Securing Cloud Applications

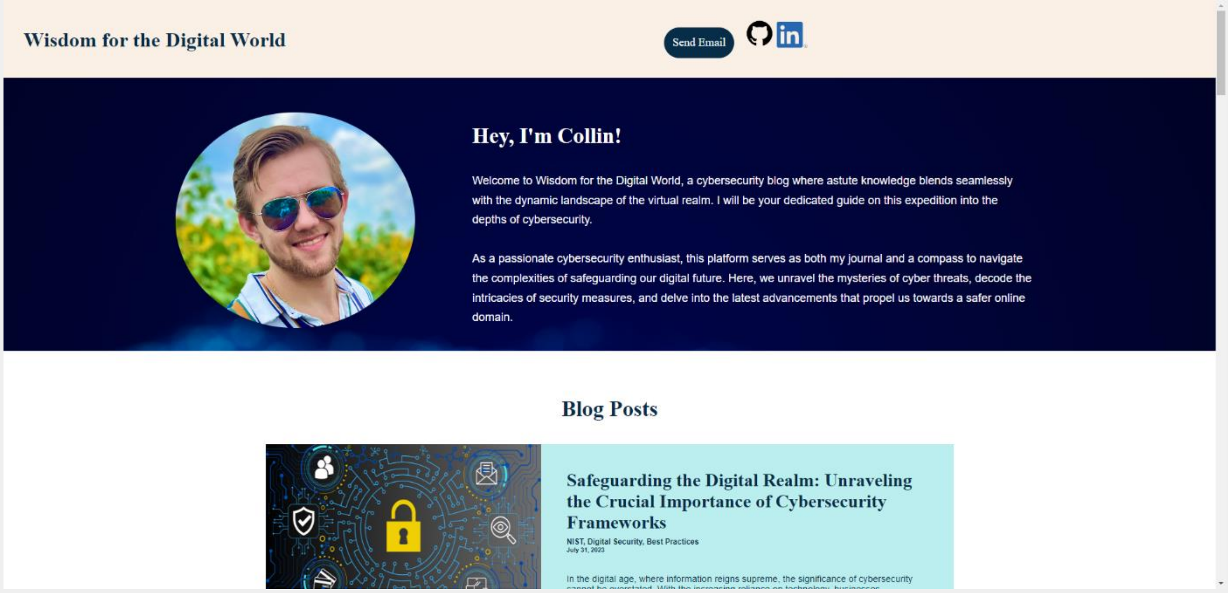
Project Technical Brief

Your Web Application

Enter the URL for the web application that you created:

```
https://collincybersec.xyz/
```

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



Hey, I'm Collin!

Welcome to Wisdom for the Digital World, a cybersecurity blog where astute knowledge blends seamlessly with the dynamic landscape of the virtual realm. I will be your dedicated guide on this expedition into the depths of cybersecurity.

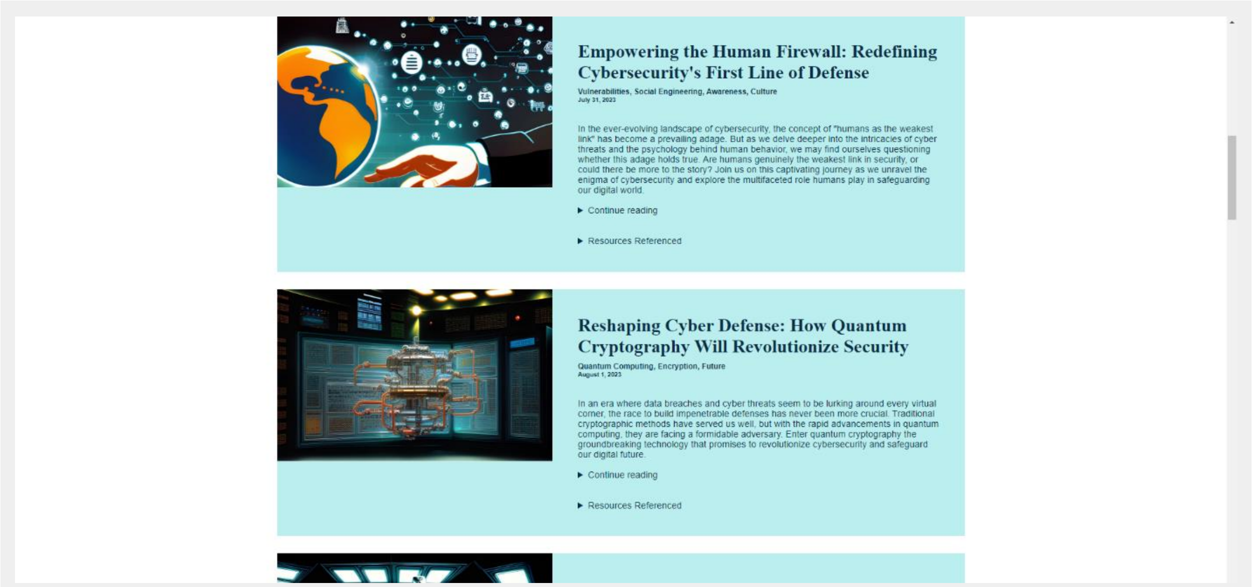
As a passionate cybersecurity enthusiast, this platform serves as both my journal and a compass to navigate the complexities of safeguarding our digital future. Here, we unravel the mysteries of cyber threats, decode the intricacies of security measures, and delve into the latest advancements that propel us towards a safer online domain.

