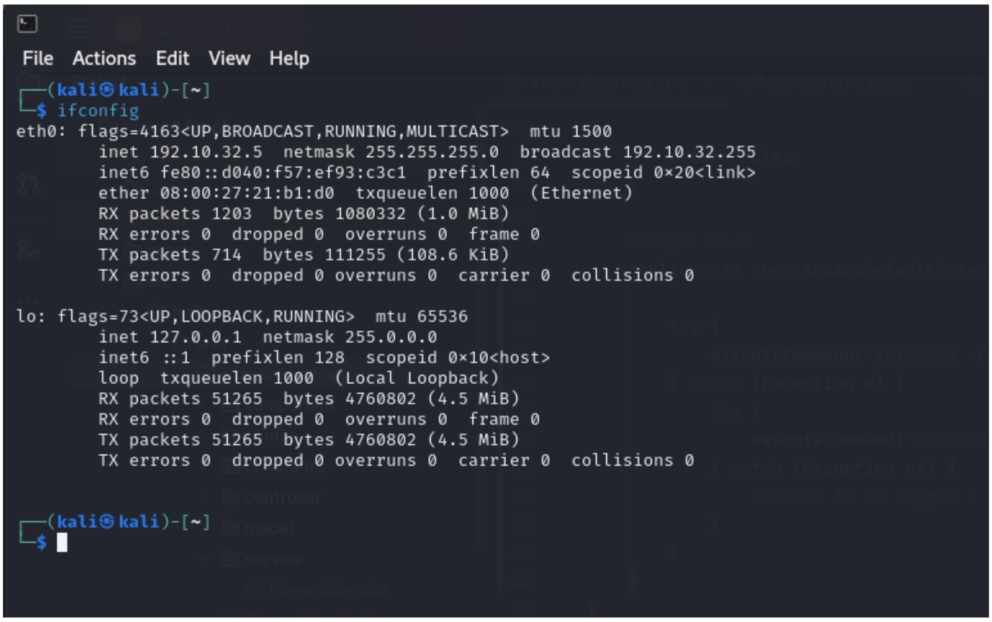
The **testing of the Firewall System** is carried out using the Two systems (Linux Based). Both the VMs are running in common windows system using Oracle Virtual box.

1. Kali Linux (Firewall System)
2. Ubuntu

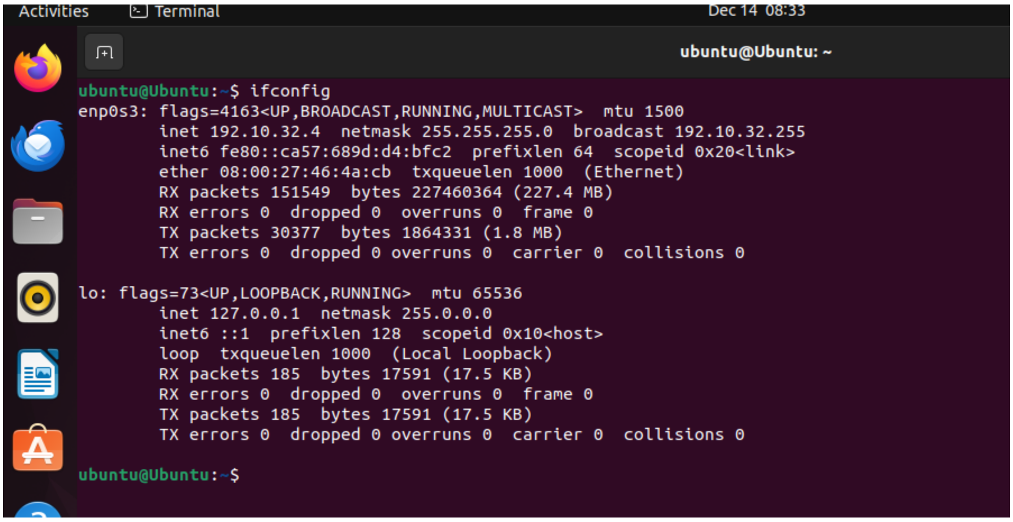
IPs of both Systems:

- Kali Linux – 192.10.32.5



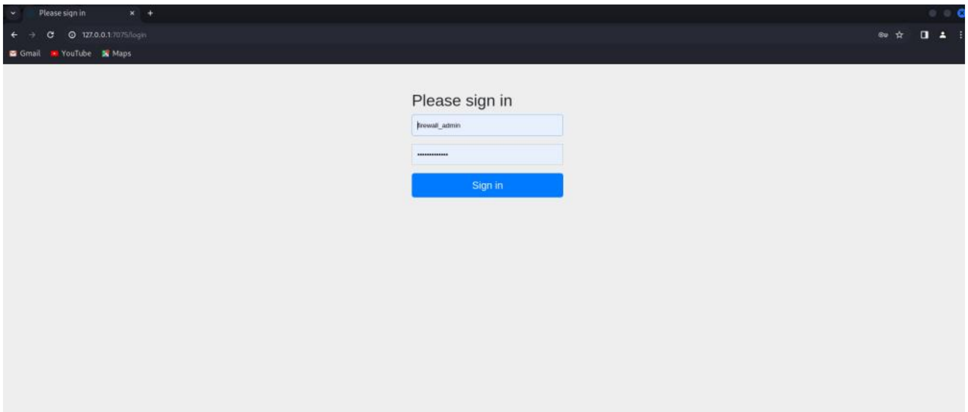
```
┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.10.32.5  netmask 255.255.255.0  broadcast 192.10.32.255
        inet6 fe80::d040:f57:ef93:c3c1  prefixlen 64  scopeid 0×20<link>
        ether 08:00:27:21:b1:d0  txqueuelen 1000  (Ethernet)
        RX packets 1203  bytes 1080332 (1.0 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 714  bytes 111255 (108.6 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0×10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 51265  bytes 4760802 (4.5 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 51265  bytes 4760802 (4.5 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

┌──(kali㉿kali)-[~]
└─$ 
```

