

# **AP - 13 SUDO, PAM, Fail2ban et UFW**

**Présenté par :**

Yassir Chellik ET Gaetan Bracale

**Année 2024 - 2025**

# **1. Prérequis**

- GANTT et schéma réseau
  - Référencement des serveurs dans DNS, inventaire dans GLPI et supervision via Nagios
- 
- Serveur de mail fonctionnel
  - Serveur Rsyslog fonctionnel

Nous avons référencé les vms dans notre serveur dns, et nous avons également testé avec un nslookup et le nom de notre machine référencer, les résultats obtenus sont : le nom de domaine, l'adresse ip de la machine et du serveur dns

```
dns      IN      A      192.168.12.1
mysql    IN      A      192.168.11.1
web      IN      A      192.168.12.2
routeur  IN      A      192.168.12.254
srvwebwordpress IN    A      192.168.11.3
srvlinuxglpi  IN    A      192.168.13.2
servermail    IN    A      192.168.12.4
srv-rancid    IN    A      192.168.13.7
srv-nagios    IN    A      192.168.13.8
omvdebian    IN    A      192.168.11.28
serverdhcpdebian IN  A      192.168.11.29
serverradius  IN    A      192.168.13.9
serv-syslog   IN    A      192.168.11.31
web-1        IN    A      192.168.11.32
web-2        IN    A      192.168.11.33
web-3        IN    A      192.168.11.34
mariadb-2    IN    A      192.168.11.37
debianclient-hhr IN  A      192.168.11.35
serverhaproxy IN  A      192.168.11.36
mariadb-2    IN    A      192.168.11.37
serverhaproxy2 IN  A      192.168.11.38
clientwindowsvpn IN  A      192.168.11.39
OpenVPN-Serv IN  A      192.168.11.42
```

```
smtp     IN      CNAME  servermail
imap     IN      CNAME  servermail
~
~
~
"/var/cache/bind/db.menuimetal.fr" 46L, 947B écrit(s)
root@dns:~# systemctl restart bind9
root@dns:~# systemctl restart bind9
root@dns:~# nslookup
> OpenVPN-Serv
Server:      192.168.12.1
Address:     192.168.12.1#53

Name:   OpenVPN-Serv.menuimetal.fr
Address: 192.168.11.42

[5]+  Stoppé                  nslookup
root@dns:~#
```

Nous allons ensuite référencer nos machine openvpn sur notre glpi, en lui installant

l'agent glpi et en les mettant dans leurs entités :

```
● glpi-agent.service - GLPI agent
   Loaded: loaded (/lib/systemd/system/glpi-agent.service; enabled; preset: enabled)
   Active: active (running) since Thu 2024-12-12 11:36:41 CET; 1 day 2h ago
     Docs: man:glpi-agent
   Main PID: 513 (glpi-agent: wai)
    Tasks: 1 (limit: 2306)
   Memory: 92.6M
      CPU: 23.676s
   CGroup: /system.slice/glpi-agent.service
           └─513 "glpi-agent: waiting"

déc. 12 11:36:41 OpenVPN-Serv systemd[1]: Started glpi-agent.service - GLPI agent.
déc. 12 11:36:42 OpenVPN-Serv glpi-agent[513]: [info] GLPI Agent starting
déc. 12 11:36:43 OpenVPN-Serv glpi-agent[513]: [info] [http server] HTTPD service started on port 62354
déc. 12 11:36:43 OpenVPN-Serv glpi-agent[513]: [info] target server0: next run: Fri Dec 13 09:38:47 2024 - http://192.168.13.2/glpi
déc. 13 09:38:47 OpenVPN-Serv glpi-agent[513]: [info] target server0: server http://192.168.13.2/glpi
déc. 13 09:38:47 OpenVPN-Serv glpi-agent[513]: [info] sending contact request to server0
déc. 13 09:38:49 OpenVPN-Serv glpi-agent[5376]: [info] running task Inventory
déc. 13 09:38:49 OpenVPN-Serv glpi-agent[5376]: [info] New inventory from OpenVPN-Serv-2024-12-12-08-52-43 for server0
déc. 13 09:39:00 OpenVPN-Serv glpi-agent[513]: [info] target server0: next run: Sat Dec 14 09:04:52 2024 - http://192.168.13.2/glpi

~
```

☐ **OpenVPN-Serv**      Entité racine ▶ Menuimetal ▶ Bâtiment-A ▶  
Etage-2 Salle serveur

☐ **clientewindowsvpn**      Entité racine ▶ Menuimetal ▶ Batiment-B ▶  
Etage-1 4 Ateliers

