COMPTE RENDU TECHNIQUE - AP 15

Techniciens : Killian Goncalves & Cristopher Boni Fuentes Groupe : 8 Date : Février 2026

Mission 0 : Prérequis et contraintes

1. Organisation et Planification

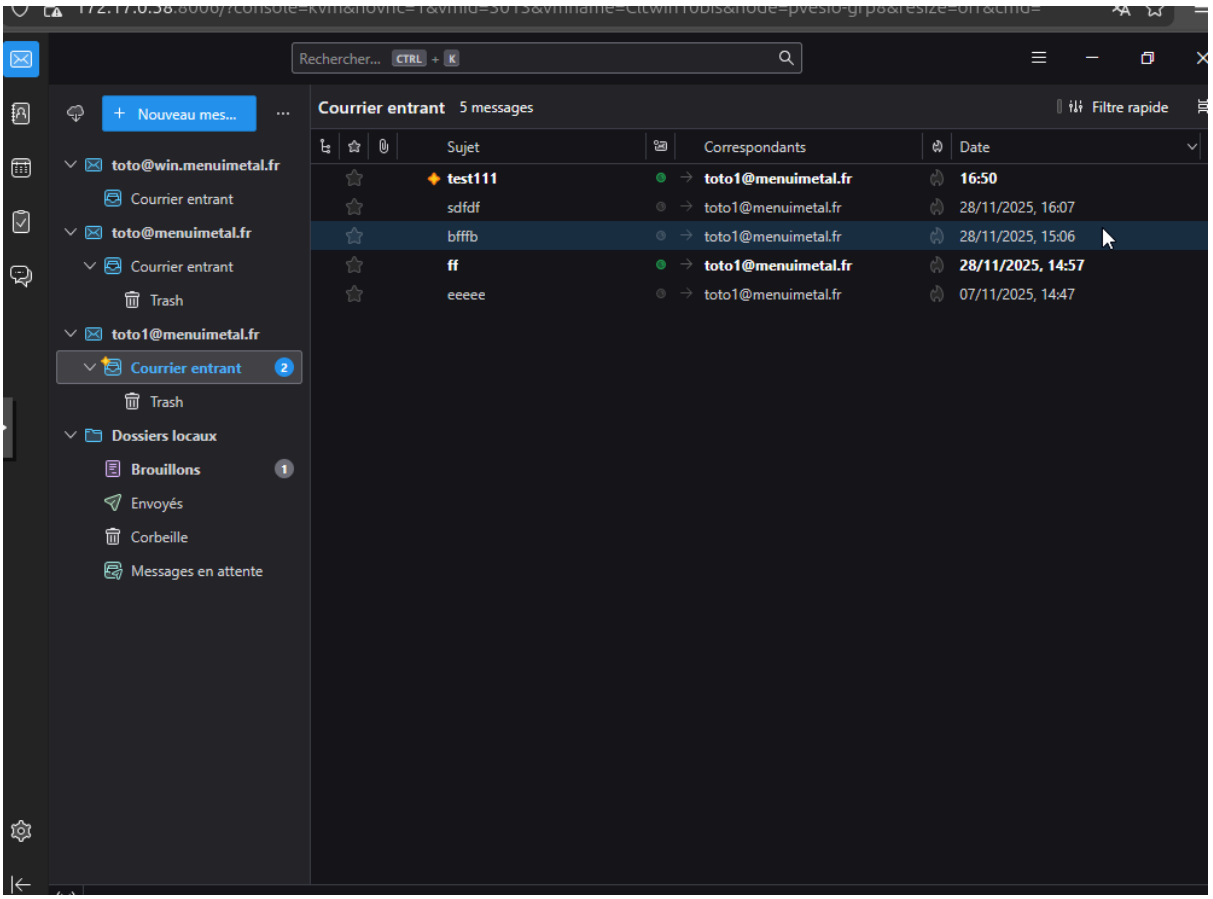
Conformément aux exigences de la mission, la première étape a consisté à organiser le travail en équipe.

- **Répartition des tâches :** Utilisation d'un diagramme de Gantt(lien Gantt) pour planifier les durées et la répartition entre les membres de l'équipe (Killian et Cristopher).
- **Mise à jour du schéma réseau :** Intégration des nouvelles machines virtuelles (Grafana, Prometheus, WebDAV) dans la topologie existante(lien shema).

2. Infrastructure Réseau et Commutation

Le groupe **8** utilise des VLANs spécifiques basés sur le chiffre **8**.

- **Configuration des switches :** Les switches Cisco Catalyst 2960G et HP ont été configurés pour supporter les VLANs suivants :
    - **VLAN 581 (LAN) :** Réseau local (192.168.11.0/24).
    - **VLAN 582 (DMZ) :** Zone démilitarisée pour le serveur WebDAV (192.168.12.0/24).
    - **VLAN 580 (GESTION) :** Réseau de supervision (192.168.13.0/24).



Mission 1 : SUDO

Questions :

1. Qu'est-ce que le concept de moindre privilège ?

Le **principe de moindre privilège** consiste à donner à un utilisateur ou à un programme **seulement les droits nécessaires pour faire son travail**, et pas plus. Cela permet **d'améliorer la sécurité du système**.

2. Avec la commande sudo, de quel groupe faut-il faire partie sous Debian ?

Il faut faire partie du **groupe sudo** pour pouvoir utiliser la commande **sudo** et avoir des privilèges d'administration.

3. Comment vérifier notre appartenance à un groupe sous Linux ?

On peut utiliser les commandes :

(groups ou id)

Ces commandes affichent les groupes auxquels appartient l'utilisateur.

