


CONFIGURATION D'UN SERVICE DE ROUTAGE

PARCOURS	SISR <input checked="" type="checkbox"/>	SLAM <input type="checkbox"/>
-----------------	---	--------------------------------------

Lieu de réalisation	Campus Montsouris	
Période de réalisation	Du : 08.09.2024	Au :
Modalité de réalisation	SEUL <input checked="" type="checkbox"/>	EN EQUIPE <input type="checkbox"/>

Intitulé de la mission	Configurer un service de routage
Description du contexte de la mission	Installer, configurer et gérer un pare-feu s'occupant du routage

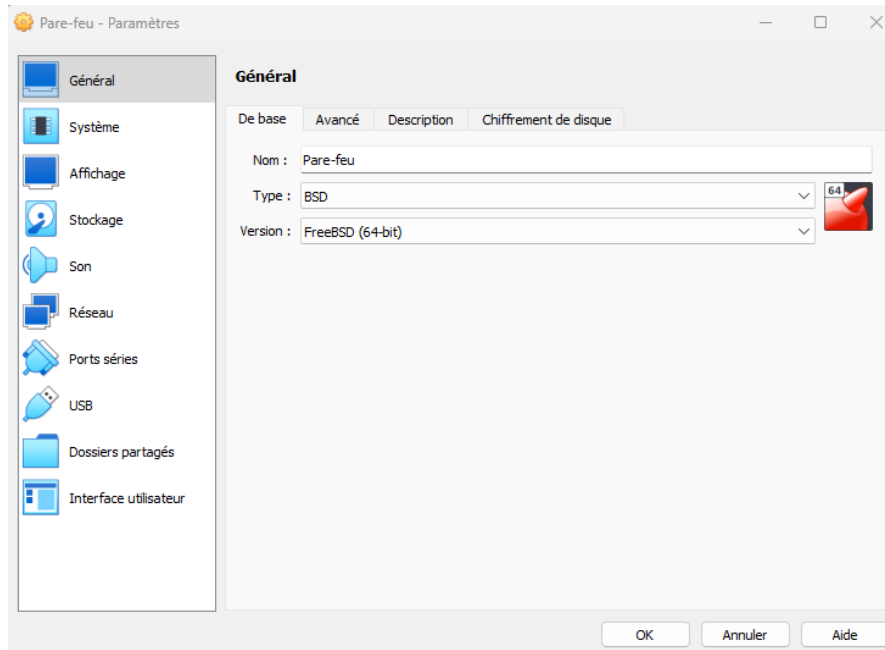
Contraintes & Résultat	Ressources fournies / contraintes techniques / Résultats attendu
	Laptop, Virtualbox, PFSense
Productions associées	Liste des documents produits et description

Modalités d'accès aux productions	Identifiants, mots de passe, URL d'un espace de stockage et présentation de l'organisation du stockage

