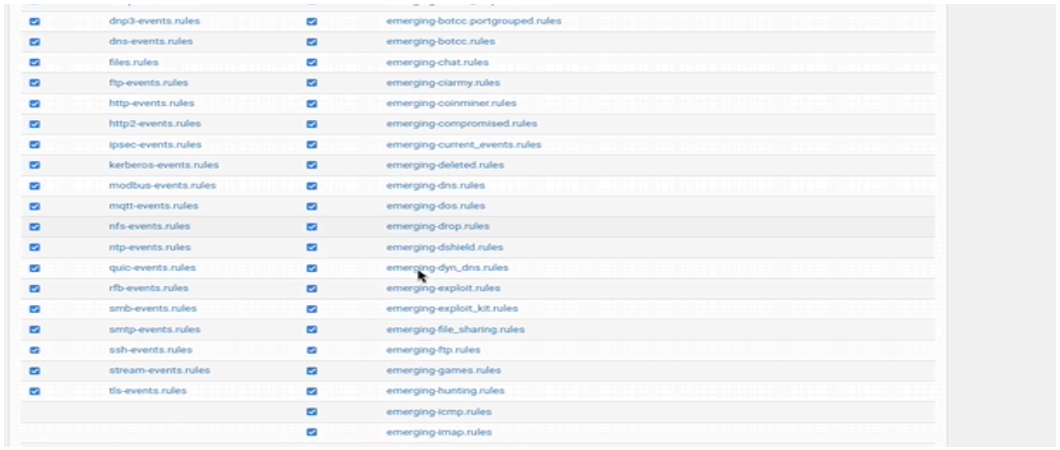
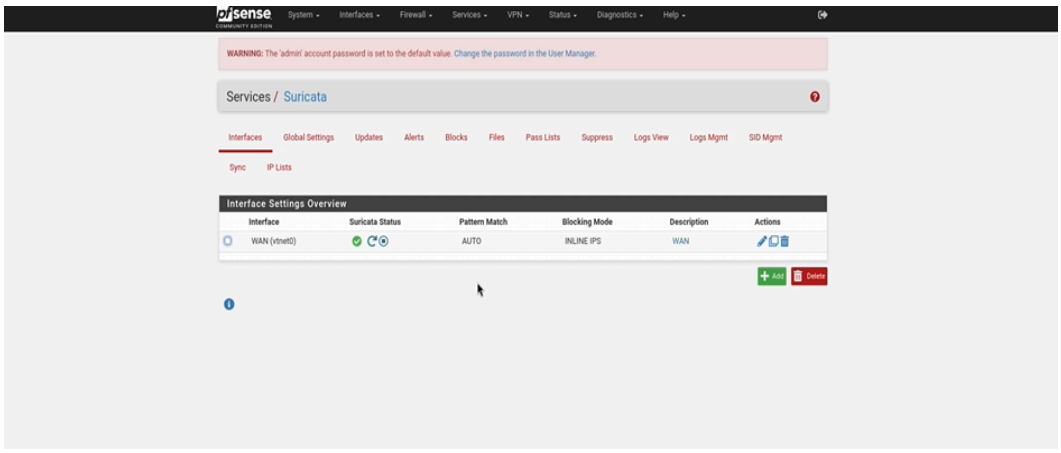
