

# IPS CON SURICATA

dns3-events.rules	dns-events.rules	files.rules	ftp-events.rules	http-events.rules	http2-events.rules	ipsec-events.rules	kerberos-events.rules	modbus-events.rules	mqtt-events.rules	nfs-events.rules	ntp-events.rules	quic-events.rules	rfb-events.rules	smb-events.rules	smtp-events.rules	ssh-events.rules	stream-events.rules	tls-events.rules	dns3-events.rules	dns-events.rules	files.rules	ftp-events.rules	http-events.rules	http2-events.rules	ipsec-events.rules	kerberos-events.rules	modbus-events.rules	mqtt-events.rules	nfs-events.rules	ntp-events.rules	quic-events.rules	rfb-events.rules	smb-events.rules	smtp-events.rules	ssh-events.rules	stream-events.rules	tls-events.rules	emerging-botcc.portgrouped.rules	emerging-botcc.rules	emerging-chat.rules	emerging-clammy.rules	emerging-colminer.rules	emerging-compromised.rules	emerging-current_events.rules	emerging-deleted.rules	emerging-dns.rules	emerging-dos.rules	emerging-drop.rules	emerging-dshield.rules	emerging-dyn_dns.rules	emerging-exploit.rules	emerging-exploit_kit.rules	emerging-file_sharing.rules	emerging-ftp.rules	emerging-games.rules	emerging-hunting.rules	emerging-icmp.rules	emerging-imap.rules
-------------------	------------------	-------------	------------------	-------------------	--------------------	--------------------	-----------------------	---------------------	-------------------	------------------	------------------	-------------------	------------------	------------------	-------------------	------------------	---------------------	------------------	-------------------	------------------	-------------	------------------	-------------------	--------------------	--------------------	-----------------------	---------------------	-------------------	------------------	------------------	-------------------	------------------	------------------	-------------------	------------------	---------------------	------------------	----------------------------------	----------------------	---------------------	-----------------------	-------------------------	----------------------------	-------------------------------	------------------------	--------------------	--------------------	---------------------	------------------------	------------------------	------------------------	----------------------------	-----------------------------	--------------------	----------------------	------------------------	---------------------	---------------------

Date	Action	Pri	Proto	Class	Src	SPort	Dst	DPort	GID:SID	Description
10/16/2025 18:52:29	⚠️	2	TCP	Misc Attack	188.165.0.43	8081	10.0.2.15	56875	1:2522286	ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 287
10/16/2025 18:48:00	⚠️	2	TCP	Misc Attack	64.65.0.20	443	10.0.2.15	34576	1:2522465	ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 466
10/16/2025 18:44:30	⚠️	2	TCP	Misc Attack	202.71.14.100	9000	10.0.2.15	59159	1:2522331	ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 332
10/16/2025 18:44:30	⚠️	2	TCP	Misc Attack	51.195.118.232	9200	10.0.2.15	1962	1:2522432	ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 433
10/16/2025 18:42:41	⚠️	2	TCP	Misc Attack	37.143.117.173	9050	10.0.2.15	6736	1:2522386	ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 387
10/16/2025	⚠️	2	TCP	Misc Attack	202.71.14.100	9000	10.0.2.15	27098	1:2522331	ET TOR Known Tor Relay/Router (Not Exit) Node

# pfSense

Firewall / Rules / OPT1



Floating WAN LAN OPT1

## Rules (Drag to Change Order)

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

## ESEMPIO DI CONFIGURAZIONE REGOLA

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

Address Family  Select the Internet Protocol version this rule applies to.

Protocol  Choose which IP protocol this rule should match.

**Source**

Source  Invert match  Source Address /

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  Destination Address /

Destination Port Range  From  To  To

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

The screenshot shows a terminal window with two panes. The left pane displays the source code of a Python script named `port_scanner.py`. The right pane shows the execution of the script and its output.

```
port_scanner.py
...
("Inserisci l'indirizzo ip:")
input()
port_range = input("Inserisci port range(es 5-200):")
low_port, high_port = map(int, port_range.split('-'))
target = input("Inserisci target ip:")
for port in range(low_port, high_port + 1):
    scan(target, port)

main_":
```

/bin/python ./media/sf\_vm/port\_scanner.py  
Inserisci l'indirizzo ip:192.168.51.4  
inserisci port range(es 5-200):1-1000  
Scanning 192.168.51.4 from port 1 to 1000...  
[OPEN] Port 23  
[OPEN] Port 21  
[OPEN] Port 25  
[OPEN] Port 22  
[OPEN] Port 53  
[OPEN] Port 80  
[OPEN] Port 111  
[OPEN] Port 139  
[OPEN] Port 445  
[OPEN] Port 513  
[OPEN] Port 512  
[OPEN] Port 514

History restored

# 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