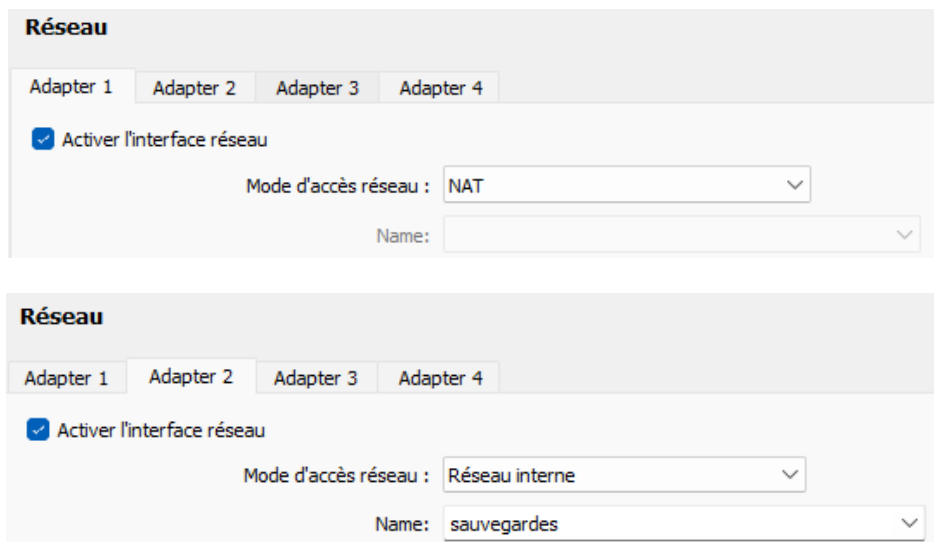
Configuration d'un pare-feu

1) Installation de la machine virtuelle

La machine virtuelle VirtualBox accueillant la solution de pare-feu PFsense est créée en se basant sur l'OS BSD 64 Bits, qui est celui sur lequel est basée la solution.



Concernant le réseau, on configure 2 cartes réseau pour le pare-feu : une en NAT pour le connecter au réseau public, et une pour notre réseau interne "sauvegardes". Cette configuration logicielle réseau permet à notre pare-feu de se trouver entre le réseau interne et le réseau public.