Blog Posts

Safeguarding the Digital Realm: Unraveling the Crucial Importance of Cybersecurity Frameworks

NIST, Digital Security, Best Practices
July 31, 2023

In the digital age, where information reigns supreme, the significance of cybersecurity cannot be overstated. With the increasing reliance on technology, businesses



Empowering the Human Firewall: Redefining Cybersecurity's First Line of Defense

Vulnerabilities, Social Engineering, Awareness, Culture
July 31, 2023

In the ever-evolving landscape of cybersecurity, the concept of "humans as the weakest link" has become a prevailing adage. But as we delve deeper into the intricacies of cyber threats and the psychology behind human behavior, we may find ourselves questioning whether this adage holds true. Are humans genuinely the weakest link in security, or could there be more to the story? Join us on this captivating journey as we unravel the enigma of cybersecurity and explore the multifaceted role humans play in safeguarding our digital world.

▶ Continue reading

▶ Resources Referenced

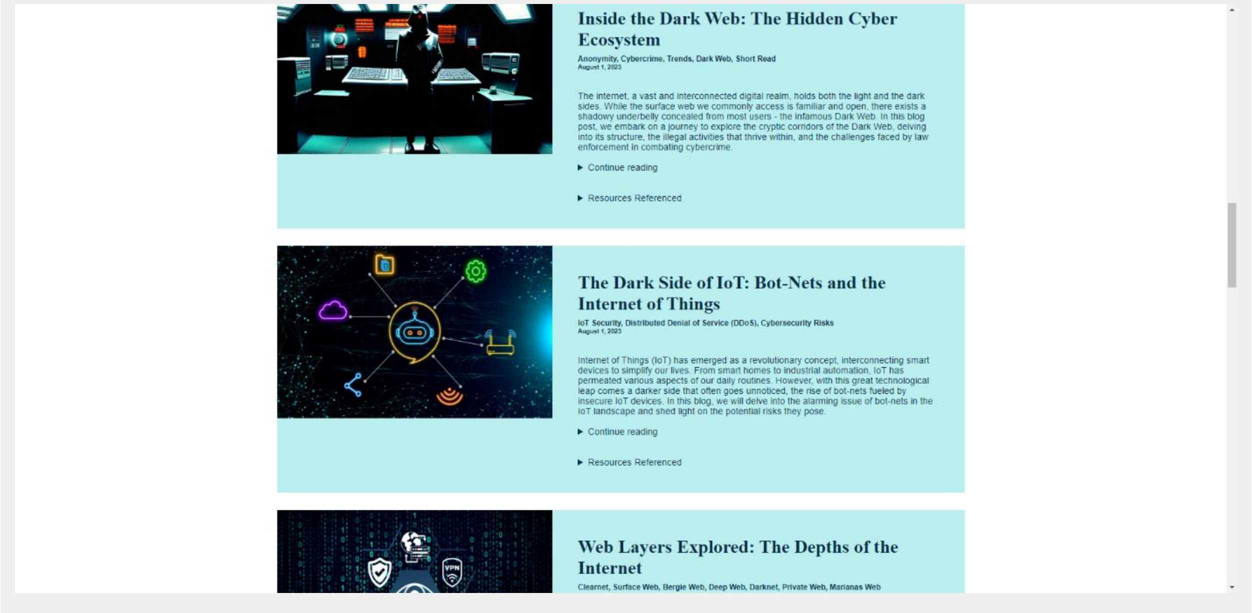
Reshaping Cyber Defense: How Quantum Cryptography Will Revolutionize Security

