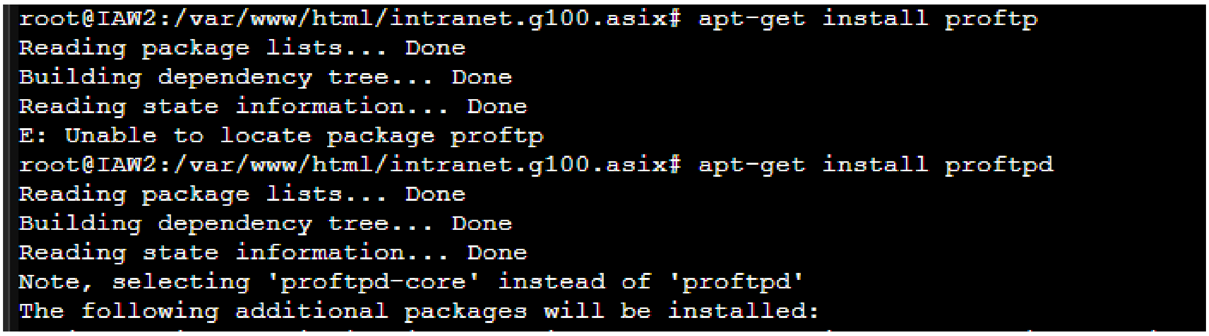
Memoria Aprendizaje SRI

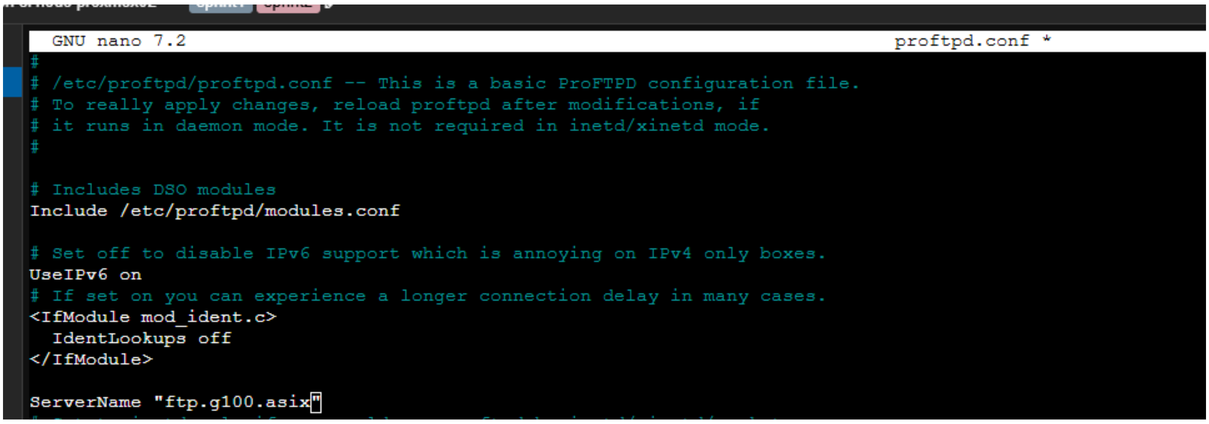
13-11-2025

Instalación proftpd



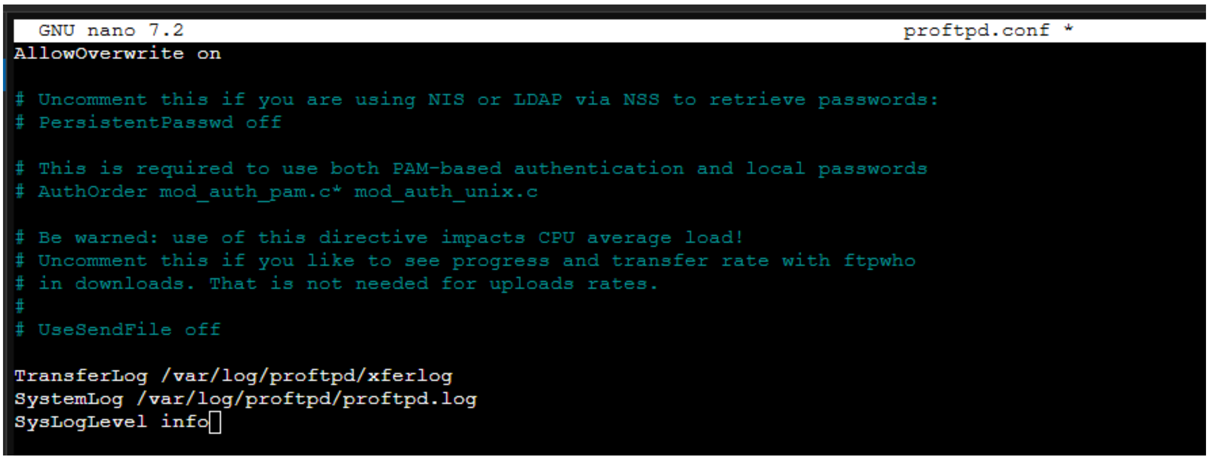
```
root@IAW2:/var/www/html/intranet.g100.asix# apt-get install proftp
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
E: Unable to locate package proftp
root@IAW2:/var/www/html/intranet.g100.asix# apt-get install proftpd
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Note, selecting 'proftpd-core' instead of 'proftpd'
The following additional packages will be installed:
```

