

Creazione regola firewall.

In questo esercizio ci viene chiesto di andare a creare una regola firewall che possa andare a bloccare l'accesso alla DVWA dalla macchina Kali Linux e che ne impedisca anche lo scan, specificando che Kali Linux e Metasploitable, siano connessi a due reti differenti.

Configurazione nuova interfaccia.

Per iniziare andremo subito a creare una nuova interfaccia a cui poi assoceremo le regole firewall.

Per eseguire ciò bisogna fare dei passaggi molto semplici.

Bisognerà recarsi sul sito di pfsense dove andremo poi ad accedere, in seguito andremo nella sezione “Interfaces” per poi arrivare alla sezione “Assignments”, da qui andando a cliccare su “Add” potremo andare a creare la nostra nuova interfaccia.

Interface Assignments

Interface Groups

Wireless

VLANs

QinQs

PPPs



GREs

GIFs

Bridges

LAGGs

Interface Groups

Name	Members	Description	Actions
lann	LAN	z	 

+

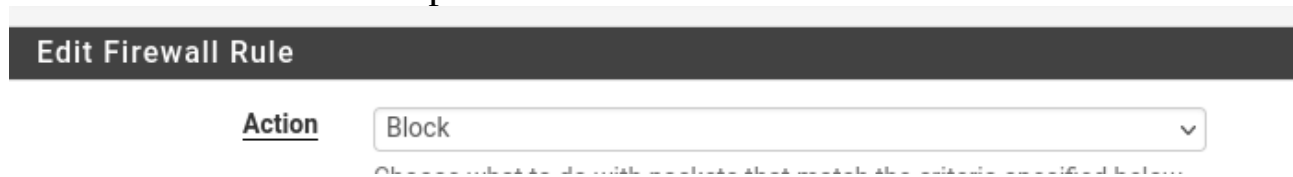
Add

In questo caso noi la siamo andati a chiamare “lann”.

Creazione regole firewall.

Per andare ad eseguire ciò, dovremo dirigerci nella sezione “Firewall” per poi proseguire nella sezione “Rules” andando a selezionare la nuova interfaccia creata, infine andremo anche in questo caso a cliccare su “Add” e ad iniziare a creare le nostre regole.

Inizieremo a configurarle andando ad impostare la sezione “Action” su “Block” come nell’esempio.



The screenshot shows the 'Edit Firewall Rule' window. The 'Action' dropdown menu is open, and 'Block' is selected. Below the dropdown, there is a partially visible line of text: 'Observe what is done with packets that match the criteria specified below'.

Per proseguire ci toccherà andare sulla sezione “Interface” e andare a selezionare la nostra interfaccia creata in precedenza “lann” come in esempio.



The screenshot shows the 'Interface' dropdown menu. The word 'lann' is selected and displayed in the dropdown box.

Andando avanti andremo a specificare l’indirizzo ip di Kali Linux dalla sezione “Source”.



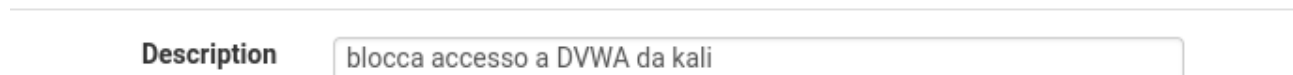
The screenshot shows the 'Source' configuration section. The 'Source' dropdown is set to 'Network'. The IP address '10.0.2.15' is entered in the adjacent field. There is also a checkbox for 'Invert match' which is unchecked.

Di seguito andremo a fare la stessa cosa con Metasploitable andando però nella sezione “Destination” e andremo poi a salvare.



The screenshot shows the 'Destination' configuration section. The 'Destination' dropdown is set to 'Network'. The IP address '10.0.2.15' is entered in the adjacent field. There is also a checkbox for 'Invert match' which is unchecked.

Infine andremo a mettere una descrizione alla regola.



The screenshot shows the 'Description' field. The text 'blocca accesso a DVWA da kali' is entered in the text box.

Blocco scan Kali.

Per proseguire, ora andremo a creare una regola firewall che ci permetta di bloccare lo scan dalla macchina Kali.

Per fare ciò dovremo sempre andare a creare una nuova regola come in precedenza.

Questa volta a differenza della prima, dovremo andare nella sezione “Protocol” e a selezionare “ICMP” ed infine avremo le nostre due regole e la nostra nuova interfaccia pronte.

FloatinglannWANLAN

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✗ 0/0 B	IPv4 TCP	10.0.2.15/24	*	*	*	*	none		blocca scan da kali	
<input type="checkbox"/>	✗ 0/0 B	IPv4 TCP	10.0.2.15/24	*	10.0.2.15/24	80 (HTTP)	*	none		blocca accesso a DVWA da kali	

Add AddDeleteToggleCopySave+ Separator

Interface AssignmentsInterface GroupsWirelessVLANsQinQsPPPsGREsGIFsBridgesLAGGs

Interface Groups

Name	Members	Description	Actions
lann	LAN	z	

+ Add

Prova.

Per andare a verificare il funzionamento delle regole, dovremo indirizzarci su Kali Linux ed andare a digitare il comando “curl http://10.0.2.15/dvwa”.

```
$ curl http://10.0.2.15/dvwa  
curl: (7) Failed to connect to 10.0.2.15 port 80 after 0 ms: Couldn't connect to server
```

Come possiamo andare a notare ci da un errore e questo vuol dire che le regole create e applicate sono andate a buon fine.

Conclusione.

Con questa configurazione, pfsense impedirà l'accesso alla DVWA sulla macchina Metasploitable dalla macchina Kali Linux e bloccherà gli scan provenienti da Kali Linux. La nuova interfaccia di rete permette di isolare meglio le due macchine su reti separate, e il firewall gestisce l'accesso in modo sicuro.