- Ubuntu – 192.10.32.4



```
ubuntu@Ubuntu:~$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.10.32.4  netmask 255.255.255.0  broadcast 192.10.32.255
        inet6 fe80::ca57:689d:d4:bfc2  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:46:4a:cb  txqueuelen 1000  (Ethernet)
        RX packets 151549  bytes 227460364 (227.4 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 30377  bytes 1864331 (1.8 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 185  bytes 17591 (17.5 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 185  bytes 17591 (17.5 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

ubuntu@Ubuntu:~$
```

- Sign In Page



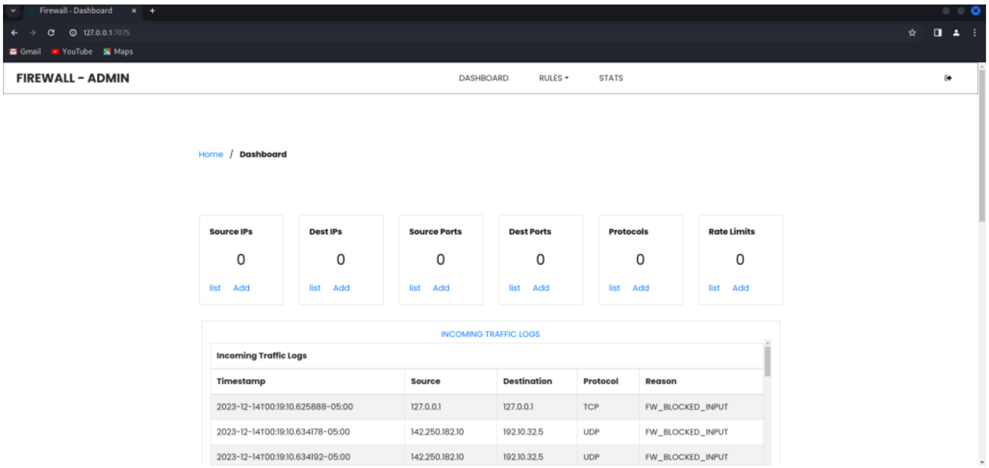
Please sign in

firewall_admin

••••••••••••••

Sign in

- Dashboard with default statistics



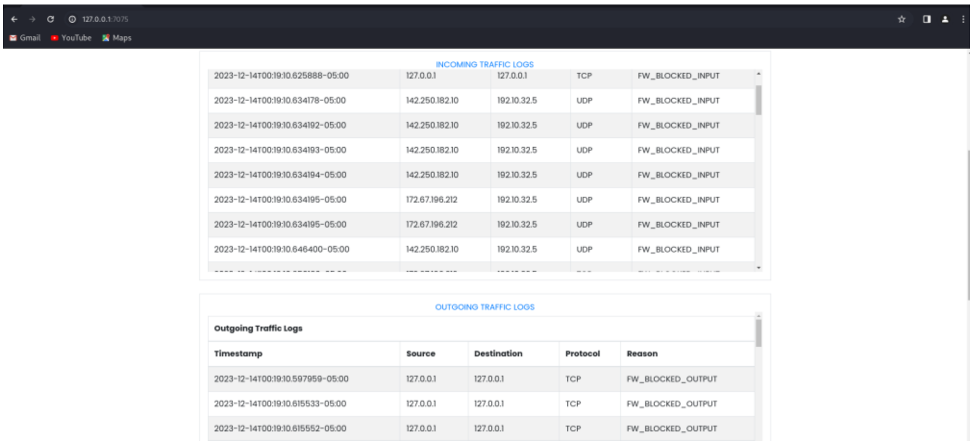
Source IPs	Dest IPs	Source Ports	Dest Ports	Protocols	Rate Limits
0	0	0	0	0	0
list Add	list Add	list Add	list Add	list Add	list Add

INCOMING TRAFFIC LOGS

Incoming Traffic Logs

Timestamp	Source	Destination	Protocol	Reason
2023-12-14T00:19:10.625888-05:00	127.0.0.1	127.0.0.1	TCP	FW_BLOCKED_INPUT
2023-12-14T00:19:10.634178-05:00	142.250.182.10	192.10.32.5	UDP	FW_BLOCKED_INPUT
2023-12-14T00:19:10.634192-05:00	142.250.182.10	192.10.32.5	UDP	FW_BLOCKED_INPUT

