apt update
apt upgrade

apt install clamav (Antivirus)
apt install clamav-daemon (un connecteur vers clamav)

Pour mettre à jour le fichier de signature de clamav

root@tech-Msg:/home/tech# freshclam
Mon Jun 19 12:56:13 2023 -> ClamAV update process started at Mon Jun 19 12:56:13 2023
Mon Jun 19 12:56:13 2023 -> daily.cvd database is up-to-date (version: 26944, sigs: 2037362, f-level: 90, builder: raynman)
Mon Jun 19 12:56:13 2023 -> main.cvd database is up-to-date (version: 62, sigs: 6647427, f-level: 90, builder: sigmgr)
Mon Jun 19 12:56:13 2023 -> bytecode.cvd database is up-to-date (version: 334, sigs: 91, f-level: 90, builder: anvilleg)

Tester clamav en ligne de commande:

root@tech-Msg:/home/tech# clamscan /home/tech
/home/tech/.bashrc: OK
/home/tech/.profile: OK
/home/tech/.sudo_as_admin_successful: Empty file
/home/tech/.Xauthority: OK
/home/tech/.bash_logout: OK

----------- SCAN SUMMARY -----------
Known viruses: 8669227
Engine version: 0.103.8
Scanned directories: 1
Scanned files: 4
Infected files: 0
Data scanned: 0.00 MB
Data read: 0.00 MB (ratio 0.00:1)
Time: 43.750 sec (0 m 43 s)
Start Date: 2023:06:19 12:57:31
End Date: 2023:06:19 12:58:15

Utiliser clamd sur TCP/IP 3310 sur 127.0.0.1

Ajouter les 2 lignes au fichier de conf :

TCPSocket 3310
TCPAddr 127.0.0.1
Relancer le daemon :

● clamav-daemon.service - Clam AntiVirus userspace daemon
     Loaded: loaded (/lib/systemd/system/clamav-daemon.service; enabled; vendor preset: enabled)
    Drop-In: /etc/systemd/system/clamav-daemon.service.d
             └─extend.conf
     Active: active (running) since Mon 2023-06-19 11:36:32 CEST; 1h 24min ago

Vérifier l’écoute sur le réseau :

```
netstat -lntp
tcp        0      0 127.0.0.1:3310          0.0.0.0:*               LISTEN      33765/clamd
```

Tester le daemon via le jeu de commandes (man):

```
root@tech-Msg:/home/tech# telnet 127.0.0.1 3310
Trying 127.0.0.1...
Connected to 127.0.0.1.
Escape character is '^]'.
PING
PONG
Connection closed by foreign host.
```

```
root@tech-Msg:/home/tech# telnet 127.0.0.1 3310
Trying 127.0.0.1...
Connected to 127.0.0.1.
Escape character is '^]'.
SCAN /home/tech
/home/tech: File path check failure: Permission denied. ERROR
/home/tech: OK
Connection closed by foreign host.
```

Normal pour les droits (File path check failure) car clamd tourne avec user clamav…

Avec un fichier appartenant à clamav :

```
tech@tech-Msg:~$ telnet 127.0.0.1 3310
Trying 127.0.0.1...
Connected to 127.0.0.1.
Escape character is '^]'.
SCAN /tmp/test
/tmp/test: OK
Connection closed by foreign host.
```

Avec le test « virus » eicar :
dans /tmp
wget https://secure.eicar.org/eicar.com
sudo chown clamav eicar.com

```
tech@tech-Msg:~$ telnet 127.0.0.1 3310
Trying 127.0.0.1...
Connected to 127.0.0.1.
Escape character is '^]'.
SCAN /tmp/eicar.com
/tmp/eicar.com: Win.Test.EICAR_HDB-1 FOUND
Connection closed by foreign host.
```

Nous allons maintenant utiliser un MTA spécialement créer pour dialoguer avec Clamd plutôt que d'utiliser une config particulièrement plus difficile à mettre en œuvre avec postfix).

Ce démon est clamsmtp, il permet de faire le lien avec clamd, puis de récupérer le message et de le transférer à une autre instance de MTA (postfix en écoute locale par exemple ou un forward vers un autre smtpd sur une autre machine).

