# GoDaddy Web Application Firewall (WAF)

# Module 4 Assignment Submission

# Scope and Objectives Report

by

Neel Prajapati

CS6525 – Software Requirements Analysis

University of New Brunswick

DISCLAIMER: This report is not affiliated in any way with GoDaddy, nor does it intend to provide an accurate view of how GoDaddy conducts their business activities. This is a learning exercise at the University of New Brunswick based on unfounded assumptions and “best guesses” made by the author. The author has no inside knowledge of how GoDaddy’s software or business practices work. The objective is to simulate how requirements analysis might have been documented during the development of WAF for GoDaddy’s.

# Table of Contents

# 1. Introduction

This document is the first requirements deliverable produced for the GoDaddy Web Application Firewall (WAF) project. The purpose of this document is to capture the project team's consensus on:

- The factors that led to the development of WAF
- The primary stakeholders who will be impacted by WAF development
- The system objectives, which define the fundamental business-level improvements GoDaddy wants to experience once WAF is deployed
- Any known constraints that may limit the design of WAF
- The preliminary system scope
- Definitions for terms and acronyms relevant to the WAF project

# 2. Project Background

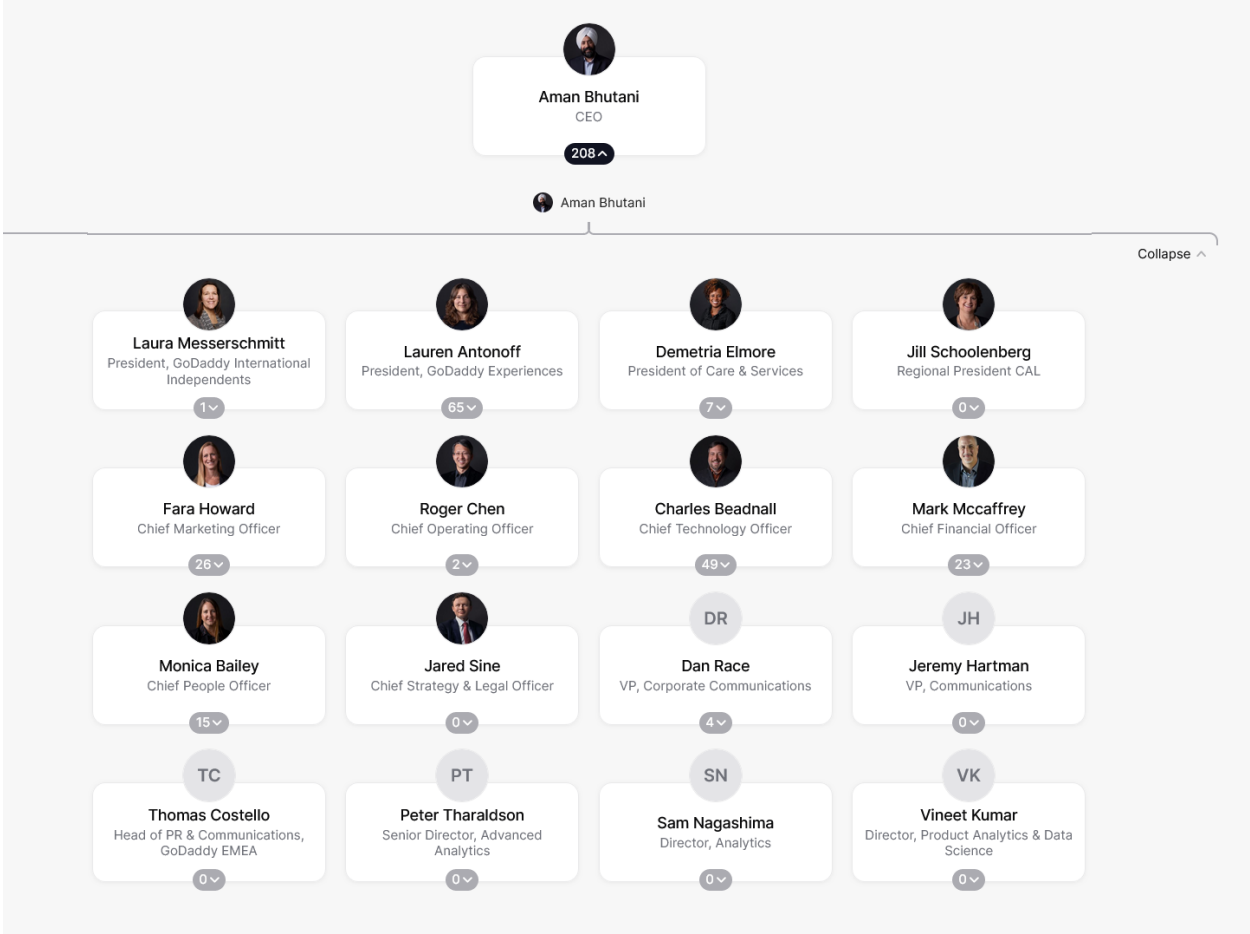
Being the largest web hosting provider by number of websites hosted, web hosting services constitute a major portion of GoDaddy's revenue. With the rise of cloud service providers, the market share of GoDaddy has been declining due to it not providing the detailed management functionality, making it less suitable for web applications with large traffic and data flows.

