Phase de mise en production guacamole

Changer le mote de passe root

```
root@apache-guaca:~# sudo passwd root
New password:
Retype new password:
passwd: password updated successfully
root@apache-guaca:~# _
```

Changer le mote de passe admin

D'ailluer Nous avons tenté de changer le nom de l'utilisateur configuré pour Guacamole, mais cette modification a entraîné des erreurs liées aux permissions, à la base de données et aux services système (Tomcat, MariaDB). Après plusieurs essais, la configuration ne fonctionnait plus correctement.

Étant en dernière semaine de stage et avec l'accord de mon responsable, j'ai décidé de conserver l'ancien nom d'utilisateur afin d'assurer la stabilité du service et d'éviter toute interruption.

```
root@apache-guaca:~# passwd zafar
New password:
Retype new password:
passwd: password updated successfully
root@apache-guaca:~#
```

Changement les information de la base de données

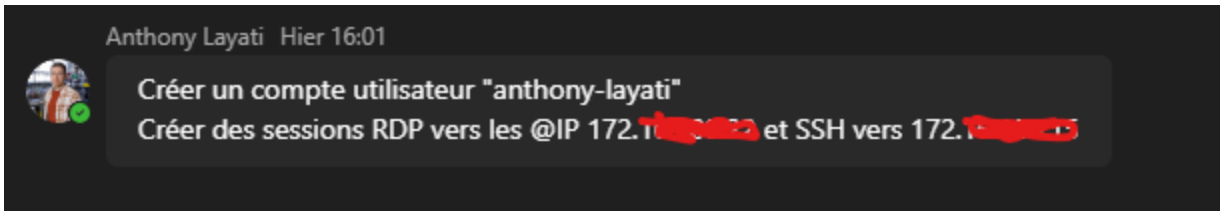
```
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> SELECT user, host FROM mysql.user;
+-------------+-----------+
| User        | Host      |
+-------------+-----------+
| mariadb.sys | localhost |
| mysql       | localhost |
| root        | localhost |
| userdb      | localhost |
+-------------+-----------+
4 rows in set (0,001 sec)

MariaDB [(none)]> RENAME USER 'userdb'@'localhost' TO 'admin'@'localhost';
Query OK, 0 rows affected (0,001 sec)

MariaDB [(none)]> ALTER USER 'admin'@'localhost' IDENTIFIED BY 'Daudruy@2025';
Query OK, 0 rows affected (0,000 sec)

MariaDB [(none)]> FLUSH PRIVILEGES;
Query OK, 0 rows affected (0,000 sec)

MariaDB [(none)]> EXIT;
Bye
```

```
zafar@apache-guaca:~# mysql -u admin -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 96
```

```
MariaDB [(none)]> GRANT ALL PRIVILEGES ON guacamole_db.* TO 'admin'@'localhost' IDENTIFIED BY '[redacted]';
Query OK, 0 rows affected (0,001 sec)

MariaDB [(none)]> FLUSH PRIVILEGES;
```

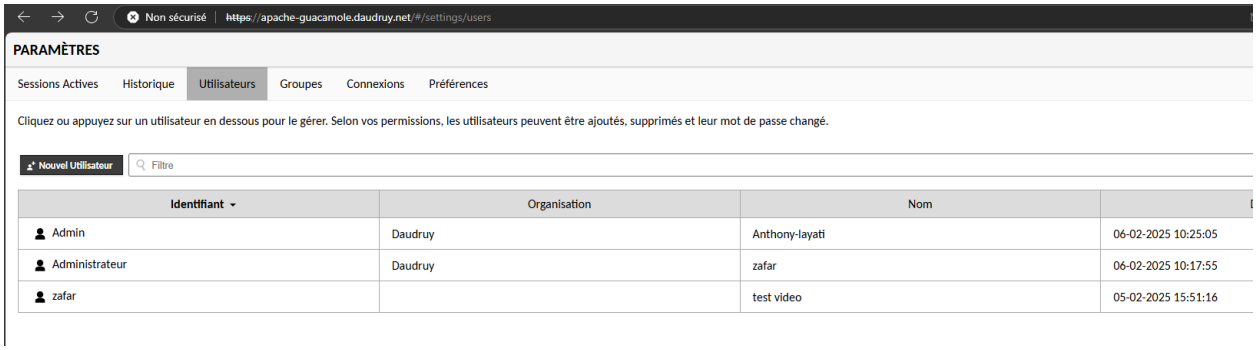
```
MariaDB [(none)]> SELECT user, host FROM mysql
+-------------+-----------+
| User        | Host      |
+-------------+-----------+
| admin       | localhost |
| mariadb.sys | localhost |
| mysql       | localhost |
| root        | localhost |
+-------------+-----------+
```

