BTS SIO · OPTION SISR · SESSION 2026
**BAGARRY Matthias**

# DOSSIER TECHNIQUE

## Mise en œuvre, sécurisation et exploitation d'un relais SMTP Postfix

## 0 CONTEXTE ET OBJECTIFS

Ce projet a été réalisé dans le cadre d'une demande formulée par mon tuteur lors de mon stage au Louvre. L'objectif n'était pas une mise en production réelle, mais la construction d'un environnement de laboratoire personnel me permettant de monter en compétences sur trois volets fondamentaux de l'administration système Linux.

▸ OBJECTIFS PÉDAGOGIQUES

Acquérir la maîtrise de la virtualisation sous VirtualBox (création de VM, allocation de ressources, configuration réseau), maîtriser le processus d'installation d'une distribution Linux avec un partitionnement LVM professionnel, et déployer un service sous Postfix en appliquant les bonnes pratiques de sécurité attendues dans un contexte professionnel.

Le serveur déployé joue le rôle de Smart Host (relais SMTP) : il centralise les envois de mails émis par des équipements internes (serveurs applicatifs, imprimantes réseau, scripts de supervision) et applique des politiques de sécurité avant de transmettre les flux vers l'extérieur.

▸ POURQUOI UN RELAIS SMTP

Dans une infrastructure d'entreprise, les équipements émetteurs de mails (imprimantes, sondes Zabbix, scripts Cron) n'ont pas vocation à parler directement à des serveurs mails publics. Un relais centralise ces flux, applique un chiffrement TLS, filtre les mails sortants (vérification des virus, du spam) et garantit la traçabilité des envois via des logs uniques.

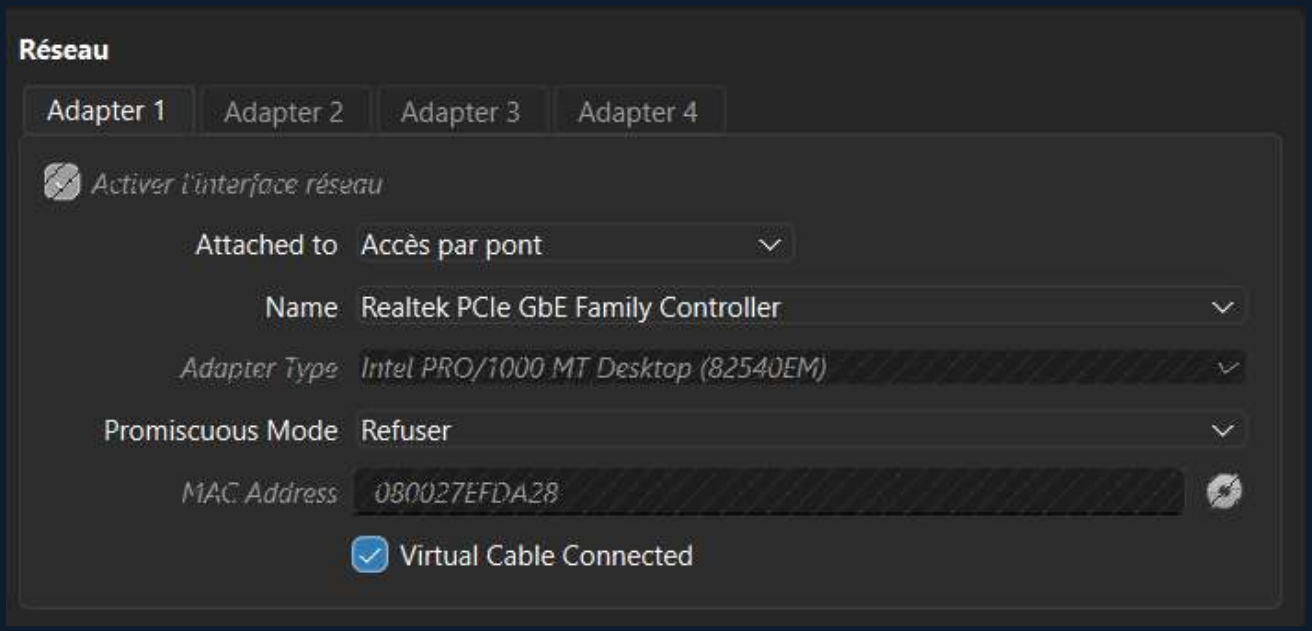
# 1 ANALYSE ET ARCHITECTURE

## 1.1 Environnement VirtualBox

| Ressource | Valeur allouée |
|---|---|
| Processeurs | 2 vCPUs |
| Mémoire Vive | 4 Go RAM |
| Disque Dur | 40 Go (Partitionnement LVM) |
| Carte Réseau | Accès par pont — interface enp0s3 |

