



Open Source Security

Secure networks start here.™ With thousands of enterprises using pfSense® software, it is rapidly becoming the world's most trusted open source network security solution.

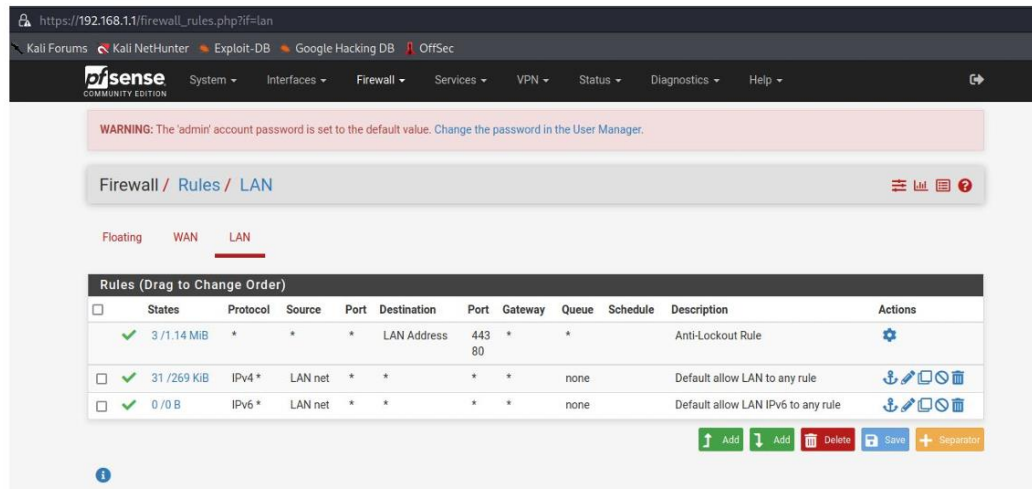
Sommario

Traccia esercizio.....	2
Traccia esercizio facoltativo	4
Requisiti.....	5
Premessa: cos'è pfSense.....	5
Installazione di pfSense	6
Collegamento tra pfSense, Kali Linux ed eventuali altre VM	10
Svolgimento della traccia principale	12
Impostare le VM in DHCP	12
Verifica connessione con DVWA (Metasploitable2).....	12
Creazione regola su pfSense per bloccare l'accesso a DVWA.....	13
La regola di blocco non funziona nella stessa rete.....	14
Configurazione in reti diverse	14
Test regola di firewall.....	17
Svolgimento esercizio facoltativo	18
Analisi dei log	18
Troubleshooting delle regole firewall	18

Traccia esercizio

Creazione pratica di una regola Firewall

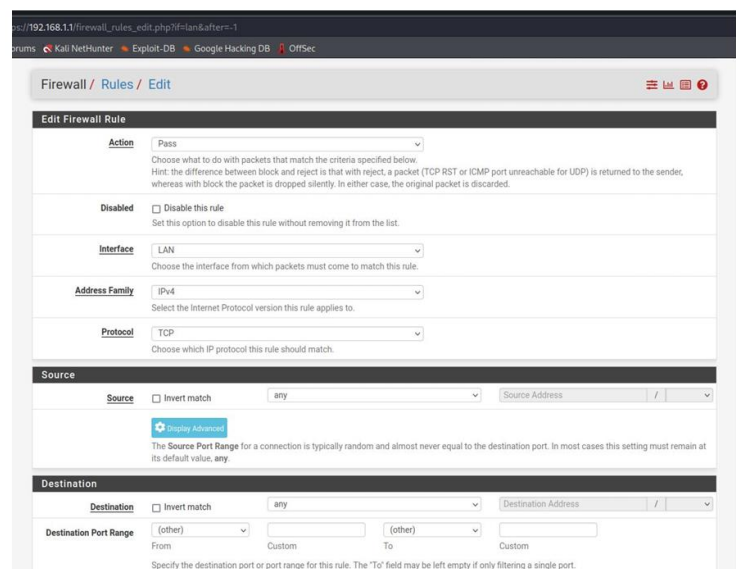
Per la creazione di una regola firewall, andare su **Firewall > Rules**. In questa sezione si può scegliere su quale interfaccia creare la regola: scegliamo LAN e clicchiamo su **Add** (come vedete ci sono 2 Add, il primo crea la regola in cima al policy set, la seconda in basso)



Cliccando su Add, possiamo aggiungere:

Informazioni generiche:

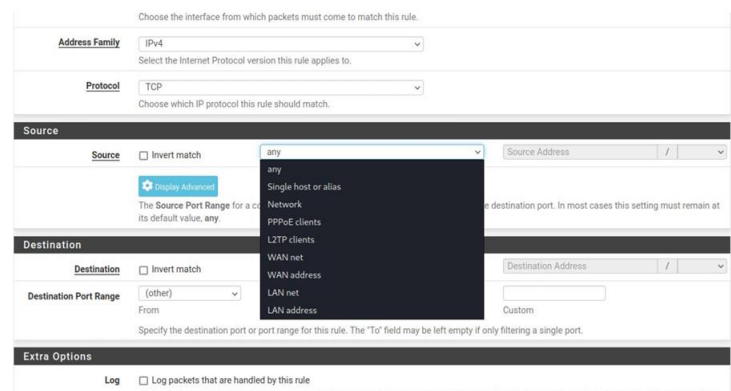
- ❑ **Action:** in questa sezione si può scegliere come gestire il traffico analizzato
- ❑ **Interface:** l'interfaccia da dove arrivano i pacchetti (es. LAN)
- ❑ **Address family:** IPv4 oppure IPv6, si sceglie la versione di protocolli IP ai quali applicare la policy
- ❑ **Protocol:** si sceglie il protocollo (es., TCP, UDP, ICMP)



Cliccando su Add, possiamo aggiungere:

Informazioni sulla sorgente:

- ❑ **Source:** in questa sezione si può scegliere che tipo di sorgente si andrà ad inserire, come un singolo IP, oppure una rete intera. Nel campo valorizzato con «source address» si andranno ad inserire eventualmente gli indirizzi IP o indirizzi rete in notazione CIDR.



Cliccando su Add, possiamo aggiungere:

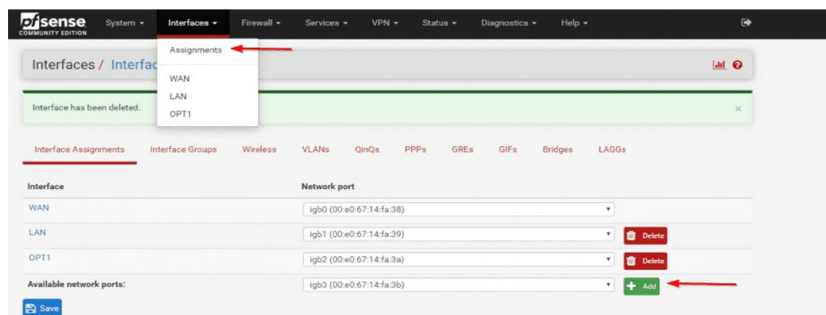
Informazioni sulla destinazione:

- **Destination:** in questa sezione si può scegliere che tipo di sorgente si andrà ad inserire, come un singolo IP, oppure una rete intera. Nel campo valorizzato con «source address» si andranno ad inserire eventualmente gli indirizzi IP o indirizzi rete in notazione CIDR.
- **Destination port range:** in questa sezione si specificano le porte destinazione. Si possono specificare: singole porte, intervalli, aliases (oggetti di porte custom)

The screenshot shows the 'Destination' tab of a pfSense Firewall Rule configuration. At the top, a note states: '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.' The 'Destination' section includes a 'Destination' dropdown set to 'any', an 'Invert match' checkbox, and a 'Destination Address' field with a slash separator. Below this is the 'Destination Port Range' section, with 'From' and 'To' dropdowns both set to '(other)', and 'Custom' checkboxes. A note below the port range section says: 'Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.' The 'Extra Options' section at the bottom has a 'Log' checkbox which is unchecked, with a hint: 'Log packets that are handled by this rule. Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the Status: System Logs: Settings page)'.

Sulla base di quanto visto, creare una regola firewall che **blocchi** l'accesso alla DVWA (su metasploitable) dalla macchina Kali Linux e ne impedisca di conseguenza lo scan (fare uno screenshot che dimostri che prima lo scan per DVWA funzionava e ora non funziona più). Un requisito fondamentale dell'esercizio è che le macchine Kali e Metasploitable siano su reti **diverse**, potete aggiungere una nuova interfaccia di rete a Pfsense in modo tale da gestire una ulteriore rete.