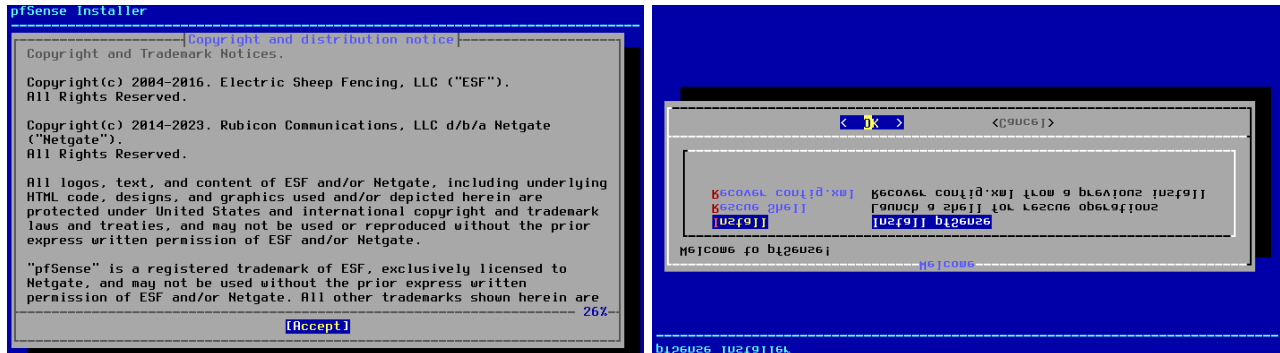


Configuration d'un pare-feu

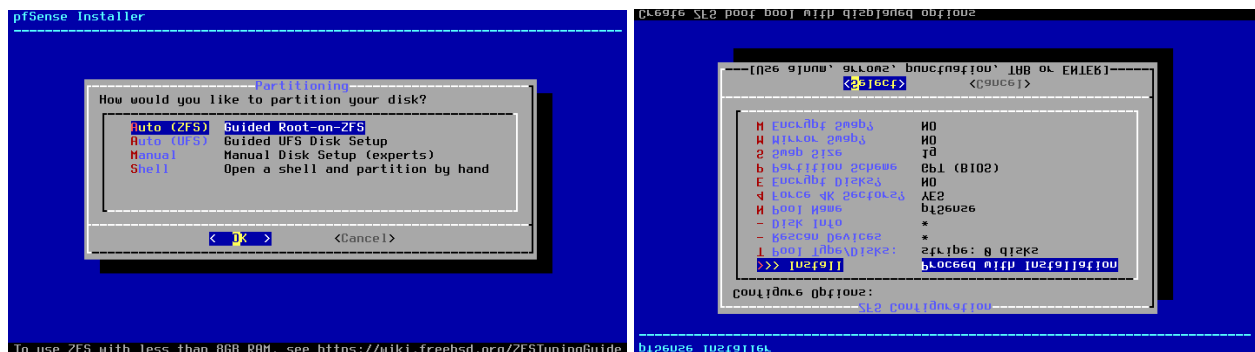
2) Installation de PFSense

A) Installation de PFSense

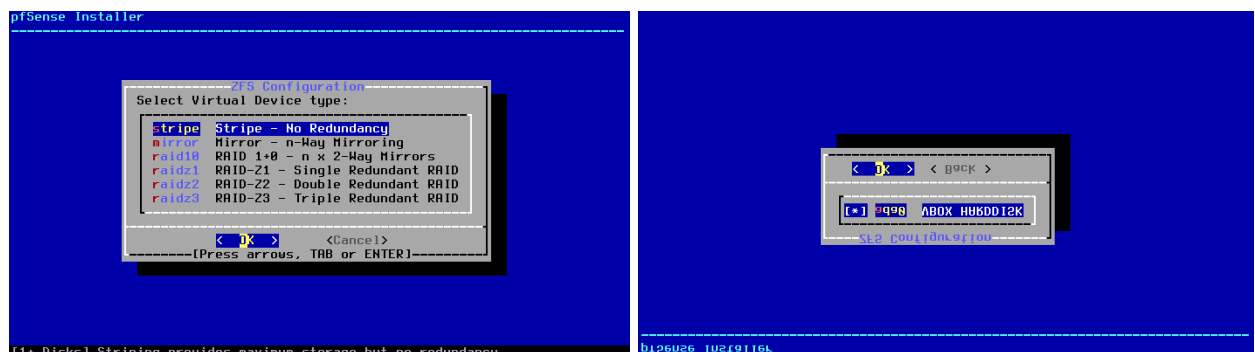
L'installation débute en suivant plusieurs étapes.



On choisit la version auto-guidée de l'installation, puis on procède directement avec l'installation.

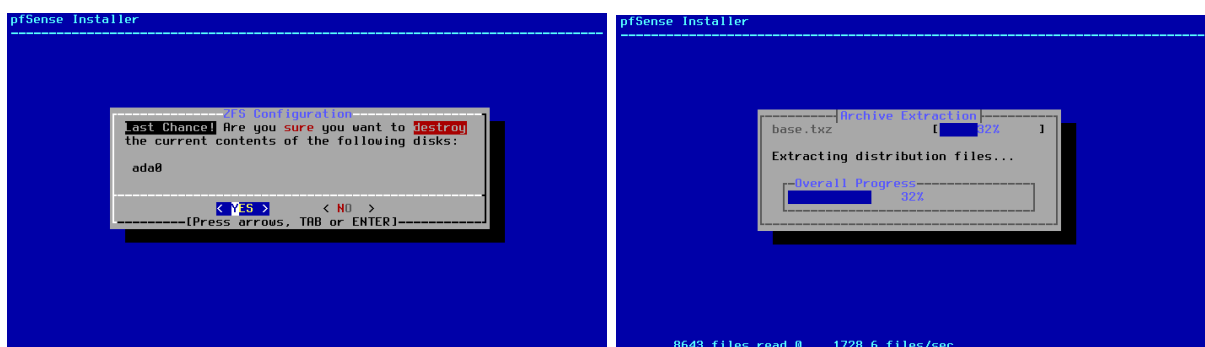


On choisit une installation rapide, sans serveur miroir ou redondance. On choisit bien le disque virtuel en appuyant sur la barre espace.



Configuration d'un pare-feu

On choisit oui pour continuer l'installation.