Quantum Computing, Encryption, Future
August 1, 2023

In an era where data breaches and cyber threats seem to be lurking around every virtual corner, the race to build impenetrable defenses has never been more crucial. Traditional cryptographic methods have served us well, but with the rapid advancements in quantum computing, they are facing a formidable adversary. Enter quantum cryptography the groundbreaking technology that promises to revolutionize cybersecurity and safeguard our digital future.

▶ Continue reading

▶ Resources Referenced



Inside the Dark Web: The Hidden Cyber Ecosystem

Anonymity, Cybercrime, Trends, Dark Web, Short Read
August 1, 2023

The internet, a vast and interconnected digital realm, holds both the light and the dark sides. While the surface web we commonly access is familiar and open, there exists a shadowy underbelly concealed from most users - the infamous Dark Web. In this blog post, we embark on a journey to explore the cryptic corridors of the Dark Web, delving into its structure, the illegal activities that thrive within, and the challenges faced by law enforcement in combating cybercrime.

▶ Continue reading

▶ Resources Referenced

The Dark Side of IoT: Bot-Nets and the Internet of Things

IoT Security, Distributed Denial of Service (DDoS), Cybersecurity Risks
August 1, 2023

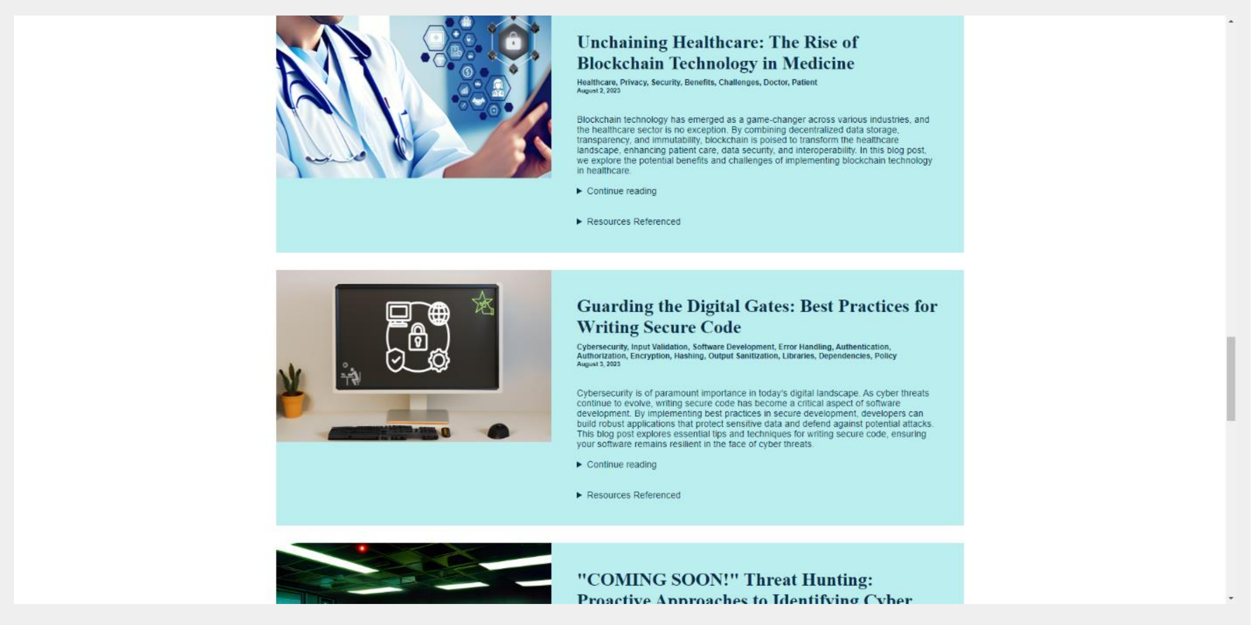
Internet of Things (IoT) has emerged as a revolutionary concept, interconnecting smart devices to simplify our lives. From smart homes to industrial automation, IoT has permeated various aspects of our daily routines. However, with this great technological leap comes a darker side that often goes unnoticed, the rise of bot-nets fueled by insecure IoT devices. In this blog, we will delve into the alarming issue of bot-nets in the IoT landscape and shed light on the potential risks they pose.