Connettetevi poi in Web GUI per attivare la nuova interfaccia e configurarla.



https://192.168.1.1/interfaces.php?if=opt1

Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

Interfaces / LAN2 (em2)

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: xxxxxxxxxx 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 /

IPv4 Upstream gateway [+ Add a new gateway](#)
If this interface is an Internet connection, select an existing Gateway from the list or add a new one using the "Add" button.
On local area network interfaces the upstream gateway should be "none".
Selecting an upstream gateway causes the firewall to treat this interface as a WAN type interface.

Traccia esercizio facoltativo

- Ispezionare i log del Firewall
<https://docs.netgate.com/pfsense/en/latest/monitoring/logs/firewall.html>
- Fare pratica con la procedura di troubleshooting delle regole firewall
<https://docs.netgate.com/pfsense/en/latest/troubleshooting/firewall.html>

Requisiti

Premessa: cos'è pfSense

pfSense è un sistema operativo basato su FreeBSD progettato per essere utilizzato come firewall e router. È una soluzione open source e offre una vasta gamma di funzionalità per la gestione della rete. Ecco alcune delle sue caratteristiche principali:

1. **Firewall e Router:** pfSense è principalmente usato per proteggere le reti gestendo il traffico in entrata e in uscita, configurando regole di filtraggio avanzate.
2. **Interfaccia web:** La configurazione e la gestione di pfSense avviene tramite un'interfaccia web intuitiva, rendendolo accessibile anche a utenti non esperti.
3. **VPN (Virtual Private Network):** pfSense supporta diversi tipi di VPN come IPsec, OpenVPN e PPTP, consentendo la connessione sicura tra reti remote.
4. **Traffic Shaping:** Offre funzionalità di "traffic shaping", che permette di prioritizzare determinati tipi di traffico, ad esempio limitando la banda per il download e assicurando che le applicazioni critiche abbiano una connettività ottimale.
5. **Monitoraggio e reportistica:** pfSense fornisce strumenti di monitoraggio del traffico e può generare report dettagliati per analizzare l'attività della rete.
6. **Gestione degli accessi:** Può essere configurato per gestire l'accesso a internet per gli utenti della rete, con funzioni come il blocco di siti specifici o la limitazione della larghezza di banda.
7. **Ridondanza e Failover:** Supporta funzionalità avanzate come la ridondanza e il failover per garantire l'affidabilità e la continuità del servizio.

In sintesi, pfSense è un sistema versatile, utilizzato in contesti aziendali e domestici per la gestione di firewall e rete con elevate prestazioni e flessibilità.

La licenza FreeBSD consente di modificare e utilizzare il codice in progetti chiusi o commerciali, richiedendo solo di dare credito agli autori originali.

Ai fini del corso, pfSense sarà utilizzato e configurato nel laboratorio virtuale, quindi installato come sistema operativo, nel presente report, con VirtualBox.

Per una migliore comprensione, il ruolo di pfSense in questo laboratorio virtuale può essere paragonato, per analogia, a quello di un modem/router in una rete domestica, svolgendo funzioni di firewall e gestione del traffico tra le macchine collegate alla rete.

Installazione di pfSense

Scaricare l'immagine .ISO scegliendo la versione per Virtual Machine dal sito ufficiale <https://www.pfsense.org/download/> e seguire le istruzioni per il download.

Download

Home | Download

Latest Stable Version

pfSense Plus & pfSense CE software downloads are available for installation via the Netgate Installer. Click the "Download" link below to redirect to our online store and download the Netgate Installer package. Refer to the documentation for [Upgrade Guides](#) and [Installation Guides](#). For pre-configured systems, see the [pfSense® firewall appliances from Netgate](#).

RELEASE NOTES

SOURCE CODE

Version: 2.7.2

DOWNLOAD

Supported by



Subscribe To The Netgate Newsletter

Product information, pfSense software announcements, and special offers. See our [newsletter archive](#) for past announcements.

Email*

Email Address

☐ I understand I am signing up to receive the newsletter, software announcements, and special offers from Netgate *

NETGATE INSTALLER

\$0⁰⁰

Shipping calculated at checkout.

Pay in 4 interest-free installments for orders over \$50.00 with [shop pay](#). [Learn more](#)
Customers using Shop Pay installments might experience a 1-2 day delay in order processing.

Installation Image

AMD64 ISO IPMI/Virtual Mach

SELECT IMAGE TYPE

AMD64 Memstick USB (Netgate 1537, 1541, 4100, 4200, 5100, 6100, 7100, 8200, All Other Intel/AMD 64-bit)

AMD64 ISO IPMI/Virtual Machines

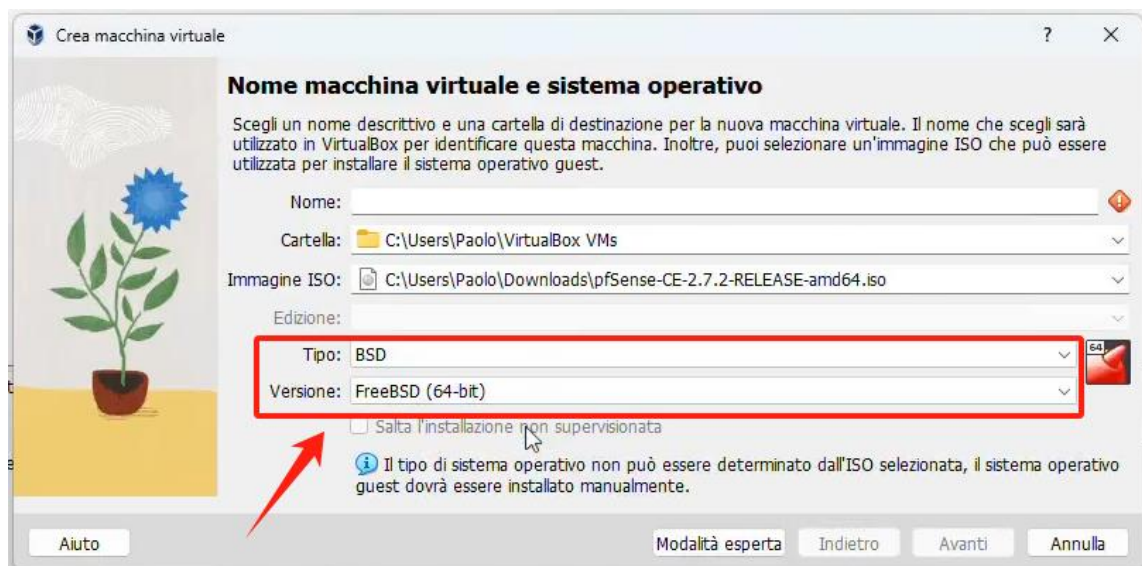
AARCH64 Memstick ARM (Netgate 1100 and 2100)