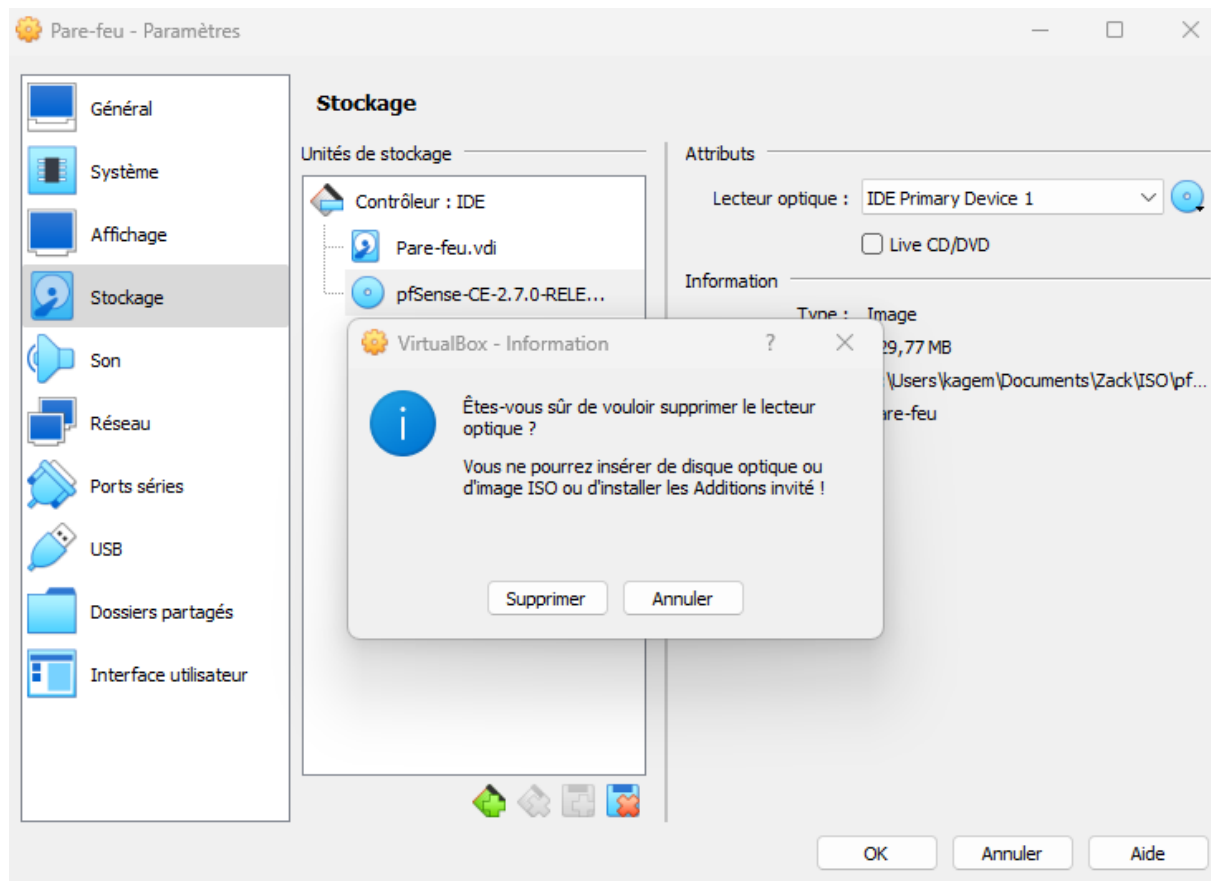
On prend bien soin de ne pas laisser redémarrer le système en boucle sur le support iso, en quittant la machine virtuelle.

```
When finished, type 'exit' to reboot.  
# exit  
Sep  8 10:10:08 reboot[1370]: rebooted by root  
Sep  8 10:10:08 syslogd: exiting on signal 15
```

Configuration d'un pare-feu

B) Configuration de PFSense

A la suite de la finalisation de la procédure d'installation, on quitte la machine virtuelle, pour éviter de reboot indéfiniment sur le support d'installation. Dans les paramètres VirtualBox, on prend bien soin de le retirer.