Premier connexion situation reel

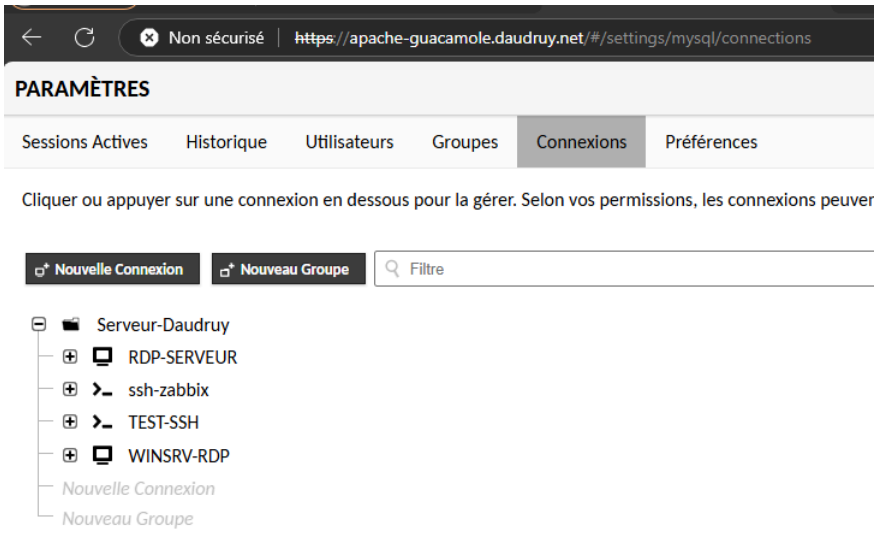



```
  GNU nano 6.2                                /etc/guacamole/guacamole.properties
#declaration de de la connexion a Mariadb
#ce fichier est utile aussi pour d'autre parametres

# MySQL ------------------------
mysql-hostname: 127.0.0.1
mysql-port: 3[redacted]
mysql-database: guacadb
mysql-username: admin
mysql-password: Daud[redacted]
#-------------------------------
```

