

Laboratorio 13/12/2024 S3-L5

CREAZIONE POLICY PFSENSE

Nel laboratorio odierno andiamo a creare una regola Firewall utilizzando il tool PFSENSE:

Procediamo dunque con la creazione della regola sul tool PFsense ma prima lanciamo su Virtual Box le macchine:

- Kali Linux
- Metaspitable2
- PFsense

Una volta attivate apriamo PFsense dal browser di Kali ed inseriamo utente e password per accedervi.

The screenshot displays the pfSense Community Edition web interface. At the top, a navigation bar includes links for System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, and Help. A warning message states: "WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager." Below this, the "Status / Dashboard" page is shown. It features two main panels: "System Information" and "Netgate Services And Support".

System Information

Name	pfSense.home.arpa
User	admin@192.168.2.5 (Local Database)
System	VirtualBox Virtual Machine Netgate Device ID: a80f84b38dd64458cbf0
BIOS	Vendor: innotek GmbH Version: VirtualBox Release Date: Fri Dec 1 2006
Version	2.7.2-RELEASE (amd64) built on Wed Dec 6 20:10:00 UTC 2023 FreeBSD 14.0-CURRENT Obtaining update status
CPU Type	Intel(R) Core(TM) i5-10210U CPU @ 1.60GHz 2 CPUs: 1 package(s) x 2 cache groups x 1 core(s) AES-NI CPU Crypto: Yes (inactive) QAT Crypto: No
Hardware crypto	Inactive
Kernel PTI	Disabled
MDS Mitigation	Inactive
Uptime	03 Hours 38 Minutes 25 Seconds
Current date/time	Fri Dec 13 14:29:54 UTC 2024

Netgate Services And Support

Contract type: Community Support
Community Support Only

NETGATE AND pfSense COMMUNITY SUPPORT RESOURCES

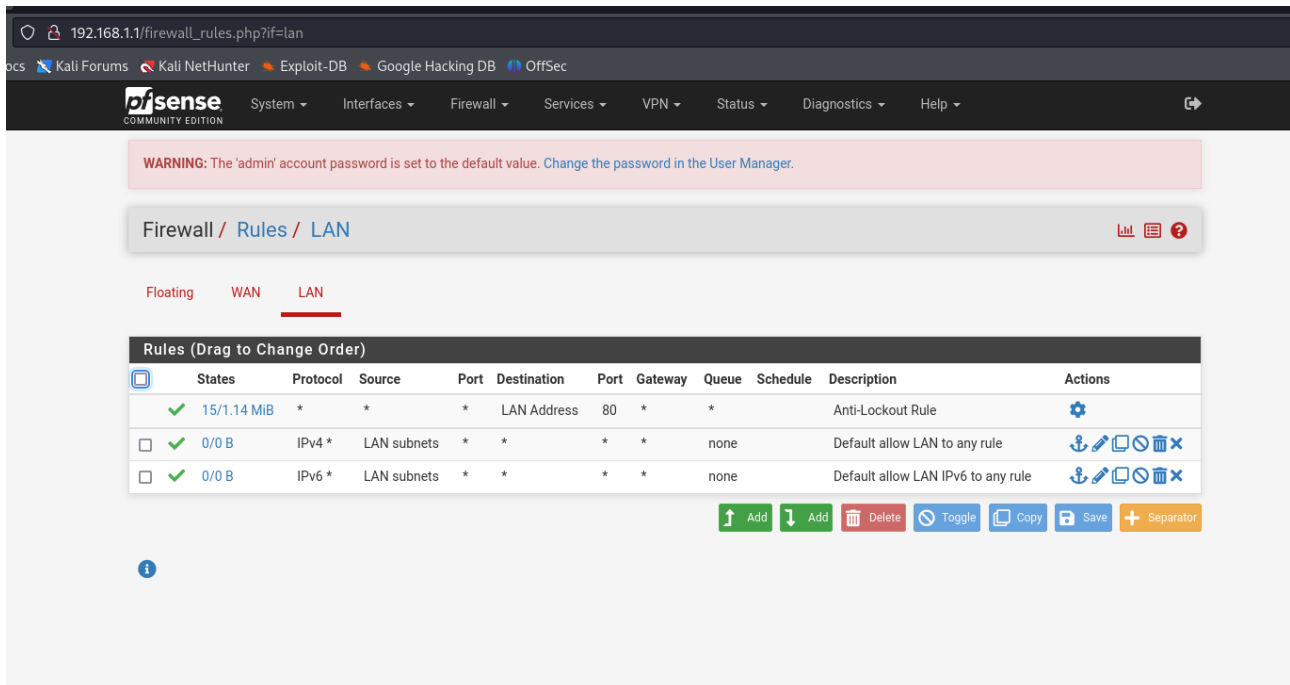
If you purchased your pfSense gateway firewall appliance from Netgate and elected **Community Support** at the point of sale or installed pfSense on your own hardware, you have access to various community support resources. This includes the [NETGATE RESOURCE LIBRARY](#).