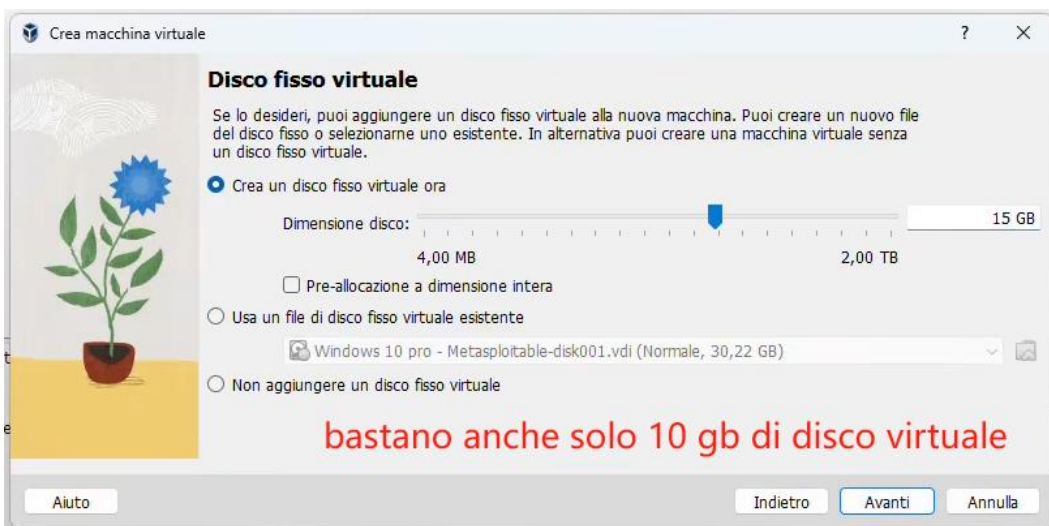
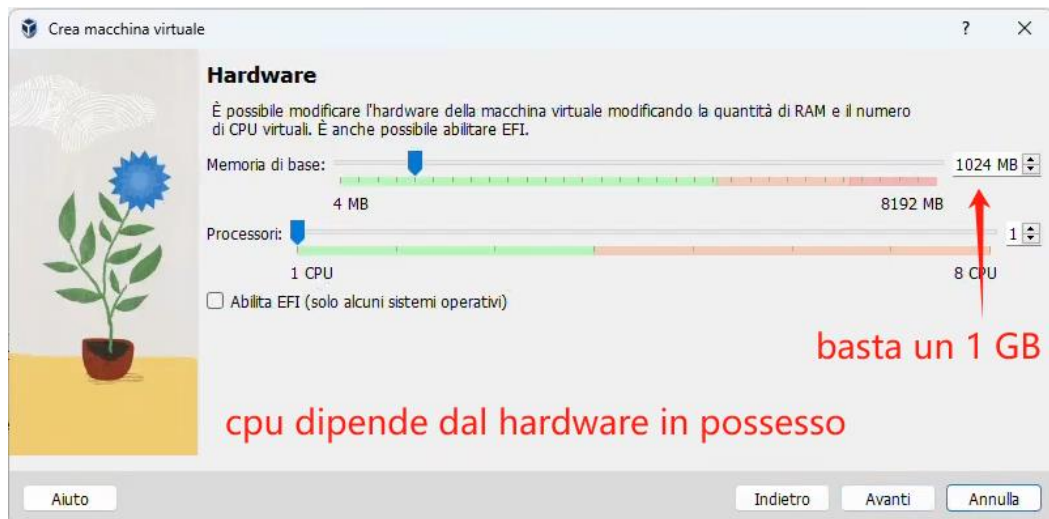
ADD TO CART

FIND A PARTNER

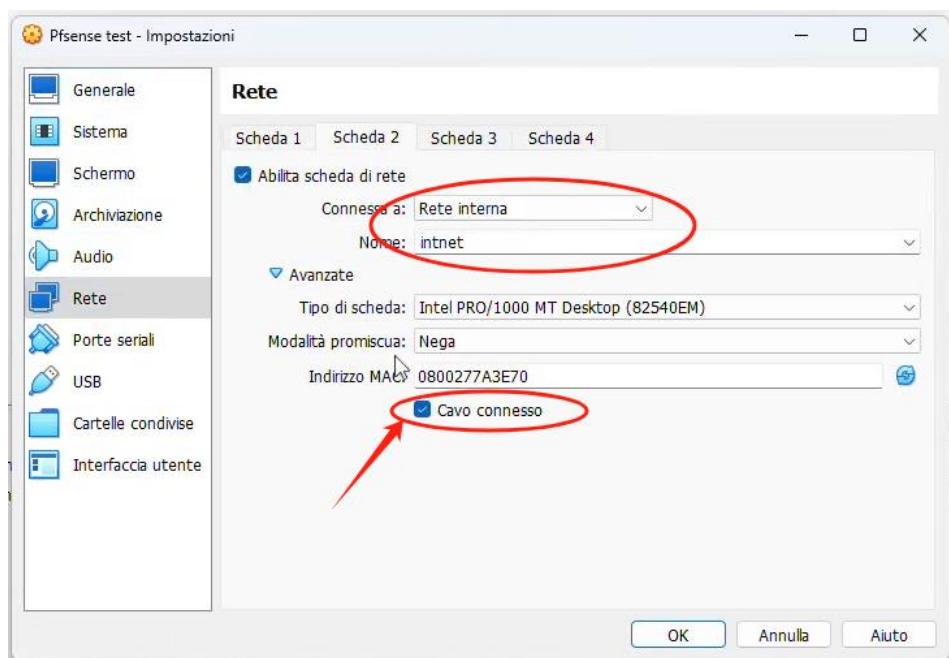


Seguire le istruzioni del report M1\W1\D3 su come installare un OS con VirtualBox con la seguente configurazione.

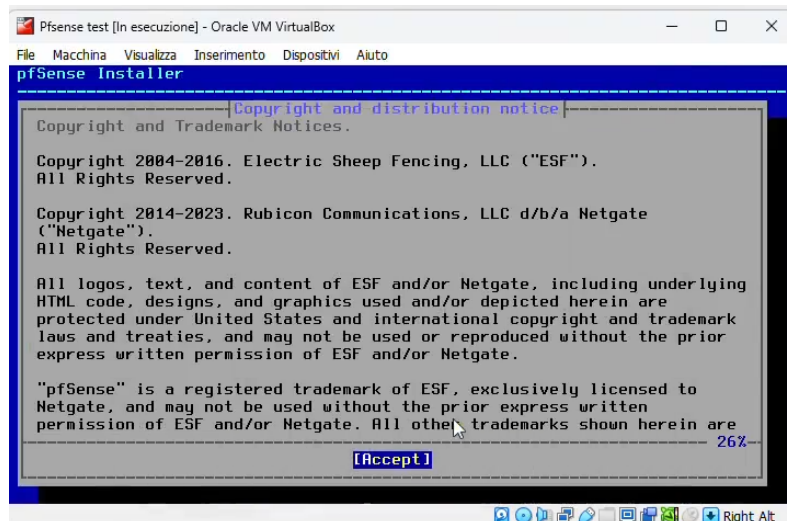




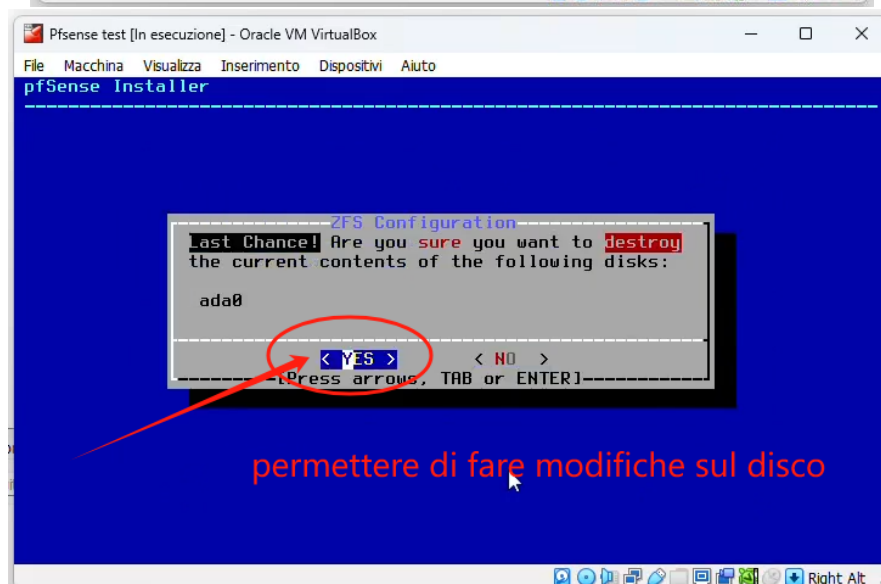
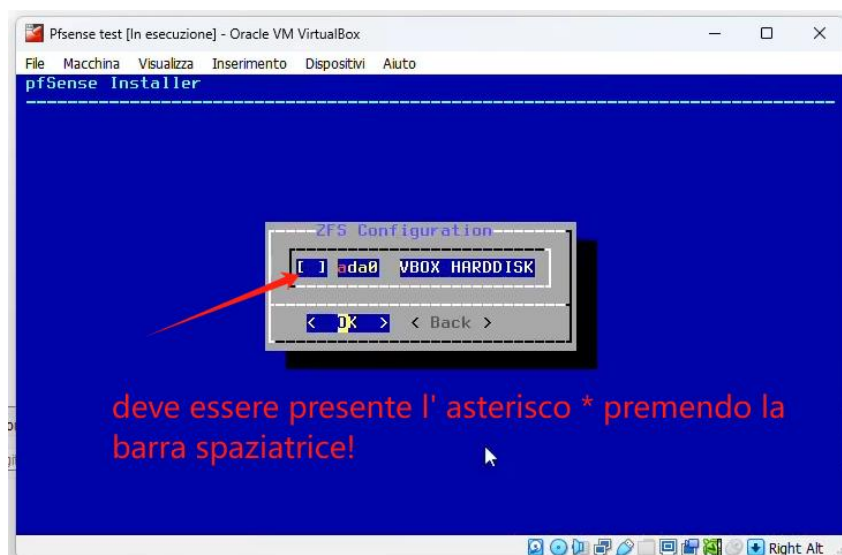
Prima di avviare la VM, molto importante è la configurazione delle schede di rete 1 e 2, abilitate, rispettivamente in **NAT** e **Rete Interna**, entrambi con **Cavo connesso**.



