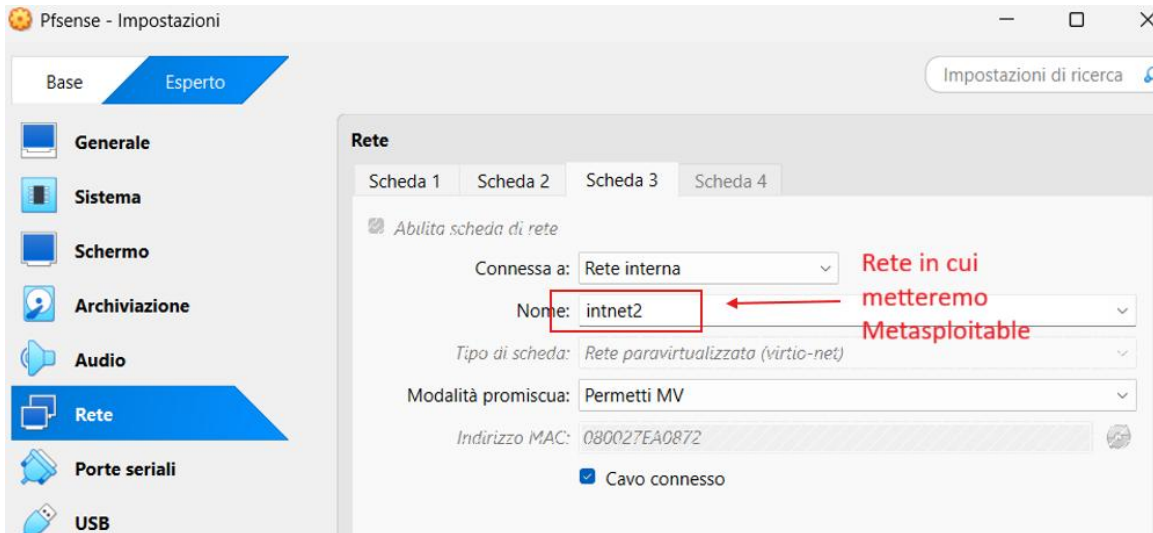
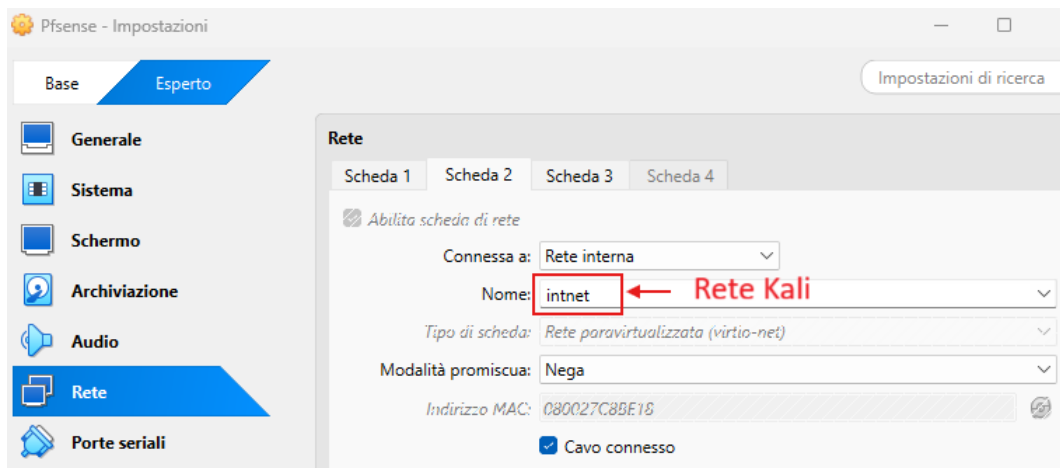


