

1. Introduzione al laboratorio

Oggi, durante il laboratorio, l'obiettivo era quello di creare una regola firewall in modo pratico, seguendo i passaggi descritti nelle slide che ci sono state fornite. L'esercizio consisteva nel configurare un firewall con pfSense e applicare una regola che limitasse la comunicazione tra due macchine virtuali.

2. Obiettivo dell'esercizio

Seguendo le indicazioni delle slide, dovevamo:

1. Configurare le reti e le interfacce su pfSense.
2. Creare una regola firewall per bloccare specifiche comunicazioni tra due macchine (ad esempio, impedire il ping).
3. Verificare che la regola funzionasse come previsto, impedendo la connessione.”

3. La mia pratica

3.1. Avvio delle macchine virtuali

La prima cosa che ho fatto è stato avviare le tre macchine virtuali:

- **Linux:** il sistema principale, il “cervello” dell'esercitazione, da cui gestiamo la creazione delle regole firewall e i test.
- **pfSense:** il firewall che serve da intermediario tra le reti e permette di creare e gestire le regole di sicurezza.
- **Metasploitable:** la macchina “cavia”, che utilizziamo per verificare se il ping da Linux viene bloccato o meno.”

3.2 Configurazione iniziale delle reti

1. Avvio delle macchine virtuali

Dopo aver avviato le tre macchine virtuali (Linux, Metasploitable e pfSense), ho iniziato a configurare le reti per garantire la comunicazione corretta tra i sistemi. Il primo passo è stato lavorare sulla rete LAN e impostare gli indirizzi IP.

2. Configurazione dell'indirizzo IP su Linux

Per collegare Linux a pfSense, ho configurato manualmente un indirizzo IP sulla macchina Linux:

- Ho scelto l'indirizzo **192.168.5.5**.
- Ho impostato la **subnet mask** su **255.255.255.0**.
- Ho salvato le impostazioni per garantire la connessione alla rete gestita da pfSense.

Questa configurazione era necessaria perché, senza un indirizzo IP corretto, non riuscivo a collegarmi alla rete gestita da pfSense.

3. Configurazione di pfSense

Una volta sistemata la rete su Linux, sono passato a pfSense:

- Ho impostato l'indirizzo IP della LAN su **192.168.5.8**.
- Questo indirizzo è servito per collegarmi all'interfaccia Web di amministrazione di pfSense.

Dopo aver configurato l'indirizzo IP, ho aperto Firefox su Linux e ho digitato **192.168.5.8** nella barra di ricerca. Questo mi ha portato alla pagina di login di pfSense, come previsto.

3.3 Accesso alla dashboard di pfSense

1. Login su pfSense

Dopo essere entrato nella schermata di login tramite il browser su Linux, ho inserito:

- L'indirizzo IP configurato precedentemente (**192.168.5.8**).
- Il nome utente e la password predefiniti di pfSense (di solito admin e pfsense, a meno che non siano stati modificati)."

2. Visualizzazione della dashboard

Una volta effettuato l'accesso, la dashboard di pfSense si presenta come segue:

A SINISTRA:

Trovi tutte le **informazioni di sistema**,
utili per conoscere i dati generali del
sistema operativo.

A DESTRA:

Trovi invece tutte le **informazioni di
supporto e/o assistenza**, utili per
risolvere eventuali problemi

pfSense COMMUNITY EDITION

System Interfaces Firewall Services VPN Status Diagnostics Help

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

Status / Dashboard

System Information	
Name	pfSense.home.arpa
User	admin@192.168.5.5 (Local Database)
System	QEMU Guest Netgate Device ID: 306134869e310f3c31f0
BIOS	Vendor: SeaBIOS Version: rel-1.16.1-0-g3208b098f51a- prebuilt.qemu.org Release Date: Tue Apr 1 2014
Version	2.7.2-RELEASE (amd64) built on Wed Dec 6 20:10:00 UTC 2023 FreeBSD 14.0-CURRENT The system is on the latest version. Version information updated at Fri Dec 13 9:08:47

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](#).

