

Exercício 2 Redes de Computadores

Passo 1

Acessar VM RedesdeC: `ssh -i ~/.ssh/id_rsa.pem azureuser@4.206.15.40`

senha: `empty`

Senha acesso sudo: `12aWc30212345`

Comandos para verificar o exercício 2:

- **Proxy HTTP (Squid):**

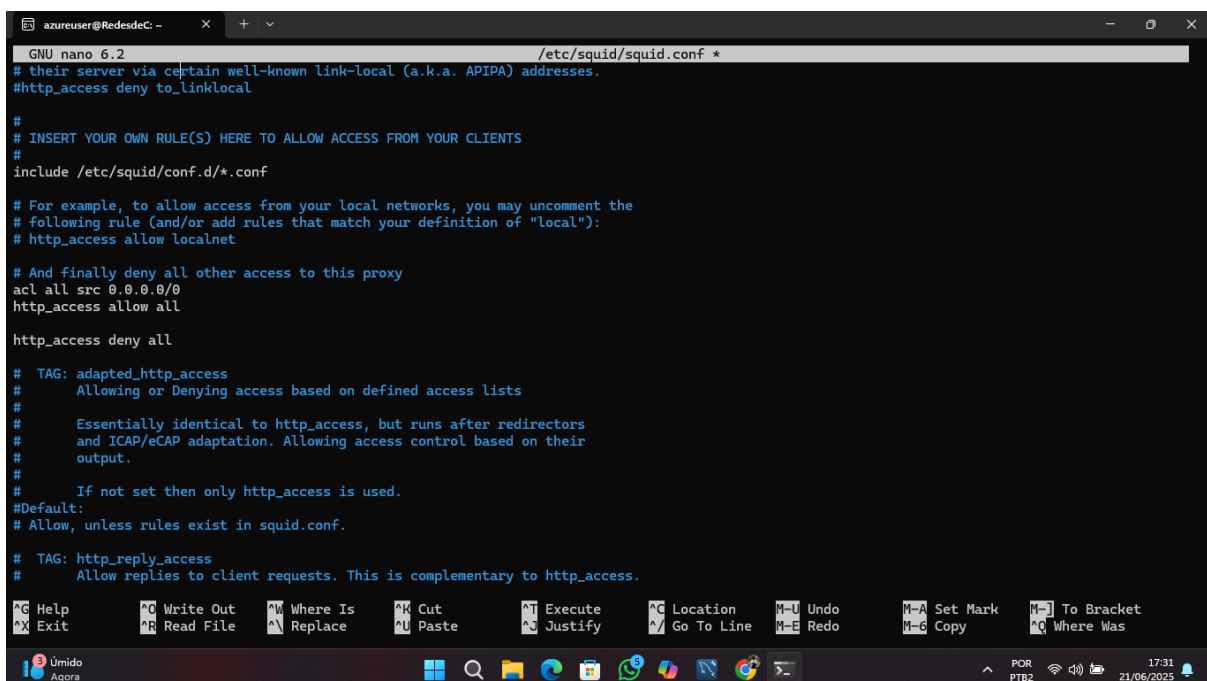
Verificar status: `sudo systemctl status squid`

Reiniciar: `sudo systemctl restart squid`

Verificar logs: `sudo tail -f /var/log/squid/access.log`

Editar config: `sudo nano /etc/squid/squid.conf`

Configurações do squid para permitir o acesso de qualquer ip:



```
GNU nano 6.2 /etc/squid/squid.conf *
# their server via certain well-known link-local (a.k.a. APIPA) addresses.
#http_access deny to_linklocal

#
# INSERT YOUR OWN RULE(S) HERE TO ALLOW ACCESS FROM YOUR CLIENTS
#
include /etc/squid/conf.d/*.conf

# For example, to allow access from your local networks, you may uncomment the
# following rule (and/or add rules that match your definition of "local"):
# http_access allow localnet

# And finally deny all other access to this proxy
acl all src 0.0.0.0/0
http_access allow all

http_access deny all

# TAG: adapted_http_access
#     Allowing or Denying access based on defined access lists
#
#     Essentially identical to http_access, but runs after redirectors
#     and ICAP/eCAP adaptation. Allowing access control based on their
#     output.
#
# If not set then only http_access is used.
#Default:
# Allow, unless rules exist in squid.conf.

# TAG: http_reply_access
#     Allow replies to client requests. This is complementary to http_access.
```