Poner ftp.g100.asix al servidor



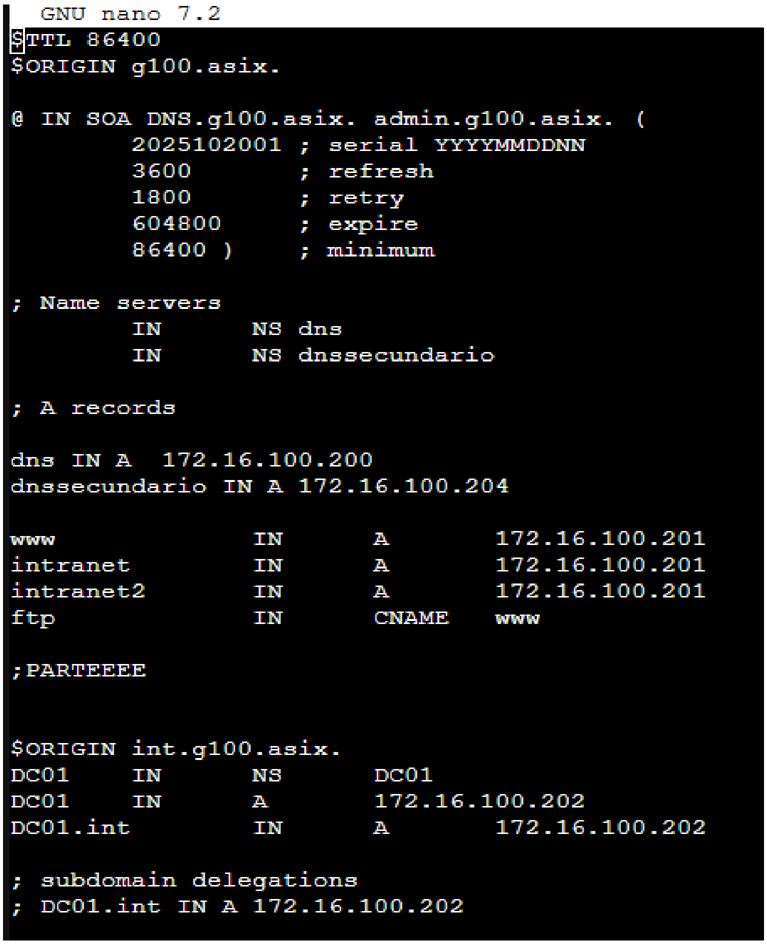
```
  GNU nano 7.2                                                  proftpd.conf *
#
# /etc/proftpd/proftpd.conf -- This is a basic ProFTPD configuration file.
# To really apply changes, reload proftpd after modifications, if
# it runs in daemon mode. It is not required in inetd/xinetd mode.
#

# Includes DSO modules
Include /etc/proftpd/modules.conf

# Set off to disable IPv6 support which is annoying on IPv4 only boxes.
UseIPv6 on
# If set on you can experience a longer connection delay in many cases.
<IfModule mod_ident.c>
  IdentLookups off
</IfModule>

ServerName "ftp.g100.asix"
```

Configurad el syslog con nivel “info” a un fichero específico dentro del directorio /var/log/.



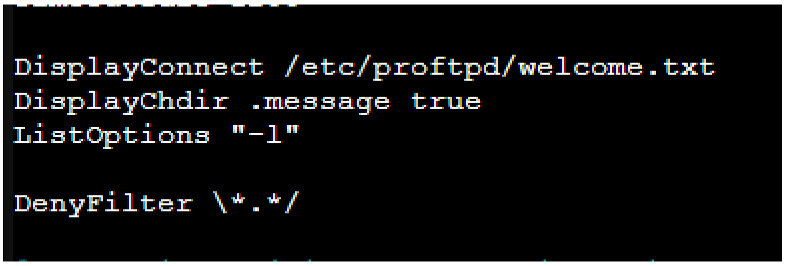
```
  GNU nano 7.2                                                      proftpd.conf *
AllowOverwrite on

# Uncomment this if you are using NIS or LDAP via NSS to retrieve passwords:
# PersistentPasswd off

# This is required to use both PAM-based authentication and local passwords
# AuthOrder mod_auth_pam.c* mod_auth_unix.c

# Be warned: use of this directive impacts CPU average load!
# Uncomment this if you like to see progress and transfer rate with ftpwho
# in downloads. That is not needed for uploads rates.
#
# UseSendFile off

TransferLog /var/log/proftpd/xferlog
SystemLog /var/log/proftpd/proftpd.log
SysLogLevel info
```

Añadir entra ftp para resolver dicho nombre

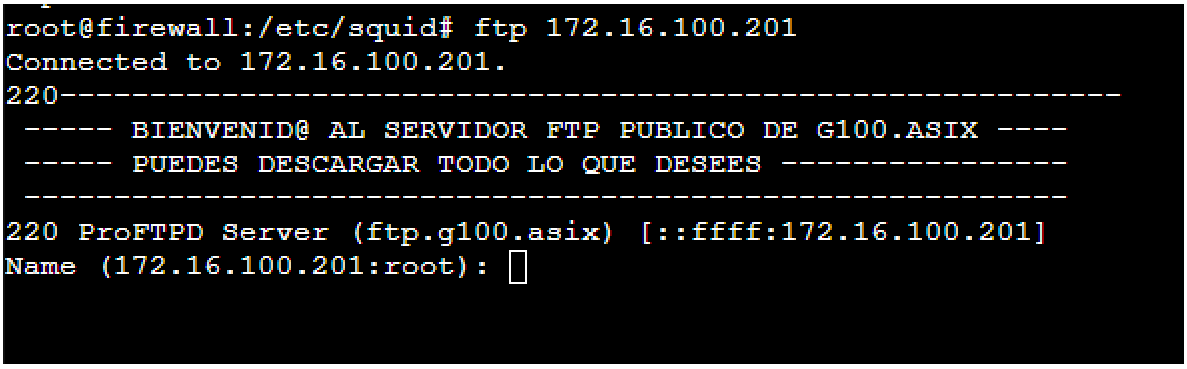


```
  GNU nano 7.2
$TTL 86400
$ORIGIN g100.asix.

@ IN SOA DNS.g100.asix. admin.g100.asix. (
        2025102001 ; serial YYYYMMDDNN
        3600       ; refresh
        1800       ; retry
        604800     ; expire
        86400 )    ; minimum

; Name servers
        IN      NS dns
        IN      NS dnssecundario

; A records

dns IN A  172.16.100.200
dnssecundario IN A 172.16.100.204

www             IN      A       172.16.100.201
intranet        IN      A       172.16.100.201
intranet2       IN      A       172.16.100.201
ftp             IN      CNAME   www

;PARTEEEE


$ORIGIN int.g100.asix.
DC01    IN      NS      DC01
DC01    IN      A       172.16.100.202
DC01.int        IN      A       172.16.100.202

; subdomain delegations
; DC01.int IN A 172.16.100.202
```