▶ Continue reading

▶ Resources Referenced

Web Layers Explored: The Depths of the Internet

Clearnet, Surface Web, Bergie Web, Deep Web, Darknet, Private Web, Marianas Web



Unchaining Healthcare: The Rise of Blockchain Technology in Medicine

Healthcare, Privacy, Security, Benefits, Challenges, Doctor, Patient
August 2, 2023

Blockchain technology has emerged as a game-changer across various industries, and the healthcare sector is no exception. By combining decentralized data storage, transparency, and immutability, blockchain is poised to transform the healthcare landscape, enhancing patient care, data security, and interoperability. In this blog post, we explore the potential benefits and challenges of implementing blockchain technology in healthcare.

▶ Continue reading

▶ Resources Referenced

Guarding the Digital Gates: Best Practices for Writing Secure Code

Cybersecurity, Input Validation, Software Development, Error Handling, Authentication, Authorization, Encryption, Hashing, Output Sanitization, Libraries, Dependencies, Policy
August 3, 2023

Cybersecurity is of paramount importance in today's digital landscape. As cyber threats continue to evolve, writing secure code has become a critical aspect of software development. By implementing best practices in secure development, developers can build robust applications that protect sensitive data and defend against potential attacks. This blog post explores essential tips and techniques for writing secure code, ensuring your software remains resilient in the face of cyber threats.

▶ Continue reading

▶ Resources Referenced

"COMING SOON!" Threat Hunting: Proactive Approaches to Identifying Cyber

Day 1 Questions

General Questions

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

```
I chose a GoDaddy domain.
```

2. What is your domain name?

```
“collincybersec.xyz” is what I chose on GoDaddy.

“https://collincybersec-webapp.azurewebsites.net” is what Azure shows.
```

Networking Questions

1. What is the IP address of your webpage?

```
20.119.8.42
```

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

```
Washington, Virginia, United States of America
```

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

```
Command Used: nslookup collincybersec-webapp.azurewebsites.net

The DNS lookup process resolved the domain "collincybersec-
webapp.azurewebsites.net" to the IP address 20.119.8.42 through a chain of
CNAME records.
```

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 selected is “Php - 8.2”. It works on the back-end,
handling logic and generating dynamic content for the web application.
```

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

```
The assets directory contained two (2) directories, “css” and “images”.

The “css” folder contained CSS files for define the presentation and layout
of the web page written.

The “images” folder contained the images used on the default web page.
```

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

```
Both the "css" and "images" directories inside the "assets" directory are
relevant to the front-end of the web application. They are used to enhance
the visual presentation and user interface of the web page and are processed
and displayed by the client-side (the user's web browser).
```

Day 2 Questions

Cloud Questions

1. What is a cloud tenant?

```
A cloud tenant refers to an individual, organization, or entity that
utilizes cloud services and resources provided by a cloud service provider
(CSP). Essentially, a tenant is a customer or user who rents or subscribes
to the services offered by the CSP. The concept of cloud tenancy is derived
from the analogy of a physical property or building, where multiple tenants
may rent different spaces within the same building.
```

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

```
An access policy on a key vault is essential for maintaining the security
and confidentiality of cryptographic keys, secrets, and certificates stored
within the vault. It allows for controlled access, adhering to the principle
of least privilege and minimizing the risk of unauthorized access. Access
policies ensure secure key management, protect sensitive data, and support
audit and compliance requirements. They also facilitate key rotation and
revocation when necessary, promoting secure development practices within an
organization. Overall, access policies play a critical role in safeguarding
cryptographic assets and maintaining the integrity of a key vault in a
multi-tenant cloud environment.
```

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

```
Keys are cryptographic pairs used for encryption and decryption, secrets are
sensitive data like passwords and API keys used for authentication, and
certificates are digital documents used for identity verification and secure
communication. Properly managing these components in a key vault ensures the
security, confidentiality, and integrity of sensitive data and cryptographic
materials used in various applications and services.