- Dashboard with INCOMING & OUTGOING Traffic Logs



INCOMING TRAFFIC LOGS

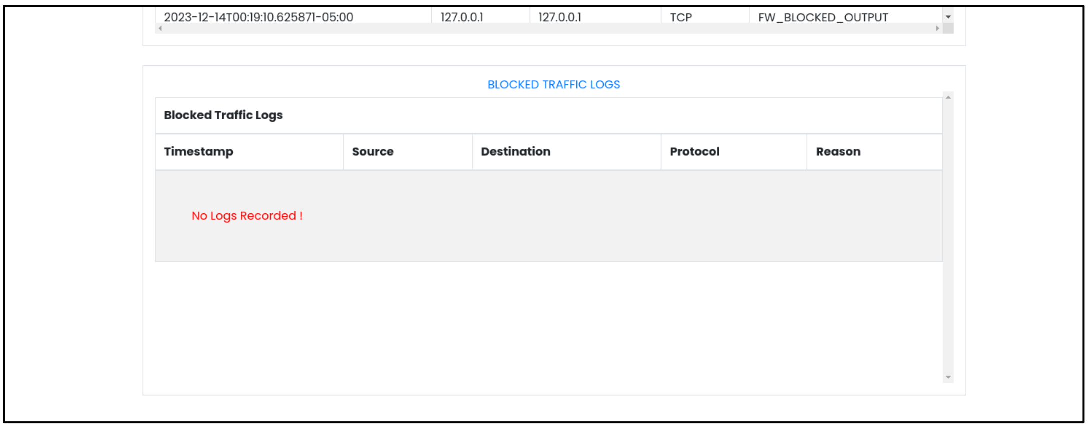
2023-12-14T00:19:10.625888-05:00	127.0.0.1	127.0.0.1	TCP	FW_BLOCKED_INPUT
2023-12-14T00:19:10.634178-05:00	142.250.182.10	192.10.32.5	UDP	FW_BLOCKED_INPUT
2023-12-14T00:19:10.634192-05:00	142.250.182.10	192.10.32.5	UDP	FW_BLOCKED_INPUT
2023-12-14T00:19:10.634193-05:00	142.250.182.10	192.10.32.5	UDP	FW_BLOCKED_INPUT
2023-12-14T00:19:10.634194-05:00	142.250.182.10	192.10.32.5	UDP	FW_BLOCKED_INPUT
2023-12-14T00:19:10.634195-05:00	172.67.196.212	192.10.32.5	UDP	FW_BLOCKED_INPUT
2023-12-14T00:19:10.634195-05:00	172.67.196.212	192.10.32.5	UDP	FW_BLOCKED_INPUT
2023-12-14T00:19:10.646400-05:00	142.250.182.10	192.10.32.5	UDP	FW_BLOCKED_INPUT

OUTGOING TRAFFIC LOGS

Outgoing Traffic Logs

Timestamp	Source	Destination	Protocol	Reason
2023-12-14T00:19:10.597959-05:00	127.0.0.1	127.0.0.1	TCP	FW_BLOCKED_OUTPUT
2023-12-14T00:19:10.615533-05:00	127.0.0.1	127.0.0.1	TCP	FW_BLOCKED_OUTPUT
2023-12-14T00:19:10.615552-05:00	127.0.0.1	127.0.0.1	TCP	FW_BLOCKED_OUTPUT

- Dashboard with Blocked Logs



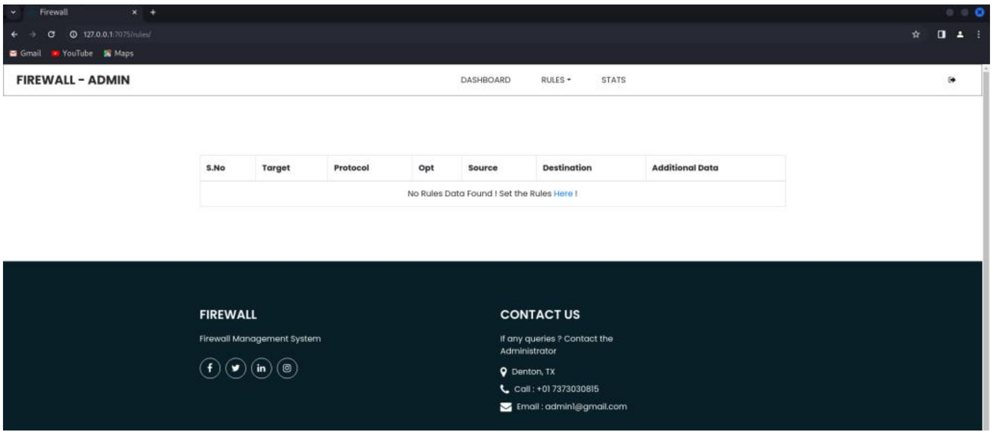
```
2023-12-14T00:19:10.625871-05:00    127.0.0.1    127.0.0.1    TCP    FW_BLOCKED_OUTPUT
```

BLOCKED TRAFFIC LOGS

Blocked Traffic Logs

Timestamp	Source	Destination	Protocol	Reason
No Logs Recorded !				

- List of Rules Available (Initially, the list will be Empty)



S.No	Target	Protocol	Opt	Source	Destination	Additional Data
No Rules Data Found ! Set the Rules Here !						

FIREWALL

Firewall Management System

CONTACT US

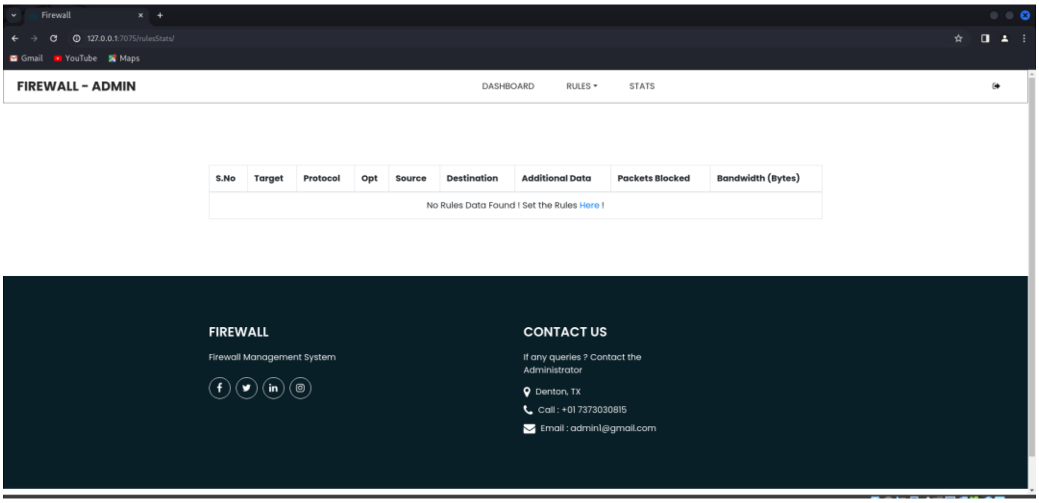
If any queries ? Contact the Administrator

Denton, TX

Call : +01 7373030815

Email : admin1@gmail.com

- List of Rules with the Data – Packets Blocked and Bandwidth (Intially, the List will be Empty)



S.No	Target	Protocol	Opt	Source	Destination	Additional Data	Packets Blocked	Bandwidth (Bytes)
No Rules Data Found ! Set the Rules Here !								

