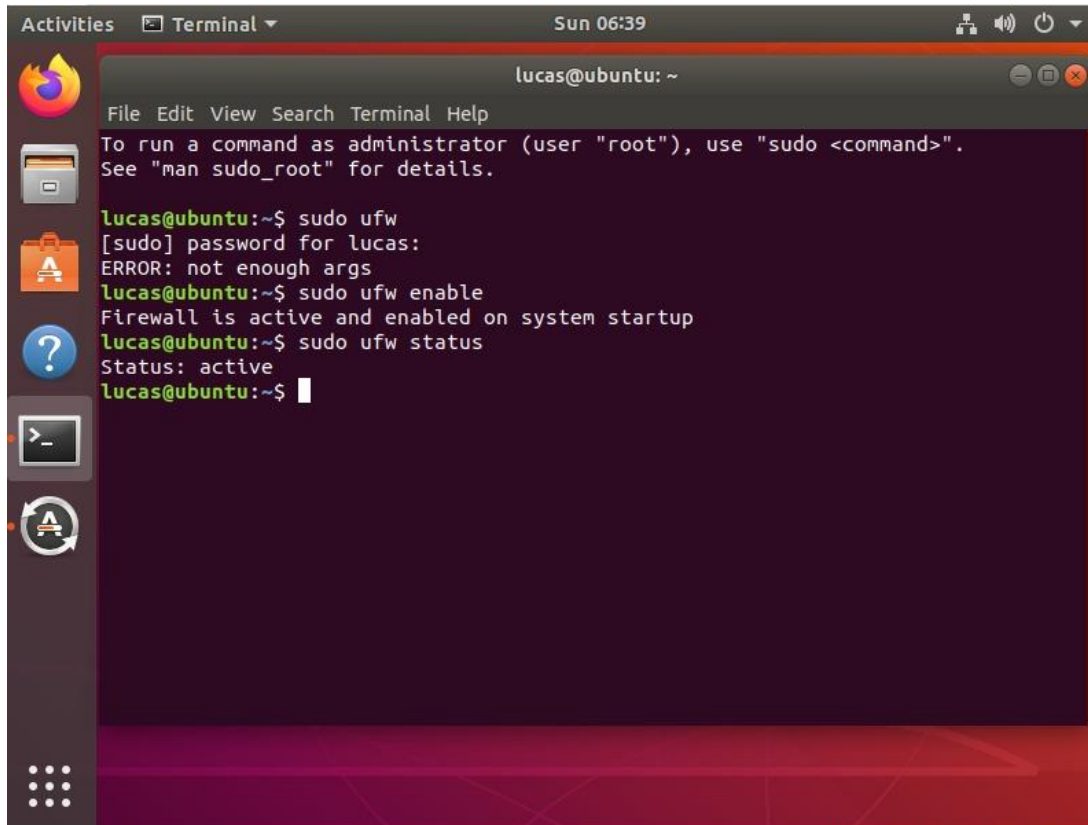


Lucas dos Santos Silva

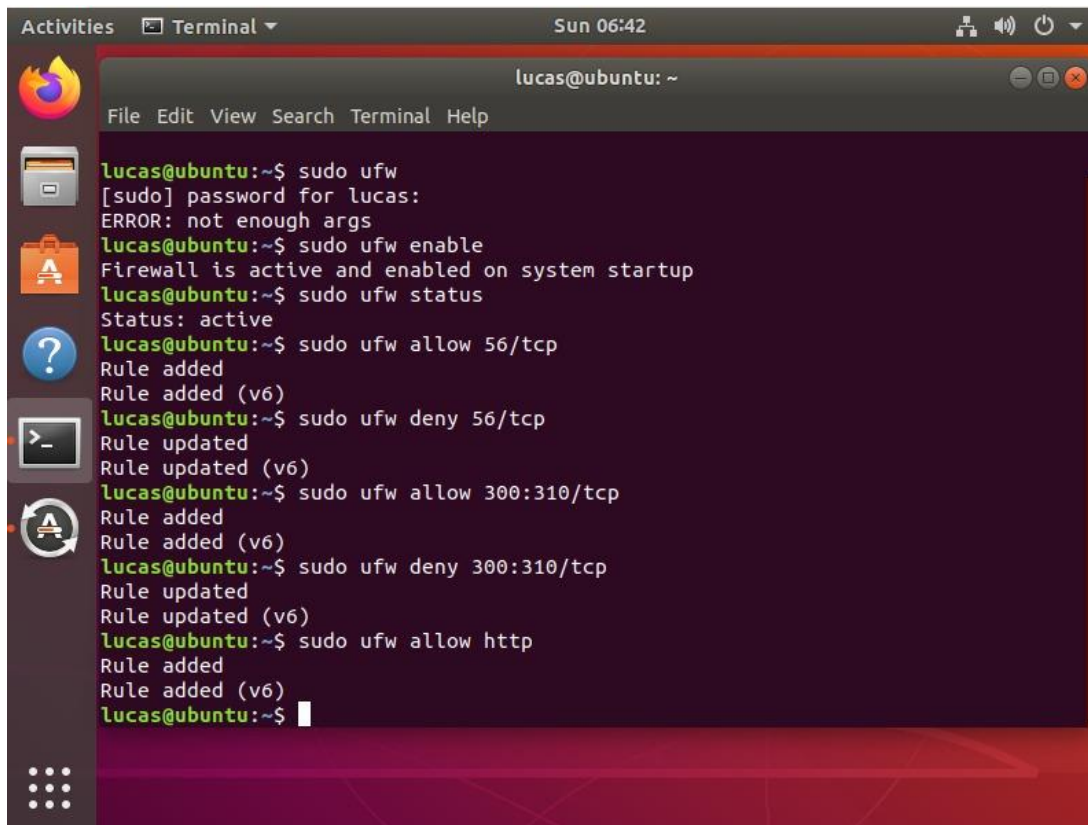
1 - habilitar o UFW



A terminal window titled 'Terminal' with a dark background and light text. The window shows the user 'lucas@ubuntu' at the prompt '~'. The user enters 'sudo ufw', followed by a password prompt and an error message 'ERROR: not enough args'. Then, the user enters 'sudo ufw enable', which outputs 'Firewall is active and enabled on system startup'. Finally, the user enters 'sudo ufw status', which outputs 'Status: active'. The terminal window has a menu bar with 'File', 'Edit', 'View', 'Search', 'Terminal', and 'Help'. The system clock at the top right shows 'Sun 06:39'.

```
lucas@ubuntu: ~  
File Edit View Search Terminal Help  
To run a command as administrator (user "root"), use "sudo <command>".  
See "man sudo_root" for details.  
  
lucas@ubuntu:~$ sudo ufw  
[sudo] password for lucas:  
ERROR: not enough args  
lucas@ubuntu:~$ sudo ufw enable  
Firewall is active and enabled on system startup  
lucas@ubuntu:~$ sudo ufw status  
Status: active  
lucas@ubuntu:~$
```