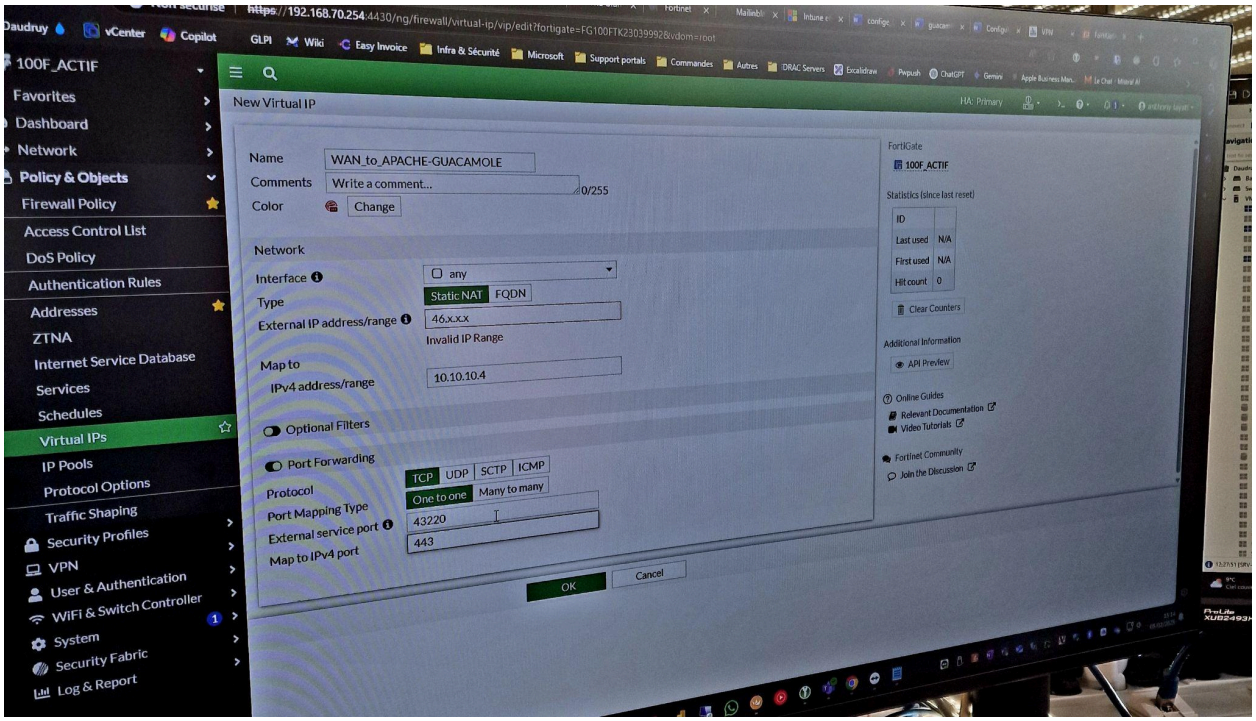
Chagemengem admin guacamole

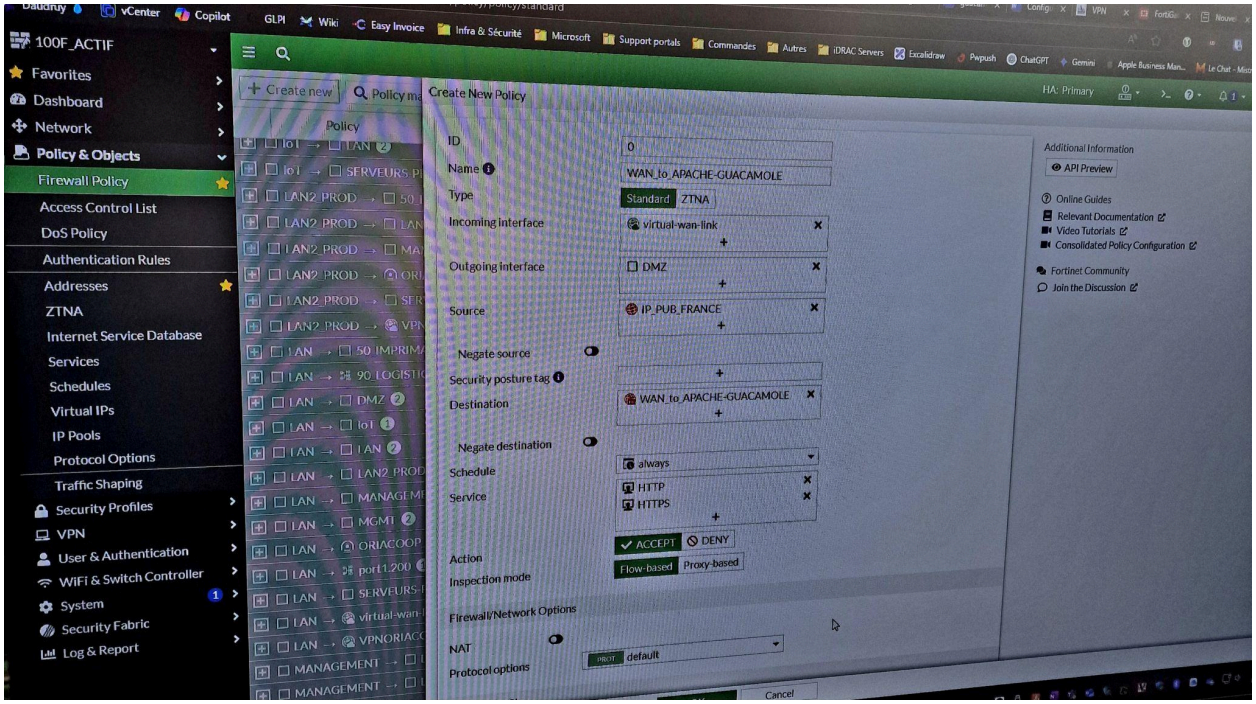


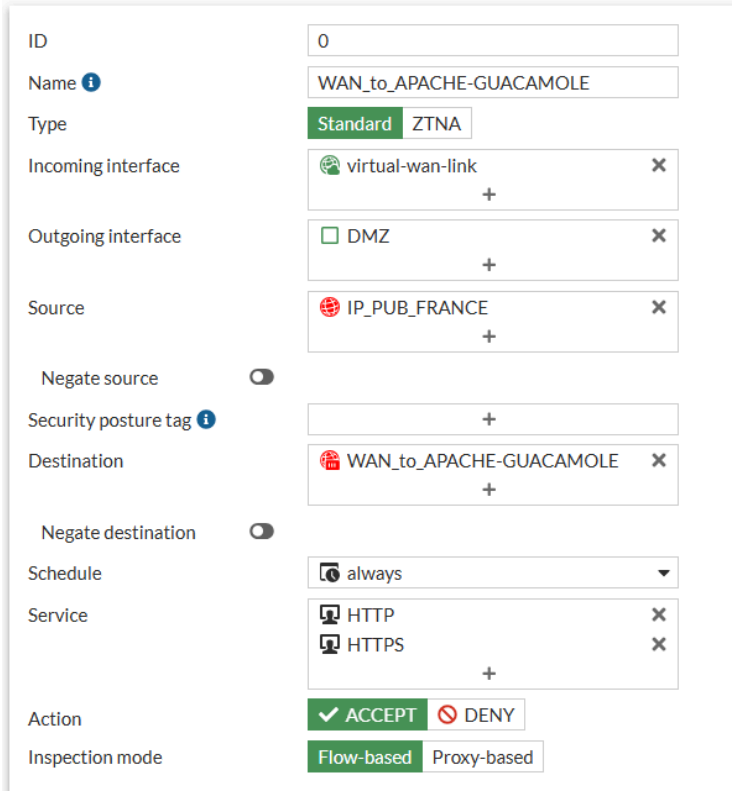
Création des nouveau connexion



Configuration NAT




100F_ACTIF
Favorites
Dashboard
Network
Policy & Objects
Firewall Policy
Access Control List
DoS Policy
Authentication Rules
Addresses
ZTNA
Internet Service Database
Services
Schedules
Virtual IPs
IP Pools
Protocol Options
Traffic Shaping
Security Profiles
VPN
User & Authentication
WiFi & Switch Controller
System
Security Fabric
Log & Report
Create new
Policy
Create New Policy
ID
0
Name
WAN_to_APACHE-GUACAMOLE
Type
Standard
ZTNA
Incoming Interface
virtual-wan-link
Outgoing Interface
DMZ
Source
IP_PUB_FRANCE
Negate source
Security posture tag
Destination
WAN_to_APACHE-GUACAMOLE
Negate destination
Schedule
always
Service
HTTP
HTTPS
Action
ACCEPT
DENY
Inspection mode
Flow-based
Proxy-based
Firewall/Network Options
NAT
Protocol options
default
Additional Information
API Preview
Online Guides
Relevant Documentation
Video Tutorials
Consolidated Policy Configuration
Fortinet Community
Join the Discussion
HA: Primary
Cancel



Config ip et port pour avoir accès depuis internet

N configure le ip et le port de guacamole pour répondre sur internet car sur wan pour le moment il y a pas de DNS et Certificate

```
 GNU nano 6.2                                guacamole.conf *
<VirtualHost *:443>
    ServerName 10.10.10.4  # depuis interent il reponde avec cette ip apres on pourra la chagenr avec un DNS
    SSLEngine on
    SSLCertificateFile /etc/ssl/certs/ton-certificat.crt
    SSLCertificateKeyFile /etc/ssl/private/ton-certificat.key

    ProxyPreserveHost On
    ProxyPass / http://127.0.0.1:8080/  # Guacamole tourne sur Tomcat sur le port 8080
    ProxyPassReverse / http://127.0.0.1:8080/

    ErrorLog ${APACHE_LOG_DIR}/guacamole_error.log
    CustomLog ${APACHE_LOG_DIR}/guacamole_access.log combined
</VirtualHost>
```