4. C'est quoi le fichier sudoers ?

Le fichier **sudoers** est un **fichier de configuration** qui définit **quels utilisateurs peuvent utiliser sudo et quelles commandes ils peuvent exécuter**.

5. C'est quoi la commande visudo ? Quel est son avantage ?

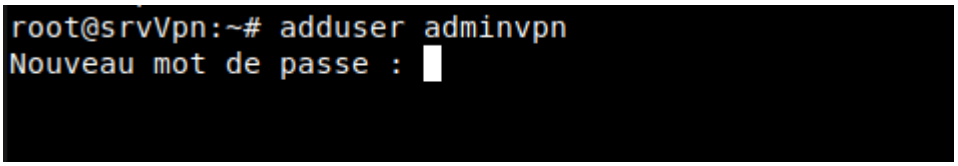
La commande **visudo** permet **de modifier le fichier sudoers en toute sécurité**.

Son avantage est qu'elle **vérifie les erreurs de syntaxe avant d'enregistrer**, ce qui évite de bloquer l'utilisation de sudo.

Objectifs attendus et contraintes :

• Un administrateur dédié (admin vpn) doit être le seul à pouvoir administrer le serviceopenvpn par l'utilisation du script easyrsa, sans avoir à saisir son mot de passe.

Création du compte dédié à l'administration exclusive d'OpenVPN
(MDP:12345678)



Identification de l'emplacement du script Easy-RSA sur le serveur afin de configurer précisément les privilèges de l'utilisateur adminvpn

```
root@srvVpn:~# find / -name easyrsa 2>/dev/null
/etc/openvpn/easy-rsa/easyrsa
/usr/share/easy-rsa/easyrsa
```

Configuration du fichier sudoers pour autoriser l'utilisateur adminvpn à exécuter le script Easy-RSA avec les privilèges root sans demande de mot de passe

```
root@srvVpn:~# visudo
```

Configuration du fichier sudoers pour autoriser l'utilisateur adminvpn à exécuter le script Easy-RSA avec les privilèges root sans demande de mot de passe.

```
adminvpn ALL=(ALL) NOPASSWD: /etc/openvpn/easy-rsa/easyrsa
```

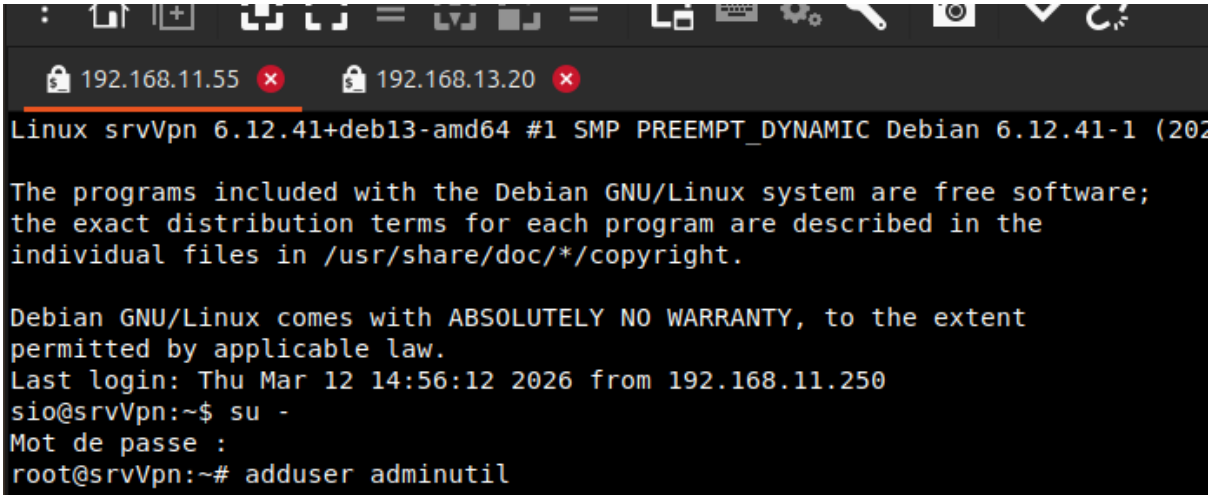
Validation du fonctionnement de sudo pour adminvpn : le script s'exécute correctement et accède aux répertoires de la PKI sans demande d'authentification

```
root@srvVpn:~# su - adminvpn
adminvpn@srvVpn:~$ sudo /etc/openvpn/easy-rsa/easyrsa help
```

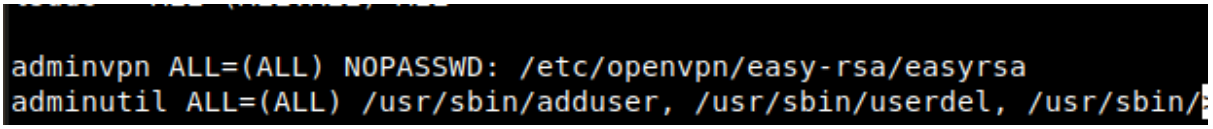
```
DIRECTORY STATUS (commands would take effect on these locations)
     EASYRSA: /home/adminvpn
         PKI: /home/adminvpn/pki
   vars-file: Missing or undefined
   CA status: CA has not been built
```

Un administrateur dédié (adminutil) doit être le seul à pouvoir administrer lesutilisateurs systèmes créés sur le serveur Linux utilisé pour Openvpn.