▸ POURQUOI L'ACCÈS PAR PONT

Le mode « pont » place la VM directement sur le réseau physique de l'hôte, avec sa propre adresse IP attribuée par le routeur. C'est indispensable pour un relais SMTP : il doit être joignable par les autres machines du réseau et émettre des mails avec une IP identifiable. Les modes « NAT » ou « réseau interne » isoleraient la VM et empêcheraient la communication inter-machines.




# 2 INFRASTRUCTURE SYSTÈME (LVM)

Le choix de LVM permet d'isoler les partitions critiques et de redimensionner les volumes logiques à chaud, sans réorganisation physique du disque.

▸ PRINCIPE DE LVM

LVM ajoute une couche logique entre les disques physiques (PV) et les points de montage. Les disques sont regroupés dans un Volume Group (VG) qui peut être découpé en Logical Volumes (LV) de tailles ajustables. Avantage majeur : étendre un volume à chaud avec lvextend + resize2fs, sans démontage ni redémarrage.

## 2.1 Initialisation et création des volumes

Selon les choix d'installation, Il est possible de configurer le LVM manuellement.

```
# Initialisation du stockage physique
pvcreate /dev/sda
vgcreate vg0 /dev/sda
# Création des volumes logiques (LV)
lvcreate -L 10G -n syst-root    vg0    # Racine /
lvcreate -L 5G  -n syst-home    vg0    # /home
lvcreate -L 10G -n syst-var     vg0    # /var
lvcreate -L 10G -n syst-var_log vg0    # /var/log
lvcreate -L 2G  -n swap         vg0    # Swap
# Afficher le détail actuel
lvs
```

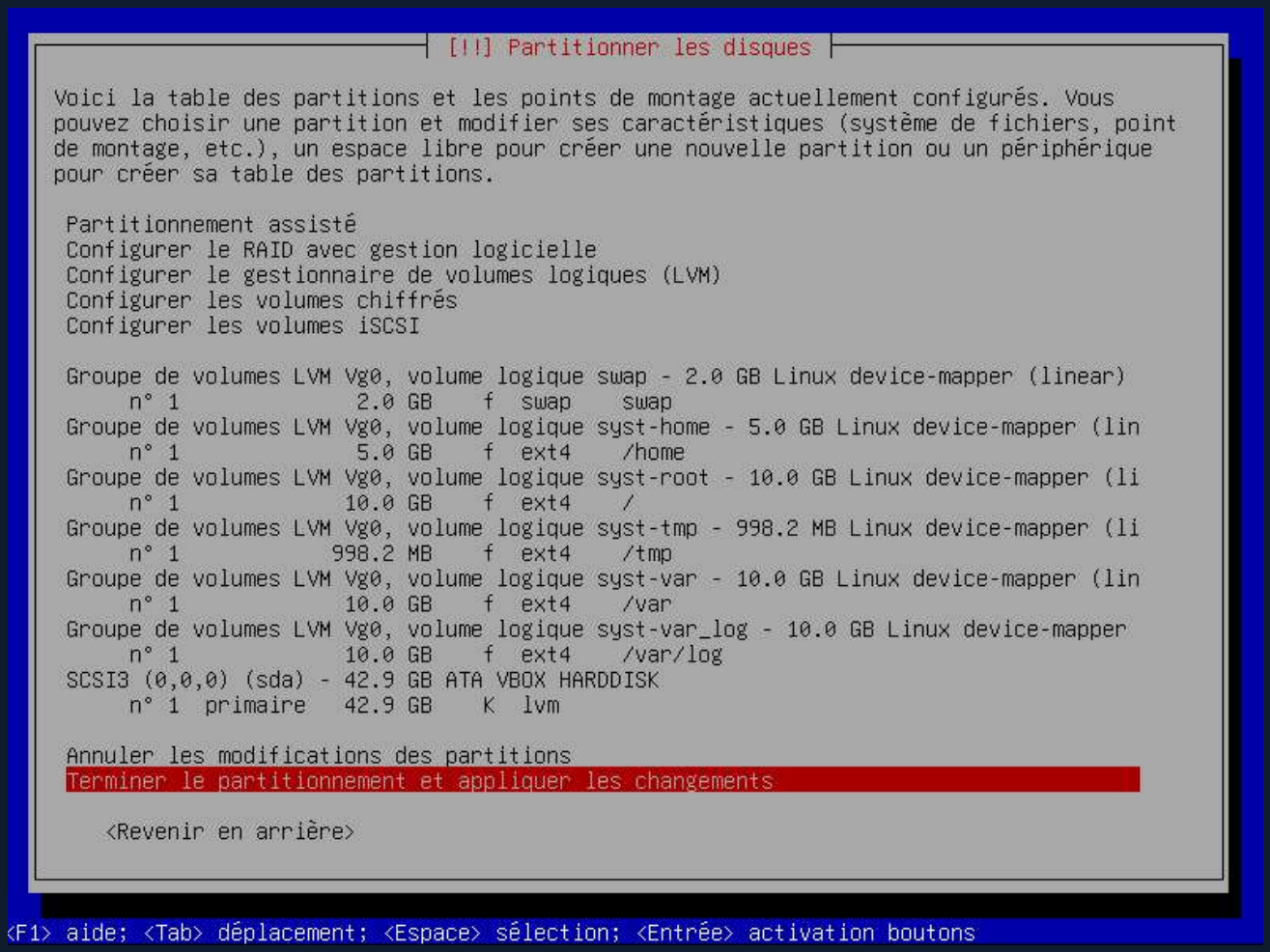
Mais pour ce dossier technique, le LVM a été directement paramétré durant l'installation de Debian.

