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

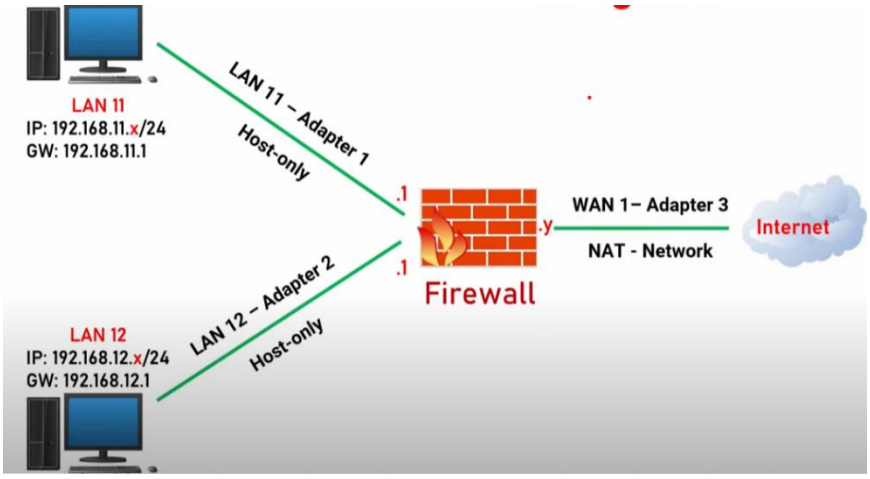
This report documents the setup, testing, and analysis of the network with and without firewall rules. Primary aim was to verify the communication between hosts and a cloud network. And evaluate the effectiveness of configured firewall in restricting traffic.

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

- 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:

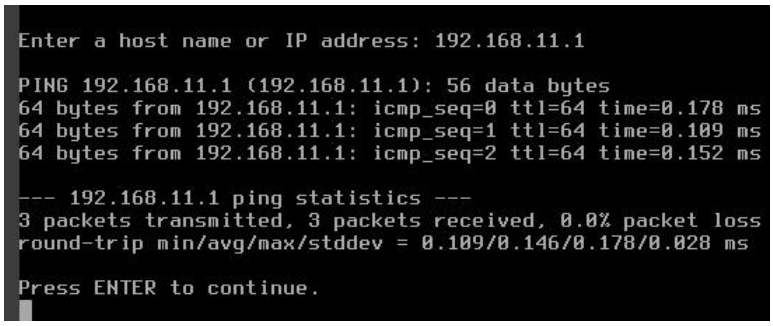
1. Ping Test: Confirms Successful communication.

With Firewall Rules:

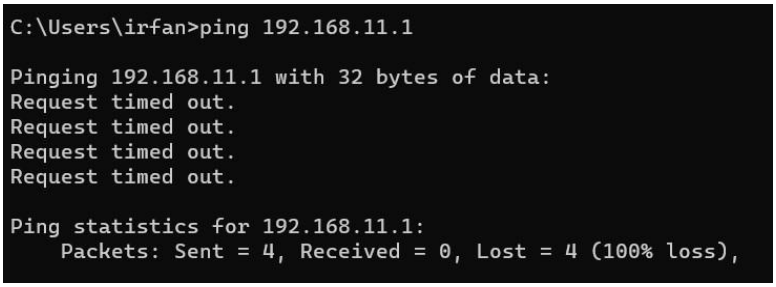
1. Ping Test: Expect Ping failure and Successful communication.
2. TCP/UDP Test: Confirms blocked/allowed connection.
3. Firewall Rules Verification: Analyse packet for blocked/ allowed traffic.