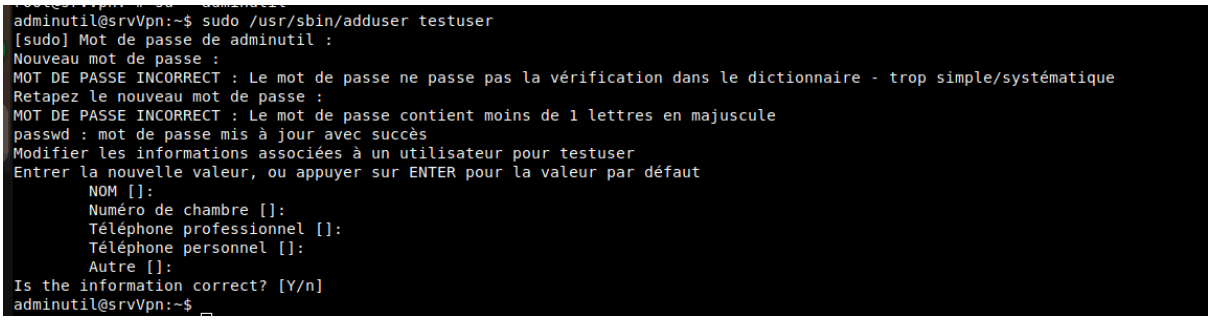
Création du second compte administrateur dédié, **adminutil**, qui sera restreint uniquement à la gestion des utilisateurs du système



Mise en place du principe de moindre privilège dans le fichier `sudoers` : l'utilisateur adminutil est limité aux seules commandes de gestion des comptes (`adduser`,`userdel`, `usermod`).

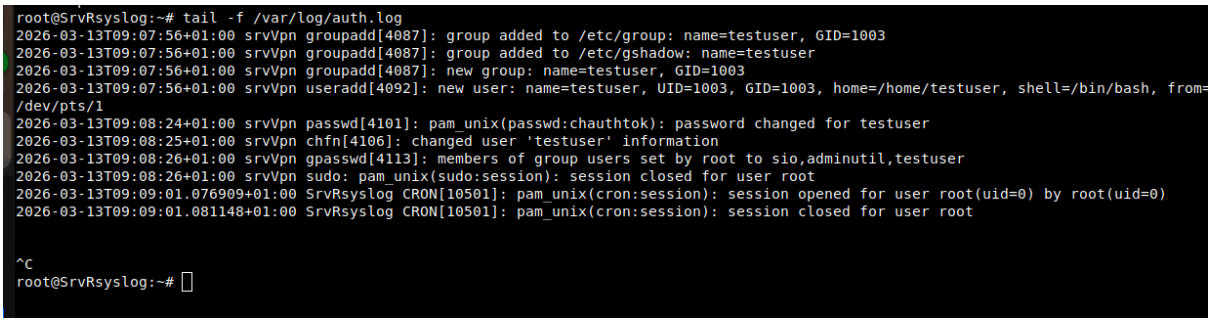


Test de validation pour l'administrateur dédié : l'utilisateur adminutil parvient à créer un nouveau compte système via sudo. Cela confirme que les privilèges de gestion des utilisateurs lui ont été correctement attribués dans le fichier sudoers.



Les logs générés par sudo (fichier /var/log/auth.log à condition d'avoir installé rsyslog) devront être redirigés vers votre serveur central rsyslog. Vous pouvez également consulter en local les logs avec la commande journalctl _COMM=sudo)

on voit les logs de `srvVpn` arriver sur le serveur de logs. Ça confirme que la redirection fonctionne.



TEST AVEC UN USER A FAIRE

Mission 2: PAM

3] Module PAM – Authentification plus robuste

Question : Quel est l'intérêt des modules PAM ?

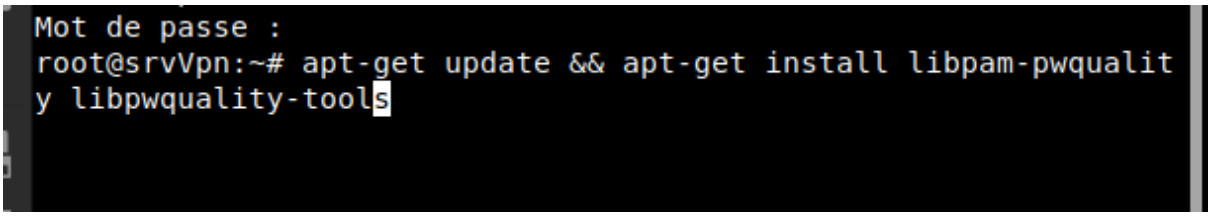
PAM (**Pluggable Authentication Modules**) est un système utilisé sous Linux qui permet de **gérer l'authentification des utilisateurs de manière centralisée et modulaire**.

Les modules PAM permettent :

- d'appliquer des **politiques de sécurité sur les mots de passe**

- de **renforcer l’authentification**
- d’ajouter des **restrictions d’accès** (horaires, services, etc.)
- de **modifier les règles de sécurité sans modifier les applications**

Grâce à PAM, un administrateur peut par exemple imposer **une longueur minimale de mot de passe, l’utilisation de caractères complexes ou des horaires d’accès**.



. Mise en place d'une politique de mots de passe (PAM pwquality)

Afin d'éviter les attaques par force brute ou par dictionnaire, la politique de création des mots de passe a été durcie.

