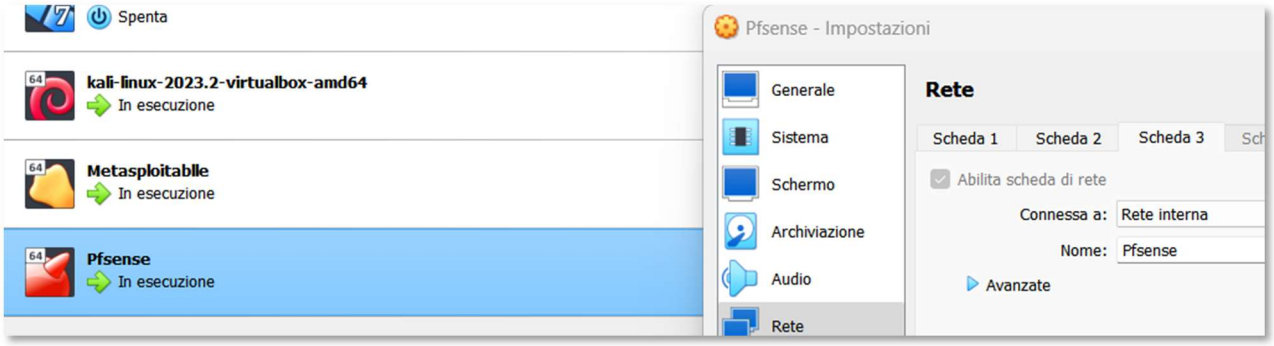
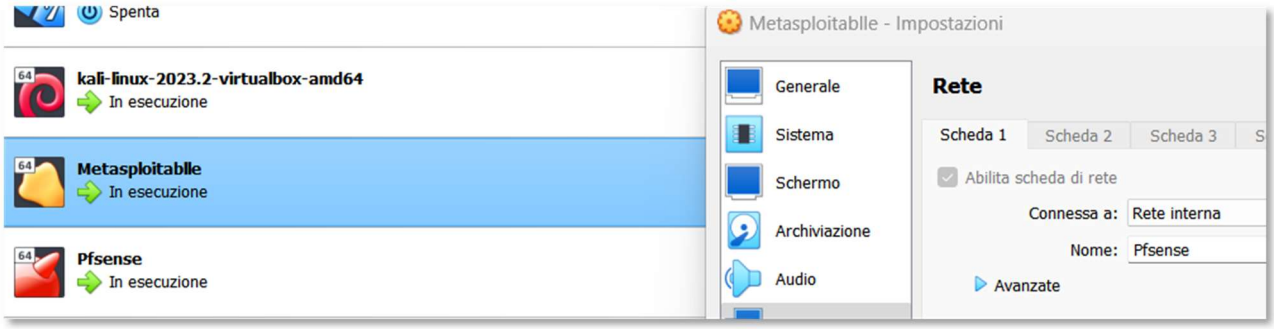
Configurazione reti su Virtual Box e macchine virtuali