Configurazione reti in VirtualBox

pfSense

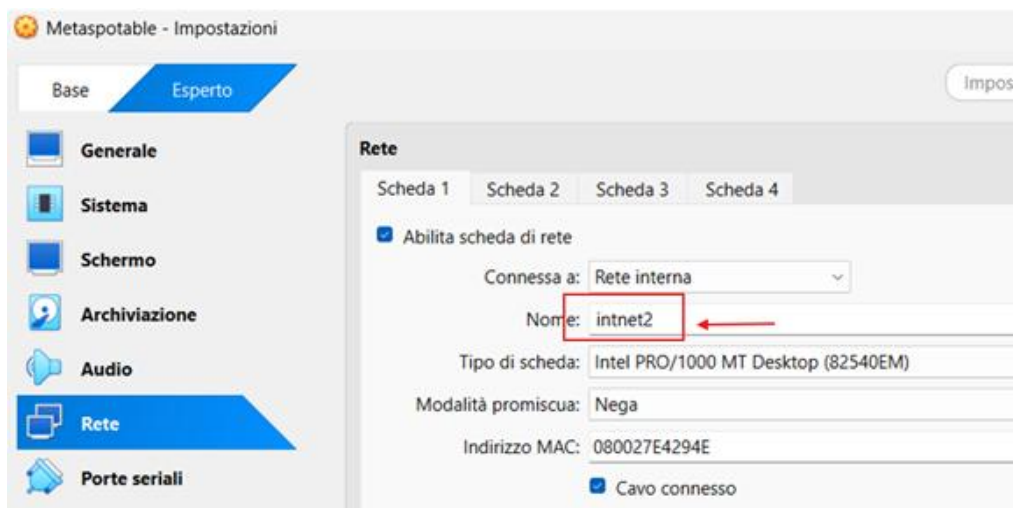
In pfSense configureremo due reti distinte, una per Kali e una per Metasploitable





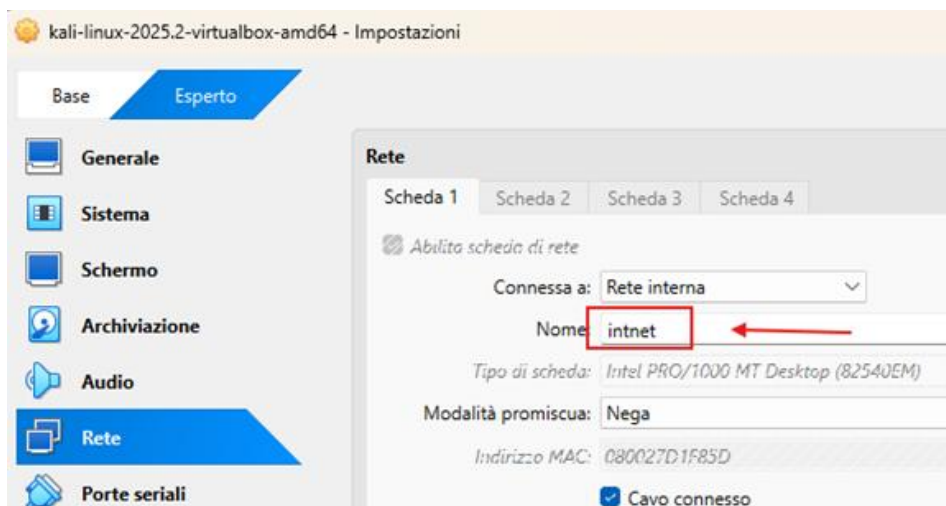
Metasploitable

Metasploitable si troverà dentro una delle 2 reti di pfSense **intnet2**



Kali

Kali si troverà dentro l'altra delle due reti interne di pfSense **intnet**



Configurazione interne delle VM

Metasploitable

Metasploitable si troverà dentro una rete (vedi immagine sotto).

```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:e4:29:4e
          inet addr:192.168.51.101  Bcast:192.168.51.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fee4:294e/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:2 errors:0 dropped:0 overruns:0 frame:0
          TX packets:63 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:128 (128.0 B)  TX bytes:5194 (5.0 KB)
          Base address:0xd010 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:124 errors:0 dropped:0 overruns:0 frame:0
          TX packets:124 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:30789 (30.0 KB)  TX bytes:30789 (30.0 KB)
```