Il faut également la mettre en supervisions sur notre serveur nagios, en lui installant l'outil NRPE et en acceptant la connection de notre serveur nagios dans le fichier de configuration :

```
ii nagios-nrpe-server      4.1.0-1+b1      amd64      Nagios Remote Plugin Ex
Server
root@OpenVPN-Serv:/#
```

```
# NOTE: This option is ignored if NRPE is running under either inetd or xinetd
allowed_hosts=127.0.0.1,192.168.13.8

# COMMAND ARGUMENT PROCESSING
# This option determines whether or not the NRPE daemon will allow clients
```

Ici nous avons eu un léger problème, en effet nous avons fait la supervision à la fin du TP, ducoup après la configuration du

parefeu, openvpn n'acceptais pas la connection des appareil distante car le firewall bloqué, ducoup il a fallu désactiver le pare feu afin de laisser nagios connecter la machine :

```
sio@srv-nagios:~$ su -  
Mot de passe :  
root@srv-nagios:~# /usr/local/nagios/libexec/check_nrpe -H 192.168.11.42  
CHECK_NRPE STATE CRITICAL: Socket timeout after 10 seconds.  
root@srv-nagios:~# /usr/local/nagios/libexec/check_nrpe -H 192.168.11.42  
CHECK_NRPE STATE CRITICAL: Socket timeout after 10 seconds.  
root@srv-nagios:~# /usr/local/nagios/libexec/check_nrpe -H 192.168.11.42  
CHECK_NRPE STATE CRITICAL: Socket timeout after 10 seconds.  
root@srv-nagios:~# /usr/local/nagios/libexec/check_nrpe -H 192.168.11.42  
CHECK_NRPE STATE CRITICAL: Socket timeout after 10 seconds.  
root@srv-nagios:~# /usr/local/nagios/libexec/check_nrpe -H 192.168.11.42  
NRPE v4.1.0  
root@srv-nagios:~#
```

```
root@OpenVPN-Serv:/# ufw status  
Status: inactive  
root@OpenVPN-Serv:/#
```

Attribué les services / plugins pour ma machine :

```
sio@srv-nagios: ~  
sio@OpenVPN-Serv: ~ x sio@C419-32: ~ x sio@srv-nagio  
# Nagios Host configuration file template  
define host {  
    use linux-server  
    host_name OpenVPN-Serv  
    alias Open Vpn Server  
    address 192.168.11.42  
    register 1  
}  
  
define service {  
    use local-service  
    host_name OpenVPN-Serv  
    service_description PING  
    check_command check_ping!100.0,20%!500.0,60%  
}  
  
define service {  
    use local-service  
    host_name OpenVPN-Serv  
    service_description Load Average  
    check_command check_local_load!15,10,5!20,15,10  
}
```

Test du serveur mail qui est opérationnel :

Limit Results: 100

Host	Status	Last Check	Duration	Status Information
OpenVPN-Serv	UP	12-13-2024 15:04:00	0d 0h 0m 25s+	PING OK - Paquets perdus = 0%, RTA = 1.06 ms

test AP 13 from toto  
TEST AP 13

4 Reactions

Archive Junk Delete Activate

**Inb...** 5 Messages Quick Fil...

toto 26/11/2024 17:20  
Tarte pour axel

toto 03/12/2024 15:18  
test AP - 12

haproxysupport@menuim... 06/12/2024 15:01  
[HAProxy Alert] Server mysql\_back/...

haproxysupport@menuim... 06/12/2024 15:04  
[HAProxy Alert] Server mysql\_back/...

toto 16:45  
test AP 13

toto <toto@menuimetal.fr>  
toto@menuimetal.fr

To jeanmorin@menuimetal.fr

test AP 13

TEST AP 13

L'organisation gantt :

## AP- 13 SUDO, PAM, Fail2ban et UFW

## 2. Partie 1 : SUDO - Affinage des privilèges

- Gestion des privilèges administratifs pour `adminvpn` et `adminutil`

Dans le fichier texte référencement des permissions sudo j'ai donné la permission d'exécuter des commandes pour éditer, accéder et voir en règle générale les dossiers demandés pour l'utilisateur `adminvpn` et la gestion des utilisateur pour l'utilisateur `adminutil`

```
adminutil ALL=(ALL) /usr/sbin/adduser, /usr/sbin/deluser, /usr/sbin/usermod
# Autoriser adminvpn à utiliser sudo uniquement dans /etc/openvpn/easy-rsa/
Cmd_Alias EASYRSA_CMDS = /usr/bin/vim /etc/openvpn/easy-rsa/*, /usr/bin/nano /etc/openvpn/easy-rsa/*,
# donne la permission d'utiliser sudo uniquement pour les commandes spécifiées
adminvpn ALL=(ALL) NOPASSWD: EASYRSA_CMDS
```

^G Aide    ^O Écrire    ^W Chercher    ^K Couper    ^T Exécuter    ^C Emplacement    M-U Ann  
^X Quitter    ^R Lire fich.    ^\ Remplacer    ^U Coller    ^J Justifier    ^\_ Aller ligne    M-E Ref