- **Fichier modifié :** `/etc/pam.d/common-password`
- **Module utilisé :** `pam_pwquality.so`
- **Configuration appliquée :** `password requisite pam_pwquality.so retry=3 minlen=10 ucredit=-1 lcredit=-1 dcredit=-1 ocredit=-1`
- **Explication des paramètres :**
  - `retry=3` : Autorise 3 tentatives maximum en cas d'erreur de saisie.
  - `minlen=10` : Impose une longueur minimale de 10 caractères.
  - `ucredit=-1` : Exige au moins 1 lettre majuscule.
  - `lcredit=-1` : Exige au moins 1 lettre minuscule.
  - `dcredit=-1` : Exige au moins 1 chiffre.
  - `ocredit=-1` : Exige au moins 1 caractère spécial

```
root@srvVpn:~# sudo nano /etc/pam.d/common-password
```

```
# and here are more per-package modules (the "Additional" block)
# end of pam-auth-update config
password requisite pam_pwquality.so retry=3 minlen=10 ucredit=-1 lcredit=-1 dcredit=-1 ocredit=-1
```

```
root@srvVpn:~# sudo nano /etc/pam.d/common-auth
root@srvVpn:~#
```

Étape 2 : Définition de la règle de restriction

- **Fichier modifié :** `/etc/security/time.conf`
- **Règle appliquée :** `*;*;adminvpn|adminutil;!Wk1542-1545`
- **Explication de la syntaxe :**
  - `*` (Service) : S'applique à tous les services (login, su, ssh, etc.).
  - `*` (Terminal) : S'applique à tous les terminaux (tty, pts, etc.).
  - `adminvpn|adminutil` (Utilisateurs) : Cible spécifiquement les comptes `adminvpn` et `adminutil`.
  - `!Wk1542-1545` (Temps) : Refuse (`!`) l'accès les jours de la semaine (`Wk` pour Weekdays) entre 15h42 et 15h45.

```
déconnexion
adminvpn@srvVpn:~$ su - adminvpn
Mot de passe :
adminvpn@srvVpn:~$ su - adminvpn
Mot de passe :
adminvpn@srvVpn:~$ ^C
adminvpn@srvVpn:~$ exit
déconnexion
adminvpn@srvVpn:~$ exit
déconnexion
root@srvVpn:~# su -
root@srvVpn:~# sudo nano /etc/security/time.conf
root@srvVpn:~#
```

```
;*;adminvpn|adminutil;!Wk1542-1545
```

3. Tests et validation

Pour vérifier l'efficacité de la restriction horaire, un test a été réalisé durant la plage de blocage (entre 15h42 et 15h45).

- **Action :** Depuis la session de l'utilisateur standard `sio`, tentative d'élévation de privilèges vers l'utilisateur restreint avec la commande `su - adminvpn`.
- **Résultat :** Après saisie du mot de passe correct, le système a retourné l'erreur **"su: Autorisation refusée"**.

- **Conclusion :** Le test est concluant. Le module `pam_time` fonctionne correctement et empêche bien l'ouverture de session pour ces utilisateurs durant la plage horaire définie, même si le mot de passe est valide.

```
déconnexion
sio@srvVpn:~$ su - adminvpn
Mot de passe :
su: Autorisation refusée
sio@srvVpn:~$
```

Installation du module de sécurité

Pour renforcer la complexité des mots de passe, il faut installer le module :

apt install libpam-pwquality

Ce module permet de **contrôler la qualité et la complexité des mots de passe**.

Configuration de la complexité des mots de passe

Modifier le fichier :

5] UFW ou le pare-feu « facile »

```
root@SrvMail:~# sudo apt install ufw
```

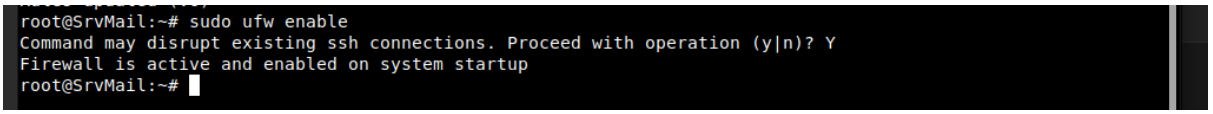
sudo ufw status verbose

```
root@SrvMail:~# sudo ufw status verbose
Status: inactive
root@SrvMail:~#
```