Development of WAF is an attempt to provide GoDaddy's customers with a comprehensive control functionality to secure their websites according to their specific needs.

# 3. Stakeholders

## GoDaddy Organizational Chart

Source:
https://theorg.com/org/godaddy




## System Owner

- **Charles Beadnail**, the Chief Technology Officer of GoDaddy, will serve as the system owner for the WAF project. Given the strategic importance and technical complexity of the project, it is essential that an individual in an executive position with technical knowhow be responsible for the success of the WAF development.

## Potential End Users

- **The Web Security Products team** is responsible for developing and maintaining all the Web security products. WAF being a security functionality, Web Security Products team will be responsible for the management and monitoring of WAF upon its successful development.

- **Regional Operations teams** look after the operations of GoDaddy services in different regions around the globe. They are primarily responsible for operations and maintenance of the servers allocated to them. The operations teams also have their cyber security teams, which will support the deployment and operations of the WAF and can provide valuable inputs to the project.
- **The Enterprise Products team** manages relationships with **Enterprise Customers** and provides them with customized service bundles suitable for their high traffic requirements. Such enterprise customers will be the primary users of WAF, access to which will be provided by the Enterprise Products team.

### Other Stakeholders

- **GoDaddy management** has members representing all aspects of the organization's activities. As a result, keeping them informed and soliciting their input on the project is critical for the positive business outcome of the WAF.
- **The Product Analytics team** is where all the new product needs are supported by data showing such a need. The team processes user feedback and recommends new functionality based on their market analysis. The Product Analytics team has the expertise to recommend specific features to be included in the WAF. They can also provide inputs on the relative importance of specific features to assist in prioritization of development of such features.
- **The Advanced Analytics team** is responsible for providing technical analytics functionalities in GoDaddy products. The WAF is expected to use state of the art data analytics for providing protection rules, making the advanced analytics team an integral R&D partner for the WAF project team.

## 4. System Objectives

The following are the system objectives for WAF.

#### OBJECTIVE-001

**Requirement:** Develop WAF with industry standard firewall functionality for deployment alongside GoDaddy CDN. The standard functionallity includes firewall rule management, monitoring and result analysis & reporting.

**Who benefits and how:** The WAF product will allow GoDaddy to extend its customer base by offering customers the ability to customize the security functionality as per their needs.

**How / when to measure:** Once WAF design is complete, compare it with standrad features of competitors' product offerings.

**Origin:** GoDaddy management provided the input for the development of WAF.

#### OBJECTIVE-002

**Requirement:** Any combination of WAF rules should not add more than 1ms of delay in any request.

**Who benefits and how:** Customers are expected to add hundreds of rules as the threats they face evolve. Application of such rules to requests if processed quickly will benefit Cloudflare by reducing resource requirements. Less than 1ms of processing time will ensure that this additional delay is imperceptible to website users.