## 2.2 Justification du dimensionnement

| Volume | Taille | Justification |
|---|---|---|
| syst-root | 10 Go | Système Debian minimal + binaires installés, marge confortable |
| syst-home | 5 Go | Peu d'utilisateurs, pas de données personnelles volumineuses |
| syst-var | 10 Go | Caches APT, paquets, base données Postfix (/var/spool/postfix) |
| syst-var_log | 10 Go | Logs mail volumineux en cas de pic de trafic ou d'attaque |
| swap | 2 Go | Débordement mémoire, suffisant pour 4 Go RAM |

▸ POURQUOI ISOLER /VAR/LOG

L'isolation de /var/log dans un volume logique dédié protège le système contre le déni de service (DoS) par saturation d'espace disque. Si le flux de mails explose ou si un attaquant génère volontairement des milliers de connexions pour remplir les logs, la saturation reste confinée à ce volume et n'affecte ni la racine, ni /var, ni le système. Le serveur continue de fonctionner.




*Partionnement du disque primaire en volume logique (LVM)*

# 3 CONFIGURATION ET SÉCURISATION

## 3.1 Installation des outils de base

```
apt-get update && apt-get full-upgrade -y
apt-get install wget curl net-tools vim-tiny sudo htop \
    openssh-server ufw telnet bsd-mailx -y
```

