A screenshot of a computer

Description automatically generated

Status Dashboard.

A screenshot of a computer

Description automatically generated

Latest version updated.

A screenshot of a computer

Description automatically generated

HTTPS Port.

A screenshot of a computer

Description automatically generated

The dashboard traffic graph.

A screenshot of a computer

Description automatically generated

I disabled inbound ICMP.

A screenshot of a computer

Description automatically generated

The IP addresses for Netflix.com.

A screenshot of a computer

Description automatically generated

Created aliases for Netflix domains.

A screenshot of a computer

Description automatically generated

I enabled every domain for Netflix, a video streaming platform.

A screenshot of a computer

Description automatically generated

I was able to login to the Netflix website, indicating my rules are working.

A screenshot of a computer

Description automatically generated

The IP address for Twitter.com, a social media website.

A screenshot of a computer

Description automatically generated

I was able to login to twitter

A screenshot of a computer

Description automatically generated

I set a rule to disable twitter.

A screenshot of a computer

Description automatically generated

I was unable to connect to twitter after I disabled it. Rules working.

A screenshot of a computer

Description automatically generated

I disabled all the port for ‘World of Warcraft’ game.

A screenshot of a computer

Description automatically generated

All the aliases I set for the IP addresses I worked with.

A screenshot of a computer

Description automatically generated

The aliases I set for the ports I worked with.

Five open ports, their protocols and their applications.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | 80 (HTTP) | 443(HTTPS) | 22 (SSH) | 25 (SMTP) | 53 (DNS) |
| Protocol | TCP/UDP | TCP/UDP | TCP/UDP | TCP | TCP/UDP |
| Application | Web traffic | Secured web traffic | Secured remote login | Sending emails between servers | Translating domain names into IP addresses and vice versa. |

Five closed ports, their protocols and their applications.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | 23 (Telnet) | 21 (FTP) | 69 (TFTP) | 1433 (MS-SQL-S) | 445 (SMB) |
| Protocol | TCP | TCP/UDP | UDP | TCP | TCP/UDP |
| Application | Unencrypted text communications. | Transfer of files. | Simple file transfers. | Database management. | File sharing and network browsing. |

My lab is in the form of a home office architecture and the vulnerabilities that might occur are:

* The default password. Any interception of traffic will leave my network under threat. The other default settings on the firewall are vulnerable too.
* A wrong IP address configuration or improperly set permissions.
* Not using the latest version of the firewall. It is necessary to regularly update.

I learnt that I could allow or deny traffic using ports, what I need to allow or deny and proper network management.