3 Activer les logs UFW

sudo ufw logging on

```
root@SrvMail:~# sudo ufw logging on
Logging enabled
```



Lire les logs

tail -f /var/log/ufw.log

```
root@SrvMail:~# tail -f /var/log/ufw.log
2026-03-12T17:04:38.262259+01:00 SrvMail kernel: [UFW BLOCK] IN=ens18 OUT= MAC=bc:24:11:05:6c:2e:bc:24:11:ee
:d7:92:08:00 SRC=192.168.11.200 DST=192.168.12.14 LEN=41 TOS=0x00 PREC=0x00 TTL=127 ID=60957 DF PROTO=TCP SP
T=53017 DPT=143 WINDOW=1022 RES=0x00 ACK URGP=0
2026-03-12T17:04:38.416050+01:00 SrvMail kernel: [UFW BLOCK] IN=ens18 OUT= MAC=bc:24:11:05:6c:2e:bc:24:11:ee
:d7:92:08:00 SRC=192.168.11.200 DST=192.168.12.14 LEN=41 TOS=0x00 PREC=0x00 TTL=127 ID=60958 DF PROTO=TCP SP
T=53015 DPT=143 WINDOW=1022 RES=0x00 ACK URGP=0
2026-03-12T17:04:42.693400+01:00 SrvMail kernel: [UFW BLOCK] IN=ens18 OUT= MAC=bc:24:11:05:6c:2e:bc:24:11:ee
:d7:92:08:00 SRC=192.168.11.200 DST=192.168.12.14 LEN=41 TOS=0x00 PREC=0x00 TTL=127 ID=60959 DF PROTO=TCP SP
T=53018 DPT=143 WINDOW=1024 RES=0x00 ACK URGP=0
2026-03-12T17:04:42.693424+01:00 SrvMail kernel: [UFW BLOCK] IN=ens18 OUT= MAC=bc:24:11:05:6c:2e:bc:24:11:ee
:d7:92:08:00 SRC=192.168.11.200 DST=192.168.12.14 LEN=41 TOS=0x00 PREC=0x00 TTL=127 ID=60960 DF PROTO=TCP SP
T=53016 DPT=143 WINDOW=1025 RES=0x00 ACK URGP=0
2026-03-12T17:04:43.264479+01:00 SrvMail kernel: [UFW BLOCK] IN=ens18 OUT= MAC=bc:24:11:05:6c:2e:bc:24:11:ee
:d7:92:08:00 SRC=192.168.11.200 DST=192.168.12.14 LEN=41 TOS=0x00 PREC=0x00 TTL=127 ID=60961 DF PROTO=TCP SP
T=53017 DPT=143 WINDOW=1022 RES=0x00 ACK URGP=0
2026-03-12T17:04:43.433504+01:00 SrvMail kernel: [UFW BLOCK] IN=ens18 OUT= MAC=bc:24:11:05:6c:2e:bc:24:11:ee
:d7:92:08:00 SRC=192.168.11.200 DST=192.168.12.14 LEN=41 TOS=0x00 PREC=0x00 TTL=127 ID=60962 DF PROTO=TCP SP
T=53015 DPT=143 WINDOW=1022 RES=0x00 ACK URGP=0
2026-03-12T17:04:47.695161+01:00 SrvMail kernel: [UFW BLOCK] IN=ens18 OUT= MAC=bc:24:11:05:6c:2e:bc:24:11:ee
:d7:92:08:00 SRC=192.168.11.200 DST=192.168.12.14 LEN=41 TOS=0x00 PREC=0x00 TTL=127 ID=60963 DF PROTO=TCP SP
T=53018 DPT=143 WINDOW=1024 RES=0x00 ACK URGP=0
2026-03-12T17:04:47.695205+01:00 SrvMail kernel: [UFW BLOCK] IN=ens18 OUT= MAC=bc:24:11:05:6c:2e:bc:24:11:ee
:d7:92:08:00 SRC=192.168.11.200 DST=192.168.12.14 LEN=41 TOS=0x00 PREC=0x00 TTL=127 ID=60964 DF PROTO=TCP SP
T=53016 DPT=143 WINDOW=1025 RES=0x00 ACK URGP=0
2026-03-12T17:04:57.697384+01:00 SrvMail kernel: [UFW BLOCK] IN=ens18 OUT= MAC=bc:24:11:05:6c:2e:bc:24:11:ee
:d7:92:08:00 SRC=192.168.11.200 DST=192.168.12.14 LEN=41 TOS=0x00 PREC=0x00 TTL=127 ID=60971 DF PROTO=TCP SP
T=53018 DPT=143 WINDOW=1024 RES=0x00 ACK URGP=0
2026-03-12T17:05:17.739800+01:00 SrvMail kernel: [UFW BLOCK] IN=ens18 OUT= MAC=bc:24:11:05:6c:2e:bc:24:11:ee
:d7:92:08:00 SRC=192.168.11.200 DST=192.168.12.14 LEN=41 TOS=0x00 PREC=0x00 TTL=127 ID=60987 DF PROTO=TCP SP
```

Générer un log pour tester

Depuis une autre machine (par exemple srvVpn ou client) on fais :

ping 192.168.12.14

ou

ssh 192.168.12.14:

```
-bash: pam_time : commande introuvable
root@SrvRsyslog:~# ping 192.168.12.14
PING 192.168.12.14 (192.168.12.14) 56(84) bytes of data.
64 bytes from 192.168.12.14: icmp_seq=1 ttl=63 time=1.23 ms
64 bytes from 192.168.12.14: icmp_seq=2 ttl=63 time=1.24 ms
64 bytes from 192.168.12.14: icmp_seq=3 ttl=63 time=1.09 ms
64 bytes from 192.168.12.14: icmp_seq=4 ttl=63 time=1.12 ms
64 bytes from 192.168.12.14: icmp_seq=5 ttl=63 time=1.32 ms
^C
--- 192.168.12.14 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4006ms
rtt min/avg/max/mdev = 1.087/1.199/1.318/0.084 ms
root@SrvRsyslog:~#
```