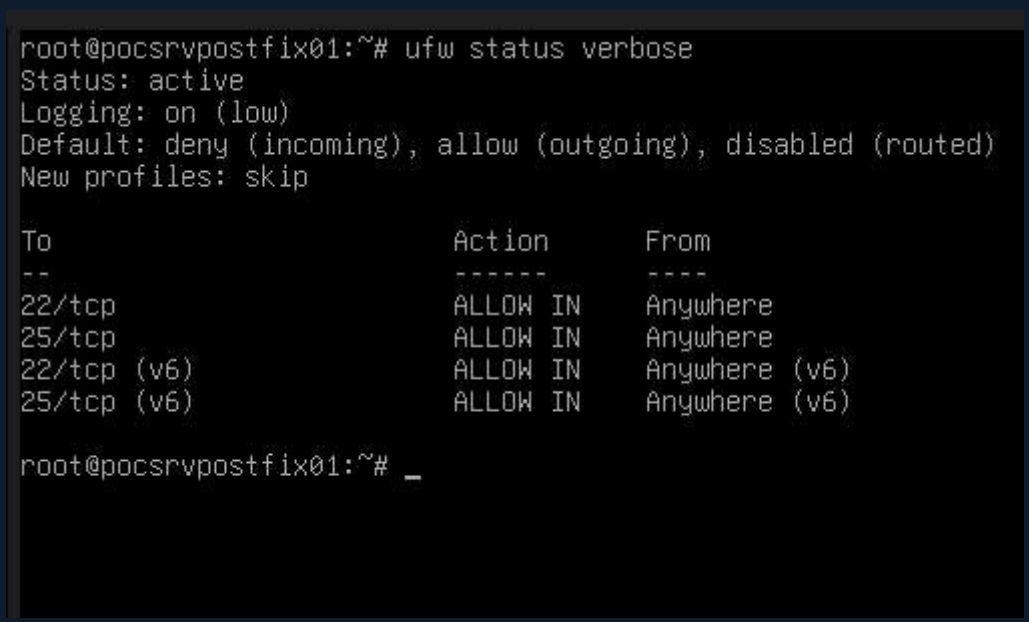
## 3.2 Durcissement (Hardening) SSH et pare-feu

Restriction de l'accès SSH et activation du pare-feu applicatif.

```
# Désactivation du login Root (force l'usage de sudo)
sed -i 's/^#PermitRootLogin.*/PermitRootLogin no/' /etc/ssh/sshd_config
systemctl restart ssh
# Configuration UFW (stratégie Default Deny)
ufw default deny incoming
ufw allow 22/tcp   # Administration (SSH)
ufw allow 25/tcp   # SMTP
ufw enable
```

▸ PRINCIPE DE DÉFENSE EN PROFONDEUR

Trois mesures complémentaires sont appliquées. (1) Désactivation du login SSH root : élimine la moitié des attaques par force brute, root étant la première cible. (2) UFW en default deny : tout ce qui n'est pas explicitement autorisé est refusé. (3) Sudo obligatoire : toute élévation de privilège laisse une trace nominative dans /var/log/auth.log, ce qui assure la traçabilité des actions administratives.




*Status du firewall avec les ports ouverts 22 et 25.*

# 4 DÉPLOIEMENT DU SERVICE POSTFIX

L'installation est réalisée via le gestionnaire de paquets de Debian. Lors de la configuration assistée, le mode « Site Internet » est sélectionné.

```
apt-get install postfix -y
```

▸ ARCHITECTURE INTERNE DE POSTFIX

Postfix n'est pas un programme unique mais un groupe de processus isolés, chacun avec son rôle : master (orchestrateur), smtpd (daemon de réception des connexions entrantes sur le port 25), smtp (protocole d'émission vers d'autres serveurs), qmgr (queue manager), cleanup (nettoyage des en-têtes), pickup (récupération des mails locaux). Cette modularité applique le principe du moindre privilège : chaque processus tourne avec des droits minimaux.

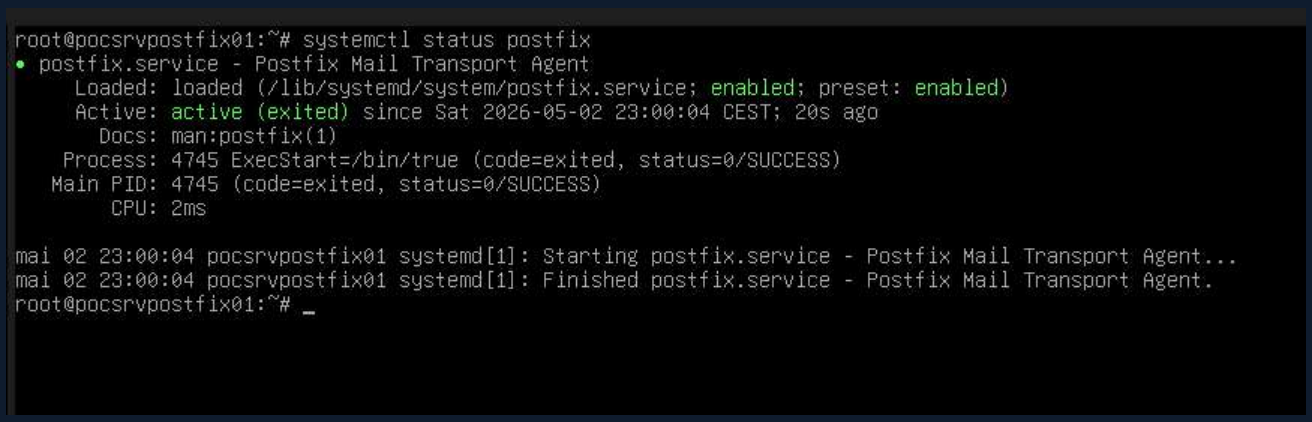
## 4.1 Configuration de base via postconf