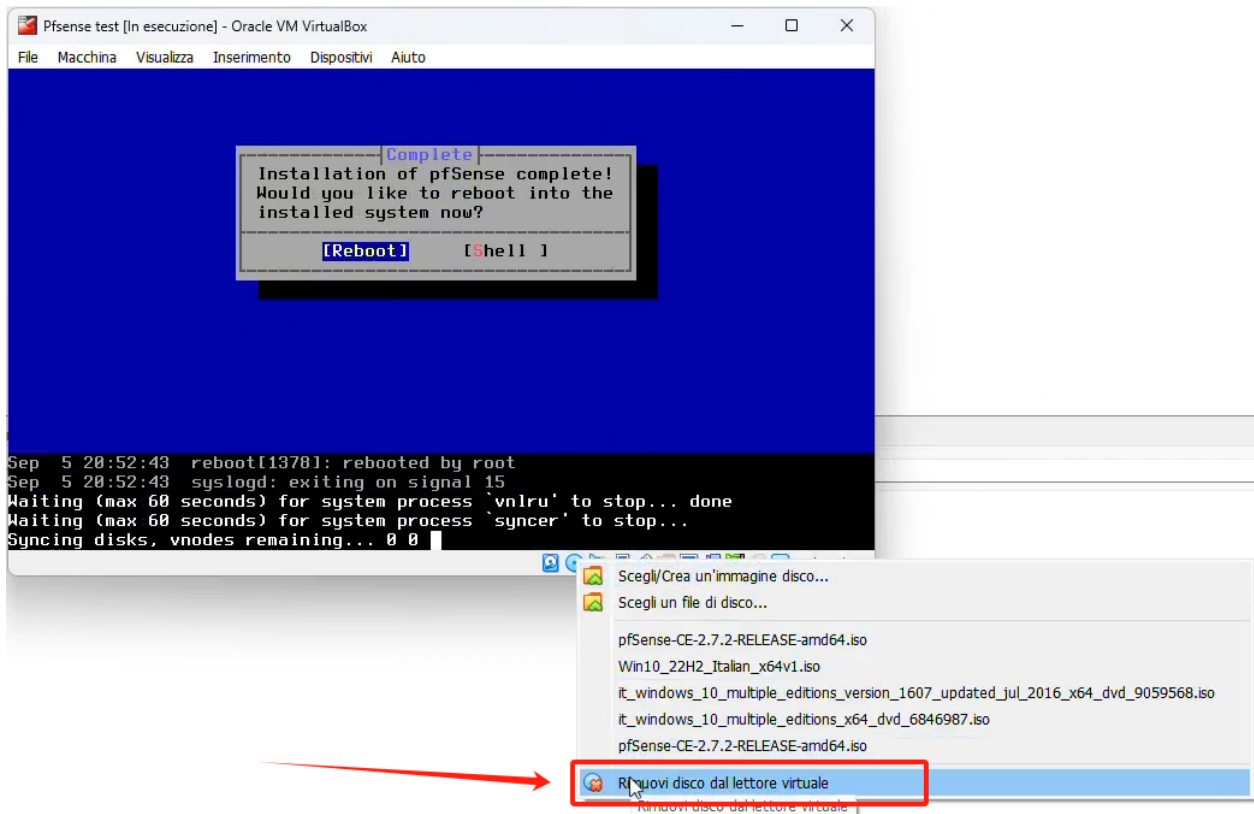
Avviare la macchina virtuale di pfSense e seguire le istruzioni intuitive per l'installazione, procedendo sempre con il tasto Invio.



Attenzione all'unico passaggio da prestare la massima attenzione per selezionare il disco e dare il permesso alla modifica dello stesso.



Alla fine del procedimento, riavviare la VM e durante il processo di riavvio, rimuovere il disco virtuale dalla VM per evitare che la macchina avvii il sistema operativo dal disco di installazione (l'ISO scaricata), invece di avviarlo dal disco virtuale.



Una volta completato l'operazione, tenere acceso pfSense.

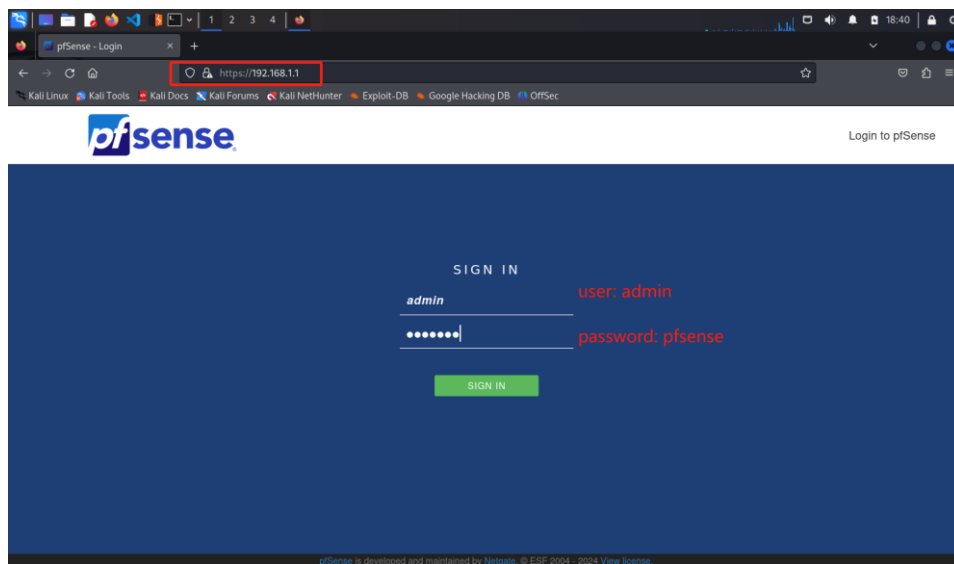
Collegamento tra pfSense, Kali Linux ed eventuali altre VM

Kali Linux deve avere la scheda di rete in rete interna con cavo connesso e deve essere in DHCP. Verificare con il comando **ip a** su terminale Kali che sia connessa correttamente alla rete di pfSense.

```
(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 08:00:27:08:c5:b4 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.100/24 brd 192.168.1.255 scope global dynamic noprefixroute eth0
        valid_lft 7110sec preferred_lft 7110sec
    inet6 fe80::aadf:3f4f:33a0:c954/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
```

In questo caso 192.168.1.100 indica perfettamente che si è connessa correttamente, pertanto per entrare nella pagina di configurazione, aprire il browser e digitare l'indirizzo di gateway, in questo caso **192.168.1.1**, bypassare eventuali avvisi di sicurezza del browser.