et dans le srv Rsyslog dans le fichier su.log si son fait un tail -f on verras tout les logs de authentification

```
50378 DPT=514 WINDOW=64240 RES=0x00 SYN URGP=0
2026-03-12T17:09:13.064143+01:00 SrvMail kernel: [UFW BLOCK] IN=ens18 OUT= MAC=bc:24:11:05:6c:2e:bc:24:11:ee
:d7:92:08:00 SRC=192.168.13.20 DST=192.168.12.14 LEN=60 TOS=0x00 PREC=0x00 TTL=63 ID=14881 DF PROTO=TCP SPT=
50378 DPT=514 WINDOW=64240 RES=0x00 SYN URGP=0
2026-03-12T17:09:14.088096+01:00 SrvMail kernel: [UFW BLOCK] IN=ens18 OUT= MAC=bc:24:11:05:6c:2e:bc:24:11:ee
:d7:92:08:00 SRC=192.168.13.20 DST=192.168.12.14 LEN=60 TOS=0x00 PREC=0x00 TTL=63 ID=14882 DF PROTO=TCP SPT=
50378 DPT=514 WINDOW=64240 RES=0x00 SYN URGP=0
2026-03-12T17:09:16.104011+01:00 SrvMail kernel: [UFW BLOCK] IN=ens18 OUT= MAC=bc:24:11:05:6c:2e:bc:24:11:ee
:d7:92:08:00 SRC=192.168.13.20 DST=192.168.12.14 LEN=60 TOS=0x00 PREC=0x00 TTL=63 ID=14883 DF PROTO=TCP SPT=
50378 DPT=514 WINDOW=64240 RES=0x00 SYN URGP=0
2026-03-12T17:09:20.200202+01:00 SrvMail kernel: [UFW BLOCK] IN=ens18 OUT= MAC=bc:24:11:05:6c:2e:bc:24:11:ee
:d7:92:08:00 SRC=192.168.13.20 DST=192.168.12.14 LEN=60 TOS=0x00 PREC=0x00 TTL=63 ID=14884 DF PROTO=TCP SPT=
50378 DPT=514 WINDOW=64240 RES=0x00 SYN URGP=0
2026-03-12T17:09:44.520038+01:00 SrvMail kernel: [UFW BLOCK] IN=ens18 OUT= MAC=bc:24:11:05:6c:2e:bc:24:11:ee
:d7:92:08:00 SRC=192.168.13.20 DST=192.168.12.14 LEN=60 TOS=0x00 PREC=0x00 TTL=63 ID=14886 DF PROTO=TCP SPT=
50378 DPT=514 WINDOW=64240 RES=0x00 SYN URGP=0
2026-03-12T17:10:18.311921+01:00 SrvMail kernel: [UFW BLOCK] IN=ens18 OUT= MAC=bc:24:11:05:6c:2e:bc:24:11:ee
:d7:92:08:00 SRC=192.168.13.20 DST=192.168.12.14 LEN=60 TOS=0x00 PREC=0x00 TTL=63 ID=14887 DF PROTO=TCP SPT=
50378 DPT=514 WINDOW=64240 RES=0x00 SYN URGP=0
^C
```

Ajouter les services mail demandés

Ton TP demande :

- ***SMTP (envoi mail)***
- ***IMAP (réception mail)***

Ajoute ces règles :

```
root@SrvMail:~# sudo ufw allow 25/tcp
Rule added
Rule added (v6)
root@SrvMail:~# sudo ufw allow 143/tcp
Rule added
Rule added (v6)
```

Vérifier les règles

```
Rule added (v6)
root@SrvMail:~# sudo ufw status numbered
Status: active

     To                         Action      From
     --                         ------      ----
[ 1] 22/tcp                     ALLOW IN    Anywhere
[ 2] 25/tcp                     ALLOW IN    Anywhere
[ 3] 143/tcp                    ALLOW IN    Anywhere
[ 4] 22/tcp (v6)                ALLOW IN    Anywhere (v6)
[ 5] 25/tcp (v6)                ALLOW IN    Anywhere (v6)
[ 6] 143/tcp (v6)               ALLOW IN    Anywhere (v6)
```

Vérifier les logs UFW

Maintenant regarde :

*ls /var/log/ufw**

Puis :

tail -f /var/log/ufw.log

```
root@SrvMail:~# tail -f /var/log/ufw.log
2026-03-12T17:17:26.344026+01:00 SrvMail kernel: [UFW BLOCK] IN=ens18 OUT= MAC=bc:24:11:05:6c:2e:bc:24:11:
:d7:92:08:00 SRC=192.168.13.20 DST=192.168.12.14 LEN=60 TOS=0x00 PREC=0x00 TTL=63 ID=30226 DF PROTO=TCP SP
53108 DPT=514 WINDOW=64240 RES=0x00 SYN URGP=0
2026-03-12T17:17:37.223221+01:00 SrvMail kernel: [UFW BLOCK] IN= OUT=ens18 SRC=192.168.12.14 DST=10.0.2.3
N=67 TOS=0x00 PREC=0x00 TTL=64 ID=9168 DF PROTO=UDP SPT=60383 DPT=53 LEN=47
2026-03-12T17:18:07.475228+01:00 SrvMail kernel: [UFW BLOCK] IN= OUT=ens18 SRC=192.168.12.14 DST=10.0.2.3
N=67 TOS=0x00 PREC=0x00 TTL=64 ID=32514 DF PROTO=UDP SPT=42403 DPT=53 LEN=47
2026-03-12T17:18:07.476924+01:00 SrvMail kernel: [UFW BLOCK] IN= OUT=ens18 SRC=192.168.12.14 DST=10.0.2.3
N=67 TOS=0x00 PREC=0x00 TTL=64 ID=43351 DF PROTO=UDP SPT=51447 DPT=53 LEN=47
2026-03-12T17:18:37.723228+01:00 SrvMail kernel: [UFW BLOCK] IN= OUT=ens18 SRC=192.168.12.14 DST=10.0.2.3
N=67 TOS=0x00 PREC=0x00 TTL=64 ID=59161 DF PROTO=UDP SPT=45046 DPT=53 LEN=47
2026-03-12T17:19:07.975227+01:00 SrvMail kernel: [UFW BLOCK] IN= OUT=ens18 SRC=192.168.12.14 DST=10.0.2.3
N=67 TOS=0x00 PREC=0x00 TTL=64 ID=63346 DF PROTO=UDP SPT=45621 DPT=53 LEN=47
2026-03-12T17:19:07.976919+01:00 SrvMail kernel: [UFW BLOCK] IN= OUT=ens18 SRC=192.168.12.14 DST=10.0.2.3
N=67 TOS=0x00 PREC=0x00 TTL=64 ID=32273 DF PROTO=UDP SPT=39440 DPT=53 LEN=47
2026-03-12T17:19:38.223351+01:00 SrvMail kernel: [UFW BLOCK] IN= OUT=ens18 SRC=192.168.12.14 DST=10.0.2.3
N=67 TOS=0x00 PREC=0x00 TTL=64 ID=7574 DF PROTO=UDP SPT=44718 DPT=53 LEN=47
2026-03-12T17:20:08.475231+01:00 SrvMail kernel: [UFW BLOCK] IN= OUT=ens18 SRC=192.168.12.14 DST=10.0.2.3
N=67 TOS=0x00 PREC=0x00 TTL=64 ID=9346 DF PROTO=UDP SPT=43093 DPT=53 LEN=47
2026-03-12T17:20:08.477143+01:00 SrvMail kernel: [UFW BLOCK] IN= OUT=ens18 SRC=192.168.12.14 DST=10.0.2.3
N=67 TOS=0x00 PREC=0x00 TTL=64 ID=53224 DF PROTO=UDP SPT=59612 DPT=53 LEN=47
```