L'outil postconf modifie le fichier main.cf en préservant son intégrité (validation de syntaxe, gestion des accolades). Les trois paramètres critiques définis ici sont : identité du serveur (myhostname) pour l'identification SMTP, contrôle d'accès (mynetworks) pour restreindre le relais aux réseaux internes, et anonymisation (smtpd_banner) pour masquer la version précise du service.

```
# Configuration de l'identité
postconf -e 'myhostname = relay-smtp01.domaine.lan'
# Limitation du relais aux réseaux autorisés (anti-relais ouvert)
postconf -e 'mynetworks = 127.0.0.0/8, 192.168.1.0/24'
# Banner SMTP anonymisée
postconf -e 'smtpd_banner = $myhostname ESMTP (Postfix Secure Relay)'
systemctl restart postfix
```

▸ OPEN RELAY : ENJEU CRITIQUE

Un serveur SMTP sans restriction est un « open relay » : il accepte de relayer les mails de n'importe qui vers n'importe où. Les spammeurs scannent Internet à la recherche de ces serveurs. Conséquence : blacklistage sur Spamhaus, SpamCop, Barracuda, et plus aucun serveur légitime n'accepte les mails. Le paramètre mynetworks limite le relais aux réseaux 127.0.0.0/8 (loopback) et 192.168.1.0/24 (LAN) uniquement. Toute autre source est refusée.




*Status Postfix en fonctionnement.*

## 4.2 Sécurisation des flux (TLS)

Pour garantir la confidentialité des échanges entre les clients et le relais, le chiffrement TLS est implémenté. Sans TLS, le SMTP circule en clair : mots de passe SASL, contenu des mails et identifiants sont lisibles par quiconque écoute le trafic réseau.

> ▸ **POURQUOI UN CERTIFICAT AUTO-SIGNÉ**
>
> Dans le cadre de ce lab personnel, un certificat auto-signé suffit pour valider techniquement la mise en place du TLS. En production, un certificat délivré par une autorité reconnue (Let's Encrypt gratuit, ou PKI interne d'entreprise) serait nécessaire pour que les clients externes acceptent la connexion sans avertissement de sécurité.

**Étape 1 — Génération du certificat auto-signé (validité 365 jours, clé RSA 2048 bits) :**

```
openssl req -new -x509 -nodes -days 365 -newkey rsa:2048 \
    -keyout /etc/ssl/private/postfix.key \
    -out    /etc/ssl/certs/postfix.crt
```

**Étape 2 — Activation du TLS dans Postfix :**

```
postconf -e 'smtpd_tls_cert_file = /etc/ssl/certs/postfix.crt'
postconf -e 'smtpd_tls_key_file = /etc/ssl/private/postfix.key'
postconf -e 'smtpd_use_tls = yes'
systemctl restart postfix
```

**Étape 3 — Ouverture du port sécurisé (Submission) dans UFW :**

```
ufw allow 587/tcp   # Port Submission (client → serveur)
```

⚠ Par défaut sur Debian, le service `submission` est commenté dans `/etc/postfix/master.cf` : Postfix n'écoute pas sur le port 587 même après l'ouverture UFW. Il faut décommenter la ligne correspondante pour que le port soit réellement actif :

```
# Décommenter dans /etc/postfix/master.cf :
submission inet n       -       y       -       -       smtpd
  systemctl restart postfix
# Vérifier que Postfix écoute bien sur 587 :
ss -tlnp | grep 587
```

▸ **LES TROIS PORTS SMTP**

Port 25 : communication serveur-serveur, historiquement en clair, reste ouvert pour la réception des mails externes. Port 587 (Submission) : clients authentifiés avec STARTTLS, recommandé pour les applications émettrices. Port 465 (SMTPS) : TLS implicite dès l'ouverture, plus ancien. Dans notre configuration, 25 reste ouvert pour les flux serveur, 587 est privilégié pour les clients internes.

