



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

Réalisé par Michel, Arnaud, Noah et Lucas - 31/05/2024

Sommaire

1. Problématique

.....2

2. Installation des machines virtuelles et pare-feu

réseaux et machines virtuelles.....3

3. Tests sur le réseau LAN

ping, ping et ping.....8



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

Réalisé par Michel, Arnaud, Noah et Lucas - 31/05/2024

1. Problématique

Dans La Société D'eau Raillée, spécialisée dans le développement de logiciels, le département informatique a récemment investi dans une infrastructure basée sur des machines virtuelles pour héberger ses applications et services internes. L'entreprise a connu quelques problèmes de sécurité et de confidentialité des données ces derniers temps, ce qui a incité le département informatique à renforcer la sécurité de son réseau.

Le responsable de la sécurité informatique, en collaboration avec l'équipe des opérations informatiques, a décidé de mettre en place un pare-feu logiciel pour sécuriser l'infrastructure. Le choix s'est porté sur l'installation d'un pare-feu logiciel sur une VM dédiée.

Tâches du technicien :

1. Sélection de la VM : Le technicien doit sélectionner une VM adaptée pour héberger le pare-feu logiciel. Cette VM doit avoir des ressources suffisantes pour exécuter le logiciel de pare-feu tout en garantissant des performances optimales.
2. Installation du système d'exploitation : Avant d'installer le pare-feu, le technicien doit installer un système d'exploitation sur la VM. Un système d'exploitation minimaliste et sécurisé est souvent recommandé pour réduire les vulnérabilités. (peu être fusionner avec l'étape suivante)
3. Installation du pare-feu logiciel : Une fois le système d'exploitation installé, le technicien installe le pare-feu logiciel choisi. Il configure les règles de pare-feu pour filtrer le trafic réseau entrant et sortant, en fonction des besoins de l'entreprise. Par exemple, il peut bloquer les connexions non autorisées, limiter l'accès à certains services, ouvrir uniquement certains ports, etc.
4. Configuration avancée : En fonction des besoins spécifiques de l'entreprise, le technicien peut devoir configurer des fonctionnalités avancées du pare-feu, telles que la surveillance du trafic, la détection des intrusions, la prévention des fuites de données, etc.
5. Tests et validation : Une fois la configuration terminée, le technicien effectue des tests pour s'assurer que le pare-feu fonctionne correctement. Il teste différentes situations, comme le blocage de connexions non autorisées, la redirection de trafic, la gestion des performances, etc.
6. Documentation : Enfin, le technicien documente toutes les étapes de mise en place du pare-feu, y compris les configurations réalisées, les règles de pare-feu, les tests effectués, etc. Cette



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

Réalisé par Michel, Arnaud, Noah et Lucas - 31/05/2024

documentation est essentielle pour assurer la maintenance future du pare-feu et pour former d'autres membres de l'équipe.

Conclusion :