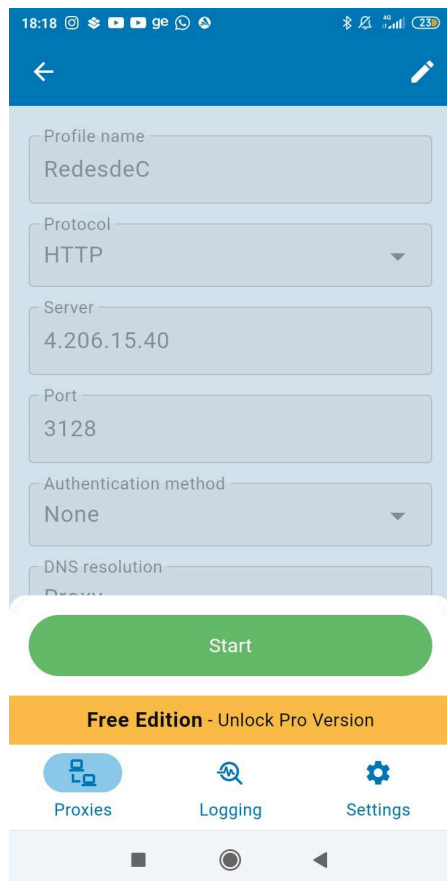
OBS: `ctrl+w` para procurar algo específico, `ctrl+o + enter` para salvar `ctrl+x` para sair (se fizer alguma modificação usar o comando para reiniciar o squid e ver os status se não há algo errado).

Passo 2

Definir o proxy para uma vpn local no meu celular com dados móveis.

Ligar o 4G e pesquisar no navegador os sites bloqueados e não bloqueados.

- Como a operadora controla os dados móveis, não é permitido que o usuário modifique essa rota.



Sites bloqueados:

facebook.com

tiktok.com

instagram.com

Ver a lista de sites bloqueados: `cat`

`/etc/squid/bloqueio.txt`

Ver onde o arquivo existe: `ls -l`

`/etc/squid/bloqueio.txt`

Exercício 3 Redes de Computadores

Passo 1

Comandos para verificar o exercício 3:

- **Servidor FTP (vsftpd):**

Verificar status: `sudo systemctl status vsftpd`

Reiniciar: `sudo systemctl restart vsftpd`

Acessar o diretório de upload: `sudo ls -l /home/userftp/ftp`
(usando sudo porque o meu usuário SSH não tem acesso direto).