Keys:
Cryptographic keys are a fundamental component of encryption and decryption
processes. They are used to secure and protect data, communications, and
```

digital identities. Keys come in pairs - a public key and a private key. The public key is shared openly and is used for encryption, while the private key is kept secret and is used for decryption. Key vaults store cryptographic keys securely, preventing unauthorized access and ensuring key management best practices. These keys can be used for various cryptographic operations, including encrypting data, generating digital signatures, and establishing secure communication channels.

Secrets:
Secrets in a key vault refer to any sensitive information or data that needs to be kept confidential, such as passwords, connection strings, API keys, or authentication tokens. These are typically used by applications and services to authenticate with other systems or access resources securely. By storing secrets in a key vault, organizations can centralize and secure their sensitive information, ensuring that only authorized applications or users can access them. Using access policies and role-based access controls, key vaults restrict access to secrets and enable the auditing of who accessed the information and when.

Certificates:
Certificates are digital documents used for identity verification and secure communication. They contain information about an entity, such as a public key, and are typically issued by a trusted third-party Certificate Authority (CA). Certificates are used in SSL/TLS to secure website connections, code signing to verify software integrity, and authentication in various network protocols. Key vaults can store and manage certificates securely, enabling organizations to easily manage the lifecycle of certificates, automate certificate renewals, and ensure secure communication across their applications and services.

Cryptography Questions

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

Cost-effective: Obtaining a certificate from a recognized certificate authority often involves a cost, especially for commercial purposes. Self-signed certificates, on the other hand, are free to create and use.

Quick and Easy Setup: Generating a self-signed certificate is a straightforward process, and it can be done quickly without the need to go through the validation process with a third-party CA. This is especially useful for testing and development environments.

Internal Use: Self-signed certificates are commonly used for internal purposes, such as securing communication between different components or services within an organization. Since internal systems often do not require validation by external CAs, self-signed certificates can serve this purpose effectively.

Encryption and Data Integrity: Like certificates issued by CAs, self-signed certificates also enable encryption and ensure data integrity during communication. This means that data transmitted over secure connections using a self-signed certificate remains encrypted and protected from potential eavesdropping and tampering.

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

No Trust by Default: The most significant drawback of self-signed certificates is that they are not trusted by default by web browsers or other software. Users visiting a website secured with a self-signed certificate will often see a warning message, indicating that the site is not trusted. This can lead to a negative user experience and may deter visitors from accessing the site.

Security Risks: Self-signed certificates are more susceptible to man-in-the-middle attacks. Since they are not issued by a trusted CA, attackers can potentially intercept communication and present their own self-signed certificate, tricking users into believing they are connecting to a legitimate site.

Not Suitable for Public-Facing Websites: Due to the lack of trust, self-signed certificates are generally unsuitable for public-facing websites or e-commerce platforms, where establishing trust with visitors is crucial for the success of the website.

Certificate Management: Managing self-signed certificates in large-scale environments can become cumbersome, as each device or user connecting to the system needs to install the self-signed certificate separately.

3. What is a wildcard certificate?

A wildcard certificate is a type of SSL/TLS (Secure Sockets Layer/Transport Layer Security) certificate that is designed to secure multiple subdomains under a single domain with a single certificate. It is denoted by an asterisk (*) symbol, known as a wildcard character, which is placed before the main domain name in the certificate. The wildcard character represents any subdomain of the main domain.

For example, if you have a wildcard certificate for "*.example.com," it will secure any subdomain under "example.com," such as "mail.example.com," "app.example.com," "blog.example.com," and so on.

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.

Here are the main reasons why SSL 3.0 is not supported:

POODLE Vulnerability: SSL 3.0 is vulnerable to a serious security flaw known as Padding Oracle On Downgraded Legacy Encryption (POODLE). This vulnerability allows attackers to exploit the protocol's padding mechanism to decrypt secure connections and gain access to sensitive information, such as login credentials and cookies.

Weak Encryption Algorithms: SSL 3.0 relies on older and weaker encryption algorithms compared to its successors, TLS 1.0, TLS 1.1, and TLS 1.2. The usage of weak algorithms makes SSL 3.0 more susceptible to cryptographic attacks and increases the risk of data interception or tampering.

Obsolete and Deprecated: SSL 3.0 was released in 1996, and its security flaws have become increasingly apparent over time. As a result, it has been deprecated and replaced by more secure versions, such as TLS 1.0, TLS 1.1, and TLS 1.2.

Lack of Forward Secrecy: SSL 3.0 lacks forward secrecy, a crucial security feature provided by its successors. Forward secrecy ensures that even if an attacker gains access to a server's private key in the future, they cannot decrypt past encrypted communications. This added protection is essential for safeguarding data in the long term.

Industry-Wide Phasing Out: In response to the numerous security vulnerabilities, major web browsers and online services have been gradually phasing out support for SSL 3.0. As a result, maintaining SSL 3.0 support can lead to compatibility issues and expose users to unnecessary security risks.

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 was shown, the certificate was implemented correctly.
```