### 4.3 Gestion des alias système

Pour assurer le suivi d'exploitation, les alertes destinées à l'administrateur root sont redirigées vers une boîte mail de gestion. Sans cette redirection, les notifications système (logs rotate, alertes cron, erreurs Postfix) restent dans la boîte locale root et ne sont jamais lues.

```
echo "root: admin@relais-smtp01.domaine.lan" >> /etc/aliases
newaliases   # Compile la base de données des alias
```

## 5 VALIDATION TECHNIQUE (RECETTE)

La phase de recette valide le bon fonctionnement du routage, la présence de la couche de sécurité et la résistance aux usages abusifs.

## 5.1 Test de connectivité simple (Telnet)

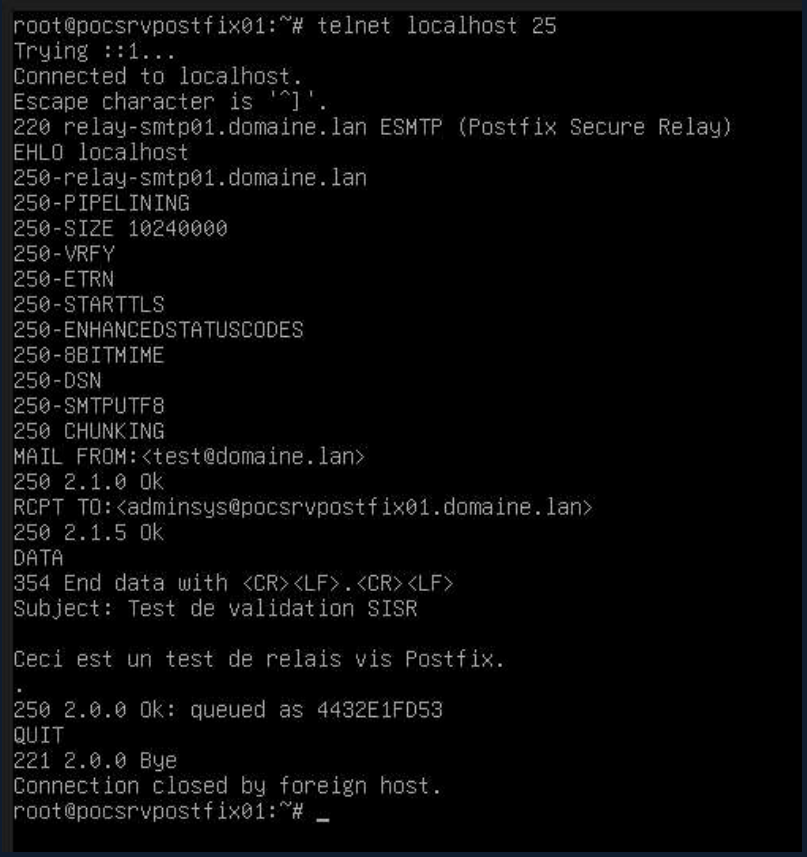
Vérification de la réponse du service sur le port 25 et de la bannière anonymisée.

```
telnet localhost 25
EHLO localhost
MAIL FROM:<test@domaine.lan>
RCPT TO:<admin@relais-smtp01.domaine.lan>
DATA
Subject: Test de validation SISR

Ceci est un test de relais via Postfix.
.
QUIT
```

▸ CRITÈRE DE SUCCÈS

Réception du code 220 relay-smtp01.domaine.lan ESMTP (Postfix Secure Relay) à la connexion, puis 250 OK après chaque commande valide. Le code 221 clôt la session sur QUIT.