Voici la démonstrations des commandes pour les utilisateurs attribuer :

```
adminvpn@OpenVPN-Serv:~$ sudo ls /root
sudo: impossible de résoudre l'hôte OpenVPN-Serv: Nom ou service inconnu
[sudo] Mot de passe de adminvpn :
Sorry, user adminvpn is not allowed to execute '/usr/bin/ls /root' as root on OpenVPN-Serv.
adminvpn@OpenVPN-Serv:~$
```

```
adminutil@OpenVPN-Serv:~$ sudo adduser
sudo: impossible de résoudre l'hôte OpenVPN-Serv: Nom ou service inconnu
adduser : Un ou deux noms maximum.
adminutil@OpenVPN-Serv:~$ sudo deluser
sudo: impossible de résoudre l'hôte OpenVPN-Serv: Nom ou service inconnu
Veuillez indiquer un nom d'utilisateur à supprimer :^C
adminutil@OpenVPN-Serv:~$ sudo usermod
sudo: impossible de résoudre l'hôte OpenVPN-Serv: Nom ou service inconnu
Utilisation : usermod[options] LOGIN
```



```

adminutil@OpenVPN-Serv:~$ sudo adduser toto
sudo: impossible de résoudre l'hôte OpenVPN-Serv: Nom ou service inconnu
Ajout de l'utilisateur « toto » ...
Ajout du nouveau groupe « toto » (1004) ...
Ajout du nouvel utilisateur « toto » (1004) avec le groupe « toto » (1004) ...
Création du répertoire personnel « /home/toto » ...
Copie des fichiers depuis « /etc/skel » ...
Nouveau mot de passe :
MOT DE PASSE INCORRECT : Aucun mot de passe fourni
Retapez le nouveau mot de passe :
Aucun mot de passe n'a été fourni.
Mot de passe : Erreur de manipulation du jeton d'authentification
passwd : mot de passe inchangé
Essayer à nouveau ? [o/N]n
Modifier les informations associées à un utilisateur pour toto
Entrer la nouvelle valeur, ou appuyer sur ENTER pour la valeur par défaut
  NOM []:
  Numéro de chambre []:
  Téléphone professionnel []:
  Téléphone personnel []:
  Autre []:
Cette information est-elle correcte ? [o/n]o
Ajout du nouvel utilisateur « toto » aux groupes supplémentaires « users » ...
Ajout de l'utilisateur « toto » au groupe « users » ...
adminutil@OpenVPN-Serv:~$ sudo deluser toto
sudo: impossible de résoudre l'hôte OpenVPN-Serv: Nom ou service inconnu
Suppression du crontab ...
Suppression de l'utilisateur « toto » ...
Fait.

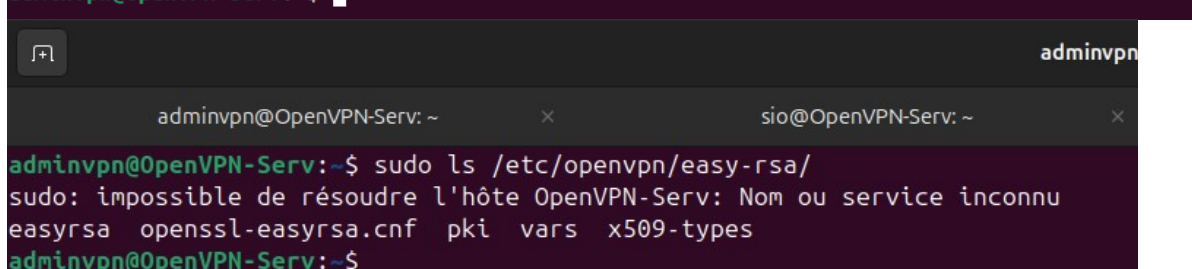
```

L'utilisateur n'as pas la permission de créer un utilisateur pour l'utilisateur adminvpn et d'accéder aux dossier attribuer pour l'autre utilisateur adminutils :

```

adminvpn@OpenVPN-Serv:~$ sudo adduser
sudo: impossible de résoudre l'hôte OpenVPN-Serv: Nom ou service inconnu
[sudo] Mot de passe de adminvpn :
Sorry, user adminvpn is not allowed to execute '/usr/sbin/adduser' as root on OpenVPN-Serv.
adminvpn@OpenVPN-Serv:~$

```



```

adminvpn@OpenVPN-Serv:~$ sudo ls /etc/openssl/easy-rsa/
sudo: impossible de résoudre l'hôte OpenVPN-Serv: Nom ou service inconnu
easyrsa openssl-easyrsa.cnf pki vars x509-types
adminvpn@OpenVPN-Serv:~$