You also may upgrade to a Netgate Global Technical Assistance Center (TAC) Support subscription. We're always on! Our team is staffed 24x7x365 and committed to delivering enterprise-class, worldwide support at a price point that is more than competitive when compared to others in our space.

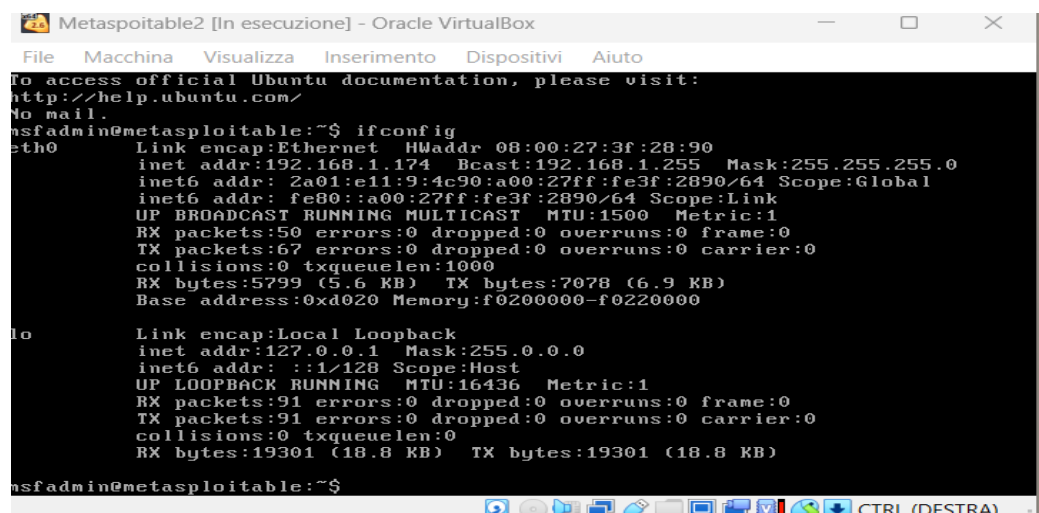
- [Upgrade Your Support](#)
- [Community Support Resources](#)
- [Netgate Global Support FAQ](#)
- [Official pfSense Training by Netgate](#)
- [Netgate Professional Services](#)
- [Visit Netgate.com](#)

If you decide to purchase a Netgate Global TAC Support subscription, you **MUST** have your **Netgate Device ID (NDI)** from your firewall in order to validate support for this unit. Write down your NDI and store it in a safe place. You can purchase TAC supports [here](#).

