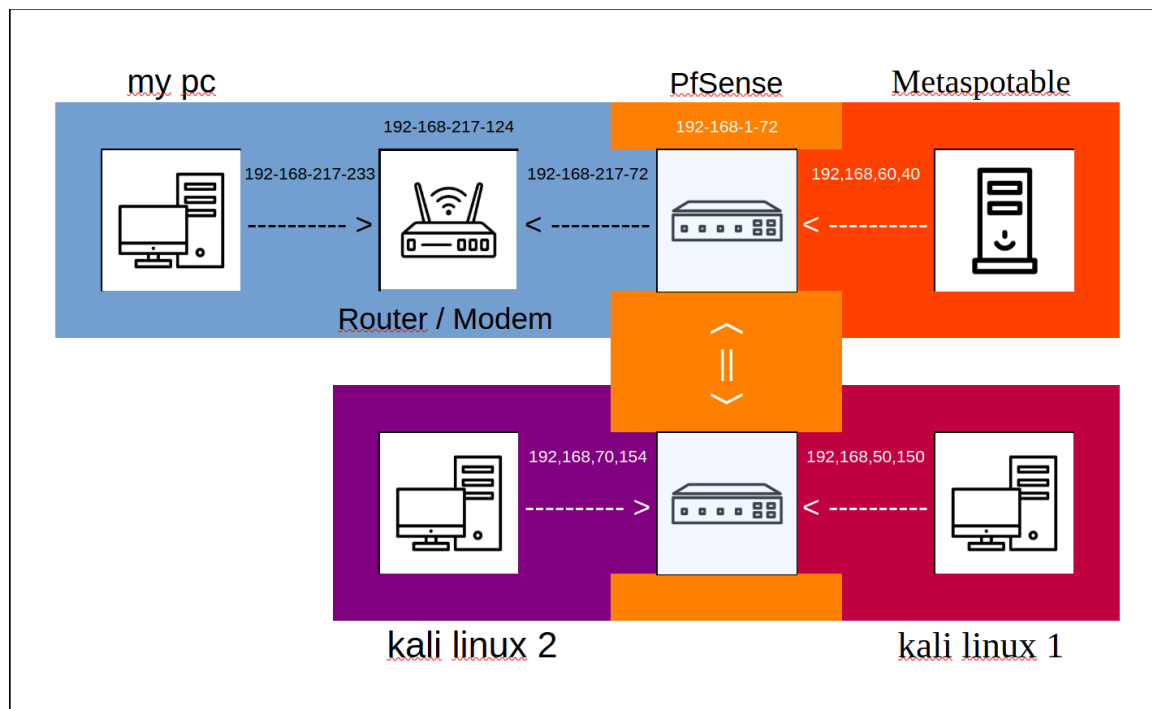


creare una regola firewall che **blocchi** l'accesso alla DVWA (su metasploitable) dalla macchina Kali Linux e ne impedisca di conseguenza lo scan. Un requisito fondamentale dell'esercizio è che le macchine Kali e Metasploitable siano su **reti diverse**.



## Descrizione della Rete

Ho simulato un'infrastruttura di rete configurando tre diverse reti, come segue:

1. ( **Kinetnet** : 192.168.50.X/24 )
2. ( **Minetnet** : (Server) 192.168.60.X/24 )
3. ( **Winetnet** : 192.168.70.X/24 ) (rete di controllo)

Queste reti sono collegate a un router, implementato tramite una macchina virtuale (VM) con sistema operativo PfSense. Con qui configurate il firewall per bloccare la comunicazione verso il server presente nella rete Minetnet.

Utilizzeremo la DVWA (Damn Vulnerable Web Application) presente su Metasploitable come server web.

Nella presente simulazione, ho deciso di introdurre una rete aggiuntiva (Winetnet) rispetto a quanto previsto nelle istruzioni del compito. Questa scelta mi ha consentito di affrontare e risolvere ulteriori problematiche che discuterò in seguito.

In questa simulazione sarà presente un solo dispositivo per ogni rete:

1. ( **Kinetnet** : **kali linux 1** )
2. ( **Minetnet** : **Metaspotable** )
3. ( **Winetnet** : **kali linux 2** ) (dispositivo di controllo)

questo per semplicità e chiarezza. Il dispositivo **Kali Linux 2** all'interno della rete **Winetnet** funge da sistema di monitoraggio e controllo, garantendo che le regole del firewall, pur essendo apparentemente corrette, non interferiscano con altre comunicazioni della o delle altre reti.

