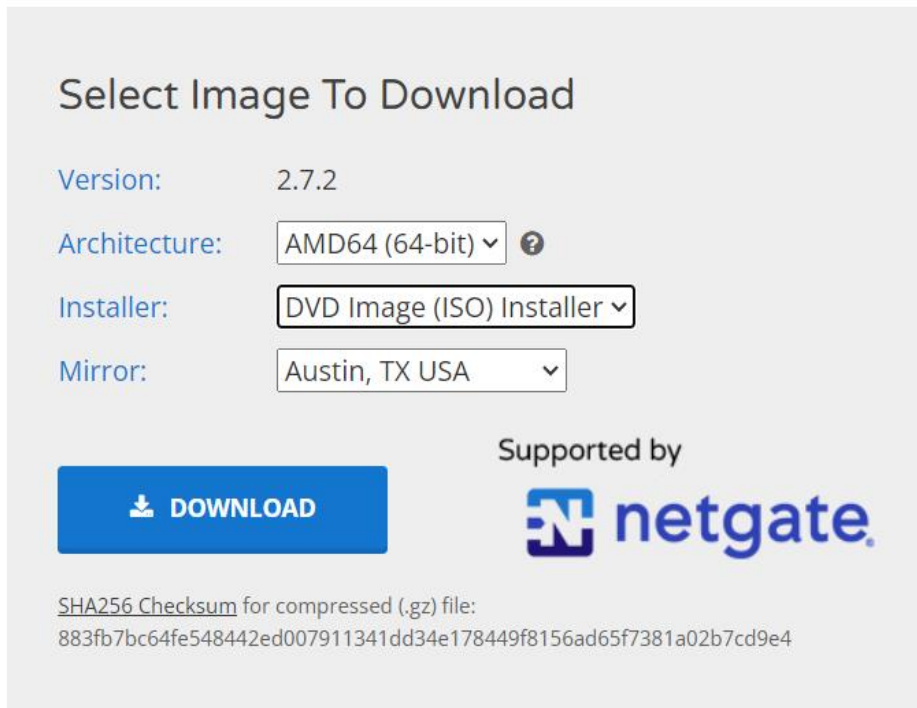


Creazione della policy con l'utilizzo di pfsense

1. Scaricare e impostare pfsense:

Eseguire il download della versione .iso di pfsense dal sito ufficiale avente le seguenti caratteristiche



Select Image To Download


Version: 2.7.2

Architecture: AMD64 (64-bit) ?

Installer: DVD Image (ISO) Installer

Mirror: Austin, TX USA

[Download](#)

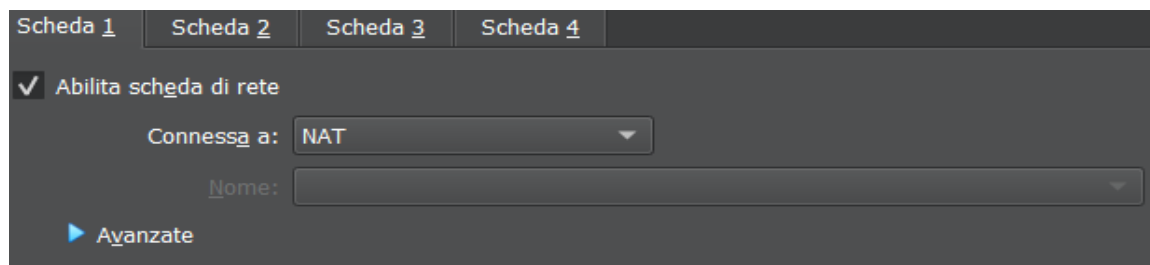
Supported by 

SHA256 Checksum for compressed (.gz) file:
883fb7bc64fe548442ed007911341dd34e178449f8156ad65f7381a02b7cd9e4

Successivamente montare il file scaricato su VB ed eseguire l'installazione procedendo con le impostazioni di default, nella fase finale prima di eseguire il reboot richiesto dall'installazione selezionare Dispositivi> Lettore ottico> pfsense.iso(altrimenti l'installazione ricomincerà dalla fase iniziale)



