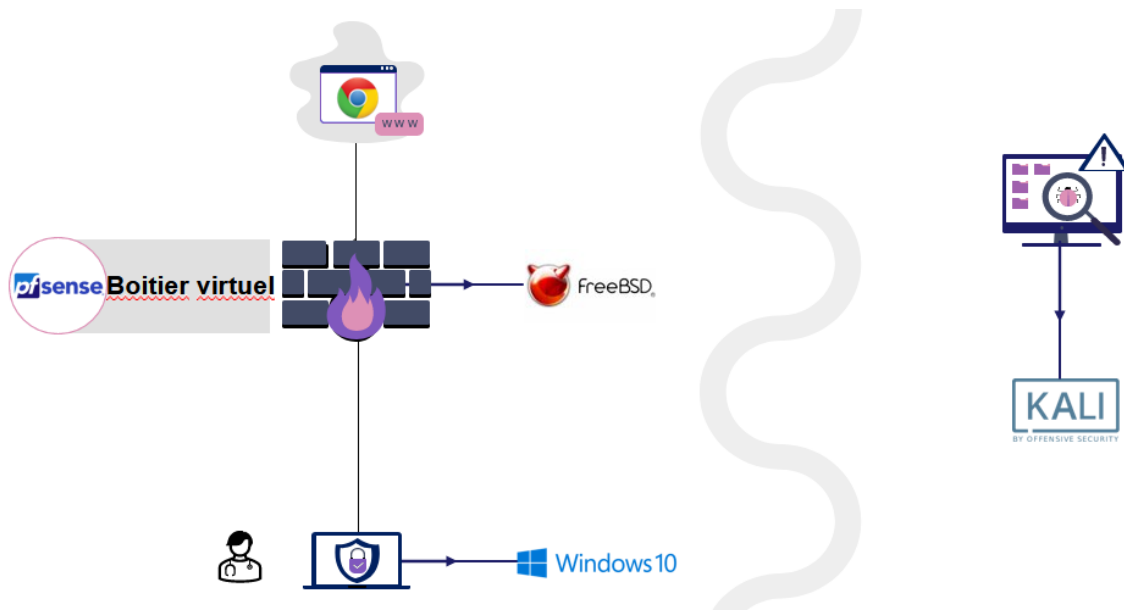


Infrastructure

Pour réaliser le projet, nous aurons besoin d'une infrastructure. Pour mieux nous adapter à la demande du client, aux contraintes et pour mieux nous concentrer sur les solutions, nous allons proposer les solutions à partir de l'infrastructure suivant :



L'infrastructure est d'abord constituée d'un routeur sous FreeBSD (Système d'exploitation UNIX libre) connecté à internet. Dans ce routeur, nous allons installer **pfSense** de sorte que notre routeur joue le rôle du pare-feu (ce sera notre boîtier virtuel qui agira en tant que rempart contre les ransomwares).

Notre infrastructure sera également constituée d'un ordinateur client sous Windows : c'est l'ordinateur qui contient les données critiques que nous devons à tout pris protéger contre les ransomwares.

Enfin nous aurons une machine externe au schéma principal sous KALI Linux que nous utiliserons pour tester le niveau de sécurité de notre infrastructure. En effet nous allons tester notre solution en faisant principalement une attaque par intrusion.

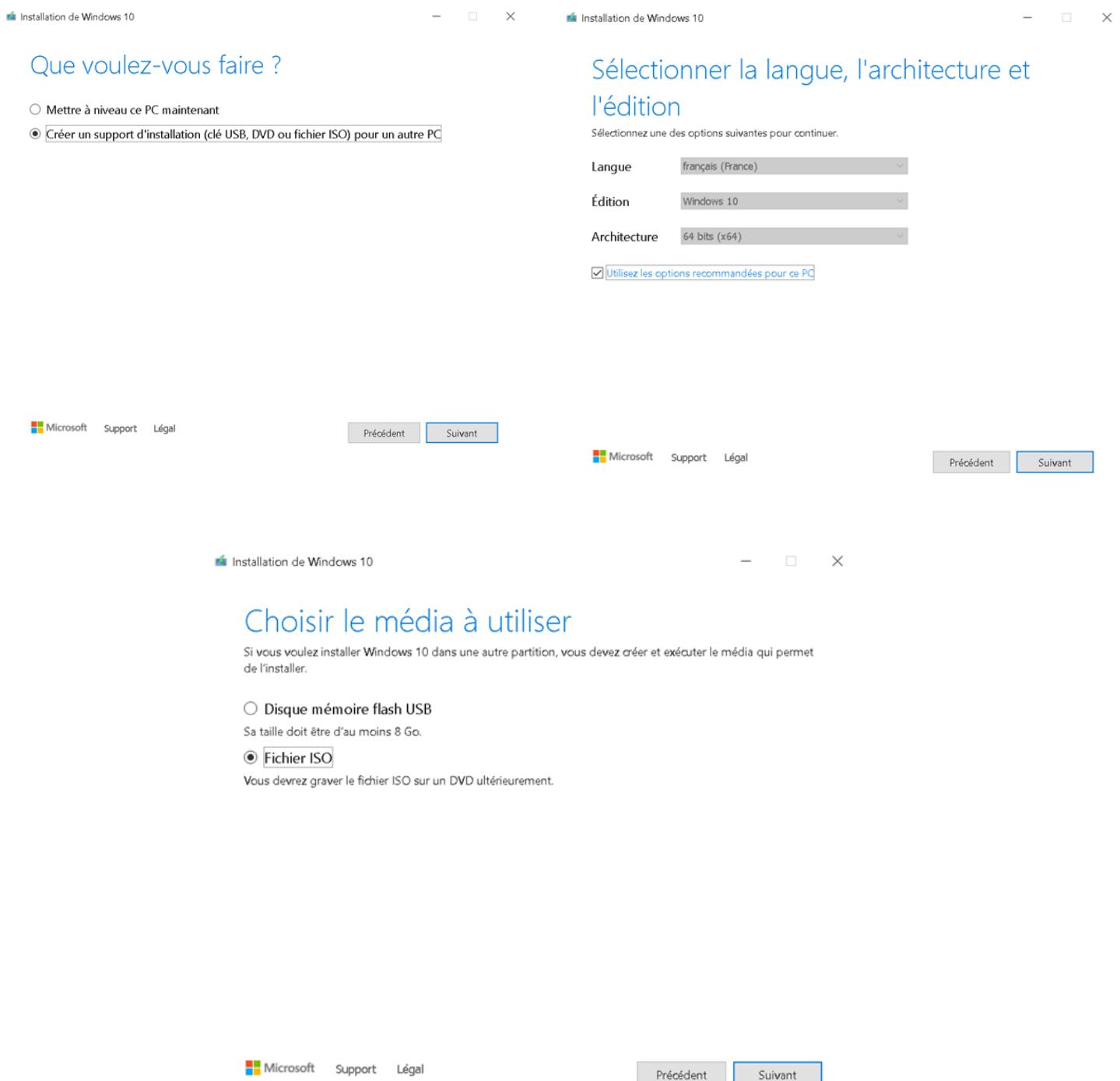
Pour modéliser notre solution, nous allons utiliser trois machines virtuelles sous virtualbox.