Credenziali di default: user **admin** password **pfSense**



Per ripristinare la password di default usare le opzioni su pfSense. In questo caso col numero 3.

```
The password for the webConfigurator has been reset and
the default username has been set to "admin".

Remember to set the password to something else than
the default as soon as you have logged into the webConfigurator.
Press ENTER to continue.
VirtualBox Virtual Machine - Netgate Device ID: 502528ff10b3808f2437

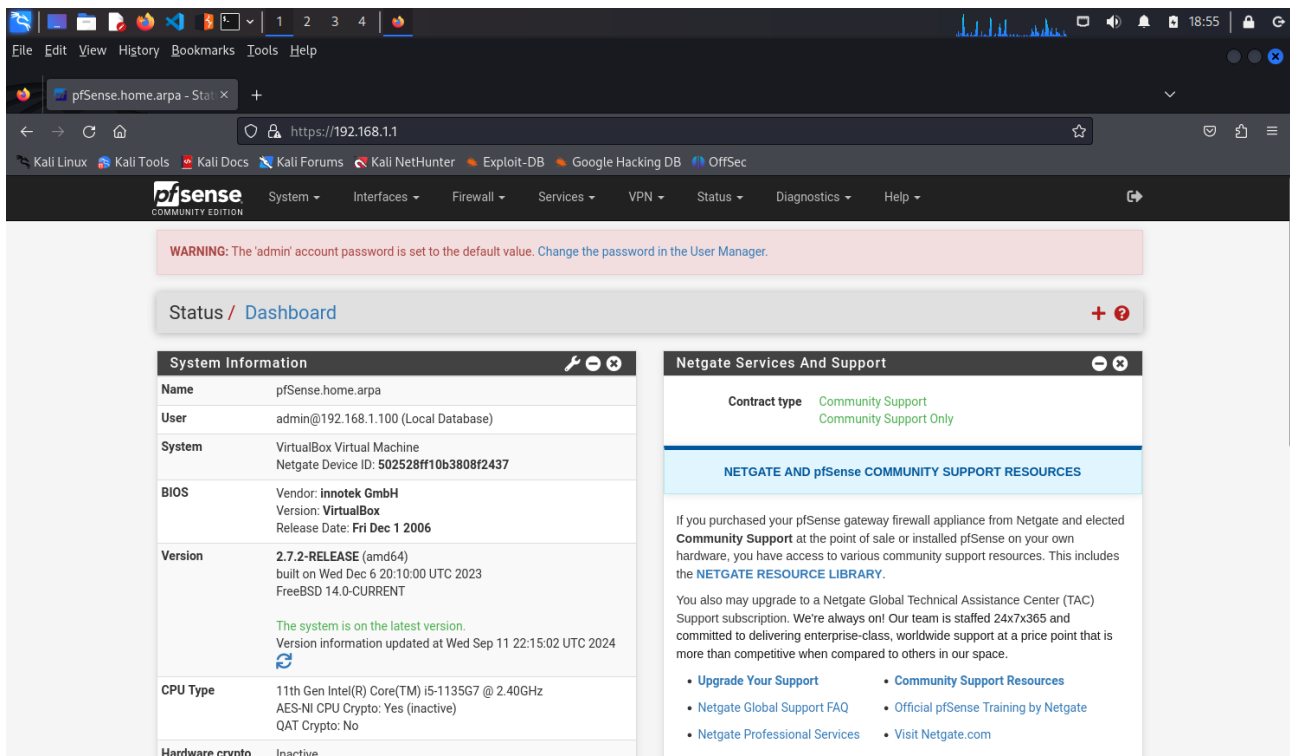
*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0      -> v4/DHCP4: 10.0.2.15/24
LAN (lan)      -> em1      -> v4: 192.168.1.1/24

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 (ssh)
6) Halt system                 15) Restore recent configuration
7) Ping host                   16) Restart PHP-FPM
8) Shell

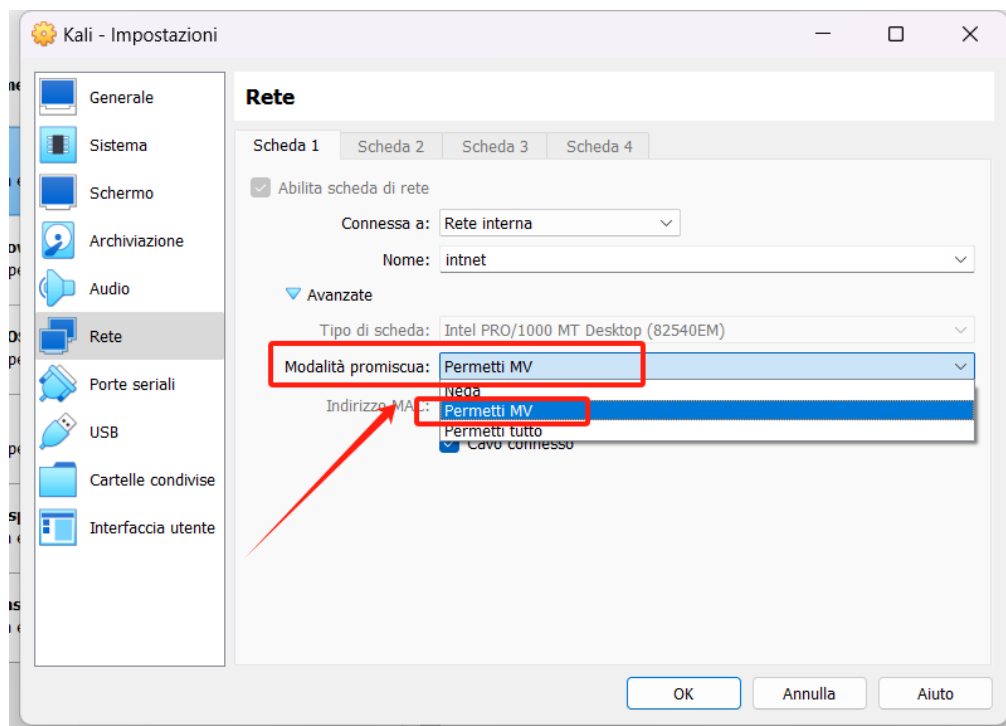
Enter an option: 3
```

Seguire passo passo la configurazione intuitiva di benvenuto.



Da questa schermata, la Dashboard si possono effettuare tutte le configurazioni e impostazioni desiderate.

Per mantenere attivo la connessione a internet, rete esterna, sulla macchina Kali Linux attivare la modalità promiscua. Questa modalità consente alla VM di vedere tutto il traffico sulla rete a cui è connessa, permettendo a pfSense di funzionare correttamente come router. **Attivarla anche su pfSense.**



La motivazione è che pfSense, nella rete del laboratorio virtuale, ha il ruolo di Server DHCP e pertanto le macchine virtuali connesse non riescono a vedere tutto il traffico di rete per configurazioni di sicurezza di default.

Svolgimento della traccia principale

Impostare le VM in DHCP

Dato che pfSense fa da server DHCP, ha il ruolo di assegnare gli indirizzi IP, pertanto è essenziale che le macchine del laboratorio virtuale siano in DHCP e rete interna. Seguire il report del M1\W1\D5 per impostare Metasploitable2 in DHCP.

```
GNU nano 2.0.7      File: /etc/network/interfaces      Modified

# 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
#address 192.168.50.101
#netmask 255.255.255.0
#network 192.168.50.0
#broadcast 192.168.50.255
#gateway 192.168.50.1

^G Get Help  ^O WriteOut  ^R Read File  ^V Prev Page  ^K Cut Text   ^C Cur Pos
^X Exit      ^J Justify   ^U Where Is   ^U Next Page  ^U UnCut Text ^T To Spell
```