Configuration d'un pare-feu

On redémarre la machine virtuelle. Cette fois ci, on boot bien sur le support déjà installé. Toutefois, l'OS ne prend en compte qu'un seul réseau, le WAN. Nous allons changer ça par la suite en se connectant au pare-feu en interface graphique.

```
6) Halt system          15) Restore recent configuration
7) Ping host            16) Restart PHP-FPM
8) Shell

Enter an option:

FreeBSD/amd64 (pfSense.home.arp) (ttyv0)

VirtualBox Virtual Machine - Netgate Device ID: 15e8ee1a80d287ee09f4

*** Welcome to pfSense 2.7.0-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em1      -> v4/DHCP4: 192.168.0.12/24

0) Logout (SSH only)    9) pfTop
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: 1
```

On ping le serveur. On est dans le réseau.

```
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: 192.168.0.1

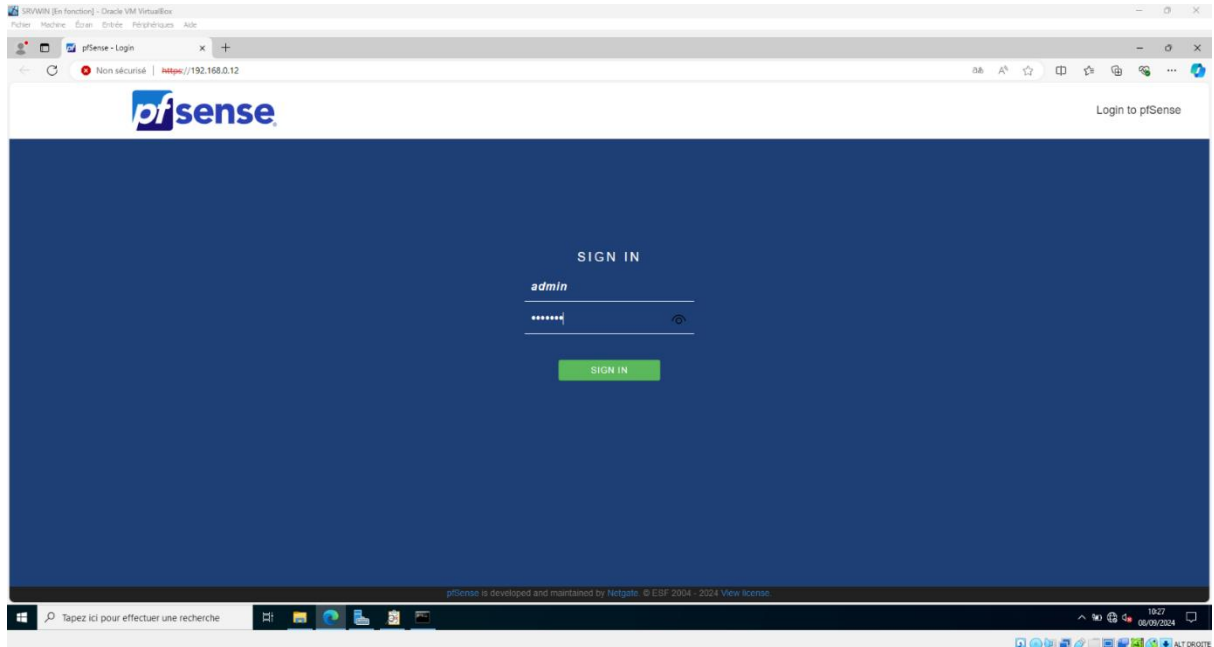
PING 192.168.0.1 (192.168.0.1): 56 data bytes
64 bytes from 192.168.0.1: icmp_seq=0 ttl=128 time=4.772 ms
64 bytes from 192.168.0.1: icmp_seq=1 ttl=128 time=4.302 ms
64 bytes from 192.168.0.1: icmp_seq=2 ttl=128 time=1.697 ms

--- 192.168.0.1 ping statistics ---
3 packets transmitted, 3 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 1.697/3.590/4.772/1.352 ms

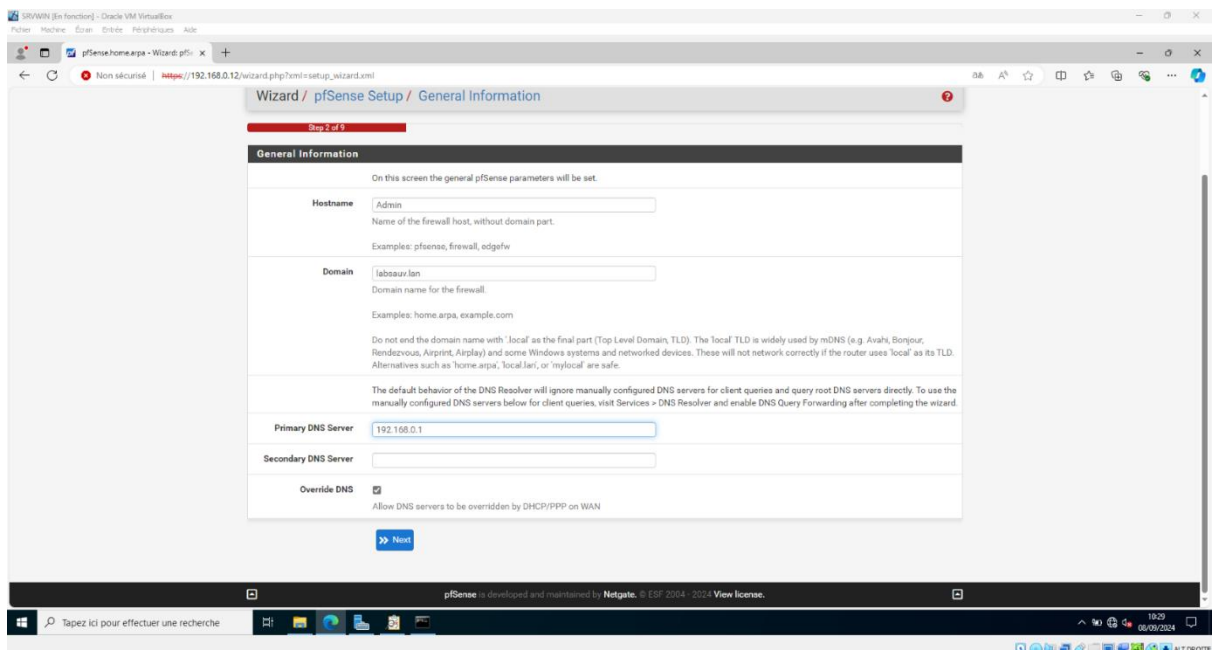
Press ENTER to continue.
```

