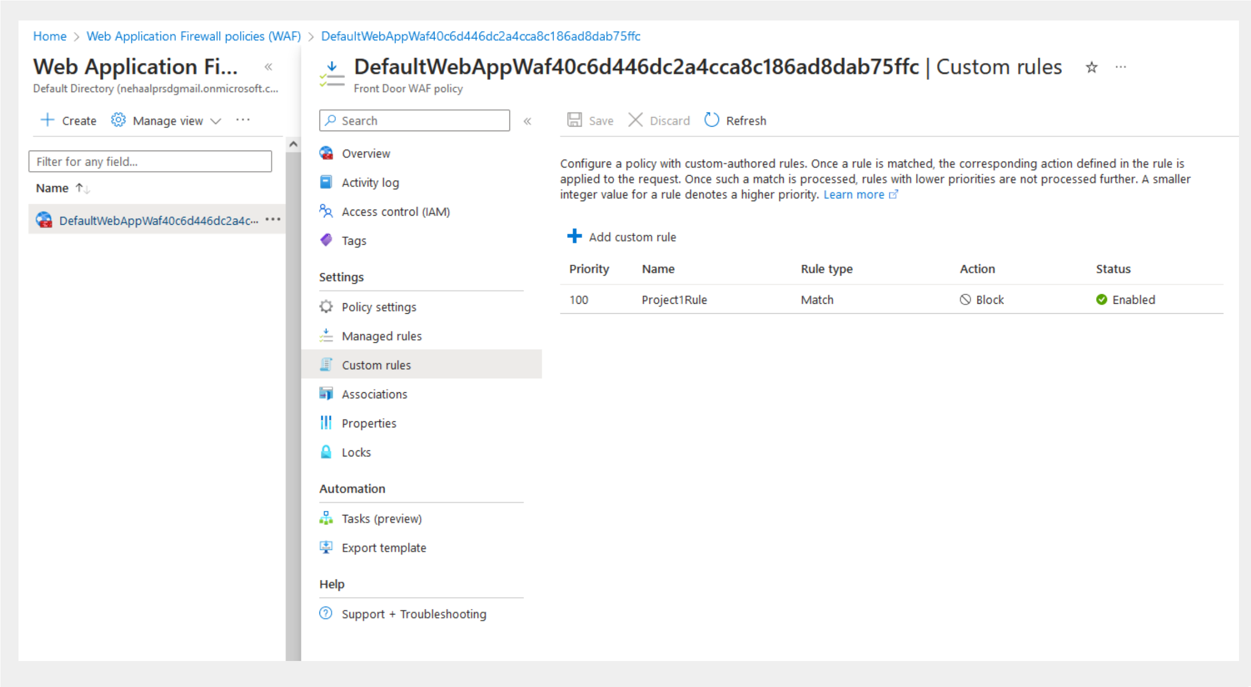
Routes

Route name (RedTeamFD-cch9aqfgdddwd2cp.z01.azurefd.net): default-webapp-route
✓ Provision succeeded
✓ Enabled

Origin groups

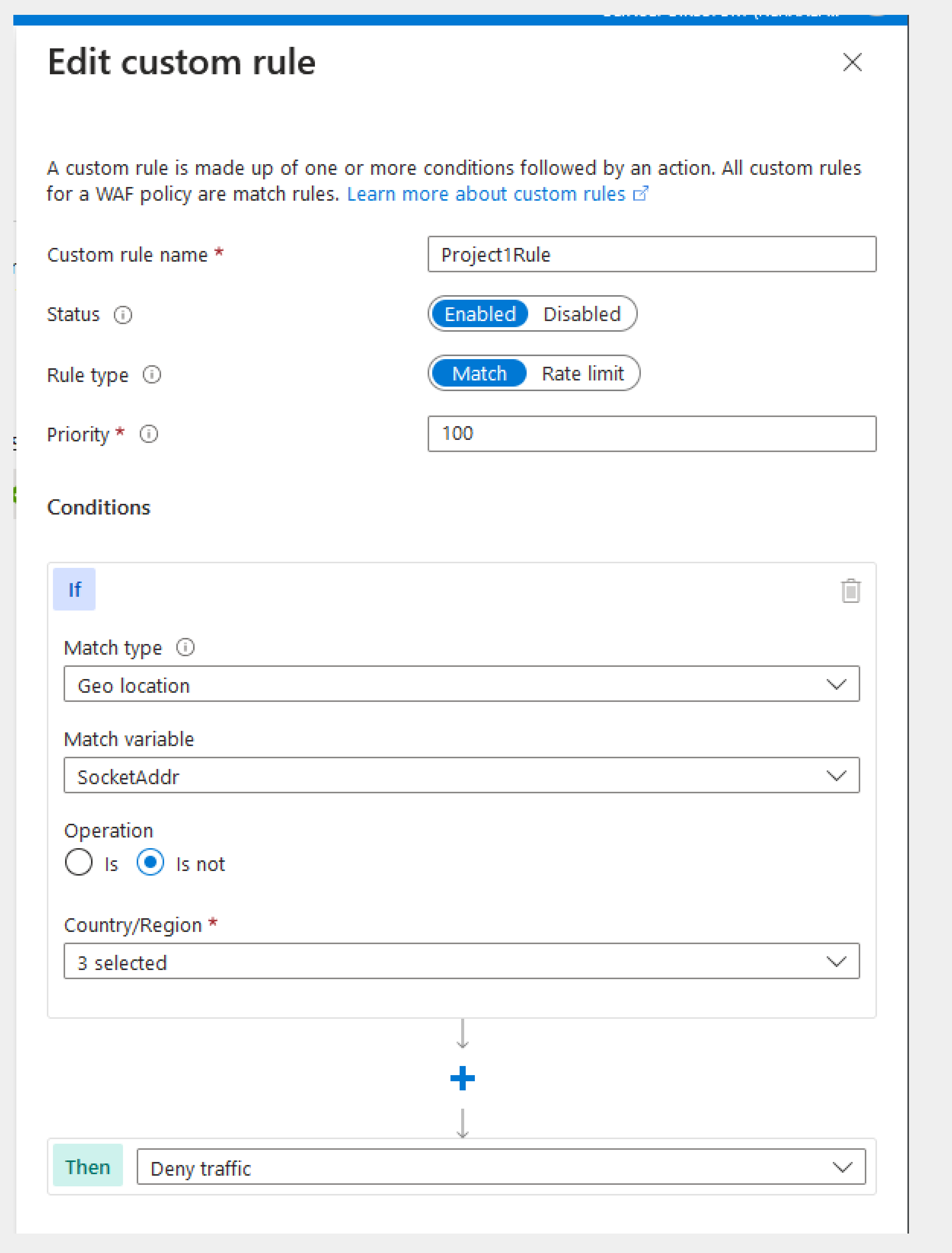
Origin group name: Red-Team
✓ Provision succeeded

   b. A WAF custom rule



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



Edit custom rule

A custom rule is made up of one or more conditions followed by an action. All custom rules for a WAF policy are match rules. Learn more about custom rules

Custom rule name * Project1Rule

Status ● Enabled ○ Disabled

Rule type ● Match ○ Rate limit

Priority * 100

Conditions

If

Match type: Geo location

Match variable: SocketAddr

Operation: ○ Is ● Is not

Country/Region *: 3 selected

Then: Deny traffic

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.*

- ***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**