

REVIEW

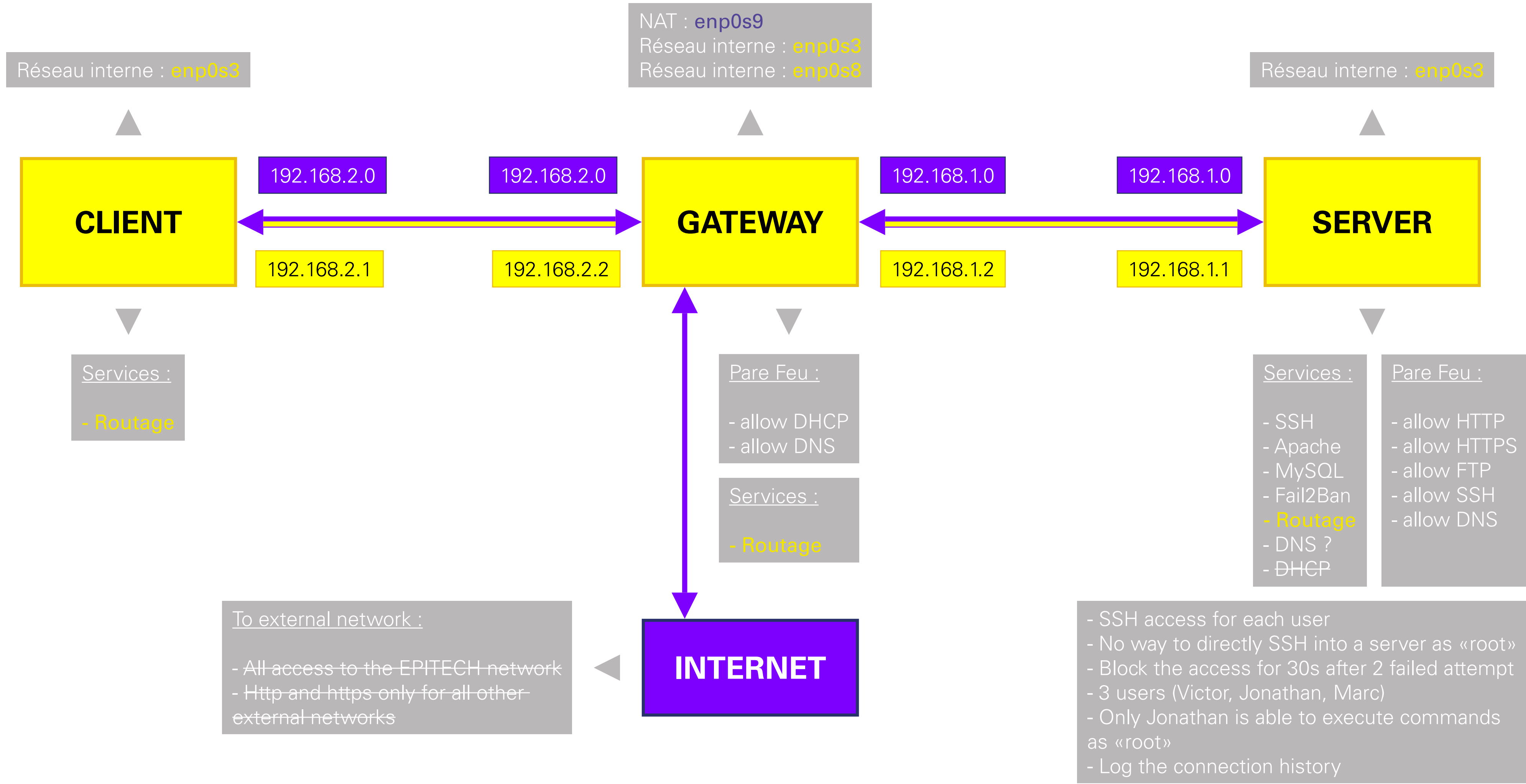
YOU SHALL NOT PASS

OBJECTIF

Réalisation d'un réseau en local constitué d'une architecture de 3 machines virtuelles (client, gateway, server) avec un système de sécurité.