On as testé ce jour là de se connecter depuis internet en tapantt 10.10.10.4:443 et ca marche de coup il reste pour le equip de chète le certificat et un nome de domaine

En local

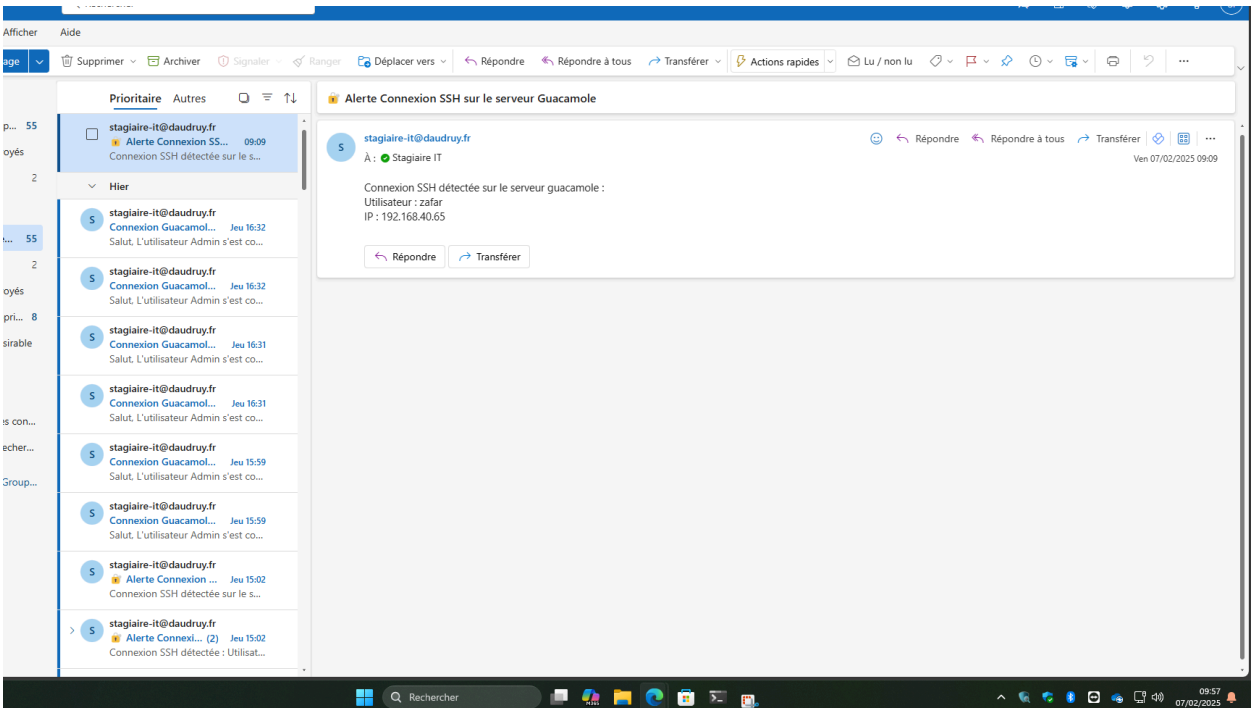
En local il ya bien un dsn configurer et un certificate autosigné que j'ai déposé sur pc après pour le dépôt de certi on peut aussi utiliser gpo

```
zafar@apache-guaca:/etc/apache2/sites-available# ls
000-default.conf  apache-guacamole.conf  default-ssl.conf  guacamole.conf
zafar@apache-guaca:/etc/apache2/sites-available#
```

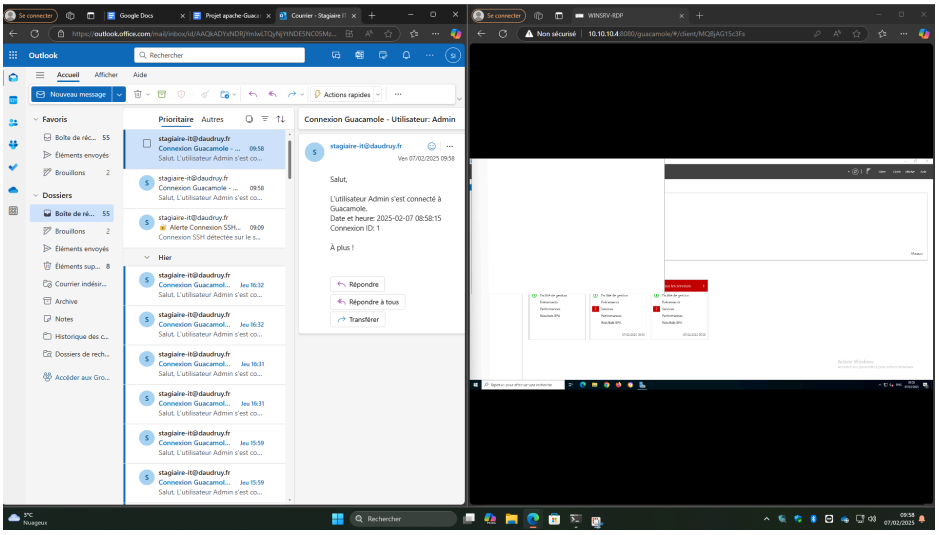
```
 GNU nano 6.2                                apache-guacamole.conf
<VirtualHost *:80>
    ServerName apache-guacamole.daudruy.net

    ProxyPreserveHost On
    ProxyPass / http://127.0.0.1:8080/guacamole/
    ProxyPassReverse / http://127.0.0.1:8080/guacamole/

    ErrorLog ${APACHE_LOG_DIR}/guacamole_error.log
    CustomLog ${APACHE_LOG_DIR}/guacamole_access.log combined
</VirtualHost>

<VirtualHost *:443>
    ServerName apache-guacamole.daudruy.net

    SSLEngine on
    SSLCertificateFile /etc/ssl/certs/apacheguac.crt
    SSLCertificateKeyFile /etc/ssl/private/apacheguac.key

    ProxyPreserveHost On
    ProxyPass / http://127.0.0.1:8080/guacamole/
    ProxyPassReverse / http://127.0.0.1:8080/guacamole/

    ErrorLog ${APACHE_LOG_DIR}/guacamole_ssl_error.log
    CustomLog ${APACHE_LOG_DIR}/guacamole_ssl_access.log combined
</VirtualHost>
```