Installation Windows sur la machine cliente

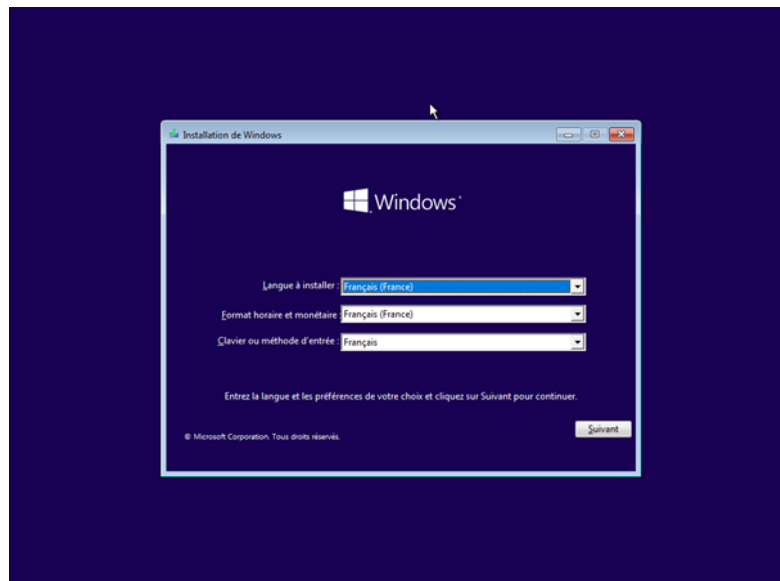
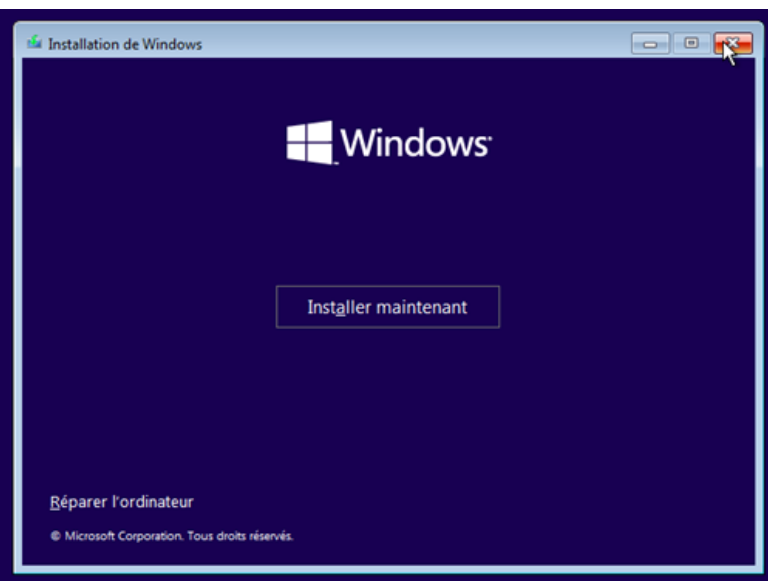
Avant de configurer notre machine cliente, nous téléchargeons l'**image ISO de Windows 10** et créer une nouvelle machine virtuelle à partir de cette image ISO. Nous téléchargeons le fichier d'installation windows 10 fournit par le lien ci-dessous:

<https://go.microsoft.com/fwlink/?LinkId=691209>

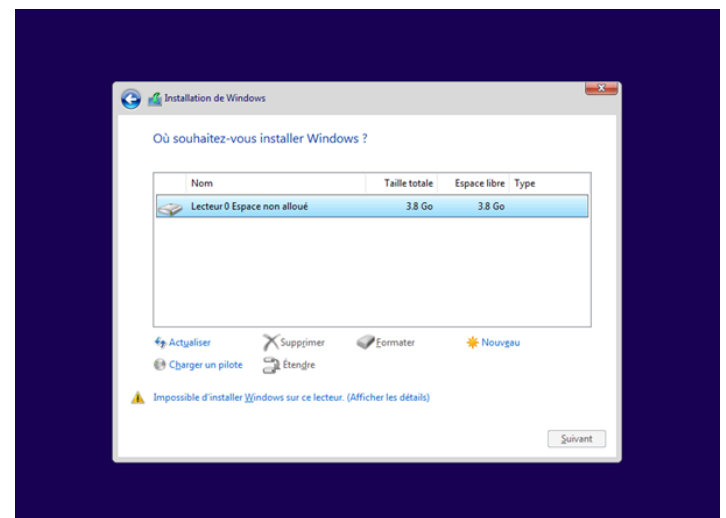
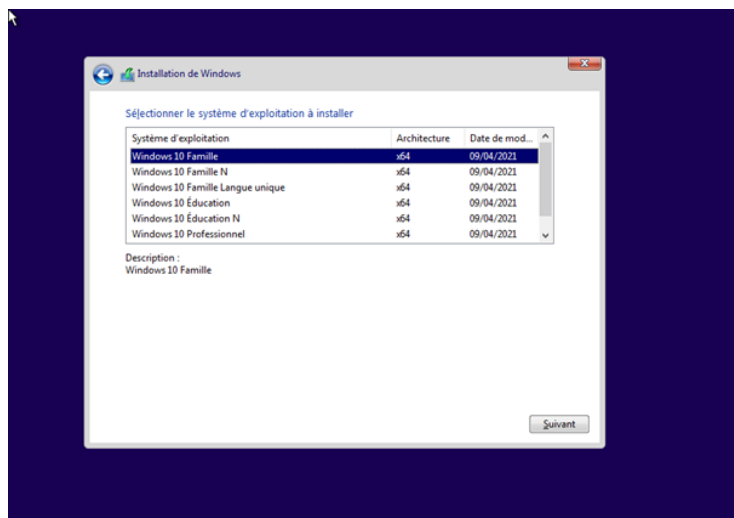
Une fois téléchargé, nous exécutons le programme d'installation et nous demandons à cette dernière de nous fournir le fichier ISO de windows 10 comme nous pouvons le voir dans les captures ci-dessous :



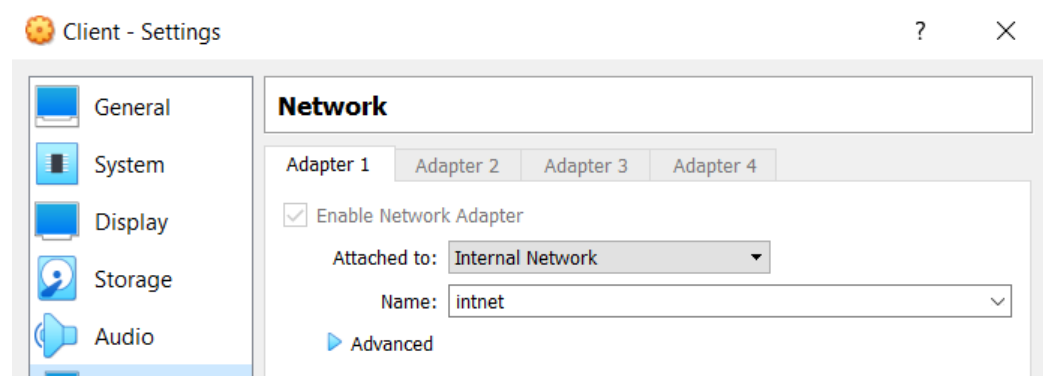
Une fois que nous avons récupéré le fichier ISO, nous pouvons maintenant nous occuper de l'installation sur la machine virtuelle.



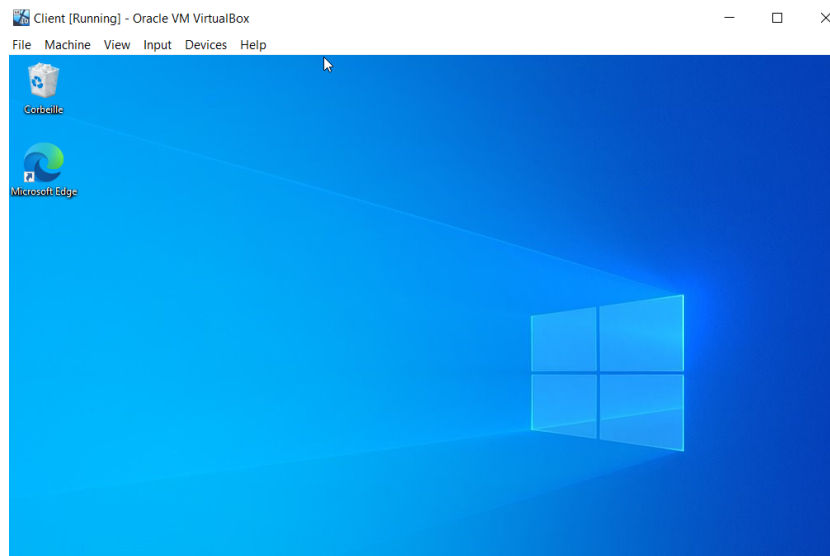
Pour notre installation, nous choisissons d'installer Windows 10 édition Familiale. Nous précisons également à l'installateur que nous possédons pas de clé de licence.