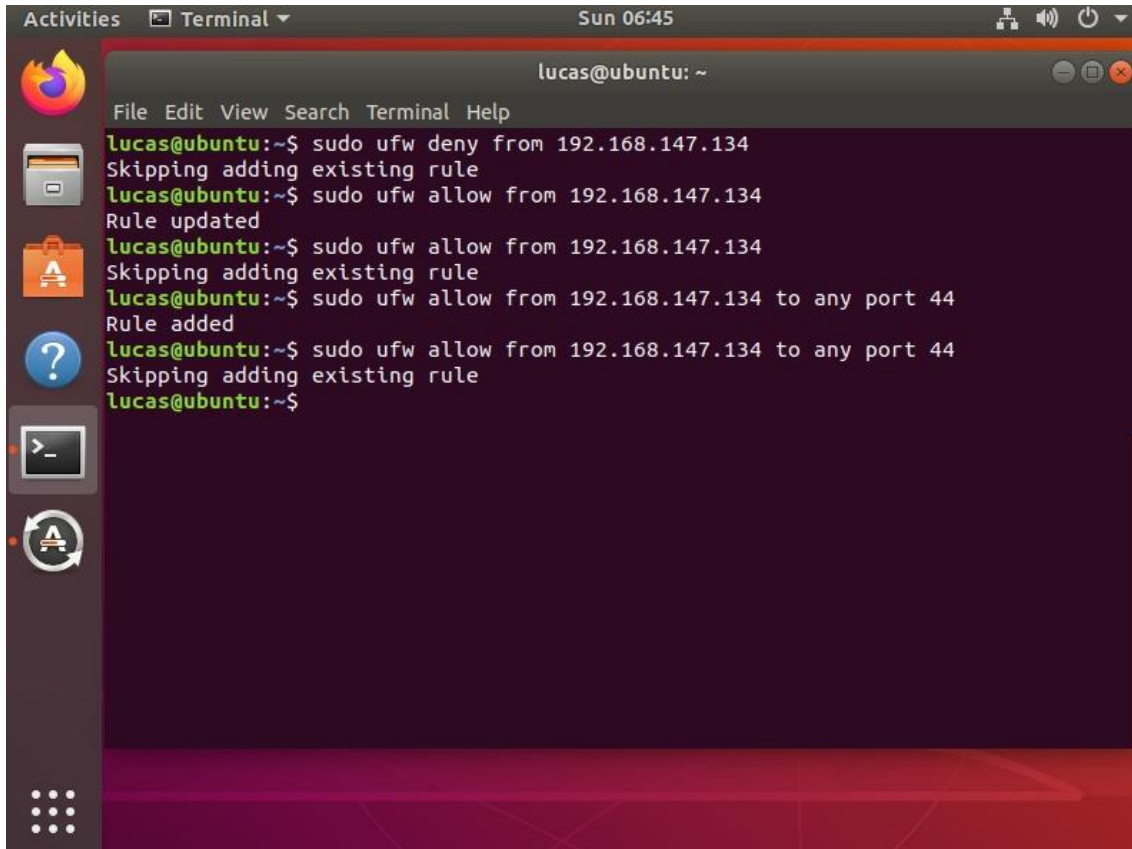
2 - Abrir e Fechar Portas com UFW



A terminal window titled 'Terminal' with a dark background and light text. The window shows the user 'lucas@ubuntu' at the prompt '~'. The user enters 'sudo ufw', followed by a password prompt and an error message 'ERROR: not enough args'. Then, the user enters 'sudo ufw enable', which outputs 'Firewall is active and enabled on system startup'. Finally, the user enters 'sudo ufw status', which outputs 'Status: active'. The user then enters 'sudo ufw allow 56/tcp', which outputs 'Rule added' and 'Rule added (v6)'. The user then enters 'sudo ufw deny 56/tcp', which outputs 'Rule updated' and 'Rule updated (v6)'. The user then enters 'sudo ufw allow 300:310/tcp', which outputs 'Rule added' and 'Rule added (v6)'. The user then enters 'sudo ufw deny 300:310/tcp', which outputs 'Rule updated' and 'Rule updated (v6)'. Finally, the user enters 'sudo ufw allow http', which outputs 'Rule added' and 'Rule added (v6)'. The terminal window has a menu bar with 'File', 'Edit', 'View', 'Search', 'Terminal', and 'Help'. The system clock at the top right shows 'Sun 06:42'.

```
lucas@ubuntu: ~  
File Edit View Search Terminal Help  
To run a command as administrator (user "root"), use "sudo <command>".  
See "man sudo_root" for details.  
  
lucas@ubuntu:~$ sudo ufw  
[sudo] password for lucas:  
ERROR: not enough args  
lucas@ubuntu:~$ sudo ufw enable  
Firewall is active and enabled on system startup  
lucas@ubuntu:~$ sudo ufw status  
Status: active  
lucas@ubuntu:~$ sudo ufw allow 56/tcp  
Rule added  
Rule added (v6)  
lucas@ubuntu:~$ sudo ufw deny 56/tcp  
Rule updated  
Rule updated (v6)  
lucas@ubuntu:~$ sudo ufw allow 300:310/tcp  
Rule added  
Rule added (v6)  
lucas@ubuntu:~$ sudo ufw deny 300:310/tcp  
Rule updated  
Rule updated (v6)  
lucas@ubuntu:~$ sudo ufw allow http  
Rule added  
Rule added (v6)  
lucas@ubuntu:~$
```