## configurazione Metaspotable

```
Metaspotable 1 [In esecuzione] - Oracle VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:17:30:8b
          inet addr:192.168.60.40  Bcast:192.168.56.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe17:308b/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:51 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:3962 (3.8 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:105 errors:0 dropped:0 overruns:0 frame:0
          TX packets:105 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:20665 (20.1 KB)  TX bytes:20665 (20.1 KB)

msfadmin@metasploitable:~$ _
```

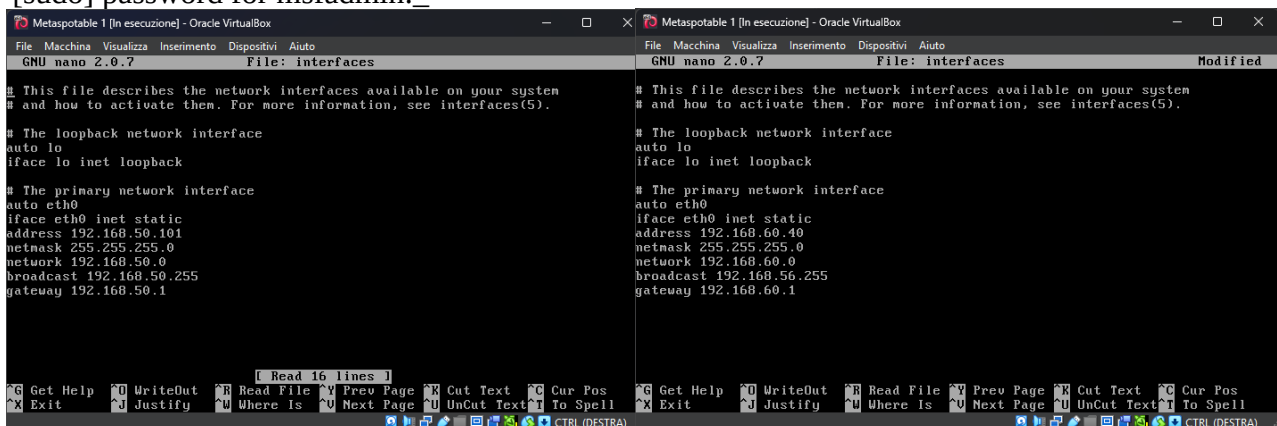
Un breve tutorial su come trovare e modificare il file dell'interfaccia di Metasploitable.

```
msf**.*~$ cd ../../..
```

```
msf**.*/$ cd etc/network
```

```
msf**.*:/etc/network$ sudo nano interfaces
```

```
[sudo] password for msfadmin:_
```



A questo punto, sar  sufficiente aggiornare i parametri (indirizzo, rete, gateway) con valori coerenti.

```
Metaspotable 1 [In esecuzione] - Oracle VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:17:30:8b
          inet addr:192.168.60.40  Bcast:192.168.56.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe17:308b/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:51 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:3962 (3.8 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:105 errors:0 dropped:0 overruns:0 frame:0
          TX packets:105 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:20665 (20.1 KB)  TX bytes:20665 (20.1 KB)

msfadmin@metasploitable:~$ _
```

Dopo un previo riavvio della VM, verifichiamo i parametri utilizzando il comando

```
Msf**.*/$ ifconfig
```

Se tutto   configurato correttamente, osserveremo i cambiamenti attesi.

## configurazione VirtualBox

- **configurazione VM PfSense**

Scheda 1	Scheda 2	Scheda 3	Scheda 4
<div>✓ Abilita scheda di rete</div> <div>Connessa a: Scheda con bridge</div> <div>Nome: MediaTek Wi-Fi 6E MT7922 (RZ616) 160MHz Wireless LAN Card</div> <div>Tipo di scheda: Intel PRO/1000 MT Desktop (82540EM)</div> <div>Modalità promiscua: Nega</div> <div>Indirizzo MAC: 080027B0A49A</div> <div>✓ Cavo connesso</div>	<div>✓ Abilita scheda di rete</div> <div>Connessa a: Rete interna</div> <div>Nome: Kintnet</div> <div>Tipo di scheda: Rete paravirtualizzata (virtio-net)</div> <div>Modalità promiscua: Nega</div> <div>Indirizzo MAC: 080027681ED2</div> <div>✓ Cavo connesso</div>	<div>✓ Abilita scheda di rete</div> <div>Connessa a: Rete interna</div> <div>Nome: Mintnet</div> <div>Tipo di scheda: Intel PRO/1000 MT Desktop (82540EM)</div> <div>Modalità promiscua: Nega</div> <div>Indirizzo MAC: 08002767219F</div> <div>✓ Cavo connesso</div>	<div>✓ Abilita scheda di rete</div> <div>Connessa a: Rete interna</div> <div>Nome: Wintnet</div> <div>Tipo di scheda: Intel PRO/1000 MT Desktop (82540EM)</div> <div>Modalità promiscua: Nega</div> <div>Indirizzo MAC: 08002743A9AB</div> <div>✓ Cavo connesso</div>