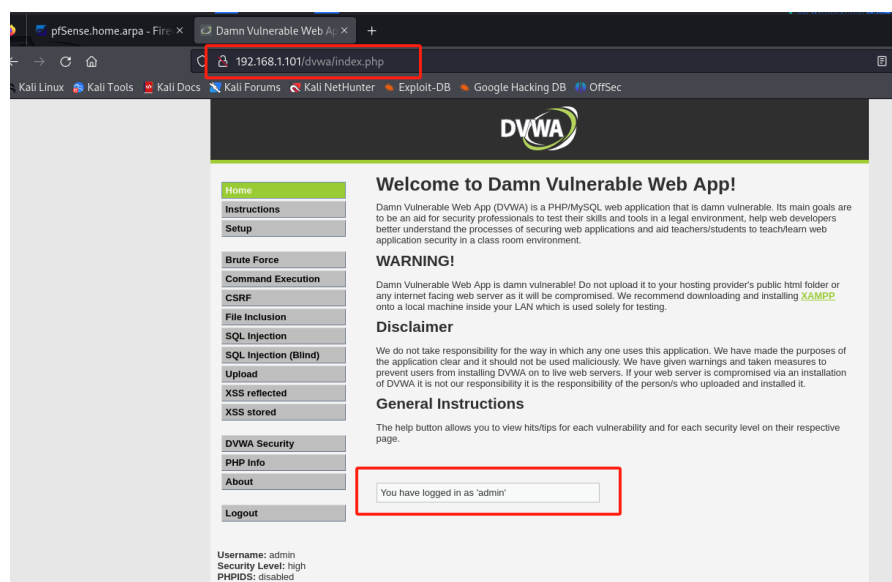
Verifica connessione con DVWA (Metasploitable2)

```
msfadmin@metasploitable:~$ ifconfig
eth0:  Link encap:Ethernet  HWaddr 08:00:27:77:37:e6
        inet addr:192.168.1.101  Bcast:192.168.1.255  Mask:255.255.255.0
        inet6 addr: fe80::a00:27ff:fe77:37e6/64 Scope:Link
        UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
        RX packets:31 errors:0 dropped:0 overruns:0 frame:0
        TX packets:56 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1000
        RX bytes:3654 (3.5 KB)  TX bytes:6178 (6.0 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:98 errors:0 dropped:0 overruns:0 frame:0
        TX packets:98 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:0
        RX bytes:21621 (21.1 KB)  TX bytes:21621 (21.1 KB)

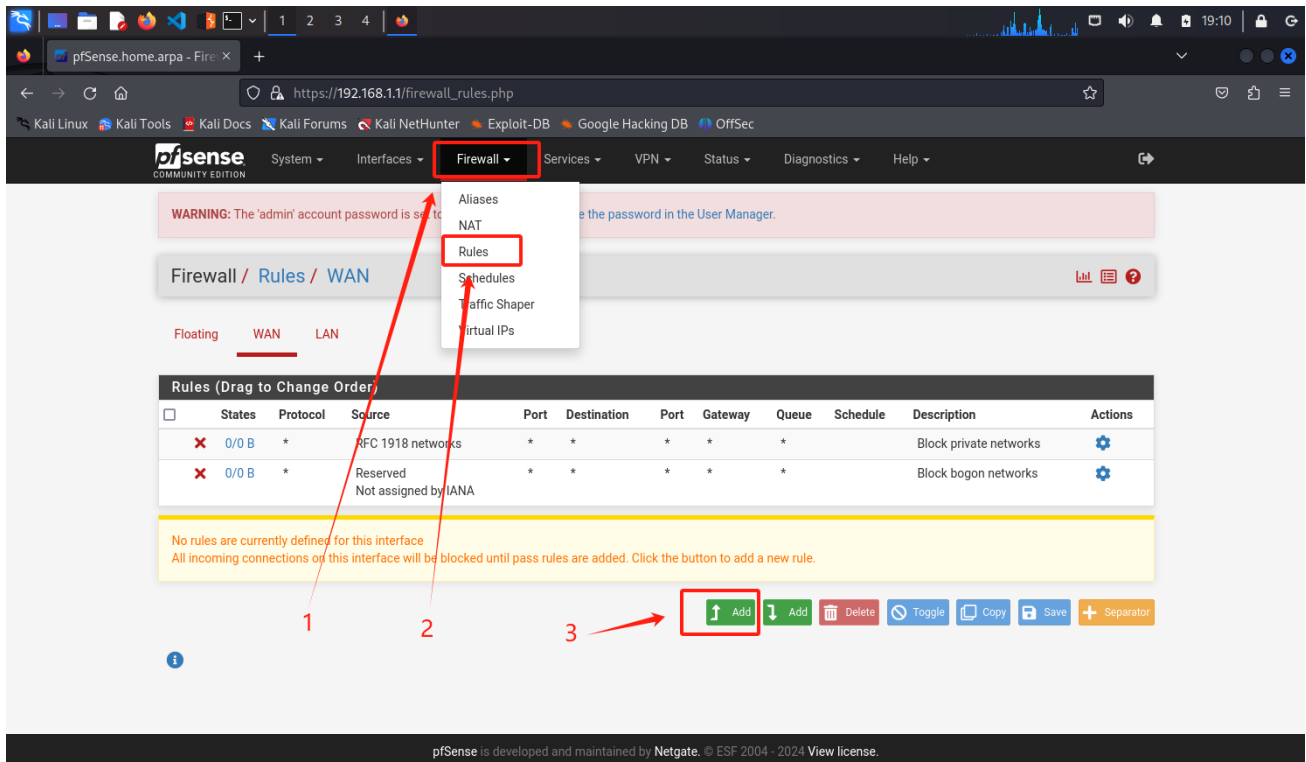
msfadmin@metasploitable:~$
```

Con il comando su Metasploitable2 **ifconfig** si ottiene l'indirizzo IP del server DVWA, in questo caso **192.168.1.101**. Pertanto tramite il browser si verifica subito la connessione al link <http://192.168.1.101/dvwa/login.php> con le credenziali **admin** e **password**.



Creazione regola su pfSense per bloccare l'accesso a DVWA

Tornare all'interfaccia di configurazione di pfSense da browser, quindi **192.168.1.1** con le credenziali note e aggiungere una nuova regola firewall come da immagine sottostante: Firewall > Rules > Add. Aggiungere una nuova regola, in questo caso è indifferente se in cima o in basso per l'ordine di priorità.



Action Block 1

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 2
Choose the interface from which packets must come to match this rule.

Address Family IPv4 3
Select the Internet Protocol version this rule applies to.

Protocol Any 4
Choose which IP protocol this rule should match.

Source

Source ☐ Invert match Address or Alias 192.168.1.100 5

Destination

Destination ☐ Invert match Address or Alias 192.168.1.100 6

Extra Options

Log ☒ Log packets that are handled by this rule 7
Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the [Status: System Logs: Settings](#) page).

Description Block_meta 8
A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.

9. salvare

1. Azione di blocco
2. Interfaccia Lan
3. Ipv4
4. Tutti i protocolli
5. L'indirizzo di origine da bloccare
6. L'indirizzo di destinazione da bloccare
7. Opzionale: i log
8. Dare una descrizione alla regola
9. Salvare la configurazione

Dopo aver configurato, nella schermata precedente, applicare i cambiamenti. p.s. in questo tentativo, si sono riavviati le macchine e pertanto il server DHCP pfSense ha assegnato 192.168.1.100 a Meta e 192.168.1.101 a Kali.

La regola di blocco non funziona nella stessa rete

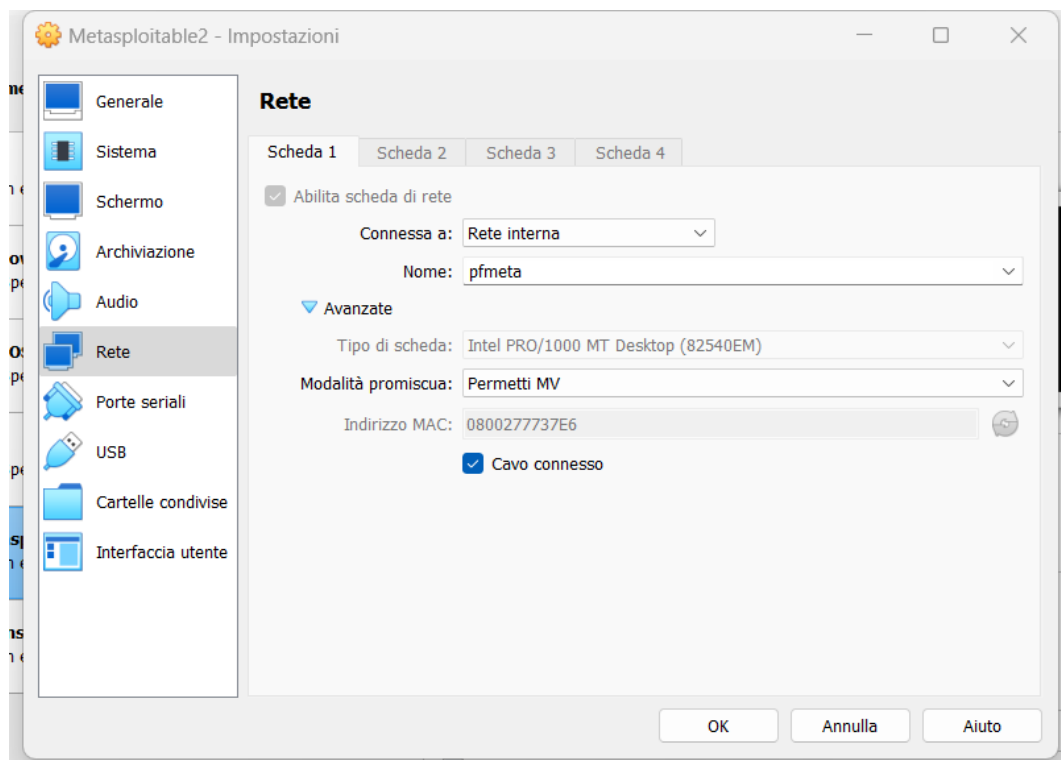
Dai test effettuati, si conclude che il blocco impostato correttamente su pfSense non funziona, né può funzionare, perché pfSense agisce come firewall tra Kali e Meta. Tuttavia, in questo caso, poiché Kali e Meta si trovano nella stessa rete interna, il loro traffico non passa attraverso il router/modem virtuale pfSense, e di conseguenza non viene filtrato da quest'ultimo.