Proof of Operation

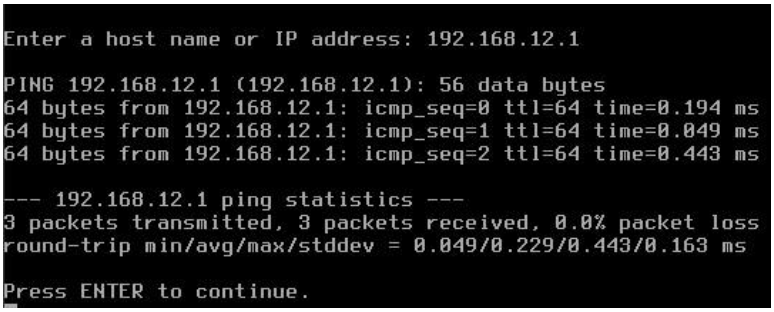
Ping Test (without Rules): LAN11



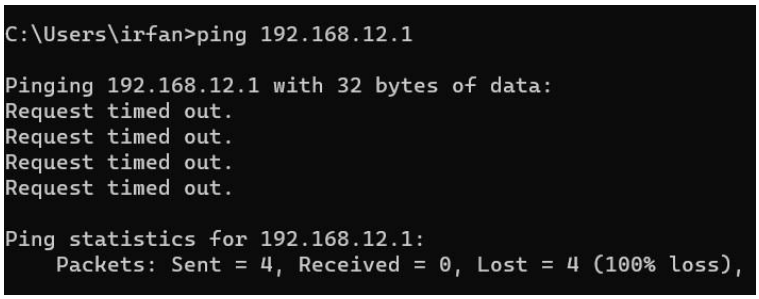
Ping Test (with Rules): LAN11



Ping Test (without Rules): LAN12



Ping Test (with Rules): LAN12



Ping Test (google)

```
Enter a host name or IP address: google.com

PING google.com (216.58.215.238): 56 data bytes
64 bytes from 216.58.215.238: icmp_seq=0 ttl=114 time=20.491 ms
64 bytes from 216.58.215.238: icmp_seq=1 ttl=114 time=21.880 ms
64 bytes from 216.58.215.238: icmp_seq=2 ttl=114 time=20.492 ms

--- google.com ping statistics ---
3 packets transmitted, 3 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 20.491/20.955/21.880/0.654 ms

Press ENTER to continue.
```

Wireshark Capture:

1.LAN11

1901	1773.485012	192.168.11.1	192.168.11.100	TCP	1514	80 → 50684 [ACK] Seq=198798 Ack=2378 Win=65792 Len=1460 [TCP segment of a reassembled PDU]
1902	1773.485167	192.168.11.1	192.168.11.100	TCP	1514	80 → 50684 [ACK] Seq=200258 Ack=2378 Win=65792 Len=1460 [TCP segment of a reassembled PDU]
1903	1773.485257	192.168.11.100	192.168.11.1	TCP	54	50684 → 80 [ACK] Seq=2378 Ack=201718 Win=262656 Len=0
1904	1773.485305	192.168.11.1	192.168.11.100	TCP	1514	80 → 50684 [ACK] Seq=201718 Ack=2378 Win=65792 Len=1460 [TCP segment of a reassembled PDU]
1905	1773.485325	192.168.11.1	192.168.11.100	TCP	1514	80 → 50684 [ACK] Seq=203178 Ack=2378 Win=65792 Len=1460 [TCP segment of a reassembled PDU]
1906	1773.485340	192.168.11.100	192.168.11.1	TCP	54	50684 → 80 [ACK] Seq=2378 Ack=204638 Win=262656 Len=0
1907	1773.485360	192.168.11.1	192.168.11.100	TCP	1514	80 → 50684 [ACK] Seq=204638 Ack=2378 Win=65792 Len=1460 [TCP segment of a reassembled PDU]
1908	1773.485383	192.168.11.1	192.168.11.100	TCP	1514	80 → 50684 [ACK] Seq=206098 Ack=2378 Win=65792 Len=1460 [TCP segment of a reassembled PDU]
1909	1773.485393	192.168.11.100	192.168.11.1	TCP	54	50684 → 80 [ACK] Seq=2378 Ack=207558 Win=262656 Len=0
1910	1773.485409	192.168.11.1	192.168.11.100	TCP	1514	80 → 50684 [ACK] Seq=207558 Ack=2378 Win=65792 Len=1460 [TCP segment of a reassembled PDU]
1911	1773.485436	192.168.11.1	192.168.11.100	TCP	1514	80 → 50684 [ACK] Seq=209018 Ack=2378 Win=65792 Len=1460 [TCP segment of a reassembled PDU]
1912	1773.485447	192.168.11.100	192.168.11.1	TCP	54	50684 → 80 [ACK] Seq=2378 Ack=210478 Win=262656 Len=0
1913	1773.485515	192.168.11.1	192.168.11.100	HTTP/J…	595	HTTP/1.1 200 OK , JavaScript Object Notation (application/json)
1914	1773.520027	192.168.11.100	192.168.11.1	TCP	54	50683 → 80 [ACK] Seq=2419 Ack=210966 Win=261376 Len=0
1915	1773.525872	192.168.11.100	192.168.11.1	TCP	54	50684 → 80 [ACK] Seq=2378 Ack=211019 Win=262144 Len=0
1916	1773.951089	192.168.11.100	192.168.11.1	HTTP	579	GET /api/core/system/status HTTP/1.1
1917	1773.951463	192.168.11.1	192.168.11.100	TCP	54	80 → 50684 [ACK] Seq=211019 Ack=2903 Win=65280 Len=0
1918	1773.984601	192.168.11.1	192.168.11.100	HTTP	712	HTTP/1.1 200 OK (text/html)
1919	1774.025118	192.168.11.100	192.168.11.1	TCP	54	50684 → 80 [ACK] Seq=2903 Ack=211677 Win=261376 Len=0
1920	1778.452200	192.168.11.100	192.168.11.1	ICMP	74	Echo (ping) request id=0x0001, seq=1155/33540, ttl=128 (reply in 1921)
1921	1778.452551	192.168.11.1	192.168.11.100	ICMP	74	Echo (ping) reply id=0x0001, seq=1155/33540, ttl=64 (request in 1920)
1922	1779.454564	192.168.11.100	192.168.11.1	ICMP	74	Echo (ping) request id=0x0001, seq=1156/33796, ttl=128 (reply in 1923)
1923	1779.455301	192.168.11.1	192.168.11.100	ICMP	74	Echo (ping) reply id=0x0001, seq=1156/33796, ttl=64 (request in 1922)
1924	1780.461523	192.168.11.100	192.168.11.1	ICMP	74	Echo (ping) request id=0x0001, seq=1157/34052, ttl=128 (reply in 1925)
1925	1780.462098	192.168.11.1	192.168.11.100	ICMP	74	Echo (ping) reply id=0x0001, seq=1157/34052, ttl=64 (request in 1924)
1926	1781.468894	192.168.11.100	192.168.11.1	ICMP	74	Echo (ping) request id=0x0001, seq=1158/34308, ttl=128 (reply in 1927)
1927	1781.469636	192.168.11.1	192.168.11.100	ICMP	74	Echo (ping) reply id=0x0001, seq=1158/34308, ttl=64 (request in 1926)
1928	1788.262632	192.168.11.100	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
1929	1789.263438	192.168.11.100	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
1930	1790.263673	192.168.11.100	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
1931	1791.264137	192.168.11.100	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
1932	1804.344891	192.168.11.1	192.168.11.100	TCP	54	80 → 50684 [FIN, ACK] Seq=211677 Ack=2903 Win=65792 Len=0
1933	1804.344988	192.168.11.100	192.168.11.1	TCP	54	50684 → 80 [ACK] Seq=2903 Ack=211678 Win=261376 Len=0
1934	1804.345073	192.168.11.1	192.168.11.100	TCP	54	80 → 50683 [FIN, ACK] Seq=210966 Ack=2419 Win=65792 Len=0
1935	1804.345126	192.168.11.100	192.168.11.1	TCP	54	50683 → 80 [ACK] Seq=2419 Ack=210967 Win=261376 Len=0