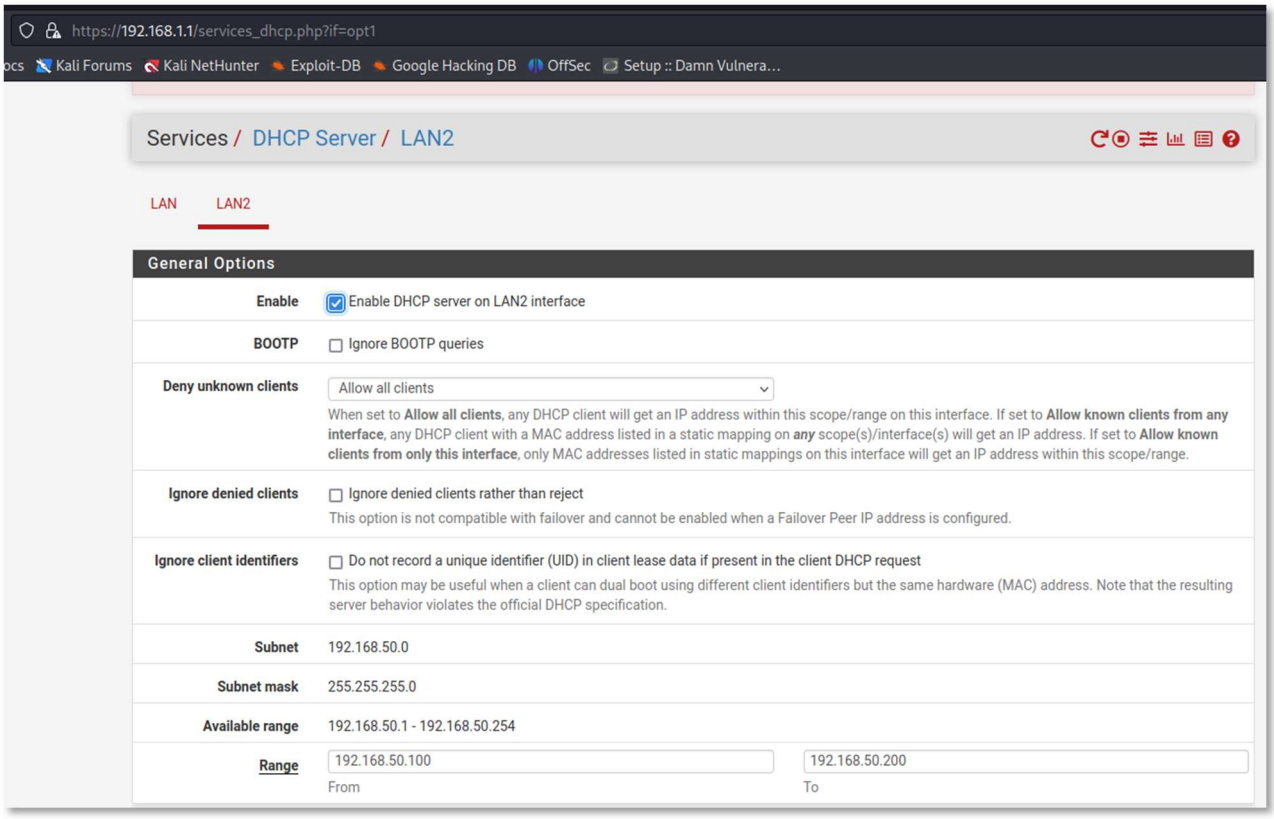
LAN2 Pfsense (rete di comunicazione Pfsense-Metasploitable)