Kali

Kali si troverà dentro l'altra rete.

```
(kali@kali)-[~]
$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:d1:f8:5d brd ff:ff:ff:ff:ff:ff
    inet 192.168.50.100/24 brd 192.168.50.255 scope global noprefixroute eth0
        valid_lft forever preferred_lft forever
    inet6 fe80::8417:1efb:8b3a:5970/64 scope link noprefixroute
        valid_lft forever preferred_lft forever

(kali@kali)-[~]
$
```

Configurazione pfSense

Kali

Interfaces / LAN (vtnet1)

General Configuration

Enable ☒ Enable interface

Description
Enter a description (name) for the interface here.

IPv4 Configuration Type

IPv6 Configuration Type

MAC Address
This field can be used to modify ("spoof") the MAC address of this interface.
Enter a MAC address in the following format: xxxxxxxxxxxx or leave blank.

MTU
If this field is blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary in some circumstances.

MSS
If a value is entered in this field, then MSS clamping for TCP connections to the value entered above minus 40 for IPv4 (TCP/IPv4 header size) minus 60 for IPv6 (TCP/IPv6 header size) will be in effect.

Speed and Duplex
Explicitly set speed and duplex mode for this interface.
WARNING: MUST be set to autoselect (automatically negotiate speed) unless the port this interface connects to has its speed and duplex fixed.

Static IPv4 Configuration

IPv4 Address ← **Rete Kali** / 24

Metasploitable

Interfaces / Metasploitable (vtnet2)

General Configuration

Enable ☒ Enable interface

Description
Enter a description (name) for the interface here.

IPv4 Configuration Type

IPv6 Configuration Type

MAC Address
This field can be used to modify ("spoof") the MAC address of this interface.
Enter a MAC address in the following format: xxxxxxxx or leave blank.

MTU
If this field is blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary in some circumstances.

MSS
If a value is entered in this field, then MSS clamping for TCP connections to the value entered above minus 40 for IPv4 (TCP/IPv4 header size) and minus 60 for IPv6 (TCP/IPv6 header size) will be in effect.

Speed and Duplex
Explicitly set speed and duplex mode for this interface.
WARNING: MUST be set to autoselect (automatically negotiate speed) unless the port this interface connects to has its speed and duplex forced.

Static IPv4 Configuration

IPv4 Address ← Rete Metasploitable /

Test Kali > Metasploitable senza regole di firewall

Ping

Facendo un ping da Kali a Metasploitable vediamo che le due macchine comunicano

```
(kali㉿kali)-[~]
$ ping 192.168.51.101
PING 192.168.51.101 (192.168.51.101) 56(84) bytes of data.
64 bytes from 192.168.51.101: icmp_seq=1 ttl=63 time=3.91 ms
64 bytes from 192.168.51.101: icmp_seq=2 ttl=63 time=3.17 ms
64 bytes from 192.168.51.101: icmp_seq=3 ttl=63 time=4.80 ms
^C
— 192.168.51.101 ping statistics —
3 packets transmitted, 3 received, 0% packet loss, time 2001ms
rtt min/avg/max/mdev = 3.173/3.959/4.799/0.664 ms
```

Traceroute

Con il Traceroute da Kali a Metasploitable notiamo che la comunicazione passa per il firewall pfSense

```
(kali㉿kali)-[~]
$ traceroute 192.168.51.101
traceroute to 192.168.51.101 (192.168.51.101), 30 hops max, 60 byte packets
1  pfSense.home.arpa 192.168.50.1 4.911 ms 4.634 ms 4.415 ms
2  192.168.51.101 (192.168.51.101) 6.442 ms 6.224 ms 5.957 ms
```

