

UFW

1-Checando status do firewall

```
Ubuntu - VMware Workstation 17 Player (Non-commercial use only)
Player ▾ | [Icons]

root@ubuntu:~# ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.149.129 netmask 255.255.255.0 broadcast 192.168.149.255
    inet6 fe80::20c:29ff:fe16:f88c prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:16:f8:8c txqueuelen 1000 (Ethernet)
    RX packets 43448 bytes 65435119 (65.4 MB)
    RX errors 168 dropped 168 overruns 0 frame 0
    TX packets 12025 bytes 661451 (661.4 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
    device interrupt 19 base 0x2000

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 112 bytes 9100 (9.1 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 112 bytes 9100 (9.1 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

root@ubuntu:~# sudo ufw status
Status: inactive
root@ubuntu:~# hostname
ubuntu
root@ubuntu:~#
```

2-Habilitando o fw e permitindo ssh

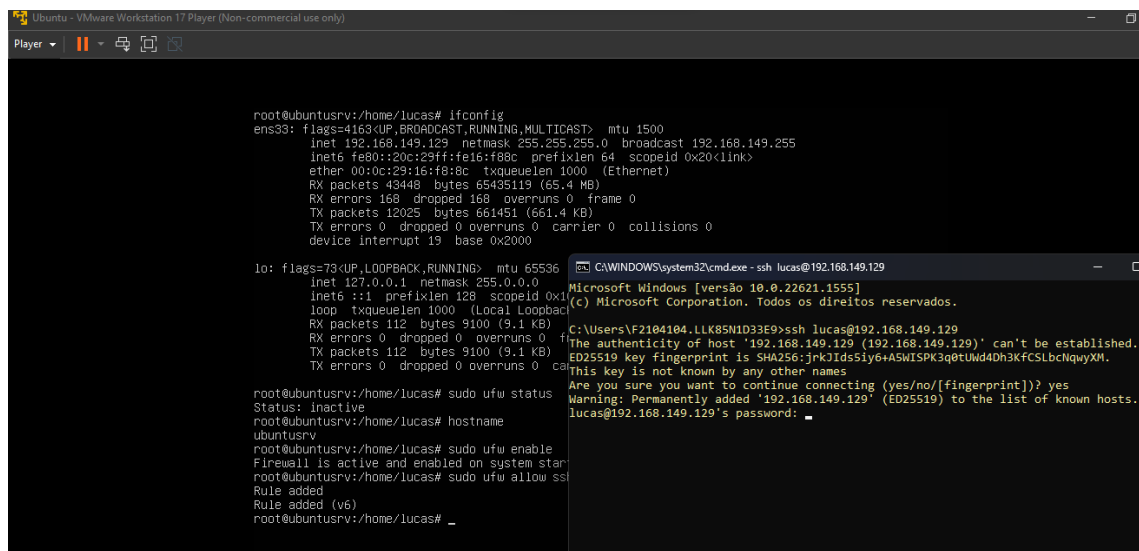
```
Ubuntu - VMware Workstation 17 Player (Non-commercial use only)
Player ▾ | [Icons]

root@ubuntu:~# ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.149.129 netmask 255.255.255.0 broadcast 192.168.149.255
    inet6 fe80::20c:29ff:fe16:f88c prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:16:f8:8c txqueuelen 1000 (Ethernet)
    RX packets 43448 bytes 65435119 (65.4 MB)
    RX errors 168 dropped 168 overruns 0 frame 0
    TX packets 12025 bytes 661451 (661.4 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
    device interrupt 19 base 0x2000

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 112 bytes 9100 (9.1 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 112 bytes 9100 (9.1 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

root@ubuntu:~# sudo ufw status
Status: inactive
root@ubuntu:~# hostname
ubuntu
root@ubuntu:~# sudo ufw enable
Firewall is active and enabled on system startup
root@ubuntu:~# sudo ufw allow ssh
Rule added
Rule added (v6)
root@ubuntu:~#
```