Mensaje de bienvenida en ftp

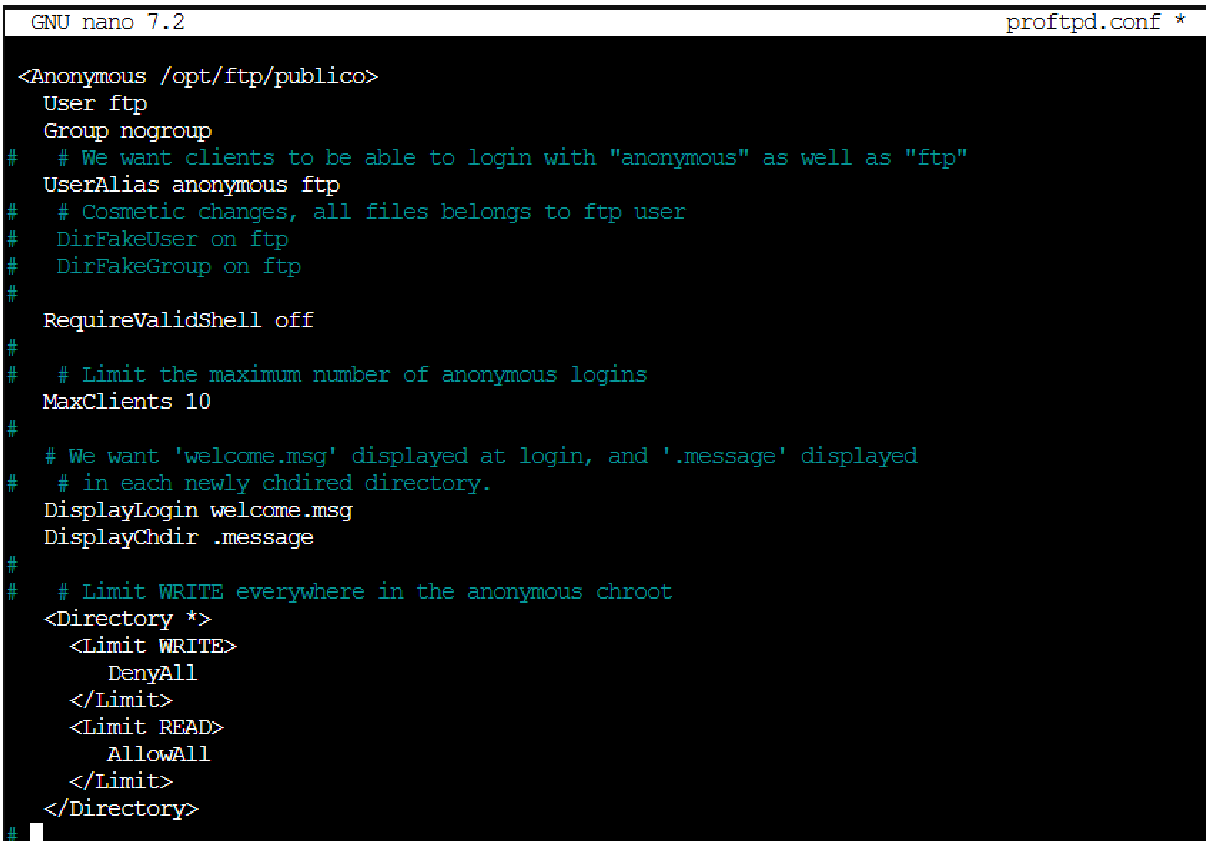


```
DisplayConnect /etc/proftpd/welcome.txt
DisplayChdir .message true
ListOptions "-l"

DenyFilter \*.*/
```



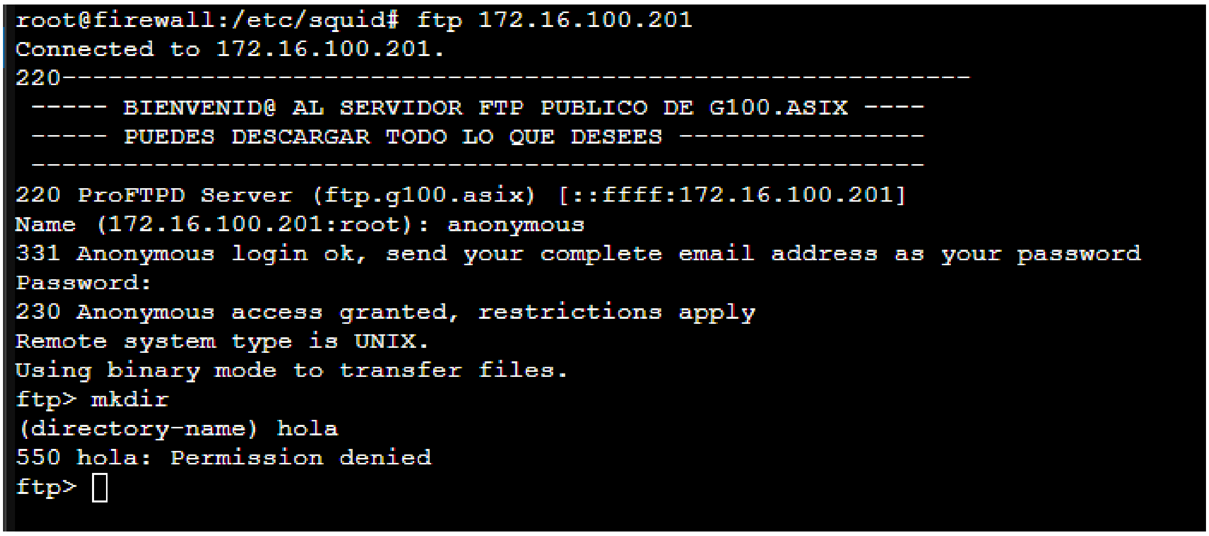
```
root@firewall:/etc/squid# ftp 172.16.100.201
Connected to 172.16.100.201.
220-----------------------------------------------------------
 ----- BIENVENID@ AL SERVIDOR FTP PUBLICO DE G100.ASIX ----
 ----- PUEDES DESCARGAR TODO LO QUE DESEES ----------------
 ----------------------------------------------------------
220 ProFTPD Server (ftp.g100.asix) [::ffff:172.16.100.201]
Name (172.16.100.201:root): 
```

Configura ftp para que el usuario anonymous entre en el directorio del sistema /opt/ftp/publico en modo lectura, sin poder escribir.



