Mise en place d'un Pare-feu Logiciel sur VM - Renforcement de la Sécurité Informatique

1. Contexte

Rappel

Pfsense ping les 2 VMs Linux.
Les 2 machines Linux ping l'adresse du LAN de Pfsense.
La machine cliente a accès à l'interface Web de Pfsense.
Les 2 machines ont accès à internet.

Livrables

Le livrable commencera par un rappel du contexte, et le sommaire comportera les points suivants : Un premier point définissant les termes NAT, WAN, LAN, et Firewall. Un second point présentant un schéma de l'infrastructure mise en place (réaliser avec draw.io par exemple). Un troisième point présentera l'installation et la configuration du firewall pfSense. Un quatrième point illustrera les tests de validation demandés.

2. Définitions

NAT (Network Address Translation) :

Le **NAT** est une technique qui permet de traduire les adresses IP privées d'un réseau local en adresses IP publiques avant l'accès à Internet. Cela permet de faire transiter le trafic d'un ensemble de machines avec des adresses IP privées via une seule adresse IP publique.

WAN (Wide Area Network) :

Un **WAN**, ou réseau étendu, est un réseau informatique couvrant une grande zone géographique, généralement interconnectant des réseaux locaux (LAN) distants. Internet est l'exemple typique d'un WAN public.

LAN (Local Area Network) :

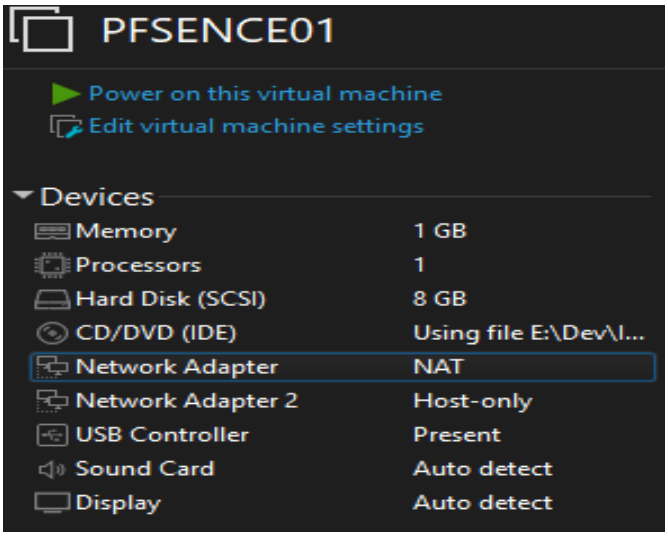
Un **LAN**, ou réseau local, est un réseau informatique privé couvrant une zone géographique restreinte, comme un bureau, un bâtiment ou un site. Les machines d'un **LAN** partagent la même plage d'adresses IP privées.

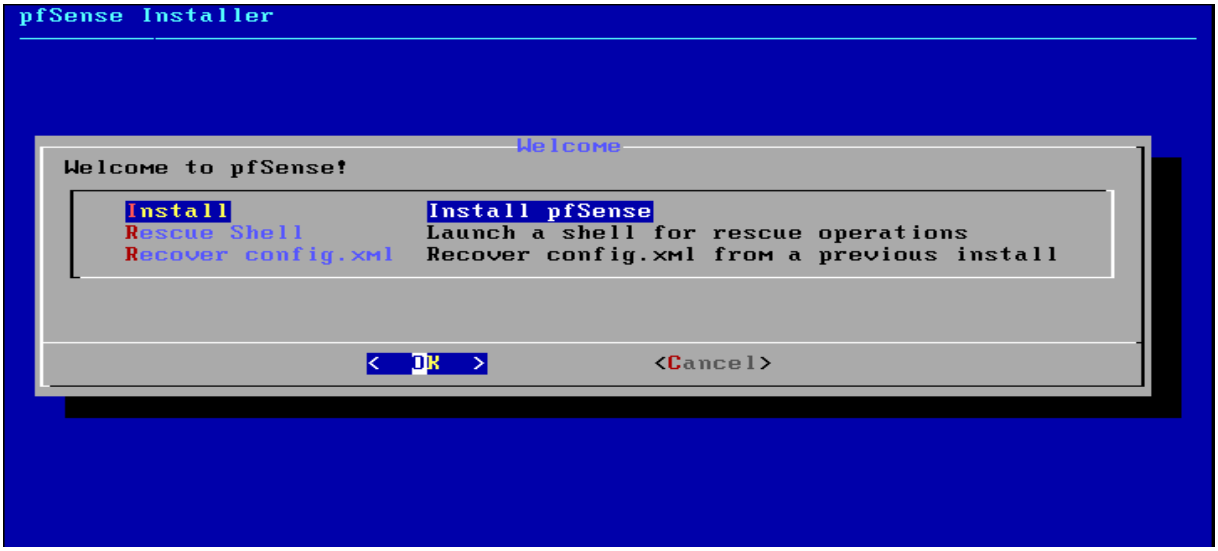
Firewall :