FIREWALL

Firewall Management System

CONTACT US

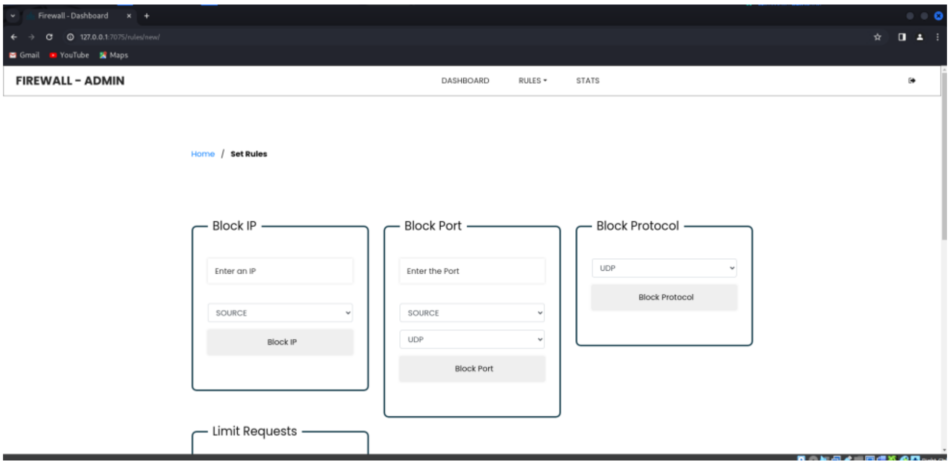
If any queries ? Contact the Administrator

Denton, TX

Call : +01 7373030815

Email : admin1@gmail.com

- Page to set the Rules

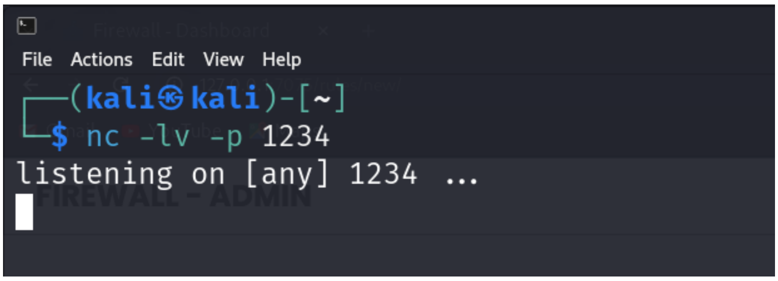


The following Use cases were executed to check the functionality of the Firewall System based on the Rules set.

Use case 1 : Blocking a destination port **TCP 1234**

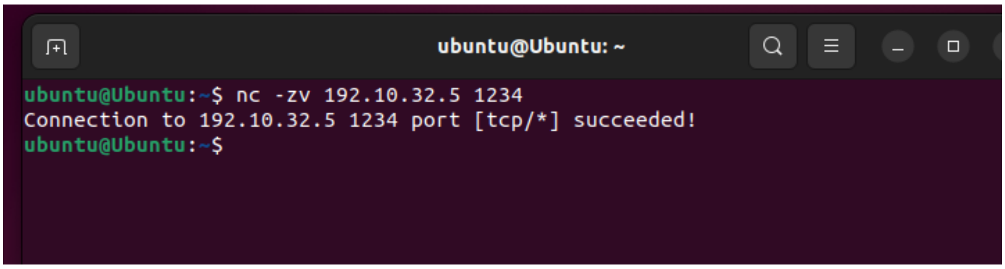
Here, using **nc** command we will try to connect from ubuntu to kali on **TCP** port **1234**.

- Kali is listening on TCP port 1234



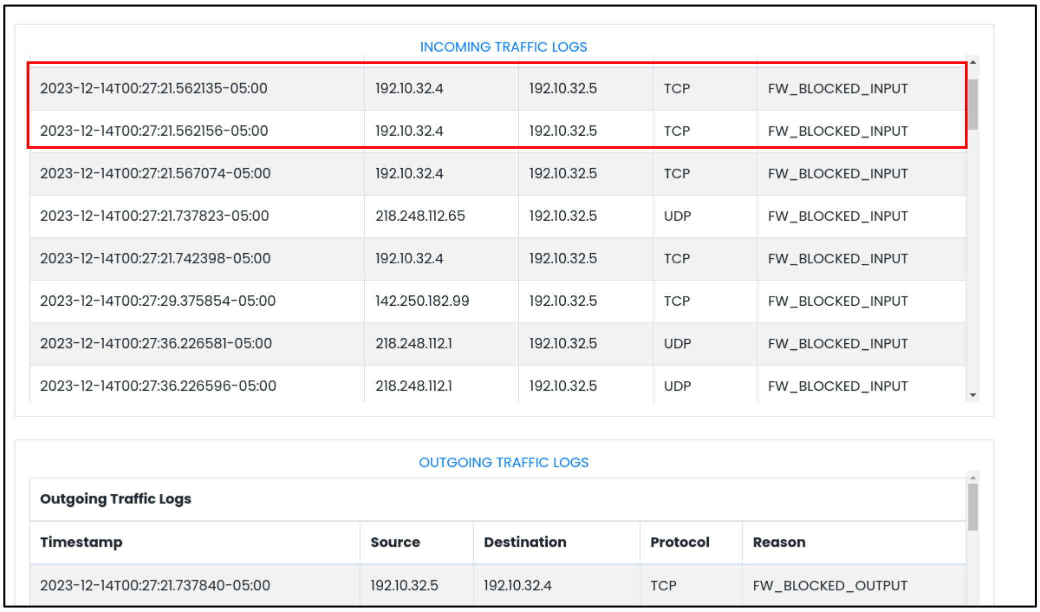
```
┌──(kali㉿kali)-[~]
└─$ nc -lv -p 1234
listening on [any] 1234 ...
```

