

S5 L1

Svolgimento Progetto

Giulia Salani

Consegna

[...] Creare una regola firewall che blocchi l'accesso alla DVWA (su metasploitable) dalla macchina Kali Linux e ne impedisca di conseguenza lo scan.

Un requisito fondamentale dell'esercizio è che le macchine Kali e Metasploitable siano su reti diverse, potete aggiungere una nuova interfaccia di rete a Pfsense in modo tale da gestire una ulteriore rete.

Connettetevi poi in Web Gui per attivare la nuova interfaccia e configurarla.

Svolgimento

Come prima cosa, procediamo ad installare pfSense come macchina virtuale su Oracle VM VirtualBox.

The screenshot shows a web browser window with the address bar displaying `pfsense.org/download/`. The browser's tab bar includes 'Pratica_S5-L1.pdf', 'Download pfSense Community', and 'Corsi'. The page features the pfSense logo and a navigation menu with links to 'Get Started', 'Cloud', 'Products', 'Services', 'Support', 'Training', 'Community', and 'Download'. A secondary menu at the top right includes 'Buy Cloud', 'Buy Appliance', 'Support', and 'Blog'. The main content area states: 'This is the most recent stable release, and the recommended version for all installations. Refer to the documentation for [Upgrade Guides](#) and [Installation Guides](#). For pre-configured systems, see the [pfSense® firewall appliances from Netgate](#).' Below this text are two buttons: 'RELEASE NOTES' and 'SOURCE CODE'. The 'Select Image To Download' section contains the following fields: 'Version: 2.7.2', 'Architecture: AMD64 (64-bit)', 'Installer: DVD Image (ISO) Installer', and 'Mirror: Austin, TX USA'. A blue 'DOWNLOAD' button is positioned below these fields. To the right of the download section is a 'Subscribe To The Netgate Newsletter' form, which includes a text input for 'Email Address', a checkbox for 'I understand I am signing up to receive the newsletter, software announcements, and special offers from Netgate.*', and a section titled 'I'm interested in...' with checkboxes for 'pfSense Plus Appliances' and 'TNSR Appliances'. The bottom of the image shows a Windows taskbar with a weather widget (5°C, Nuvoloso), a search bar, and various application icons. The system clock indicates 19:09 on 18/12/2023.

Pratica_S5-L1.pdf | Download pfSense Community | Corsi

pfsense.org/download/

READ LATER | Discord | CHINESE | Home Page - Red H... | Find email address... | Microsoft Word - co... | CISCO | BRUTE FORCE

Buy Cloud | Buy Appliance | Support | Blog

pfSense

Get Started | Cloud | Products | Services | Support | Training | Community | Download

This is the most recent stable release, and the recommended version for all installations. Refer to the documentation for [Upgrade Guides](#) and [Installation Guides](#). For pre-configured systems, see the [pfSense® firewall appliances from Netgate](#).

RELEASE NOTES | SOURCE CODE

Select Image To Download

Version: 2.7.2

Architecture: AMD64 (64-bit) ?

Installer: DVD Image (ISO) Installer

Mirror: Austin, TX USA

Supported by **netgate**

DOWNLOAD

Subscribe To The Netgate Newsletter

Product information, pfSense software announcements, and special offers. See our [newsletter archive](#) for past announcements.

Email*

Email Address

☐ I understand I am signing up to receive the newsletter, software announcements, and special offers from Netgate.*