Un **firewall** (pare-feu) est un dispositif de sécurité réseau qui surveille et filtre le trafic entrant et sortant selon un ensemble de règles prédéfinies. Il agit comme une barrière de protection entre un réseau privé (LAN) et un réseau public (WAN/Internet), permettant ou bloquant les connexions selon les besoins.

3. Schéma de l'infrastructure

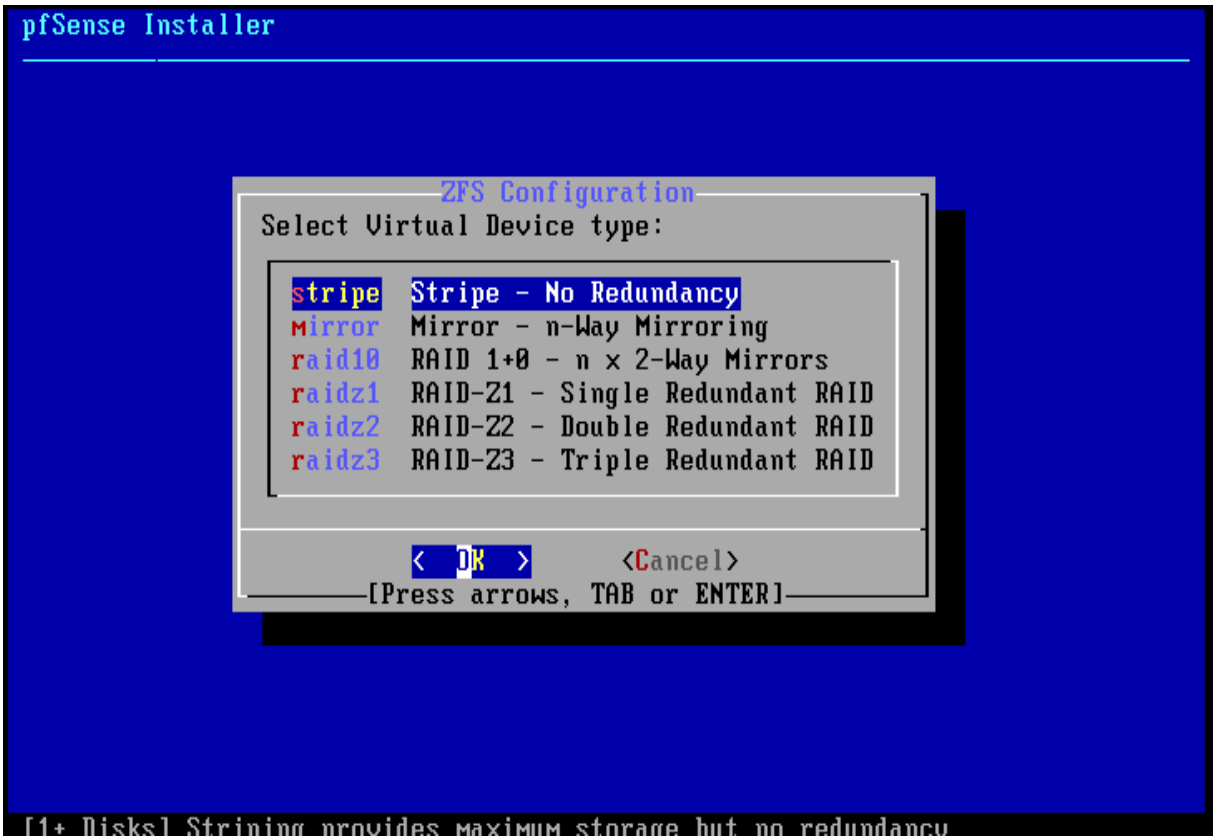
4. Installation et configuration de pfSense