- **configurazione VM kali linux 1**

Scheda 1	Scheda 2	Scheda 3	Scheda 4
<div>✓ Abilita scheda di rete</div> <div>Connessa a: Rete interna</div> <div>Nome: Kintnet</div> <div>Tipo di scheda: Intel PRO/1000 MT Desktop (82540EM)</div> <div>Modalità promiscua: Nega</div> <div>Indirizzo MAC: 0800276F33F5</div> <div>✓ Cavo connesso</div>			

Host connesso al router tramite la porta virtuale Kintnet.

- **configurazione VM Metaspotable**

Scheda 1	Scheda 2	Scheda 3	Scheda 4
<div>✓ Abilita scheda di rete</div> <div>Connessa a: Rete interna</div> <div>Nome: Mintnet</div> <div>Tipo di scheda: Intel PRO/1000 MT Desktop (82540EM)</div> <div>Modalità promiscua: Nega</div> <div>Indirizzo MAC: 080027CC07AC</div> <div>✓ Cavo connesso</div>			

server connesso al router tramite la porta virtuale Mintnet.

- **configurazione VM kali linux 2**

Scheda 1	Scheda 2	Scheda 3	Scheda 4
<div>✓ Abilita scheda di rete</div> <div>Connessa a: Rete interna</div> <div>Nome: Wintnet</div> <div>Tipo di scheda: Intel PRO/1000 MT Desktop (82540EM)</div> <div>Modalità promiscua: Nega</div> <div>Indirizzo MAC: 080027F4A089</div> <div>✓ Cavo connesso</div>			

Controllo connesso al router tramite la porta virtuale Wintnet.

## configurazione PfSense

- interfaccia testuale

```
WAN (wan)      -> em0      -> v4/DHCP4: 192.168.1.71/24
LAN (lan)      -> vtnet0   -> v4: 192.168.50.1/24
LAN1 (opt1)    -> em1      -> v4: 192.168.60.1/24
LAN2 (opt2)    -> em2      -> v4: 192.168.70.1/24

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
```

- interfacce

In primo luogo, è necessario abilitare le interfacce per le porte “fisiche”.

Interface	Network port
WAN	em0 (08:00:27:b0:a4:9a)
LAN	vtnet0 (08:00:27:68:1e:d2)   Delete
LAN1	em1 (08:00:27:67:21:9f)   Delete
LAN2	em2 (08:00:27:43:a9:ab)   Delete

Save

Corrispondendo agli indirizzi MAC delle schede di rete.

- Reti 1

Attivando l'interfaccia, sarà possibile configurare un IP statico per questa rete 192.168.50.1.

General Configuration

Enable

☒ Enable interface

Description

LAN

Enter a description (name) for the interface here.

IPv4 Configuration Type

Static IPv4

IPv6 Configuration Type

None

Static IPv4 Configuration

IPv4 Address

192.168.50.1

IPv4 Upstream gateway

None

- **Rete 2**

Attivando l'interfaccia, sarà possibile configurare un IP statico per questa rete 192.168.60.1.

General Configuration

Enable

☒ Enable interface

Description

LAN1

Enter a description (name) for the interface here.

IPv4 Configuration Type

Static IPv4

IPv6 Configuration Type

None

- **Rete 3**

Attivando l'interfaccia, sarà possibile configurare un IP statico per questa rete 192.168.70.1.

General Configuration

Enable

☒ Enable interface

Description

LAN2

Enter a description (name) for the interface here.

IPv4 Configuration Type

Static IPv4

IPv6 Configuration Type

None

Static IPv4 Configuration





































IPv4 Address

192.168.70.1

IPv4 Upstream gateway

None

- **configurazione firewall**

Rules (Drag to Change Order)											
<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓	0/16.96 MIB	IPv4 *	LAN2 subnets	*	*	*	*	none	Default allow LAN to any rule	    
<input type="checkbox"/>	✓	0/0 B	IPv6 *	LAN2 subnets	*	*	*	*	none	Default allow LAN IPv6 to any rule	    
Rules (Drag to Change Order)											
<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓	0/0 B	IPv4 *	LAN1 subnets	*	*	*	*	none	Default allow LAN to any rule	    
<input type="checkbox"/>	✓	0/0 B	IPv6 *	LAN1 subnets	*	*	*	*	none	Default allow LAN IPv6 to any rule	    
Rules (Drag to Change Order)											
<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	✓	0/1.58 MIB	*	*	*	LAN Address	80	*	*	Anti-Lockout Rule	
<input type="checkbox"/>	✗	0/0 B	IPv4 *	*	*	LAN1 subnets	*	*	none		    
<input type="checkbox"/>	✓	5/18.56 MiB	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	    

- **regola firewall**

Edit Firewall Rule

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

Any

Choose which IP protocol this rule should match.

