**FORMAN CHRISTIAN COLLEGE**

**(A CHARTERED UNIVERSITY)**

**DEPARTMENT OF COMPUTER SCIENCE**

**LAHORE, PAKISTAN**

**(2021)**

**TITLE:** API-FIREWALL

**Project Proposal by:**

Hassan Afzal 22-11025

Mir Hassan 22-11007

**Advisor:**

Mr. Saad Saleem

1

***PROJECT DESCRIPTION***

* **INTRODUCTION**

The AP Firewall is a micro-firewall and an API-native application acting as an enterprise architectures security gateway, acting as the only exit and entrance for all the API calls. API protection is executed by it, which on the basis of openAPI generates a protection configuration which is the definition of ones API and it once it is deployed, the configuration is ran by API firewall and it provides a virtual host for that particular API. For the protection of APIs used for data transfer and security reasons,

API firewalls are used widely these days. APIs are and integral part of transfer strategies and yet they're are widely ignored by developers and security departments, leading to hackings and API breaches widely. That’s why knowledge of API firewall is necessary in order to which we need to learn what traffic should be allowed and what traffic needs to be blocked to create a secure system.

First of all we will need to download Dockers in order to turn the Firewall on. When turning the firewall on we need to turn the OpenAPI specifications on in order to let the API firewall work. Once the firewall is at work it will determine that if the request and responses received are according to the defined schema, in order to block the traffic that's not defined according to specifications. Steps for completion of project:

* Downloading Dockers
* Running API Firewall
* Specifying Schema
* Request and response testing
* Final report on the allowed and blocked/logged traffic

* **PROBLEM STATEMENT**

Businesses these days use APIs for connection to the services and for data transfer. Which means that API that could be hacked can lead to a breach of data. To stop such API abuse issues we use API-Firewalls for which we need to have proper knowledge of what data was allowed and what traffic was blocked.

* **WORK DIVISION**

**Hassan Chaudhry**

* Developing Project Plan
* Assigning tasks
* Research and implementation
* Documentation
* Specifying schema and testing

**Mir Hassan**

* Determining project milestones
* Extensive research on similar works
* Analysis of traffic
* Specifying schema and testing
* **COSTING:**

No costing is involved as all the required material is already available.

* Applicable Books.
* An individual machine with at least 16 GB RAM.
* 500 GB/1TB Hard Disk Drive.
* Internet access.
* **PROJECT DEVELOPMENT METHODLOGY / ARCHITECTURE**

The areas where the knowledge is required to complete this project are:

* Dockers
* API-FIREWALL

***PROJECT OUTCOMES***

Our objective is to check the blocked traffic of the API firewall and how it was blocked or logged using STDOUT or STDERR logs after we define the schema required in openAPI 3.0 specifications for a positive security system of Wallarm API firewall. We also look into the speed results of the API firewall testings in order to improve the process. The main learning objectives of our project would be:

* Gathering information about API firewall
* Specifying schema of API Firewall
* Firewall work flow and traffic blockage
* Factors to improve firewall security and speeding up process.

This would help us improve our information security skills in order to defend our own or the client’s business system from breaches during data or request transfer between multiple systems.

**REFERENCES**

1. [www.github.com/Sbinsaleem/api-firewall](http://www.github.com/Sbinsaleem/api-firewall)
2. <https://hub.docker.com/_/api-firewall>
3. https://docs.42crunch.com/latest/content/concepts/api\_firewall.htm#:~:text=API%20Firewall%20is%20an%20API,exit%20for%20all%20API%20calls.