```

## Redirection des logs de SUDO vers le serveur central Rsyslog dans un fichier spécifique :

```
root@OpenVPN-Serv:~# systemctl status rsyslog.service
● rsyslog.service - System Logging Service
   Loaded: loaded (/lib/systemd/system/rsyslog.service; enabled; preset: enab>
   Active: active (running) since Thu 2024-12-12 14:06:51 CET; 24h ago
   TriggeredBy: ● syslog.socket
     Docs: man:rsyslogd(8)
           man:rsyslog.conf(5)
           https://www.rsyslog.com/doc/
   Main PID: 1891 (rsyslogd)
     Tasks: 4 (limit: 2306)
    Memory: 3.1M
       CPU: 184ms
    CGroup: /system.slice/rsyslog.service
           └─1891 /usr/sbin/rsyslogd -n -iNONE

déc. 12 14:06:51 OpenVPN-Serv systemd[1]: Starting rsyslog.service - System Log>
déc. 12 14:06:51 OpenVPN-Serv systemd[1]: Started rsyslog.service - System Logg>
déc. 12 14:06:51 OpenVPN-Serv rsyslogd[1891]: imuxsock: Acquired UNIX socket '/>
déc. 12 14:06:51 OpenVPN-Serv rsyslogd[1891]: [origin software="rsyslogd" swVer>
lines 1-18/18 (END)
```

## Envoie des logs vers le serveur central, configuration du fichier rsyslog.conf

```
# Emergencies are sent to everybody logged in.
#
*.emerg                                :omusrmsg:*

*.*@192.168.11.31:514

~

60,1      Bas
```

```
syslog.log
root@serv-syslog:/var/log/clients/192.168.11.42#
```

```

2024-12-12T16:19:09+01:00 OpenVPN-Serv sudo: adminvpn : unable to resolve host OpenVPN-Serv: Name or service not known
2024-12-12T16:19:10+01:00 OpenVPN-Serv sudo: adminvpn : TTY=pts/3 ; PWD=/home/adminvpn ; USER=root ; COMMAND=/usr/bin/vim /etc/openvpn/easy-rsa/
2024-12-12T16:19:10+01:00 OpenVPN-Serv sudo: pam_unix(sudo:session): session opened for user root(uid=0) by adminvpn(uid=1003)
2024-12-12T16:19:13+01:00 OpenVPN-Serv sudo: pam_unix(sudo:session): session closed for user root
2024-12-12T16:19:23+01:00 OpenVPN-Serv sudo: adminvpn : unable to resolve host OpenVPN-Serv: Name or service not known
2024-12-12T16:19:23+01:00 OpenVPN-Serv sudo: adminvpn : TTY=pts/3 ; PWD=/home/adminvpn ; USER=root ; COMMAND=/usr/bin/ls /etc/openvpn/easy-rsa/
2024-12-12T16:19:23+01:00 OpenVPN-Serv sudo: pam_unix(sudo:session): session opened for user root(uid=0) by adminvpn(uid=1003)
2024-12-12T16:19:23+01:00 OpenVPN-Serv sudo: pam_unix(sudo:session): session closed for user root
2024-12-12T16:20:44+01:00 OpenVPN-Serv sudo: adminvpn : unable to resolve host OpenVPN-Serv: Name or service not known
2024-12-12T16:20:45+01:00 OpenVPN-Serv sudo: adminvpn : command not allowed ; TTY=pts/3 ; PWD=/home/adminvpn ; USER=root ; COMMAND=/usr/sbin/adduser
2024-12-12T16:22:06+01:00 OpenVPN-Serv sudo: root : unable to resolve host OpenVPN-Serv: Name or service not known
2024-12-12T16:22:06+01:00 OpenVPN-Serv sudo: root : TTY=pts/1 ; PWD=/root ; USER=root ; COMMAND=/usr/bin/ls /root
2024-12-12T16:22:06+01:00 OpenVPN-Serv sudo: pam_unix(sudo:session): session opened for user root(uid=0) by sio(uid=0)
2024-12-12T16:22:06+01:00 OpenVPN-Serv sudo: pam_unix(sudo:session): session closed for user root
2024-12-12T16:22:17+01:00 OpenVPN-Serv sudo: adminvpn : unable to resolve host OpenVPN-Serv: Name or service not known
2024-12-12T16:22:19+01:00 OpenVPN-Serv sudo: adminvpn : command not allowed ; TTY=pts/3 ; PWD=/home/adminvpn ; USER=root ; COMMAND=/usr/bin/ls /root
2024-12-12T16:22:26+01:00 OpenVPN-Serv sudo: adminvpn : unable to resolve host OpenVPN-Serv: Name or service not known
2024-12-12T16:22:26+01:00 OpenVPN-Serv sudo: adminvpn : TTY=pts/3 ; PWD=/home/adminvpn ; USER=root ; COMMAND=/usr/bin/vim /etc/openvpn/easy-rsa/
2024-12-12T16:22:26+01:00 OpenVPN-Serv sudo: pam_unix(sudo:session): session opened for user root(uid=0) by adminvpn(uid=1003)
2024-12-12T16:22:31+01:00 OpenVPN-Serv sudo: pam_unix(sudo:session): session closed for user root