Quindi testare il blocco correttamente e obbligare il traffico tra Meta e Kali attraverso pfSense, si può configurare con due reti diverse: Kali nel gateway 192.168.1.1 & Meta nel gateway 192.168.50.1

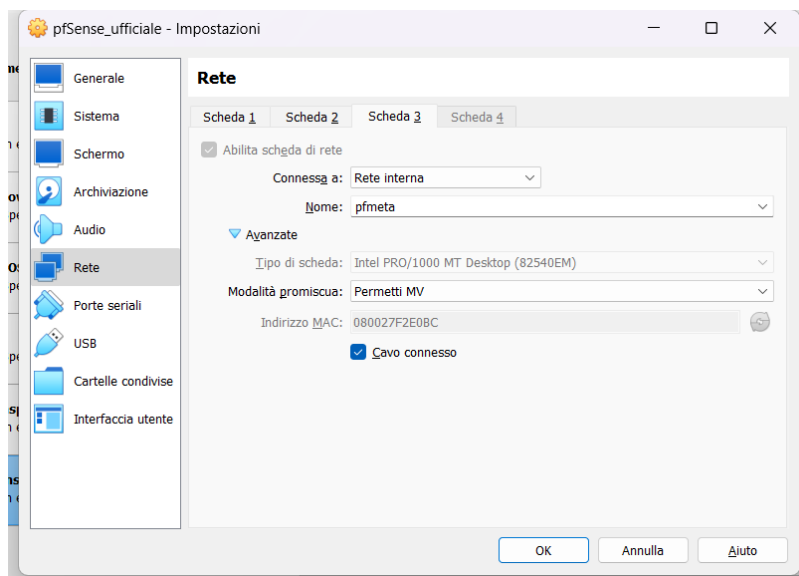
Configurazione in reti diverse

Configurare su Virtual Box, un'altra rete interna.

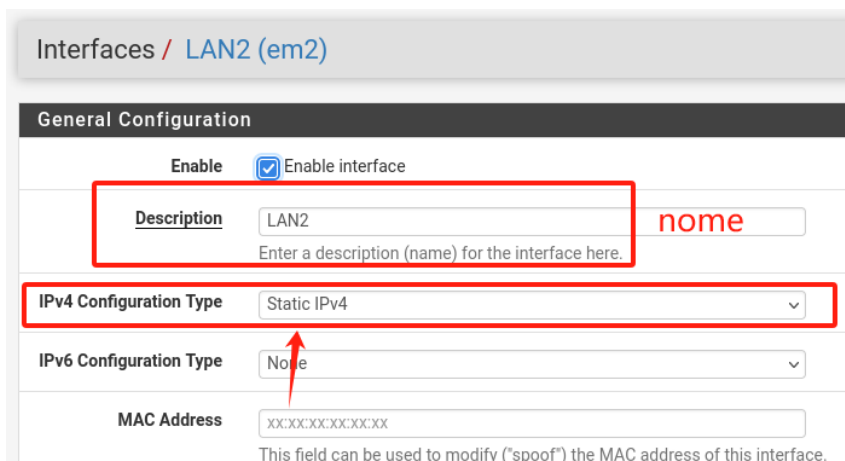
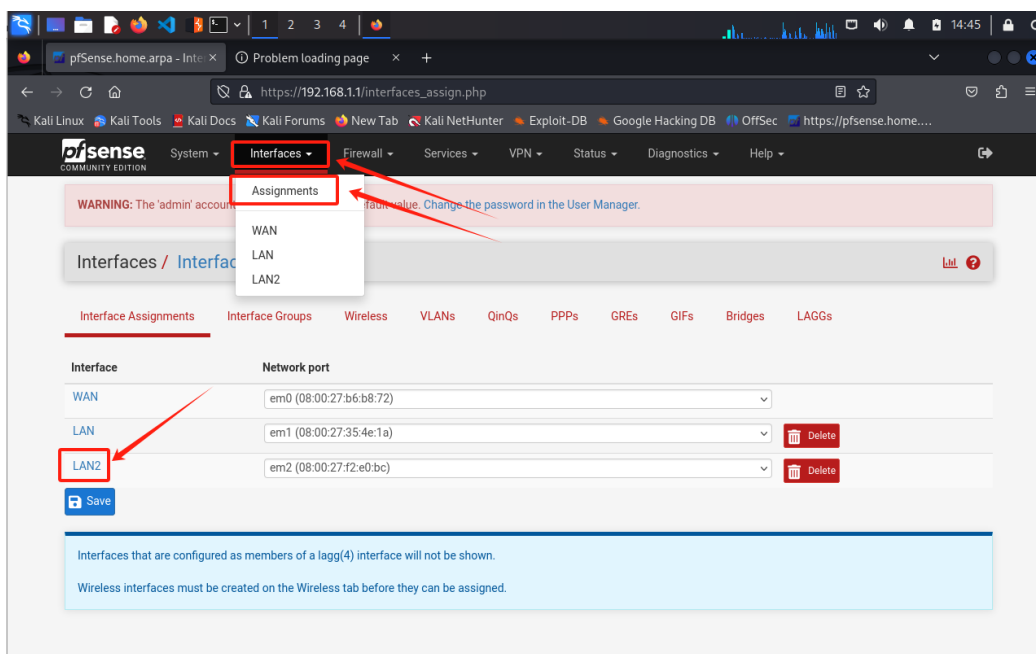
Metasploitable2 cambiare con un nome a piacere la rete interna, in questo caso **pfmeta**



Invece su pfSense aggiungere una nuova scheda di rete chiamandola con lo stesso nome di Meta.



Da Kali andare nella pagina di configurazione di pfSense andare su **Interfaces > Assignments** e cliccare su **opt1** (quest'ultimo si potrà modificarlo con un nome personalizzato, LAN2 in questo caso).



Static IPv4 Configuration

IPv4 Address: /

IPv4 Upstream gateway: [+ Add a new gateway](#)

If this interface is an Internet connection, select an existing Gateway from the list or add a new one using the "Add" button. On local area network interfaces the upstream gateway should be "none". Selecting an upstream gateway causes the firewall to treat this interface as a WAN type interface. Gateways can be managed by [clicking here](#).

Reserved Networks

Block private networks ☐

Inserire l'indirizzo di gateway, in questo caso il 192.168.50.1 in subnet 24 e salvare.

Attivare il servizio del DHCP Server in **Services > DHCP Server**

Services / DHCP Server / LAN2

ISC DHCP has reached end-of-life and will be removed in a future release.

General DHCP Options

DHCP Backend: ISC DHCP

☒ Enable DHCP server on LAN2 interface

BOOTP: ☐ Ignore BOOTP queries

Deny Unknown Clients: ☐ Allow all clients

Ignore Denied Clients: ☐ Ignore denied clients rather than reject

Primary Address Pool

Subnet: 192.168.50.0/24

Subnet Range: 192.168.50.1 - 192.168.50.254

Address Pool Range: From To

The specified range for this pool must not be within the range configured on any other address pool for this interface.

Additional Pools: [+ Add Address Pool](#)

If additional pools of addresses are needed inside of this subnet outside of the above range, they may be specified here.

Impostare il range di indirizzi IP che il server DHCP potrà assegnare e salvare.

Con questa configurazione Metasploitable2, una volta riavviato, si conatterà alla rete 192.168.50.1 e lanciare il comando **ip a** o **ifconfig** per ottenere l'indirizzo IP.