Première idée :

Clamsmtp va recevoir les messages de l'extérieur sans aucun contrôle, il va les passer à clamd pour être scanné par clamav.

Rapidement on se rend compte que clamsmtp ne peux pas écouter sous les ports inférieur à 1024 (pas root). On ne doit (peut) pas faire tourner le process avec le compte root.

Pas grave nous allons faire tourner un postfix qui va relayer le message sur le port du clamsmtp (10025 par défaut) en écoute sur 127.0.0.1 (pas la peine d'ouvrir sur le réseau).

La conf du postfix pour ça :

smtpd_relay_restrictions = permit_mynetworks permit_sasl_authenticated defer_unauth_destination
myhostname = tech-Msg.sciences.etud.u-picardie.fr
alias_maps = hash:/etc/aliases
alias_database = hash:/etc/aliases
myorigin = /etc/mailname
mydestination = $myhostname, isri.com, tech-Msg, localhost.localdomain, localhost
relayhost = 127.0.0.1:10025
mynetworks = 127.0.0.0/8 [::ffff:127.0.0.0]/104 [::1]/128
mailbox_size_limit = 0
recipient_delimiter = +
inet_interfaces = all
inet_protocols = all

Il faut ensuite envoyer à clamd (127.0.0.1:3310) qui traitera le message (tests virus).
En sortie on renvoie vers le serveur suivant (ici on va pas se compliquer la vie, on forward vers le serveur de la FAC (smtp.u-picardie.fr:25).

Le fichier de config de clamsmtp.conf :

root@tech-Msg:/home/tech# cat /etc/clamsmtpd.conf

Be sure that clamd can also handle this many connections
MaxConnections: 16

Amount of time (in seconds) to wait on network IO
TimeOut: 30

Keep Alives (ie: NOOP's to server)
#KeepAlives: 0

Send XCLIENT commands to receiving server
#XClient: off

Address to listen on (defaults to all local addresses on port 10025)
clamsmtp écoute ici...
Listen: 127.0.0.1:10025

The address clamd is listening on
la conf de clamd est juste à la suite...
ClamAddress: 127.0.0.1:3310

A header to add to all scanned email
On pourra vérifier dans le code source du message reçu sur mon adresse mail upjv
Header: X-Virus-Scanned: ClamAV using ClamSMTP P.VANIET

Directory for temporary files
#TempDirectory: /tmp

What to do when we see a virus (use 'bounce' or 'pass' or 'drop'
Action: drop

Whether or not to keep virus files
#Quarantine: off

Enable transparent proxy support
#TransparentProxy: off

User to switch to
User: clamav

Virus actions: There's an option to run a script every time a virus is found.
!IMPORTANT! This can open a hole in your server's security big enough to drive
farm vehicles through. Be sure you know what you're doing. !IMPORTANT!
#VirusAction: /path/to/some/script.sh

PidFile: /var/run/clamsmtp.pid

Faire suivre le message scanné vers le serveur de la FAC
bien entendu il faut donc utiliser une adresse u-picardie pour acceptation des messages…
sinon message je ne suis pas un « open bar »…
#OutAddress: 127.0.0.1:25
OutAddress: smtp.u-picardie.fr:25

Le fichier de conf de clamav :

root@tech-Msg:/home/tech# cat /etc/clamav/clamd.conf

LocalSocket /var/run/clamav/clamd.ctl
FixStaleSocket true
LocalSocketGroup clamav
LocalSocketMode 666
TemporaryDirectory is not set to its default /tmp here to make overriding
the default with environment variables TMPDIR/TMP/TEMP possible
User clamav
ScanMail true
ScanArchive true
ArchiveBlockEncrypted false
MaxDirectoryRecursion 15
FollowDirectorySymlinks false
FollowFileSymlinks false
ReadTimeout 180
MaxThreads 12
MaxConnectionQueueLength 15
LogSyslog false
LogRotate true
LogFacility LOG_LOCAL6
LogClean false
LogVerbose false
PreludeEnable no
PreludeAnalyzerName ClamAV
DatabaseDirectory /var/lib/clamav
OfficialDatabaseOnly false
SelfCheck 3600
Foreground false
Debug false
ScanPE true
MaxEmbeddedPE 10M
ScanOLE2 true
ScanPDF true
ScanHTML true
MaxHTMLNormalize 10M
MaxHTMLNoTags 2M
MaxScriptNormalize 5M
MaxZipTypeRcg 1M
ScanSWF true
ExitOnOOM false
LeaveTemporaryFiles false
AlgorithmicDetection true
ScanELF true
IdleTimeout 30
CrossFilesystems true
PhishingSignatures true