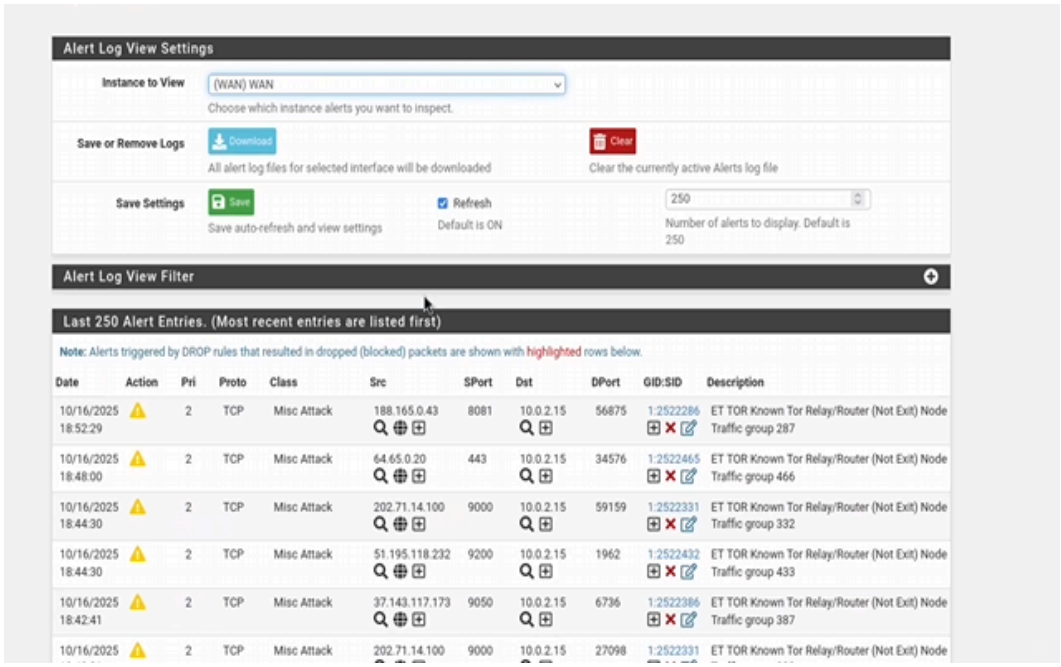
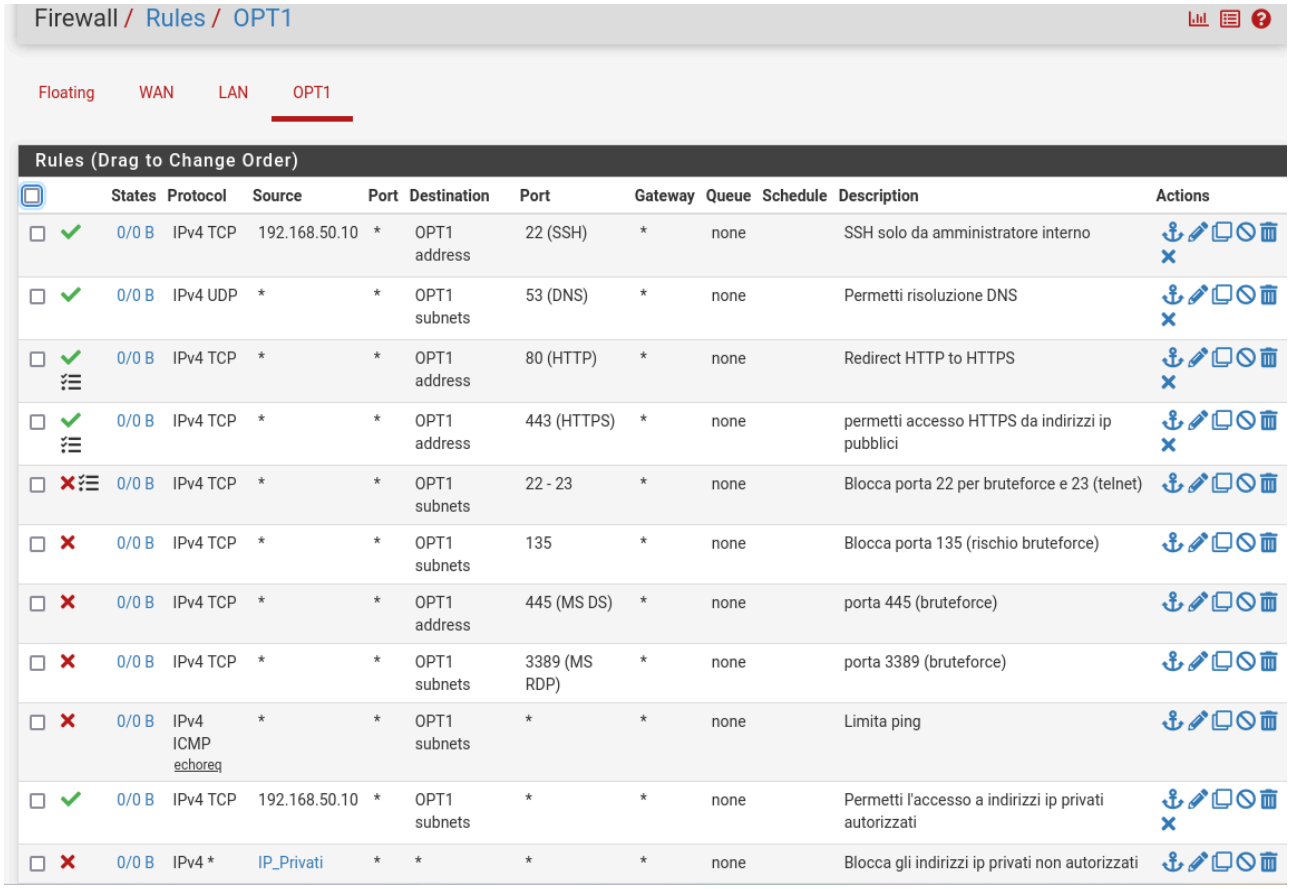
IPS CON SURICATA