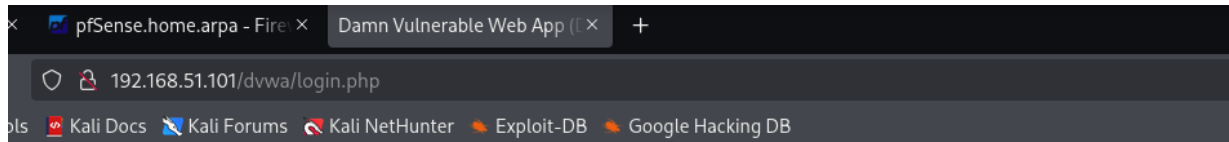
Wireshark

Anche monitorando i pacchetti del ping su Wireshark notiamo che la destinazione risponde

22	21.092478372	192.168.51.101	192.168.50.100	ICMP	98 Echo (ping) reply	id=0x0006, seq=4/1024, ttl=63 (request in 21)
23	22.090942334	192.168.50.100	192.168.51.101	ICMP	98 Echo (ping) request	id=0x0006, seq=5/1280, ttl=64 (reply in 24)
24	22.093706053	192.168.51.101	192.168.50.100	ICMP	98 Echo (ping) reply	id=0x0006, seq=5/1280, ttl=63 (request in 23)
25	23.096685756	192.168.50.100	192.168.51.101	ICMP	98 Echo (ping) request	id=0x0006, seq=6/1536, ttl=64 (reply in 26)
26	23.101350419	192.168.51.101	192.168.50.100	ICMP	98 Echo (ping) reply	id=0x0006, seq=6/1536, ttl=63 (request in 25)
27	24.098765789	192.168.50.100	192.168.51.101	ICMP	98 Echo (ping) request	id=0x0006, seq=7/1792, ttl=64 (reply in 28)
28	24.102642918	192.168.51.101	192.168.50.100	ICMP	98 Echo (ping) reply	id=0x0006, seq=7/1792, ttl=63 (request in 27)
29	25.100532812	192.168.50.100	192.168.51.101	ICMP	98 Echo (ping) request	id=0x0006, seq=8/2048, ttl=64 (reply in 30)
30	25.103854871	192.168.51.101	192.168.50.100	ICMP	98 Echo (ping) reply	id=0x0006, seq=8/2048, ttl=63 (request in 29)
31	26.177919760	192.168.50.100	192.168.51.101	ICMP	98 Echo (ping) request	id=0x0006, seq=9/2304, ttl=64 (reply in 32)
32	26.180732272	192.168.51.101	192.168.50.100	ICMP	98 Echo (ping) reply	id=0x0006, seq=9/2304, ttl=63 (request in 31)
33	27.193514901	192.168.50.100	192.168.51.101	ICMP	98 Echo (ping) request	id=0x0006, seq=10/2560, ttl=64 (reply in 34)
34	27.196226124	192.168.51.101	192.168.50.100	ICMP	98 Echo (ping) reply	id=0x0006, seq=10/2560, ttl=63 (request in 33)

DVWA

Accediamo regolarmente a DVWA



Username

admin

Password

•••••

Login

Regola di firewall che impedisce a Kali di raggiungere Metasploitable

Configurazione regola in pfSense

Action ☐ Block **La nuova regola Blocca (Block)...**

Choose what to do with packets that match the criteria specified below.
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

Disabled ☐ Disable this rule
Set this option to disable this rule without removing it from the list.

Interface LAN
Choose the interface from which packets must come to match this rule.

Address Family IPv4
Select the Internet Protocol version this rule applies to.

Protocol TCP
Choose which IP protocol this rule should match.

Source

Source ☐ Invert match Address or Alias 192.168.50.100 /

Destination ...sulla porta 80.

Destination ☐ Invert match Address or Alias 192.168.51.101 /

Destination Port Range HTTP (80) From Custom HTTP (80) To

Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.