Editar config: `sudo nano /etc/vsftpd.conf`

Passo 2

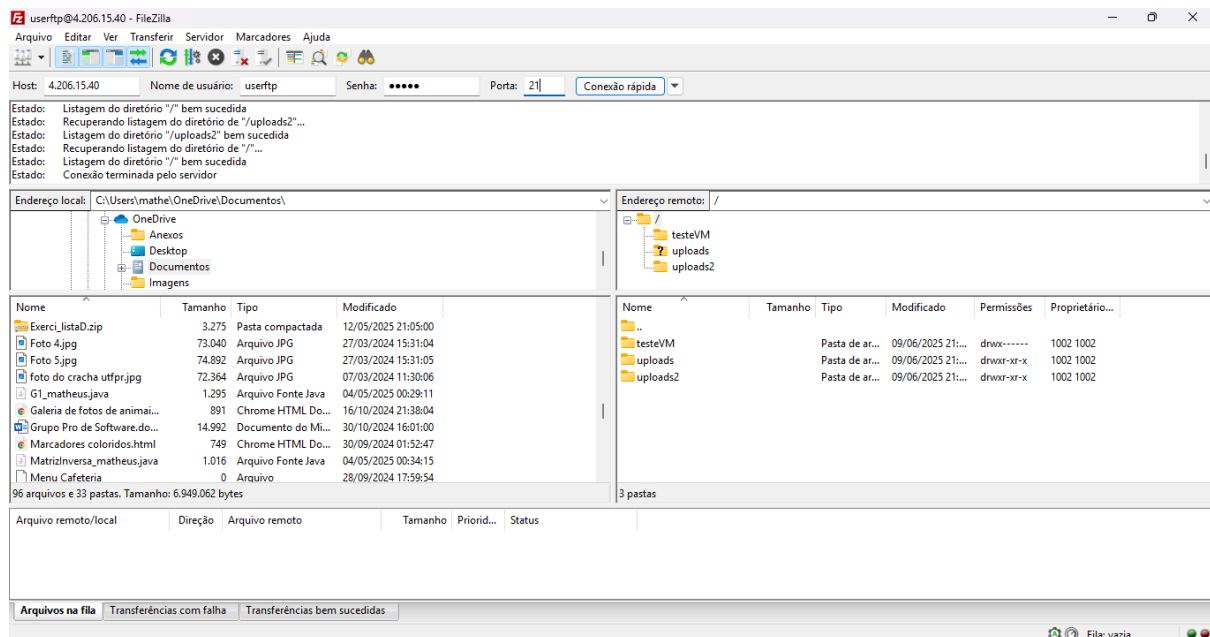
Acessar o usuário ftp no FileZilla

Host: `ftp://4.206.15.40`

Username: `userftp`

Senha: `empty`

Porta: `21`



OBS: Fazer Upload de um arquivo e Download e verificar no diretório, excluir e verificar no diretório novamente.

Exercício 5 Redes de Computadores

Passo 1

Ligar a VPN VNetHomeOffice

Verificar a conexão básica da VM com endereço privado

Comando no bash: `ping 10.0.0.4`

Acessar a VM com o comando: `ssh -i ~/RedesAC2_key.pem azureuser@10.0.0.4`

OBS: Acessar a VM com a VPN desativada não dá certo pois ela é a “porta” que permite a conexão com a rede privada necessária para acessar a VM

Extra:

instalei um servidor web Apache que só pode ser acessado por conta de uma regra de segurança que permite o tráfego com a VPN ligada.

Abrir o arquivo do site: `sudo nano /etc/apache2/ports.conf`

Ver os status: `sudo systemctl status apache2`

Link: <http://10.0.0.4:8080>

Exercício 6 Redes de Computadores

Passo 1

Acessar a VM RedesAC2

Comando: `ssh azureuser@40.82.176.244`

Senha: 12aWc30212345

Verificar os serviços: `sudo systemctl status asterisk`
`sudo systemctl status apache2`

link FreePBX: <http://40.82.176.244/admin/config.php?display=extensions>

Login: azureuser

Senha: 12aWc30212345

The screenshot shows the FreePBX Administration web interface in a browser. The address bar indicates the URL `40.82.176.244/admin/config.php?display=extensions&tech_hardware=pjsip_generic`. The interface has a top navigation bar with tabs: Admin, Applications, Connectivity, Dashboard, Reports, and Settings. The main content area is titled 'Add PJSIP Extension 101' and includes sub-tabs for General, Voicemail, Advanced, and Pin Sets. The 'General' tab is active, showing a form to add a new extension. The form includes a note: 'This device uses PJSIP technology listening on Port 5060 (UDP)'. The fields are filled with: User Extension: 101, Display Name: User1, Outbound CID: (empty), Emergency CID: (empty), and Secret: PasswordUs3r1@nkn9. A password strength indicator shows 'Strong'. At the bottom right of the form are 'Submit' and 'Reset' buttons. The footer of the interface displays the FreePBX logo, a copyright notice for Sangoma Technologies Inc. (FreePBX 17.0.19.21), and the Sangoma logo. The browser's status bar at the very bottom shows a temperature of 18°C, weather 'Nublado', and system icons for network, volume, and time (23:08 on 21/06/2025).