pfSense



	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✓	0/0 B	IPv4 TCP	192.168.50.10	*	OPT1 address	22 (SSH)	*	none		SSH solo da amministratore interno	
✓	0/0 B	IPv4 UDP	*	*	OPT1 subnets	53 (DNS)	*	none		Permetti risoluzione DNS	
✓	0/0 B	IPv4 TCP	*	*	OPT1 address	80 (HTTP)	*	none		Redirect HTTP to HTTPS	
✓	0/0 B	IPv4 TCP	*	*	OPT1 address	443 (HTTPS)	*	none		permetti accesso HTTPS da indirizzi ip pubblici	
✗	0/0 B	IPv4 TCP	*	*	OPT1 subnets	22 - 23	*	none		Blocca porta 22 per bruteforce e 23 (telnet)	
✗	0/0 B	IPv4 TCP	*	*	OPT1 subnets	135	*	none		Blocca porta 135 (rischio bruteforce)	
✗	0/0 B	IPv4 TCP	*	*	OPT1 address	445 (MS DS)	*	none		porta 445 (bruteforce)	
✗	0/0 B	IPv4 TCP	*	*	OPT1 subnets	3389 (MS RDP)	*	none		porta 3389 (bruteforce)	
✗	0/0 B	IPv4 ICMP echoreq	*	*	OPT1 subnets	*	*	none		Limita ping	
✓	0/0 B	IPv4 TCP	192.168.50.10	*	OPT1 subnets	*	*	none		Permetti l'accesso a indirizzi ip privati autorizzati	
✗	0/0 B	IPv4 *	IP_Privati	*	*	*	*	none		Blocca gli indirizzi ip privati non autorizzati	

ESEMPIO DI CONFIGURAZIONE REGOLA

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 — ☐ Disable this rule

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

Interface — OPT1

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

Address Family — IPv4

Select the Internet Protocol version this rule applies to.

Protocol — TCP

Choose which IP protocol this rule should match.

Source

Source — ☐ Invert match | Any | Source Address | /

Display Advanced

The **Source Port Range** for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, **any**.