```

### **3. Partie 2 : PAM - Renforcement de l'authentification**

- Mise en place des règles de complexité des mots de passe pour les administrateurs
- Configuration des restrictions horaires d'accès pour `adminvpn` et `adminutil`

PAM (Pluggable Authentication Modules) est un système flexible sous Linux qui gère l'authentification des utilisateurs. Il permet d'ajouter ou de modifier facilement des méthodes d'authentification (comme mots de passe, clés...) pour les services. PAM agit comme un intermédiaire entre les applications et les mécanismes d'authentification.

Nous allons commencer par installer le paquet pam

```
root@OpenVPN-Serv:~# dpkg -l | grep libpam-pwquality
ii  libpam-pwquality:amd64      1.4.5-1+b1                amd64
    PAM module to check password strength
root@OpenVPN-Serv:~#
```

Les fichiers de configuration de PAM se trouvent principalement dans le répertoire `/etc/pam.d/`. Voici les principaux fichiers et leur rôle :

## /etc/pam.d/common-auth

Gère les règles d'authentification (par exemple, mot de passe ou biométrie).

## /etc/pam.d/common-account

Vérifie si un compte utilisateur est valide ou actif.

## /etc/pam.d/common-password

Définit les règles pour la gestion des mots de passe, comme la complexité ou la durée de validité.

## /etc/pam.d/common-session

Gère les sessions utilisateurs (montage de répertoires, paramètres à appliquer).

## /etc/pam.d/login

Spécifique au service de connexion des utilisateurs via login.

Ici nous allons modifier le fichier de config common-password pour déterminer les paramètres de création de mot de passe comme par exemple, la taille des mdp, combien d'essai de création, les majuscules et chiffres requis...

```
GNU nano 7.2 /etc/pam.d/common-password *
# "OBSOLETE_CHECKS_ENAB" option in login.defs. See the pam_unix manpage
# for other options.

# As of pam 1.0.1-6, this file is managed by pam-auth-update by default.
# To take advantage of this, it is recommended that you configure any
# local modules either before or after the default block, and use
# pam-auth-update to manage selection of other modules. See
# pam-auth-update(8) for details.

# here are the per-package modules (the "primary" block)
password requisite pam_pwquality.so retry=3 minlen=10 ucredit=-1 lcredit=-1 dcredit=-1 pcredit=-1
password [success=1 default=ignore] pam_unix.so obscure use_authtok try_first_pass yescrypt
# here's the fallback if no module succeeds
```

Voici un test :

```
adminutil@OpenVPN-Serv:~$ passwd
Changement du mot de passe pour adminutil.
Mot de passe actuel :
Nouveau mot de passe :
MOT DE PASSE INCORRECT : Le mot de passe contient moins de 1 chiffres
Nouveau mot de passe :
MOT DE PASSE INCORRECT : Le mot de passe contient moins de 1 lettres en majuscule
Nouveau mot de passe :
MOT DE PASSE INCORRECT : Le mot de passe contient moins de 1 chiffres
Mot de passe : Nombre maximum de tentatives épuisées pour le service
passwd : mot de passe inchangé
adminutil@OpenVPN-Serv:~$
```

Pour gérer le temps ou des restrictions horaires dans PAM, on utilise le module `pam_time.so`.

Il permet de restreindre l'accès aux services (comme login ou ssh) en fonction de plages horaires ou de jours définis. Les règles se configurent dans le fichier `/etc/security/time.conf`. Par exemple,

on peut interdire les connexions à certains utilisateurs le week-end ou en dehors des heures de travail.

```
GNU nano 7.2 /etc/pam.d/common-auth
#
# As of pam 1.0.1-6, this file is managed by pam-auth-u
# To take advantage of this, it is recommended that you
# local modules either before or after the default bloc
# pam-auth-update to manage selection of other modules.
# pam-auth-update(8) for details.
#
# here are the per-package modules (the "Primary" block
auth [success=1 default=ignore] pam_unix.so nul
# here's the fallback if no module succeeds
auth requisite pam_deny.so
# prime the stack with a positive return value if there
# this avoids us returning an error just because nothin
# since the modules above will each just jump around
auth required pam_permit.so
# and here are more per-package modules (the "Additional
# end of pam-auth-update config

account required pam_time.so

```

^G Aide    ^O Écrire    ^W Chercher    ^K Couper    ^T  
^X Quitter    ^R Lire fich.    ^\ Remplacer    ^U Coller    ^J