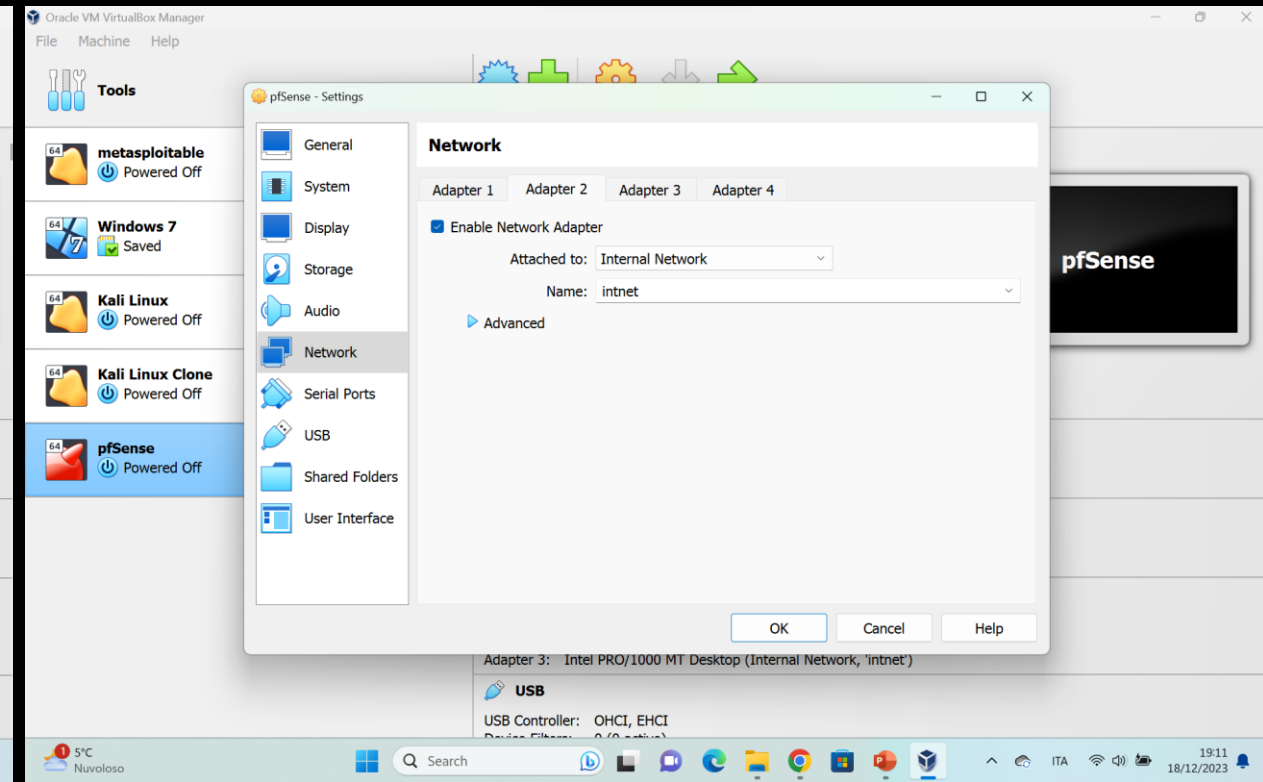
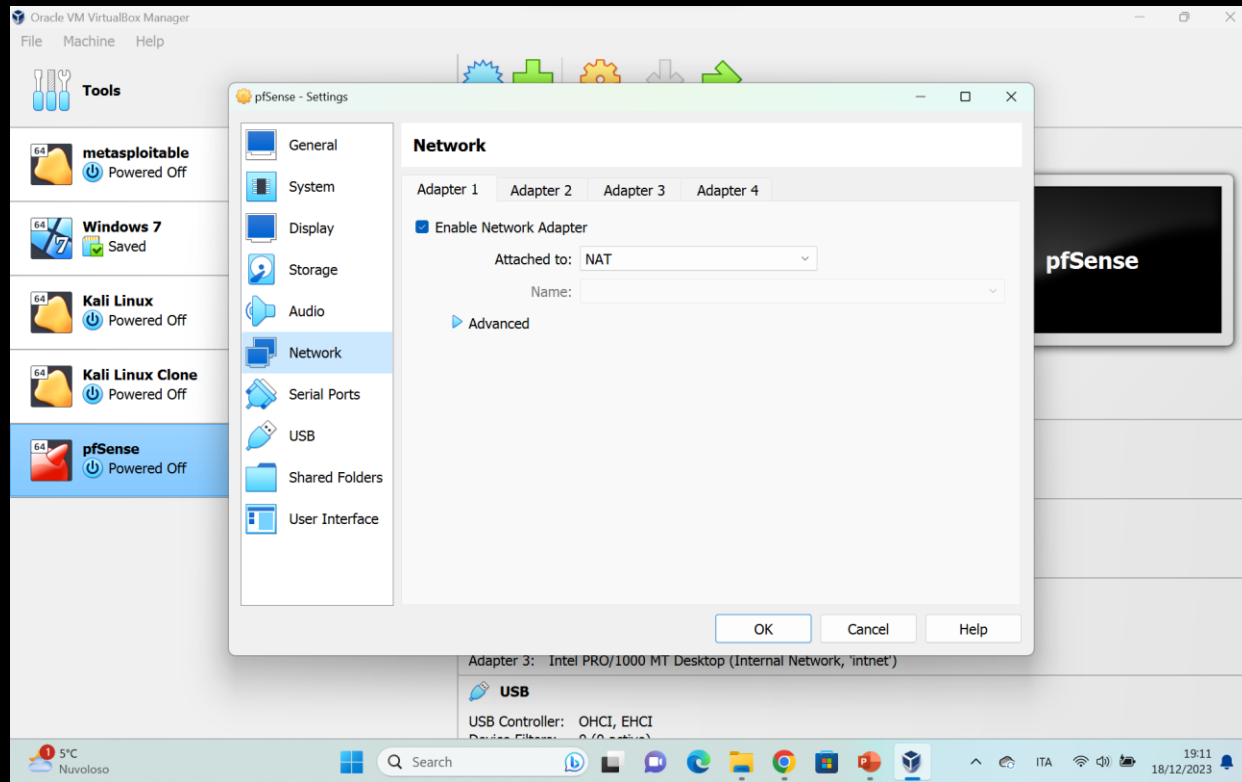
I'm interested in...