Source

Source

☐ Invert match

Any

Source Address

/

Destination

Destination

☐ Invert match

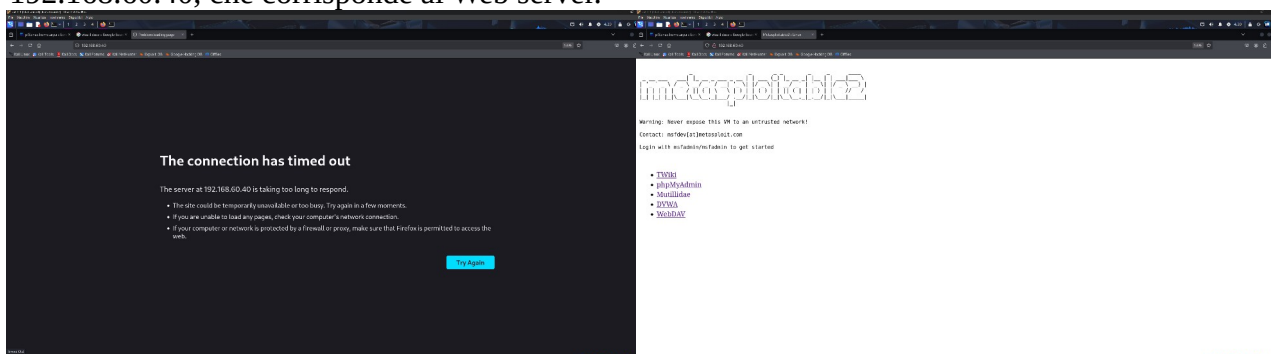
LAN1 subnets

Destination Address

/

La regola stabilisce il blocco del traffico proveniente dall'interfaccia LAN1-subnets verso l'interfaccia LAN per tutti i protocolli IPv4.

Per verificare il corretto funzionamento della nuova regola del firewall accedere all'indirizzo IP 192.168.60.40, che corrisponde al Web server.