Ici nous avons dit qu'il n'est pas autorisé de se connecter entre 14h et 15h, pour dire qu'il est autorisé il faut enlever le point d'exclamation avant la plage d'horaire :











```
# by the applying process.
#
#
# Here is a simple example: running blank on tty* (any ttyX)
# the users 'you' and 'me' are denied service all of the time
#
#blank;tty* & !ttyp*;you|me;!Al0000-2400
#
# Another silly example, user 'root' is denied xsh access
# from pseudo terminals at the weekend and on mondays.
#xsh;ttyp*;root;!WdMo0000-2400
#
# End of example file.
#
*;*;adminutil;!Th1400-1500
```

```
gaetan@C419-31:~/Téléchargements$ ssh adminutil@192.168.11.42 -p 2222
adminutil@192.168.11.42's password:
Connection closed by 192.168.11.42 port 2222
gaetan@C419-31:~/Téléchargements$
```



```
GNU nano 7.2 /etc/security/time.conf
# by the applying process.
#
#
# Here is a simple example: running blank on tty* (any
# the users 'you' and 'me' are denied service all of th
#
#blank;tty* & !ttyp*;you|me;!A10000-2400
#
# Another silly example, user 'root' is denied xsh acce
# from pseudo terminals at the weekend and on mondays.
#xsh;ttyp*;root;!WdMo0000-2400
#
# End of example file.
#
*;*;adminutil;A10800-1700

```

 Aide	 Écrire	 Chercher	 Couper	 ^T
 Quitter	 Lire fich.	 Remplacer	 ^U Coller	 ^J

## 4. Partie 3 : OpenVPN et Fail2ban Manque de temps, Absence de yassir de 4h justifié :

- Mise en place de l'authentification PAM pour OpenVPN
- Configuration de Fail2ban pour OpenVPN (création de filtres, prisons et notifications par mail)

Voici les logs pour prouver que notre openvpn fonctionne et fournie une adresse IP :

```
2024-12-12T14:05:52+01:00 OpenVPN-Serv openvpn[1748]: 192.168.14.39:62678 [SIO] Peer Connection Initiated with [AF_INET]192.168.14.39:62678
2024-12-12T14:05:52+01:00 OpenVPN-Serv openvpn[1748]: 192.168.14.39:62678 [SIO] Peer Connection Initiated with [AF_INET]192.168.14.39:62678
2024-12-12T14:05:52+01:00 OpenVPN-Serv openvpn[1748]: SIO/192.168.14.39:62678 MULTI_sva: pool returned IPv4=10.8.0.2, IPv6=(Not enabled)
2024-12-12T14:05:52+01:00 OpenVPN-Serv openvpn[1748]: SIO/192.168.14.39:62678 MULTI_sva: pool returned IPv4=10.8.0.2, IPv6=(Not enabled)
2024-12-12T14:05:52+01:00 OpenVPN-Serv openvpn[1748]: SIO/192.168.14.39:62678 MULTI: Learn: 10.8.0.2 -> SIO/192.168.14.39:62678
2024-12-12T14:05:52+01:00 OpenVPN-Serv openvpn[1748]: SIO/192.168.14.39:62678 MULTI: Learn: 10.8.0.2 -> SIO/192.168.14.39:62678
2024-12-12T14:05:52+01:00 OpenVPN-Serv openvpn[1748]: SIO/192.168.14.39:62678 MULTI: primary virtual IP for SIO/192.168.14.39:62678: 10.8.0.2
2024-12-12T14:05:52+01:00 OpenVPN-Serv openvpn[1748]: SIO/192.168.14.39:62678 MULTI: primary virtual IP for SIO/192.168.14.39:62678: 10.8.0.2
2024-12-12T14:05:52+01:00 OpenVPN-Serv openvpn[1748]: SIO/192.168.14.39:62678 SENT CONTROL [SIO]: 'PUSH_REPLY,block-ipv6,ifconfig-ipv6 10.8.0.2/24
fddd:1194:1194::1,redirect-gateway def1 ipv6 bypass-dhcp,dhcp-option DNS 192.168.12.1,block-outside-dns,route-gateway 10.8.0.1,topology subnet,ping 10,pin
g-restart 120,ifconfig 10.8.0.2 255.255.255.0,peer-id 0,cipher AES-256-GCM,protocol-flags cc-exit tls-ekm dyn-tls-crypt,tun-mtu 1500' (status=1)
2024-12-12T14:05:52+01:00 OpenVPN-Serv openvpn[1748]: SIO/192.168.14.39:62678 SENT CONTROL [SIO]: 'PUSH_REPLY,block-ipv6,ifconfig-ipv6 10.8.0.2/24
fddd:1194:1194::1,redirect-gateway def1 ipv6 bypass-dhcp,dhcp-option DNS 192.168.12.1,block-outside-dns,route-gateway 10.8.0.1,topology subnet,ping 10,pin
g-restart 120,ifconfig 10.8.0.2 255.255.255.0,peer-id 0,cipher AES-256-GCM,protocol-flags cc-exit tls-ekm dyn-tls-crypt,tun-mtu 1500' (status=1)
2024-12-12T14:05:53+01:00 OpenVPN-Serv openvpn[1748]: SIO/192.168.14.39:62678 Data Channel: cipher 'AES-256-GCM', peer-id: 0
2024-12-12T14:05:53+01:00 OpenVPN-Serv openvpn[1748]: SIO/192.168.14.39:62678 Timers: ping 10, ping-restart 240
2024-12-12T14:05:53+01:00 OpenVPN-Serv openvpn[1748]: SIO/192.168.14.39:62678 Timers: ping 10, ping-restart 240
2024-12-12T14:05:53+01:00 OpenVPN-Serv openvpn[1748]: SIO/192.168.14.39:62678 Protocol options: explicit-exit-notify 1, protocol-flags cc-exit tls-ekm dyn-tls-c
rypt
2024-12-12T14:05:53+01:00 OpenVPN-Serv openvpn[1748]: SIO/192.168.14.39:62678 Protocol options: explicit-exit-notify 1, protocol-flags cc-exit tls-ekm dyn-tls-c
rypt
```