**How / when to measure:** Once WAF development is complete, measure the introduced delay.

**Origin:** The Product Analytics team provided the input for the objective.

### OBJECTIVE-003

**Requirement:** Provide alternate interaction less challenge mechanisms in place of traditional Captcha challenge.

**Who benefits and how:** Captcha discourages human visitors of websites from proceeding with solving the challenge and then continuing their visit. An interaction less or minimal interaction challenge reduces the inconvenience for the website users.

**How / when to measure:** Upon deployment the functioning alternate challenge mechanism functionality must be made available.

**Origin:** The Product Analytics team provided the input for the objective.

### OBJECTIVE-004

**Requirement:** To enable bot management functionality that calculates bot score for each request based on data analytics.

**Who benefits and how:** Malicious bots are known to cause cyber-attacks such as credential stuffing, DDoS and disturb the website analytics. With Web Security Products teams' analysis showcasing that ⅔ of traffic is generated by bots, an effective bot management functionality is going to benefit GoDaddy, its web hosting customers as well as the users of hosted websites.

**How / when to measure:** Before deployment the Bot management functionality to be successfully demonstrated on existing customers' web hostings.

**Origin:** The Product Analytics team and the Web Security Products team provided the input for the objective.

### OBJECTIVE-005

**Requirement:** Once deployed, WAF functionality can be enabled for all web hosting customers, irrespective of service selected.

**Who benefits and how:** The WAF product is being targeted towards enterprise customers, however it is likely that other customers in future may request access to WAF.

The ability to extend the WAF service to all customers will benefit GoDaddy by not requiring any changes to WAF for extension its offering to other categories of customers.

**How / when to measure:** Once WAF development is complete, is it possible to make it available to any web hosting customer of GoDaddy?

**Origin:** The Product Analytics team and the Web Security Products team provided the input for the objective.

### OBJECTIVE-006

**Requirement:** Allow for selective enablement of WAF functionality for each customer.

**Who benefits and how:** The WAF is being developed as a comprehensive service, however not all customers will be willing to pay for an all-inclusive bundle. The ability to enable different features as per the customers' needs will benefit the enterprise products team by letting them provide a tailor-made product bundle to each customer.

**How / when to measure:** Once WAF development has been completed, is it possible to offer combinations of different features of WAF to each customer?

**Origin:** The Enterprise Products team provided the input for the objective.

### OBJECTIVE-007

**Requirement:** Develop WAF that allows creation of firewall rules based on calculated scores such as bot score, attack score and threat score.

**Who benefits and how:** The implementation behind the data analytics-based scores may evolve in the future. Scores provide a level of abstraction, to avoid having customers dealing with the ever-changing identification analytics. With such an arrangement, rules created by customers based on scores will not have to change as the score calculation models change in the background to accommodate the evolving nature of threats, attacks, bots, etc.

**How / when to measure:** Once WAF development is complete, is it possible to create firewall rules based on scores?

**Origin:** The Enterprise Products team provided the input for the objective.

### OBJECTIVE-008

**Requirement:** Ensure that WAF features made available to customers comply with country specific regulations that apply to them.

**Who benefits and how:** different countries have varying privacy regulations that influence how data is stored, transmitted and processed. WAF will be deployed along with CDN, as a result the customers served will be from many different countries and even multinationals organizations, virtually all having global user bases. For this reason, regulation compliance will directly benefit the customers by streamlining their use of WAF.

**How / when to measure:** Once WAF development is complete, are all features in compliance with the prevalent regulations of jurisdiction in which they are to be deployed?

**Origin:** The Enterprise Products team provided the input for the objective.

### OBJECTIVE-009

**Requirement:** Design WAF to have high availability and reliability through proper integration with CDN.

**Who benefits and how:** High availability and redundancy are core characteristics of GoDaddy CDN. With proper integration with CDN, the services of WAF will stay online even if some nodes fail. Interruption free operation of WAF will benefit GoDaddy as well as WAF customers.

