

**SECURE WIRELESS AND MOBILE NETWORKS**

**CURRICULUM: RESILIENT AND SECURE CYBER PHYSICAL SYSTEMS**

**Submitted to Professor Tomasso Pecorella**

**Assignment 3 – Firewall Configuration**

**Cheriya Puthan Veettil Muhammed Irfan**

**Matricular – 7127908**

**Abstract**

This report documents the setup, testing, and analysis of the network with and without firewall rules. Primary aim was to verify the communication between hosts and a cloud network. And evaluate the effectiveness of configured firewall in restricting traffic.

**Introduction**

This experiment aims to access the communications between two host and a cloud network under different firewall rules and without any firewall rules. The firewall rule added to restrict specific traffic. Wireshark was used to packet capture and analysis.

**Setup**

A diagram of a firewall

Description automatically generated

* LAN11

IP- 192.168.11.1

* LAN12

IP- 192.168.12.1

* WAN 1

IP- 111.111.111.116

Tools and Software

* Virtual Box
* OPNsense (user: root, password: rootadmin)
* Wireshark

Network Types

* Host-only network – LAN11
* Host-only network#2 – LAN12
* Nat Network

**Verification Plan**

With out Firewall Rules:

1. Ping Test: Confirms Successful communication.

With Firewall Rules:

1. Ping Test: Expect Ping failure and Successful communication.
2. TCP/UDP Test: Confirms blocked/allowed connection.
3. Firewall Rules Verification: Analyse packet for blocked/ allowed traffic.

**Proof of Operation**

A computer screen with white text

Description automatically generatedPing Test (without Rules): LAN11

A computer screen shot of a black screen

Description automatically generatedPing Test (with Rules): LAN11

A computer screen with white text

Description automatically generatedPing Test (without Rules): LAN12

A computer screen with white text

Description automatically generated

Ping Test (with Rules): LAN12

A computer screen with white text

Description automatically generatedPing Test (google)

Wireshark Capture:

A table with numbers and letters

Description automatically generated1.LAN11

A table with numbers and symbols

Description automatically generated2.LAN12

3.WAN1

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generatedFirewall Rules

LAN11

A screenshot of a computer

Description automatically generatedLAN12

A screenshot of a computer

Description automatically generatedFloating

**Discussion**

1. Effectiveness of firewall configuration
   1. Checked configured rules successfully restricted/allowed specific types of traffic.
   2. Firewall blocked traffic that set-in firewall rule for LAN’s.
2. Traffic types used to restrict/allowed for communicated.
   1. ICMP
   2. TCP
   3. UDP
3. Created Alias for Wikipedia under Firewall Alias and then created firewall block rules using the alias. After that it is possible to load all other website’s apart from the Wikipedia.

Findings

\*If firewall is down or not functioning properly, there is no barrier/filter for incoming and outgoing traffic. It makes unauthorized access to network.

\*Sometimes it makes false positives.

**Conclusion**

From this assignment served exploration of network security through the implementation and testing of firewall configuration. At first confirmed the seamless communication between Host’s and cloud in the absence of firewall rules. Introduction of firewall rules makes controlling the traffic over network. Testing the effectiveness of firewall configuration highlights the importance of rule creation, that makes balance between securing the network and allowing only essential communication.

This assignment provides valuable information of relationship between firewall and network.