Rete 192.168.50.0/24

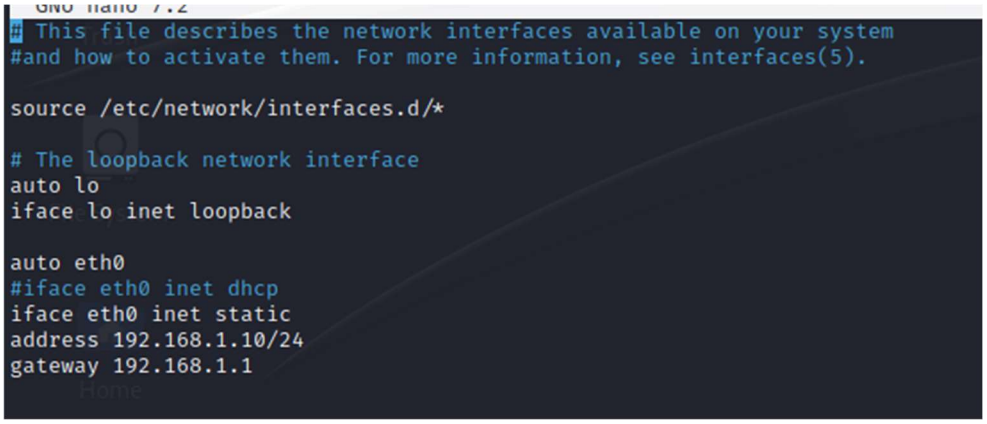




Abilitazione servizio DHCP per LAN2 Pfsense da tool web su Kali



Configurazione IP (statico) su /etc/network/interfaces della macchina Linux

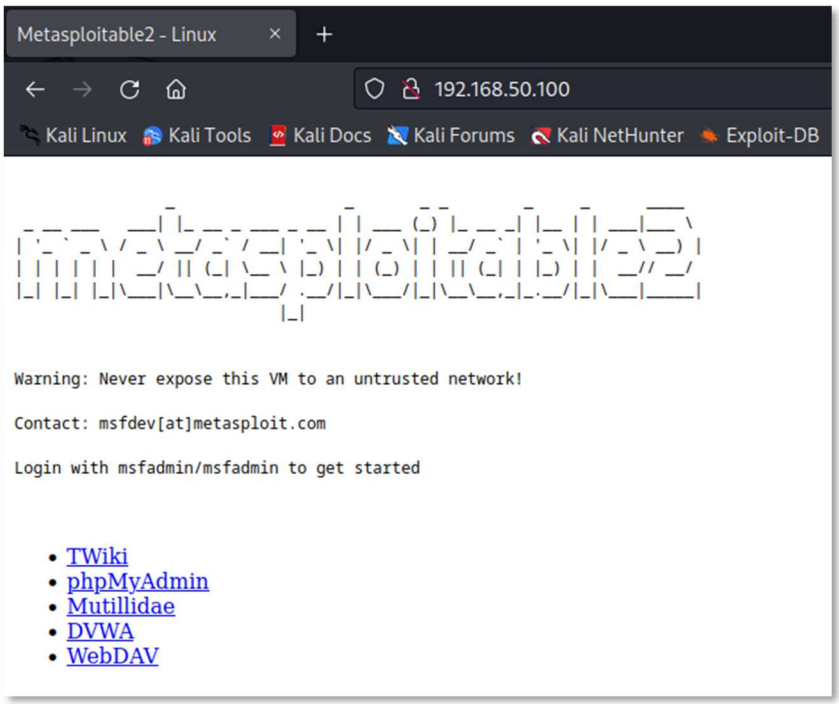


Configurazione IP DHCP su /etc/network/interfaces della macchina Metasploitable