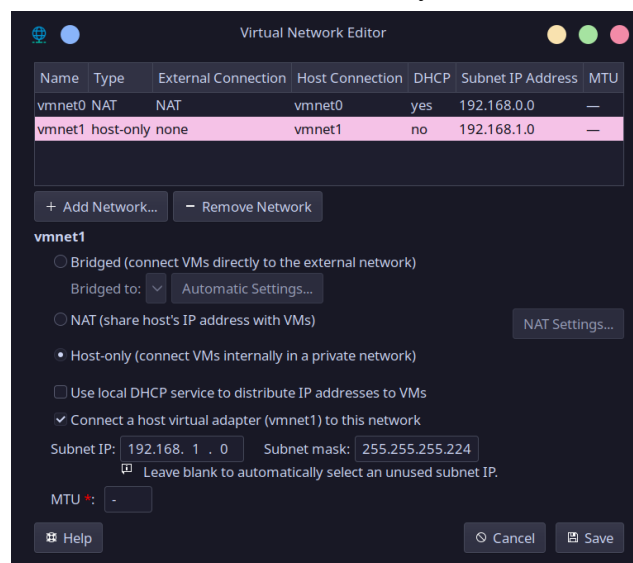
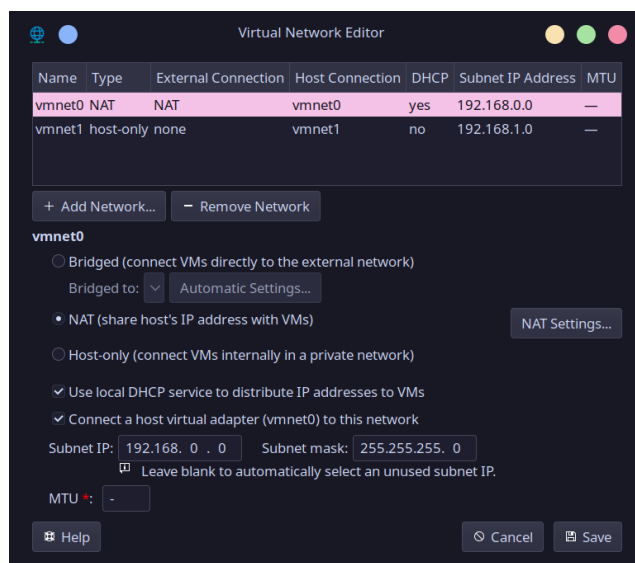
En mettant en place un pare-feu logiciel sur une VM, l'entreprise renforce la sécurité de son infrastructure informatique. Le technicien joue un rôle crucial dans ce processus, en sélectionnant les bons outils, en les configurant correctement et en s'assurant de leur bon fonctionnement. Ce pare-feu contribue à protéger les données sensibles de l'entreprise et à garantir la disponibilité et l'intégrité de ses services.

2. Installation du système d'exploitation et pare-feu

Pour ce brief, nous allons avoir besoin de différentes machines virtuelles, toutes avec leur propres caractéristiques :

- ➔ Une VM pour pfSense 1 coeur, 1 Go de Ram, 8 Go de stockage, 2 cartes réseaux, une en NAT pour simuler un réseau WAN, une en host-only pour simuler votre LAN (sans DHCP).
- ➔ Une VM pour le client qui sera la seule machine à avoir accès à l'interface graphique de pfSense, 1 coeur 2 Go de Ram, 30 Go de stockage avec une distribution linux avec interface graphique autre que debian (Ici OpenSUSE). La carte sera en IP fixe sur une carte host-only
- ➔ Une Vm pour le serveur Web avec les même caractéristiques que la VM client mais sans interface graphique (Ici Debian).

Avant de créer nos VMs, il faut aller dans la configuration des réseaux virtuels de notre hyperviseur (ici VMWare Workstation), et créer deux réseaux : Un réseau NAT, et un réseau en host-only :





Mise en place d'un Pare-feu Logiciel sur VM :

Renforcement de la Sécurité Informatique

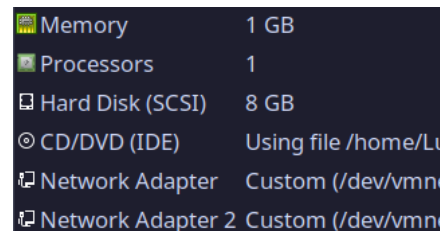
Réalisé par Michel, Arnaud, Noah et Lucas - 31/05/2024

Une fois les réseaux virtuels configurés, nous pouvons commencer à configurer nos machines virtuelles.

a. Mise en place de pfSense

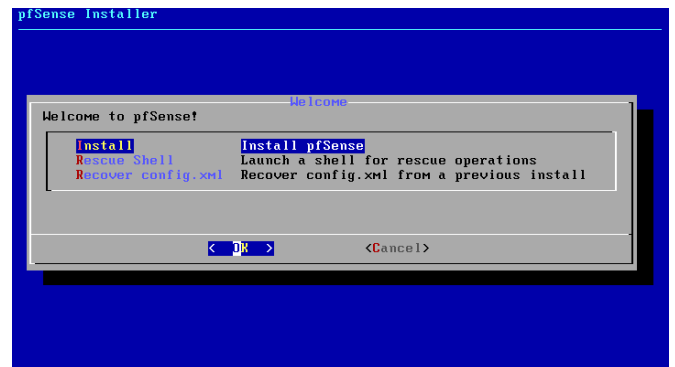
La VM est configurée avec les consignes données :

- ➔ 1 Coeur
- ➔ 1 Go de Ram
- ➔ 8 Go de stockage
- ➔ L'ISO d'installation de pfSense
- ➔ 2 cartes réseaux :
 - ➔ une sur notre réseau virtuel NAT pour simuler un réseau WAN
 - ➔ une sur notre réseau virtuel host-only pour simuler votre LAN (sans DHCP).