☐ pfSense Plus Appliances

☐ TNSR Appliances

5°C Nuvoloso | Search | 19:09 18/12/2023

Configuriamo due NIC sulla macchina virtuale: una interfaccia WAN e una interfaccia LAN.



Una volta installato pfSense, facciamo un ping da pfSense prima a google (screenshot di sx) poi a kali (screenshot di dx).

Prima di pingare Kali, è stato modificato il suo indirizzo IP e portato sulla stessa rete di pfSense.

```
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults  13) Update from console
5) Reboot system              14) Enable Secure Shell (sshd)
6) Halt system                15) Restore recent configuration
7) Ping host                  16) Restart PHP-FPM
8) Shell
```

Enter an option: 7

Enter a host name or IP address: www.google.com

```
PING www.google.com (216.58.204.228): 56 data bytes
64 bytes from 216.58.204.228: icmp_seq=0 ttl=109 time=146.065 ms
64 bytes from 216.58.204.228: icmp_seq=1 ttl=109 time=122.777 ms
64 bytes from 216.58.204.228: icmp_seq=2 ttl=109 time=389.950 ms

--- www.google.com ping statistics ---
3 packets transmitted, 3 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 122.777/219.597/389.950/120.832 ms
```

Press ENTER to continue.

```
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults  13) Update from console
5) Reboot system              14) Enable Secure Shell (sshd)
6) Halt system                15) Restore recent configuration
7) Ping host                  16) Restart PHP-FPM
8) Shell
```