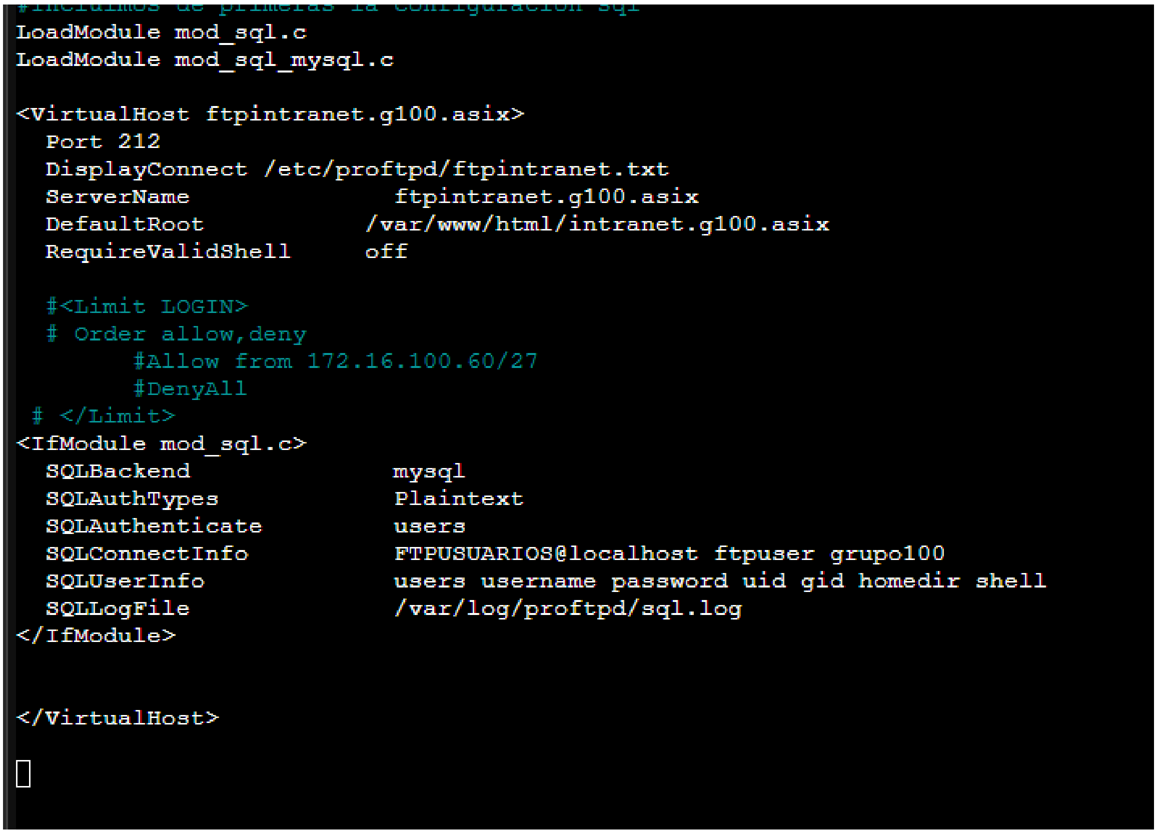
```
  GNU nano 7.2                                                              proftpd.conf *

 <Anonymous /opt/ftp/publico>
   User ftp
   Group nogroup
#    # We want clients to be able to login with "anonymous" as well as "ftp"
   UserAlias anonymous ftp
#    # Cosmetic changes, all files belongs to ftp user
#    DirFakeUser on ftp
#    DirFakeGroup on ftp
#
   RequireValidShell off
#
#    # Limit the maximum number of anonymous logins
   MaxClients 10
#
   # We want 'welcome.msg' displayed at login, and '.message' displayed
#    # in each newly chdired directory.
   DisplayLogin welcome.msg
   DisplayChdir .message
#
#    # Limit WRITE everywhere in the anonymous chroot
   <Directory *>
     <Limit WRITE>
        DenyAll
     </Limit>
     <Limit READ>
        AllowAll
     </Limit>
   </Directory>
# 
```