## **5. Partie 4 : UFW - Configuration du pare-feu**

- Configuration des règles de pare-feu pour le serveur OpenVPN et le serveur de mail

UFW (Uncomplicated Firewall) est un outil simple pour gérer les règles du pare-feu sur Linux, basé sur iptables. Il est conçu pour rendre la configuration des pare-feu plus accessible, avec une interface intuitive en ligne de commande.

Fonctions principales :

Activer/désactiver le pare-feu :

`sudo ufw enable` pour l'activer.

`sudo ufw disable` pour le désactiver.

Autoriser ou bloquer des connexions :

Exemple : `sudo ufw allow 22` autorise le SSH.

Exemple : `sudo ufw deny 80` bloque le HTTP.

Lister les règles actives :

`sudo ufw status` affiche les règles en cours.

Gestion avancée :

Spécifier une IP source : `sudo ufw allow from 192.168.1.X`.

Définir une plage de ports : `sudo ufw allow 1000:2000/tcp`.

UFW est idéal pour configurer rapidement des pare-feu sans complexité inutile.

Ici nous allons accepter la connection depuis le server mail via un ssh et notre machine cliente openvpn :

```
root@OpenVPN-Serv:~# ufw allow from 192.168.14.39 to any port 1194 proto udp
root@OpenVPN-Serv:~# ufw allow from 192.168.12.4 to any port 2222 proto tcp
sio@OpenVPN-Serv:~$ exit
déconnexion
Connection to 192.168.11.42 closed.
gaetan@C419-31:~$ ssh sio@192.168.11.42 -p 2222
```

```
adminvpn@OpenVPN-Serv: ~ x sio@OpenVPN-Serv: ~
root@OpenVPN-Serv:~# ufw status numbered
Status: active

    To Action From
    --
[ 1] 2222/tcp ALLOW IN 192.168.12.4
[ 2] 1194/udp ALLOW IN 192.168.14.39
root@OpenVPN-Serv:~#
```

Voici un test, j'ai pu me connecter en ssh sur mon serveur mail jusqu'à mon serveur openvpn :

```

sio@C419-32:~$ ssh sio@192.168.12.4
sio@192.168.12.4's password:
Linux servermail 6.1.0-25-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.106-3 (2024-08-26) 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: Thu Dec 12 11:30:24 2024 from 192.168.12.250
sio@servermail:~$ ssh sio@192.168.11.42
C
sio@servermail:~$ ssh sio@192.168.11.42 -p 2222
The authenticity of host '[192.168.11.42]:2222 ([192.168.11.42]:2222)' can't be established.
ED25519 key fingerprint is SHA256:PpuM17hi1M6thT218VvcSwRGqf8v3JzLOjcJSEfL+XI.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[192.168.11.42]:2222' (ED25519) to the list of known hosts.
sio@192.168.11.42's password:
Linux OpenVPN-Serv 6.1.0-28-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.119-1 (2024-11-22) 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: Thu Dec 12 16:24:30 2024 from 192.168.11.251
sio@OpenVPN-Serv:~$ exit
Déconnexion
Connection to 192.168.11.42 closed.
sio@servermail:~$ ufw
bash: ufw : commande introuvable
sio@servermail:~$ 