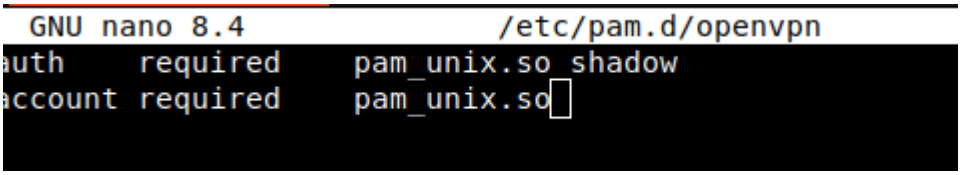
Mission 3: *Fail2ban et OpenVPN*

Questions :

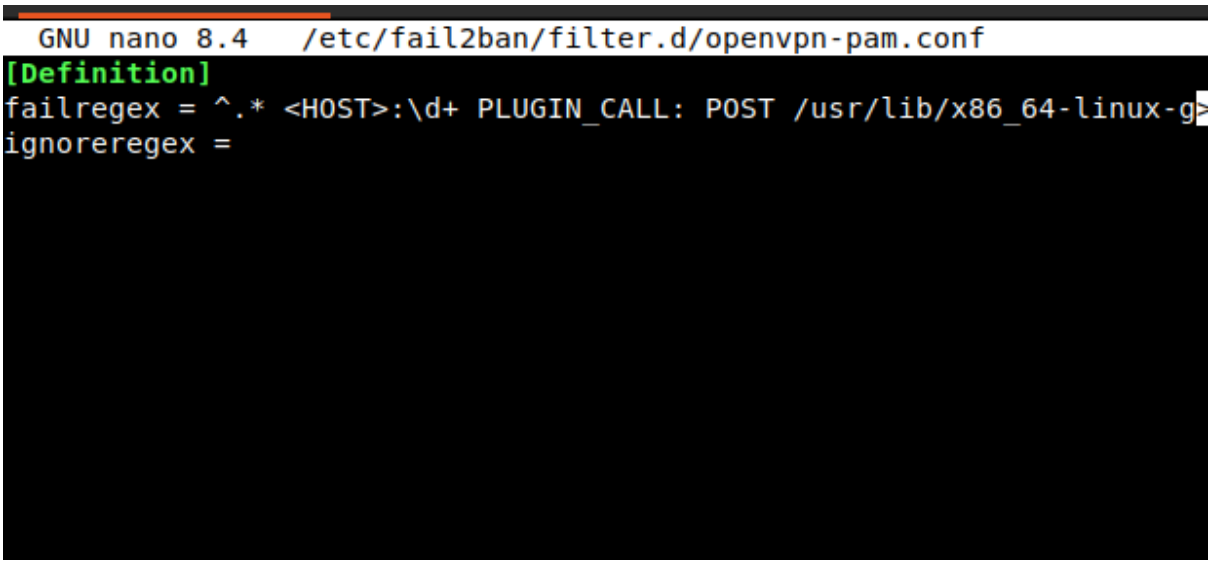
• C'est quoi l'authentification multi facteur ?

*C'est une méthode de sécurité qui demande **deux preuves différentes** pour se connecter : un élément que l'on possède (le **certificat OpenVPN**) et un élément que l'on connaît (le **login/mot de passe**).*