Enter an option: 7

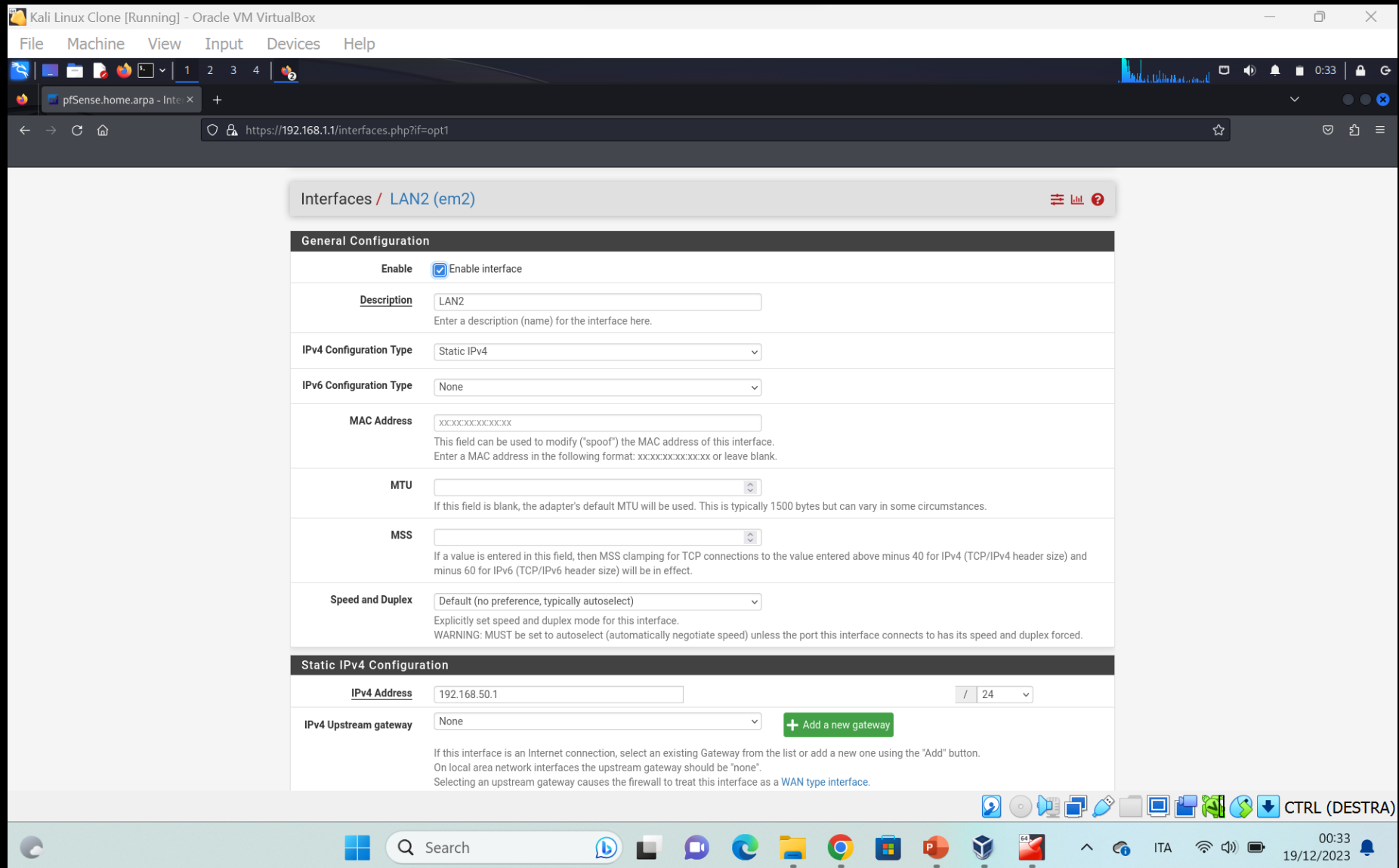
Enter a host name or IP address: 192.168.1.100

```
PING 192.168.1.100 (192.168.1.100): 56 data bytes
64 bytes from 192.168.1.100: icmp_seq=0 ttl=64 time=2.895 ms
64 bytes from 192.168.1.100: icmp_seq=1 ttl=64 time=1.182 ms
64 bytes from 192.168.1.100: icmp_seq=2 ttl=64 time=1.056 ms

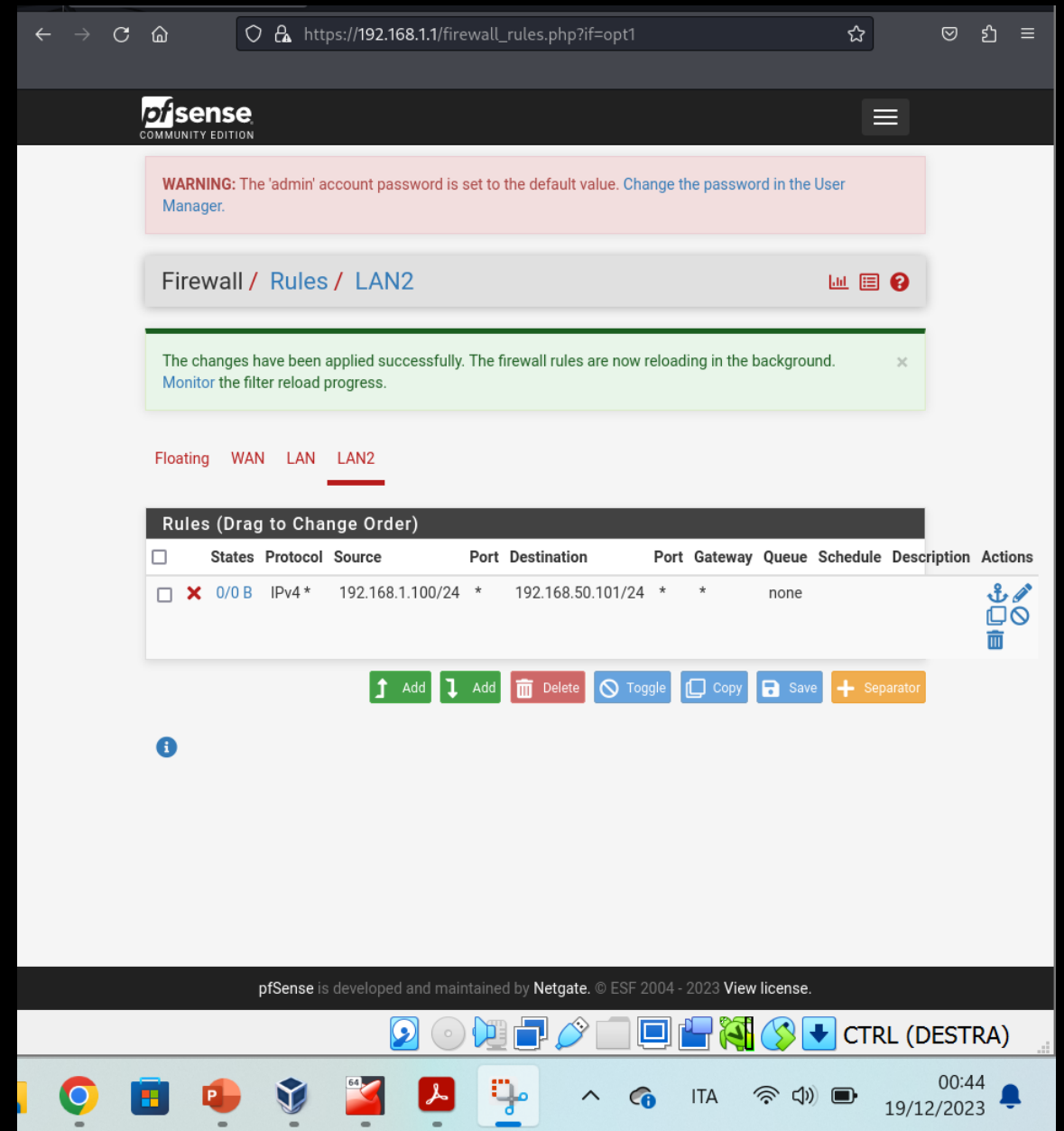