2. Dopo l'installazione, eseguire il settaggio delle schede di rete di pfsense -Scheda 1 impostata su NAT



Scheda 1 Scheda 2 Scheda 3 Scheda 4

☒ Abilita scheda di rete

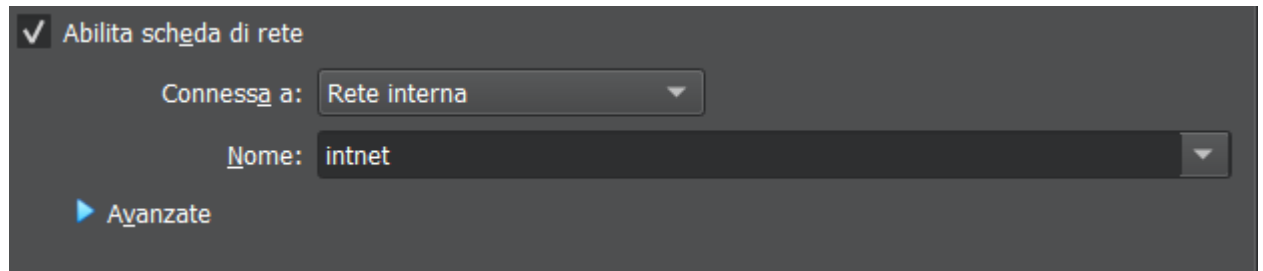
Connessa a: NAT

Nome:

[Avanzate](#)

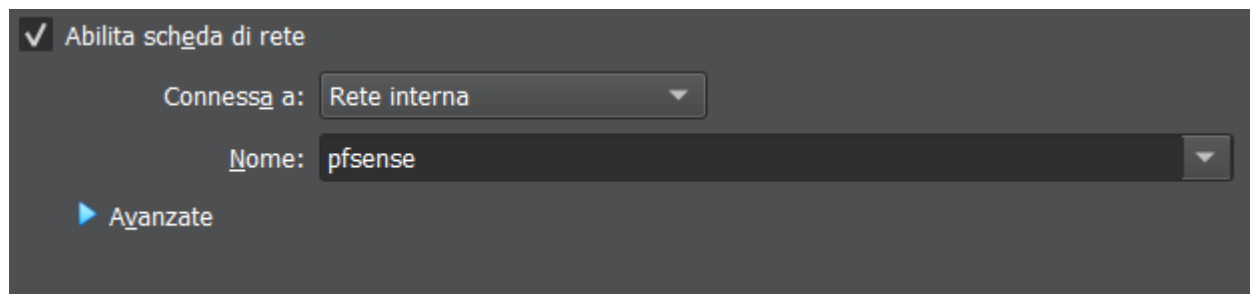
In questo modo la macchina avrà un accesso alla rete internet "WAN"

-Scheda 2 su Rete interna



La seconda scheda servirà alla macchina per essere connessa alla rete interna di VB LAN

-Scheda 3 su rete interna:



Ha la stessa funzionalità della Scheda 2 ma sarà dedicata per creare un collegamento con Metasploitable 2 (imposteremo anche la scheda di rete di Metasploitable 2 come nell'immagine)

3. Terminata l'installazione verifichiamo il funzionamento della macchina.

Dopo aver acceso pfSense ed atteso il suo caricamento vedremo le 2 schede di rete attive sia la WAN che la LAN.

Premiamo 7 e INVIO e inseriamo IP di Google 8.8.8.8, questa operazione è necessaria per vedere se la macchina è connessa alla rete esterna della VB (internet)



Passiamo alla configurazione di Kali / Meta

Quesito importante dell'esercizio è che queste 2 macchine devono stare su 2 reti diverse.

Per far cio con il comando `sudo nano /etc/network/interfaces` modificare address e gateway, **inserendo come subnet quella di Pfsense (.1.)** e successivamente usando il comando `sudo reboot`.

```
File Actions Edit View Help
GNU nano 7.2
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

auto eth0
iface eth0 inet static

address 192.168.1.100
netmask 255.255.255.0
gateway 192.168.1.1
```

In questo modo avremo le 2 macchine su 2 reti differenti.