**How / when to measure:** Once WAF design is complete, perform audit of the design to ensure that it meets high availability and reliability standards.

**Origin:** The Enterprise Products team provided the input for the objective.

*Inspired by ChatGPT 3.5 – see Section 8

## 5. Known Constraints that Limit the Software Design

Constraints are factors that limit how the software can be designed.

### CONSTRAINT-001

**Requirement:** Advanced features of WAF rely on data analytics done on user requests. All such analysis on requests will have to be performed immediately, as customer requests containing data can not be stored for future analysis.

**Rationale:** Data in the requests passing through GoDaddy servers may contain sensitive information, as a result making GoDaddy responsible for securing it if it is stored. Customers will also have to be informed of such storage of data through policy change, which can cause backlash.

**How / when to measure:** Once WAF development is complete, is WAF storing any information that was part of the data being transferred by requests?

**Origin:** The Advanced Analytics team and the Web Security Products team provided the input for the constraint.

# 6. Preliminary System Scope

System scope defines what functionality is to be included in WAF.

This section defines WAF SYSTEM in the following ways:

- An informal description of the current vision for WAF functionality.
- A list of business events and associated use cases, which help to clarify scope by identifying data flowing in and out of the boundary of the system scope.
- A context diagram, which provides a visual representation of data flowing in and out of the boundary of the system scope.
- A list of capabilities that are to be excluded from WAF, which can help lessen potential ambiguity in how system scope might be interpreted.

## Informal Description of Functionality

GoDaddy provides web hosting services and web security for the hosted web sites. In an effort to make the services more suitable to the needs of large websites receiving huge amounts of traffic, GoDaddy is developing a WAF that provides its customers the ability to manage the security of their hosted sites as per their own security posture.

When developed, WAF will be a dashboard that will allow customers to set and manage rules to filter traffic with the intention of keeping their websites safe. The WAF will also provide analytics on the performance of set rules and will also let the customers check the details of individual requests that have been blocked by specific firewall rules.

## Business Events

A **business event** is an action that initiates some part of the work GoDaddy performs while supporting the Enterprise Products team and Enterprise customers. The response to each event is called a **business use case**, representing a discrete functional **partition** of the work. Later, this partitioning will enable us to focus on one business use case at a time when determining more detailed requirements. The **inputs and outputs** clarify the **scope** of the work (in other words, what's in versus what's out).