Configuration d'un pare-feu

On quitte la version en ligne de commandes pour la version en interface graphique. On se connecte au pare-feu avec le protocole HTTP, en tapant l'adresse IP dans le navigateur. On rentre les identifiants par défaut.



On définit le serveur comme serveur DNS principal.



Configuration d'un pare-feu

On rajoute le LAN qu'on a comme seconde interface réseau.

The screenshot shows the pfSense web interface for configuring the LAN interface (em1). The browser address bar shows `https://192.168.1.54/interfaces.php?if=lan`. The interface has a navigation menu with options like System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, and Help. The main content area is titled "Interfaces / LAN (em1)" and contains a yellow notification box stating: "The LAN configuration has been changed. The changes must be applied to take effect. Don't forget to adjust the DHCP Server range if needed after applying." with an "Apply Changes" button. Below this is the "General Configuration" section with the following fields:

- Enable:** ☒ Enable interface
- Description:** (Help text: Enter a description (name) for the interface here.)
- IPv4 Configuration Type:**
- IPv6 Configuration Type:**
- MAC Address:** (Help text: This field can be used to modify ("spoof") the MAC address of this interface. Enter a MAC address in the following format: xxxxxxxx:xxxx:xxxx or leave blank.)
- MTU:** (Help text: If this field is blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary in some circumstances.)
- MSS:** (Help text: If a value is entered in this field, then MSS clamping for TCP connections to the value entered above minus 40 for IPv4 (TCP/IPv4 header size) and minus 60 for IPv6 (TCP/IPv6 header size) will be in effect.)