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

```
The validity period is as follows:

Issued On   Wednesday, August 2, 2023 at 7:00:00 PM
Expires On  Saturday, February 3, 2024 at 5:59:59 PM
```

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

```
Yes, GeoTrust Global TLS RSA4096 SHA256 2022 CA1.
```

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

```
Yes, DigiCert Global Root CA.
```

    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.

```
Microsoft Azure.
```

Day 3 Questions

Cloud Security Questions

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

Azure Web Application Gateway and Azure Front Door are both Azure services that play a significant role in managing and optimizing web traffic for applications hosted on Azure. While they have some similarities, they also have distinct features and use cases.

Similarities:

1. **Traffic Routing**: Both services are responsible for routing and directing incoming web traffic to backend web applications hosted in Azure. They act as reverse proxies, receiving requests from clients and forwarding them to the appropriate backend servers.

2. **SSL Termination**: Both services can terminate SSL/TLS (Secure Sockets Layer/Transport Layer Security) connections, relieving backend servers from handling the encryption and decryption process. This enhances backend server performance and simplifies certificate management.

3. **Load Balancing**: Both services support load balancing capabilities to distribute incoming traffic across multiple backend servers, improving application scalability and performance.

4. **Global Distribution**: Both Azure Web Application Gateway and Azure Front Door are designed to handle web applications with a global user base. They provide mechanisms for distributing traffic to geographically dispersed backend pools, enhancing the user experience and reducing latency.

Differences:

1. **Layer of Operation**: Azure Web Application Gateway operates at the application layer (Layer 7 of the OSI model). It can inspect HTTP and HTTPS traffic, making it ideal for routing and load balancing traffic for web applications based on URL path, host headers, and other HTTP-specific attributes.

Azure Front Door operates at the network edge, closer to the client, and can handle traffic at both the application layer (Layer 7) and transport layer (Layer 4). It is primarily designed for global HTTP(S) load balancing and optimizing content delivery, offering features such as content caching and acceleration.

2. **Use Cases**: Azure Web Application Gateway is best suited for scenarios where advanced web application delivery and protection features are needed, such as SSL offloading, session affinity, URL-based routing, and WAF (Web Application Firewall) capabilities.

Azure Front Door is designed for scenarios where you require a global HTTP(S) load balancer with content acceleration and caching. It is ideal for multi-region applications, improving performance for geographically dispersed users.

3. **Backend Target Types**: Azure Web Application Gateway can route traffic to backend VMs (Virtual Machines), Azure App Services, or any public IP address.

Azure Front Door can route traffic to backend pools consisting of Azure App Services, Azure VMs, and even external endpoints outside of Azure.

4. **Security Features**: Azure Web Application Gateway offers Web Application Firewall (WAF) capabilities to protect web applications from common web vulnerabilities and attacks.

Azure Front Door provides rate-limiting, authentication, and integration with Azure Monitor for monitoring and alerting.

In summary, Azure Web Application Gateway and Azure Front Door are both powerful Azure services for managing and optimizing web traffic, but they target different use cases and operate at different layers of the network stack. Web Application Gateway focuses on application-layer features and security for web applications, while Front Door is more geared towards global HTTP(S) load balancing and content acceleration. The choice between the two depends on the specific requirements of your web applications and your traffic optimization needs.

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

SSL offloading, also known as SSL termination or SSL acceleration, is a process where SSL/TLS (Secure Sockets Layer/Transport Layer Security) encryption and decryption tasks are offloaded from the backend servers to a dedicated device or service, such as a load balancer or a gateway.

Benefits of SSL Offloading:

Reduced Backend Server Load: SSL/TLS encryption and decryption are computationally intensive processes that can put a significant burden on backend servers, especially when handling a large number of client connections. Offloading these tasks to a dedicated device, such as a load balancer or gateway, frees up backend resources to focus on serving application logic and improving overall performance.

