



# 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://rinkscyberblog.azurewebsites.net/
```

### Day 1 Questions

#### General Questions

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

```
Azure free domain
```

2. What is your domain name?

```
rinkscyberblog.azurewebsites.net
```

#### Networking Questions

1. What is the IP address of your webpage?

20.211.64.7

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

Australia East

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

```
nslookup rinkscyberblog.azurewebsites.net
```

```
Server:      8.8.8.8
```

```
Address:     8.8.8.8#53
```

```
Non-authoritative answer:
```

```
rinkscyberblog.azurewebsites.net    canonical name =
```

```
waws-prod-sy3-079.sip.azurewebsites.windows.net.
```

```
waws-prod-sy3-079.sip.azurewebsites.windows.net canonical name =
```

```
waws-prod-sy3-079-3aec.australiaeast.cloudapp.azure.com.
```

```
Name: waws-prod-sy3-079-3aec.australiaeast.cloudapp.azure.com
```

```
Address: 20.211.64.7
```

## 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?

When creating the web app, PHP7.4 runtime stack was selected.

PHP is a **back end** development language only. PHP belongs to the LAMP stack, which stands for Linux, Apache, MySQL, and PHP/Perl/Python. To develop a web app with this technology stack, a software engineer needs to know four different syntax systems, as well as HTML and CSS

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

Assets directory contained a file called `style.css`. This file controls visual design and layout of the website.

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

Style.css is the css file so it works at the front end

## Day 2 Questions

### Cloud Questions

1. What is a cloud tenant?

A tenant is essentially a customer who purchases cloud computing resources. This could be an individual user, a group of users, or an entire department or company. There are two types of cloud tenant architecture,

**Single-tenant cloud architecture** is one where a single software instance and its supporting infrastructure/database serves only one customer. In a single-tenant environment, all customer data and interactions are separate from every other customer. **Eg:** in real estate analogy, In a single-tenant cloud, each customer lives alone in a single apartment building which has its own security system and facilities and is completely isolated from neighboring buildings.

A **multi-tenant architecture** is one where a single software instance and database serves multiple customers (i.e. Tenants). **Eg:** in real estate analogy, tenants live in different apartments inside a single apartment building. They share the same security and facilities. But each tenant has a key to their respective apartments so their privacy is guaranteed within their apartment.

**Tenant in Microsoft Azure cloud** service represents the organization created in Azure Active Directory. Azure Active Directory organizes all the users and applications into a group, and these groups are called as tenants. An app developer receives the tenant as a dedicated instance of Azure Active Directory to generate a relationship with Microsoft cloud service. This tenant id can be used to sign-in credentials to Azure, Microsoft 365 or Microsoft Intune as each Azure AD tenant has a unique identity and app registration.

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

Because 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 secret, keys and certificates

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

**Cryptographic keys:** Supports multiple key types and algorithms, and enables the use of software-protected and HSM-protected keys.

**Secrets:** Provides secure storage of secrets, such as passwords and database connection strings.

**Certificates:** Supports certificates, which are built on top of keys and secrets and add an automated renewal feature.

## Cryptography Questions

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

- Self-signed SSL certificates are free
- They are fast and easy to issue
- They are flexible and customizable
- They're suitable for internal (intranet) sites or testing environments
- They encrypt the incoming and outgoing data with the same ciphers as any other paid SSL certificates

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

- No browsers and operating systems trust self-signed certificates
- If compromised, they pose a serious risk
- They cannot be revoked by a CA
- The browsers will not show visual indicators or trust like a padlock symbol and HTTPS in front of the domain name