3-Conectando via ssh



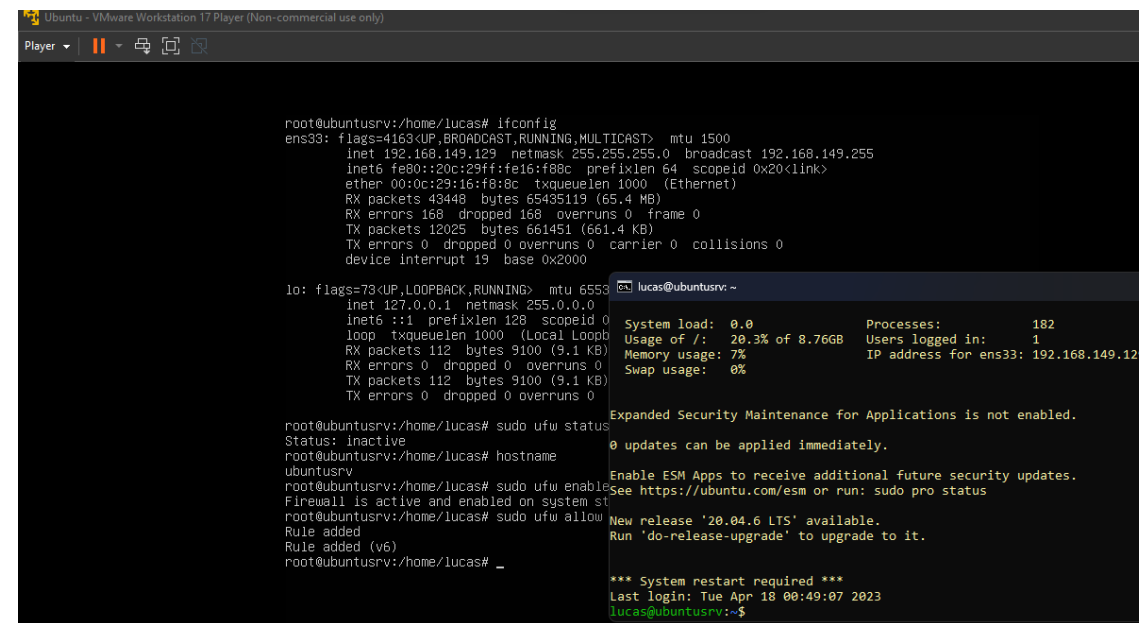
```
root@ubuntu:~# ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.149.129 netmask 255.255.255.0 broadcast 192.168.149.255
    inet6 fe80::20c:29ff:fe16:f8bc prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:16:f8:8c txqueuelen 1000 (Ethernet)
    RX packets 43448 bytes 65435119 (65.4 MB)
    RX errors 168 dropped 168 overruns 0 frame 0
    TX packets 12025 bytes 661451 (661.4 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
    device interrupt 19 base 0x2000

root@ubuntu:~# sudo ufw status
Status: inactive
root@ubuntu:~# hostname
ubuntu
root@ubuntu:~# sudo ufw enable
Firewall is active and enabled on system start
root@ubuntu:~# sudo ufw allow ssh
Rule added
Rule added (v6)
root@ubuntu:~#
```

```
C:\WINDOWS\system32\cmd.exe - ssh lucas@192.168.149.129
Microsoft Windows [versão 10.0.22621.1555]
(c) Microsoft Corporation. Todos os direitos reservados.

C:\Users\F2104104.LLK85N1033E9>ssh lucas@192.168.149.129
The authenticity of host '192.168.149.129 (192.168.149.129)' can't be established.
ED25519 key fingerprint is SHA256:jrk0lids5iyG+ASWISPK3q0tUWd4Dh3KfCSLbChqwyX0.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.149.129' (ED25519) to the list of known hosts.
lucas@192.168.149.129's password: _
```

4-Conexão bem-sucedida



```
root@ubuntu:~# ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.149.129 netmask 255.255.255.0 broadcast 192.168.149.255
    inet6 fe80::20c:29ff:fe16:f8bc prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:16:f8:8c txqueuelen 1000 (Ethernet)
    RX packets 43448 bytes 65435119 (65.4 MB)
    RX errors 168 dropped 168 overruns 0 frame 0
    TX packets 12025 bytes 661451 (661.4 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
    device interrupt 19 base 0x2000

root@ubuntu:~# sudo ufw status
Status: inactive
root@ubuntu:~# hostname
ubuntu
root@ubuntu:~# sudo ufw enable
Firewall is active and enabled on system start
root@ubuntu:~# sudo ufw allow ssh
Rule added
Rule added (v6)
root@ubuntu:~#
```

```
lucas@ubuntu:~$
System load: 0.0      Processes: 182
Usage of /: 20.3% of 8.76GB  Users logged in: 1
Memory usage: 7%      IP address for ens33: 192.168.149.129
Swap usage: 0%

Expanded Security Maintenance for Applications is not enabled.
0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

New release '20.04.6 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

*** System restart required ***
Last login: Tue Apr 18 00:49:07 2023
lucas@ubuntu:~$
```