Comprobamos que no se puede escribir



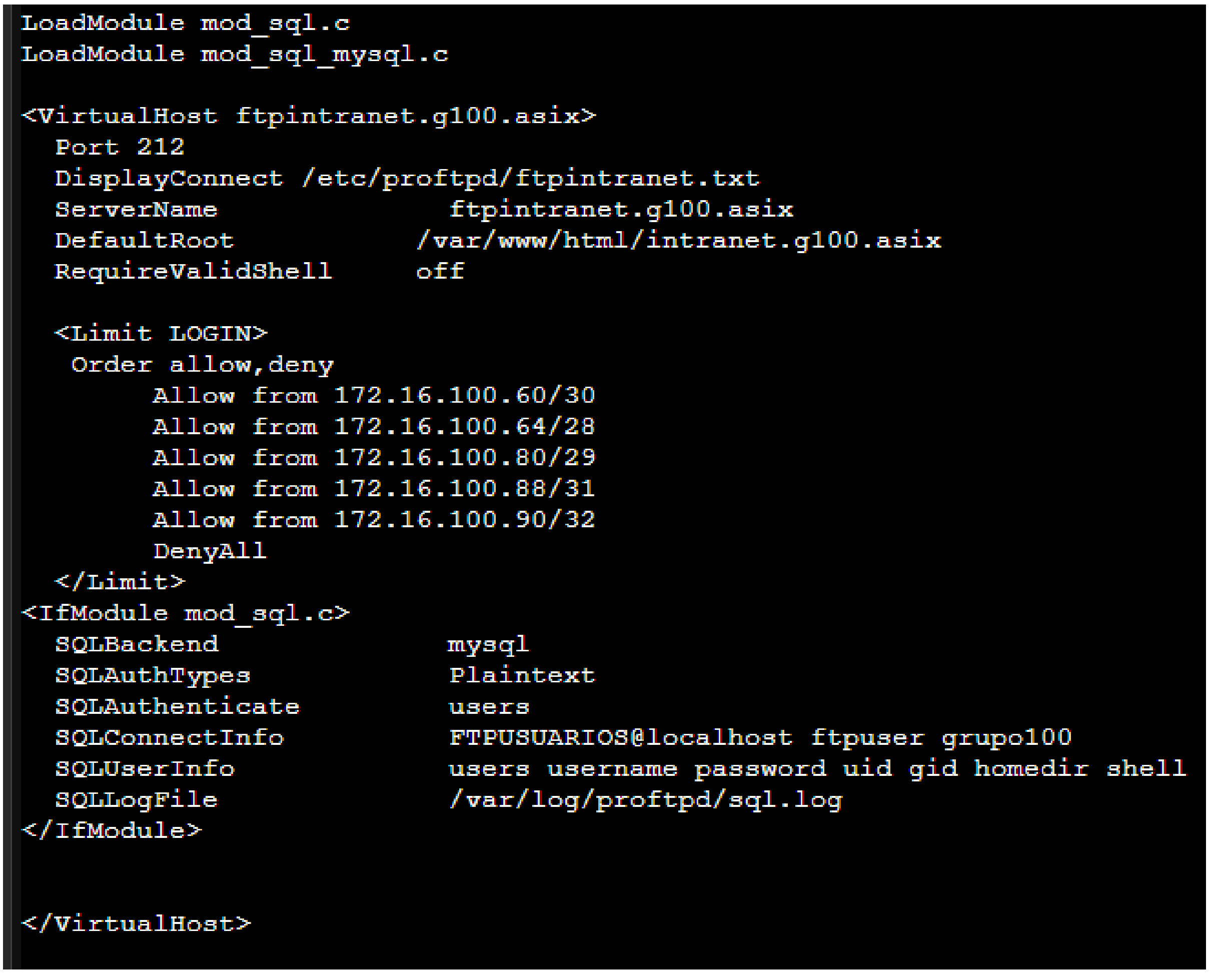
```
root@firewall:/etc/squid# ftp 172.16.100.201
Connected to 172.16.100.201.
220-------------------------------------------------------------
 ----- BIENVENID@ AL SERVIDOR FTP PUBLICO DE G100.ASIX ----
 ----- PUEDES DESCARGAR TODO LO QUE DESEES -----------------
 ----------------------------------------------------------

220 ProFTPD Server (ftp.g100.asix) [::ffff:172.16.100.201]
Name (172.16.100.201:root): anonymous
331 Anonymous login ok, send your complete email address as your password
Password:
230 Anonymous access granted, restrictions apply
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> mkdir
(directory-name) hola
550 hola: Permission denied
ftp> 
```

Configuración de virtual host ftpintranet.g100.asix



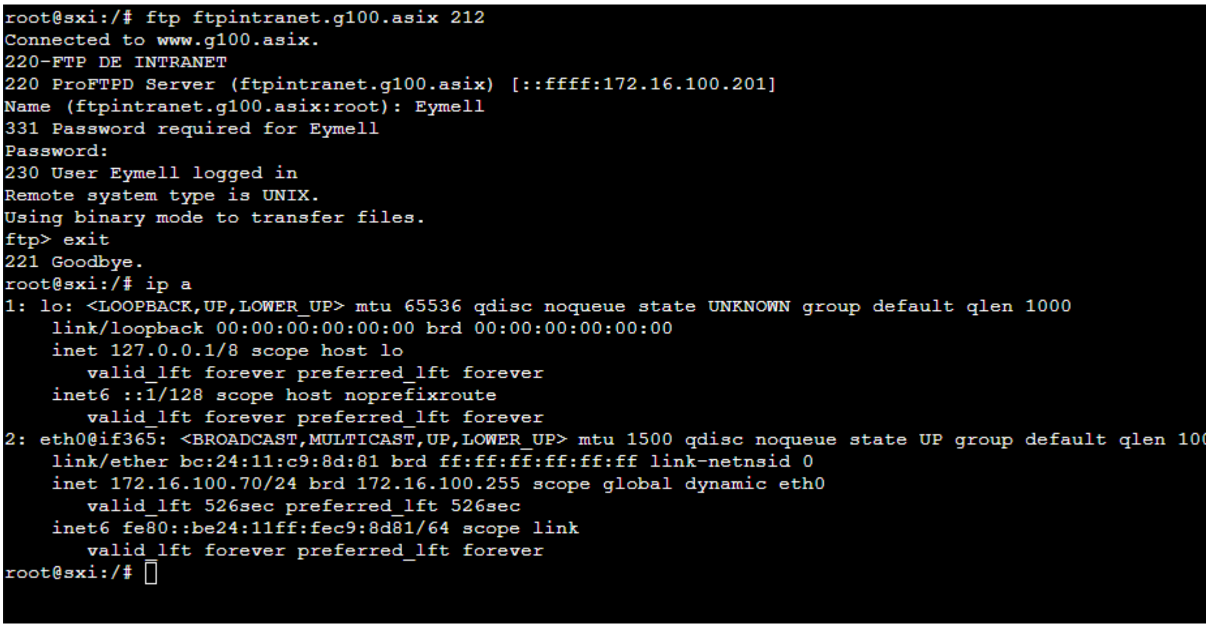
```
#Incluimos de primeras la configuracion sql
LoadModule mod_sql.c
LoadModule mod_sql_mysql.c

<VirtualHost ftpintranet.g100.asix>
  Port 212
  DisplayConnect /etc/proftpd/ftpintranet.txt
  ServerName                ftpintranet.g100.asix
  DefaultRoot             /var/www/html/intranet.g100.asix
  RequireValidShell       off

  #<Limit LOGIN>
  # Order allow,deny
        #Allow from 172.16.100.60/27
        #DenyAll
 # </Limit>
<IfModule mod_sql.c>
  SQLBackend                mysql
  SQLAuthTypes              Plaintext
  SQLAuthenticate           users
  SQLConnectInfo            FTPUSUARIOS@localhost ftpuser grupo100
  SQLUserInfo               users username password uid gid homedir shell
  SQLLogFile                /var/log/proftpd/sql.log
</IfModule>


</VirtualHost>

```

Limitamos las ips desde la 172.16.100.60 a la 172.16.100.90.