Test des script

Script envoi notification connexion ssh sur serveur guacamole



Script envie notification connexion rdp :



Automatiser le script de conversion vidéo et envoi vers NAS

```
  GNU nano 6.2                                  /tmp/crontab.2WItPE/crontab
#
# Notice that tasks will be started based on the cron's system
# daemon's notion of time and timezones.
#
# Output of the crontab jobs (including errors) is sent through
# email to the user the crontab file belongs to (unless redirected).
#
# For example, you can run a backup of all your user accounts
# at 5 a.m every week with:
# 0 5 * * 1 tar -zcf /var/backups/home.tgz /home/
#
# For more information see the manual pages of crontab(5) and cron(8)
#
# m h  dom mon dow   command



# script s'exécute tous les 10 jours à 13h (1 PM) pour supprimer les videos de NAS
0 13 */10 * * /opt/scripts/nas_supprime.sh



#Automatiser l'exécution du script pour envoie et conversion des video
0 */2 * * * /bin/bash /opt/scripts/envoie_et_nettoie.sh >> /var/log/envoie_et_nettoie.log 2>&1
```

```
Étape 1.1 : Conversion du fichier 20250128-125117 - RDP - Administrateur en .m4v
guacenc: INFO: Guacamole video encoder (guacenc) version 1.5.5
guacenc: INFO: 1 input file(s) provided.
guacenc: INFO: Video will be encoded at 1280x720 and 2000000 bps.
guacenc: INFO: Encoding "/var/lib/guacamole/recordings/d9666d3f-5d6a-335d-bf49-e052d6130967/20250128-125117 - RDP -
nistrateur" to "/var/lib/guacamole/recordings/d9666d3f-5d6a-335d-bf49-e052d6130967/20250128-125117 - RDP - Administr
.m4v"
```

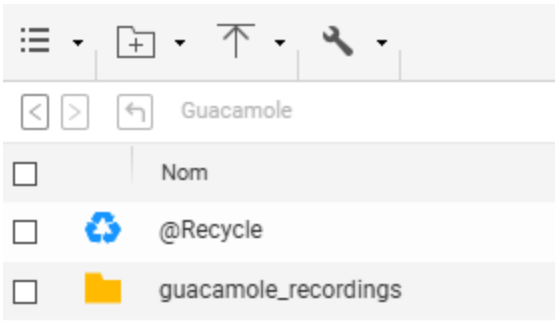
```
sent 8.355.152 bytes  received 35 bytes  16.710.374,00 bytes/sec
total size is 8.352.991  speedup is 1,00
Fichier 20250205-145117 - RDP - zafar transféré avec succès vers le NAS.==========================
Étape 1.3 : Suppression du fichier local /var/lib/guacamole/recordings/ff8a25da-2118-3dd8-a03f-fe1af05a6896/20250205-145
117 - RDP - zafar et fichier converti
Fichier local 20250205-145117 - RDP - zafar supprimé avec succès.
Étape 1.4 : Vérification et suppression du répertoire /var/lib/guacamole/recordings/ff8a25da-2118-3dd8-a03f-fe1af05a6896
```

