

Installazione e configurazione regole Firewall PfSense – Alessio Russo Modulo 3 Esercitazione 3

Innanzitutto abbiamo proceduto con la configurazione di PfSense configurando una rete WAN e due LAN le quali sono abilitate su gateway delle due macchine virtuali. Nelle immagini sotto le tre configurazioni PfSense Kali e Metasploitable

```
PfSense [Running]
Starting CRON... done.
pfSense 2.7.2-RELEASE amd64 20231206-2010
Bootup complete

FreeBSD/amd64 (pfSense.home.arpa) (ttyv0)

VirtualBox Virtual Machine - Netgate Device ID: 1b42d9e09b63e36c3a1b

*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0      -> v4/DHCP4: 10.0.2.15/24
LAN (lan)      -> em1      -> v4: 192.168.50.1/24
LAN2 (opt1)    -> em2      -> v4: 192.168.49.1/24

0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults  13) Update from console
5) Reboot system              14) Enable Secure Shell (sshd)
6) Halt system                 15) Restore recent configuration
7) Ping host                   16) Restart PHP-FPM
8) Shell

Enter an option: █
```

```
(kali㉿kali)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.50.100 netmask 255.255.255.0 broadcast 192.168.50.255
    inet6 fe80::a00:27ff:feeb:7ef5 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:cb:7e:f5 txqueuelen 1000 (Ethernet)