- From ubuntu, the connection is successful to the Kali on TCP port 1234



```
ubuntu@Ubuntu:~$ nc -zv 192.10.32.5 1234
Connection to 192.10.32.5 1234 port [tcp/*] succeeded!
ubuntu@Ubuntu:~$
```

- The Incoming and Outgoing logs were recorded and Displayed in the Dashboard



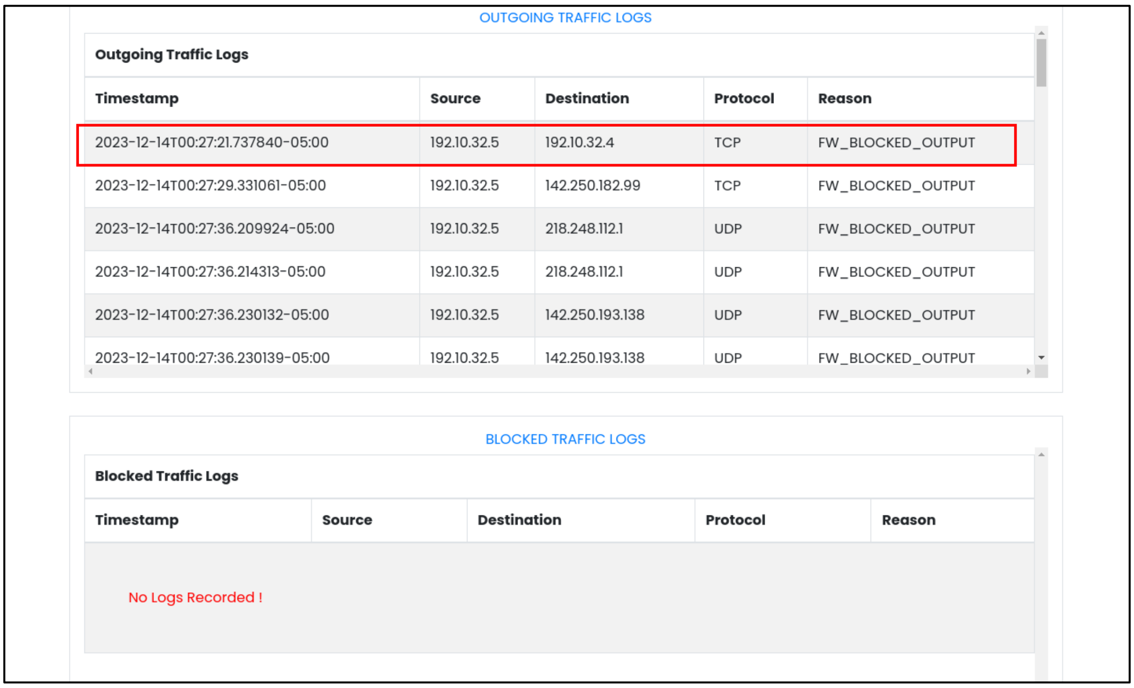
INCOMING TRAFFIC LOGS

2023-12-14T00:27:21.562135-05:00	192.10.32.4	192.10.32.5	TCP	FW_BLOCKED_INPUT
2023-12-14T00:27:21.562156-05:00	192.10.32.4	192.10.32.5	TCP	FW_BLOCKED_INPUT
2023-12-14T00:27:21.567074-05:00	192.10.32.4	192.10.32.5	TCP	FW_BLOCKED_INPUT
2023-12-14T00:27:21.737823-05:00	218.248.112.65	192.10.32.5	UDP	FW_BLOCKED_INPUT
2023-12-14T00:27:21.742398-05:00	192.10.32.4	192.10.32.5	TCP	FW_BLOCKED_INPUT
2023-12-14T00:27:29.375854-05:00	142.250.182.99	192.10.32.5	TCP	FW_BLOCKED_INPUT
2023-12-14T00:27:36.226581-05:00	218.248.112.1	192.10.32.5	UDP	FW_BLOCKED_INPUT
2023-12-14T00:27:36.226596-05:00	218.248.112.1	192.10.32.5	UDP	FW_BLOCKED_INPUT

OUTGOING TRAFFIC LOGS

Outgoing Traffic Logs

Timestamp	Source	Destination	Protocol	Reason
2023-12-14T00:27:21.737840-05:00	192.10.32.5	192.10.32.4	TCP	FW_BLOCKED_OUTPUT