Diagramme

Notre réseau actuel :



Routage

/etc/network/interfaces

Passerelle (gateway) entre un réseau et un autre.

CLIENT

GATEWAY

SERVER

```
GNU nano 3.2 /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

# Client network interface
auto enp0s3
allow-hotplug enp0s3
iface enp0s3 inet static
    address 192.168.2.1
    network 192.168.2.0
    netmask 255.255.255.0
    gateway 192.168.2.2
```

```
GNU nano 3.2 /etc/network
# This file describes the network interfaces available
# and how to activate them. For more information, see

#source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto enp0s9
allow-hotplug enp0s9
iface enp0s9 inet dhcp
post-up iptables-restore < /etc/iptables_rules.save

# Client network interface
auto enp0s3
allow-hotplug enp0s3
iface enp0s3 inet static
    address 192.168.2.2
    network 192.168.2.0
    netmask 255.255.255.0

# Server network interface
auto enp0s8
allow-hotplug enp0s8
iface enp0s8 inet static
    address 192.168.1.2
    network 192.168.1.0
    netmask 255.255.255.0
```

```
GNU nano 3.2 /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

# Server network interface
auto enp0s3
allow-hotplug enp0s3
iface enp0s3 inet static
    address 192.168.1.1
    network 192.168.1.0
    netmask 255.255.255.0
    gateway 192.168.1.2
    post-up iptables-restore < /etc/iptables.rules
```

SSH + Fail2Ban

ssh nom_utilisateur@ip_server

«Secure Shell» est un protocole de communication sécurisé. Il permet de se connecter à un hôte à distance de façon sécurisée sur un réseau qui ne l'est pas forcément. Fail2ban lit les fichiers de log et bannit les adresses IP qui ont obtenu un trop grand nombre d'échecs lors de l'authentification.

MARC

```
root@client:~# ssh Victor@192.168.1.1
Victor@192.168.1.1's password:
Linux server 4.19.0-6-amd64 #1 SMP Debian 4.19.67-2+deb10u1 (2019-09-20) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Wed Nov 13 23:19:07 2019 from 192.168.2.1
Victor@server:~$ sudo whoami
[sudo] Mot de passe de Victor :
Victor n'apparaît pas dans le fichier sudoers. Cet événement sera signalé.
Victor@server:~$
```

VICTOR

```
Victor@server:~$ ssh Marc@192.168.1.1
Marc@192.168.1.1's password:
Linux server 4.19.0-6-amd64 #1 SMP Debian 4.19.67-2+deb10u1 (2019-09-20) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Sun Nov 17 13:46:33 2019 from 192.168.1.1
Marc@server:~$ sudo whoami
[sudo] Mot de passe de Marc :
Marc n'apparaît pas dans le fichier sudoers. Cet événement sera signalé.
Marc@server:~$
```

JONATHAN

```
Marc@server:~$ ssh Jonathan@192.168.1.1
Jonathan@192.168.1.1's password:
Linux server 4.19.0-6-amd64 #1 SMP Debian 4.19.67-2+deb10u1 (2019-09-20) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Wed Nov 13 12:28:01 2019 from 192.168.1.1
Jonathan@server:~$ sudo whoami
[sudo] Mot de passe de Jonathan :
root
Jonathan@server:~$
```

ROOT

```
Jonathan@server:~$ ssh root@192.168.1.1
root@192.168.1.1's password:
Permission denied, please try again.
root@192.168.1.1's password: _
```

LOG

/var/log/auth.log

FAIL2BAN

/etc/fail2ban/jail.local

Pare Feu

Iptables est un logiciel libre grâce auquel l’administrateur système peut configurer les chaînes et règles du pare-feu en espace noyau. Netfilter est un framework implémentant le pare-feu au sein du noyau Linux.