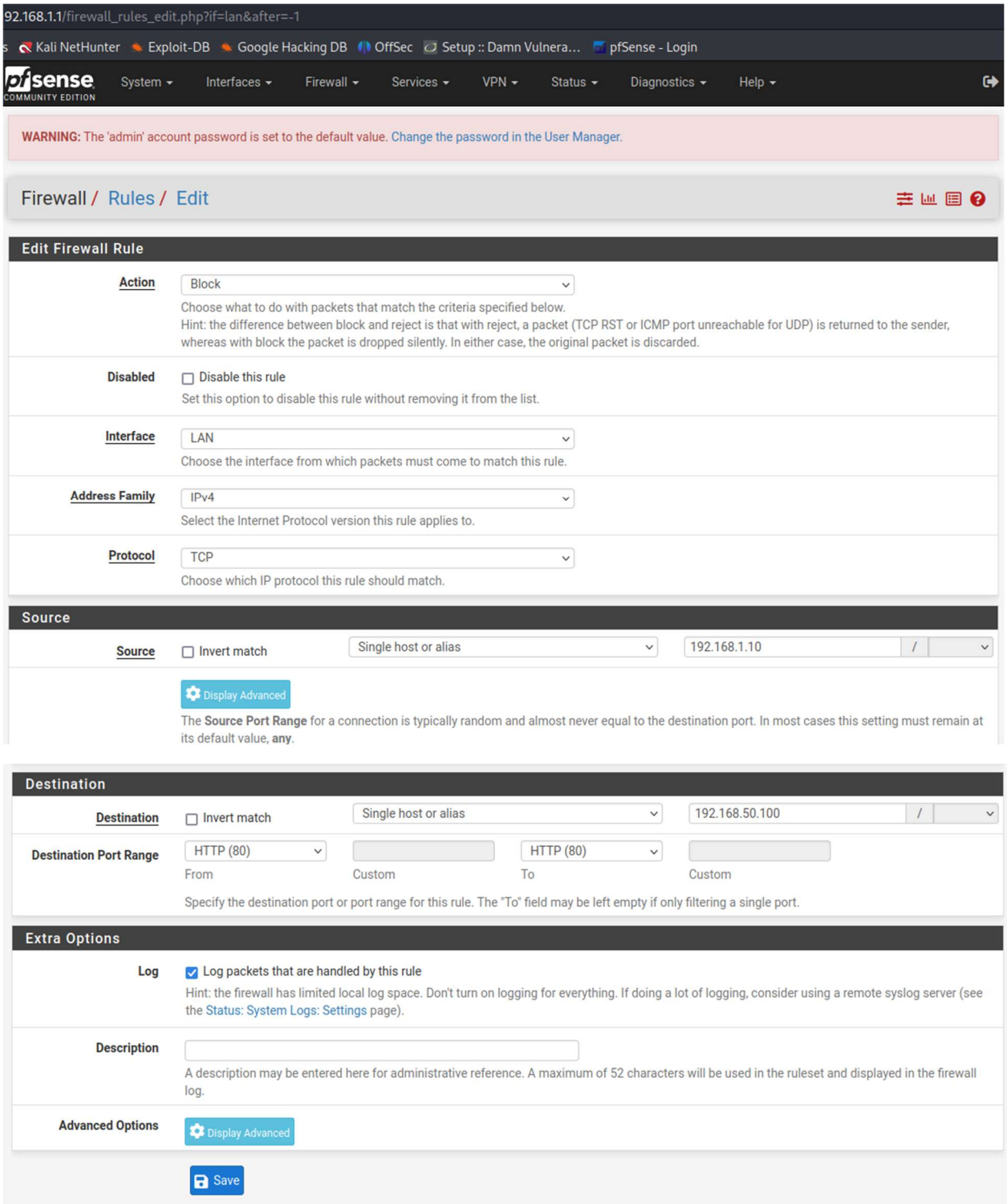
```
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto eth0
iface eth0 inet dhcp

#iface eth0 inet static
#address 192.168.32.101
#netmask 255.255.255.0
#network 192.168.32.0
#broadcast 192.168.32.255
#gateway 192.168.32.1
```