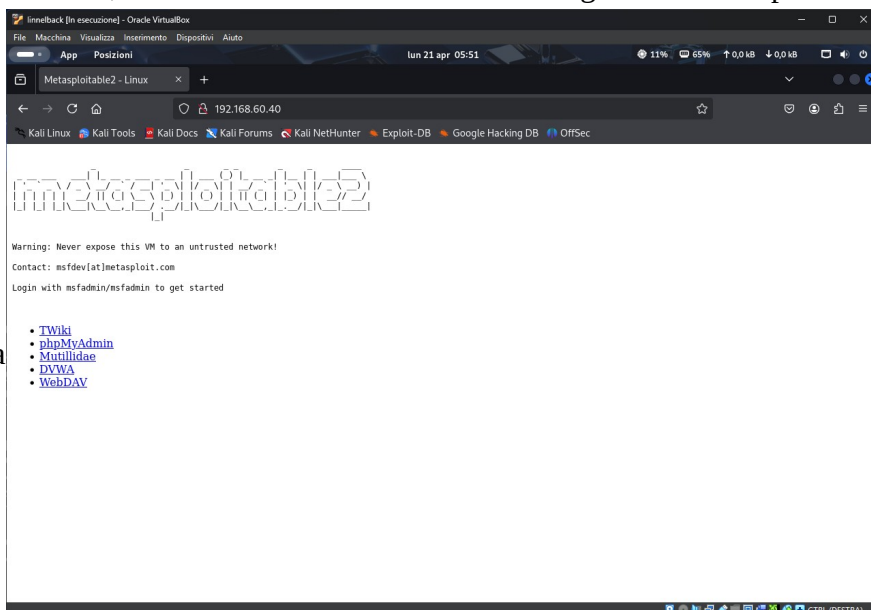


Regola attivata

regola disattivata

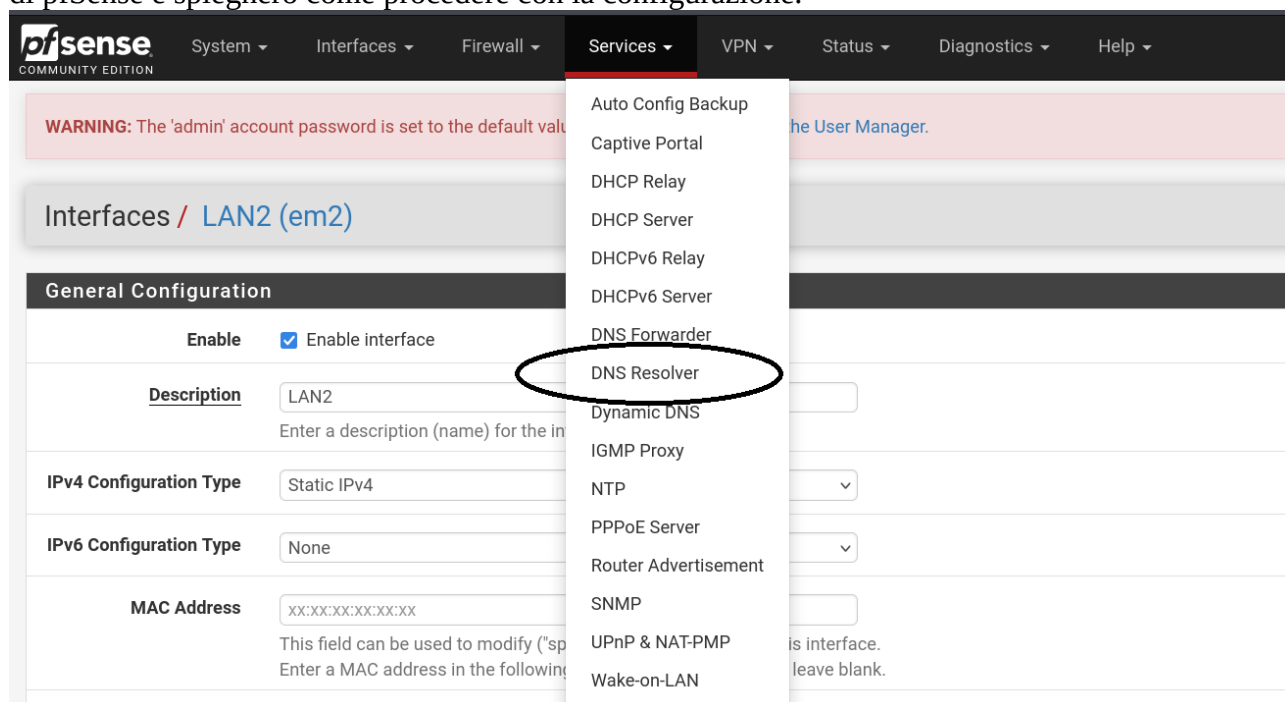
Introducendo il dispositivo di controllo, osserviamo che la modifica della regola non ha impatto sul funzionamento delle altre reti.

Per differenziare la **VM (Kali Linux 2)** dalla **VM (Kali Linux 1)**, ho configurato la seconda utilizzando l'interfaccia grafica **GNOME**, mentre la prima è basata su **KDE Plasma**.



## Configurazione DNS

Come indicato in precedenza, l'utilizzo di una terza VM mi ha permesso di identificare problemi e trovare soluzioni. Ad esempio, ho scoperto che di base solo la "LAN0" aveva accesso a Internet, il che mi ha portato a configurare il **DNS Resolver**, illustrerò dove si trova questa opzione nei menu di pfSense e spiegherò come procedere con la configurazione.



Accedendo al menu DNS Resolver, ci troveremo di fronte a un'interfaccia più complessa rispetto a quelle precedentemente viste. In questo caso ci concentreremo esclusivamente sugli aspetti essenziali relativi a questa semplificata e specifica rete.

**Come primo passo è necessario attivare il servizio DNS.**

### General DNS Resolver Options

Enable ☒ Enable DNS resolver

**Questa configurazione regola quali reti possono usufruire del servizio**

#### Network Interfaces



**Questa configurazione gestisce l'interfaccia attraverso la quale i pacchetti vengono instradati prima di essere inviati verso l'esterno, nel contesto della rete WAN.**

#### Outgoing Network Interfaces



**Le seguenti tre configurazioni sono indispensabili per garantire il corretto funzionamento di una rete semplice come questa.**

**Desidero fornire un'ultima informazione: nella cartella "ping" della repository m1s3L5 è possibile trovare i ping relativi a tutte le macchine attive, sia con regole attive che disattive.**