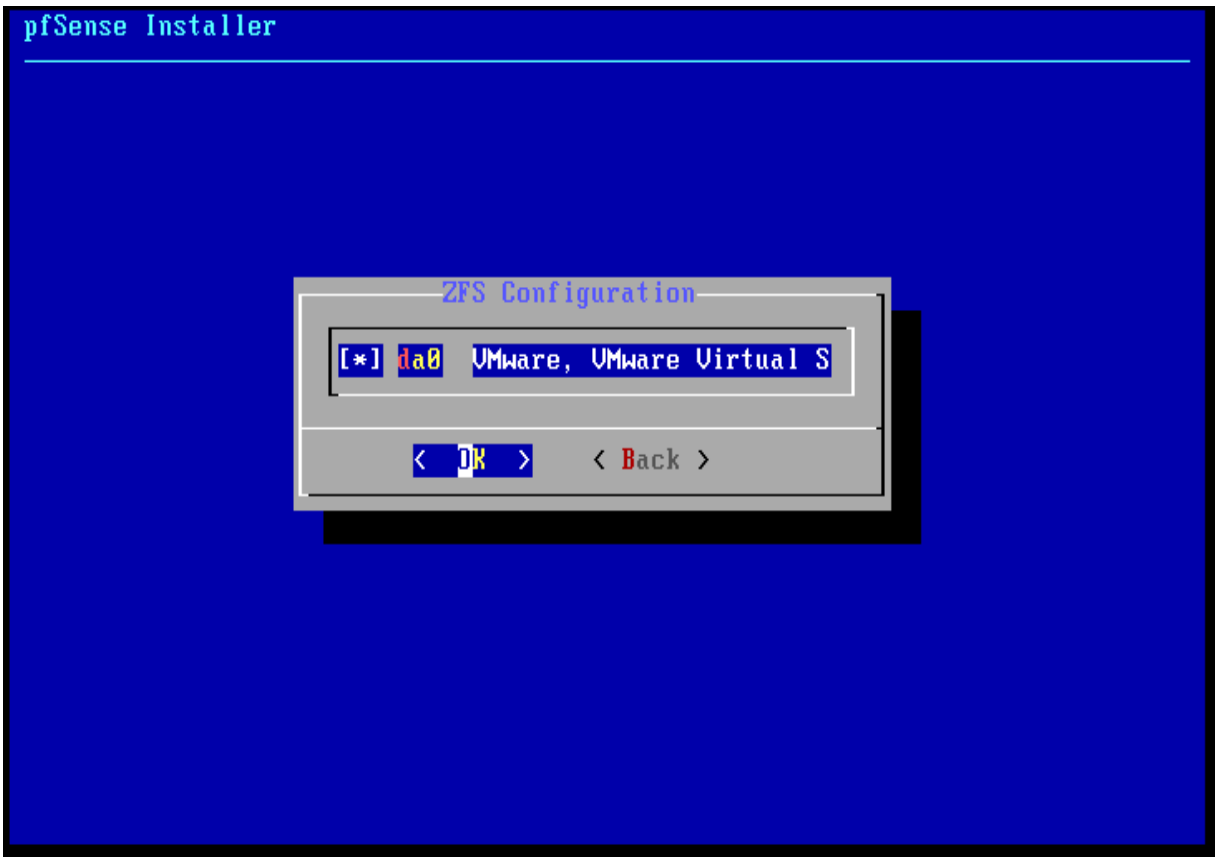




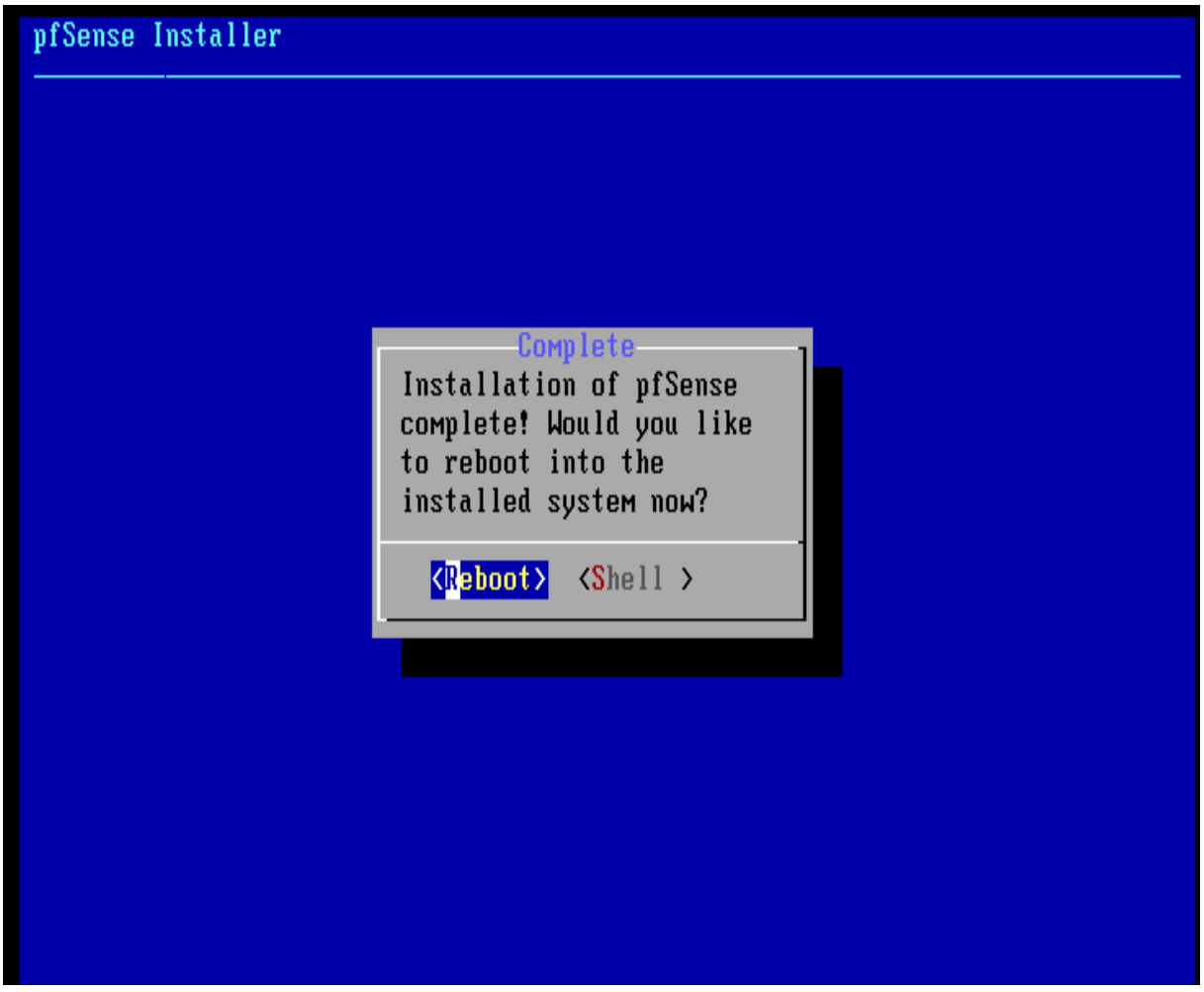

pfSense Installer
Keymap Selection
The system console driver for pfSense defaults to standard "US"
keyboard map. Other keymaps can be chosen below.
( ) Estonian
( ) Finnish
( ) French
( ) French (MacBook/MacBook Pro) (accent keys)
( ) French (accent keys)
( ) French Canadian (accent keys)
( ) French Dvorak-like
( ) French Dvorak-like (accent keys)
( ) German
( ) German (accent keys)
( ) German (no accent keys)
( ) Greek (101 keys)
36%
<Select>
<Cancel>
[Press arrows, TAB or ENTER]


pfSense Installer
Partitioning
How would you like to partition your disk?
Auto (ZFS) Guided Root-on-ZFS
Auto (UFS) BIOS Guided Disk Setup using BIOS boot method
Auto (UFS) UEFI Guided Disk Setup using UEFI boot method
Manual Manual Disk Setup (experts)
Shell Open a shell and partition by hand
< OK >
<Cancel>


pfSense Installer
ZFS Configuration
Select Virtual Device type:
stripe Stripe - No Redundancy
mirror Mirror - n-Way Mirroring
raid10 RAID 1+0 - n x 2-Way Mirrors
raidz1 RAID-Z1 - Single Redundant RAID
raidz2 RAID-Z2 - Double Redundant RAID
raidz3 RAID-Z3 - Triple Redundant RAID
< OK > <Cancel>
[Press arrows, TAB or ENTER]
[1+ Disks] Striping provides maximum storage but no redundancy


pfSense Installer
ZFS Configuration
[*] da0 VMware, VMware Virtual S
< OK > < Back >