Réinitialiser toutes les règles :
iptables -t filter -F
iptables -t filter -X

Tout bloquer :
iptables -t filter -P INPUT DROP
iptables -t filter -P FORWARD DROP
iptables -t filter -P OUTPUT DROP

Autoriser localhost:
iptables -t filter -A INPUT -i lo -j ACCEPT
iptables -t filter -A OUTPUT -o lo -j ACCEPT

Autoriser les connexions déjà établies :
iptables -A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
iptables -A OUTPUT -m state --state RELATED,ESTABLISHED -j ACCEPT

Ouverture port HTTP 80 et HTTPS 443 pour serveur web :
iptables -t filter -A OUTPUT -p tcp --dport 80 -j ACCEPT
iptables -t filter -A INPUT -p tcp --dport 80 -j ACCEPT
iptables -t filter -A OUTPUT -p tcp --dport 443 -j ACCEPT
iptables -t filter -A INPUT -p tcp --dport 443 -j ACCEPT

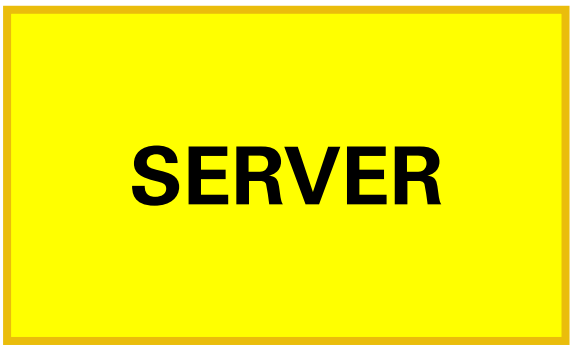
Autoriser ping :
iptables -t filter -A INPUT -p icmp -j ACCEPT
iptables -t filter -A OUTPUT -p icmp -j ACCEPT

Ouverture port SSH 22 :
iptables -t filter -A OUTPUT -p tcp --dport 22 -j ACCEPT
iptables -t filter -A INPUT -p tcp --dport 22 -j ACCEPT

Ouverture port DNS 53:
iptables -t filter -A OUTPUT -p udp --dport 53 -j ACCEPT
iptables -t filter -A INPUT -p udp --dport 53 -j ACCEPT

Ouverture port DHCP 68 :
iptables -t filter -A OUTPUT -p udp --dport 68 -j ACCEPT
iptables -t filter -A INPUT -p udp --dport 68 -j ACCEPT

Ouverture port FTP :
iptables -t filter -A OUTPUT -p tcp --dport 21 -j ACCEPT
iptables -t filter -A OUTPUT -p tcp --dport 20 -j ACCEPT
iptables -t filter -A INPUT -p tcp --dport 20 -j ACCEPT
iptables -t filter -A INPUT -p tcp --dport 21 -j ACCEPT
iptables -t filter -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT



```
GNU nano 3.2 iptables.rules
# Generated by xtables-save v1.8.2 on Fri Nov 15 10:19:20 2019
*filter
:INPUT DROP [0:0]
:FORWARD DROP [0:0]
:OUTPUT DROP [5710:430880]
-A INPUT -i lo -j ACCEPT
-A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
-A INPUT -p tcp -m tcp --dport 80 -j ACCEPT
-A INPUT -p tcp -m tcp --dport 443 -j ACCEPT
-A INPUT -p icmp -j ACCEPT
-A INPUT -p tcp -m tcp --dport 22 -j ACCEPT
-A INPUT -p udp -m udp --dport 53 -j ACCEPT
-A INPUT -p tcp -m tcp --dport 20 -j ACCEPT
-A INPUT -p tcp -m tcp --dport 21 -j ACCEPT
-A INPUT -m state --state RELATED,ESTABLISHED
-A OUTPUT -o lo -j ACCEPT
-A OUTPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
-A OUTPUT -p tcp -m tcp --sport 80 -j ACCEPT
-A OUTPUT -p tcp -m tcp --sport 443 -j ACCEPT
-A OUTPUT -p icmp -j ACCEPT
-A OUTPUT -p tcp -m tcp --sport 22 -j ACCEPT
-A OUTPUT -p udp -m udp --sport 53 -j ACCEPT
-A OUTPUT -p tcp -m tcp --sport 21 -j ACCEPT
-A OUTPUT -p tcp -m tcp --sport 20 -j ACCEPT
COMMIT
# Completed on Fri Nov 15 10:19:21 2019
```



```
GNU nano 3.2 /etc/iptables.rules
# Generated by xtables-save v1.8.2 on Wed Nov 13 21:46:18 2019
*nat
:PREROUTING ACCEPT [1068:78658]
:INPUT ACCEPT [0:0]
:POSTROUTING ACCEPT [2:120]
:OUTPUT ACCEPT [436:32374]
-A POSTROUTING -o enp0s3 -j MASQUERADE
-A POSTROUTING -o enp0s3 -j MASQUERADE
-A POSTROUTING -o enp0s9 -j MASQUERADE
COMMIT
# Completed on Wed Nov 13 21:46:18 2019
# Generated by xtables-save v1.8.2 on Wed Nov 13 21:46:18 2019
*filter
:INPUT DROP [0:0]
:FORWARD DROP [0:0]
:OUTPUT DROP [0:0]
-A INPUT -i lo -j ACCEPT
-A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
-A INPUT -p udp -m udp --dport 53 -j ACCEPT
-A INPUT -p udp -m udp --dport 68 -j ACCEPT
-A OUTPUT -o lo -j ACCEPT
-A OUTPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
-A OUTPUT -p udp -m udp --sport 53 -j ACCEPT
-A OUTPUT -p udp -m udp --sport 68 -j ACCEPT
COMMIT
# Completed on Wed Nov 13 21:46:19 2019
```