PhishingScanURLs true
PhishingAlwaysBlockSSLMismatch false
PhishingAlwaysBlockCloak false
PartitionIntersection false
DetectPUA false
ScanPartialMessages false
HeuristicScanPrecedence false
StructuredDataDetection false
CommandReadTimeout 30
SendBufTimeout 200
MaxQueue 100
ExtendedDetectionInfo true
OLE2BlockMacros false
AllowAllMatchScan true
ForceToDisk false
DisableCertCheck false
DisableCache false
MaxScanTime 120000
MaxScanSize 100M
MaxFileSize 25M
MaxRecursion 16
MaxFiles 10000
MaxPartitions 50
MaxIconsPE 100
PCREMatchLimit 10000
PCRERecMatchLimit 5000
PCREMaxFileSize 25M
ScanXMLDOCS true
ScanHWP3 true
MaxRecHWP3 16
StreamMaxLength 25M
LogFile /var/log/clamav/clamav.log
LogTime true
LogFileUnlock false
LogFileMaxSize 0
Bytecode true
BytecodeSecurity TrustSigned
BytecodeTimeout 60000
OnAccessMaxFileSize 5M
TCPSocket 3310
TCPAddr 127.0.0.1

TEST de la config :

```
root@tech-Msg:/home/tech# telnet 127.0.0.1 25
Trying 127.0.0.1...
Connected to 127.0.0.1.
Escape character is '^]'.
220 tech-Msg.sciences.etud.u-picardie.fr ESMTP Postfix (Ubuntu)
helo pvans
250 tech-Msg.sciences.etud.u-picardie.fr
mail from:pascal.vaniet@u-picardie.fr
250 2.1.0 Ok
rcpt to: pascal.vaniet@u-picardie.fr
250 2.1.5 Ok
data
354 End data with <CR><LF>.<CR><LF>
subject: encore un essai

coucou beu !!!
.
250 2.0.0 Ok: queued as ECDF8A00DD
quit
221 2.0.0 Bye
Connection closed by foreign host.
```

J’ai bien reçu le message dans mon lecteur thunderbird configuré pour les messages de la FAC.
On peut vérifier la ligne ajoutée par le serveur smtp clamsmtp :

```
Return-Path: <pascal.vaniet@u-picardie.fr>
Received: from lmtpproxyd (imap-01.vm.u-picardie.fr [10.0.132.110])
        by cyrus-backend-pers-1-14 (Cyrus 3.2.6-Debian-3.2.6-2~bpo10+1) with LMTPA;
        Mon, 19 Jun 2023 15:31:07 +0200
X-Cyrus-Session-Id: cyrus-1687181467-2621456-1-18341034969846593327
X-Sieve: CMU Sieve 3.0
Received: from smtp.u-picardie.fr (smtp-in-02.vm.u-picardie.fr [10.0.132.228])
        by imap.u-picardie.fr (Cyrus 3.2.5-Debian-3.2.5-2~bpo10+1) with LMTPA;
        Mon, 19 Jun 2023 15:31:07 +0200
X-Cyrus-Session-Id: cyrus-1687181467-2039333-1-2813528000501036250
Received: from smtp-out1-upjv.u-picardie.fr (smtp-out-04.vm.u-picardie.fr [10.0.132.199])
        (using TLSv1.2 with cipher ADH-AES256-GCM-SHA384 (256/256 bits))
        (No client certificate requested)
        by smtp.u-picardie.fr (Postfix) with ESMTPS id 4Ql9dR5TzRz3wfN
        for <pascal.vaniet@u-picardie.fr>; Mon, 19 Jun 2023 15:31:07 +0200 (CEST)
Received: from passoire-02.vm.u-picardie.fr (passoire-02.vm.u-picardie.fr [10.0.132.142])
        by smtp-out1-upjv.u-picardie.fr (Postfix) with ESMTP id 4Ql9dR5Jw3z10Fj
        for <pascal.vaniet@u-picardie.fr>; Mon, 19 Jun 2023 15:31:07 +0200 (CEST)
X-Virus-Scanned: Debian amavisd-new at u-picardie.fr
X-Spam-Flag: NO
X-Spam-Score: -2.089
X-Spam-Level:
X-Spam-Status: No, score=-2.089 tagged_above=-5 required=3.2
        tests=[ALL_TRUSTED=-1, BAYES_00=-1.9, DKIM_SIGNED=0.1,
        DKIM_VALID=-0.1, DKIM_VALID_AU=-0.1, DKIM_VALID_EF=-0.1,
```