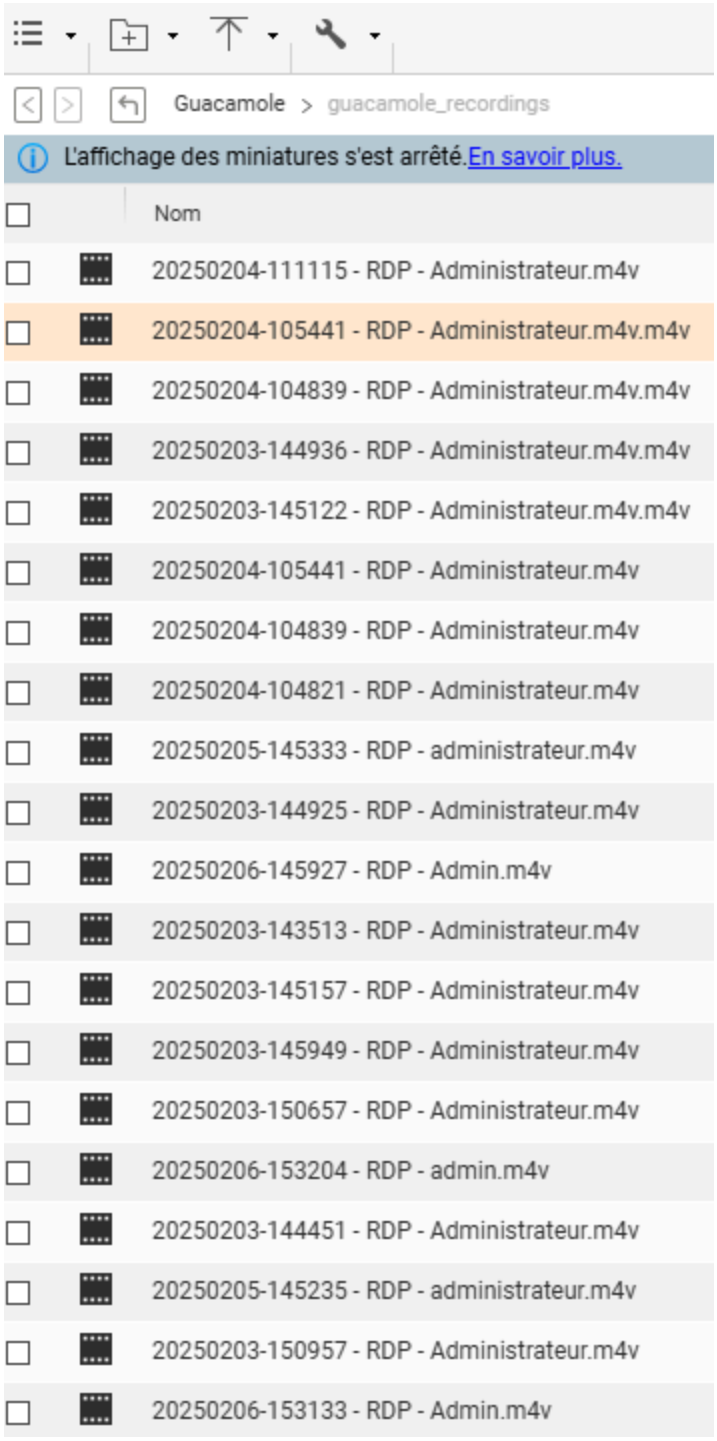
Le vedio sont transmis sur nas

```
zafar@apache-guaca:/opt/scripts$ sudo ls -l /mnt/nas/guacamole_recordings/
total 525652
-rwxr-xr-x 1 root root   5684234 févr.  7 09:06 '20250128-125117 - RDP - Administrateur.m4v'
-rwxr-xr-x 1 root root   1666610 févr.  7 09:05 '20250203-143513 - RDP - Administrateur.m4v'
-rwxr-xr-x 1 root root     10761 févr.  7 09:06 '20250203-144441 - RDP - Administrateur.m4v'
-rwxr-xr-x 1 root root   1195583 févr.  7 09:05 '20250203-144451 - RDP - Administrateur.m4v'
-rwxr-xr-x 1 root root     10761 févr.  7 09:02 '20250203-144925 - RDP - Administrateur.m4v'
-rwxr-xr-x 1 root root   1329092 févr.  7 09:05 '20250203-144936 - RDP - Administrateur.m4v'
-rwxr-xr-x 1 root root     10761 févr.  4 11:12 '20250203-144936 - RDP - Administrateur.m4v.m4v'
-rwxr-xr-x 1 root root   1742395 févr.  7 09:05 '20250203-145122 - RDP - Administrateur.m4v'
-rwxr-xr-x 1 root root     10761 févr.  4 11:12 '20250203-145122 - RDP - Administrateur.m4v.m4v'
-rwxr-xr-x 1 root root   5517383 févr.  7 09:05 '20250203-145157 - RDP - Administrateur.m4v'
-rwxr-xr-x 1 root root     10761 févr.  7 09:05 '20250203-145232 - RDP - Administrateur.m4v'
-rwxr-xr-x 1 root root     10761 févr.  7 09:05 '20250203-145949 - RDP - Administrateur.m4v'
-rwxr-xr-x 1 root root   2930123 févr.  7 09:05 '20250203-150657 - RDP - Administrateur.m4v'
-rwxr-xr-x 1 root root     10761 févr.  7 09:05 '20250203-150742 - RDP - Administrateur.m4v'
-rwxr-xr-x 1 root root     10761 févr.  7 09:06 '20250203-150806 - RDP - Administrateur.m4v'
-rwxr-xr-x 1 root root     10761 févr.  7 09:05 '20250203-150957 - RDP - Administrateur.m4v'
-rwxr-xr-x 1 root root   1844228 févr.  4 11:15 '20250204-104821 - RDP - Administrateur.m4v'
-rwxr-xr-x 1 root root   2261745 févr.  4 11:15 '20250204-104839 - RDP - Administrateur.m4v'
-rwxr-xr-x 1 root root     10761 févr.  4 11:12 '20250204-104839 - RDP - Administrateur.m4v.m4v'
-rwxr-xr-x 1 root root  21576876 févr.  4 11:15 '20250204-105441 - RDP - Administrateur.m4v'
```