MySQL

sudo systemctl status mysql

MySQL est un serveur de base de données SQL (Structured Query Language) rapide, stable, entièrement multi-utilisateur et multitâche. SQL est le langage de requêtes de base de données le plus populaire au monde.



SERVER



```
root@server:~# sudo systemctl status mysql
• mysql.service - MySQL Community Server
  Loaded: loaded (/lib/systemd/system/mysql.service; enabled; vendor preset: enabled)
  Active: active (running) since Sun 2019-11-17 15:31:43 CET; 36min ago
    Docs: man:mysqld(8)
           http://dev.mysql.com/doc/refman/en/using-systemd.html
  Process: 425 ExecStartPre=/usr/share/mysql-8.0/mysql-systemd-start pre (code=exited, status=0/SUCCESS)
 Main PID: 475 (mysqld)
   Status: "Server is operational"
    Tasks: 38 (limit: 4701)
  Memory: 430.4M
    CGroup: /system.slice/mysql.service
            └─475 /usr/sbin/mysqld

nov. 17 15:31:37 server systemd[1]: Starting MySQL Community Server...
nov. 17 15:31:43 server systemd[1]: Started MySQL Community Server.
lines 1-15/15 (END)
```



Apache

`sudo systemctl status apache2`

C'est un serveur HTTP permettant à un site web de communiquer avec un navigateur en utilisant le protocole HTTP(S). Il est produit par la Apache Software Foundation. C'est un logiciel libre fourni sous la licence spécifique Apache. On utilise généralement Apache en conjonction avec d'autres logiciels, permettant d'interpréter du code et d'accéder à des bases de données. Le cas le plus courant est celui d'un serveur LAMP (Linux, Apache, MySQL, PHP).



SERVER



```
root@server:~# sudo systemctl status apache2
• apache2.service - The Apache HTTP Server
  Loaded: loaded (/lib/systemd/system/apache2.service; enabled; vendor preset: enabled)
  Active: active (running) since Sun 2019-11-17 15:31:40 CET; 40min ago
    Docs: https://httpd.apache.org/docs/2.4/
  Process: 477 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
 Main PID: 502 (apache2)
   Tasks: 55 (limit: 4701)
  Memory: 11.2M
   CGroup: /system.slice/apache2.service
           └─502 /usr/sbin/apache2 -k start
             └─503 /usr/sbin/apache2 -k start
               └─504 /usr/sbin/apache2 -k start

nov. 17 15:31:39 server systemd[1]: Starting The Apache HTTP Server...
nov. 17 15:31:40 server apachectl[477]: AH00558: apache2: Could not reliably determine the server's
nov. 17 15:31:40 server systemd[1]: Started The Apache HTTP Server.
lines 1-16/16 (END)
```


DHCP

service isc-dhcp-server status

Le Dynamic Host Configuration Protocol est le protocole utilisé pour l'assignation automatique des paramètres IP à des équipements informatiques. Il permet de faciliter l'administration surtout sur les grands réseaux ou l'attribution statique d'adresse à chaque poste est très fastidieuse (de plus les risques de conflit d'adresse sont son grand). Le protocole DHCP permet de transporter les informations comme : l'adresse IP de la machine, l'adresse du serveur DNS, l'adresse de la Passerelle, l'adresse de Broadcast ...