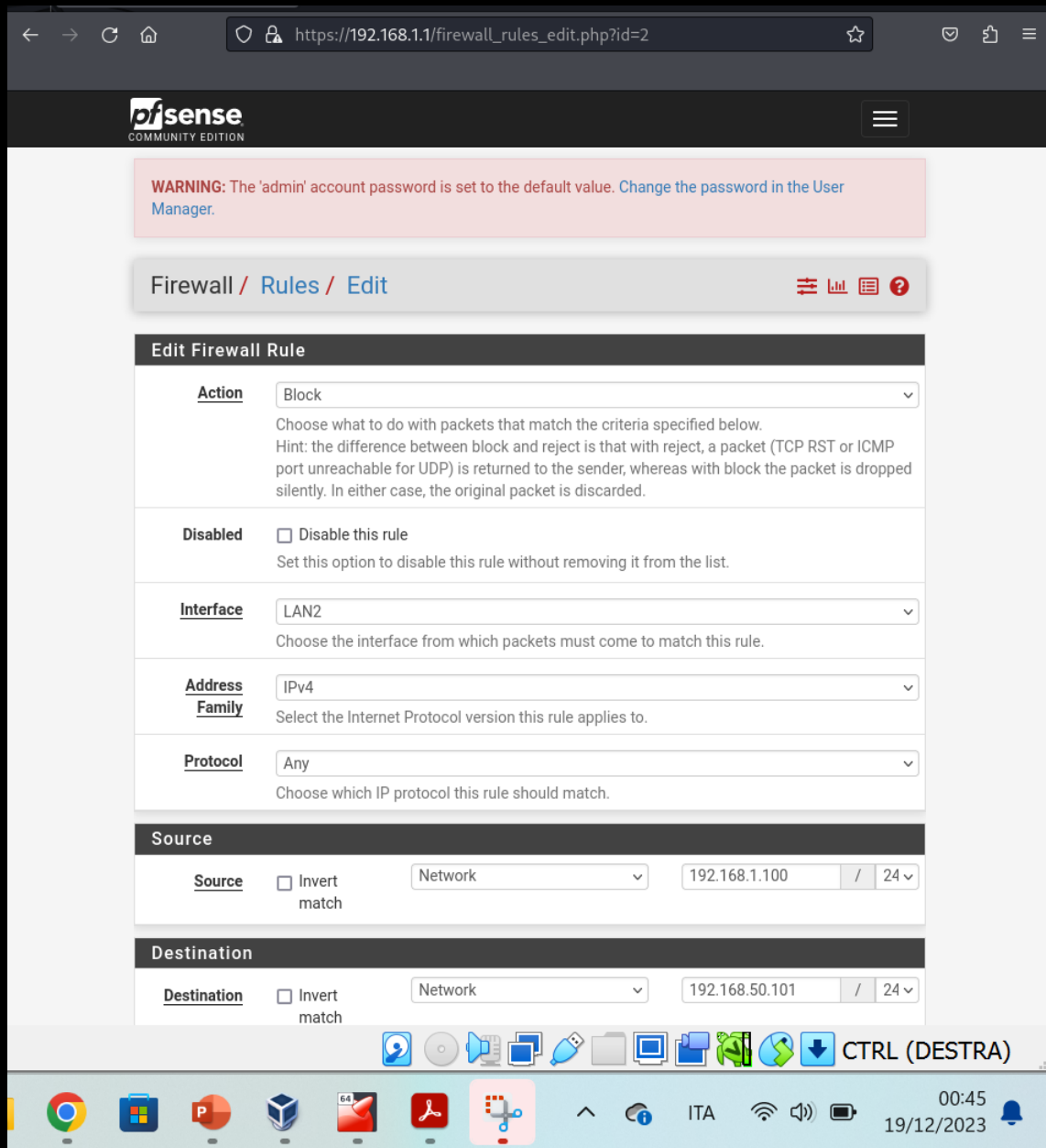
--- 192.168.1.100 ping statistics ---
3 packets transmitted, 3 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 1.056/1.711/2.895/0.839 ms
```