## 5.2 Test du chiffrement TLS (OpenSSL)

Vérification que le serveur propose bien l'extension STARTTLS et accepte les connexions chiffrées.

```
openssl s_client -starttls smtp -connect localhost:587
```

▸ CRITÈRE DE SUCCÈS

Affichage de la chaîne BEGIN CERTIFICATE suivie du certificat auto-signé, puis établissement d'un cipher sécurisé (ex : ECDHE-RSA-AES256-GCM-SHA384). Une erreur de type « STARTTLS not supported » indiquerait un échec de configuration.

```
Server Temp Key: X25519, 253 bits
---
SSL handshake has read 1773 bytes and written 410 bytes
Verification error: self-signed certificate
---
New, TLSv1.3, Cipher is TLS_AES_256_GCM_SHA384
Server public key is 2048 bit
Secure Renegotiation IS NOT supported
Compression: NONE
Expansion: NONE
No ALPN negotiated
Early data was not sent
Verify return code: 18 (self-signed certificate)
---
250 CHUNKING
---
Post-Handshake New Session Ticket arrived:
SSL-Session:
    Protocol  : TLSv1.3
    Cipher    : TLS_AES_256_GCM_SHA384
    Session-ID: B6F0D310F5871C5B37E58CFB56CB9276CD8E71473F69B8E0904E6475E4A9CC40
    Session-ID-ctx:
    Resumption PSK: EF3AC5EA900A7505B0F8FAD8643AA5CE2FC2306FFCABBD8287EAFC229EF80C166974A6ED553AD8C70D6D81E84D70D4F9
    PSK identity: None
    PSK identity hint: None
    SRP username: None
    TLS session ticket lifetime hint: 7200 (seconds)
    TLS session ticket:
    0000 - ba 41 38 da 3c 31 6c e2-91 25 de fc db d0 4a e7   .A8.<1l..%....J.
    0010 - f6 8e 4a a0 ea 2d 31 1a-35 3e 9b ba 31 a1 f6 45   ..J..-1.5>..1..E
    0020 - 03 0c f8 fc b5 21 e9 19-83 f1 27 88 a1 bf 99 4d   .....!....'....M
    0030 - 55 bc dd dc 74 1a 07 6f-a8 8e 7d c5 cb 38 aa 58   U...t..o..}..8.X
    0040 - b8 27 6f 1c 7f c5 8a 70-e5 33 76 a8 25 10 32 d9   .'o....p.3v.%.2.
    0050 - 1e 88 14 97 95 48 59 63-27 06 d0 1f 81 44 ec 78   .....HYc'....D.x
    0060 - 8b 3b 0b 04 ae fe be 8b-53 8a fd f7 cd 55 53 db   .;......S....US.
    0070 - 87 66 9b 7e 41 cb 6c 80-05 ed a2 a4 76 e0 c9 f9   .f.~A.l.....v...
    0080 - cd eb b1 6b 09 c1 db 12-14 b3 b7 bd 6f 39 6b 09   ...k........o9k.
    0090 - 2c 2b e8 34 ae d1 9d d9-51 da 90 0a 10 dc da cb   ,+.4....Q.......
    00a0 - 07 8b 65 a3 cb 40 86 db-84 7b 86 54 2b b8 9f bb   ..e..@...{.T+...
    00b0 - 4f b7 2d 0f ba e5 67 7f-6f bb aa ac 4d d7 b4 27   O.-...g.o...M..'
    00c0 - dc 72 9e 4e ae 31 68 99-2b 32 44 c0 38 c9 09 3b   .r.N.1h.+2D.8..;

    Start Time: 1777758923
    Timeout   : 7200 (sec)
    Verify return code: 18 (self-signed certificate)
    Extended master secret: no
    Max Early Data: 0
---
read R BLOCK
```

## 5.3 Test anti-relais ouvert (sécurité)

Vérification que le serveur refuse bien de relayer un mail dont la source et la destination sont toutes deux externes aux réseaux de confiance.

```
# Depuis une machine hors du réseau 192.168.1.0/24
telnet relay-smtp01.domaine.lan 25
EHLO attaquant.externe.com
MAIL FROM:<spammer@externe.com>
RCPT TO:<victime@autre-domaine.com>
```

▸ CRITÈRE DE SUCCÈS

Le serveur doit répondre par un code 554 Relay access denied. Si la réponse est 250 OK, la configuration est vulnérable et doit être corrigée immédiatement (vérifier le paramètre mynetworks).

```
root@pocsrvpostfix01:~# telnet pocsrvpostfix01.domaine.lan 25
Trying 127.0.0.1...
Connected to pocsrvpostfix01.domaine.lan.
Escape character is '^]'.
220 relay-smtp01.domaine.lan ESMTP (Postfix Secure Relay)
EHLO attaquant.externe.com
250-relay-smtp01.domaine.lan
250-PIPELINING
250-SIZE 10240000
250-VRFY
250-ETRN
250-STARTTLS
250-ENHANCEDSTATUSCODES
250-8BITMIME
250-DSN
250-SMTPUTF8
250 CHUNKING
MAIL FROM:<spammer@externe.com>
250 2.1.0 Ok
RCPT TO:<victime@autre-domaine.com>
554 5.7.1 <victime@autre-domaine.com>: Relay access denied
```

