

Firewall Setup Project Documentation

1. Purpose and Types of Firewalls

A firewall acts as a barrier to control network traffic, ensuring only authorized communications occur between trusted internal networks and untrusted external networks.

Types of Firewalls:

- Network-Based Firewalls: Protect entire networks by monitoring and filtering traffic at the network level.
- Host-Based Firewalls: Secure individual devices by controlling incoming and outgoing traffic specific to that device.

2. Getting Started

Prerequisites:

1. Environment:

- A virtual machine (e.g., VirtualBox, VMware) or physical machine with Parrot OS installed.

2. User Permissions:

- Administrative/root access to configure firewall rules.

3. Networking Knowledge:

- Familiarity with basic networking concepts, including IP addresses and ports.

3. Setup Instructions

Step 1: Clone the Repository:

Run the following commands to clone the repository containing resources for this project:

Firewall Setup Project Documentation

...

```
git clone https://github.com/iliamax/firewall-setup.git
```

```
cd firewall-setup
```

...

Step 2: Install Required Tools:

Install `ufw` (Uncomplicated Firewall) for managing firewall rules:

...

```
sudo apt update
```

```
sudo apt install ufw -y
```

...

4. Configuring Firewall Rules

Step 1: Enable the Firewall:

Activate the firewall to start managing traffic:

...

```
sudo ufw enable
```

...

Step 2: Allow Specific Traffic:

To allow traffic to a service or port, use:

...

```
sudo ufw allow <service/port>
```

...

Firewall Setup Project Documentation

Examples:

- Allow SSH traffic:

...

```
sudo ufw allow ssh
```

...

- Allow HTTP traffic:

...

```
sudo ufw allow 80
```

...

Step 3: Deny Specific Traffic:

To block unwanted traffic:

...

```
sudo ufw deny <service/port>
```

...

Example:

- Block a specific IP address:

...

```
sudo ufw deny from <IP>
```

...

Step 4: Limit Traffic:

To prevent abuse, use the `limit` rule:

...

```
sudo ufw limit <service/port>
```

Firewall Setup Project Documentation

...

Example:

- Limit SSH login attempts:

...

```
sudo ufw limit ssh
```

...

Step 5: View and Manage Rules:

- List all active rules:

...

```
sudo ufw status numbered
```

...

- Remove a rule by its number:

...

```
sudo ufw delete <rule_number>
```

...

5. Contributing

How to Contribute:

1. Fork the repository.
2. Create a branch for your feature or fix:

...

```
git checkout -b feature-name
```

...

Firewall Setup Project Documentation

3. Commit your changes:

...

```
git commit -m 'Add feature-name'
```

...

4. Push to your fork:

...

```
git push origin feature-name
```

...

5. Create a pull request.

6. License

This project is licensed under the MIT License. Refer to the LICENSE file for details.