

Pfsense è un firewall virtuale: è un software open-source basato su FreeBSD che funge da firewall, router e dispositivo di sicurezza per reti informatiche. È progettato per gestire e controllare il traffico di rete, offrendo funzionalità avanzate come filtraggio degli indirizzi IP, VPN, bilanciamento del carico, controllo di accesso, monitoraggio del traffico e molto altro. Serve principalmente a proteggere le reti da minacce esterne, permettendo agli amministratori di configurare regole di sicurezza, monitorare l'attività di rete e ottimizzare le prestazioni del sistema. È particolarmente utile per reti aziendali o domesiche che necessitano di un alto livello di sicurezza e controllo del traffico.

FreeBSD è un sistema operativo open-source conosciuto per la sua affidabilità, sicurezza, performance e la sua natura altamente stabile e sicura che lo rende una scelta popolare per i server. È una delle varianti più popolari del sistema operativo BSD (Berkeley Software Distribution), derivato da UNIX. FreeBSD è utilizzato per diversi contesti come i server web, desktop, dispositivi di rete e sistemi embedded. Ha un'architettura modulare che consente una maggiore flessibilità e scalabilità.

Creazione policy Pfsense

1. Istallazione della nuova macchina virtuale con OS pfSense. Per eseguire l'accesso l'username e la password di default sono «admin» e «pfSense».

È necessario rimuovere la seconda opzione che rappresenta il pacchetto di installazione e che, se non rimosso, fa ripartire l'installazione all'infinito.

Poi andiamo sulle impostazioni della nuova macchina pfsense e creiamo 2 NIC (interfacce di rete) su “Rete”:

Scheda 1 -> connessa a NAT = interfaccia WAN

Scheda 2 -> connessa ad INTERN/Rete interna = interfaccia LAN (bisogna attivare la scheda 2 su Interna).

Dopo l'istallazione, riavviare la macchina. Controllare la "lista dei boot" (l'ordine in cui il computer cerca i dispositivi di avvio quando viene acceso). Questa lista è solitamente configurata nel BIOS o nell'UEFI del computer -> opzione "Ordine di avvio" o "Sequenza di avvio" serve per vedere e modificare la lista dei dispositivi di avvio. È importante assicurarsi che il disco rigido sia elencato come prima scelta per garantire che il sistema si avvii correttamente dal disco rigido.

- Ora si possono vedere le configurazioni di rete sulla Shell di pfsense. La macchina ha quindi 2 interfacce di rete, una WAN e due LAN.

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

WAN (wan)      -> em0      -> v4: 192.168.1.2/24
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 (sshd)
6) Halt system                 15) Restore recent configuration
7) Ping host                   16) Restart PHP-FPM
8) Shell

Enter an option: █
```

- Proviamo ad inviare un ping a www.google.com per accertarci che le configurazioni dell'interfaccia WAN siano corrette e che ci sia connettività verso Internet. Selezioniamo Ping host con il numero 7, poi scriviamo l'host da pingare.

```
Starting syslog...done.
Starting CRON... done.
pfSense 2.6.0-RELEASE amd64 Mon Jan 31 19:57:53 UTC 2022
Bootstrap complete

FreeBSD/amd64 (pfSense.home.arp) (ttyv0)

VirtualBox Virtual Machine - Netgate Device ID: 51c64a7758bea501cf26

*** Welcome to pfSense 2.6.0-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 (sshd)
6) Halt system                 15) Restore recent configuration
7) Ping host                   16) Restart PHP-FPM
8) Shell

Enter an option: [
```



Ps. In caso sia necessario cambiare le configurazioni di rete, per tornare alle configurazioni originarie è sufficiente scegliere l'opzione 4) Reset to factory default.

Un requisito fondamentale dell'esercizio è che le macchine Kali e Metasploitable siano su reti diverse.

-Avviare Meta.

-Poi bisogna andare nella configurazione di rete di Kali linux in INTERN (non è necessario sia connessa a Internet) e, 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. In tal modo, senza toccare la configurazione di Meta, Kali e Meta risulteranno avere due reti diverse. Non modifichiamo le impostazioni di pfsense perchè, come per inetsim ad esempio, sarebbe più lungo e difficile.