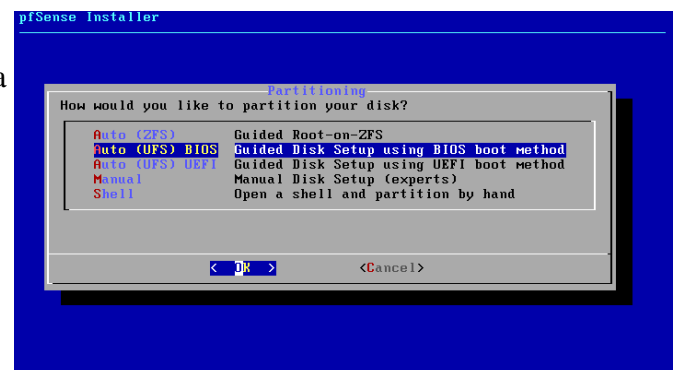


Memory	1 GB
Processors	1
Hard Disk (SCSI)	8 GB
CD/DVD (IDE)	Using file /home/Lu
Network Adapter	Custom (/dev/vmnet0)
Network Adapter 2	Custom (/dev/vmnet1)

Une fois la VM lancée, l'installation de pfSense se lance, et il suffit de suivre les instructions afin de réaliser l'installation.



Note : Nous sélectionnerons ici une installation utilisant la méthode de démarrage BIOS.





Mise en place d'un Pare-feu Logiciel sur VM : Renforcement de la Sécurité Informatique Réalisé par Michel, Arnaud, Noah et Lucas - 31/05/2024

Une fois l'installation terminée, pfSense démarre, et nous demande de configurer les cartes réseau. Il faut sélectionner notre carte réseau **NAT pour le WAN**, et notre carte réseau **host-only pour le LAN**. Une fois fait, nous pouvons commencer à configurer les adresses attribuées de notre pfSense en utilisant l'option "2) Set interface(s) IP address".

Nous voulons ici configurer la carte réseau LAN, il faudra donc sélectionner 2.

```
Enter an option: 2
Available interfaces:
1 - WAN (em0 - dhcp)
2 - LAN (em1 - static)
Enter the number of the interface you wish to configure: █
```

En premier, nous définissons l'adresse LAN de notre VM pfSense, puis son masque de sous réseau. Notre réseau est 192.168.1.0/27, et nous avons opté pour définir 192.168.1.30/27 comme adresse IP pour pfSense.

```
Enter the new LAN IPv4 address. Press <ENTER> for none:
> 192.168.1.30
Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
     255.255.0.0   = 16
     255.0.0.0     = 8
Enter the new LAN IPv4 subnet bit count (1 to 32):
> 27 █
```

Il faut ensuite dire oui pour activer le serveur DHCP, et définir notre plage d'adresses DHCP. Il nous faut 15 adresses, donc ici 192.168.1.1 - 192.168.1.15.

```
Do you want to enable the DHCP server on LAN? (y/n) y
Enter the start address of the IPv4 client address range: 192.168.1.1
Enter the end address of the IPv4 client address range: 192.168.1.15 █
```

La carte réseau WAN devrait logiquement se configurer d'elle même à l'installation, mais il est possible de la configurer nous-même via la même manipulation en cas de besoin.

Notre pfSense est désormais prêt à être utilisé !



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

Réalisé par Michel, Arnaud, Noah et Lucas - 31/05/2024

b. Mise en place du serveur Debian

La VM est configurée avec les consignes données :

- 1 Coeur
- 2 Go de Ram
- 30 Go de stockage
- L'ISO d'installation de Debian
- 1 cartes réseaux sur notre réseau virtuel host-only.

Memory	2 GB
Processors	1
Hard Disk (SCSI)	30 GB
CD/DVD (SATA)	Using file /home/Luc
Network Adapter	Custom (/dev/vmnet

Note : Si vous utilisez une ISO netinstall, il vous faudra un accès vers internet pour effectuer l'installation. Dans ce cas, vous pouvez temporairement mettre la carte réseau en NAT pour l'installation, et la remettre sur notre réseau host-only après l'installation.

