



Build Week 1

PF SENSE



Contents

01

Introduzione a PF Sense

02

comunicazione tra client e server

03

Creazione regola che blocca l'accesso alla DWVA

04

Sblocco comunicazione tra client e server

05

Conclusioni e ringraziamenti

1. Introduzione a PF Sense

pfSense, una piattaforma open source per firewall e router basata su FreeBSD. Il software è progettato per una gestione molto avanzata del traffico di rete attraverso un'interfaccia web intuitiva. Utilizza un firewall stateful che permette un controllo molto preciso delle connessioni e la creazione di regole per bloccare la comunicazione indesiderata. Supporta NAT, così l'indirizzo IP privato è associato ad un indirizzo IP pubblico (PAT) permettendo a diversi dispositivi di utilizzare un singolo IP pubblico. Inoltre, supporta VPN come IPsec e la configurazione VLAN per una maggiore sicurezza. Gestisce anche entrambe le forme di routing avanzato. Si può aggiungere come add-on funzioni di IDS/IPS come ulteriore controllo della linea.

2. Comunicazione tra client e server

Comunicazione tra client di Kali e server di metasploitable avvenuta correttamente

```
(kali@kali)-[~]
$ ping 192.168.50.101
PING 192.168.50.101 (192.168.50.101) 56(84) bytes of data:
64 bytes from 192.168.50.101: icmp_seq=1 ttl=63 time=1.57 ms
64 bytes from 192.168.50.101: icmp_seq=2 ttl=63 time=1.38 ms
64 bytes from 192.168.50.101: icmp_seq=3 ttl=63 time=3.58 ms
64 bytes from 192.168.50.101: icmp_seq=4 ttl=63 time=1.33 ms
64 bytes from 192.168.50.101: icmp_seq=5 ttl=63 time=1.30 ms
64 bytes from 192.168.50.101: icmp_seq=6 ttl=63 time=1.17 ms
64 bytes from 192.168.50.101: icmp_seq=7 ttl=63 time=1.89 ms
64 bytes from 192.168.50.101: icmp_seq=8 ttl=63 time=1.33 ms
64 bytes from 192.168.50.101: icmp_seq=9 ttl=63 time=1.11 ms
64 bytes from 192.168.50.101: icmp_seq=10 ttl=63 time=1.46 ms
^C
--- 192.168.50.101 ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9221ms
rtt min/avg/max/mdev = 1.112/1.611/3.579/0.688 ms

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

```
Metasploitable2 [Running] - Oracle VirtualBox
iface lo inet loopback

# The primary network interface
auto eth0
iface eth0 inet static
address 192.168.50.101
gateway 192.168.50.254
netmask 255.255.255.0
dns-nameservers 192.168.50.254

[ Read 14 lines ]

root@metasploitable:/home/msfadmin# ping 192.168.1.101
PING 192.168.1.101 (192.168.1.101) 56(84) bytes of data.

--- 192.168.1.101 ping statistics ---
6 packets transmitted, 0 received, 100% packet loss, time 4999ms

root@metasploitable:/home/msfadmin#
```

3. Creazione regola che blocca l'accesso alla DWVA

The screenshot displays a network security configuration interface with a terminal window open on the right.

Terminal Window (Clone di meta2 [In esecuzione] - Oracle VirtualBox):

