Proxy Firewall Development with Dashboard

**Architecture and Design:**

**A diagram of a security system

Description automatically generated**

**setup and configuration:**

1.open project as gradle project.

2. set projcet sdk2 java1.8.

3. Execute gradle clean

4. execute gradle build.

5. Now the jar file will be generated in the build directory of the firewall project(PROJECT\_DIRECTORY\_PATH/build/libs/\*.jar)

6. sudo java -jar PATH\_TO\_JAR\_FILE

7. The jar file needs to be executed only on unix/linux.

8. For installation of ip tables execute the below commands:

sudo apt update

sudo apt install iptables

NOTE: iptable data will be cleared once after booting of the system

**API DOCUMENTATION:**

1. **API Related to IP Blocking:** curl -X POST -H "Content-Type: application/json" -d "{'ipAddress'='10.20.123.43', 'hostType'='SOURCE'}" <http://127.0.0.1:7075/firewall/block-ip/>

This header specifies that the data being sent in the request body is in JSON format. The data is sent in JSON format and includes information about the IP address to be blocked and its host type.

‘curl’ command is making a POST request to <http://127.0.0.1:7075/firewall/block-ip/> with a JSON payload specifying an IP address and host type to block. The server at that endpoint is expected to process the request and take action, such as blocking the specified IP address in a firewall.

1. **API Related to Port Blocking:** curl -X POST -H "Content-Type: application/json" -d "{'portnumber'=' ', 'hostType'='SOURCE'}" <http://127.0.0.1:7075/firewall/block-port/>

Headers: `Content-Type: application/json` - This header specifies that the data being sent in the request body is in JSON format.

Request Body (Data): The data is sent in JSON format and includes information about the port number to be blocked and its host type:

```json {'portnumber'=' ', 'hostType'='SOURCE'}

API Endpoint URL: `http://127.0.0.1:7075/firewall/block-port/` - This is the URL of the API endpoint. It suggests that the API is related to firewall management and specifically involves blocking a port.

POST request to a local server at "http://127.0.0.1:7075/firewall/block-por", providing JSON data in the request body with information about port blocking, specifically setting the 'portnumber' to an empty string and 'hostType' to 'SOURCE'. The purpose and outcome of this request depend on the specific functionality of the server and API being accessed.

1. curl -X POST -H "Content-Type: application/json" -d "{'protocol’=’getProtocol()’}" <http://127.0.0.1:7075/firewall/block-protocol/>

**HTTP Method:** `POST` - Indicates that the request is creating a new resource on the server.

**Headers:** `Content-Type: application/json` - Specifies that the data being sent in the request body is in JSON format.

**Request Body (Data):** The data is sent in JSON format and includes information about the protocol to be blocked: ```json

{'protocol'='getProtocol()'}

```

Note: `getProtocol()` seems to be a placeholder or a function call that might be dynamically obtaining the protocol.

**API Endpoint URL:** `http://127.0.0.1:7075/firewall/block-protocol/` - This is the URL of the API endpoint. It indicates that the API is related to blocking a specific protocol.

JSON data in the request body. The JSON data includes a key "protocol" with the value "getProtocol()". The purpose and functionality of this command depend on the specific API or service that is listening at the provided URL. It suggests that the request is related to a firewall and involves blocking a protocol, but the exact details would depend on the implementation of the API or service at the specified endpoint.

1. **API Related to firewall Management:** curl -X POST -H "Content-Type: application/json" -d "{'SourceIP’=' ', 'request'='SOURCE',’ruleName’=’ ‘}" <http://127.0.0.1:7075/firewall/limit-requests/>

**HTTP Method**: `POST` - Indicates that the request is creating a new resource on the server.

Headers: `Content-Type: application/json` - Specifies that the data being sent in the request body is in JSON format.

**Request Body (Data):** The data is sent in JSON format and includes information about the source IP, request type, and rule name: ```json

{'SourceIP’=' ', 'request'='SOURCE', ’ruleName’=’ ‘}

**API Endpoint URL:** `http://127.0.0.1:7075/firewall/limit-requests/` - This is the URL of the API endpoint. It suggests that the API is related to firewall management and involves limiting requests based on specified criteria.

|  |
| --- |
|  |
|  |

l