Con lo stesso comando andiamo ad cambiare le impostazioni di rete di Meta cambiando in suo IP da statico ad DHCP sostituendo la dicitura `STATIC` con `DHCP` e commentando le altre voci sotto

```
# 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
gateway 192.168.50.1
```

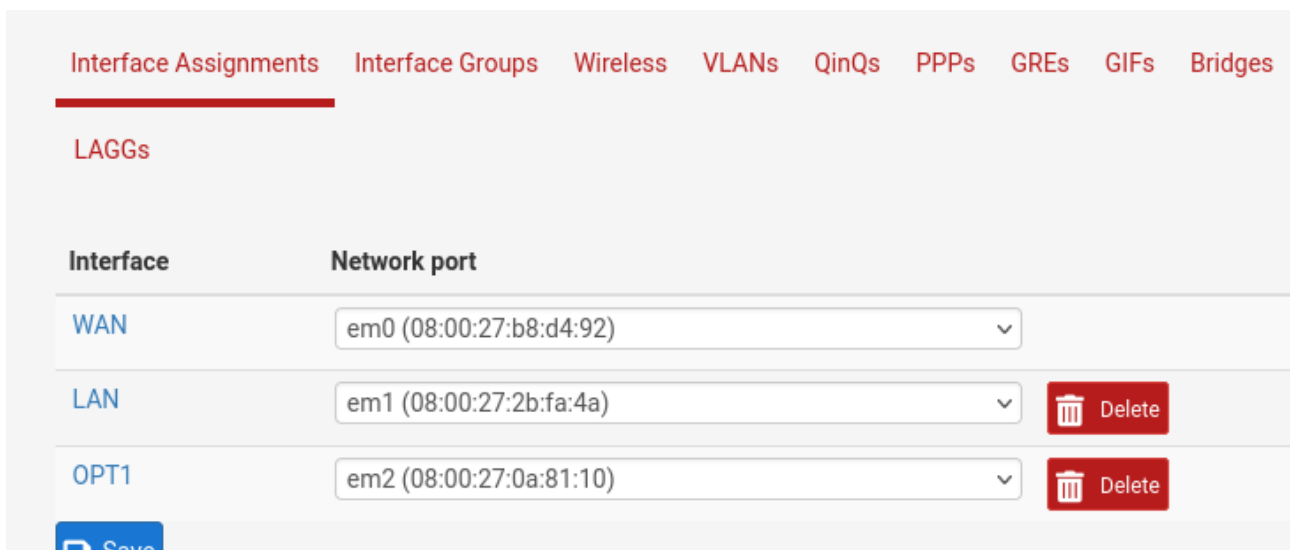
Ora controlliamo se Kali comunica con Pfsense: eseguiamo dunque un ping da Kali sull IP di pfsense.

```
File Actions Edit View Help
zsh: corrupt history file /home/kali/.zsh_history
(kali@kali)-[~]
$ ping 192.168.1.1
PING 192.168.1.1 (192.168.1.1) 56(84) bytes of data.
64 bytes from 192.168.1.1: icmp_seq=1 ttl=64 time=0.722 ms
64 bytes from 192.168.1.1: icmp_seq=2 ttl=64 time=0.342 ms
64 bytes from 192.168.1.1: icmp_seq=3 ttl=64 time=0.376 ms
^C
— 192.168.1.1 ping statistics —
3 packets transmitted, 3 received, 0% packet loss, time 2034ms
rtt min/avg/max/mdev = 0.342/0.480/0.722/0.171 ms
(kali@kali)-[~]
$
```

Configurazione dell'interfaccia di rete

Inseriamo l'IP di pfSense nel browser di Kali, proseguiamo con i permessi alla pagina ed in seguito inseriamo il login di default USER admin PASSWORD pfSense ed entriamo nel menu grafico del FIREWALL.

Prima azione è quella di creare una nuova interfaccia di rete affinché la rete di meta sia gestita "FILTRATA" da pfSense. Seguire il seguente percorso Menu> Interfaces> Interfaces Assignments ed aggiungere la Available network ports:



Salvare

Ora ci occorre settare la nuova interfaccia di rete con i dati di Meta 2.

Ci spostiamo su Menu> Interfaces> OPT1

Le azioni da compiere all'interno di questo sotto menu sono:

1 abilitare l'interfaccia

2 configurare IPv4 Configuration su "Static IPv4"

3 inserire nel riquadro IPv4 Address l IP di meta con la notazione CIDR /24

General Configuration

Enable

☒ Enable interface

Description

OPT1

Enter a description (name) for the interface here.

IPv4 Configuration Type

Static IPv4

IPv6 Configuration Type

None

MAC Address

xxxxxxxxxxxx

This field can be used to modify ("spoof") the MAC address of this interface.
Enter a MAC address in the following format: xx:xx:xx:xx:xx:xx 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

Default (no preference, typically autoselect)

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

192.168.50.101

/ 24

IPv4 Upstream gateway

None

+ Add a new gateway

Salviamo e diamo conferma delle nostre modifiche

The OPT1 configuration has been changed.
The changes must be applied to take effect.
Don't forget to adjust the DHCP Server range if needed after applying.