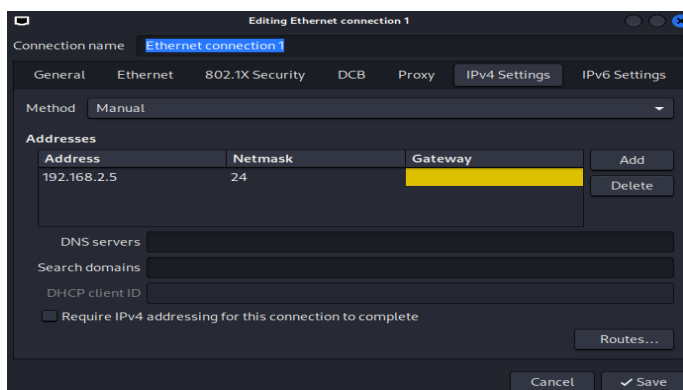
Per creare la regola Firewall selezioniamo dal menù la voce Firewall e dal menù a tendina il comando “Rules”



Clicchiamo su “add” ed iniziamo ad impostare la nostra regola, per farlo però dobbiamo conoscere gli indirizzi IP da inserire considerando che un requisito fondamentale dell’esercizio è che le macchine Kali e Metasploitable Controlliamo l’indirizzo di Metasploitable con il comando ifconfig:



Andiamo quindi prima ad impostare gli indirizzi IP delle nostre macchine Kali e PfSense.



Come si vede da queste due immagini a queste due macchine assegneremo due indirizzi IP con la stessa rete mentre su Metasploitable2 lasceremo l'indirizzo IP originario:

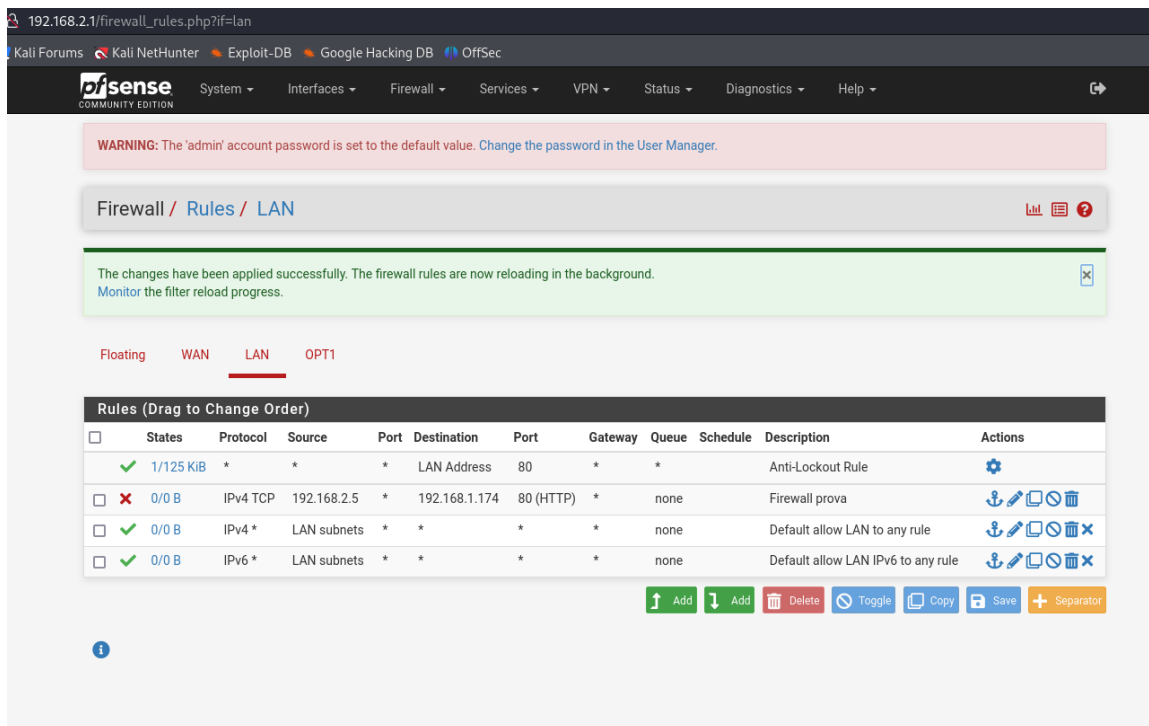
- Kali: 192.168.2.5
- PfSense: 192.168.2.1
- Metasploitable2: 192.168.1.174

Adesso riapriamo PFsense dal browser Kali e lanciamolo utilizzando il nuovo indirizzo IP.

