# TP7 : On dit chiffrer pas crypter

## II. Serveur Web

### 1. HTTP

😇 Lister les ports en écoute sur la machine

```
[dylan@web ~]$ sudo ss -lnpt | grep 80
LISTEN 0      511          0.0.0.0:80        0.0.0.0:*    users:
(("nginx",pid=11173,fd=6),("nginx",pid=11172,fd=6))
LISTEN 0      511             [::]:80           [::]:*    users:
(("nginx",pid=11173,fd=7),("nginx",pid=11172,fd=7))
```

😇 Ouvrir le port dans le firewall de la machine

```
[dylan@web ~]$ sudo firewall-cmd --permanent --add-port=80/tcp
success
[dylan@web ~]$ sudo firewall-cmd --reload
success
```

## C. Tests client

😇 Vérifier que ça a pris effet

```
[dylan@client1 ~]$ ping sitedefou.tp7.b1
PING sitedefou.tp7.b1 (10.7.1.11) 56(84) bytes of data.
64 bytes from sitedefou.tp7.b1 (10.7.1.11): icmp_seq=1 ttl=64 time=1.11 ms
64 bytes from sitedefou.tp7.b1 (10.7.1.11): icmp_seq=2 ttl=64 time=0.882 ms
64 bytes from sitedefou.tp7.b1 (10.7.1.11): icmp_seq=3 ttl=64 time=0.936 ms
^C
--- sitedefou.tp7.b1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2005ms
rtt min/avg/max/mdev = 0.882/0.976/1.110/0.097 ms
```

```
[dylan@client1 ~]$ curl http://sitedefou.tp7.b1
meow !
```

## D. Analyze

😇 Voir la connexion établie

```
[dylan@client1 ~]$ sudo ss -npt | grep "10.7.1.11:80"
ESTAB 0      0               10.7.1.101:40666         10.7.1.11:80    users:
(("firefox",pid=13910,fd=61))
```

## 2. On rajoute un S

Lister les ports en écoute sur la machine

```
[dylan@web ~]$ sudo ss -lnpt | grep "443"
LISTEN 0      511        10.7.1.11:443       0.0.0.0:*    users:
(("nginx",pid=1500,fd=6),("nginx",pid=1499,fd=6))
```

Gérer le firewall

```
[dylan@web ~]$ sudo firewall-cmd --permanent --add-port=443/tcp
success
[dylan@web ~]$ sudo firewall-cmd --reload
success
[dylan@web ~]$ sudo firewall-cmd --permanent --remove-port=80/tcp
success
[dylan@web ~]$ sudo firewall-cmd --reload
success
```

## B. Test test test analyyyze

Capture tcp_https.pcap

# III. Serveur VPN

## 1. Install et conf Wireguard

Prouvez que vous avez bien une nouvelle carte réseau wg0

```
[dylan@vpn ~]$ 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: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP
group default qlen 1000
    link/ether 08:00:27:a0:0f:b0 brd ff:ff:ff:ff:ff:ff
```

```
    inet 10.7.1.111/24 brd 10.7.1.255 scope global noprefixroute enp0s3
       valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fea0:fb0/64 scope link
       valid_lft forever preferred_lft forever
3: enp0s8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP
group default qlen 1000
    link/ether 08:00:27:07:dd:11 brd ff:ff:ff:ff:ff:ff
    inet 10.7.2.111/24 brd 10.7.2.255 scope global noprefixroute enp0s8
       valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fe07:dd11/64 scope link
       valid_lft forever preferred_lft forever
😇10: wg0: <POINTOPOINT,NOARP,UP,LOWER_UP> mtu 1420 qdisc noqueue state UNKNOWN
group default qlen 1000
    link/none
    inet 10.7.200.1/24 scope global wg0
       valid_lft forever preferred_lft forever
```

😇 Déterminer sur quel port écoute Wireguard

```
[dylan@vpn ~]$ sudo ss -lnpu | grep 51820
UNCONN 0      0            0.0.0.0:51820      0.0.0.0:*
UNCONN 0      0               [::]:51820         [::]:*
```

😇 Ouvrez ce port dans le firewall

```
[dylan@vpn ~]$ sudo firewall-cmd --permanent --add-port=51820/udp
success
[dylan@vpn ~]$ sudo firewall-cmd --reload
success
```

# 3.Proofs

😇 Ping ping ping !

```
[dylan@client1 ~]$ ping 10.7.200.1
PING 10.7.200.1 (10.7.200.1) 56(84) bytes of data.
64 bytes from 10.7.200.1: icmp_seq=1 ttl=64 time=2.21 ms
64 bytes from 10.7.200.1: icmp_seq=2 ttl=64 time=1.28 ms
64 bytes from 10.7.200.1: icmp_seq=3 ttl=64 time=0.764 ms
64 bytes from 10.7.200.1: icmp_seq=4 ttl=64 time=1.49 ms
^C
--- 10.7.200.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3018ms
rtt min/avg/max/mdev = 0.764/1.435/2.211/0.519 ms
```

😇 Prouvez que vous avez toujours un accès internet

```
[dylan@client1 ~]$ traceroute 1.1.1.1
traceroute to 1.1.1.1 (1.1.1.1), 30 hops max, 60 byte packets
 1  _gateway (10.7.200.1)  2.388 ms  1.605 ms  2.251 ms
 2  * * *
 3  * * *
 4  * * *
 5  * * *
 6  * * *
```

## 4. Private service

```
[dylan@client1 ~]$ ping 10.7.200.37
PING 10.7.200.37 (10.7.200.37) 56(84) bytes of data.
64 bytes from 10.7.200.37: icmp_seq=1 ttl=64 time=0.041 ms
64 bytes from 10.7.200.37: icmp_seq=2 ttl=64 time=0.046 ms
64 bytes from 10.7.200.37: icmp_seq=3 ttl=64 time=0.048 ms
^X64 bytes from 10.7.200.37: icmp_seq=4 ttl=64 time=0.064 ms
^C
--- 10.7.200.37 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3091ms
rtt min/avg/max/mdev = 0.041/0.049/0.064/0.008 ms
```

```
[dylan@client1 ~]$ curl -k https://10.7.200.37
meow !
```