OUTGOING TRAFFIC LOGS

Outgoing Traffic Logs

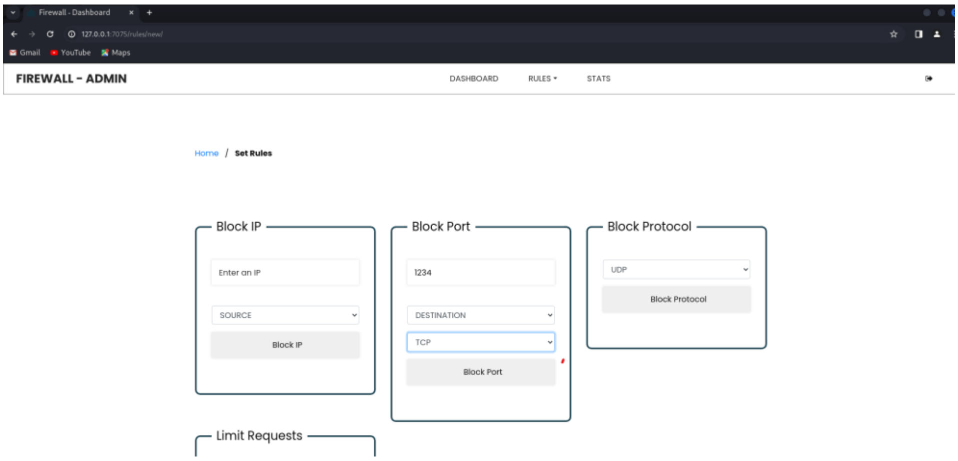
Timestamp	Source	Destination	Protocol	Reason
2023-12-14T00:27:21.737840-05:00	192.10.32.5	192.10.32.4	TCP	FW_BLOCKED_OUTPUT
2023-12-14T00:27:29.331061-05:00	192.10.32.5	142.250.182.99	TCP	FW_BLOCKED_OUTPUT
2023-12-14T00:27:36.209924-05:00	192.10.32.5	218.248.112.1	UDP	FW_BLOCKED_OUTPUT
2023-12-14T00:27:36.214313-05:00	192.10.32.5	218.248.112.1	UDP	FW_BLOCKED_OUTPUT
2023-12-14T00:27:36.230132-05:00	192.10.32.5	142.250.193.138	UDP	FW_BLOCKED_OUTPUT
2023-12-14T00:27:36.230139-05:00	192.10.32.5	142.250.193.138	UDP	FW_BLOCKED_OUTPUT

BLOCKED TRAFFIC LOGS

Blocked Traffic Logs

Timestamp	Source	Destination	Protocol	Reason
No Logs Recorded !				

- Adding a rule to block Destination port TCP 1234



Block IP

Enter an IP

SOURCE

Block IP

Block Port

1234

DESTINATION

TCP

Block Port

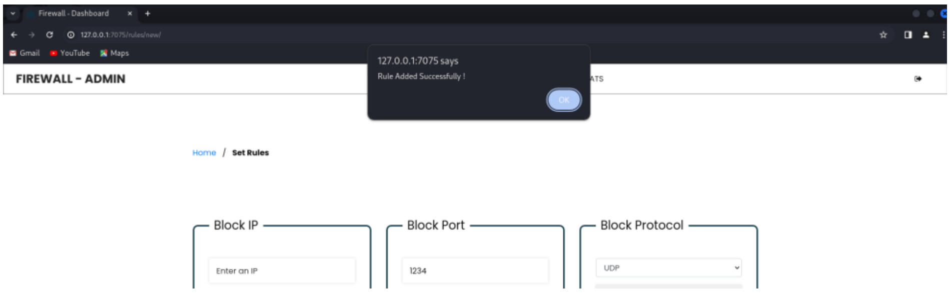
Block Protocol

UDP

Block Protocol

Limit Requests

- After successful login, An alert message will be displayed.



127.0.0.1:7075 says

Rule Added Successfully !