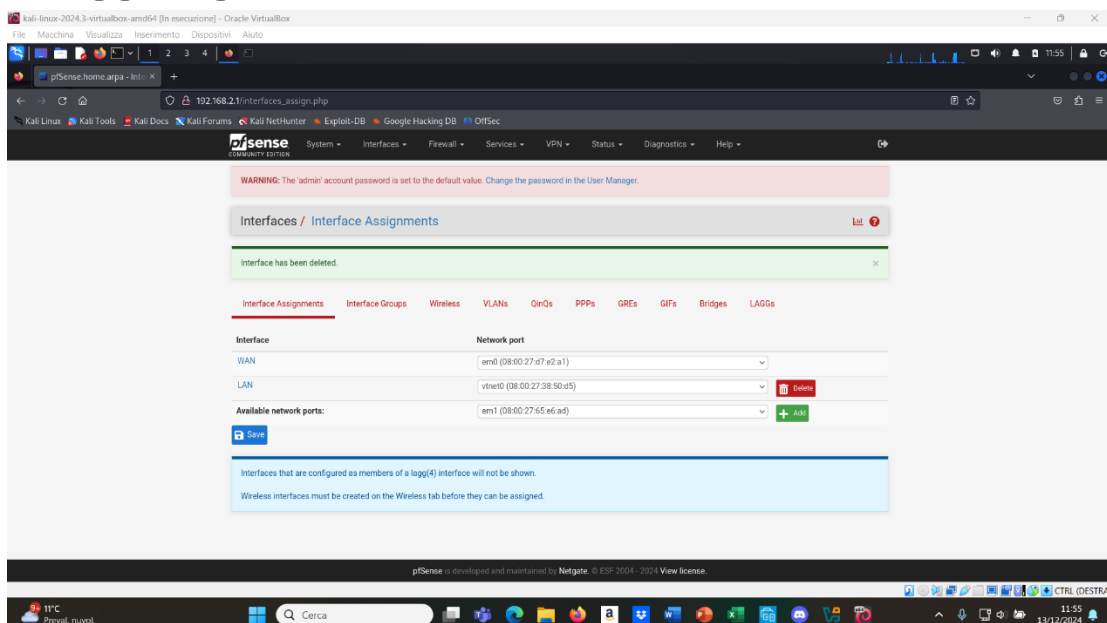
Ora possiamo impostare la nostra regola Firewall.

Action	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	<input type="checkbox"/> 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	<input type="checkbox"/> Invert match	Address or Alias	192.168.2.5 /
<div>⚙ Display Advanced</div> <p>The Source Port Range for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, any.</p>			
Destination			
Destination	<input type="checkbox"/> Invert match	Address or Alias	192.168.1.174 /
Destination Port Range	HTTP (80)	Custom	HTTP (80) Custom
	From	To	
Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.			
Extra Options			

Impostiamo in source l' indirizzo di Kali e in Destination quello di Metasploitable2, aggiungendo come porta di destinazione HTTP (80). Ora salviamo ed avremo configurato la nostra nuova regola Firewall:



A questo punto possiamo aggiungere una nuova interfaccia di rete a Pfsense in modo tale da gestire una ulteriore rete. Per farlo dobbiamo assegnare una terza scheda di rete a PFsense dalle impostazioni di rete della macchina virtuale e successivamente avremo la possibilità di aggiungerla.