5-Criação de regra negando ssh

```
root@ubuntusrv:/home/lucas# ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.149.129 netmask 255.255.255.0 broadcast 192.168.149.255
    inet6 fe80::20c:29ff:fe16:f88c prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:16:f8:8c txqueuelen 1000 (Ethernet)
    RX packets 43448 bytes 65435119 (65.4 MB)
    RX errors 168 dropped 168 overruns 0 frame 0
    TX packets 12025 bytes 661451 (661.4 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
    device interrupt 19 base 0x2000

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 112 bytes 9100 (9.1 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 112 bytes 9100 (9.1 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

root@ubuntusrv:/home/lucas# sudo ufw status
Status: inactive
root@ubuntusrv:/home/lucas# hostname
ubuntusrv
root@ubuntusrv:/home/lucas# sudo ufw enable
Firewall is active and enabled on system startup
root@ubuntusrv:/home/lucas# sudo ufw allow ssh
Rule added
Rule added (v6)
root@ubuntusrv:/home/lucas# sudo ufw deny ssh
Rule updated
Rule updated (v6)
root@ubuntusrv:/home/lucas# _
```

6-Conexão malsucedida após criação da regra de deny

```
root@ubuntusrv:/home/lucas# ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.149.129 netmask 255.255.255.0 broadcast 192.168.149.255
    inet6 fe80::20c:29ff:fe16:f88c prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:16:f8:8c txqueuelen 1000 (Ethernet)
    RX packets 43448 bytes 65435119 (65.4 MB)
    RX errors 168 dropped 168 overruns 0 frame 0
    TX packets 12025 bytes 661451 (661.4 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
    device interrupt 19 base 0x2000

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10
    loop txqueuelen 1000 (Local Loopback)
    RX packets 112 bytes 9100 (9.1 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 112 bytes 9100 (9.1 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

root@ubuntusrv:/home/lucas# sudo ufw status
Status: inactive
root@ubuntusrv:/home/lucas# hostname
ubuntusrv
root@ubuntusrv:/home/lucas# sudo ufw enable
Firewall is active and enabled on system start
root@ubuntusrv:/home/lucas# sudo ufw allow ssh
Rule added
Rule added (v6)
root@ubuntusrv:/home/lucas# sudo ufw deny ssh
Rule updated
Rule updated (v6)
root@ubuntusrv:/home/lucas# _
```

```
C:\WINDOWS\system32\cmd.exe
C:\Users\F2104104.LLK85N1D33E9>ssh lucas@192.168.149.129
ssh: connect to host 192.168.149.129 port 22: Connection timed out
C:\Users\F2104104.LLK85N1D33E9>_
```

7-Teste de ICMP bem-sucedido

```
Ubuntu - VMware Workstation 17 Player (Non-commercial use only)
Player
root@ubuntu:~# ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
    inet 192.168.149.129 netmask 255.255.255.0  broadcast 192.168.149.255
    inet6 fe80::20c:29ff:fe16:f88c prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:16:f8:8c txqueuelen 1000 (Ethernet)
    RX packets 43448 bytes 65435119 (65.4 MB)
    RX errors 168 dropped 168 overruns 0 frame 0
    TX packets 12025 bytes 661451 (661.4 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
    device interrupt 19 base 0x2000

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 112 bytes 9100 (9.1 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 112 bytes 9100 (9.1 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

root@ubuntu:~# sudo ufw status
Status: inactive
root@ubuntu:~# hostname
ubuntu
root@ubuntu:~# sudo ufw enable
Firewall is active and enabled on system start
root@ubuntu:~# sudo ufw allow ssh
Rule added
Rule added (v6)
root@ubuntu:~# sudo ufw deny ssh
Rule updated
Rule updated (v6)
root@ubuntu:~# _
```

```
C:\WINDOWS\system32\cmd.exe
C:\Users\F2104104.LLK85N1D33E9>ping 192.168.149.129

Disparando 192.168.149.129 com 32 bytes de dados:
Resposta de 192.168.149.129: bytes=32 tempo<1ms TTL=64
Resposta de 192.168.149.129: bytes=32 tempo<1ms TTL=64
Resposta de 192.168.149.129: bytes=32 tempo<1ms TTL=64
Resposta de 192.168.149.129: bytes=32 tempo<1ms TTL=64

Estatísticas do Ping para 192.168.149.129:
    Pacotes: Enviados = 4, Recebidos = 4, Perdidos = 0 (0% de perda).
    Aproximar um número redondo de vezes em milissegundos:
    Mínimo = 0ms, Máximo = 1ms, Média = 0ms
```

8-Acessar o diretório /etc/ufw/before.rules com o vim

```
Ubuntu - VMware Workstation 17 Player (Non-commercial use only)
Player
root@ubuntu:~# ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
    inet 192.168.149.129 netmask 255.255.255.0  broadcast 192.168.149.255
    inet6 fe80::20c:29ff:fe16:f88c prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:16:f8:8c txqueuelen 1000 (Ethernet)
    RX packets 43503 bytes 65441732 (65.4 MB)
    RX errors 168 dropped 168 overruns 0 frame 0
    TX packets 12074 bytes 668741 (668.7 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
    device interrupt 19 base 0x2000

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 112 bytes 9100 (9.1 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 112 bytes 9100 (9.1 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

root@ubuntu:~# vim /etc/ufw/before.rules_
```