MISSING_HEADERS=1.021, T_SCC_BODY_TEXT_LINE=-0.01]
autolearn=no autolearn_force=no
Received: from smtp.u-picardie.fr ([10.0.132.228])
by passoire-02.vm.u-picardie.fr (passoire-02.vm.u-picardie.fr [10.0.132.142]) (amavisd-new, port 10041)
with LMTP id wPavEgRHZpYK for <pascal.vaniet@u-picardie.fr>;
Mon, 19 Jun 2023 15:31:01 +0200 (CEST)
Received: from tech-Msg.sciences.etud.u-picardie.fr (pascal.sciences.etud.u-picardie.fr [10.1.16.50])
by smtp.u-picardie.fr (Postfix) with ESMTP id 4Ql9dJ6wNqz3wfN
for <pascal.vaniet@u-picardie.fr>; Mon, 19 Jun 2023 15:31:00 +0200 (CEST)
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; d=u-picardie.fr;
s=smtp; t=1687181461;
h=from:from:reply-to:subject:subject:date:date:message-id:message-id:to:
cc; bh=BZPeGxEaFMi5VNDbgEhmot9mjoXpjebhTCu7ApBFdQU=;

b=QEGHIwJGryrYq02ulFGOiy9w/PyiVnBhodCn77ZnHxLvzrmq6Y8Tlz7gP89lrpD0jMt2Yw
EtXn538ZISNjVBz9gJ7UAb6laj2iltMJ7rai9PvtwUfojMqyIy8PHj1wxj6+8y6ypyfTvy
LlbNBZarcx/csVttQrnINIlpHnP6AN/ZsQgTWSaGFDmDe82/t/Nl8lH6O8+lzAp3n3zzqh

cB8ff4bDWCoAayjnKMgHuIZAkCmNQ/TlmlcIB9VBAqgM0s5fF5JYTAgLa1wPCVcrbXnejd
jjQTQTh+QX9U4C/hl77cQJQgogzrT6WJiXFmwuKUwf4B8TCLgKYcPBpE+hStLw==
Received: from pvans (localhost [127.0.0.1])
by tech-Msg.sciences.etud.u-picardie.fr (Postfix) with SMTP id ECDF8A00DD
for <pascal.vaniet@u-picardie.fr>; Mon, 19 Jun 2023 15:30:26 +0200 (CEST)
subject: encore un essai
Message-Id: <20230619133040.ECDF8A00DD@tech-Msg.sciences.etud.u-picardie.fr>
Date: Mon, 19 Jun 2023 15:30:26 +0200 (CEST)
From: pascal.vaniet@u-picardie.fr
X-Virus-Scanned: ClamAV using ClamSMTP P.VANIET
X-Spamd-Bar: ++
Authentication-Results: smtp.u-picardie.fr;
none
X-Rspamd-Server: passoire-04
X-Rspamd-Queue-Id: 4Ql9dJ6wNqz3wfN
X-Spamd-Result: default: False [2.00 / 1000.00];
MISSING_TO(2.00)[];
RCVD_NO_TLS_LAST(0.10)[];
MIME_GOOD(-0.10)[text/plain];
FROM_EQ_ENVFROM(0.00)[];
NEURAL_HAM(-0.00)[-1.000];
ARC_NA(0.00)[];
FROM_NO_DN(0.00)[];
DKIM_SIGNED(0.00)[u-picardie.fr:s=smtp];
MIME_TRACE(0.00)[0:+];
UPJV_FROM(0.00)[u-picardie.fr];
MID_RHS_MATCH_FROMTLD(0.00)[];
RCVD_COUNT_TWO(0.00)[2]

coucou beu !!!