```
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 192.168.1.100/24
gateway 192.168.1.1
```

Home

esercizio

Home

È possibile aggiungere e configurare la nuova interfaccia di rete su PfSense per gestire un’ulteriore rete separata. È possibile farlo attraverso la sua interfaccia di amministrazione web (Web Gui) -> accedere all’interfaccia di amministrazione web di pfSense dal browser, di solito digitando l’indirizzo IP del pfSense nella barra degli indirizzi.

Poi bisogna creare la terza scheda di rete sulla macchina pfsense, che corrisponde ad un’altra LAN, ed attivarla su Interna.

2. Configurare l’interfaccia di rete posta sulla LAN2

Nel browser di Kali -> inserire l’IP (LAN) di pfsense -> accettare il rischio -> inserire credenziali di default. Cliccare sulla scritta “pfsense”.

Quindi una volta connesso, vai alla sezione relativa alla configurazione delle interfacce di rete: in “Interfaces”. Clicca su “Assignments” per assegnare una nuova interfaccia di rete. Qui dovresti vedere tutte le interfacce di rete disponibili sulla macchina pfSense (visualizzerai qui una scheda di rete fisica aggiuntiva e se stai virtualizzando, potresti dover prima aggiungere una nuova interfaccia virtuale nel software di virtualizzazione e quindi assegnarla a pfSense).

Una volta configurata l’interfaccia di rete, potrai utilizzare PfSense per gestire questa nuova rete separata, ad esempio applicando regole di firewall o configurando le impostazioni di routing.

- Ho creato l’interfaccia della LAN2 su Interna con Add.

The screenshot shows the pfSense interface at https://192.168.1.1/interfaces_assign.php. At the top, there's a warning message: "WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager." Below this, the title is "Interfaces / Interface Assignments". There are tabs for "Interface Assignments" (which is selected), "Interface Groups", "Wireless", "VLANs", "QinQs", "PPPs", "GREs", "GIFs", "Bridges", and "LAGGs". The main table has two columns: "Interface" and "Network port". It shows "WAN" assigned to "em0 (08:00:27:be:16:31)" and "LAN" assigned to "em1 (08:00:27:08:2b:fc)". Under "Available network ports:", "em2 (08:00:27:88:dc:91)" is listed. To the right of each port entry are a "Delete" button and an "Add" button. A blue "Save" button is located at the bottom left of the table area.

- Ho poi inserito i dati necessari: ✓ Enable interfaces (abilitiamo il servizio dhcp sull’interfaccia appena creata e attiviamola), sostituire OPT1 con LAN2, Ipv4 -> Static IPv4, Static IPv4 configuration -> in “IPv4 Address” inserire la sottorete di Meta (Gateway) /24. Infine salvare e “Apply changes”.

Impostazioni:

-**Action:** in questa sezione si può scegliere come gestire il traffico analizzato

-**Interface:** l’interfaccia da dove arrivano i pacchetti

-**Source:** in questa sezione si può scegliere che tipo di sorgente si andrà ad inserire, come un singolo IP, oppure una rete intera.

-**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.

3. Creare una regola firewall che blocchi l'accesso alla DVWA (su metasploitable) dalla macchina Kali Linux e ne impedisca di conseguenza lo scan.

Voglio creare una regola Firewall per impedire l'accesso dalla macchina di Kali Linux al server di Meta quindi per impedire a Kali Linux di interagire con l'applicazione DVWA, ospitata su Metasploitable.

Firewall/Rules/LAN2 per creare la nuova regola.

In LAN2, premere Add e inserire:

- in “Action”: Block
- in “Protocol”: Any
- in Source: prima Network, poi IP di Kali /24
- in Destination: prima Network, poi IP di Meta /24.

Infine Save e Apply changes, ottenendo il risultato grafico della nuova regola impostata.

The screenshot shows the pfSense Firewall Rules configuration. The top navigation bar has tabs for Floating, WAN, LAN, and LAN2, with LAN2 selected. Below the tabs is a table titled "Rules (Drag to Change Order)". The table has columns for States, Protocol, Source, Port, Destination, Port, Gateway, Queue, Schedule, Description, and Actions. A single rule is listed: "0/0 B" (IPv4 *) from "192.168.1.100/24" to "192.168.50.101/24" on port * to *. The "Actions" column shows icons for edit, delete, toggle, copy, save, and separator. Below the table are buttons for Add, Delete, Toggle, Copy, Save, and Separator.

Ho poi tentato il ping da Kali all'indirizzo IP di Meta, per testare l'efficacia della regola settata nel Virtual Firewall.

Come si vede nell'immagine, la comunicazione fra le due macchine potrebbe avvenire perché, nonostante siano su due reti diverse, **comunicano tramite pfsense** dato che abbiamo attivato le interfacce. **La connessione però viene bloccata dal Firewall stesso** e per questo vedremo che i pacchetti sono stati persi e non sono arrivati.

```
(kali㉿kali)-[~]
$ ping 192.168.50.101
PING 192.168.50.101 (192.168.50.101) 56(84) bytes of data.
^C
--- 192.168.50.101 ping statistics ---
5 packets transmitted, 0 received, 100% packet loss, time 4139ms

(kali㉿kali)-[~]
$
```

Qualora, invece, tentando il ping, la risposta fosse stata “Host unreachable”, allora le due macchine non avrebbero avuto alcun tipo di comunicazione.

In questo caso quindi la regola inserita fa in modo che le macchine con la sottorete che abbiamo inserito abbiano un cancello bloccato davanti che non consente il passaggio.

The screenshot shows a dual-boot desktop environment. On the left is a Kali Linux desktop with a terminal window showing a successful ping to 192.168.50.101. On the right is a pfSense interface window titled "Firewall / Rules / LAN2". The pfSense interface shows a warning message: "The firewall rule configuration has been changed. The changes must be applied for them to take effect." Below this is a table with one rule: "0/0 B" (IPv4 *) from "192.168.1.100/24" to "192.168.50.101/24" on port * to *. The "Actions" column includes icons for edit, delete, toggle, copy, save, and separator. A green "Apply Changes" button is visible at the bottom right of the pfSense interface. The pfSense interface also includes tabs for Floating, WAN, LAN, and LAN2, with LAN2 selected.