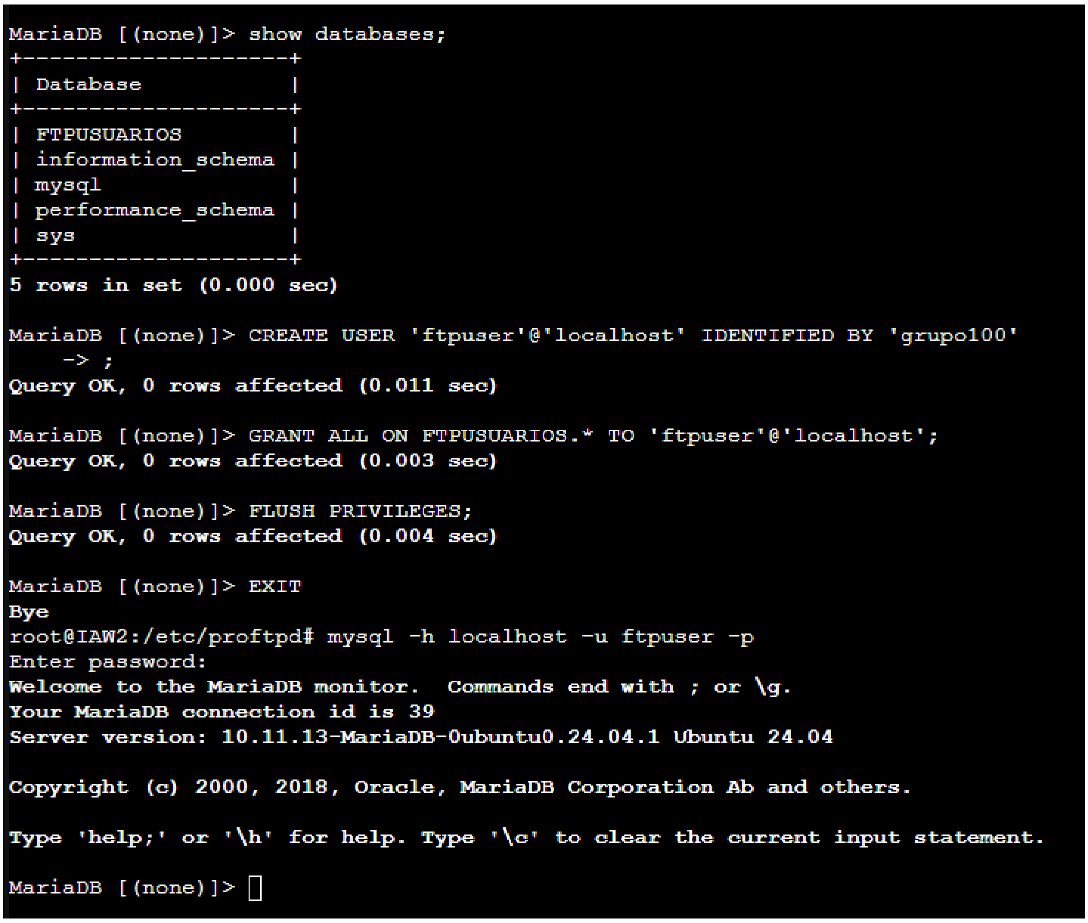
```
LoadModule mod_sql.c
LoadModule mod_sql_mysql.c

<VirtualHost ftpintranet.g100.asix>
  Port 212
  DisplayConnect /etc/proftpd/ftpintranet.txt
  ServerName              ftpintranet.g100.asix
  DefaultRoot            /var/www/html/intranet.g100.asix
  RequireValidShell      off

  <Limit LOGIN>
   Order allow,deny
        Allow from 172.16.100.60/30
        Allow from 172.16.100.64/28
        Allow from 172.16.100.80/29
        Allow from 172.16.100.88/31
        Allow from 172.16.100.90/32
        DenyAll
  </Limit>
<IfModule mod_sql.c>
  SQLBackend                mysql
  SQLAuthTypes              Plaintext
  SQLAuthenticate           users
  SQLConnectInfo            FTPUSUARIOS@localhost ftpuser grupo100
  SQLUserInfo               users username password uid gid homedir shell
  SQLLogFile                /var/log/proftpd/sql.log
</IfModule>


</VirtualHost>
```

Comprobar que los equipos dentro del rango pueden acceder al servidor ftp



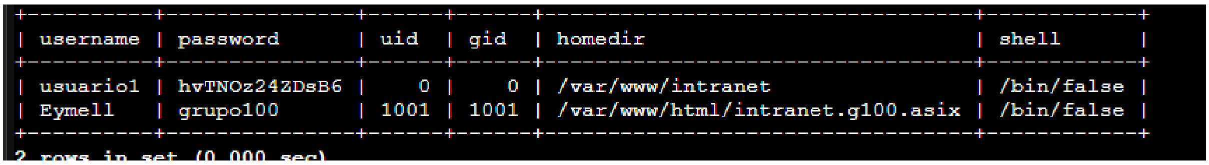
```
root@sxi:/# ftp ftpintranet.g100.asix 212
Connected to www.g100.asix.
220-FTP DE INTRANET
220 ProFTPD Server (ftpintranet.g100.asix) [::ffff:172.16.100.201]
Name (ftpintranet.g100.asix:root): Eymell
331 Password required for Eymell
Password:
230 User Eymell logged in
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> exit
221 Goodbye.
root@sxi:/# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0@if365: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default qlen 10
    link/ether bc:24:11:c9:8d:81 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 172.16.100.70/24 brd 172.16.100.255 scope global dynamic eth0
       valid_lft 526sec preferred_lft 526sec
    inet6 fe80::be24:11ff:fec9:8d81/64 scope link
       valid_lft forever preferred_lft forever
root@sxi:/# 
```

Creación de usuario que puede acceder a la base de datos de los usuarios.