Ne pas oublier de décocher les interfaces graphiques !
On peut aussi cocher SSH server afin de gagner du temps sur l'installation de notre SSH.

Une fois l'installation terminée, nous allons passer sur l'utilisateur root (**su -**) et installer nginx :

apt-get install nginx

Puis démarrer le service nginx :

systemctl enable --now nginx

Nous allons désormais mettre en place la configuration d'IP statique sur notre debian. Pour ça, il faudra aller éditer le fichier **/etc/network/interfaces** avec **nano**.

Il faut remplacer "dhcp" par "static" sur notre interface principale (ici ens33) et préciser l'IP de notre machine avec son masque de sous réseau, ainsi que la gateway (l'IP de notre pfSense). Puis, **systemctl restart networking**

```
[!] Software selection
At the moment, only the core of the system is installed. To tune the system to your
needs, you can choose to install one or more of the following predefined collections of
software.

Choose software to install:
[ ] Debian desktop environment
[ ] ... GNOME
[ ] ... Xfce
[ ] ... GNOME Flashback
[ ] ... KDE Plasma
[ ] ... Cinnamon
[ ] ... MATE
[ ] ... LXDE
[ ] ... LXQt
[ ] web server
[*] SSH server
[ ] standard system utilities

<Continue>

Tab> moves: <Space> selects: <Enter> activates buttons
```

```
GNU nano 7.2 /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

# The primary network interface
allow-hotplug ens33
iface ens33 inet static
    address 192.168.1.29/27
    gateway 192.168.1.30
```



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

Réalisé par Michel, Arnaud, Noah et Lucas - 31/05/2024

c. Mise en place du client OpenSUSE

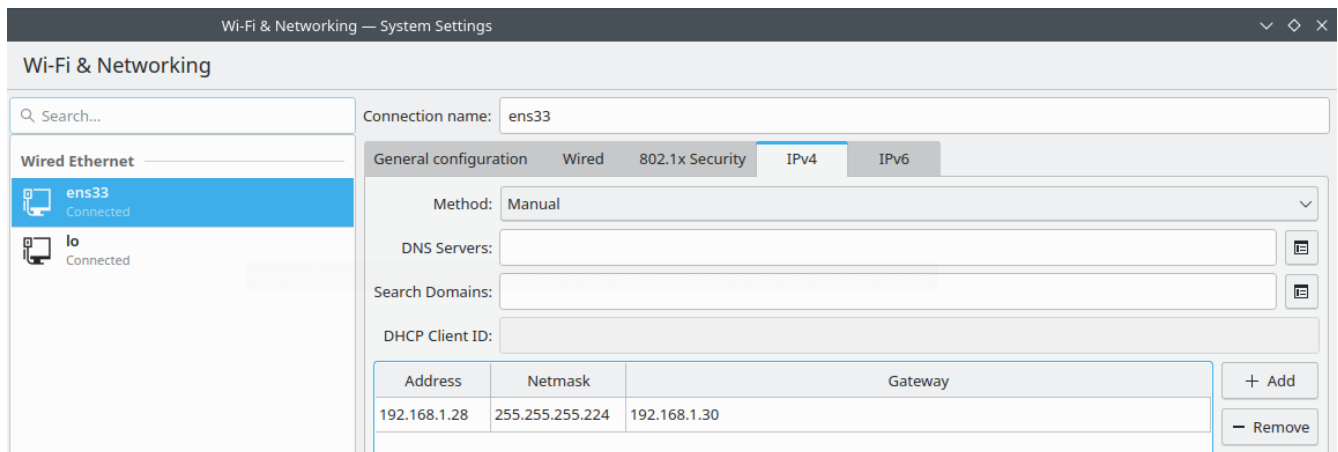
La VM est configurée avec les consignes données :

- 1 Coeur
- 2 Go de Ram
- 30 Go de stockage
- L'ISO d'installation d'OpenSUSE
- 1 cartes réseaux sur notre réseau virtuel host-only.