Per farlo selezioniamo “+add” e abilitiamo l’ interfaccia nelle configurazioni generali:

The screenshot shows a web browser window with the URL `192.168.2.1/interfaces.php?if=opt1`. The browser's address bar and tabs are visible at the top. A green notification bar at the top of the page states "The changes have been applied successfully." Below this, the "General Configuration" section is displayed. It includes a "Description" field with the value "OPT1", "IPv4 Configuration Type" set to "Static IPv4", "IPv6 Configuration Type" set to "None", a "MAC Address" field with a placeholder "xxxxxxxxxxxx", "MTU" and "MSS" fields with dropdown arrows, and a "Speed and Duplex" field set to "Default (no preference, typically autoselect)". Below the general configuration is the "Static IPv4 Configuration" section, which shows the "IPv4 Address" as "192.168.1.174" and the "IPv4 Upstream gateway" as "None". A green button labeled "+ Add a new gateway" is located next to the gateway field. At the bottom of the static IPv4 configuration, a note states: "If this interface is an Internet connection, select an existing Gateway from the list or add a new one using the 'Add' button."

Ora che abbiamo finito di creare la regola Firewall e configurato la nuova interfaccia ci dobbiamo assicurare che il Firewall blocchi le comunicazioni tra gli indirizzi IP impostati.

Per farlo utilizziamo il comando ping sia dal terminale di Kali Linux che da quello di Metasploitable2 che infatti ci restituiranno le seguenti risposte:

Questo è il ping e lo scan da Kali a Metasploitable2:

```
(kali@kali)-[~]
$ ping 192.168.1.174
ping: connect: Network is unreachable

(kali@kali)-[~]
$ ping 192.168.1.174
ping: connect: Network is unreachable

(kali@kali)-[~]
$ nmap -v -A -sV 192.168.1.174
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-13 06:23 EST
NSE: Loaded 156 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 06:23
Completed NSE at 06:23, 0.00s elapsed
Initiating NSE at 06:23
Completed NSE at 06:23, 0.00s elapsed
Initiating NSE at 06:23
Completed NSE at 06:23, 0.00s elapsed
Initiating Ping Scan at 06:23
Scanning 192.168.1.174 [2 ports]
Completed Ping Scan at 06:23, 0.00s elapsed (1 total hosts)
Nmap scan report for 192.168.1.174 [host down]
NSE: Script Post-scanning.
Initiating NSE at 06:23
Completed NSE at 06:23, 0.00s elapsed
Initiating NSE at 06:23
Completed NSE at 06:23, 0.00s elapsed
Initiating NSE at 06:23
Completed NSE at 06:23, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 0.30 seconds

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

Questo è il ping inverso:

```
Metasploitable2 [In esecuzione] - Oracle VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto

inet6 addr: 2a01:e11:9:4c90:a00:27ff:fe3f:2890/64 Scope:Global
inet6 addr: fe80::a00:27ff:fe3f:2890/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:46 errors:0 dropped:0 overruns:0 frame:0
TX packets:67 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:5525 (5.3 KB) TX bytes:7070 (6.9 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:91 errors:0 dropped:0 overruns:0 frame:0
TX packets:91 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:19301 (18.8 KB) TX bytes:19301 (18.8 KB)

msfadmin@metasploitable:~$ ping 192.168.2.5
PING 192.168.2.5 (192.168.2.5) 56(84) bytes of data.
From 192.168.1.254 icmp_seq=1 Destination Host Unreachable
From 192.168.1.254 icmp_seq=2 Destination Host Unreachable
From 192.168.1.254 icmp_seq=3 Destination Host Unreachable
From 192.168.1.254 icmp_seq=4 Destination Host Unreachable
```

BONUS:

Impostare una regola su PfSense per bloccare da Kali il telnet verso Metasploitable.

Prendendo come riferimento quanto già fatto prima impostiamo anche una regola Firewall per bloccare il telnet (selezioneremo quindi la porta 23) da Kali verso Metasploitable.

192.168.2.1/firewall_rules_edit.php?id=1

Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

Action 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 192.168.2.5 /

The **Source Port Range** for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, **any**.

Destination

Destination ☐ Invert match Address or Alias 192.168.1.174 /

Destination Port Range Telnet (23) Custom Custom
From Custom To Custom
Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.

Extra Options