### 3. What is a wildcard certificate?

A wildcard certificate is a digital certificate that is applied to a domain and all its subdomains. Wildcard notation consists of an asterisk and a period before the domain name. SSL certificates often use wildcards to extend SSL encryption to subdomain

### 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.

To ensure the safety of the users, Microsoft completely disables SSL 3.0 in Azure websites by default to protect customers from the vulnerability. Because according to Microsoft it has a flaw that could allow an attacker to decrypt information, such as authentication cookies.

### 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 error because connection is secure and the website has a valid certificate. You can see the padlock sign.

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

03/14/2022 to 3/9/2023

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

Yes , Microsoft Azure TLS Issuing CA 01

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.

Entrust Root Certification Authority  
COMODO RSA Certification Authority

## 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** is a single global entry point which uses an edge network to create scalable web applications. The fully managed service can be configured as a load balancer for an application that runs on Azure. It operates at OSI layer 7 , also known as application layer.

**Azure Web Application Gateway** is a web traffic load balancer, also operating at OSI layer 7, that manages application content traffic. Its setup process is similar to Azure Front Door.

#### Similarities:

- Both resides in front of your web application in order to protect it
- They work on Application Layer 7 of OSI model
- Their primary solution is a load balancer
- They can incorporate a web application firewall (WAF) to protect against web vulnerability attacks
- They have additional features such as URL path-based routing and

SSL/TLS termination.

**Differences:**

- The **Web Application Gateway** is more regional, to protect a web application in a single region in your cloud
- The **Azure Front Door** is more global and is better suited when you have a variety of regions in a cloud environment.

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 process of removing the SSL based encryption from incoming traffic. When information is transmitted through SSL secure protocol, the web server takes action to encrypt and/or decrypt your web traffic. This process assigns a substantial load on the web server which will affect the performance of the web server. To deal with the added burden of encryption data on the server, many networks now employ SSL offloading. This network solution involves the removal of SSL encryption from incoming traffic before it reaches the web server. SSL offloading is taking care of the SSL process on a separate device so it doesn't affect the web server's performance.

**Benefits of SSL offloading:**

- Smooth loading of website
- Boost the page load speed time
- Faster response from the Web server
- Better web server performance
- Enhance stability of the website
- Auto-scaling the web servers during the peak hours of traffic
- Use as load balancer for serving web traffic using different servers

3. What OSI layer does a WAF work on?

Web Application Layer (WAF) is a part of Layer 7 Application Layer in OSI model, it is designed to examine all HTTP or HTTPS traffic between external users and web applications. It detects and prevents malicious sources from gaining access to users or web applications.

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

A **SQL injection** attack consists of insertion or “injection” of a SQL query via the input data from the client to the application. A successful SQL injection exploit can read sensitive data from the database, modify database data (insert/Update/Delete), execute administration operations on the database (such as shutdown the DBMS), recover the content of a given file present on the DBMS file system and in some cases issue commands to the operating system. SQL injection attack, in which SQL commands are injected into data-plane input in order to affect the execution of predefined SQL commands.

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, Our website is running on a MySQL database and this could be one of the reasons if the front door isn't enabled it is vulnerable to SQL injection attack.

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?

**Yes,** If the custom WAF rule is set to block all traffic from Canada, then anyone residing in Canada will not be able to access the website. This is because we have configured a Geographic match rule statement listing Canada as one of the countries that we want to block traffic from.

However this custom WAF rule can be bypassed if someone residing in Canada uses VPN or proxy to connect the website