✓ Apply Changes

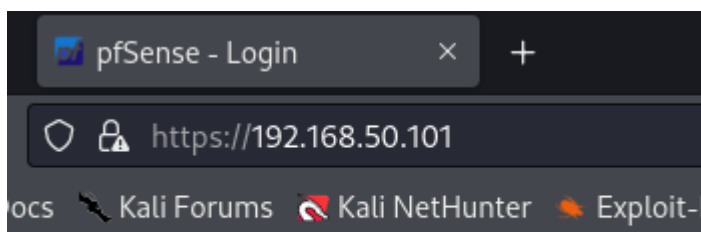
Ora abilitiamo la funzione DHCP sulla interfaccia di rete appena settata, in questo modo potremo raggiungere il server meta dal browser di kali .

Seguiamo il percorso Menu>Services>DHCP Server> OPT1 ed iniziamo il settaggio come nell immagine

| General DHCP Options | |
|---------------------------|--|
| DHCP Backend | ISC DHCP |
| Enable | <input checked="" type="checkbox"/> Enable DHCP server on OPT1 interface |
| BOOTP | <input type="checkbox"/> Ignore BOOTP queries |
| Deny Unknown Clients | <div>Allow all clients</div> <p>When set to Allow all clients, any DHCP client will get an IP address within this scope/range on this interface. If set to Allow known clients from any interface, any DHCP client with a MAC address listed in a static mapping on any scope(s)/interface(s) will get an IP address. If set to Allow known clients from only this interface, only MAC addresses listed in static mappings on this interface will get an IP address within this scope/range.</p> |
| Ignore Denied Clients | <input type="checkbox"/> Ignore denied clients rather than reject This option is not compatible with failover and cannot be enabled when a Failover Peer IP address is configured. |
| Ignore Client Identifiers | <input type="checkbox"/> Do not record a unique identifier (UID) in client lease data if present in the client DHCP request This option may be useful when a client can dual boot using different client identifiers but the same hardware (MAC) address. Note that the resulting server behavior violates the official DHCP specification. |
| Primary Address Pool | |
| Subnet | 192.168.50.0/24 |
| Subnet Range | 192.168.50.1 - 192.168.50.254 |
| Address Pool Range | <div>192.168.50.100</div> <div>192.168.50.200</div> <div>From To</div> <p>The specified range for this pool must not be within the range configured on any other address pool for this interface.</p> |
| Additional Pools | + Add Address Pool |

Salviamo , confermiamo le modifiche

Verifichiamo se adesso il server di Meta 2 e raggiungibile tramite il suo IP



vediamo nell immagine che e tutto funzionante

| | | | |
|----------------|----------------|---------|-----------------------|
| 192.168.1.100 | 192.168.50.101 | TCP | 74 58100 → 443 [SYN] |
| 192.168.50.101 | 192.168.1.100 | TCP | 74 443 → 58100 [SYN] |
| 192.168.1.100 | 192.168.50.101 | TCP | 66 58100 → 443 [ACK] |
| 192.168.1.100 | 192.168.50.101 | TLSv1.3 | 583 Client Hello |
| 192.168.50.101 | 192.168.1.100 | TCP | 66 443 → 58100 [ACK] |
| 192.168.50.101 | 192.168.1.100 | TLSv1.3 | 316 Server Hello, Cha |
| 192.168.1.100 | 192.168.50.101 | TCP | 66 58100 → 443 [ACK] |
| 192.168.1.100 | 192.168.50.101 | TLSv1.3 | 146 Change Cipher Spe |
| 192.168.1.100 | 192.168.50.101 | TLSv1.3 | 236 Application Data |
| 192.168.1.100 | 192.168.50.101 | TLSv1.3 | 417 Application Data |
| 192.168.50.101 | 192.168.1.100 | TCP | 66 443 → 58100 [ACK] |
| 192.168.50.101 | 192.168.1.100 | TCP | 66 443 → 58100 [ACK] |
| 192.168.50.101 | 192.168.1.100 | TCP | 66 443 → 58100 [ACK] |
| 192.168.50.101 | 192.168.1.100 | TLSv1.3 | 145 Application Data |
| 192.168.50.101 | 192.168.1.100 | TLSv1.3 | 137 Application Data |