Memory	2 GB
Processors	1
Hard Disk (SCSI)	30 GB
CD/DVD (SATA)	Using file /home/Luc
Network Adapter	Custom (/dev/vmnet

OpenSUSE possède une installation graphique relativement facile, il suffit de se laisser guider et de suivre les instructions à l'écran.

Une fois notre client OpenSUSE installé, il faut configurer notre adresse IP statique. Ici, nous utiliseront l'interface graphique de notre environnement de bureau (KDE Plasma dans notre cas).





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

Réalisé par Michel, Arnaud, Noah et Lucas - 31/05/2024

3. Tests sur le réseau LAN

Nous allons désormais effectuer des tests afin de vérifier que nos machines peuvent bel et bien communiquer entre elles.

```
Enter a host name or IP address: 192.168.1.29

PING 192.168.1.29 (192.168.1.29): 56 data bytes
64 bytes from 192.168.1.29: icmp_seq=0 ttl=64 time=0.417 ms
64 bytes from 192.168.1.29: icmp_seq=1 ttl=64 time=1.576 ms
64 bytes from 192.168.1.29: icmp_seq=2 ttl=64 time=2.327 ms

--- 192.168.1.29 ping statistics ---
3 packets transmitted, 3 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 0.417/1.448/2.327/0.786 ms
```

pfSense vers Debian

```
Enter a host name or IP address: 192.168.1.28

PING 192.168.1.28 (192.168.1.28): 56 data bytes
64 bytes from 192.168.1.28: icmp_seq=0 ttl=64 time=3.135 ms
64 bytes from 192.168.1.28: icmp_seq=1 ttl=64 time=2.118 ms
64 bytes from 192.168.1.28: icmp_seq=2 ttl=64 time=0.426 ms

--- 192.168.1.28 ping statistics ---
3 packets transmitted, 3 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 0.426/1.893/3.135/1.117 ms
```

pfSense vers OpenSUSE

```
root@debian-nginx:~# ping 192.168.1.28
PING 192.168.1.28 (192.168.1.28) 56(84) bytes of data.
64 bytes from 192.168.1.28: icmp_seq=1 ttl=64 time=1.51 ms
64 bytes from 192.168.1.28: icmp_seq=2 ttl=64 time=1.89 ms
64 bytes from 192.168.1.28: icmp_seq=3 ttl=64 time=0.990 ms
^C
--- 192.168.1.28 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2004ms
rtt min/avg/max/mdev = 0.990/1.462/1.887/0.367 ms
```

Debian vers OpenSUSE

```
root@debian-nginx:~# ping 192.168.1.30
PING 192.168.1.30 (192.168.1.30) 56(84) bytes of data.
64 bytes from 192.168.1.30: icmp_seq=1 ttl=64 time=1.37 ms
64 bytes from 192.168.1.30: icmp_seq=2 ttl=64 time=1.65 ms
64 bytes from 192.168.1.30: icmp_seq=3 ttl=64 time=1.46 ms
^C
--- 192.168.1.30 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2004ms
rtt min/avg/max/mdev = 1.373/1.491/1.645/0.113 ms
```

Debian vers pfSense

```
lucas@localhost:~$ ping 192.168.1.29
PING 192.168.1.29 (192.168.1.29) 56(84) bytes of data.
64 bytes from 192.168.1.29: icmp_seq=1 ttl=64 time=1.30 ms
64 bytes from 192.168.1.29: icmp_seq=2 ttl=64 time=1.37 ms
64 bytes from 192.168.1.29: icmp_seq=3 ttl=64 time=1.33 ms
^C
--- 192.168.1.29 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2004ms
rtt min/avg/max/mdev = 1.304/1.336/1.373/0.028 ms
```

openSUSE vers Debian

```
lucas@localhost:~$ ping 192.168.1.30
PING 192.168.1.30 (192.168.1.30) 56(84) bytes of data.
64 bytes from 192.168.1.30: icmp_seq=1 ttl=64 time=0.984 ms
64 bytes from 192.168.1.30: icmp_seq=2 ttl=64 time=0.422 ms
64 bytes from 192.168.1.30: icmp_seq=3 ttl=64 time=1.23 ms
^C
--- 192.168.1.30 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2019ms
rtt min/avg/max/mdev = 0.422/0.879/1.233/0.339 ms^C
```

openSUSE vers pfSense