SERVER

```
root@server:~# service isc-dhcp-server status
• isc-dhcp-server.service - LSB: DHCP server
   Loaded: loaded (/etc/init.d/isc-dhcp-server; generated)
   Active: failed (Result: exit-code) since Sun 2019-11-17 15:31:42 CET; 49min ago
     Docs: man:systemd-sysv-generator(8)
   Process: 478 ExecStart=/etc/init.d/isc-dhcp-server start (code=exited, status=1/FAILURE)

nov. 17 15:31:40 server dhcpd[500]: bugs on either our web page at www.isc.org or in the README file
nov. 17 15:31:40 server dhcpd[500]: before submitting a bug. These pages explain the proper
nov. 17 15:31:40 server dhcpd[500]: process and the information we find helpful for debugging.
nov. 17 15:31:40 server dhcpd[500]:
nov. 17 15:31:40 server dhcpd[500]: exiting.
nov. 17 15:31:42 server isc-dhcp-server[478]: Starting ISC DHCPv4 server: dhcpdcheck syslog for diag
nov. 17 15:31:42 server isc-dhcp-server[478]: failed!
nov. 17 15:31:42 server systemd[1]: isc-dhcp-server.service: Control process exited, code=exited, st
nov. 17 15:31:42 server systemd[1]: isc-dhcp-server.service: Failed with result 'exit-code'.
nov. 17 15:31:42 server systemd[1]: Failed to start LSB: DHCP server.
lines 1-16/16 (END)
```

DNS

/etc/bind/

La mise en place d'un serveur DNS sur un réseau permet de remplacer les adresses IP des machines par un nom. Ainsi, il est possible d'associer plusieurs noms à la même machine pour mettre en évidence les différents services possibles.