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



[Home](#) > [App Services](#) > [rinksyberblog](#) >

## Azure Front Door ...

×



### Azure Front Door

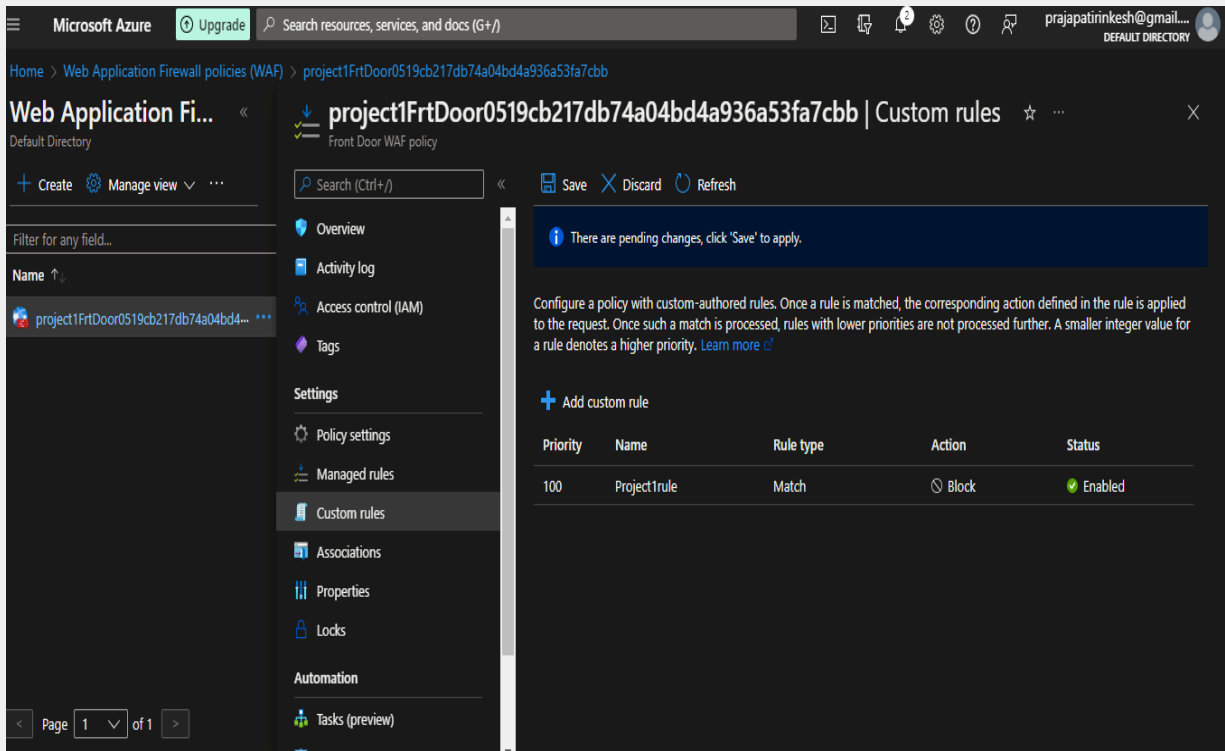
Azure Front Door Service is Microsoft's highly available and scalable web application acceleration platform and global HTTP(s) load balancer. It provides built-in DDoS protection and application layer security and caching. Front Door enables you to build applications that maximize and automate high-availability and performance for your end-users. Use Front Door with Azure services including Web/Mobile Apps, Cloud Services and Virtual Machines – or combine it with on-premises services for hybrid deployments and smooth cloud migration. [Learn more](#)



Azure Front Door is configured for your web app

[project1-fri-door](#)

## b. A WAF custom rule



## 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 the project has been graded.***

yes

Home > App Services > rinkscyberblog

## App Services

Default Directory

+ Create Manage view ...

Filter for any field...

Name ↑

rinkscyberblog

### rinkscyberblog | Custom domains

App Service

cus Refresh Troubleshoot FAQs

#### Settings

- Custom domains
- TLS/SSL settings
- TLS/SSL settings (preview)

Configure and manage custom domains assigned to your app. [Learn more](#)

IP address: 20.211.64.7

Custom Domain Verification ID: 1C2E7553656F7D1F859AF250144687FCAF5E869D4A57D36596F4F14F2F472A56

HTTPS Only: Off

+ Add custom domain

Status Filter

All (1) Not Secure (0) Secure (1)

SSL STATE	ASSIGNED CUSTOM DOMAINS	SSL Binding
Secure	rinkscyberblog.azurewebsites.net	

⚠ This subscription is not eligible to purchase App Service Domains

Home > Key vaults >

## Create a key vault

Basics Access policy Networking Tags **Review + create**

🔗 [View Automation Template](#)

### Basics

Subscription	Azure subscription 1
Resource group	RG_RedTeam_AusEast
Key vault name	rinkscyberblog1-KeyVault
Region	East US
Pricing tier	Standard
Soft-delete	Enabled
Purge protection during retention period	Disabled
Days to retain deleted vaults	90 days

### Access policy

Previous Next Review + create

Microsoft Azure


Upgrade

Search resources, services, and docs (G+)

prajapatirinkesh@gmail...  
DEFAULT DIRECTORY

[Home](#) > [App Services](#) > [rinkscyberblog](#) >

# Azure Front Door



## Azure Front Door

Azure Front Door Service is Microsoft's highly available and scalable web application acceleration platform and global HTTP(s) load balancer. It provides built-in DDoS protection and application layer security and caching. Front Door enables you to build applications that maximize and automate high-availability and performance for your end-users. Use Front Door with Azure services including Web/Mobile Apps, Cloud Services and Virtual Machines – or combine it with on-premises services for hybrid deployments and smooth cloud migration. [Learn more](#)

### Integrate Azure Front Door with your app

Front Door instance \*

project1-Frt-Door

Create new...

OK

11:02 AM

[Home](#) >

# Web Application Firewall policies (WAF)

Default Directory

[+ Create](#)

[Manage view](#)

[Refresh](#)

[Export to CSV](#)

[Open query](#)

[Assign tags](#)

Filter for any field...

Subscription == all

Type == all

Resource group == all

Location == all

Add filter

No grouping

List view

<input type="checkbox"/>	Name ↑↓	Type ↑↓	Resource group ↑↓	Location ↑↓	Subscription ↑↓	
<input checked="" type="checkbox"/>	project1FrtDoor0519cb217db74a04bd4a936a53fa7cbb	Front Door WAF policy	RG_RedTeam_AusEast	Global	Azure subscription 1	...

< Previous

Page 1 of 1

Next >

Showing 1 to 1 of 1 records.

Give feedback

Home > App Services > rinkscyberblog

App Services

Default Directory

Create

Manage view

Filter for any field...

Name ↑↓

rinkscyberblog

Page 1 of 1

rinkscyberblog | Security

App Service

Search (Ctrl+J)

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Security

Events (preview)

Deployment

Quickstart

Deployment credentials

Deployment slots

Deployment Center

Settings

Configuration

For enhanced security with just-in-time access, adaptive application controls and more, upgrade your subscription's Microsoft Defender for Cloud plan

Visit Microsoft Defender for Cloud to manage security across your virtual networks, data, apps, and more

Recommendations

Security alerts

Microsoft Defender for App ServicUnknownes

0

0

Recommendations

Defender for Cloud continuously monitors the configuration of your app services to identify potential security vulnerabilities and recommends actions to mitigate them.

✓

✓

✓