2.LAN12

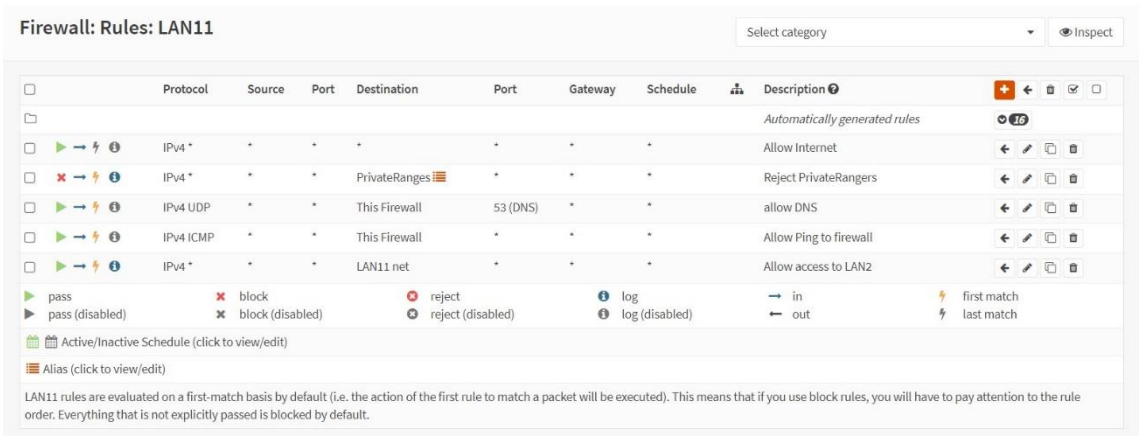
40	133.140212	192.168.12.1	192.168.12.100	ICMP	74	Echo (ping) reply id=0x0001, seq=1172/37892, ttl=64 (request in 39)
41	134.149129	192.168.12.100	192.168.12.1	ICMP	74	Echo (ping) request id=0x0001, seq=1173/38148, ttl=128 (reply in 42)
42	134.149881	192.168.12.1	192.168.12.100	ICMP	74	Echo (ping) reply id=0x0001, seq=1173/38148, ttl=64 (request in 41)
43	135.157796	192.168.12.100	192.168.12.1	ICMP	74	Echo (ping) request id=0x0001, seq=1174/38404, ttl=128 (reply in 44)
44	135.158522	192.168.12.1	192.168.12.100	ICMP	74	Echo (ping) reply id=0x0001, seq=1174/38404, ttl=64 (request in 43)
45	161.535248	192.168.12.100	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
46	162.536374	192.168.12.100	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
47	163.536870	192.168.12.100	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
48	164.537688	192.168.12.100	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
49	281.539722	192.168.12.100	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
50	282.540821	192.168.12.100	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
51	283.540811	192.168.12.100	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
52	284.541097	192.168.12.100	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
53	341.994054	192.168.12.100	192.168.12.1	ICMP	74	Echo (ping) request id=0x0001, seq=1179/39684, ttl=128 (reply in 54)
54	341.994559	192.168.12.1	192.168.12.100	ICMP	74	Echo (ping) reply id=0x0001, seq=1179/39684, ttl=64 (request in 53)
55	342.996644	192.168.12.100	192.168.12.1	ICMP	74	Echo (ping) request id=0x0001, seq=1180/39940, ttl=128 (reply in 56)
56	342.997371	192.168.12.1	192.168.12.100	ICMP	74	Echo (ping) reply id=0x0001, seq=1180/39940, ttl=64 (request in 55)
57	344.006559	192.168.12.100	192.168.12.1	ICMP	74	Echo (ping) request id=0x0001, seq=1181/40196, ttl=128 (reply in 58)
58	344.006877	192.168.12.1	192.168.12.100	ICMP	74	Echo (ping) reply id=0x0001, seq=1181/40196, ttl=64 (request in 57)
59	345.010244	192.168.12.100	192.168.12.1	ICMP	74	Echo (ping) request id=0x0001, seq=1182/40452, ttl=128 (reply in 60)
60	345.010992	192.168.12.1	192.168.12.100	ICMP	74	Echo (ping) reply id=0x0001, seq=1182/40452, ttl=64 (request in 59)
61	346.863223	0a:00:27:00:00:1d	PcsCompu_8c:4c:59	ARP	42	Who has 192.168.12.1? Tell 192.168.12.100
62	346.864001	PcsCompu_8c:4c:59	0a:00:27:00:00:1d	ARP	42	192.168.12.1 is at 08:00:27:8c:4c:59
63	363.968901	192.168.12.100	192.168.12.1	ICMP	74	Echo (ping) request id=0x0001, seq=1183/40708, ttl=128 (reply in 64)
64	363.969199	192.168.12.1	192.168.12.100	ICMP	74	Echo (ping) reply id=0x0001, seq=1183/40708, ttl=64 (request in 63)
65	364.971502	192.168.12.100	192.168.12.1	ICMP	74	Echo (ping) request id=0x0001, seq=1184/40964, ttl=128 (reply in 66)
66	364.972214	192.168.12.1	192.168.12.100	ICMP	74	Echo (ping) reply id=0x0001, seq=1184/40964, ttl=64 (request in 65)
67	365.980225	192.168.12.100	192.168.12.1	ICMP	74	Echo (ping) request id=0x0001, seq=1185/41220, ttl=128 (reply in 68)
68	365.980967	192.168.12.1	192.168.12.100	ICMP	74	Echo (ping) reply id=0x0001, seq=1185/41220, ttl=64 (request in 67)
69	366.987738	192.168.12.100	192.168.12.1	ICMP	74	Echo (ping) request id=0x0001, seq=1186/41476, ttl=128 (reply in 70)
70	366.988456	192.168.12.1	192.168.12.100	ICMP	74	Echo (ping) reply id=0x0001, seq=1186/41476, ttl=64 (request in 69)
71	401.541731	192.168.12.100	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
72	402.543406	192.168.12.100	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
73	403.544524	192.168.12.100	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
74	404.544602	192.168.12.100	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1