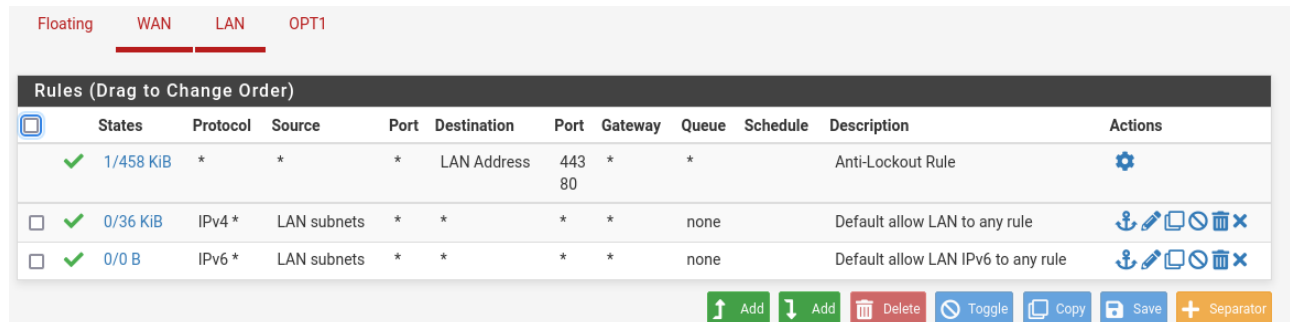
E avviene lo scambio di pacchetti TCP e la creazione di un ponte di comunicazione tramite l'utilizzo di SYN,SYN ACK ,ACK da entrambe le macchine coinvolte nella trasmissione.

Impostazione delle POLICY del FIREWALL

Lo scopo finale dell'esercitazione è quella di impedire la comunicazione tra Kali e Meta attraverso l'uso di un firewall (pfSense). Per impedire la comunicazione ci basta settare una POLICY "regola"

Torniamo sull'impostazione grafica di pfSense

Seguiamo il percorso Menu>FIREWALL>Rules e selezioniamo la voce LAN



Selezioniamo ADD con la freccia rivolta verso l'alto, qui possiamo iniziare a scrivere la nostra regola:

1 nella voce Action selezioniamo Block

2 nella voce Source (sorgente) impostiamo network e inseriamo IP di Kali in notazione CIDR/24

3 nella voce Destination (destinazione) impostiamo network, inseriamo l'IP di Meta 2 in notazione CIDR/24

Mentre nella voce Destination Port Range impostiamo le porte 80 http e la 443 https

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) is sent back to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

Source
Source ☐ Invert match Network 192.168.1.100 / 24
[Display Advanced](#)
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 Network 192.168.50.101 / 24
Destination Port Range HTTP (80) 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.

Salviamo, accettiamo le modifiche e testiamo la nostra regola.

Come vediamo nelle immagini qui sotto la policy del firewall è stata settata a dovere in quanto tutti i tentativi di connessione da parte di Kali verso Meta vengono filtrati e respinti dal firewall

| | | | | |
|---------------|----------------|-----|-------------------------|-------------------|
| 192.168.1.100 | 192.168.50.101 | TCP | 74 [TCP Retransmission] | 59014 → 443 [SYN] |
| 192.168.1.100 | 192.168.50.101 | TCP | 74 [TCP Retransmission] | 59024 → 443 [SYN] |
| 192.168.1.100 | 192.168.50.101 | TCP | 74 [TCP Retransmission] | 59014 → 443 [SYN] |
| 192.168.1.100 | 192.168.50.101 | TCP | 74 [TCP Retransmission] | 59024 → 443 [SYN] |
| 192.168.1.100 | 192.168.50.101 | TCP | 74 [TCP Retransmission] | 59014 → 443 [SYN] |
| 192.168.1.100 | 192.168.50.101 | TCP | 74 [TCP Retransmission] | 59024 → 443 [SYN] |
| 192.168.1.100 | 192.168.50.101 | TCP | 74 [TCP Retransmission] | 59014 → 443 [SYN] |
| 192.168.1.100 | 192.168.50.101 | TCP | 74 [TCP Retransmission] | 59024 → 443 [SYN] |
| 192.168.1.100 | 192.168.50.101 | TCP | 74 [TCP Retransmission] | 59014 → 443 [SYN] |