SERVER

```
PING mondomaine.lan(localhost (::1)) 56 data bytes
64 bytes from localhost (::1): icmp_seq=1 ttl=64 time=0.015 ms
64 bytes from localhost (::1): icmp_seq=2 ttl=64 time=0.021 ms
64 bytes from localhost (::1): icmp_seq=3 ttl=64 time=0.022 ms

--- mondomaine.lan ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 33ms
rtt min/avg/max/mdev = 0.015/0.019/0.022/0.004 ms
root@server:/etc/bind# dig mondomaine.lan

; <<>> DiG 9.11.5-P4-5.1-Debian <<>> mondomaine.lan
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 2139
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 2
;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 4096
;; COOKIE: f220d5eb04d49d63ed8a725dd167a87a080579c3cbc963 (good)
;; QUESTION SECTION:
;mondomaine.lan.                IN      A

;; ANSWER SECTION:
mondomaine.lan.                604800 IN      A      192.168.1.1

;; AUTHORITY SECTION:
mondomaine.lan.                604800 IN      NS      ns.mondomaine.lan.

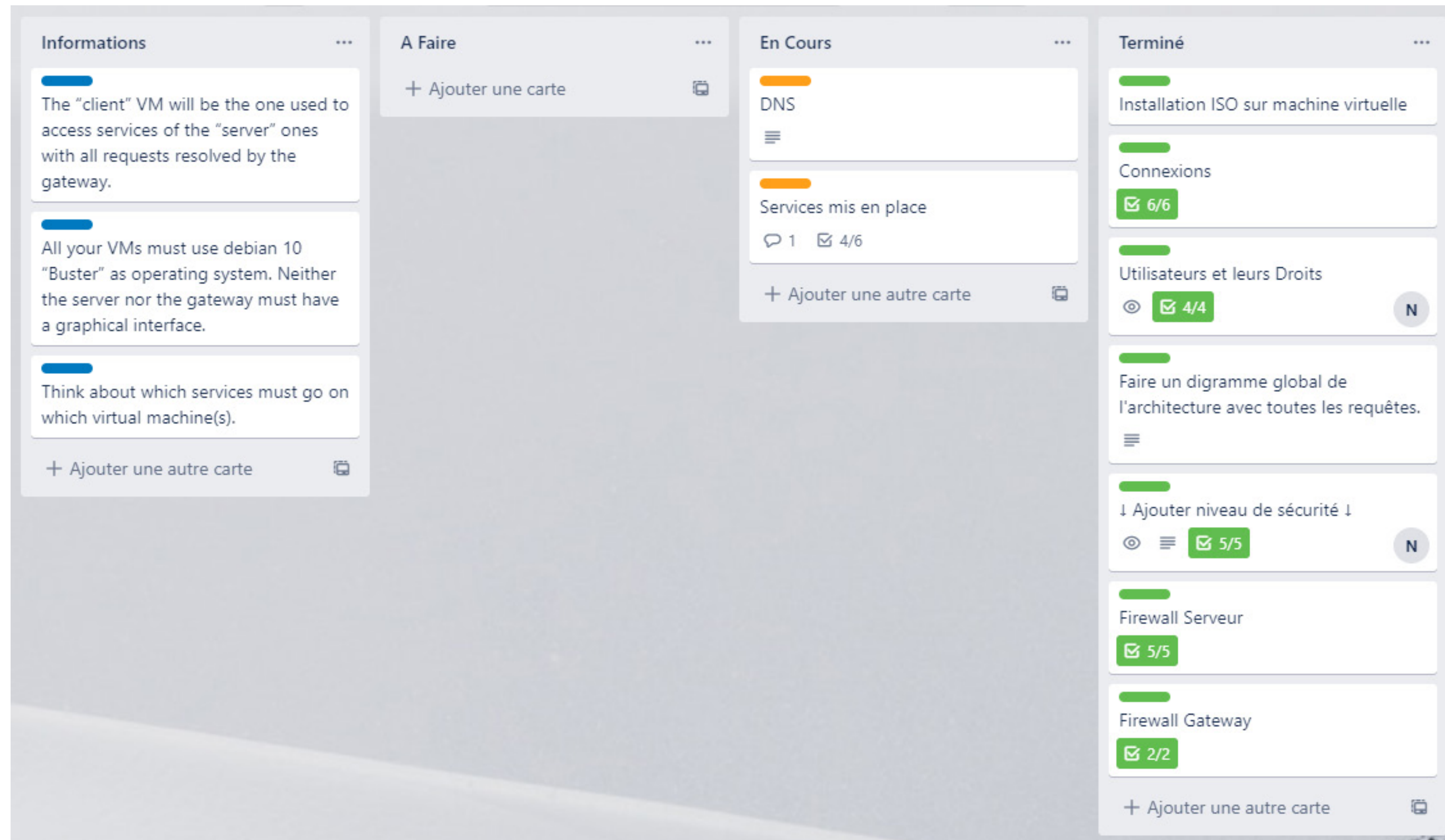
;; ADDITIONAL SECTION:
ns.mondomaine.lan.             604800 IN      A      192.168.1.1

;; Query time: 0 msec
;; SERVER: 192.168.1.1#53(192.168.1.1)
;; WHEN: dim. nov. 17 16:30:48 CET 2019
;; MSG SIZE rcvd: 120
```

```
root@server:/etc/bind# sudo systemctl status bind9
• bind9.service - BIND Domain Name Server
   Loaded: loaded (/lib/systemd/system/bind9.service; enabled; vendor preset: enabled)
   Active: active (running) since Sun 2019-11-17 15:31:39 CET; 1h 4min ago
     Docs: man:named(8)
   Process: 428 ExecStart=/usr/sbin/named $OPTIONS (code=exited, status=0/SUCCESS)
   Main PID: 442 (named)
      Tasks: 4 (limit: 4701)
     Memory: 17.3M
    CGroup: /system.slice/bind9.service
            └─442 /usr/sbin/named -4
```

Trello

Organisation du travail



FIN