3.WAN1

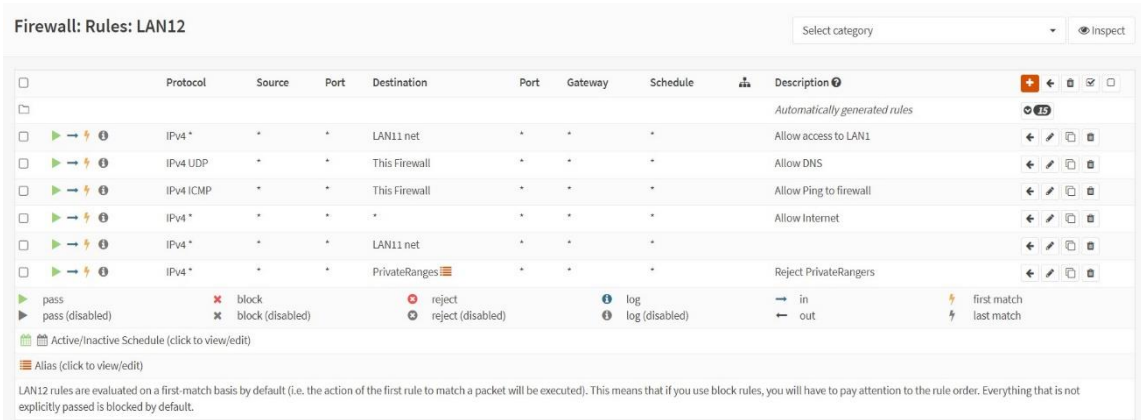
10.0.1.29	4.2.2.2	DNS	95	Standard query 0x7c96 AAAA 3.opnsense.pool.ntp.org.localdomain
4.2.2.2	10.0.1.29	DNS	95	Standard query response 0x7c96 AAAA 3.opnsense.pool.ntp.org.localdomain
10.0.1.29	8.8.8.8	DNS	95	Standard query 0x7c96 AAAA 3.opnsense.pool.ntp.org.localdomain
8.8.8.8	10.0.1.29	DNS	95	Standard query response 0x7c96 AAAA 3.opnsense.pool.ntp.org.localdomain
10.0.1.29	4.2.2.2	DNS	95	Standard query 0x7c96 AAAA 3.opnsense.pool.ntp.org.localdomain
4.2.2.2	10.0.1.29	DNS	95	Standard query response 0x7c96 AAAA 3.opnsense.pool.ntp.org.localdomain
10.0.1.29	8.8.8.8	ICMP	74	Echo (ping) request id=0x0001, seq=1211/47876, ttl=128 (reply in 103)
8.8.8.8	10.0.1.29	ICMP	74	Echo (ping) reply id=0x0001, seq=1211/47876, ttl=116 (request in 102)
51.13.112.137	10.0.1.29	TCP	54	443 → 50888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
10.0.1.29	8.8.8.8	ICMP	74	Echo (ping) request id=0x0001, seq=1212/48132, ttl=128 (reply in 106)
8.8.8.8	10.0.1.29	ICMP	74	Echo (ping) reply id=0x0001, seq=1212/48132, ttl=116 (request in 105)
10.0.1.29	8.8.8.8	ICMP	74	Echo (ping) request id=0x0001, seq=1213/48388, ttl=128 (reply in 108)
8.8.8.8	10.0.1.29	ICMP	74	Echo (ping) reply id=0x0001, seq=1213/48388, ttl=116 (request in 107)
10.0.1.29	8.8.8.8	DNS	83	Standard query 0xe567 A 0.opnsense.pool.ntp.org
8.8.8.8	10.0.1.29	DNS	147	Standard query response 0xe567 A 0.opnsense.pool.ntp.org A 162.159.200.123
10.0.1.29	8.8.8.8	ICMP	74	Echo (ping) request id=0x0001, seq=1214/48644, ttl=128 (reply in 112)
8.8.8.8	10.0.1.29	ICMP	74	Echo (ping) reply id=0x0001, seq=1214/48644, ttl=116 (request in 111)
10.0.1.29	4.2.2.2	DNS	83	Standard query 0xe567 A 0.opnsense.pool.ntp.org
4.2.2.2	10.0.1.29	DNS	147	Standard query response 0xe567 A 0.opnsense.pool.ntp.org A 90.187.112.137 A
52.113.194.132	10.0.1.29	TCP	54	443 → 50895 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
10.0.1.29	8.8.8.8	DNS	83	Standard query 0xe567 A 0.opnsense.pool.ntp.org
8.8.8.8	10.0.1.29	DNS	147	Standard query response 0xe567 A 0.opnsense.pool.ntp.org A 162.159.200.123
10.0.1.29	4.2.2.2	DNS	83	Standard query 0xe567 A 0.opnsense.pool.ntp.org
4.2.2.2	10.0.1.29	DNS	147	Standard query response 0xe567 A 0.opnsense.pool.ntp.org A 176.9.42.91 A 16
10.0.1.29	162.159.130.234	TLSv1.2	105	Application Data
162.159.130.234	10.0.1.29	TCP	54	443 → 50624 [ACK] Seq=33 Ack=103 Win=7 Len=0
162.159.130.234	10.0.1.29	TLSv1.2	86	Application Data
10.0.1.29	162.159.130.234	TCP	54	50624 → 443 [ACK] Seq=103 Ack=65 Win=254 Len=0
10.0.1.29	8.8.8.8	DNS	83	Standard query 0xf6e3 AAAA 0.opnsense.pool.ntp.org
8.8.8.8	10.0.1.29	DNS	83	Standard query response 0xf6e3 AAAA 0.opnsense.pool.ntp.org