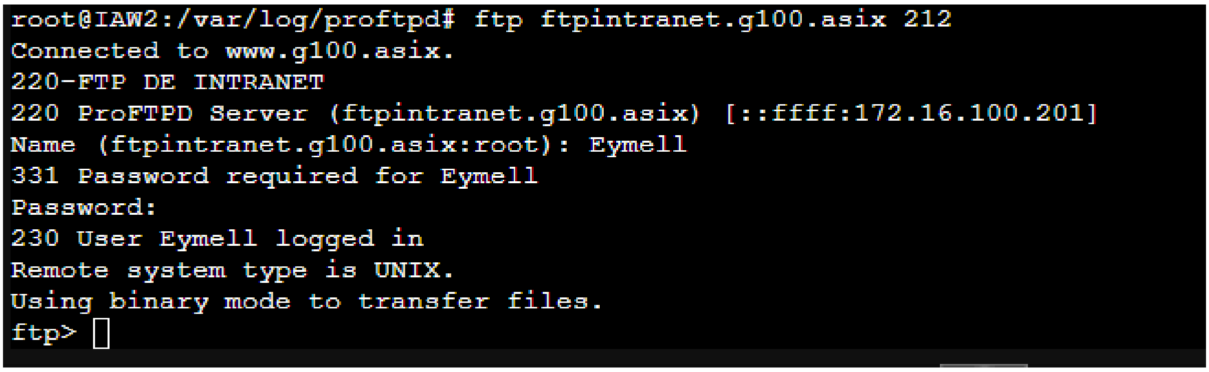
```
MariaDB [(none)]> show databases;
+--------------------+
| Database           |
+--------------------+
| FTPUSUARIOS        |
| information_schema |
| mysql              |
| performance_schema |
| sys                |
+--------------------+
5 rows in set (0.000 sec)

MariaDB [(none)]> CREATE USER 'ftpuser'@'localhost' IDENTIFIED BY 'grupo100'
    -> ;
Query OK, 0 rows affected (0.011 sec)

MariaDB [(none)]> GRANT ALL ON FTPUSUARIOS.* TO 'ftpuser'@'localhost';
Query OK, 0 rows affected (0.003 sec)

MariaDB [(none)]> FLUSH PRIVILEGES;
Query OK, 0 rows affected (0.004 sec)

MariaDB [(none)]> EXIT
Bye
root@IAW2:/etc/proftpd# mysql -h localhost -u ftpuser -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 39
Server version: 10.11.13-MariaDB-0ubuntu0.24.04.1 Ubuntu 24.04

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

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

MariaDB [(none)]> 
```

Crear tabla para almacenar los usuarios virtuales que accederán al ftpintranet.g100.asix. (Create Table users)



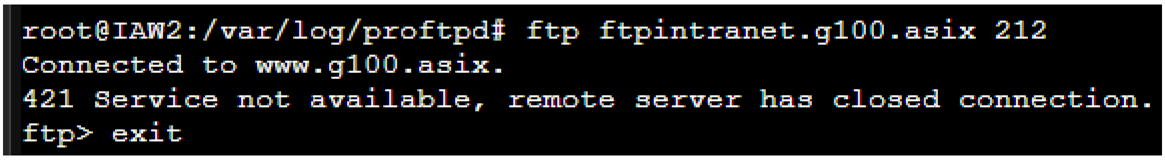
```
+----------+--------------+------+------+---------------------------------+------------+
| username | password     | uid  | gid  | homedir                         | shell      |
+----------+--------------+------+------+---------------------------------+------------+
| usuario1 | hvTNOz24ZDsB6 |    0 |    0 | /var/www/intranet               | /bin/false |
| Eymell   | grupo100     | 1001 | 1001 | /var/www/html/intranet.g100.asix | /bin/false |
+----------+--------------+------+------+---------------------------------+------------+
2 rows in set (0.000 sec)
```

Verificamos que el usuario Eymell puede entrar en el ftpintranet. g100.asix

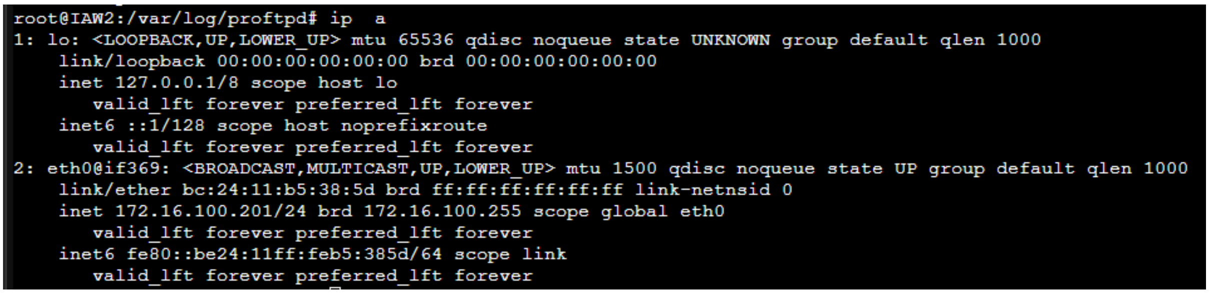


```
root@IAW2:/var/log/proftpd# ftp ftpintranet.g100.asix 212
Connected to www.g100.asix.
220-FTP DE INTRANET
220 ProFTPD Server (ftpintranet.g100.asix) [::ffff:172.16.100.201]
Name (ftpintranet.g100.asix:root): Eymell
331 Password required for Eymell
Password:
230 User Eymell logged in
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> 
```

Verificamos que desde fuera del rango no pueden entrar.