```
msfadmin@metasploitable:~$ 1
-bash: 1: command not found
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:43:48:87
          inet addr:192.168.50.101  Bcast:192.168.50.255  Mask:
          inet6 addr: fe80::a00:27ff:fe43:4887/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:4 errors:0 dropped:0 overruns:0 frame:0
          TX packets:85 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:270 (270.0 B)  TX bytes:8283 (8.0 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:143 errors:0 dropped:0 overruns:0 frame:0
          TX packets:143 errors:0 dropped:0 overruns:0 carrier:
          collisions:0 txqueuelen:0
          RX bytes:37589 (36.7 KB)  TX bytes:37589 (36.7 KB)
```

Firewall Rules Table:

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule
✓ 0/6 KiB	*	*	*	LAN Address	80	*	*	
✗ 1/42 KiB	IPv4 *	LAN subnets	*	*	*	*	none	
✓ 0/0 B	IPv6 *	LAN subnets	*	*	*	*	none	

Buttons: Add, Add, Delete, Toggle, Copy, Save, Separator

Message: The connection has timed out. The server at 192.168.50.101 is taking too long to respond.

Buttons: Try Again, Timed Out

Wireshark Packet Capture (eth0):

No.	Time	Source	Destination	Protocol	Length	Info
98	272.448088704	192.168.1.101	192.168.50.101	Echo (ping) request	8	id=0x23d2, seq=48/12288, ttl=64 (no response found!)
99	273.471821311	192.168.1.101	192.168.50.101	Echo (ping) request	8	id=0x23d2, seq=49/12544, ttl=64 (no response found!)
100	274.495747225	192.168.1.101	192.168.50.101	Echo (ping) request	8	id=0x23d2, seq=50/12800, ttl=64 (no response found!)
101	275.519690296	192.168.1.101	192.168.50.101	Echo (ping) request	8	id=0x23d2, seq=51/13056, ttl=64 (no response found!)
102	276.544398918	192.168.1.101	192.168.50.101	Echo (ping) request	8	id=0x23d2, seq=52/13312, ttl=64 (no response found!)
103	277.567820371	192.168.1.101	192.168.50.101	Echo (ping) request	8	id=0x23d2, seq=53/13568, ttl=64 (no response found!)
104	278.592050152	192.168.1.101	192.168.50.101	Echo (ping) request	8	id=0x23d2, seq=54/13824, ttl=64 (no response found!)
105	279.616412652	192.168.1.101	192.168.50.101	Echo (ping) request	8	id=0x23d2, seq=55/14080, ttl=64 (no response found!)

Wireshark Details:

- Frame 105: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface eth0, id 0
- Ethernet II, Src: PCSSystemtec_ad:25:87 (08:00:27:ad:25:87), Dst: PCSSystemtec_6b:f4:63 (08:00:27:6b:f4:63)
- Internet Protocol Version 4, Src: 192.168.1.101, Dst: 192.168.50.101
- Internet Control Message Protocol

Status: Packets: 105 · Displayed: 105 (100.0%) · Dropped: 0 (0.0%) · Profile: Default


4. Sblocco comunicazione tra client e server

Kali Linux

Metasploitable2 - Linux

192.168.50.101

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB



Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started

- [TWiki](#)
- [phpMyAdmin](#)
- [Mutillidae](#)
- [DVWA](#)
- [WebDAV](#)

pfSense.home.arpa - Firewall

192.168.50.254/firewall_rules.php?if=lan

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB

The changes have been applied successfully. The firewall rules are now reloading in the background.
Monitor the filter reload progress.

Floating WAN LAN OPT1

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule
<input checked="" type="checkbox"/>	✓	0/6 KiB	*	*	*	LAN Address	80	*	*
<input type="checkbox"/>	✓	1/2 KiB	IPv4 *	LAN subnets	*	*	*	*	none
<input type="checkbox"/>	✓	0/0 B	IPv6 *	LAN subnets	*	*	*	*	none

kali@kali: ~/Desktop

File Actions Edit View Help

```

64 bytes from 192.168.50.254: icmp_seq=16 ttl=64 time=0.314 ms
^C
— 192.168.50.254 ping statistics —
16 packets transmitted, 16 received, 0% packet loss, time 15351ms
rtt min/avg/max/mdev = 0.186/0.251/0.412/0.068 ms

(kali@kali)-[~/Desktop]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.1.101 netmask 255.255.255.0 broadcast 192.168.1.255
    inet6 fe80::40a6:8c57:c120:772d prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:ad:25:87 txqueuelen 1000 (Ethernet)
    RX packets 626 bytes 413888 (404.1 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 499 bytes 85607 (83.6 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 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 8 bytes 480 (480.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 8 bytes 480 (480.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

(kali@kali)-[~/Desktop]
$

```

5. Conclusioni e ringraziamenti

in conclusione, raccomandiamo vivamente l'utilizzo di PfSense all'azienda Theta che ha come obiettivo quello di rafforzare la propria infrastruttura di rete, ottimizzando al contempo la sicurezza e la gestione del traffico. Con la sua affidabilità e la capacità di affrontare sfide di sicurezza in continua evoluzione, PfSense rappresenta un investimento strategico per la protezione delle reti aziendali.

Ci teniamo a rinnovare i nostri ringraziamenti all'azienda Theta per averci dato l'opportunità di lavorare con loro.

Cordialmente,
NexusMind Group