Firewall Rules

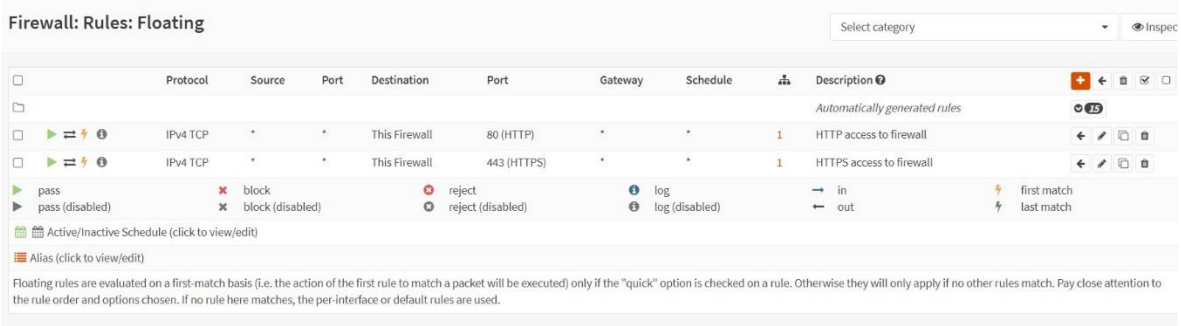
LAN11



LAN12



Floating



Discussion

1. Effectiveness of firewall configuration
    a. Checked configured rules successfully restricted/allowed specific types of traffic.
    b. Firewall blocked traffic that set-in firewall rule for LAN's.
2. Traffic types used to restrict/allowed for communicated.
    a. ICMP
    b. TCP
    c. UDP

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.

*OPNsense is wide topic to explore.

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 provide valuable information of relationship between firewall and network.