Verifica connettività da Kali a Metasploitable

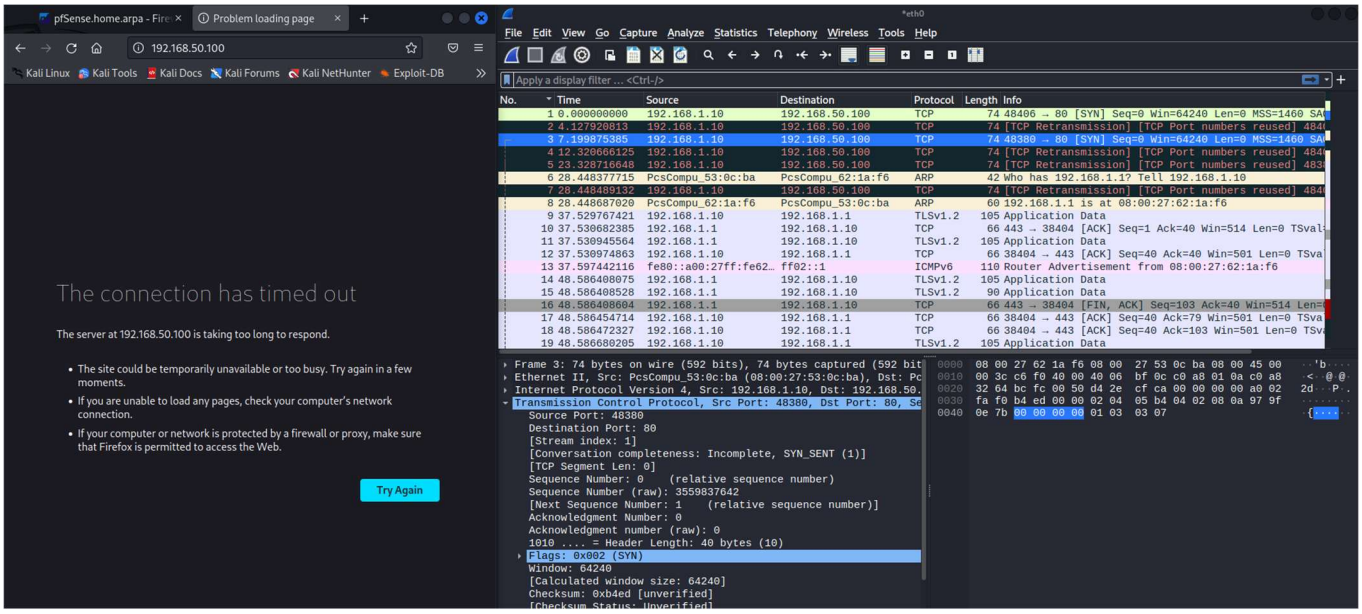
```
┌──(kali㉿kali)-[~]
└─$ ping 192.168.50.100
PING 192.168.50.100 (192.168.50.100) 56(84) bytes of data.
64 bytes from 192.168.50.100: icmp_seq=1 ttl=63 time=2.01 ms
64 bytes from 192.168.50.100: icmp_seq=2 ttl=63 time=1.95 ms
64 bytes from 192.168.50.100: icmp_seq=3 ttl=63 time=1.75 ms
64 bytes from 192.168.50.100: icmp_seq=4 ttl=63 time=1.86 ms
64 bytes from 192.168.50.100: icmp_seq=5 ttl=63 time=1.79 ms
^X64 bytes from 192.168.50.100: icmp_seq=6 ttl=63 time=1.58 ms
64 bytes from 192.168.50.100: icmp_seq=7 ttl=63 time=1.78 ms
64 bytes from 192.168.50.100: icmp_seq=8 ttl=63 time=0.375 ms
```



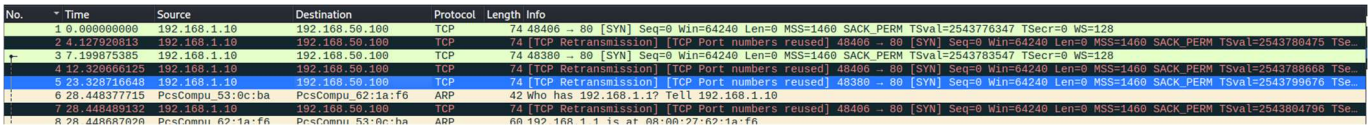
Creazione regola su Pfsense (da web tool su Kali) che blocca il traffico sulla porta 80 da Kali a Metasploitable con abilitazione dei log