Senha User1: PasswordUs3r1@nkn9

FreePBX Administration

Inseguro 40.82.176.244/admin/config.php?display=extensions&tech_hardware=pjsip_generic

Admin Applications Connectivity Dashboard Reports Settings Apply Config

Add PJSIP Extension 102

General Voicemail Advanced Pin Sets

— Add Extension

This device uses PJSIP technology listening on Port 5060 (UDP)

User Extension 102

Display Name User2

Outbound CID

Emergency CID

Secret PasswordUs3r2@nkn9

Strong

Submit Reset

freePBX FreePBX is a registered trademark of Sangoma Technologies Inc. FreePBX 17.0.19.21 is licensed under the GPL Copyright© 2007-2025 Sangoma

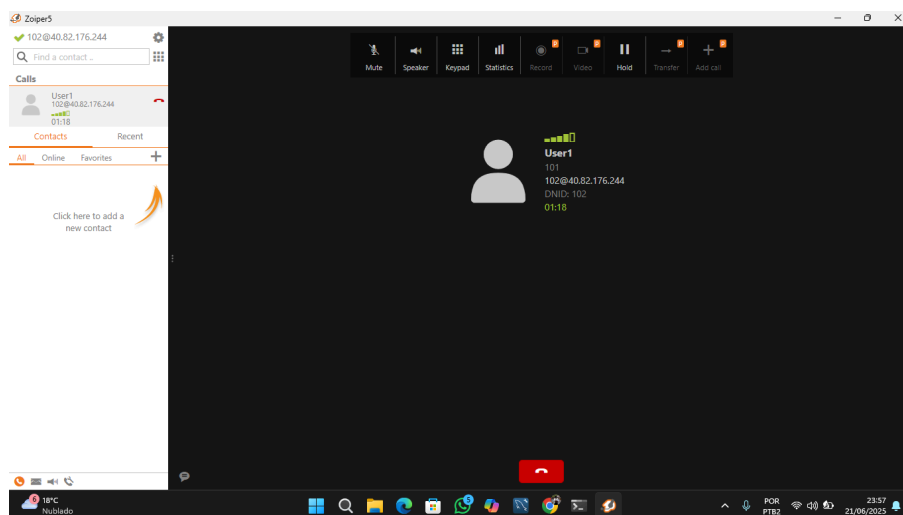
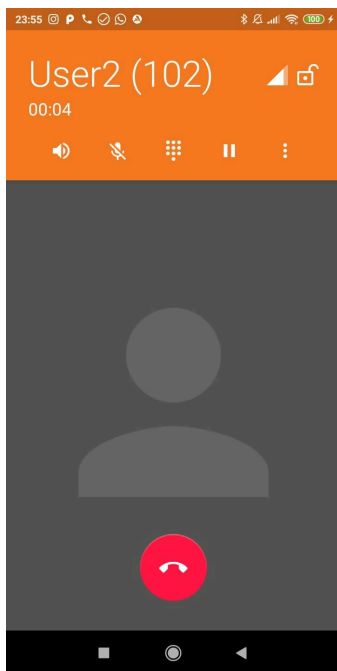
17°C Nublado

POR PTB2 23:11 21/06/2025

Senha User2: PasswordUs3r2@nkn9

Passo 2

Usar o Zoiper do celular(User1) para chamar o 102(User102) do notebook.



OBS: Quando for fazer a chamada usar o comando (sudo asterisk -rvvv) para mostrar ao vivo o procedimento da chamada