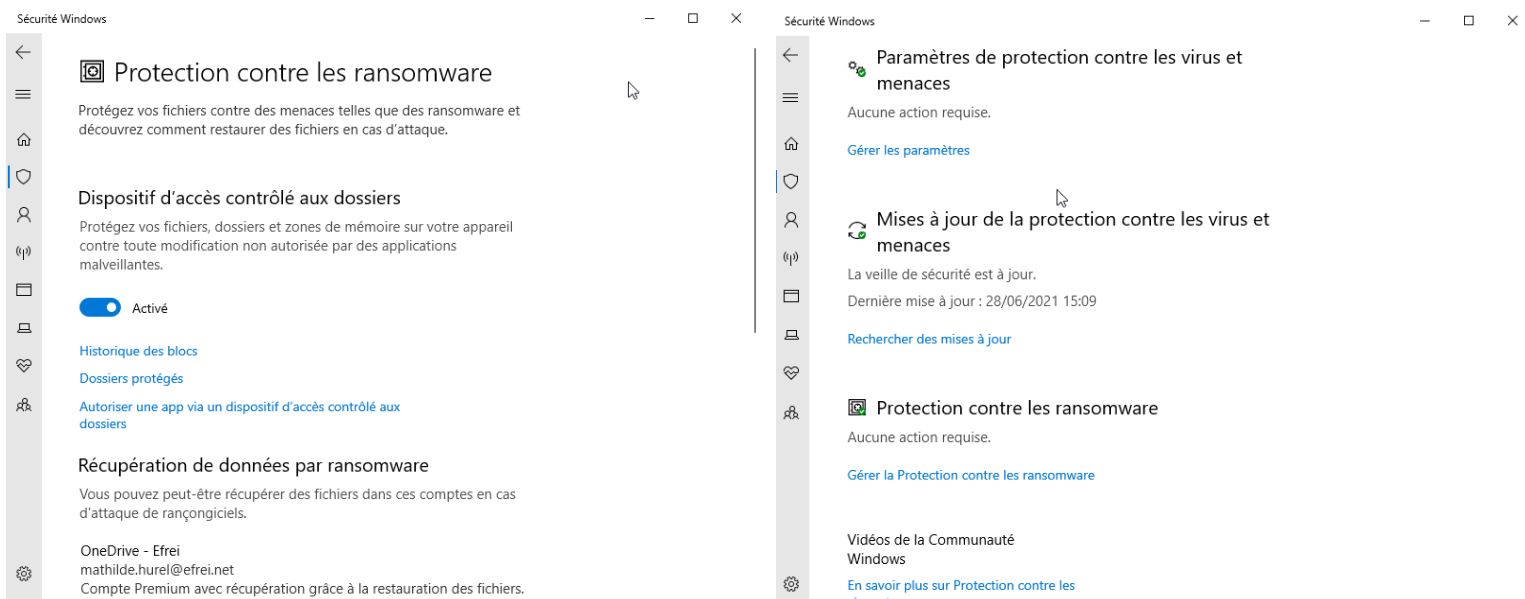
Une fois l'installation terminée, nous allons mettre la machine client en réseau interne afin qu'il ne reçoive internet qu'à partir du routeur.



Nous pouvons à présent utiliser la machine Windows.



L'utilisateur doit avoir un compte premium Office 365 comme celui qu'on a avec l'Efrei. Nous avons utilisé notre adresse mail de l'Efrei pour paramétrer le Windows Defender contre les ransomwares.



Dans notre machine client sous windows nous donnons à cette dernière l'adresse 192.168.1.1 et nous assignons l'adresse 192.168.1.254 (l'adresse du pare-feu comme adresse passerelle)

```
PS C:\Users\client> ipconfig

Configuration IP de Windows

Carte Ethernet Ethernet :

    Suffixe DNS propre à la connexion. . . . :
    Adresse IPv6 de liaison locale. . . . . : fe80::f975:cce9:63d2:f317%3
    Adresse IPv4. . . . . : 192.168.1.1
    Masque de sous-réseau. . . . . : 255.255.255.0
    Passerelle par défaut. . . . . : 192.168.1.254
```

Notre machine Windows est donc opérationnelle.

Installation du pare-feu

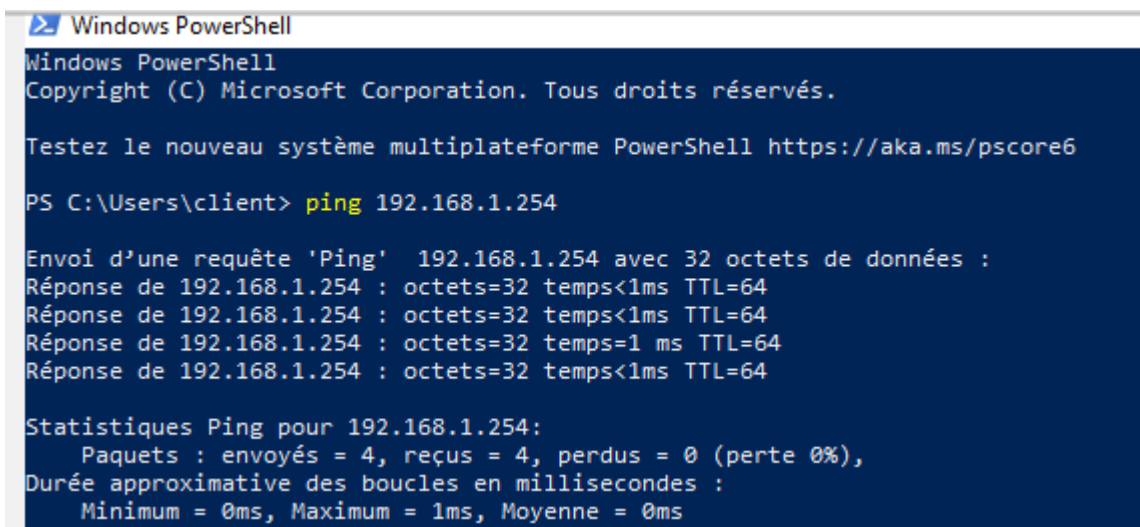
Maintenant que nous avons installé notre machine Windows, nous allons maintenant installer et configurer le pare-feu dans notre routeur sous FreeBSD.