    RX packets 371 bytes 28167 (27.5 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 405 bytes 31525 (30.7 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 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 7 bytes 504 (504.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 7 bytes 504 (504.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

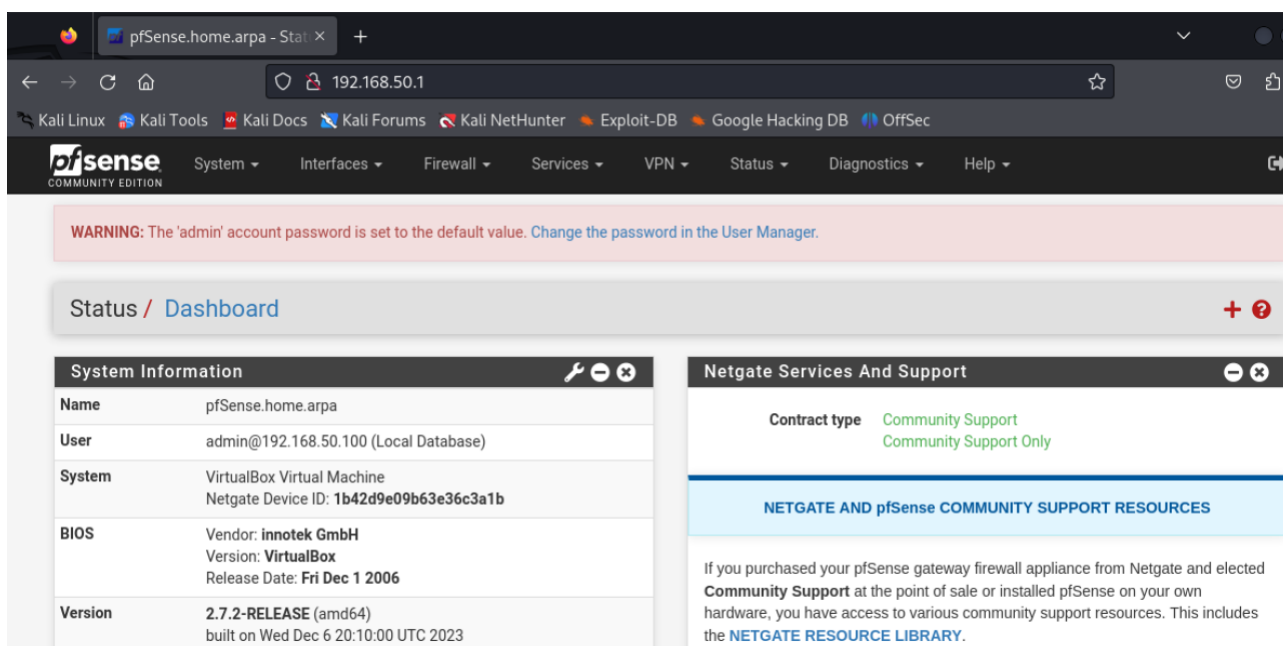
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
nsfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:9d:f5:e4
          inet addr:192.168.49.101  Bcast:192.168.49.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe9d:f5e4/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1 errors:0 dropped:0 overruns:0 frame:0
          TX packets:57 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:64 (64.0 B)  TX bytes:4942 (4.8 KB)
          Base address:0xd020 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:132 errors:0 dropped:0 overruns:0 frame:0
          TX packets:132 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:34877 (34.0 KB)  TX bytes:34877 (34.0 KB)

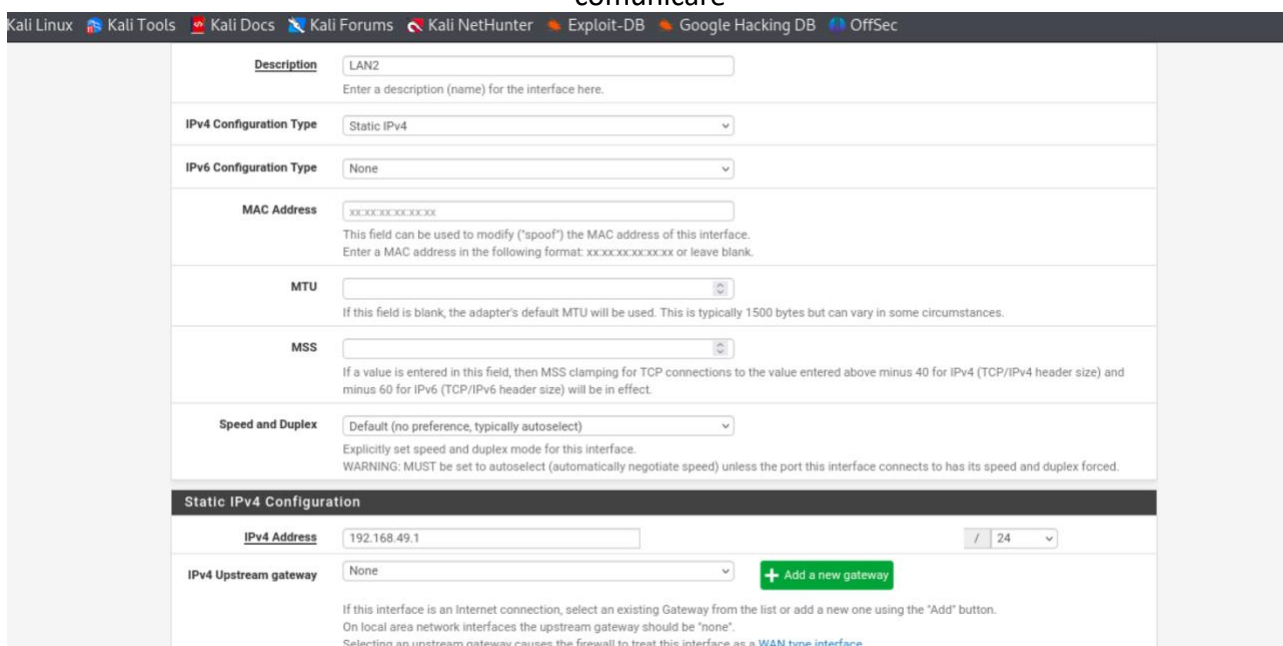
nsfadmin@metasploitable:~$
```