Block IP

Enter an IP

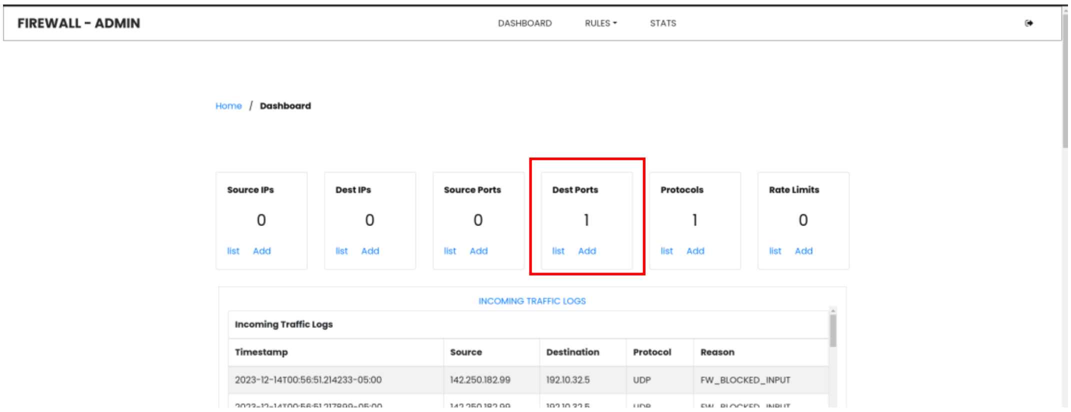
Block Port

1234

Block Protocol

UDP

- Blocked destination ports count will be reflected in Dashboard



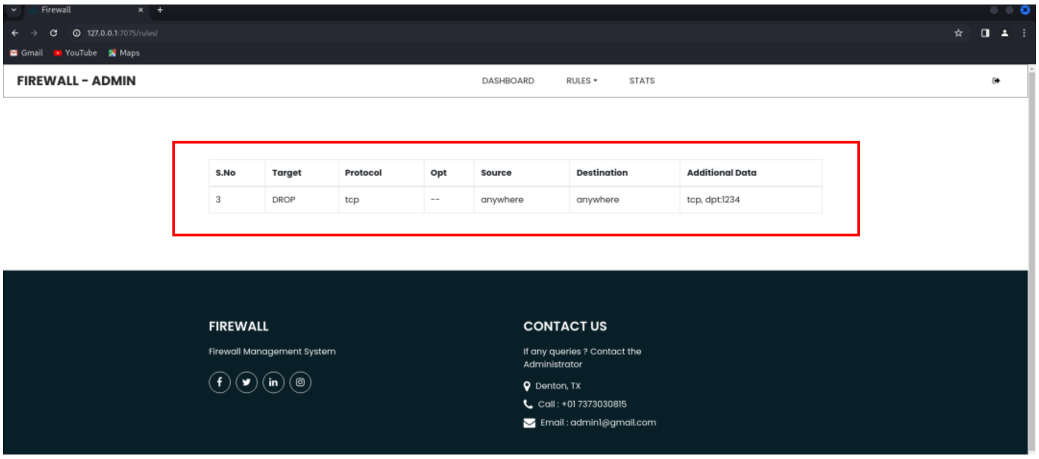
Source IPs	Dest IPs	Source Ports	Dest Ports	Protocols	Rate Limits
0	0	0	1	1	0

INCOMING TRAFFIC LOGS

Incoming Traffic Logs

Timestamp	Source	Destination	Protocol	Reason
2023-12-14T00:56:51.214233-05:00	142.250.182.99	192.10.32.5	UDP	FW_BLOCKED_INPUT
2023-12-14T00:56:51.217899-05:00	142.250.182.99	192.10.32.5	UDP	FW_BLOCKED_INPUT

- Available rules will be displayed in "rules list page"



S.No	Target	Protocol	Opt	Source	Destination	Additional Data
3	DROP	tcp	--	anywhere	anywhere	tcp, dpt:1234

FIREWALL

Firewall Management System

CONTACT US

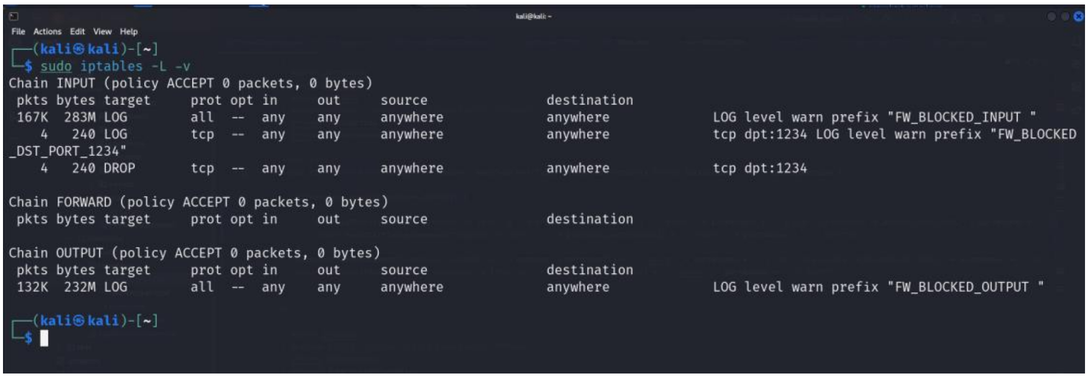
If any queries ? Contact the Administrator

Denton, TX

Call : +01 7373030815

Email : admin1@gmail.com

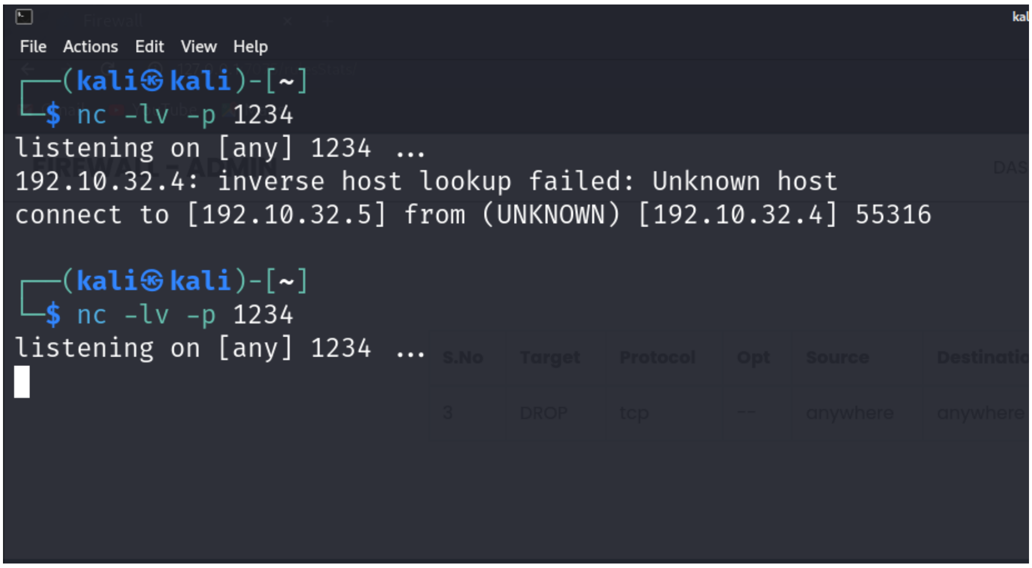
- Rule added in IPTables



```
┌──(kali㉿kali)-[~]
└─$ sudo iptables -L -v
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
 167K  283M LOG        all  --  any    any     anywhere             anywhere             LOG level warn prefix "FW_BLOCKED_INPUT "
    4   240 LOG        tcp  --  any    any     anywhere             anywhere             tcp dpt:1234 LOG level warn prefix "FW_BLOCKED
_DST_PORT_1234"
    4   240 DROP       tcp  --  any    any     anywhere             anywhere             tcp dpt:1234

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
 132K  232M LOG        all  --  any    any     anywhere             anywhere             LOG level warn prefix "FW_BLOCKED_OUTPUT "

┌──(kali㉿kali)-[~]
└─$ 
```