Dans notre routeur (boîtier virtuel) qui contient pfSENSE, nous configurons les adresses de la façon suivante:

Nous configurons le LAN à l'adresse 192.168.1.254

```
*** Welcome to pfSense 2.5.1-RELEASE (amd64) on pfSense ***  
  
WAN (wan)      -> em0      -> v4/DHCP4: 10.0.2.15/24  
LAN (lan)      -> em1      -> v4: 192.168.1.254/24
```

Testons la connectivité entre le routeur et la machine cliente :



```
Windows PowerShell  
Copyright (C) Microsoft Corporation. Tous droits réservés.  
  
Testez le nouveau système multiplateforme PowerShell https://aka.ms/pscore6  
  
PS C:\Users\client> ping 192.168.1.254  
  
Envoi d'une requête 'Ping' 192.168.1.254 avec 32 octets de données :  
Réponse de 192.168.1.254 : octets=32 temps<1ms TTL=64  
Réponse de 192.168.1.254 : octets=32 temps<1ms TTL=64  
Réponse de 192.168.1.254 : octets=32 temps=1 ms TTL=64  
Réponse de 192.168.1.254 : octets=32 temps<1ms TTL=64  
  
Statistiques Ping pour 192.168.1.254:  
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),  
    Durée approximative des boucles en millisecondes :  
        Minimum = 0ms, Maximum = 1ms, Moyenne = 0ms
```

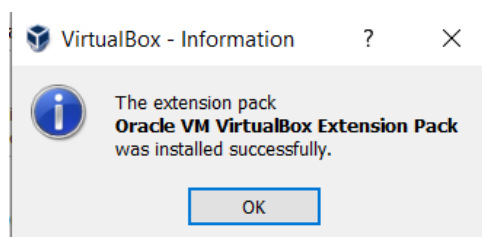
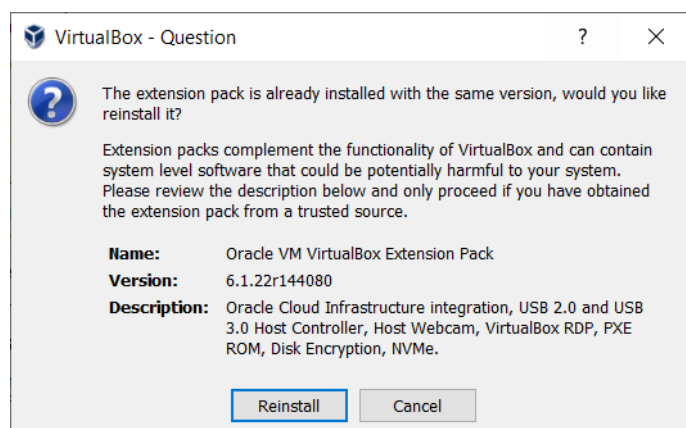
La connectivité est bien établie entre les deux machines.

Port USB

Sur la machine virtuelle Windows 10, télécharger **USBfix** qui est un logiciel gratuit analysant les périphériques USB

<https://www.01net.com/telecharger/windows/Securite/antivirus-antitrojan/fiches/129890.html>
<https://www.01net.com/telecharger/windows/Securite/antivirus-antitrojan/fiches/129890.html>

Sur votre PC, télécharger **Extension Pack** de Virtual Box afin de pouvoir monter des clefs USB
https://download.virtualbox.org/virtualbox/6.1.22/Oracle_VM_VirtualBox_Extension_Pack-6.1.22.vbox-extpack



Brancher une clef USB

Créer un fichier texte à partir du **Bloc Notes** et copier coller cette ligne **au caractère près** :

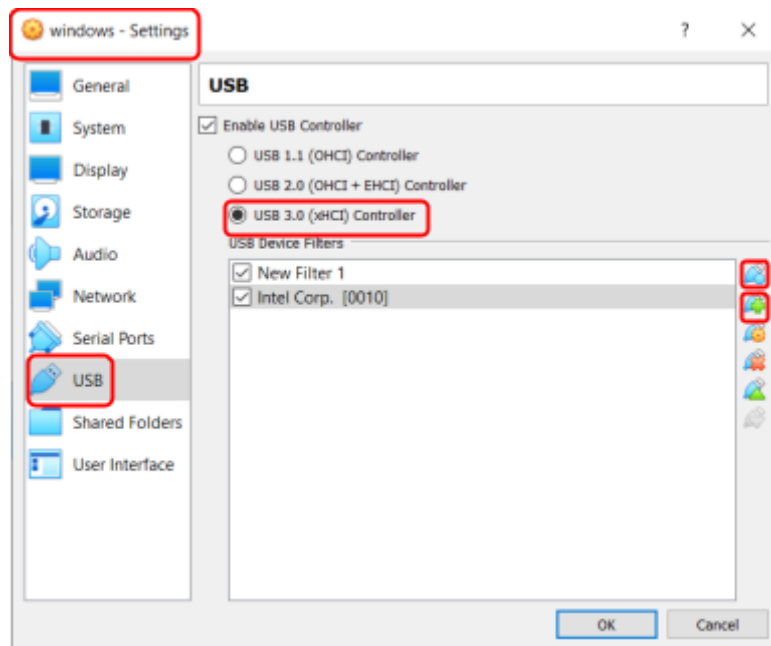
X5O!P%@AP[4\PZX54(P^)7CC)7}\$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!\$H+H*

Sauvegarder le fichier sur votre clef USB en le nommant 'test_virus.txt' par exemple (ou 'eicar.com' qui est le nom général de ce type de fichier).

Ensuite dans Virtualbox, aller dans la **Configuration** de la machine virtuelle windows 10, puis dans **USB**. La case Activer le contrôleur **USB** doit être cochée

Ensuite sélectionner le **Contrôleur USB** sur lequel on branche la clef (**Contrôleur 3.0** pour ma part)

Cliquer sur l'icône de la **clef USB avec un petit rond bleu** à droite de la page pour Ajouter un filtre USB, et ensuite sur l'icône en dessus représentant une **clef USB avec une croix verte** pour Ajouter le filtre correspondant à votre clef USB (**Generic Mass Storage** pour ma part)



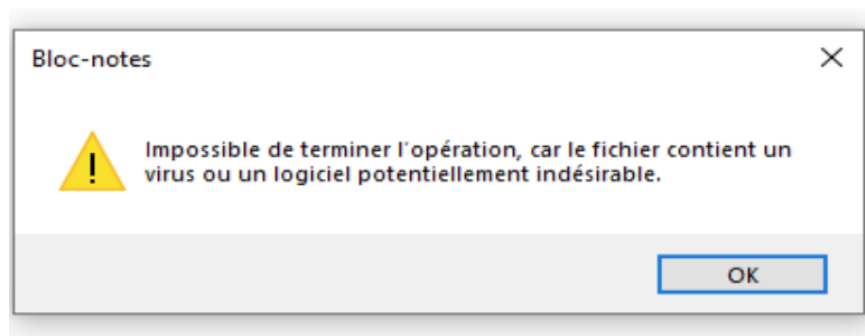
Fermer et réouvrir Virtualbox

Lancer la machine virtuelle Windows 10 tout en laissant la clef USB branchée.

