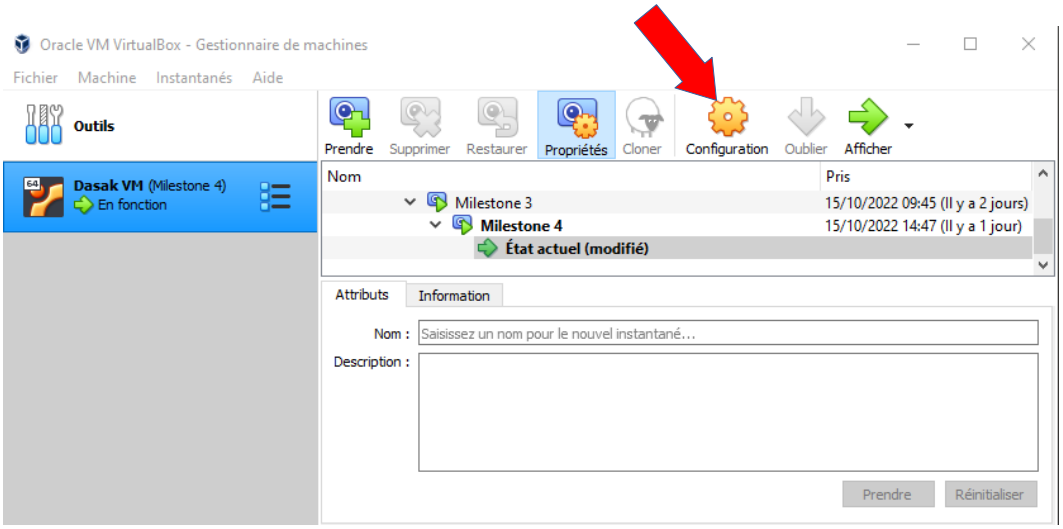
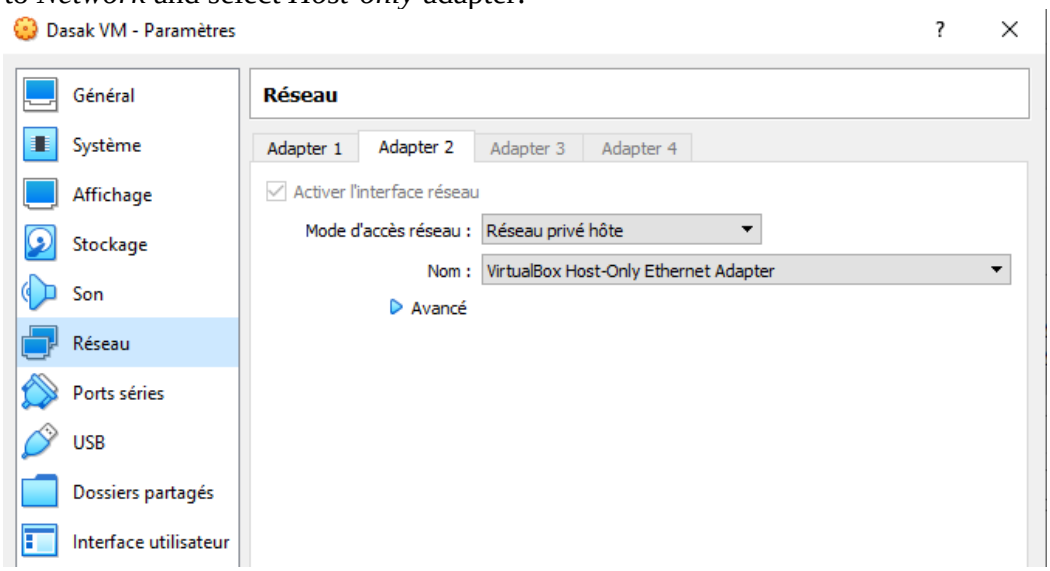
Documentation for the firewall problem

For this problem, we chose a very simple network configuration. We used the Dasak VM, which runs on Ubuntu, to host NodeBB, MongoDB, and the firewall. The host machine (Windows in our case), was like a client connecting from the internet to the forum:

First, we needed to enable communication from the host machine to the VM. To do this, open VirtualBox, select your VM and click on *Settings*:



Then, go to *Network* and select *Host-only* adapter:



After that, you can go to your VM and run ifconfig to find the IP of the machine on the dedicated interface. Try to ping this IP from the windows host. If it replies, then you have successfully connected the two computers.