```

Nous avons également ajouté notre adresse IP de notre poste physique afin de laisser une connection ssh pour qu'elle ne sois pas refuser :

```
sio@OpenVPN-Serv:~$ su -
Mot de passe :
root@OpenVPN-Serv:~# ufw status
Status: active

To Action From
--
2222/tcp ALLOW 192.168.12.4
1194/udp ALLOW 192.168.14.39
2222/tcp ALLOW 192.168.11.251

root@OpenVPN-Serv:~#
```

```
2: eno1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether f8:b1:56:bd:4f:47 brd ff:ff:ff:ff:ff:ff
    altname enp0s25
    inet 172.17.219.32/16 brd 172.17.255.255 scope global eno1
        valid_lft forever preferred_lft forever
    inet6 fe80::fab1:56ff:febd:4f47/64 scope link
        valid_lft forever preferred_lft forever
3: vlan430@eno1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default qlen 1000
    link/ether f8:b1:56:bd:4f:47 brd ff:ff:ff:ff:ff:ff
    inet 192.168.13.251/24 brd 192.168.13.255 scope global vlan430
        valid_lft forever preferred_lft forever
    inet6 fe80::fab1:56ff:febd:4f47/64 scope link
        valid_lft forever preferred_lft forever
4: vlan431@eno1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default qlen 1000
    link/ether f8:b1:56:bd:4f:47 brd ff:ff:ff:ff:ff:ff
    inet 192.168.11.251/24 brd 192.168.11.255 scope global vlan431
        valid_lft forever preferred_lft forever
    inet6 fe80::fab1:56ff:febd:4f47/64 scope link
        valid_lft forever preferred_lft forever
5: vlan434@eno1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default qlen 1000
    link/ether f8:b1:56:bd:4f:47 brd ff:ff:ff:ff:ff:ff
    inet 192.168.14.251/24 brd 192.168.14.255 scope global vlan434
        valid_lft forever preferred_lft forever
    inet6 fe80::fab1:56ff:febd:4f47/64 scope link
        valid_lft forever preferred_lft forever
6: vlan432@eno1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default qlen 1000
    link/ether f8:b1:56:bd:4f:47 brd ff:ff:ff:ff:ff:ff
    inet 192.168.12.251/24 brd 192.168.12.255 scope global vlan432
        valid_lft forever preferred_lft forever
    inet6 fe80::fab1:56ff:febd:4f47/64 scope link
        valid_lft forever preferred_lft forever
```

```
sio@C419-32:~$ ssh sio@192.168.11.42 -p 2222
sio@192.168.11.42's password:
Linux OpenVPN-Serv 6.1.0-28-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.119-1 (2024-11-22) 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: Thu Dec 12 16:39:41 2024 from 192.168.12.4
sio@OpenVPN-Serv:~$
```



- Configuration du pare-feu sur le routeur

Voici la configuration de UFW sur le routeur, les ip autorisées à accéder au protocole SSH ou DNS des serveur de leurs réseaux :

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

To Action From
--
22/tcp ALLOW IN 192.168.13.0/24
22/tcp ALLOW IN 192.168.11.0/24
22/tcp ALLOW IN 192.168.12.0/24
53/tcp ALLOW IN 192.168.13.0/24
53/tcp ALLOW IN 192.168.12.0/24
53/tcp ALLOW IN 192.168.11.0/24

root@routeur:~#
```

Démonstration de tentative de connexion en ssh au routeur sur une vm client sur le vlan invité donc pas accès au routeur :



```

sio@debianclt: ~
valid_lft forever preferred_lft forever
inet6 ::1/128 scope host noprefixroute
valid_lft forever preferred_lft forever
2: ens18: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP g
up default qlen 1000
link/ether bc:24:11:01:e6:05 brd ff:ff:ff:ff:ff:ff
altname enp0s18
inet 192.168.14.34/24 brd 192.168.14.255 scope global noprefixroute ens18
valid_lft forever preferred_lft forever
inet6 fe80::4ba4:f541:70c7:d96c/64 scope link noprefixroute
valid_lft forever preferred_lft forever
sio@debianclt:~$ ssh sio@192.168.14.254
^C
sio@debianclt:~$ ssh sio@192.168.14.254 -p 2222
^C
sio@debianclt:~$ ssh sio@192.168.11.254 -p 2222
^C
sio@debianclt:~$ ssh sio@192.168.11.254
^C
sio@debianclt:~$ ssh sio@192.168.11.36
^C
sio@debianclt:~$ ssh sio@192.168.11.36 -p 2222
^C

```

```

root@srv-nagios:/usr/local/nagios/etc/servers# ssh sio21@192.168.13.254
The authenticity of host '192.168.13.254 (192.168.13.254)' can't be established.
ED25519 key fingerprint is SHA256:f4gwC0mtqg0ytAs+7f2CDdzCYWnuJuTKcEiFUtQmv9I.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.13.254' (ED25519) to the list of known hosts.
sio21@192.168.13.254's password:
Linux routeur 5.10.0-32-amd64 #1 SMP Debian 5.10.223-1 (2024-08-10) 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.
You have new mail.
Last login: Fri Dec 13 16:27:01 2024 from 192.168.11.251
sio21@routeur:~$ 

```