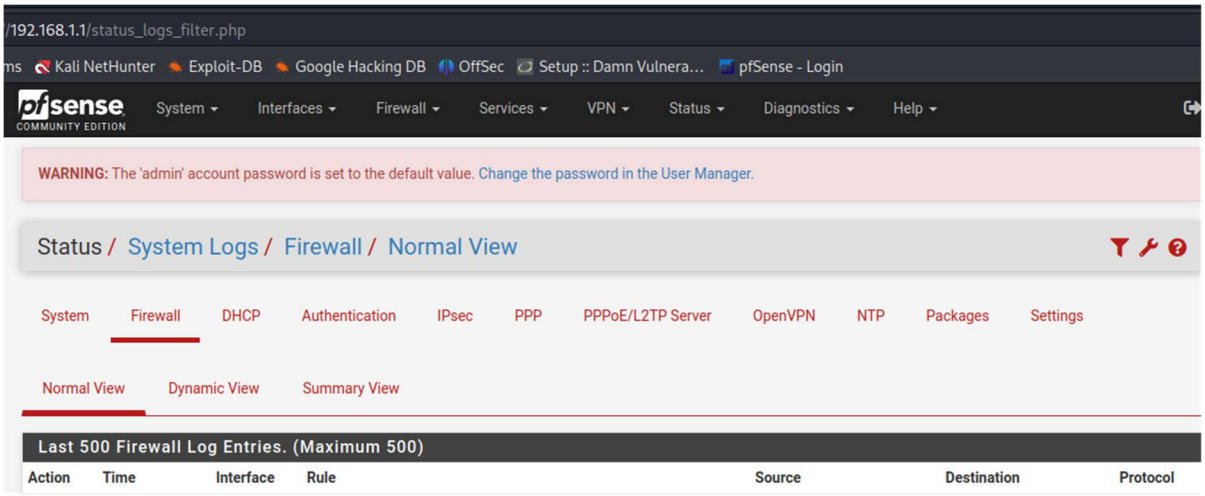
Tentativo di connessione sulla porta 80 da Kali a Metasploitable dopo applicazione regola di firewall e verifica dell'irraggiungibilità da browser web. Analisi dei pacchetti con Wireshark.



Tentativi di connessione senza risposta:



Verifica dell'applicazione della regola di Firewall anche dai log di pfsense abilitati con la creazione della regola



Last 500 Firewall Log Entries. (Maximum 500)

Action	Time	Interface	Rule	Source	Destination	Protocol
✕	Jul 23 11:55:15	LAN	USER_RULE (1690113252)	192.168.1.10:48380	192.168.50.100:80	TCP:S
✕	Jul 23 11:55:15	LAN	USER_RULE (1690113252)	192.168.1.10:48392	192.168.50.100:80	TCP:S
✕	Jul 23 11:55:16	LAN	USER_RULE (1690113252)	192.168.1.10:48380	192.168.50.100:80	TCP:S
✕	Jul 23 11:55:16	LAN	USER_RULE (1690113252)	192.168.1.10:48392	192.168.50.100:80	TCP:S
✕	Jul 23 11:55:18	LAN	USER_RULE (1690113252)	192.168.1.10:48380	192.168.50.100:80	TCP:S
✕	Jul 23 11:55:18	LAN	USER_RULE (1690113252)	192.168.1.10:48392	192.168.50.100:80	TCP:S
✕	Jul 23 11:55:20	LAN	USER_RULE (1690113252)	192.168.1.10:48406	192.168.50.100:80	TCP:S
✕	Jul 23 11:55:21	LAN	USER_RULE (1690113252)	192.168.1.10:48406	192.168.50.100:80	TCP:S
✕	Jul 23 11:55:22	LAN	USER_RULE (1690113252)	192.168.1.10:48380	192.168.50.100:80	TCP:S
✕	Jul 23 11:55:23	LAN	USER_RULE (1690113252)	192.168.1.10:48406	192.168.50.100:80	TCP:S
✕	Jul 23 11:55:27	LAN	USER_RULE (1690113252)	192.168.1.10:48406	192.168.50.100:80	TCP:S
✕	Jul 23 11:55:30	LAN	USER_RULE (1690113252)	192.168.1.10:48380	192.168.50.100:80	TCP:S
✕	Jul 23 11:55:36	LAN	USER_RULE (1690113252)	192.168.1.10:48406	192.168.50.100:80	TCP:S
✕	Jul 23 11:55:47	LAN	USER_RULE (1690113252)	192.168.1.10:48380	192.168.50.100:80	TCP:S
✕	Jul 23 11:55:52	LAN	USER_RULE (1690113252)	192.168.1.10:48406	192.168.50.100:80	TCP:S
✕	Jul 23 11:56:19	LAN	USER_RULE (1690113252)	192.168.1.10:48380	192.168.50.100:80	TCP:S
✕	Jul 23 11:56:25	LAN	USER_RULE (1690113252)	192.168.1.10:48406	192.168.50.100:80	TCP:S