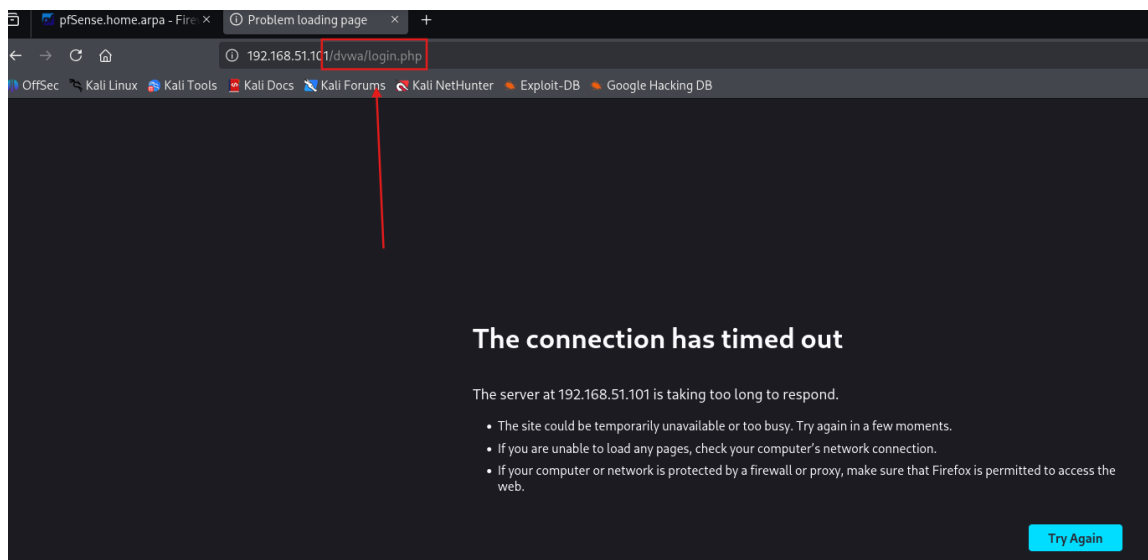
...le comunicazioni provenienti dall'IP di Kali (192.168.50.100)...

...verso l'IP di Metasploitable (192.168.51.101)...

Ping

Il ping funzionerà perché l'IP di Metasploitable è raggiungibile, ma non avremo accesso a DWA perché gira sulla porta 80

```
(kali@kali)-[~]
$ ping 192.168.51.101
PING 192.168.51.101 (192.168.51.101) 56(84) bytes of data:
64 bytes from 192.168.51.101: icmp_seq=1 ttl=63 time=2.75 ms
64 bytes from 192.168.51.101: icmp_seq=2 ttl=63 time=4.39 ms
64 bytes from 192.168.51.101: icmp_seq=3 ttl=63 time=3.03 ms
```



Facendo nmap notiamo che lo stato della porta 80 è **filtered**

```
(kali㉿kali)-[~]
└─$ nmap -p 80 192.168.51.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-10 09:35 EDT
Nmap scan report for 192.168.51.101
Host is up (0.0021s latency).

PORT      STATE      SERVICE
80/tcp    filtered  http

Nmap done: 1 IP address (1 host up) scanned in 0.40 seconds
```


Su Wireshark vedremo che il client invia richieste senza ricevere risposta dal server

tcp.stream eq 05

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.50.100	192.168.51.101	TCP	74	34456 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
3	1.033831647	192.168.50.100	192.168.51.101	TCP	74	[TCP Retransmission] 34456 → 80 [SYN] Seq=0 Win=
5	2.053807219	192.168.50.100	192.168.51.101	TCP	74	[TCP Retransmission] 34456 → 80 [SYN] Seq=0 Win=
7	3.078814069	192.168.50.100	192.168.51.101	TCP	74	[TCP Retransmission] 34456 → 80 [SYN] Seq=0 Win=
9	4.102287724	192.168.50.100	192.168.51.101	TCP	74	[TCP Retransmission] 34456 → 80 [SYN] Seq=0 Win=
12	5.132480916	192.168.50.100	192.168.51.101	TCP	74	[TCP Retransmission] 34456 → 80 [SYN] Seq=0 Win=
15	7.142490866	192.168.50.100	192.168.51.101	TCP	74	[TCP Retransmission] 34456 → 80 [SYN] Seq=0 Win=
17	11.274477694	192.168.50.100	192.168.51.101	TCP	74	[TCP Retransmission] 34456 → 80 [SYN] Seq=0 Win=
19	19.465871466	192.168.50.100	192.168.51.101	TCP	74	[TCP Retransmission] 34456 → 80 [SYN] Seq=0 Win=
21	35.594366063	192.168.50.100	192.168.51.101	TCP	74	[TCP Retransmission] 34456 → 80 [SYN] Seq=0 Win=
26	69.638924367	192.168.50.100	192.168.51.101	TCP	74	[TCP Retransmission] 34456 → 80 [SYN] Seq=0 Win=

Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface eth0, id 0

Ethernet II, Src: PCSSystemtec_d1:f8:5d (08:00:27:d1:f8:5d), Dst: PCSSystemtec_da:f0:f3 (08:00:27:da:f0:f3)

Internet Protocol Version 4, Src: 192.168.50.100, Dst: 192.168.51.101

Transmission Control Protocol, Src Port: 34456, Dst Port: 80, Seq: 0, Len: 0

Source Port: 34456

Destination Port: 80

[Stream index: 0]

[Stream Packet Number: 1]

[Conversation completeness: Incomplete, SYN_SENT (1)]

...0... = RST: Absent

...0... = FIN: Absent

...0... = Data: Absent

...0... = ACK: Absent

...0... = SYN-ACK: Absent

...1... = SYN: Present

[Completeness Flags:S]

[TCP Segment Len: 0]

Sequence Number: 0 (relative sequence number)

Sequence Number (raw): 2699638679

[Next Sequence Number: 1 (relative sequence number)]

Acknowledgment Number: 0

Acknowledgment number (raw): 0

1010 = Header Length: 40 bytes (10)

Flags: 0x002 (SYN)

Window: 64240

[Calculated window size: 64240]

Checksum: 0xa748 (unverified)

0000 08 00 27 d1

0010 00 3c 7f 9d

0020 33 65 86 9d

0030 fa f0 e7 4d

0040 0a 3f 00 00

Dal log di pfSense vedremo inoltre i tentativi di accesso bloccati

✖	Sep 9 21:16:29	WAN	Block private networks from WAN block 192.168/16 (12004)	192.168.1.17:17500	192.168.1.255:17500	UDP
✖	Sep 9 21:16:59	WAN	Block private networks from WAN block 192.168/16 (12004)	192.168.1.17:17500	192.168.1.255:17500	UDP
✖	Sep 9 21:17:29	WAN	Block private networks from WAN block 192.168/16 (12004)	192.168.1.17:17500	192.168.1.255:17500	UDP
✖	Sep 9 21:17:52	WAN	Block private networks from WAN block 192.168/16 (12004)	192.168.1.1	224.0.0.1	IGMP
✖	Sep 9 21:17:59	WAN	Block private networks from WAN block 192.168/16 (12004)	192.168.1.17:17500	192.168.1.255:17500	UDP
✖	Sep 9 21:18:29	WAN	Block private networks from WAN block 192.168/16 (12004)	192.168.1.17:17500	192.168.1.255:17500	UDP
✖	Sep 9 21:18:59	WAN	Block private networks from WAN block 192.168/16 (12004)	192.168.1.17:17500	192.168.1.255:17500	UDP
✖	Sep 9 21:19:29	WAN	Block private networks from WAN block 192.168/16 (12004)	192.168.1.17:17500	192.168.1.255:17500	UDP
✖	Sep 9 21:19:58	WAN	Block private networks from WAN block 192.168/16 (12004)	192.168.1.1	224.0.0.1	IGMP
✖	Sep 9 21:20:00	WAN	Block private networks from WAN block 192.168/16 (12004)	192.168.1.17:17500	192.168.1.255:17500	UDP
✖	Sep 9 21:20:30	WAN	Block private networks from WAN block 192.168/16 (12004)	192.168.1.17:17500	192.168.1.255:17500	UDP