Press ENTER to continue.

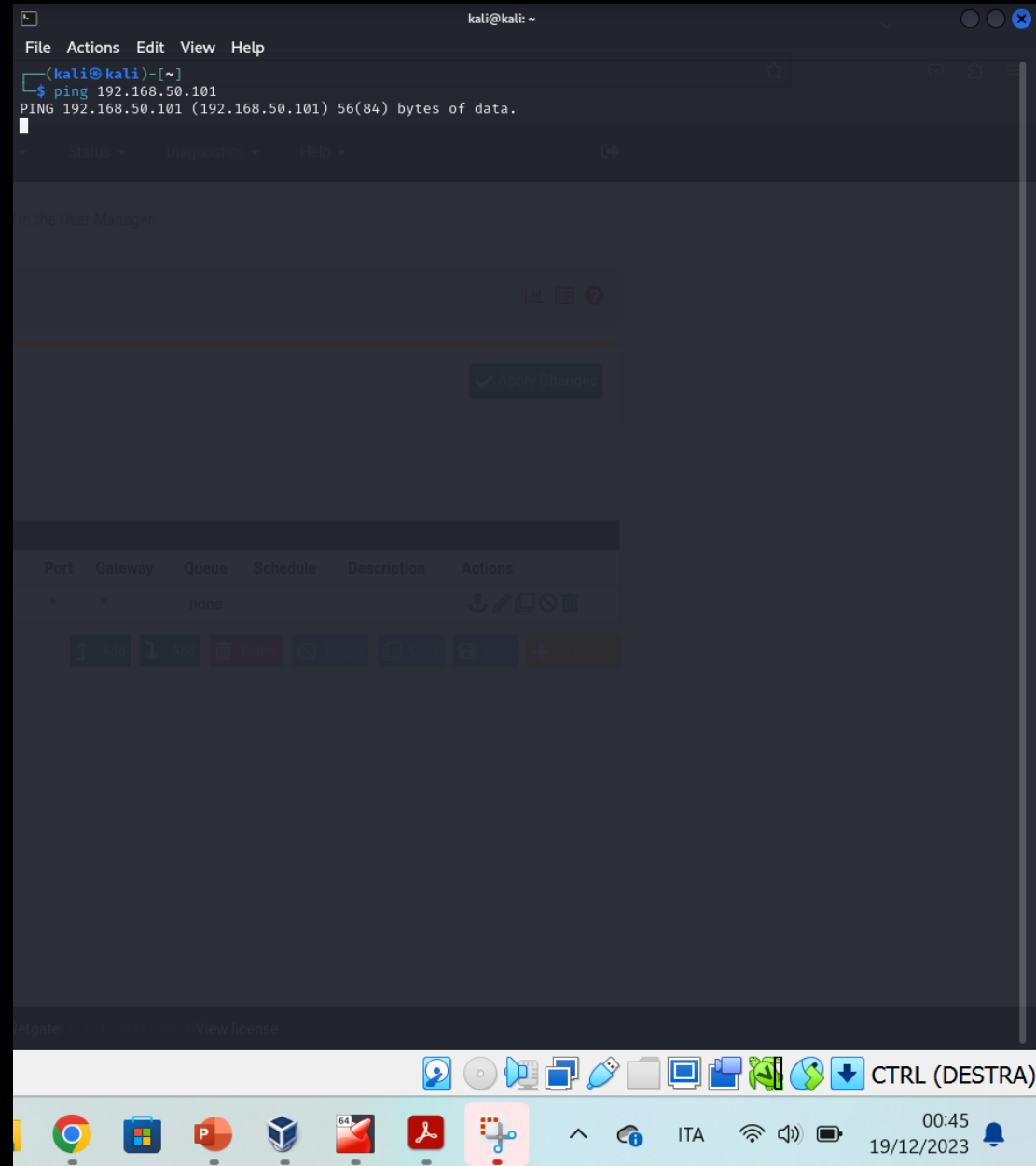
Creiamo ora una terza NIC su pfSense, sempre internal. La configureremo dalla webGUI di pfSense, nel tab «interfaces». Questa volta, l'IP è sulla rete di metasploitable.



A questo punto creiamo una nuova regola nel tab firewall della WebGUI pfSense, con cui blocchiamo la connessione da Kali (IP source) a meta (IP destination):



Proviamo quindi a pingare meta, ma il ping non viene lasciato passare dal firewall. Se fosse stato un problema di configurazione, invece, l'host sarebbe risultato unreachable:



The screenshot shows a Kali Linux terminal window with the title 'kali@kali: ~'. The terminal output is as follows:

```
File Actions Edit View Help
(kali@kali)-[~]
└─$ ping 192.168.50.101
PING 192.168.50.101 (192.168.50.101) 56(84) bytes of data.
```

The terminal window is overlaid on a desktop environment. The desktop background is dark. At the bottom, there is a taskbar with various application icons including Google Chrome, a file manager, a presentation application, a terminal, a PDF reader, and a system tray with icons for network, volume, and battery. The system tray also displays the time '00:45' and the date '19/12/2023'. A 'CTRL (DESTRA)' label is visible on the right side of the taskbar.