Celle-ci ne va plus apparaître sur votre PC mais bien sur la machine virtuelle.



Un message de Windows Defender va directement s'afficher en déclarant qu'une menace a été détectée. Puis lorsqu'on essaye d'ouvrir le fichier sur la clef, un nouveau message apparaît :



Ensuite on ouvre USBFix et on lance une analyse de la clef USB



Aucune menace n'est détectée car le faux virus test est bloqué



On ouvre le rapport d'analyse et le logiciel a bien analysé la clef USB, le disque USB D:\, ainsi que le fichier virus.txt

```
#-----  
#-UsbFix Antivirus Premium  
#-----  
# Version : 11.032  
# Base de données :  
# Contact : https://www.usb-antivirus.com/fr/contact  
#-----  
# Type de scan : USB  
# Utilisateur : medecin (Administrateur)  
# Appareil : DESKTOP-3UNGMTU  
# Lancé : 05/07/2021 17:23:09  
#-----  
  
----- | Disques analysés |  
  
D:\      FAT32      (8GB/8GB)      [Removable]  
  
----- | D:\ - Disque USB (FAT32) |  
  
[25/06/2021 - 15:14:30 | A | 0 Ko] - virus.txt.txt  
[04/12/2017 - 13:58:22 | HD] - .Spotlight-V100  
[25/06/2021 - 11:59:44 | D] - autorun.inf
```


KALI

```
(kali㉿kali)-[~]
$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:0e:34:8d brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic eth0
        valid_lft 86299sec preferred_lft 86299sec
    inet6 fe80::a00:27ff:fe0e:348d/64 scope link
        valid_lft forever preferred_lft forever
```

```
File Actions Edit View Help
GNU nano 5.4 /etc/network/interfaces
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

#interface eth0
allow-hotplug eth0
iface eth0 inet dhcp
```

```
(root㉿kali)-[/home/kali/Downloads]
# sudo nix run -f channel:nixos-unstable nmap_graphical
```

sudo nix run -f channel:nixos-unstable nmap_graphical

The screenshot shows a Kali Linux terminal window with the command `sudo nix run -f channel:nixos-unstable nmap_graphical` being executed. The terminal output shows a warning about the locale and the start of the `nmap-graphical` process. The Zenmap GUI is open, showing the 'Intense scan' profile and the 'Nmap Output' tab. The terminal output includes a warning about the locale and the start of the `nmap-graphical` process.

Scan Tools Profile Help

Target: 192.168.1.254 Profile: Intense scan

Command: nmap -T4 -A -v 192.168.1.254

Hosts Services Nmap Output Ports/Hosts Topology HostDetails Scans

OS Host

192.168.1.254

```

nmap-T4 -A -v 192.168.1.254
Initiating Service Scan at 11:52
Initiating OS detection (try #1) against 192.168.1.254
Retrying OS detection (try #2) against 192.168.1.254
Initiating Traceroute at 11:52
Completed Traceroute at 11:52, 0.02s elapsed
Initiating Parallel DNS resolution of 2 hosts. at 11:52
Completed Parallel DNS resolution of 2 hosts. at 11:52, 0.03s elapsed
NSE: Script scanning 192.168.1.254.
Initiating NSE at 11:52
Completed NSE at 11:52, 0.00s elapsed
Initiating NSE at 11:52
Completed NSE at 11:52, 0.00s elapsed
Initiating NSE at 11:52
Completed NSE at 11:52, 0.00s elapsed
Nmap scan report for 192.168.1.254
Host is up (0.0064s latency).
All 1000 scanned ports on 192.168.1.254 are filtered
Too many fingerprints match this host to give specific OS details
Network Distance: 2 hops

TRACEROUTE (using port 80/tcp)
HOP RTT ADDRESS
1 7.87 ms 10.0.2.2
2 7.88 ms 192.168.1.254

NSE: Script Post-scanning.
Initiating NSE at 11:52
Completed NSE at 11:52, 0.00s elapsed
Initiating NSE at 11:52
Completed NSE at 11:52, 0.00s elapsed
Initiating NSE at 11:52
Completed NSE at 11:52, 0.00s elapsed
Read data files from: /nix/store/wg7lzp87izk0g2mlfakiqlmkpfigmbx6-nmap-graphical-7.80/bin/./share/nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.27 seconds
Raw packets sent: 2053 (94.624KB) | Rcvd: 19 (792B)