Il secondo step prevedeva l'accesso e la configurazione di PfSense in modo che si potesse accedere da kali Linux.

Entrando in Firefox e digitando l'IP assegnato un case di configurazione riusciamo ad accedere come da immagine



Procediamo successivamente alla creazione di una seconda rete LAN in modo che Kali e Metasploitable siano su due gateway differenti ma tramite PfSense possano comunque comunicare



Successivamente creiamo la regola di Block della comunicazione tra la macchina Kali e metasploitable andando ad inserire IP sorgente quello di mali Linux e IP di destinazione quello della macchina metasploitable i postando il block sul protocollo http porta 80 e analizzando la chiamata da browser con wireshark si nota che le due macchine non comunicano

FloatingWANLANLAN2

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
<input checked="" type="checkbox"/>	✓	14/244 KiB	*	*	*	LAN Address	80	*	*	Anti-Lockout Rule
<input type="checkbox"/>	✗	0/0 B	IPv4 TCP	192.168.50.100	*	192.168.49.101	80 (HTTP)	*	none	Kali -Meta - Blocked
<input type="checkbox"/>	✓	18/57 KiB	IPv4 *	LAN subnets	*	*	*	none		Default allow LAN to any rule
<input type="checkbox"/>	✓	0/0 B	IPv6 *	LAN subnets	*	*	*	none		Default allow LAN IPv6 to any rule

↑ Add

↓ Add

🗑 Delete

🔄 Toggle

📄 Copy

🔒

i

Time	Source	Destination	Protocol	Length	Info
21 15.176887685	192.168.50.100	192.168.49.101	TCP	74	44696 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2490699193 TSecr=0 WS=128
32 15.428663718	192.168.50.100	192.168.49.101	TCP	74	44696 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2490699445 TSecr=0 WS=128
34 16.102552105	192.168.50.100	192.168.49.101	TCP	74	[TCP Retransmission] 44696 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=24907002
35 16.449559974	192.168.50.100	192.168.49.101	TCP	74	[TCP Retransmission] 44696 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=24907004
37 17.210705383	192.168.50.100	192.168.49.101	TCP	74	[TCP Retransmission] 44696 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=24907015
38 17.472307777	192.168.50.100	192.168.49.101	TCP	74	[TCP Retransmission] 44696 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=24907014
40 18.241477541	192.168.50.100	192.168.49.101	TCP	74	[TCP Retransmission] 44696 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=24907022
42 18.500629363	192.168.50.100	192.168.49.101	TCP	74	[TCP Retransmission] 44696 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=24907025
45 19.264033240	192.168.50.100	192.168.49.101	TCP	74	[TCP Retransmission] 44696 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=24907032
46 19.520529059	192.168.50.100	192.168.49.101	TCP	74	[TCP Retransmission] 44696 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=24907035
50 20.280250038	192.168.50.100	192.168.49.101	TCP	74	[TCP Retransmission] 44696 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=24907043
51 20.546883680	192.168.50.100	192.168.49.101	TCP	74	[TCP Retransmission] 44696 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=24907040
56 22.365180039	192.168.50.100	192.168.49.101	TCP	74	[TCP Retransmission] 44696 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=24907069
57 22.500330728	192.168.50.100	192.168.49.101	TCP	74	[TCP Retransmission] 44696 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=24907065
62 26.400661432	192.168.50.100	192.168.49.101	TCP	74	[TCP Retransmission] 44696 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=24907104
63 26.650136551	192.168.50.100	192.168.49.101	TCP	74	[TCP Retransmission] 44696 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=24907100

Infine andiamo a vedere i log del firewall PfSense e notiamo che effettivamente la regola impostata blocca le connessioni

Action	Time	Interface	Rule	Source	Destination	Protocol
✗	Jan 7 18:18:17	LAN	Block DVWA (1704651332)	192.168.50.100:49628	192.168.49.101:80	TCP:S
✗	Jan 7 18:18:17	LAN	Block DVWA (1704651332)	192.168.50.100:49632	192.168.49.101:80	TCP:S
✗	Jan 7 18:18:18	LAN	Block DVWA (1704651332)	192.168.50.100:49628	192.168.49.101:80	TCP:S
✗	Jan 7 18:18:18	LAN	Block DVWA (1704651332)	192.168.50.100:49632	192.168.49.101:80	TCP:S
✗	Jan 7 18:18:19	LAN	Block DVWA (1704651332)	192.168.50.100:49628	192.168.49.101:80	TCP:S