Simplified Certificate Management: By performing SSL termination at the load balancer or gateway, you can manage SSL/TLS certificates in a central location. This eliminates the need to install and manage individual certificates on each backend server, streamlining certificate maintenance.

Better Performance and Scalability: SSL offloading improves the responsiveness and scalability of web applications. Backend servers can process more requests in less time since they are relieved of the CPU-intensive SSL/TLS operations.

Enhanced Security and Compliance: SSL offloading allows you to implement additional security measures, such as Web Application Firewall (WAF) inspection, at the load balancer or gateway, enhancing the security posture of your web applications.

Support for Legacy Backends: In some cases, backend servers might not support the latest SSL/TLS versions or encryption ciphers. SSL offloading allows you to maintain secure client connections while using less secure protocols or cipher suites for communication between the load balancer/gateway and the backend servers.

To summarize, SSL offloading is a valuable feature of Azure Web Application Gateway and Azure Front Door that helps improve the performance, scalability, and security of web applications by handling SSL/TLS encryption and decryption tasks on behalf of the backend servers. It simplifies certificate management, reduces server load, and enhances overall application performance.

3. What OSI layer does a WAF work on?

A Web Application Firewall (WAF) typically operates at the application layer, which is Layer 7 of the OSI (Open Systems Interconnection) model.

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

Chosen rule: SQL injection

Definition: The Web Application Firewall (WAF) managed rule "SQL injection" is a security feature designed to protect web applications from SQL injection attacks. SQL injection is a type of web application vulnerability where malicious SQL code is injected into input fields or parameters of a web application, allowing an attacker to manipulate the application's underlying database and potentially gain unauthorized access to sensitive data or perform harmful operations.

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?

The absence of the Front Door does not directly impact my website's susceptibility to SQL injection. Azure Front Door is primarily a global HTTP(S) load balancer and content accelerator that optimizes traffic delivery. While it may offer certain security features, it is not specifically designed to protect against application-level vulnerabilities like SQL injection.

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?

If I were to create a custom Web Application Firewall (WAF) rule to block all traffic from Canada, it would mean that anyone who is physically located in Canada would likely not be able to access my website.

This is due to the following:

IP Address-Based Blocking: WAF rules are often based on filtering traffic by IP addresses. By blocking all traffic from Canada, the WAF would reject any incoming requests originating from IP addresses associated with Canadian ISPs (Internet Service Providers).

Geolocation Accuracy: Geolocation databases are used to map IP addresses to specific geographic locations. While they can be quite accurate, they are not perfect. There may be instances where an IP address appears to be associated with Canada but is, in fact, being used by someone outside the country. Conversely, there might be cases where someone in Canada is using an IP address associated with another country.

Residency vs. Location: Blocking traffic from Canada based solely on IP addresses would affect both Canadian residents and non-residents temporarily in Canada, such as tourists or business travelers. Similarly, it would not block access from Canadian citizens who are currently residing outside the country.

