

ASR – atividade 5

Instalando o UFW

```
root@localhost:~# apt install ufw
Reading package lists... Done
Building dependency tree
Reading state information... Done
ufw is already the newest version (0.36-6).
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
```

Configurando e conectando

```
root@localhost:~# ufw enable
Command may disrupt existing ssh connections. Proceed with operation (y|n)? y
Firewall is active and enabled on system startup
```

```
root@localhost:~# ufw default deny incoming
Default incoming policy changed to 'deny'
(be sure to update your rules accordingly)
root@localhost:~# ufw default allow outgoing
Default outgoing policy changed to 'allow'
(be sure to update your rules accordingly)
```

```
root@localhost:~# ufw allow ssh
Rule added
```

O comando `ufw allow ssh` permite a conexão com o servidor

```
root@localhost:~# ssh root@23.92.26.196
root@23.92.26.196's password: █
```

Você deve inserir a senha do server, se ela estiver correta você irá se conectar (evidenciado pelo texto de “Welcome to the server!” na última linha da imagem abaixo)

```

* Documentation: https://help.ubuntu.com
* Management:   https://landscape.canonical.com
* Support:       https://ubuntu.com/advantage

System information as of Sat 08 Apr 2024 11:56:43 PM UTC

System load:          0.17
Usage of /:           8.9% of 24.06GB
Memory usage:         21%
Swap usage:           0%
Processes:            118
Users logged in:      1
IPv4 address for eth0: 23.92.26.196
IPv6 address for eth0: 2600:3c01::f03c:92ff:fe36:12f6

0 updates can be installed immediately.
0 of these updates are security updates.

*** System restart required ***
Last login: Sat Apr 08 23:53:12 2024 from 192.53.124.115
Welcome to the server!
root@localhost:~#

```

Com o comando abaixo, é possível bloquear todos os IPs, exceto o que foi dado permissão

```

root@localhost:~# ufw allow from 192.53.124.115 to any port 22
Rule added

```

Ao tentar entrar por um IP não permitido, não haverá resposta

```

root@localhost:~# % ssh root@23.92.26.196

```

Também é possível negar conexões usando o comando:

```

root@localhost:~# ufw deny http
Rule added

```

Colocando from + IP para ser bloqueado no fim do comando, ele não será mais capaz de se conectar. Ao tentar fazer o mesmo, não haverá resposta.

```

root@localhost:~# ssh root@23.92.26.196

```

Caso necessário, também é possível desabilitar o UFW

```

root@localhost:~# ufw disable
Firewall stopped and disabled on system startup

```