## 5.4 Commandes de diagnostic et exploitation

| Commande | Usage |
|---|---|
| tail -f /var/log/mail.log | Suivi en temps réel des transactions et erreurs |
| mailq | Vérification de la file d'attente (mails en deferred) |
| postconf -n | Vérification des paramètres actifs (non-défaut) |
| postfix check | Validation de la syntaxe de la configuration |
| systemctl status postfix | État du service et sous-processus |

> ▸ **INDICATEUR DE SUCCÈS D'ENVOI**
>
> Dans /var/log/mail.log, la mention status=sent (delivered to maildir) confirme que le mail a été envoyé. La mention status=deferred indique un échec temporaire avec une nouvelle tentative d'envoi automatique. Un status=bounced signale un échec définitif après cinq jours (configuration postfix par défaut)

```
root@pocsrvpostfix01:~# tail /var/log/mail.log
2026-05-03T00:26:41.736037+02:00 pocsrvpostfix01 postfix/master[7093]: terminating on signal 15
2026-05-03T00:26:42.840722+02:00 pocsrvpostfix01 postfix/postfix-script[7527]: starting the Postfix mail system
2026-05-03T00:26:42.851150+02:00 pocsrvpostfix01 postfix/master[7529]: daemon started -- version 3.7.11, configuration /etc/postfix
2026-05-03T00:32:36.074414+02:00 pocsrvpostfix01 postfix/smtpd[7634]: connect from localhost[::1]
2026-05-03T00:33:52.033378+02:00 pocsrvpostfix01 postfix/smtpd[7634]: 07C601FE7F: client=localhost[::1]
2026-05-03T00:34:31.832886+02:00 pocsrvpostfix01 postfix/cleanup[7640]: 07C601FE7F: message-id=<20260502223352.07C601FE7F@relay-smtp01.domaine.lan>
2026-05-03T00:34:31.848720+02:00 pocsrvpostfix01 postfix/qmgr[7531]: 07C601FE7F: from=<test@domaine.lan>, size=387, nrcpt=1 (queue active)
2026-05-03T00:34:31.866230+02:00 pocsrvpostfix01 postfix/local[7642]: 07C601FE7F: to=<adminsys@pocsrvpostfix01.domaine.lan>, relay=local, delay=77, delays=77/0.01/0/0.01, dsn=2.0.0, status=sent (delivered to mailbox)
2026-05-03T00:34:31.867015+02:00 pocsrvpostfix01 postfix/qmgr[7531]: 07C601FE7F: removed
2026-05-03T00:34:36.015004+02:00 pocsrvpostfix01 postfix/smtpd[7634]: disconnect from localhost[::1] ehlo=1 mail=1 rcpt=1 data=1 quit=1 commands=5
root@pocsrvpostfix01:~#
```

```
root@pocsrvpostfix01:~# telnet localhost 25
Trying ::1...
Connected to localhost.
Escape character is '^]'.
220 relay-smtp01.domaine.lan ESMTP (Postfix Secure Relay)
EHLO localhost
250-relay-smtp01.domaine.lan
250-PIPELINING
250-SIZE 10240000
250-VRFY
250-ETRN
250-STARTTLS
250-ENHANCEDSTATUSCODES
250-8BITMIME
250-DSN
250-SMTPUTF8
250 CHUNKING
MAIL FROM:<test@domaine.lan>
250 2.1.0 Ok
RCPT TO:<adminsys@pocsrvpostfix01.domaine.lan>
250 2.1.5 Ok
DATA
354 End data with <CR><LF>.<CR><LF>
Subject : Test log Postfix

Corps du mail.Test.

.
250 2.0.0 Ok: queued as 07C601FE7F
QUIT
221 2.0.0 Bye
Connection closed by foreign host.
root@pocsrvpostfix01:~#
```