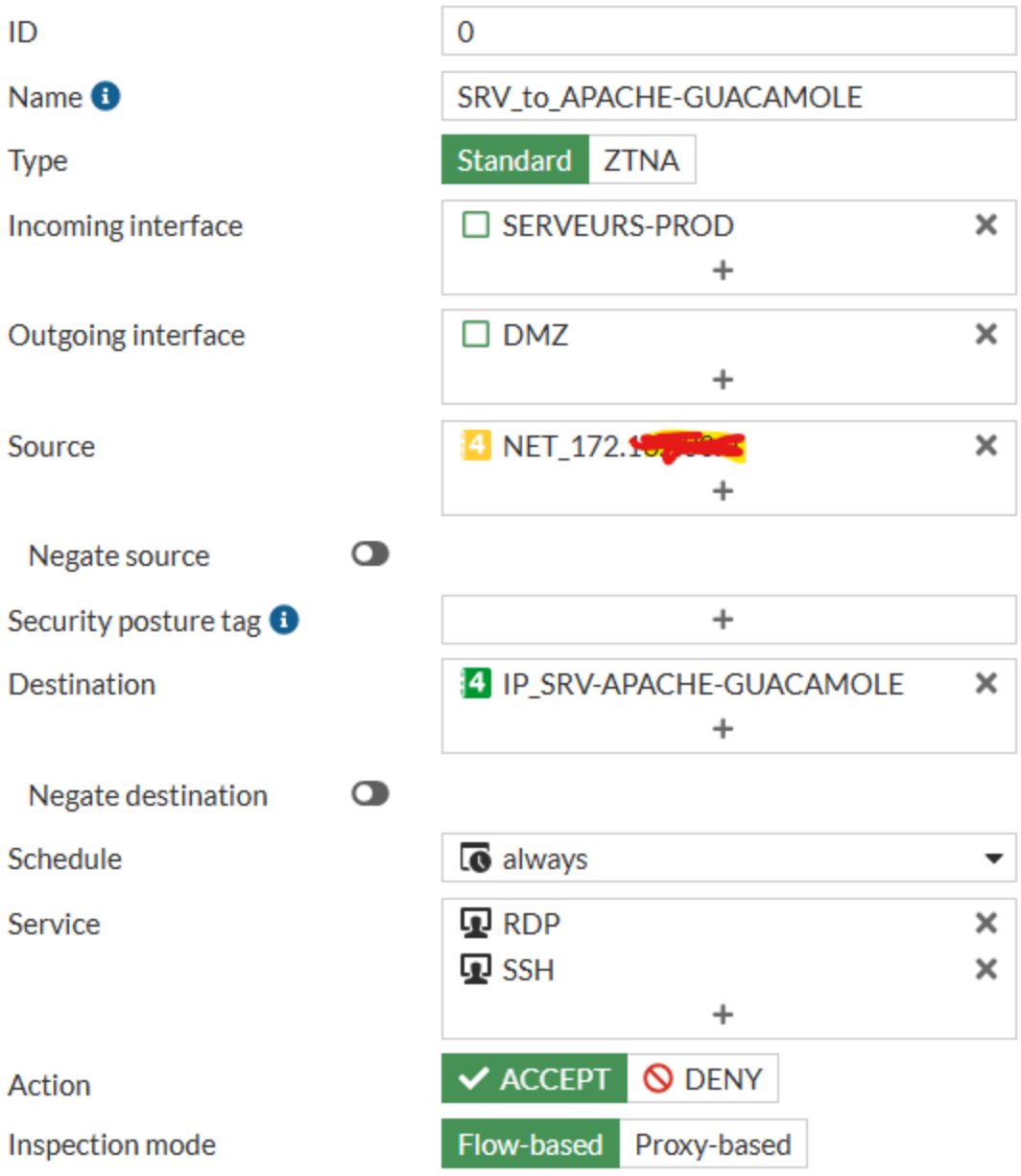
Dossier local ets vide apres execution de script

```
zafar@apache-guaca:/var/lib/guacamole/recordings$ ls
zafar@apache-guaca:/var/lib/guacamole/recordings$
```




Guacamole > guacamole_recordings
L'affichage des miniatures s'est arrêté. En savoir plus.
Nom
20250204-111115 - RDP - Administrateur.m4v
20250204-105441 - RDP - Administrateur.m4v.m4v
20250204-104839 - RDP - Administrateur.m4v.m4v
20250203-144936 - RDP - Administrateur.m4v.m4v
20250203-145122 - RDP - Administrateur.m4v.m4v
20250204-105441 - RDP - Administrateur.m4v
20250204-104839 - RDP - Administrateur.m4v
20250204-104821 - RDP - Administrateur.m4v
20250205-145333 - RDP - administrateur.m4v
20250203-144925 - RDP - Administrateur.m4v
20250206-145927 - RDP - Admin.m4v
20250203-143513 - RDP - Administrateur.m4v
20250203-145157 - RDP - Administrateur.m4v
20250203-145949 - RDP - Administrateur.m4v
20250203-150657 - RDP - Administrateur.m4v
20250206-153204 - RDP - admin.m4v
20250203-144451 - RDP - Administrateur.m4v
20250205-145235 - RDP - administrateur.m4v
20250203-150957 - RDP - Administrateur.m4v
20250206-153133 - RDP - Admin.m4v

Création de policy sur pare-feu pour laisser paser les connexion entre guacamole et les service de production



Nettoyage de disque local et nas

```
zafar@apache-guaca:/var/lib/guacamole/recordings$ sudo /opt/scripts/
envoie_et_nettoie.sh      monitor_guacamole_ssh.py  watch_guac_log.sh
guac_notify.sh            nas_supprime.sh
zafar@apache-guaca:/var/lib/guacamole/recordings$ sudo /opt/scripts/
envoie_et_nettoie.sh      monitor_guacamole_ssh.py  watch_guac_log.sh
guac_notify.sh            nas_supprime.sh
zafar@apache-guaca:/var/lib/guacamole/recordings$ sudo /opt/scripts/nas_supprime.sh
Suppression de tous les fichiers dans le répertoire /mnt/nas/guacamole_recordings/
Tous les fichiers ont été supprimés avec succès.
zafar@apache-guaca:/var/lib/guacamole/recordings$ ls -l /mnt/nas/guacamole_recordings/
total 0
zafar@apache-guaca:/var/lib/guacamole/recordings$
```