Of course, it is not necessary to do it this way, you could for example run several machines or Vms that would represent different parts of the Network (the best example would be one computer for NodeBB, one for MongoDB, one for the firewall and one for the client.

To install NodeBB on your Linux server, please refer to the official documentation:
https://docs.nodebb.org/installing/os/ubuntu/

Next step is to define the firewall rules. If it is not done already, install iptables on the VM by running: *sudo apt-get install iptables*
After that, you can run the script *firewall.sh* included in the deliverables. Here is a screenshot of it:

```
#Flush all chains:
sudo iptables -F INPUT
sudo iptables -F OUTPUT
sudo iptables -F FORWARD

#Set DROP Default policy:
sudo iptables -P INPUT DROP
sudo iptables -P OUTPUT DROP
sudo iptables -P FORWARD DROP

#allowing web traffic on port 4567:
sudo iptables -A INPUT -p tcp --dport 4567 -j ACCEPT
sudo iptables -A OUTPUT -p tcp --sport 4567 -m conntrack --ctstate ESTABLISHED -j ACCEPT

#allowing loopback traffic (for connection to MongoDB):
sudo iptables -I INPUT -i lo -p tcp --sport 27017 -j ACCEPT
sudo iptables -I INPUT -i lo -p tcp --dport 27017 -j ACCEPT
sudo iptables -I OUTPUT -o lo -p tcp --sport 27017 -j ACCEPT
sudo iptables -I OUTPUT -o lo -p tcp --dport 27017 -j ACCEPT

#allow related connections:
sudo iptables -A INPUT -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT
```

To verify, run this command to display the firewall rules: *sudo iptables -vL*
You should have the following configuration:

```
Chain INPUT (policy DROP 21 packets, 3132 bytes)
 pkts bytes target     prot opt in     out     source               destination
 1640  388K ACCEPT     tcp  --  lo     any     anywhere             anywhere             tcp dpt:27017
 1049  269K ACCEPT     tcp  --  lo     any     anywhere             anywhere             tcp spt:27017
  980  127K ACCEPT     tcp  --  any    any     anywhere             anywhere             tcp dpt:4567
    0     0 ACCEPT     all  --  any    any     anywhere             anywhere             ctstate RELATED,ESTABLISHED

Chain FORWARD (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy DROP 330 packets, 30972 bytes)
 pkts bytes target     prot opt in     out     source               destination
 1640  388K ACCEPT     tcp  --  any    lo      anywhere             anywhere             tcp dpt:27017
 1049  269K ACCEPT     tcp  --  any    lo      anywhere             anywhere             tcp spt:27017
  988 3036K ACCEPT     tcp  --  any    any     anywhere             anywhere             tcp spt:4567 ctstate ESTABLISHED
```

Unfortunately, these rules will disappear everytime you restart the VM. To prevent that, you must store the configuration in a file by entering: `sudo iptables-save > path/to/file`
You can then retrieve them with: `sudo iptables-restore < path/to/file`

Once this is done, start NodeBB on the VM by running *./nodebb start*.
Then go back to the Windows Host, and connect to the forum on your browser: <IP adress>:4567
<IP adress> is the same adress you pinged earlier to connect to the VM. You should be able to access NodeBB, register an account, write posts, etc.

PS: If you have a network with more than 2 machines, then many rules in the INPUT and OUTPUT chain should be moved to the FORWARD chain. You will also need to verify the source and destination IP to make sure you have the communications you expected.