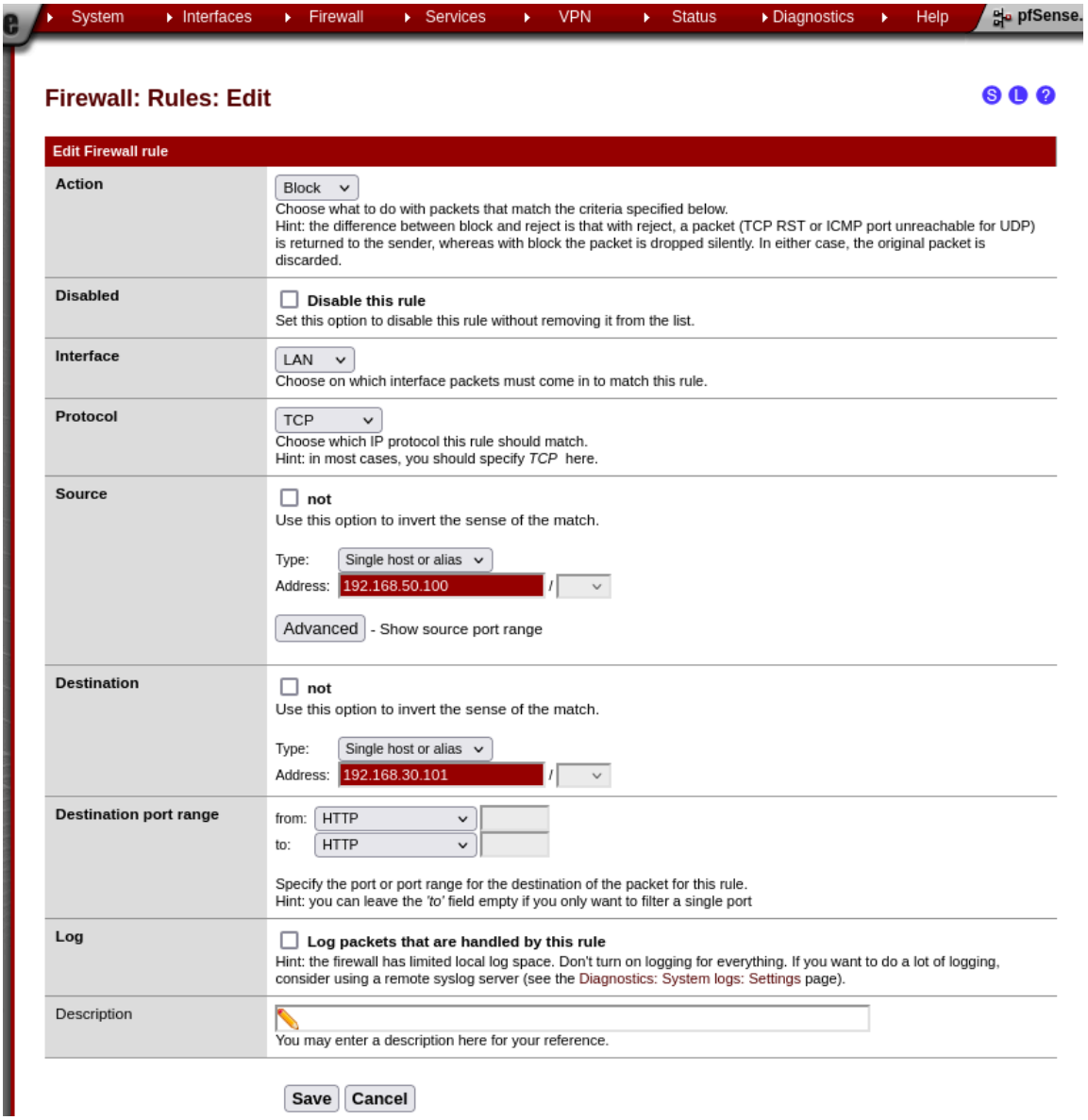
Nell'ambito di questo esercizio, è stato richiesto di configurare una regola firewall utilizzando PfSense al fine di impedire l'accesso alla Damn Vulnerable Web Application (DVWA) situata su Metasploitable dalla macchina Kali Linux. Inoltre, era fondamentale garantire che questo blocco impedisse qualsiasi tentativo di scansione della DVWA da parte di Kali Linux.

Per raggiungere questo obiettivo, abbiamo inizialmente configurato due reti separate su PfSense, isolando così le macchine Kali Linux e Metasploitable. Successivamente, è stata aggiunta un'interfaccia di rete aggiuntiva a PfSense per gestire una terza rete, necessaria per separare le due macchine.

Utilizzando PfSense, è stata quindi creata una regola firewall specifica per bloccare tutto il traffico proveniente dalla macchina Kali Linux diretto alla DVWA su Metasploitable. Ciò includeva il blocco di tutti i pacchetti provenienti dalla rete di Kali Linux indirizzati alla porta in cui DVWA era in ascolto.

Dopo l'implementazione della regola, è stato verificato che l'accesso alla DVWA da parte di Kali Linux fosse effettivamente bloccato. Inoltre, è stato testato che qualsiasi tentativo di scansione della DVWA da parte di Kali Linux fosse impedito dalla regola firewall.



System | Interfaces | Firewall | Services | VPN | Status | Diagnostics | Help | pfSense

Firewall: Rules

The settings have been applied. The firewall rules are now reloading in the background.
You can also monitor the reload progress

Close

Floating | WAN | LAN | OPT1

	ID	Proto	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
▶		*	*	*	LAN Address	22 80	*	*		Anti-Lockout Rule
☐ ▶		*	LAN net	*	*	*	*	none		Default allow LAN to any rule
☐ ✖		TCP	192.168.50.100	*	192.168.30.101	80 (HTTP)	*	none		

pass
pass (disabled)
block
block (disabled)
reject
reject (disabled)
log
log (disabled)

Hint:

Rules are evaluated on a first-match basis (i.e. the action of the first rule to match a packet will be executed). This means that if you use block rules, you'll have to pay attention to the rule order. Everything that isn't explicitly passed is blocked by default.