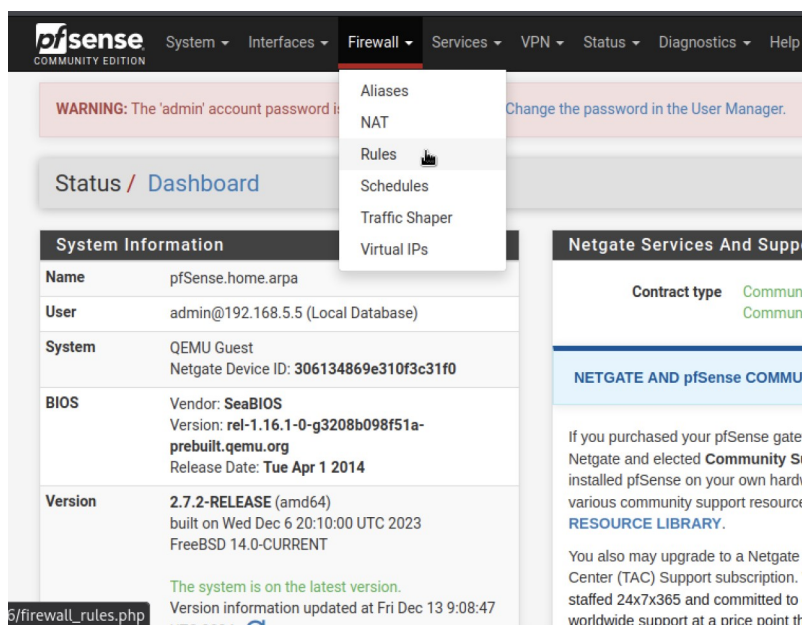
You also may upgrade to a Netgate Global Technical Assistance Center (TAC) Support subscription. We're always on! Our team is staffed 24x7x365 and committed to delivering enterprise-class, worldwide support at a price point that is more than competitive

3.4 Navigazione nella Dashboard e Configurazione del Firewall

Una volta entrati nella dashboard di pfSense e avendo visto la struttura generale, ci dirigiamo verso la sezione **Firewall** e poi su **Rules**, come evidenziato nell'immagine a destra.

- **Firewall:** Qui possiamo visualizzare e configurare le regole di accesso al nostro sistema, permettendo o bloccando il traffico in base a diverse condizioni.
- **Rules:** In questa sezione possiamo definire le regole specifiche per le interfacce di rete, come ad esempio quale traffico è permesso tra le diverse reti (WAN, LAN, ecc.).

Questa parte è cruciale per gestire la sicurezza del nostro sistema, consentendo di configurare filtri e protezioni in base alle esigenze specifiche.



3.5 Configurazione delle Regole del Firewall per LAN

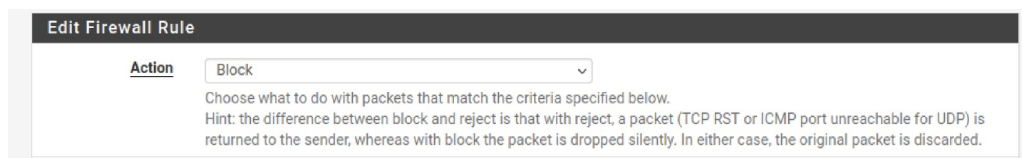
Una volta cliccato su **Rules**, ci dirigiamo verso **LAN**, che è l'interfaccia che dobbiamo configurare.

- Dopo aver selezionato **LAN**, si aprirà un modulo con diverse opzioni da configurare.

Questo modulo ci permette di definire le regole di accesso per il traffico che passa attraverso la rete **LAN**, stabilendo quali connessioni siano consentite o bloccate.

A questo punto, nella prossima pagina, possiamo procedere con le modifiche necessarie per definire le regole che meglio si adattano alle esigenze della nostra rete.

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



Edit Firewall Rule

Action Block

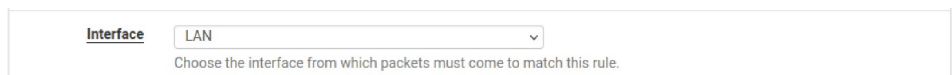
Choose what to do with packets that match the criteria specified below.
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

Disabled:
in questa sezione si può disabilitare le regole.



Disabled ☐ Disable this rule
Set this option to disable this rule without removing it from the list.

Interface : l'interfaccia da dove arrivano i pacchetti.