On a finalement 2 réseaux, le WAN comme réseau publique (carte réseau NAT dans VirtualBox) et le LAN comme réseau privé (carte réseau interne "sauvegardes").

```
php-fpm[379]: /index.php: Successful login for user 'admin' from: 192.168.1.63 (Local Database)

FreeBSD/amd64 (Admin.labsauv.lan) (ttyv0)

VirtualBox Virtual Machine - Netgate Device ID: 15e8ee1a80d287ee09f4

*** Welcome to pfSense 2.7.0-RELEASE (amd64) on Admin ***

WAN (wan)      -> em0      -> v4/DHCP4: 192.168.1.54/24
LAN (lan)      -> em1      -> v4/DHCP4: 192.168.0.12/24

0) Logout (SSH only)          9) pfTop
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: 
```


Configuration d'un pare-feu

Voici le plan d'adressage de notre réseau

Réseau interne Sauvegardes				
Réseau (A)	Masque décimal	Masque CIDR	Diffusion	
192.168.0.0	255.255.255.0	/24	192.168.0.255	
Equipements	Première	Dernière	Fixe	Dynamique
Serveur	192.168.0.1		x	
Cient	192.168.0.11			x
Routeur	192.168.0.254		x	

Maintenant que le routeur a été configuré, on peut démarrer nos tests de ping entre lui et les machines de notre réseau pour voir si la connectivité intra réseau est bonne.

```
Enter a host name or IP address: 192.168.0.1

PING 192.168.0.1 (192.168.0.1): 56 data bytes
64 bytes from 192.168.0.1: icmp_seq=0 ttl=128 time=1.324 ms
64 bytes from 192.168.0.1: icmp_seq=1 ttl=128 time=1.118 ms
64 bytes from 192.168.0.1: icmp_seq=2 ttl=128 time=1.711 ms

--- 192.168.0.1 ping statistics ---
3 packets transmitted, 3 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 1.118/1.384/1.711/0.246 ms
```

```
Enter a host name or IP address: 192.168.0.11

PING 192.168.0.11 (192.168.0.11): 56 data bytes
64 bytes from 192.168.0.11: icmp_seq=0 ttl=128 time=1.589 ms
64 bytes from 192.168.0.11: icmp_seq=1 ttl=128 time=0.760 ms
64 bytes from 192.168.0.11: icmp_seq=2 ttl=128 time=2.352 ms

--- 192.168.0.11 ping statistics ---
3 packets transmitted, 3 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 0.760/1.567/2.352/0.650 ms
```

Configuration d'un pare-feu

La connectivité intra réseau fonctionne. Nous tentons maintenant de ping le réseau public avec notre serveur et notre client.

```
C:\Users\Administrateur>ping google.com

Envoi d'une requête 'ping' sur google.com [172.217.20.174] avec 32 octets de données :
Réponse de 172.217.20.174 : octets=32 temps=9 ms TTL=111
Réponse de 172.217.20.174 : octets=32 temps=10 ms TTL=111
Réponse de 172.217.20.174 : octets=32 temps=11 ms TTL=111
Réponse de 172.217.20.174 : octets=32 temps=7 ms TTL=111

Statistiques Ping pour 172.217.20.174:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 7ms, Maximum = 11ms, Moyenne = 9ms
```

```
C:\Users\lewis.hamilton>ping 8.8.8.8

Envoi d'une requête 'Ping' 8.8.8.8 avec 32 octets de données :
Réponse de 8.8.8.8 : octets=32 temps=11 ms TTL=111
Réponse de 8.8.8.8 : octets=32 temps=14 ms TTL=111
Réponse de 8.8.8.8 : octets=32 temps=10 ms TTL=111
Réponse de 8.8.8.8 : octets=32 temps=11 ms TTL=111

Statistiques Ping pour 8.8.8.8:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 10ms, Maximum = 14ms, Moyenne = 11ms
```

Nos machines pingent bien le réseau public, elles ont accès à internet grâce au rôle de routage du pare-feu.