Création un super utilisateur

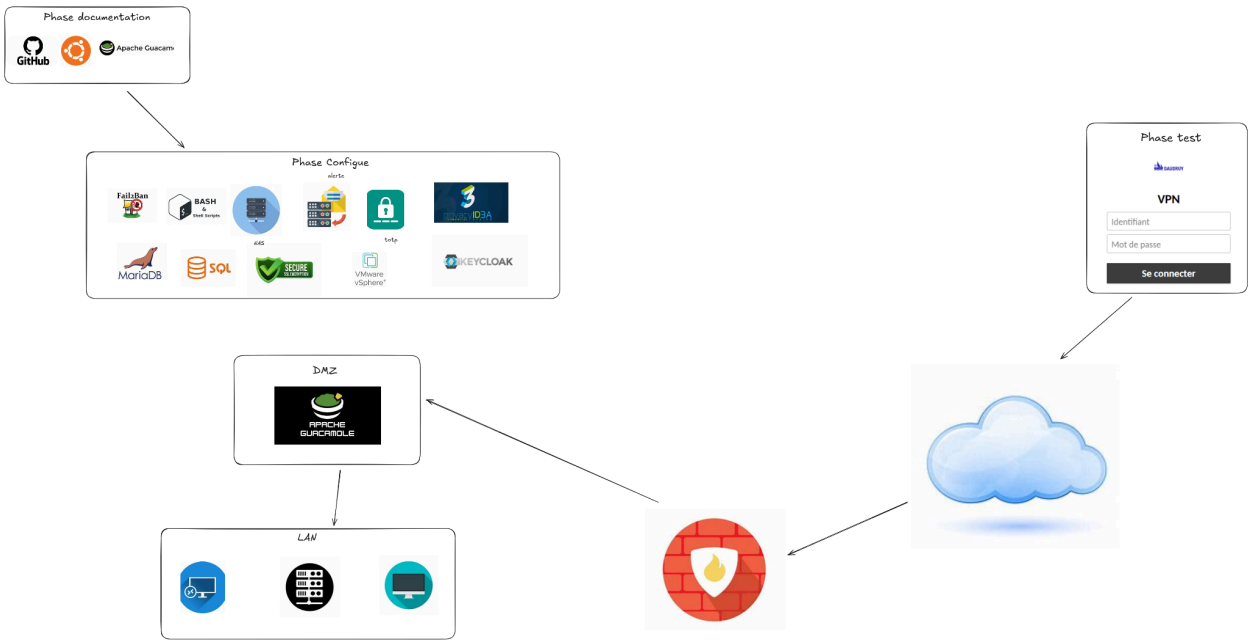

```
C:\Users\stagiaire-it>ssh admin@10.10.10.4
################################################################################
#
#    AVERTISSEMENT DE SÉCURITÉ - ENTREPRISE DAUDRUY
#
# Vous accédez à un système sécurisé de l'entreprise Daudruy. Toute
# connexion est enregistrée, y compris votre adresse IP, votre heure de
# connexion et votre nom d'utilisateur. Ces informations peuvent être
# utilisées à des fins de sécurité et de conformité avec la législation
```

```
Last login: Fri Feb  7 13:41:55 2025 from 192.168.40.65
 apache-guaca  admin  ~
```

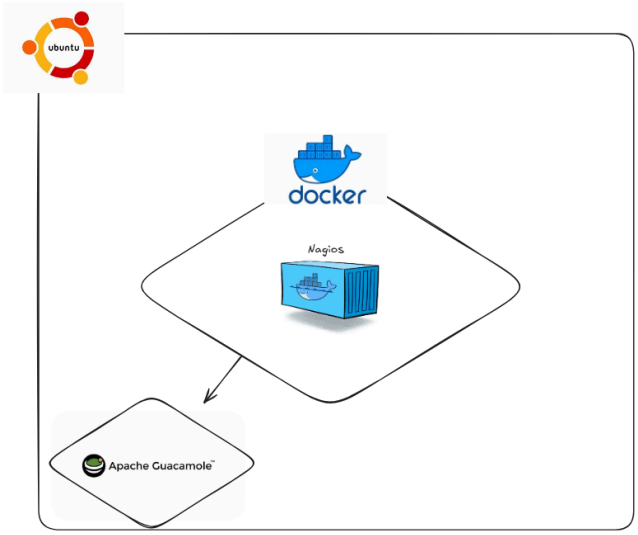
Changer le banner

```
C:\Users\stagiaire-it>ssh admin@10.10.10.4
##############################################################################
#      🚨 AVERTISSEMENT DE SÉCURITÉ – ENTREPRISE DAUDRUY 🚨
#
#      ⚠️ Accès strictement réservé aux utilisateurs autorisés.
#      🕵️ Toute connexion est enregistrée et notifiée à l'équipe IT.
#      🔴 Une tentative d'accès non autorisée peut entraîner des poursuites.
#
#      📩 Support IT : support@daudruy.fr
#
#      ──────────────────────────────────────────────────────────
#      🔒 SECURITY WARNING – DAUDRUY COMPANY 🔒
#
#      ⚠️ Authorized users only. Unauthorized access is prohibited.
#      🕵️ All logins are logged and notified to the IT team.
#      🔴 Violations may result in legal action.
#
#      📩 IT Support : support@daudruy.fr
##############################################################################
```

Test depuis wan




Nagios
KEYCLOAK
privacyIDEA
Fail2Ban
Apache Guacamole
utile


ubuntu
docker
Nagios
Apache Guacamole