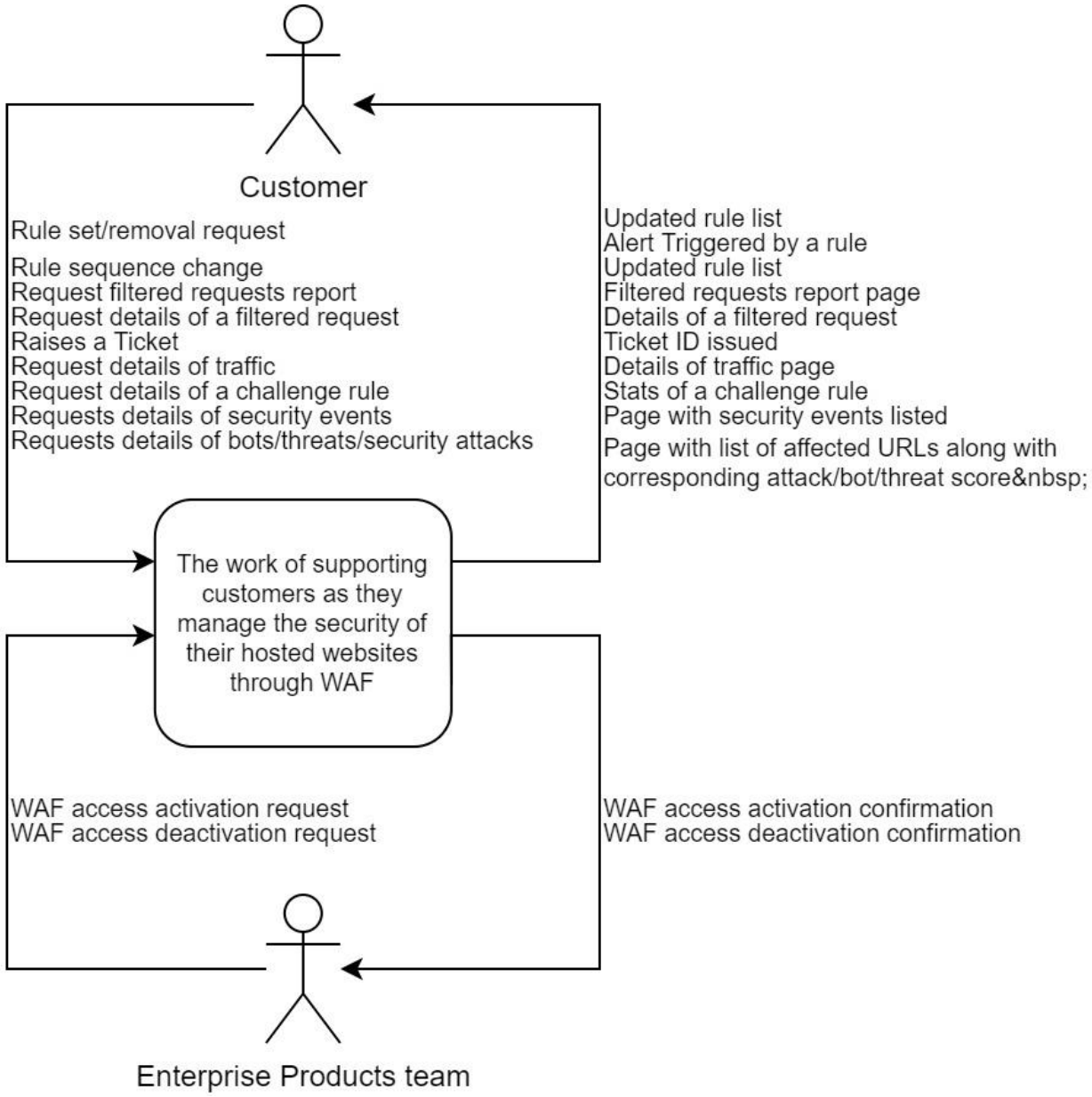
| **Event Name** (include initiating actor)<br>○ Supports Objective(s) | **Input and Output** | **Use Case Summary** |
|---|---|---|
| **EVENT-001**<br>Enterprise Products team enables/disables WAF functionality for a customer<br>○ OBJECTIVE-006 | WAF functionality info. And Customer ID (in)<br>WAF functionality enabled/disabled (out) | Upon receiving the request to enable/disable a WAF functionality for a customer, the Enterprise Products team subscribes/unsubscribes that customer to the requested functionality. |
| **EVENT-002**<br>Customer sets/removes a firewall rule<br>○ OBJECTIVE-003<br>○ OBJECTIVE-007 | Rule information (in)<br>Rule list updated (out) | Provide confirmation of successful rule list update. |
| **EVENT-003**<br>Rule triggers alert<br>○ OBJECTIVE-001 | Customer receives alert (out) | Alert sent to the communication mode selected by customer. |
| **EVENT-004**<br>Customer alters the sequence in which the the rules are applied<br>○ OBJECTIVE-001 | Sequence alteration request (in)<br>Confirmation of sequence alterations (out) | Sequence change recorded |
| **EVENT-005**<br>Customer requests a report of requests filtered by a rule | Report request (in)<br>Report page displayed (out) | Report page contains graphs showcasing numbers of requests filtered in a period. |