```

Filter Hosts

On réalise ensuite un scan sur la machine Windows

```

Zenmap
Scan Tools Profile Help
Target: 192.168.1.1 Profile: Intense scan
Command: nmap -T4 -A -v 192.168.1.1

Hosts Services Nmap Output Ports/Hosts Topology Host Details Scans
OS Host
192.168.1.1
nmap -T4 -A -v 192.168.1.1
Starting Nmap 7.80 ( https://nmap.org ) at 2021-07-05 04:39 EDT
NSE: Loaded 151 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 04:39
Completed NSE at 04:39, 0.00s elapsed
Initiating NSE at 04:39
Completed NSE at 04:39, 0.00s elapsed
Initiating NSE at 04:39
Completed NSE at 04:39, 0.00s elapsed
Initiating NSE at 04:39
Completed NSE at 04:39, 0.00s elapsed
Initiating Ping Scan at 04:39
Scanning 192.168.1.1 [4 ports]
Completed Ping Scan at 04:39, 0.03s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 04:39
Completed Parallel DNS resolution of 1 host. at 04:39, 0.02s elapsed
Initiating SYN Stealth Scan at 04:39
Scanning 192.168.1.1 [1000 ports]
Discovered open port 135/tcp on 192.168.1.1
Discovered open port 445/tcp on 192.168.1.1
Discovered open port 139/tcp on 192.168.1.1
Discovered open port 3580/tcp on 192.168.1.1
Completed SYN Stealth Scan at 04:39, 4.96s elapsed (1000 total ports)
Initiating Service scan at 04:39
Scanning 4 services on 192.168.1.1
Completed Service scan at 04:39, 6.20s elapsed (4 services on 1 host)
Initiating OS detection (try #1) against 192.168.1.1
Retrying OS detection (try #2) against 192.168.1.1
Initiating Traceroute at 04:40
Completed Traceroute at 04:40, 0.02s elapsed
Initiating Parallel DNS resolution of 2 hosts. at 04:40
Completed Parallel DNS resolution of 2 hosts. at 04:40, 0.01s elapsed
NSE: Script scanning 192.168.1.1.
Initiating NSE at 04:40
Completed NSE at 04:40, 7.79s elapsed
Initiating NSE at 04:40
Completed NSE at 04:40, 0.07s elapsed
Initiating NSE at 04:40

```

```

Zenmap
Scan Tools Profile Help
Target: 192.168.1.1 Profile: Intense scan
Command: nmap -T4 -A -v 192.168.1.1

Hosts Services Nmap Output Ports/Hosts Topology Host Details Scans
OS Host
192.168.1.1
nmap -T4 -A -v 192.168.1.1
Completed Parallel DNS resolution of 2 hosts. at 04:40, 0.01s elapsed
NSE: Script scanning 192.168.1.1.
Initiating NSE at 04:40
Completed NSE at 04:40, 7.79s elapsed
Initiating NSE at 04:40
Completed NSE at 04:40, 0.07s elapsed
Initiating NSE at 04:40
Completed NSE at 04:40, 0.00s elapsed
Nmap scan report for 192.168.1.1
Host is up (0.0018s latency).
Not shown: 990 filtered ports
PORT      STATE SERVICE          VERSION
135/tcp   open  msrpc            Microsoft Windows RPC
139/tcp   open  netbios-ssn     Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds?
3580/tcp  open  http             National Instruments LabVIEW service locator httpd 1.0.0
|_ http-methods:
|_ Supported Methods: GET
|_ http-server-header: NI Service Locator/1.0.0 (SLServer)
|_ http-title: Service Unavailable
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: bridge|general purpose
Running (JUST GUESSING): Oracle Virtualbox (98%), QEMU (92%)
OS CPE: cpe:/o:oracle:virtualbox cpe:/a:qemu:qemu
Aggressive OS guesses: Oracle Virtualbox (98%), QEMU user mode network gateway (92%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
TCP Sequence Prediction: Difficulty=17 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_ clock-skew: 1s
|_ smb2-security-mode:
|_ 2.02:
|_ Message signing enabled but not required

```

```
Network Distance: 2 hops
TCP Sequence Prediction: Difficulty=17 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_ clock-skew: 1s
|_ smb2-security-mode:
|   2.02:
|       Message signing enabled but not required
|_ smb2-time:
|   date: 2021-07-05T08:40:08
|_ start_date: N/A

TRACEROUTE (using port 80/tcp)
HOP RTT ADDRESS
1 1.58 ms 10.0.2.2
2 1.62 ms 192.168.1.1

NSE: Script Post-scanning.
Initiating NSE at 04:40
Completed NSE at 04:40, 0.00s elapsed
Initiating NSE at 04:40
Completed NSE at 04:40, 0.00s elapsed
Initiating NSE at 04:40
Completed NSE at 04:40, 0.00s elapsed
Initiating NSE at 04:40
Completed NSE at 04:40, 0.00s elapsed
Read data files from: /nix/store/wg7lzp87izk0g2zlfakiqlmkpfigmbx6-nmap-graphical-7.80/bin/./share/nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 24.45 seconds
Raw packets sent: 2052 (93.38KB) | Rcvd: 652 (26.78KB)
```