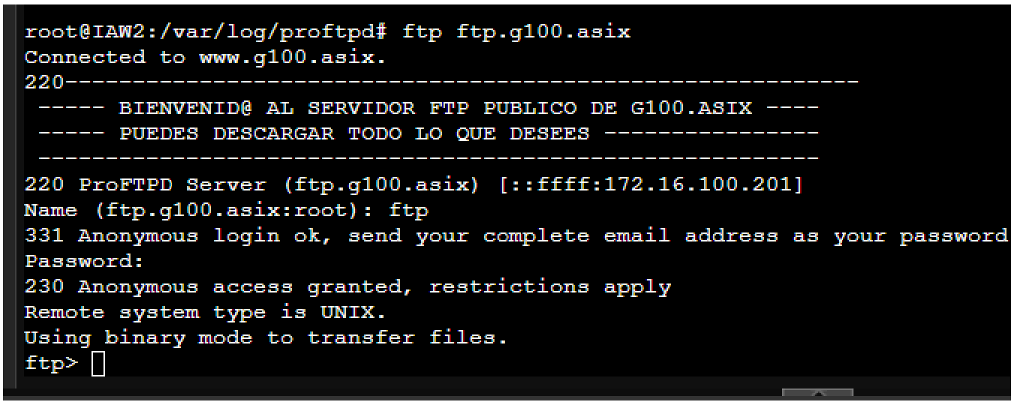
```
root@IAW2:/var/log/proftpd# ftp ftpintranet.g100.asix 212
Connected to www.g100.asix.
421 Service not available, remote server has closed connection.
ftp> exit
```



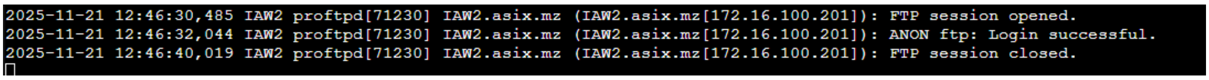
```
root@IAW2:/var/log/proftpd# ip  a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0@if369: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default qlen 1000
    link/ether bc:24:11:b5:38:5d brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 172.16.100.201/24 brd 172.16.100.255 scope global eth0
       valid_lft forever preferred_lft forever
    inet6 fe80::be24:11ff:feb5:385d/64 scope link
       valid_lft forever preferred_lft forever
```

Logs

Conexión al servidor ftp

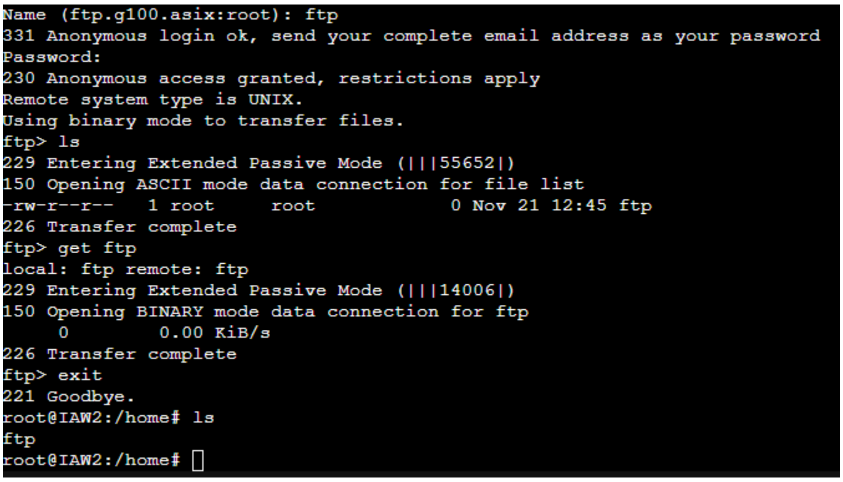


```
root@IAW2:/var/log/proftpd# ftp ftp.g100.asix
Connected to www.g100.asix.
220-----------------------------------------------------------
 ----- BIENVENID@ AL SERVIDOR FTP PUBLICO DE G100.ASIX ----
 ----- PUEDES DESCARGAR TODO LO QUE DESEES ----------------
 ---------------------------------------------------------
220 ProFTPD Server (ftp.g100.asix) [::ffff:172.16.100.201]
Name (ftp.g100.asix:root): ftp
331 Anonymous login ok, send your complete email address as your password
Password:
230 Anonymous access granted, restrictions apply
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> 
```

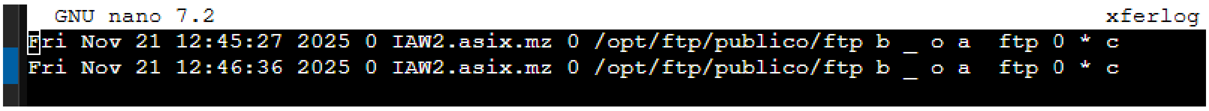


```
2025-11-21 12:46:30,485 IAW2 proftpd[71230] IAW2.asix.mz (IAW2.asix.mz[172.16.100.201]): FTP session opened.
2025-11-21 12:46:32,044 IAW2 proftpd[71230] IAW2.asix.mz (IAW2.asix.mz[172.16.100.201]): ANON ftp: Login successful.
2025-11-21 12:46:40,019 IAW2 proftpd[71230] IAW2.asix.mz (IAW2.asix.mz[172.16.100.201]): FTP session closed.
```

Descarga de archivos



```
Name (ftp.g100.asix:root): ftp
331 Anonymous login ok, send your complete email address as your password
Password:
230 Anonymous access granted, restrictions apply
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||55652|)
150 Opening ASCII mode data connection for file list
-rw-r--r--   1 root     root            0 Nov 21 12:45 ftp
226 Transfer complete
ftp> get ftp
local: ftp remote: ftp
229 Entering Extended Passive Mode (|||14006|)
150 Opening BINARY mode data connection for ftp
     0        0.00 KiB/s
226 Transfer complete
ftp> exit
221 Goodbye.
root@IAW2:/home# ls
ftp
root@IAW2:/home# 
```



```
  GNU nano 7.2                                                        xferlog
Fri Nov 21 12:45:27 2025 0 IAW2.asix.mz 0 /opt/ftp/publico/ftp b _ o a  ftp 0 * c
Fri Nov 21 12:46:36 2025 0 IAW2.asix.mz 0 /opt/ftp/publico/ftp b _ o a  ftp 0 * c
```

Estas líneas indican.

La fecha de la transferencia, el tiempo que duro la transferencia, el servidor remoto, el tamaño del archivo transferido y el nombre del archivo.

b = el tipo de transferencia b de binary.

_ = indica si hubo alguna accion especial _ significa que no hubo.

o = significa que se descargo un archivo.

a = hace referencia al modo de acceso a de anonymous.

Ftp = el nombre del servicio utilizado.

0 = el metodo de autenticacion 0 para usuarios anonimos.

* = indica la id del usuario autenticado * para usuarios anonimos.

c = indica que la trasferencia se ha completado