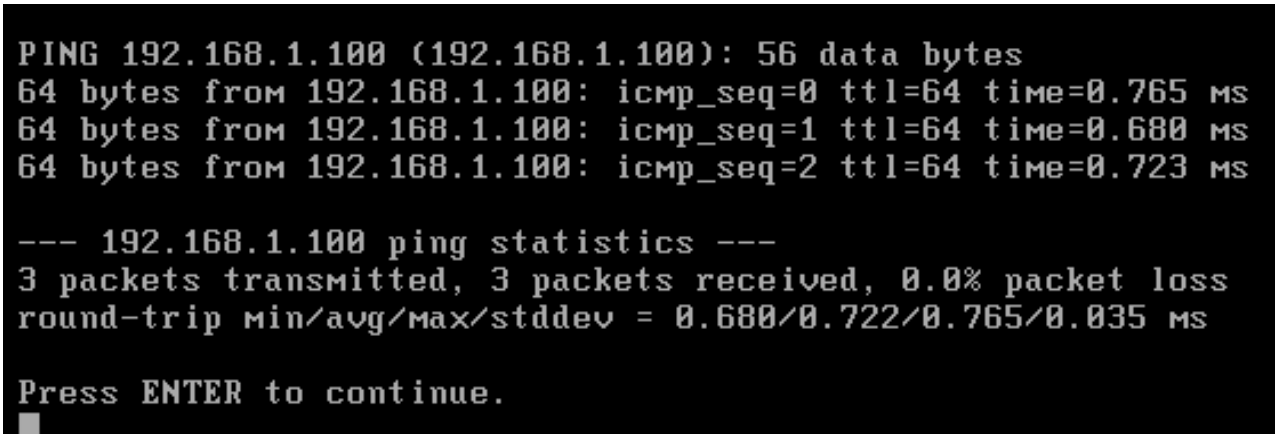

pfSense Installer
ZFS Configuration
Last Chance! Are you sure you want to destroy
the current contents of the following disks:
da0
< YES >
< NO >
[Press arrows, TAB or ENTER]


pfSense Installer
Complete
Installation of pfSense
complete! Would you like
to reboot into the
installed system now?
<Reboot>
<Shell >