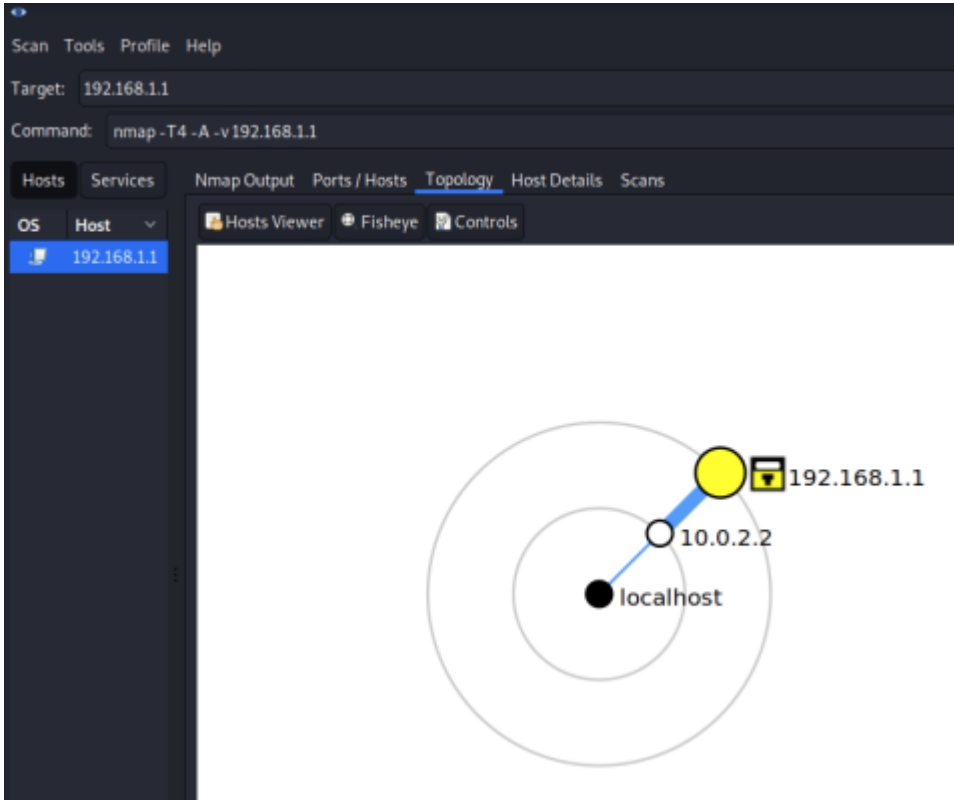
Scan Tools Profile Help

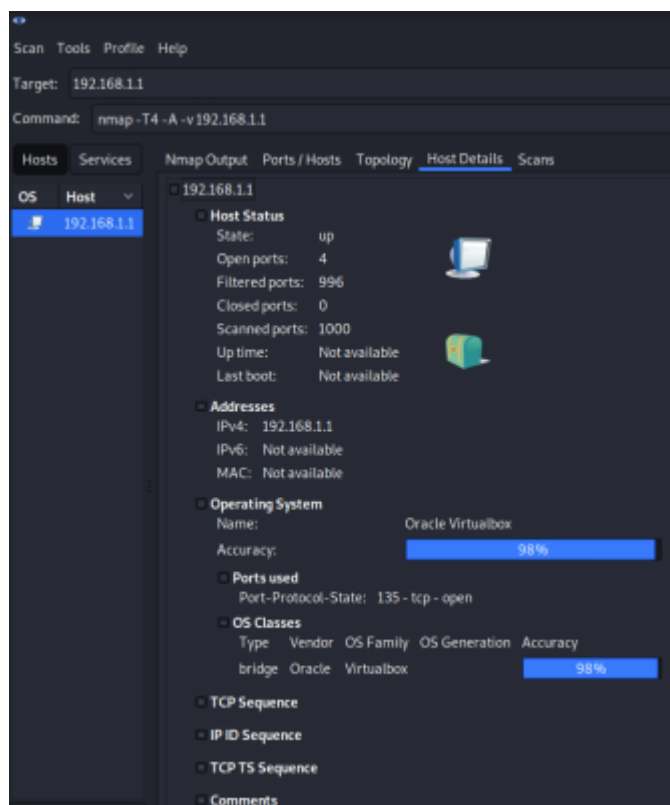
Target: 192.168.1.1


Command: nmap -T4 -A -v 192.168.1.1

Hosts Services Nmap Output Ports/Hosts Topology Host Details Scans

OS	Host	Port	Protocol	State	Service	Version
	192.168.1.1	135	tcp	open	msrpc	Microsoft Windows RPC
	192.168.1.1	139	tcp	open	netbios-ssn	Microsoft Windows netbios-ssn
	192.168.1.1	445	tcp	open	microsoft-ds	
	192.168.1.1	3580	tcp	open	http	National Instruments LabVIEW service locator httpd 1.0.0





Scan Details	
Policy:	Malware Scan
Status:	Completed
Severity Base:	CVSS v2.0 
Scanner:	Local Scanner
Start:	Today at 4:39 AM
End:	Today at 4:41 AM
Elapsed:	3 minutes

Host Details	
IP:	192.168.1.1
OS:	AIX 5.3
Start:	Today at 4:39 AM
End:	Today at 4:41 AM
Elapsed:	2 minutes
KB:	Download

Risk Level	Count
Critical	1
High	1
Medium	1
Low	1
Info	1

pfSense

```
PS C:\Users\medecin> Start-Process powershell -Verb runas
```

```
PS C:\Windows\system32> New-NetIPAddress -InterfaceAlias "Ethernet" 192.168.1.1 -PrefixLength "24" -DefaultGateway 192.168.1.254
```

```
IPAddress : 192.168.1.1
InterfaceIndex : 8
InterfaceAlias : Ethernet
AddressFamily : IPv4
Type : Unicast
PrefixLength : 24
PrefixOrigin : Manual
SuffixOrigin : Manual
AddressState : Tentative
ValidLifetime : Infinite ([TimeSpan]::MaxValue)
PreferredLifetime : Infinite ([TimeSpan]::MaxValue)
SkipAssSource : False
PolicyStore : ActiveStore

IPAddress : 192.168.1.1
InterfaceIndex : 8
InterfaceAlias : Ethernet
AddressFamily : IPv4
Type : Unicast
PrefixLength : 24
PrefixOrigin : Manual
SuffixOrigin : Manual
AddressState : Invalid
ValidLifetime : Infinite ([TimeSpan]::MaxValue)
PreferredLifetime : Infinite ([TimeSpan]::MaxValue)
SkipAssSource : False
PolicyStore : PersistentStore
```

```
PS C:\Windows\system32> ping 192.168.1.254
```

```
Envoi d'une requête 'Ping' 192.168.1.254 avec 32 octets de données :
Réponse de 192.168.1.254 : octets=32 temps<1ms TTL=64
Réponse de 192.168.1.254 : octets=32 temps<1ms TTL=64
Réponse de 192.168.1.254 : octets=32 temps<1ms TTL=64
Réponse de 192.168.1.254 : octets=32 temps<1ms TTL=64
```

```
Statistiques Ping pour 192.168.1.254:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 0ms, Maximum = 0ms, Moyenne = 0ms
```



[Login to pfSense](#)

SIGN IN

admin

pfSense

SIGN IN

```
Enter an option:
```

```
Message from syslogd@pfSense at Jun 26 14:01:11 ...
```

```
php-fpm[68227]: /index.php: Successful login for user 'admin' from: 192.168.1.1 (Local Database)
```