Interface LAN

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

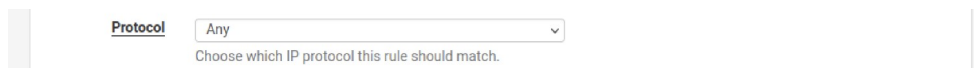
Address family:
Ipv4 oppure ipv6, si sceglie la versione di protocolli ip ai quali applicare la policy



Address Family IPv4

Select the Internet Protocol version this rule applies to.

Protocol : si sceglie il protocollo, in questo caso ho scelto any per semplicità



Protocol Any

Choose which IP protocol this rule should match.

Terminata la prima parte della configurazione delle regole per la rete **LAN**, passiamo alla **seconda parte** che comprende diverse sezioni importanti come **Risorse**, **Destinazione**, **Opzioni Extra e Informazioni sulle Regole**.

Qui inseriamo indirizzo di sorgente, nel mio caso ho inserito quello di MetaSloitable



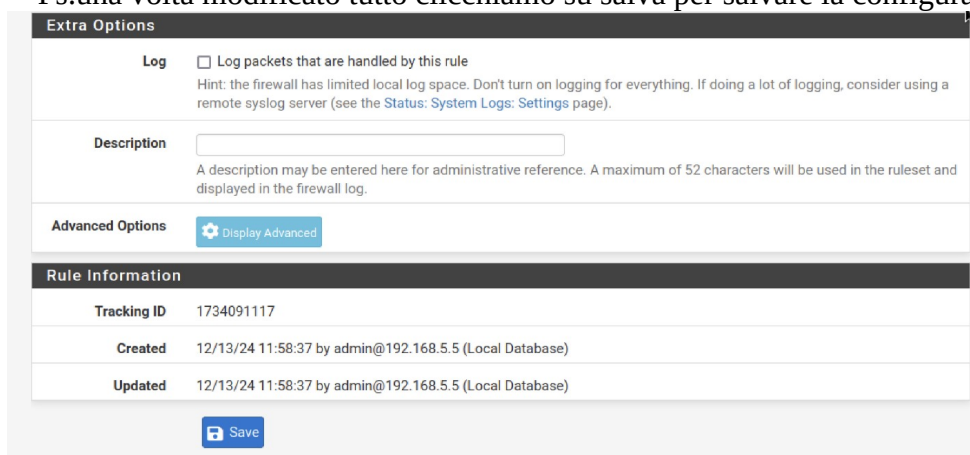
Source ☐ Invert match Address or Alias 192.168.1.39 /

Invece, inseriamo indirizzo di destinazione, nel mio caso ho inserito quello di Linux



Destination ☐ Invert match Address or Alias 192.168.5.5 /

Mentre in questa sezione troviamo, opzioni extra e informazioni sulle regole.
Ps. una volta modificato tutto clicchiamo su salva per salvare la configurazione



Extra Options

Log ☐ 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).

Description
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.

Advanced Options [Display Advanced](#)

Rule Information

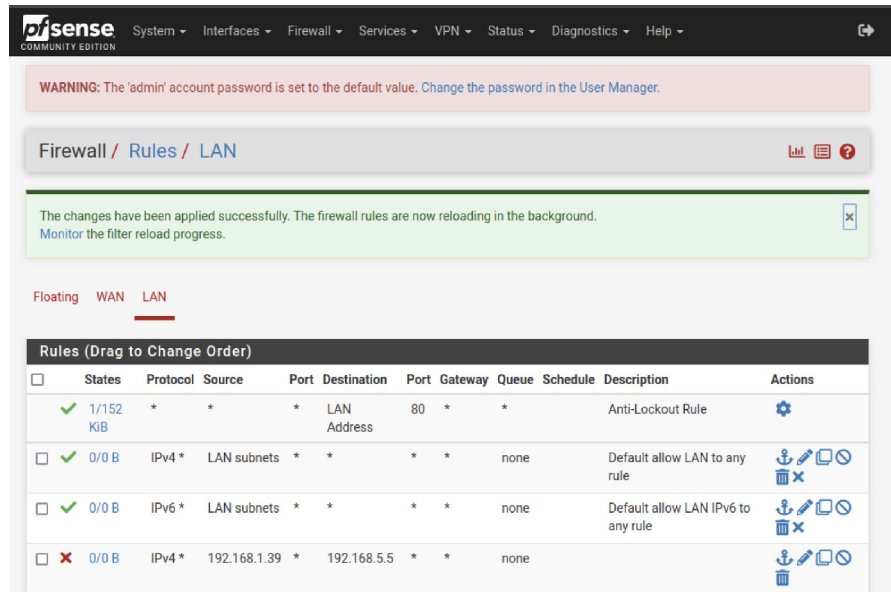
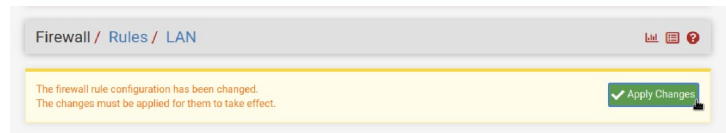
Tracking ID	1734091117
Created	12/13/24 11:58:37 by admin@192.168.5.5 (Local Database)
Updated	12/13/24 11:58:37 by admin@192.168.5.5 (Local Database)