Destination

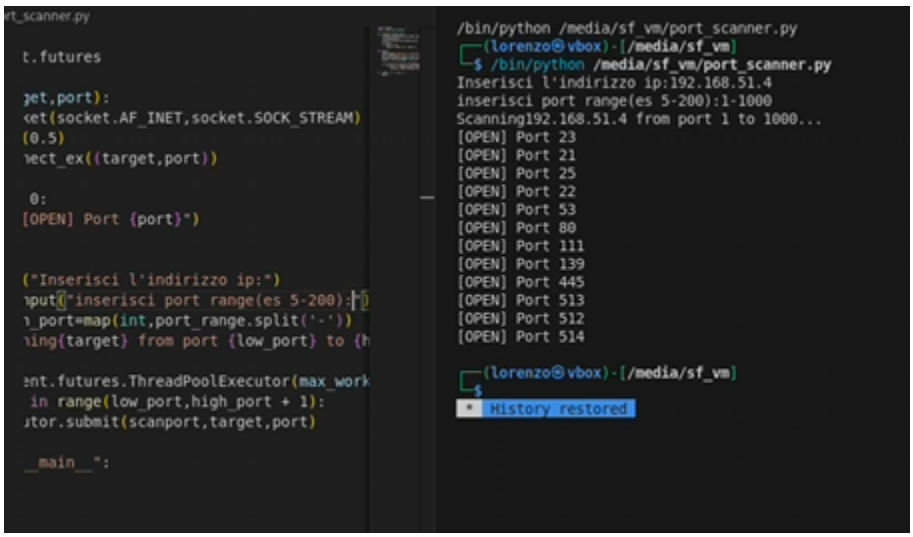
Destination — ☐ Invert match | OPT1 subnets | Destination Address | /

Destination Port Range — SSH (22) (From) | Custom | Telnet (23) (To) | Custom

Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.

Extra Options

PORT SCANNER



HTTP REQUEST e Sniffer credenziali

```
┌──(kali㉿kali)-[~/Documents]
└─$ sudo python HttpRequest_v3.py
Digita l'indirizzo IP del target (es. 192.168.20.10): 192.168.20.10
Digita il percorso della risorsa (es. /index.php o /mutillidae/): /dvwa/login.php

═══════════════════════════════════════════════════
Inizio la scansione dei verbi su: http://192.168.20.10/dvwa/login.php
═══════════════════════════════════════════════════

── Test con verbo: GET ──
Risposta: 200 OK

── Test con verbo: POST ──
Risposta: 200 OK

── Test con verbo: PUT ──
Risposta: 200 OK
⟹ ATTENZIONE! Il server ha risposto 200 OK a una richiesta potenzialmente pericolosa.

── Test con verbo: DELETE ──
Risposta: 200 OK
⟹ ATTENZIONE! Il server ha risposto 200 OK a una richiesta potenzialmente pericolosa.

═══════════════════════════════════════════════════
Scansione completata.
```

```
┌──(kali㉿kali)-[~/Documents]
┌──(kali㉿kali)-[~/Documents]
└─$ sudo python Sniffer_v2.py
Avvio sniffer per traffico HTTP (porta 80)... Premi CTRL+C per fermare.
Cercando dati di login...
──[ Pacchetto HTTP con possibili credenziali trovato! ]──
POST /dvwa/login.php HTTP/1.1
Host: 192.168.20.10
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:140.0) Gecko/20100101 Firefox/140.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 44
Origin: http://192.168.20.10
Connection: keep-alive
Referer: http://192.168.20.10/dvwa/login.php
Cookie: security=high; PHPSESSID=0b6c8cce668a738335e5db4274c99160
Upgrade-Insecure-Requests: 1
Priority: u=0, i

username=admin&password=password&Login=Login
──────────────────────────────────────────────────
──[ Pacchetto HTTP con possibili credenziali trovato! ]──
GET /dvwa/index.php HTTP/1.1
Host: 192.168.20.10
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:140.0) Gecko/20100101 Firefox/140.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.168.20.10/dvwa/login.php
Connection: keep-alive
Cookie: security=high; PHPSESSID=0b6c8cce668a738335e5db4274c99160
Upgrade-Insecure-Requests: 1
Priority: u=0, i
```

RETE CISCO PKT