*On crée le fichier de configuration **PAM** pour OpenVPN.*

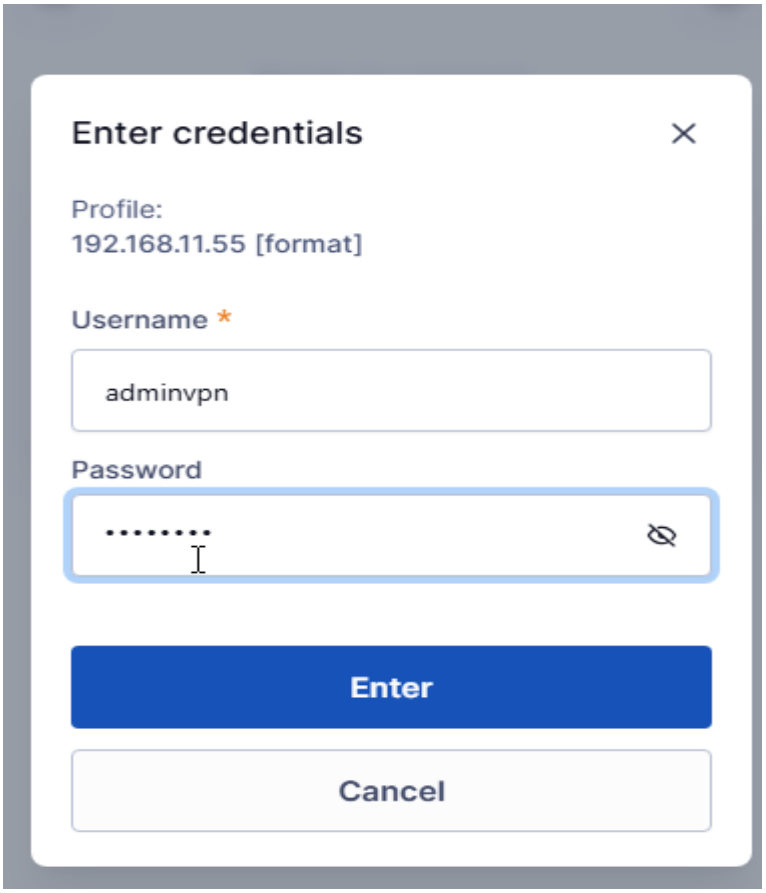


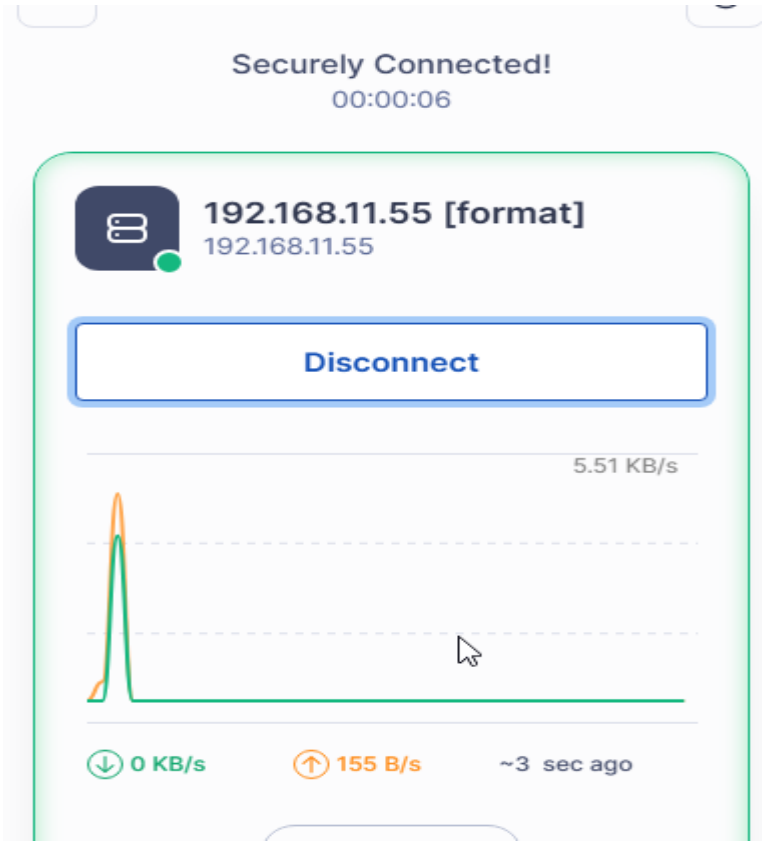
*Ajout du plugin d'authentification PAM pour l'authentification double facteur et activation de l'option **`ifconfig-pool-persist`** pour assurer le suivi des adresses IP attribuées aux clients*



```
  GNU nano 8.4              /etc/fail2ban/jail.local *
[openvpn-pam]
enabled  = true
port     = 1194
protocol = udp
filter   = openvpn-pam
logpath  = /var/log/openvpn.log
maxretry = 3
bantime  = 3600
```

```
Fichier  Edition  Format  Affichage  Aide
client
dev tun
proto udp
remote 192.168.11.55 1194
nobind
auth-nocache
remote-cert-tls server
auth-user-pass
```


Enter credentials
Profile:
192.168.11.55 [format]
Username *
adminvpn
Password
Enter
Cancel


Securely Connected!
00:00:06
192.168.11.55 [format]
192.168.11.55
Disconnect
5.51 KB/s
0 KB/s
155 B/s
~3 sec ago

Mission 4 : UFW

```
Mot de passe :
root@SrvMail:~# apt install ufw
```

```
root@SrvMail:~# ufw logging on
Logging enabled
```

Bloquer le trafic entrant par défaut avec la commande : `ufw default deny incoming`

Bloquer également le trafic sortant selon la consigne avec la commande : `ufw default deny outgoing`

```
root@SrvMail:~# ufw default deny incoming
Default incoming policy changed to 'deny'
(be sure to update your rules accordingly)
```

*Éditez le fichier de configuration : (/etc/default/ufw) puis modifier la ligne **IPV6=yes** en **IPV6=no** dans le fichier de configuration afin de désactiver les règles liées à IPv6.*

```
  GNU nano 8.4                                  /etc/default/ufw
# /etc/default/ufw
#

# Set to yes to apply rules to support IPv6 (no means only IPv6 on loopback
# accepted). You will need to 'disable' and then 'enable' the firewall for
# the changes to take affect.
IPV6=no
```

```
root@SrvMail:~# ufw status verbose
Status: active
Logging: on (low)
Default: deny (incoming), deny (outgoing), disabled (routed)
New profiles: skip

To                         Action      From
--                         ------      ----
22/tcp                     ALLOW IN    Anywhere
25/tcp                     ALLOW IN    Anywhere
143/tcp                    ALLOW IN    Anywhere
```