[Save](#)

Applicazione delle Modifiche e Passaggio al Prossimo Step

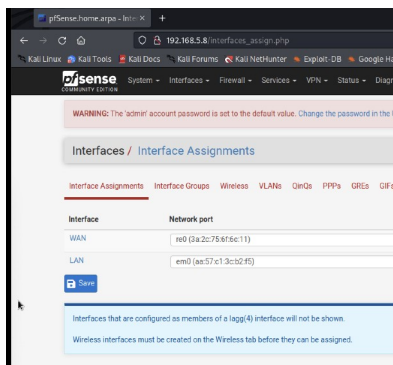
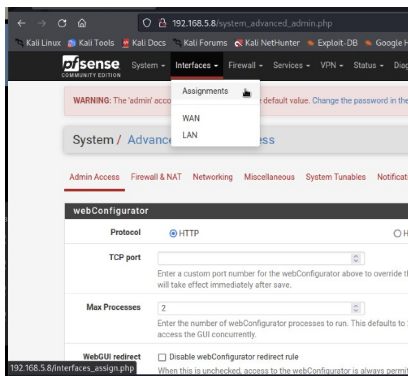
Una volta completata la configurazione delle regole e salvato tutto, procediamo con l'applicazione delle modifiche. Come si vede nell'immagine accanto a destra, è necessario cliccare sul pulsante “**Apply Changes**” per rendere effettive le nuove regole del firewall.

Questo step è fondamentale per assicurarsi che tutte le modifiche vengano applicate correttamente e che la configurazione del firewall entri in azione.



Assegnazione degli Indirizzi IP e Verifica delle Configurazioni WAN e LAN

Una volta applicate anche le ultime modifiche, possiamo proseguire con la **verifica delle assegnazioni degli indirizzi IP** per le interfacce **WAN** e **LAN**, come mostrato nell'immagine a sinistra. In questa fase, dobbiamo assicurarci che gli indirizzi IP siano stati correttamente configurati per entrambe le interfacce, in modo che la comunicazione tra le reti avvenga senza problemi.



Se tutto è stato configurato correttamente, dovremmo vedere gli indirizzi IP assegnati sia per la **WAN** (la connessione verso l'esterno) sia per la **LAN** (la rete interna). Questa assegnazione è cruciale per il funzionamento del firewall e per garantire che il traffico venga correttamente indirizzato.

Verifica del Funzionamento del Firewall tramite Ping

Al termine di questi ultimi passi, possiamo testare il funzionamento del Firewall eseguendo un **ping** dalla macchina **Linux** verso **Metasploit Table**. Questo test permette di verificare se il traffico tra le due macchine è correttamente gestito dal firewall.

Nel mio caso, purtroppo, non sono riuscito a completare correttamente la configurazione del firewall a causa di alcuni problemi tecnici. Come **controprova**, nell'immagine seguente, è possibile vedere l'effettivo collegamento di **ping** tra la macchina virtuale **Metasploit Table** e l'indirizzo IP della macchina **Linux**, che conferma che il traffico sta effettivamente passando, nonostante il firewall non fosse completamente operativo.

