Mission 4 — Mettre en place le serveur de logs (rsyslog)

Objectif : Réceptionner les logs en **UDP/TCP 514** sur une VM Debian/Ubuntu.
Sur PC Ubuntu :

Activer la réception des logs :

```
sudo nano /etc/rsyslog.conf
```

Décommenter :

```
module(load="imudp")
input(type="imudp" port="514")
```

Redémarrer :

```
sudo systemctl restart rsyslog
```

Pour voir les logs :

```
sudo tail -f /var/log/syslog
```

PuTTy routeur + switch :

Activer l'horodatage :

```
service timestamps log datetime msec localtime show-timezone
service sequence-numbers
```

Logs interfaces (UP/DOWN) Switch et Routeur :

```
logging event link-status
```

5. ACL avec logs (seulement Routeur)

```
ip access-list extended SECURITE
   deny ip any any log
   permit ip any any

interface gi0/0/0
   ip access-group SECURITE in

interface gi0/0/1
   ip access-group SECURITE in
```

Port-Security (Switch) :

Téléphone + PC téléphone :

```
interface range fa0/6 , fa0/7, fa0/8
   switchport mode access
   switchport port-security
   switchport port-security maximum 2
   switchport port-security mac-address sticky
   switchport port-security violation restrict
```

CaméraIP :

```
interface range fa0/19 , fa0/20
   switchport mode access
   switchport port-security
   switchport port-security maximum 1
   switchport port-security mac-address sticky
   switchport port-security violation shutdown
```

Sur PC Ubuntu :

Activer la réception des logs :

```
sudo nano /etc/rsyslog.conf
```

Décommenter :

```
module(load="imudp")
input(type="imudp" port="514")
```

Redémarrer :

```
sudo systemctl restart rsyslog
```

Pour voir les logs :

```
sudo tail -f /var/log/syslog
```

Revision #2
Created 15 March 2026 19:59:06 by Raphaël
Updated 26 March 2026 13:03:50 by Raphaël