| | | |
|---|---|---|
| ○ OBJECTIVE-001 | | |
| **EVENT-006**<br>Customer requests details of a filtered request<br>○ OBJECTIVE-00x | Details of filtered request requested (in)<br>Details page displayed (out) | Page contains information of filtered request such as time, payload size, region, IP address, etc. |
| **EVENT-007**<br>Customer raises a ticket for an issue<br>○ OBJECTIVE-001 | Ticket request received by system (in)<br>Ticket ID issued (out) | Ticket request recorded in the system. Tickets could cover issues such as continuous challenge application on a customer, false positive filtering of a request, etc. |
| **EVENT-008**<br>Customer requests details of traffic grouped by IP address, region, date, time etc.<br>○ OBJECTIVE-001 | Details of traffic request (in)<br>Traffic details page displayed (out) | Provides summary of traffic as timeseries graph. |
| **EVENT-009**<br>Customer requests details of filtered requests grouped by region, date, time etc.<br>○ OBJECTIVE-001 | Details of request filteration based on selected critieria requested (in)<br>Filtered requests page displayed (out) | Lists requests filtered and provides stats of filteration. |
| **EVENT-010**<br>Customer requests details of a challenge rule.<br>○ OBJECTIVE-001 | Request for stats of challenge performance (in)<br>Stats information displayed (out) | Provides information such as rule hit count and success rate. |
| **EVENT-011**<br>Requests details of security events grouped by region, date, time, etc.<br>○ OBJECTIVE-001 | Request for details of security events for selected criteria (in)<br>Display page with security events listed (out) | Security events include unusually high rate of requests, removal of large amount of data, etc. |

| | | |
|---|---|---|
| **EVENT-012**<br>Customer request details of bots/threats/security attacks based on URLs attacked. Filtered based on criteria such as time, date, region, network provider, IP.<br>○ OBJECTIVE-001 | Request for details of bot/threat/security for selected criteria (in)<br>Display page with list of affected URLs along with attack/bot/threat score(Out) | Attack Information can include frequency of attacks, types of attacks ( SQL injection, cross site scripting), etc.<br><br>For Bot management, information will be stats of requests categorized into likely humans and likely bots along with histograms of scores. |

## Context Diagram

The following context diagram provides a visual summary of the “inputs and outputs” identified for the business events on the preceding pages. These inputs and outputs clarify the scope of the functionality to be included in WAF.



## Functionality to be Excluded

The following are examples of business functions that are not within the scope of WAF:

- Any billing and payment processing of services of WAF enabled for customers.
- Any functionality of malware detection on data not destined for GoDaddy, i.e., data that is passing through GoDaddy systems but is GoDaddy is not the recipient.
- Any new hardware development.
- Manual Cyber-attack response service.
- Traffic monitoring service by security expert.
- Security of any components of GoDaddy infrastructure.
- Security of the data of customers and their visitors stored on GoDaddy servers.

*Inspired by ChatGPT 3.5 – see Section 8

## 7. Terminology and Acronyms

*NOTE: The information in this section will be updated throughout the project as new terminology arises.*

**WAF -** Web Application Firewall

**CDN -** Content Delivery Network

**Enterprise customers** - In web hosting context, these are customers with large hostings that require large bandwidth due to the volume of traffic

**DDoS -** Distributed Denial of Service Attack

**Credential Stuffing -** Cyber attack which uses stolen credentials data to take control of multiple accounts

**Bot/Threat/Attack score -** Scores ranging from 1 to 100, calculated using data analytics that simplify creation of firewall rules for bot management, attack response and threat analytics

**IP -** Internet Protocol (address)

## 8. Ideas Suggested by ChatGPT

The following query was submitted to ChatGPT 3.5 on [date], producing the results shown below. These results were used as a completeness check for the requirements presented in preceding sections of this document.

Note: Text in this section marked with yellow highlighting has been used to enhance ideas presented elsewhere in this document.