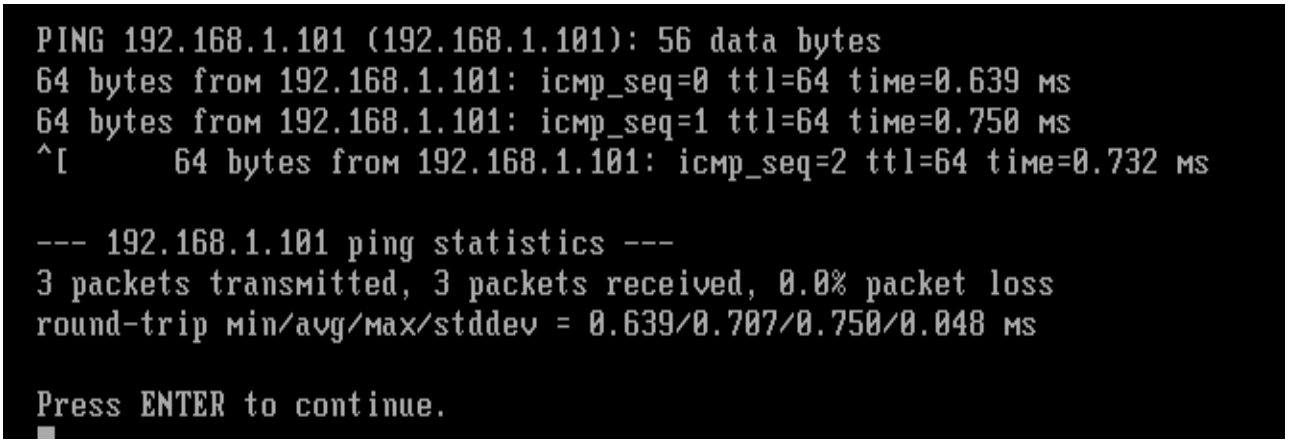
5. Tests de validation

- Ping de pfSense vers les machines Client et Serveur

UBUNTU 22

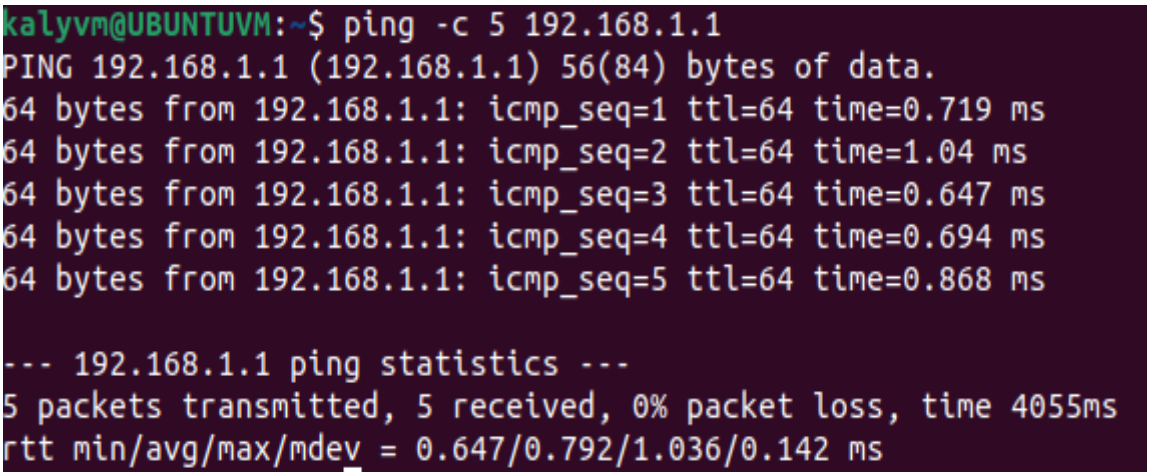


DEBIAN 12



- Ping des machines vers l'IP LAN de pfSense

UBUNTU 22



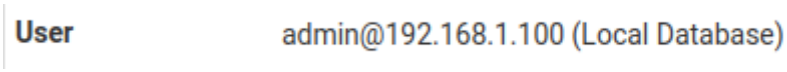
DEBIAN 12

```
kalyvm@debian:~$ ping -c 5 192.168.1.1
PING 192.168.1.1 (192.168.1.1) 56(84) bytes of data.
64 bytes from 192.168.1.1: icmp_seq=1 ttl=64 time=0.751 ms
64 bytes from 192.168.1.1: icmp_seq=2 ttl=64 time=0.617 ms
64 bytes from 192.168.1.1: icmp_seq=3 ttl=64 time=0.701 ms
64 bytes from 192.168.1.1: icmp_seq=4 ttl=64 time=0.638 ms
64 bytes from 192.168.1.1: icmp_seq=5 ttl=64 time=0.687 ms

--- 192.168.1.1 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4057ms
rtt min/avg/max/mdev = 0.617/0.678/0.751/0.047 ms
```

- Accès à l'interface web de pfSense depuis le Client

UBUNTU 22



- Vérification de la connectivité Internet pour le Client et Serveur

UBUNTU 22

```
kalyvm@UBUNTUVM:~$ ping -c 5 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=127 time=7.81 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=127 time=7.65 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=127 time=7.41 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=127 time=8.92 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=127 time=8.07 ms

--- 8.8.8.8 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4008ms
rtt min/avg/max/mdev = 7.407/7.972/8.922/0.521 ms
```

DEBIAN 12

```
kalyvm@debian:~$ ping -c 5 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=127 time=7.25 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=127 time=7.08 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=127 time=8.46 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=127 time=8.39 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=127 time=8.77 ms

--- 8.8.8.8 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4010ms
rtt min/avg/max/mdev = 7.077/7.989/8.768/0.688 ms
```