

Configurazione di PFsense su VirtualBox per la Gestione di Reti e Firewall

In questa guida, verrà descritta l'installazione e la configurazione di PFsense su VirtualBox, con particolare attenzione alla gestione delle regole del firewall e delle reti. Le immagini delle configurazioni di LAN e LAN2 sono incluse a supporto della spiegazione.

Installazione di PFsense

1. Creazione della Macchina Virtuale:

- Avviare VirtualBox e creare una nuova macchina virtuale.
- Importare la ISO di PFsense e selezionarla come disco di avvio.

2. Configurazione delle Schede di Rete:

- Assegnare tre schede di rete alla macchina virtuale:
- Una per la WAN.
- Due per le LAN.
- Impostare la rete della WAN su "NAT".
- Impostare le reti delle due LAN su "Rete Interna" (ad esempio, "inet" e "inet2").

3. Installazione di PFsense:

- Avviare la macchina virtuale e seguire le istruzioni per l'installazione di PFsense.
- Dopo l'installazione, configurare le schede di rete:
- LAN1: IP 192.168.50.1.
- LAN2: IP 192.168.100.1.

Configurazione delle Macchine Virtuali

1. Configurazione di Metasploitable2:

- Avviare Metasploitable2 su VirtualBox e assegnarla alla rete interna "inet2".
- Impostare un IP statico IPv4 (192.168.100.101) e come gateway l'IP di PFsense (192.168.100.1).

2. Configurazione di Kali Linux:

- Avviare Kali Linux su VirtualBox e assegnarla alla rete interna "inet".
- Impostare un IP statico IPv4 (192.168.50.100) e come gateway l'IP di PFsense (192.168.50.1).

Configurazione delle Regole del Firewall su PFSense

1. Accesso all'interfaccia Web di PFSense:

- Da Kali Linux, aprire un browser e collegarsi all'indirizzo IP 192.168.50.1.
- Accedere all'interfaccia web di PFSense.

2. Impostazione delle Regole del Firewall:

- Configurare le regole del firewall per gestire il traffico tra le due LAN.

The screenshot shows the PFSense firewall rule configuration interface. The browser address bar displays the URL `192.168.50.1/firewall_rules_edit.php?id=1`. The form is for editing a rule with ID 1.

Action: Block

Disabled: ☐ Disable this rule

Interface: LAN

Address Family: IPv4

Protocol: TCP

Source: ☐ Invert match Address or Alias 192.168.50.100

Destination: ☐ Invert match Address or Alias 192.168.100.101

Destination Port Range: HTTP (80) From Custom To Custom

Extra Options: ☒ Log packets that are handled by this rule

Description: blocco_DVWA_da_Kali

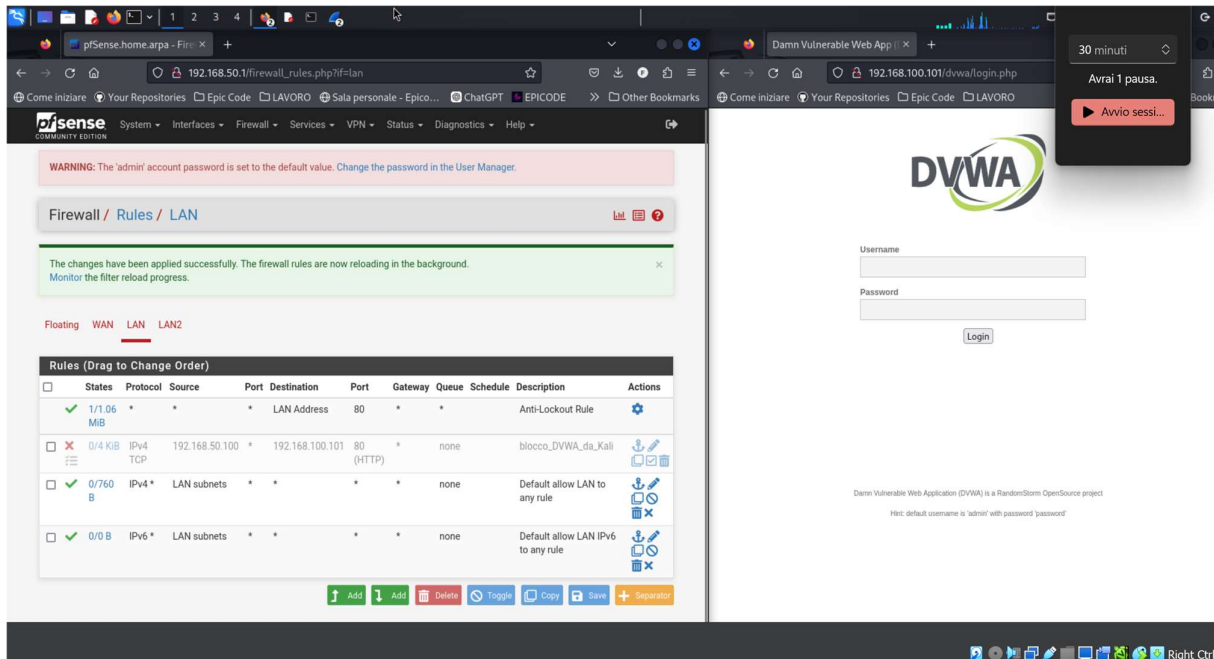
Rule Information:

Field	Value
Tracking ID	1720217372
Created	7/5/24 22:09:32 by admin@192.168.50.100 (Local Database)
Updated	7/6/24 13:41:40 by admin@192.168.50.100 (Local Database)

[Save](#)

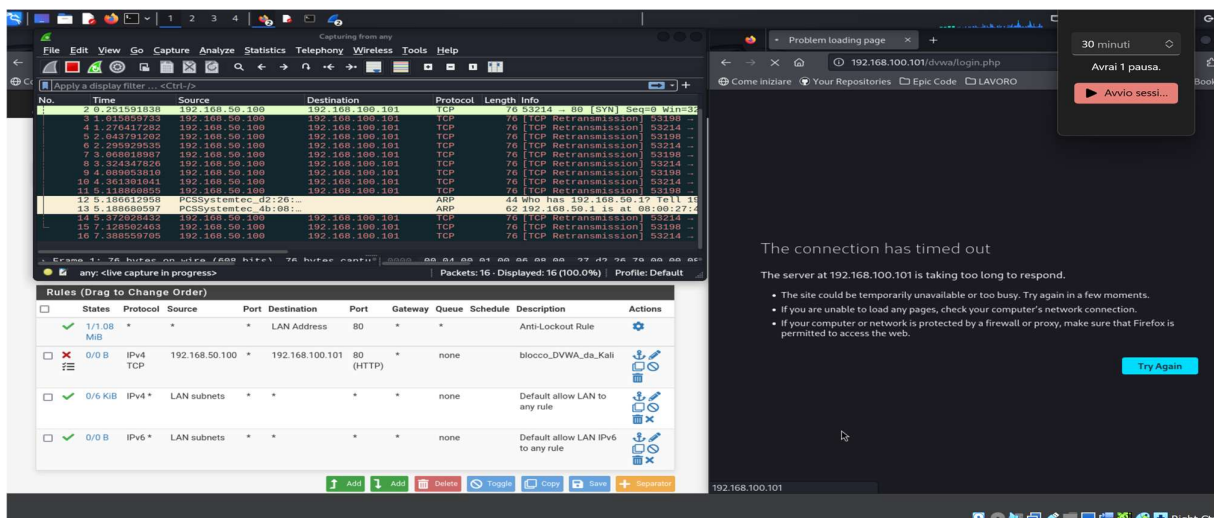
3. Regola di Blocco, con regola disabilitata:

- Lasciare la regola disattivata inizialmente per permettere la connessione a DVWA.



4. Attivazione della Regola di Blocco:

- Attivare la regola di blocco e verificare con Wireshark che la connessione viene effettivamente bloccata.
- Il browser su Kali Linux tenterà di connettersi a DVWA, ma le richieste non verranno risolte.



Verifica dei Log di PFSense

1. Controllo dei Log:

- Utilizzare lo strumento di log di PFSense per verificare le azioni delle regole del firewall.
- Come mostrato nella figura seguente, la connessione è stata bloccata dalla regola chiamata "blocco_DVWA_da_Kali".

The screenshot shows two browser windows. The left window displays the PFSense 'Status / System Logs / Firewall / Normal View' page. It lists the 'Last 500 Firewall Log Entries' with columns for Action, Time, Interface, Rule, Source, Destination, and Protocol. All entries show a blocked connection (red X) from 192.168.50.100 to 192.168.100.101:80 via the LAN interface, blocked by the rule 'blocco_DVWA_da_Kali (1720217372)'. The right window shows a 'Problem loading page' error for '192.168.100.101/dvwa/login.php' with the message 'The connection has timed out' and a 'Try Again' button.

Action	Time	Interface	Rule	Source	Destination	Protocol
✗	Jul 6 12:57:30	LAN	blocco_DVWA_da_Kali (1720217372)	192.168.50.100:43496	192.168.100.101:80	TCP:S
✗	Jul 6 12:57:31	LAN	blocco_DVWA_da_Kali (1720217372)	192.168.50.100:43488	192.168.100.101:80	TCP:S
✗	Jul 6 12:57:33	LAN	blocco_DVWA_da_Kali (1720217372)	192.168.50.100:43496	192.168.100.101:80	TCP:S
✗	Jul 6 12:57:33	LAN	blocco_DVWA_da_Kali (1720217372)	192.168.50.100:43488	192.168.100.101:80	TCP:S
✗	Jul 6 12:57:33	LAN	blocco_DVWA_da_Kali (1720217372)	192.168.50.100:43496	192.168.100.101:80	TCP:S
✗	Jul 6 12:57:37	LAN	blocco_DVWA_da_Kali (1720217372)	192.168.50.100:43488	192.168.100.101:80	TCP:S
✗	Jul 6 12:57:37	LAN	blocco_DVWA_da_Kali (1720217372)	192.168.50.100:43496	192.168.100.101:80	TCP:S
✗	Jul 6 12:57:45	LAN	blocco_DVWA_da_Kali (1720217372)	192.168.50.100:43488	192.168.100.101:80	TCP:S
✗	Jul 6 12:57:46	LAN	blocco_DVWA_da_Kali (1720217372)	192.168.50.100:43496	192.168.100.101:80	TCP:S

Con questa configurazione, le due macchine virtuali Kali e Metasploitable2 possono comunicare attraverso PFSense, e le regole del firewall possono essere gestite per controllare il traffico tra le diverse reti.