**The query submitted to ChatGPT:**

Provide a list of system objectives for Web Application Firewall project

**The result returned by ChatGPT:**
Sure, here's a list of potential system objectives for a Web Application Firewall (WAF) project:
1. **Security Enhancement**: Protect web applications from common security threats such as SQL injection, cross-site scripting (XSS), cross-site request forgery (CSRF), and other OWASP Top 10 vulnerabilities.
2. **Access Control**: Control and monitor access to web applications based on predefined security policies and rules.
3. **Traffic Inspection**: Analyze incoming and outgoing web traffic to detect and block malicious activities, anomalies, and suspicious patterns.

4. **Real-time Monitoring**: Provide real-time monitoring and logging capabilities to track and analyze web traffic for security incidents and potential threats.
5. **Performance Optimization**: Optimize the performance of web applications by offloading security-related tasks to the WAF, reducing the workload on application servers.
6. **Compliance**: Ensure compliance with industry standards and regulations (e.g., PCI DSS, HIPAA) by implementing necessary security controls and logging mechanisms.
7. **Scalability**: Scale the WAF solution to accommodate increasing web traffic and application complexity without sacrificing security or performance.
8. **Customization**: Allow customization of security rules, policies, and configurations to adapt to the specific requirements of different web applications and environments.
9. **Ease of Management**: Provide a user-friendly interface for configuration, management, and monitoring of the WAF solution, minimizing the need for manual intervention and technical expertise.
10. **High Availability**: Ensure high availability and reliability of the WAF solution through redundancy, failover mechanisms, and proactive monitoring to prevent downtime and ensure continuous protection.
11. **Threat Intelligence Integration**: Integrate with threat intelligence feeds and databases to stay updated on emerging threats and incorporate threat intelligence into security policies and decision-making processes.
12. **Reporting and Analytics**: Generate comprehensive reports and analytics on web traffic, security events, and incidents to facilitate compliance audits, security assessments, and performance optimization efforts.
13. **Incident Response**: Provide capabilities for incident response, including alerting, blocking, and mitigation of security incidents in real-time to minimize the impact of security breaches or attacks.
14. **API Integration**: Offer APIs for seamless integration with other security tools, applications, and infrastructure components to enable automation, orchestration, and interoperability.

These objectives can serve as a foundation for defining the scope, requirements, and success criteria of a WAF project.

**The query submitted to ChatGPT:**

provide a list of items that should be excluded from the scope of Web Application Firewall project

**The result returned by ChatGPT:**

Certainly! Here's a list of items that might be excluded from the scope of a Web Application Firewall (WAF) project:

1. Network-level security measures: Items related to firewall rules, network segmentation, and intrusion detection/prevention systems (IDS/IPS) should be excluded from the WAF project scope.

2. Server hardware and infrastructure: Configuration or maintenance of physical server hardware, network switches, routers, and other infrastructure components are typically outside the scope of a WAF project.

3. Operating system (OS) security: Security measures specific to the underlying operating system of the web servers, such as patch management, antivirus software, and OS-level firewalls, are not usually part of a WAF project.

4. Application development or coding: Responsibilities related to coding, programming, or development of the web applications themselves are generally not included in the WAF project scope.

5. Database security: Activities related to securing databases, such as database access controls, encryption, and database activity monitoring, would typically fall outside the scope of a WAF project.

6. Business continuity and disaster recovery planning: While important for overall security posture, activities related to business continuity planning, disaster recovery procedures, and data backup strategies are usually not part of a WAF project.

7. Compliance and regulatory requirements: Ensuring compliance with industry standards or regulatory requirements (e.g., PCI DSS, GDPR) may be addressed separately from the WAF implementation.

8. User training and awareness: Educating users about security best practices and raising awareness about potential threats typically falls outside the scope of a WAF project.

9. Performance tuning and optimization: Fine-tuning web server performance, load balancing, caching strategies, and other performance optimization tasks are generally not part of the WAF project scope.

10. Legal or contractual obligations: Activities related to legal matters, contractual agreements, or negotiations with vendors or third parties would be handled separately from the technical implementation of a WAF.