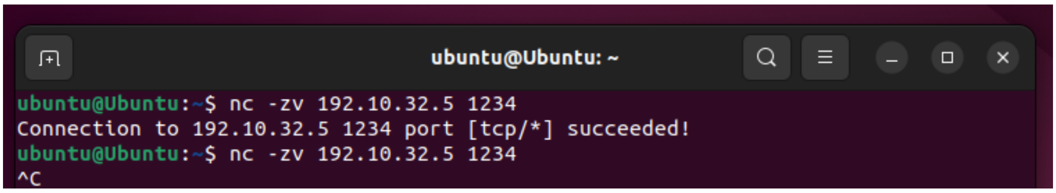
Currently, a Rule for blocking Destination TCP port 1234 has been added successfully in the IPTables. Now, let's try to reconnect to the Kali from Ubuntu on same TCP port 1234

- Kali is listening on TCP port 1234



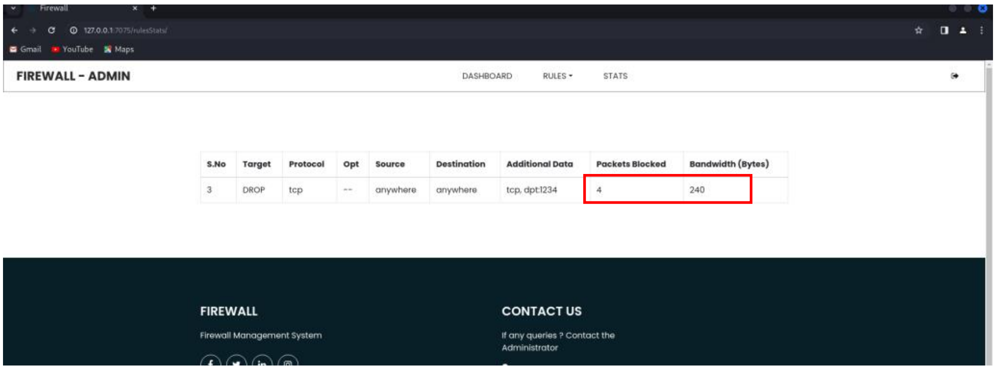
```
┌──(kali㉿kali)-[~]
└─$ nc -lv -p 1234
listening on [any] 1234 ...
192.10.32.4: inverse host lookup failed: Unknown host
connect to [192.10.32.5] from (UNKNOWN) [192.10.32.4] 55316

┌──(kali㉿kali)-[~]
└─$ nc -lv -p 1234
listening on [any] 1234 ...
```

- Ubuntu is trying to connect on TCP port 1234. But, there is no response and the connection is not established.



```
ubuntu@Ubuntu:~$ nc -zv 192.10.32.5 1234
Connection to 192.10.32.5 1234 port [tcp/*] succeeded!
ubuntu@Ubuntu:~$ nc -zv 192.10.32.5 1234
^C
```

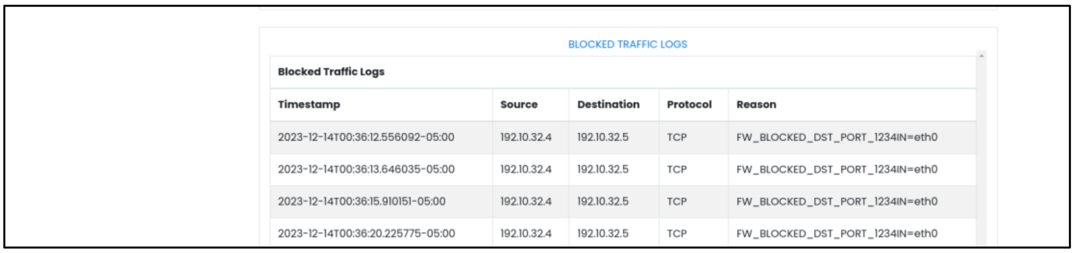
- In the statistics page the below details with Number of packets Blocked and Bandwidth is displayed.


Firewall
127.0.0.1:7075/rulesStats/
Gmail
YouTube
Maps
FIREWALL - ADMIN
DASHBOARD
RULES
STATS

S.No	Target	Protocol	Opt	Source	Destination	Additional Data	Packets Blocked	Bandwidth (Bytes)
3	DROP	tcp	--	anywhere	anywhere	tcp, dpt:1234	4	240

FIREWALL
Firewall Management System
CONTACT US
If any queries ? Contact the Administrator

- In the Dashboard, the logs for BLOCKED traffic were displayed.



Blocked Traffic Logs

Timestamp	Source	Destination	Protocol	Reason
2023-12-14T00:36:12.556092-05:00	192.10.32.4	192.10.32.5	TCP	FW_BLOCKED_DST_PORT_1234IN=eth0
2023-12-14T00:36:13.646035-05:00	192.10.32.4	192.10.32.5	TCP	FW_BLOCKED_DST_PORT_1234IN=eth0
2023-12-14T00:36:15.910151-05:00	192.10.32.4	192.10.32.5	TCP	FW_BLOCKED_DST_PORT_1234IN=eth0
2023-12-14T00:36:20.225775-05:00	192.10.32.4	192.10.32.5	TCP	FW_BLOCKED_DST_PORT_1234IN=eth0