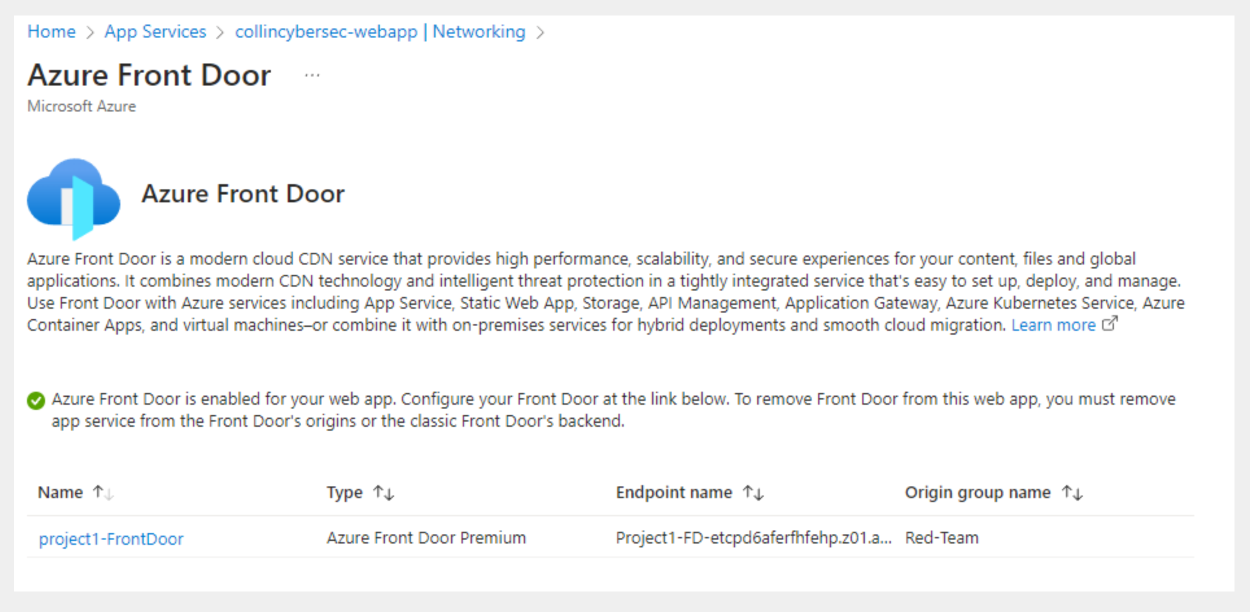
Proxy Servers and VPNs: People might use proxy servers or virtual private networks (VPNs) to hide their true locations or bypass restrictions. If someone in Canada uses a VPN server located outside Canada, they may be able to access the website despite the blocking rule.

Collateral Blocking: Blocking an entire country could inadvertently affect legitimate visitors from Canada who are not causing any harm or security risks. This can lead to a negative user experience for some of your potential customers.

Legal and Ethical Considerations: Blocking an entire country may raise legal and ethical concerns, especially if there is no valid reason or justification for the restriction. International businesses need to be mindful of applicable laws and regulations, including privacy and data protection requirements.

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

    a. Azure Front Door enabled



Azure Front Door

Microsoft Azure

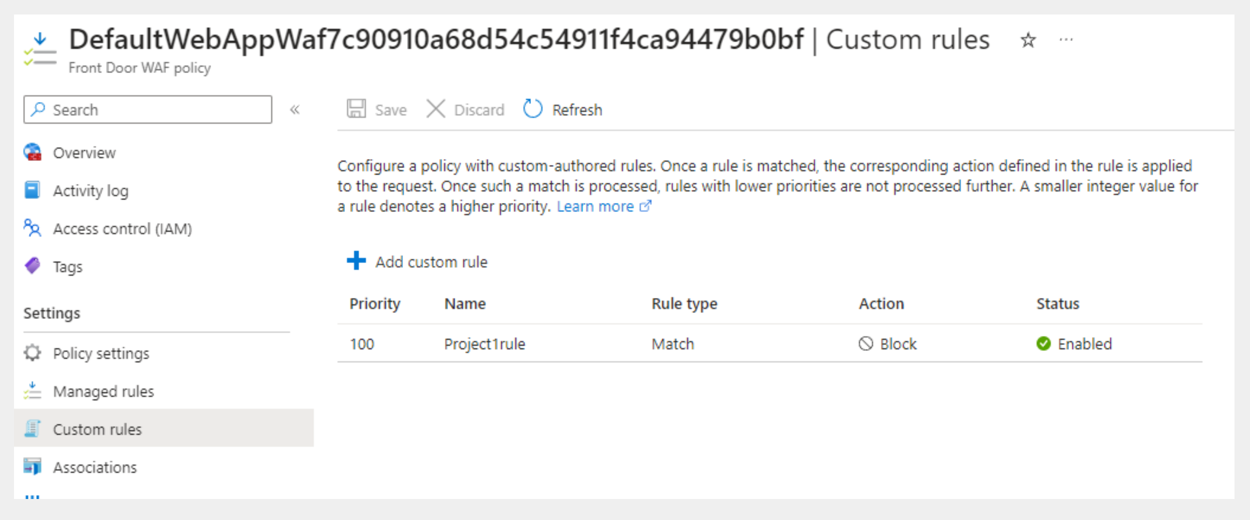
Azure Front Door

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 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-etcpd6aferfhfehp.z01.a...	Red-Team

b. A WAF custom rule


DefaultWebAppWaf7c90910a68d54c54911f4ca94479b0bf | Custom rules

Front Door WAF policy

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.*

- ***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