Firewall / Rules / LAN

Floating LAN LAN2

Rules (Drag to Change Order)

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✓	2/711 KiB	*	*	LAN Address	443	*	*	*	Anti-Logout Rule	Settings
✗	0/2 KiB	IPv4 *	*	192.168.50.100	*	*	none	*	Block_meta	Add Edit Delete Copy Paste
✓	12/363 KiB	IPv4 *	LAN subnets	*	*	*	none	*	Default allow LAN to any rule	Add Edit Delete Copy Paste
✓	0/0 B	IPv6 *	LAN subnets	*	*	*	none	*	Default allow LAN IPv6 to any rule	Add Edit Delete Copy Paste

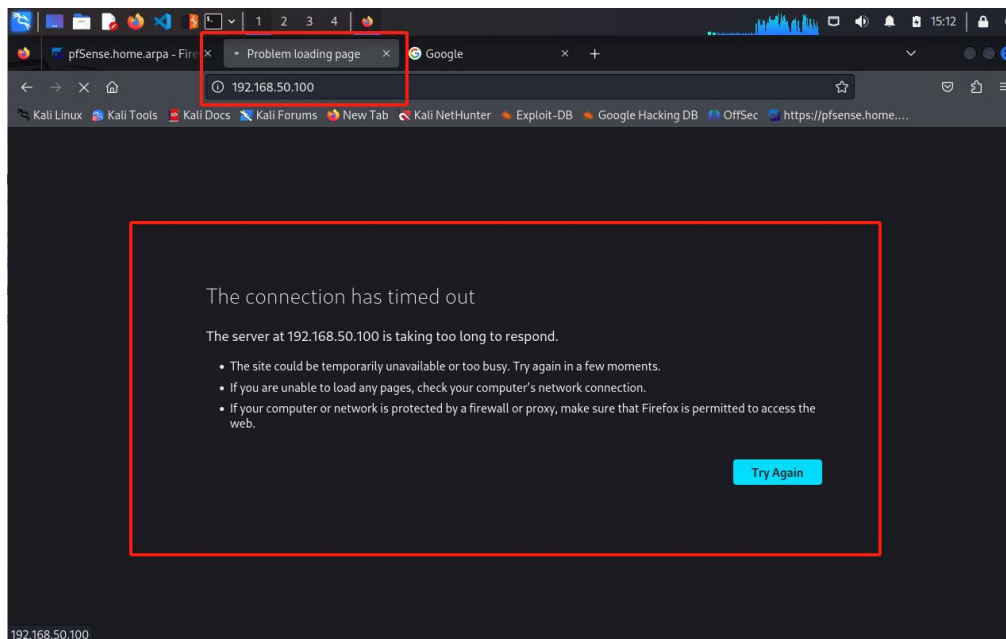
[Add](#) [Add](#) [Delete](#) [Toggle](#) [Copy](#) [Save](#) [Separator](#)

Su **Firewall > Rules** LAN impostare nuovamente la regola bloccando l'indirizzo IP di Metasploitable2.

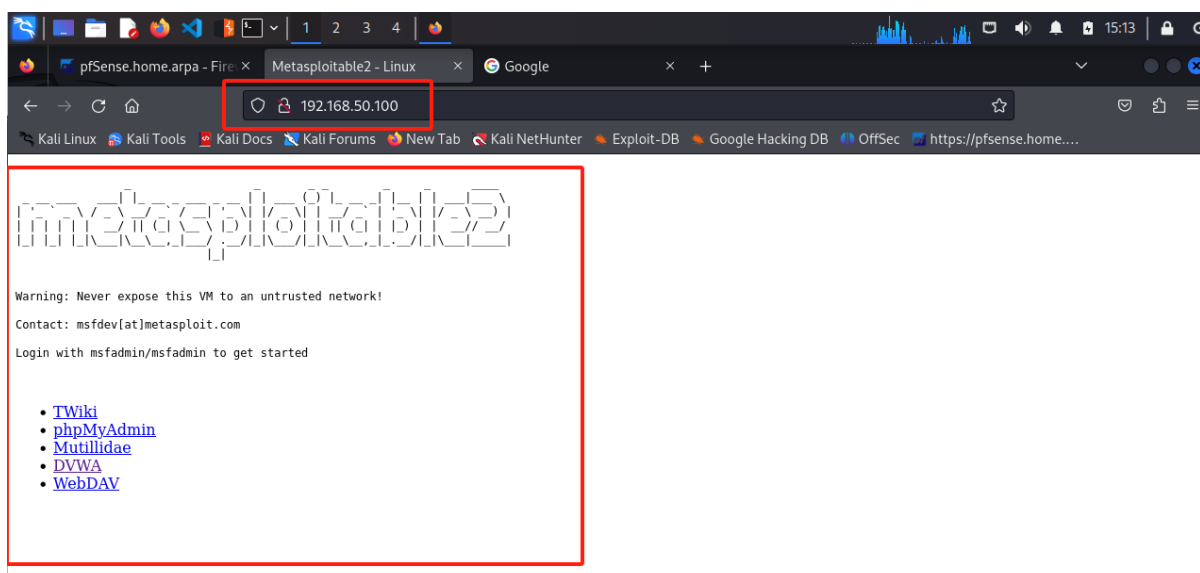
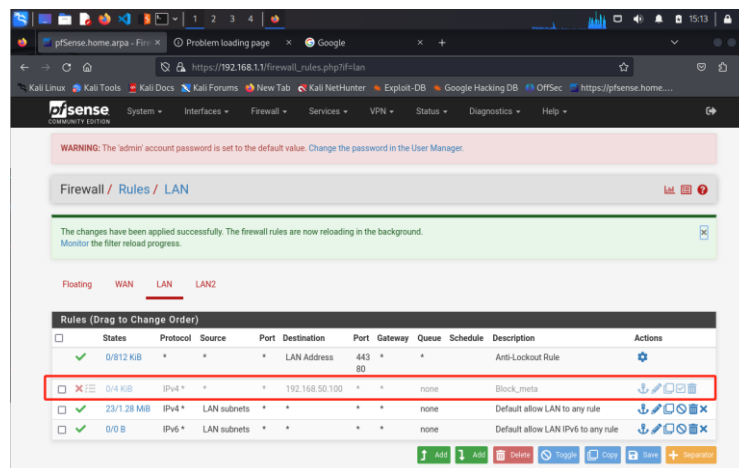
In questo caso è 192.168.50.100 per Metasploitable2 e 192.168.1.100 per Kali Linux.

Test regola di firewall

La regola di firewall su LAN funziona correttamente.



Se si disattiva la regola, il server DVWA di Meta ricomincia a funzionare.



Svolgimento esercizio facoltativo

Analisi dei log

WARNING: The 'admin' account password is set to the default value. [Change the password in the System Settings.](#)

Status / System Logs / Firewall / Normal View

System **Firewall** DHCP Authentication IPsec PPP PPPoE/L2

Normal View **Dynamic View** Summary View

Last 500 Firewall Log Entries. (Maximum 500)

Action	Time	Interface	Rule	Destination	Protocol
✗	Sep 17 19:50:49	LAN2	Default deny rule IPv4 (1000000103)	192.168.50.100:48325	UDP
✗	Sep 17 19:50:49	LAN2	Default deny rule IPv4 (1000000103)	192.168.50.100:48325	UDP
✗	Sep 17 19:50:49	LAN2	Default deny rule IPv4 (1000000103)	192.168.50.100:47867	UDP
✗	Sep 17 19:50:49	LAN2	Default deny rule IPv4 (1000000103)	192.168.50.100:47867	UDP
✗	Sep 17 19:50:49	LAN2	Default deny rule IPv4 (1000000103)	192.168.50.100:33723	UDP
✗	Sep 17 19:50:49	LAN2	Default deny rule IPv4 (1000000103)	192.168.50.100:51054	UDP
✗	Sep 17 19:50:49	LAN2	Default deny rule IPv4 (1000000103)	192.168.50.100:51054	UDP

Recandosi nella sezione come da figura, si notano tutti i tentativi di connessione all'indirizzo IP bloccato da pfSense 192.168.50.100 in qualsiasi protocollo (era stato impostato ANY).

Troubleshooting delle regole firewall

Visitare la pagina web <https://docs.netgate.com/pfsense/en/latest/troubleshooting/firewall.html> ed esplorare le impostazioni di pfSense raggiungibile anche dal dominio <https://pfsense.home.arpa/>