9-No arquivo before.rules comentas as linhas “ok icmp codes for input” e “ok icmp code for forward conforme abaixo e em seguida salvar o arquivo e sair

```
Ubuntu - VMware Workstation 17 Player (Non-commercial use only)
Player ▾ | [Pause] [Full Screen] [Close]

# drop INVALID packets (logs these in loglevel medium and higher)
-A ufw-before-input -m conntrack --ctstate INVALID -j ufw-logging-deny
-A ufw-before-input -m conntrack --ctstate INVALID -j DROP

# ok icmp codes for INPUT
#-A ufw-before-input -p icmp --icmp-type destination-unreachable -j ACCEPT
#-A ufw-before-input -p icmp --icmp-type time-exceeded -j ACCEPT
#-A ufw-before-input -p icmp --icmp-type parameter-problem -j ACCEPT
#-A ufw-before-input -p icmp --icmp-type echo-request -j ACCEPT

# ok icmp code for FORWARD
#-A ufw-before-forward -p icmp --icmp-type destination-unreachable -j ACCEPT
#-A ufw-before-forward -p icmp --icmp-type time-exceeded -j ACCEPT
#-A ufw-before-forward -p icmp --icmp-type parameter-problem -j ACCEPT
#-A ufw-before-forward -p icmp --icmp-type echo-request -j ACCEPT

# allow dhcp client to work
-A ufw-before-input -p udp --sport 67 --dport 68 -j ACCEPT

#
# ufw-not-local
#
-A ufw-before-input -j ufw-not-local

# if LOCAL, RETURN
-A ufw-not-local -m addrtype --dst-type LOCAL -j RETURN

# if MULTICAST, RETURN
-A ufw-not-local -m addrtype --dst-type MULTICAST -j RETURN

# if BROADCAST, RETURN
-A ufw-not-local -m addrtype --dst-type BROADCAST -j RETURN

# all other non-local packets are dropped
-A ufw-not-local -m limit --limit 3/min --limit-burst 10 -j ufw-logging-deny
-A ufw-not-local -j DROP
:wq!
```

10- Reiniciar o serviço do UFW

```
Ubuntu - VMware Workstation 17 Player (Non-commercial use only)
Player
root@ubuntusrv:/home/lucas# ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.149.129 netmask 255.255.255.0 broadcast 192.168.149.255
    inet6 fe80::20c:29ff:fe16:f88c prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:16:f8:8c txqueuelen 1000 (Ethernet)
    RX packets 43503 bytes 65441732 (65.4 MB)
    RX errors 168 dropped 168 overruns 0 frame 0
    TX packets 12074 bytes 668741 (668.7 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
    device interrupt 19 base 0x2000

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 112 bytes 9100 (9.1 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 112 bytes 9100 (9.1 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

root@ubuntusrv:/home/lucas# sudo ufw reload
Firewall reloaded
root@ubuntusrv:/home/lucas# _
```

11- Teste de ping após bloqueio de ICMP no servidor

```
Ubuntu - VMware Workstation 17 Player (Non-commercial use only)
Player
root@ubuntusrv:/home/lucas# ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.149.129 netmask 255.255.255.0 broadcast 192.168.149.255
    inet6 fe80::20c:29ff:fe16:f88c prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:16:f8:8c txqueuelen 1000 (Ethernet)
    RX packets 43503 bytes 65441732 (65.4 MB)
    RX errors 168 dropped 168 overruns 0 frame 0
    TX packets 12074 bytes 668741 (668.7 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
    device interrupt 19 base 0x2000

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 112 bytes 9100 (9.1 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 112 bytes 9100 (9.1 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

root@ubuntusrv:/home/lucas# sudo ufw reload
Firewall reloaded
root@ubuntusrv:/home/lucas# _
```

```
C:\WINDOWS\system32\cmd.exe
C:\Users\F2104104.LLK85N1D33E9>ping 192.168.149.129
Disparando 192.168.149.129 com 32 bytes de dados:
Esgotado o tempo limite do pedido.
Esgotado o tempo limite do pedido.
Esgotado o tempo limite do pedido.
Esgotado o tempo limite do pedido.

Estatísticas do Ping para 192.168.149.129:
    Pacotes: Enviados = 4, Recebidos = 0, Perdidos = 4 (100% de perda),
C:\Users\F2104104.LLK85N1D33E9>
```

FIM