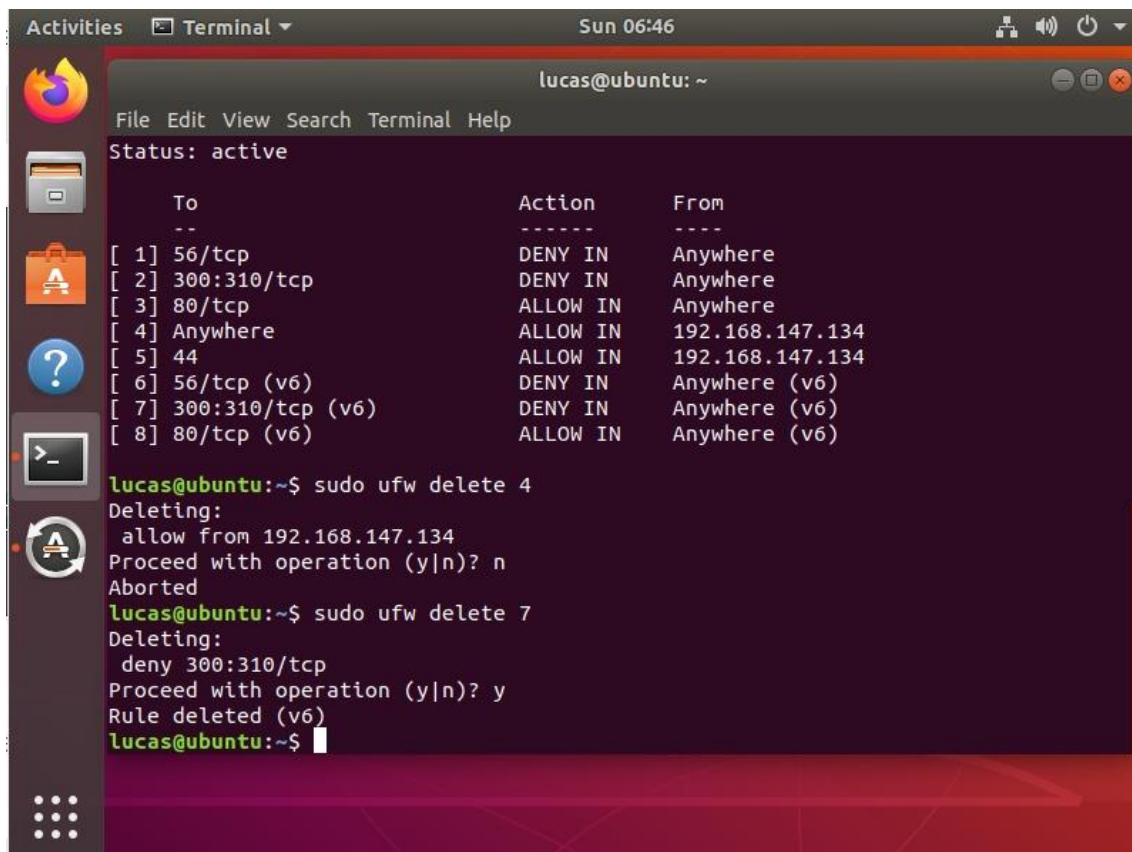
3 - Permitir ou Negar Conexões com Endereços de IP



A terminal window titled 'Terminal' with the user 'lucas@ubuntu: ~'. The window shows the following commands and output:

```
lucas@ubuntu:~$ sudo ufw deny from 192.168.147.134
Skipping adding existing rule
lucas@ubuntu:~$ sudo ufw allow from 192.168.147.134
Rule updated
lucas@ubuntu:~$ sudo ufw allow from 192.168.147.134
Skipping adding existing rule
lucas@ubuntu:~$ sudo ufw allow from 192.168.147.134 to any port 44
Rule added
lucas@ubuntu:~$ sudo ufw allow from 192.168.147.134 to any port 44
Skipping adding existing rule
lucas@ubuntu:~$
```

4 - Deletar uma Regra Específica no Firewall Ubuntu usando **sudo ufw status numbered**



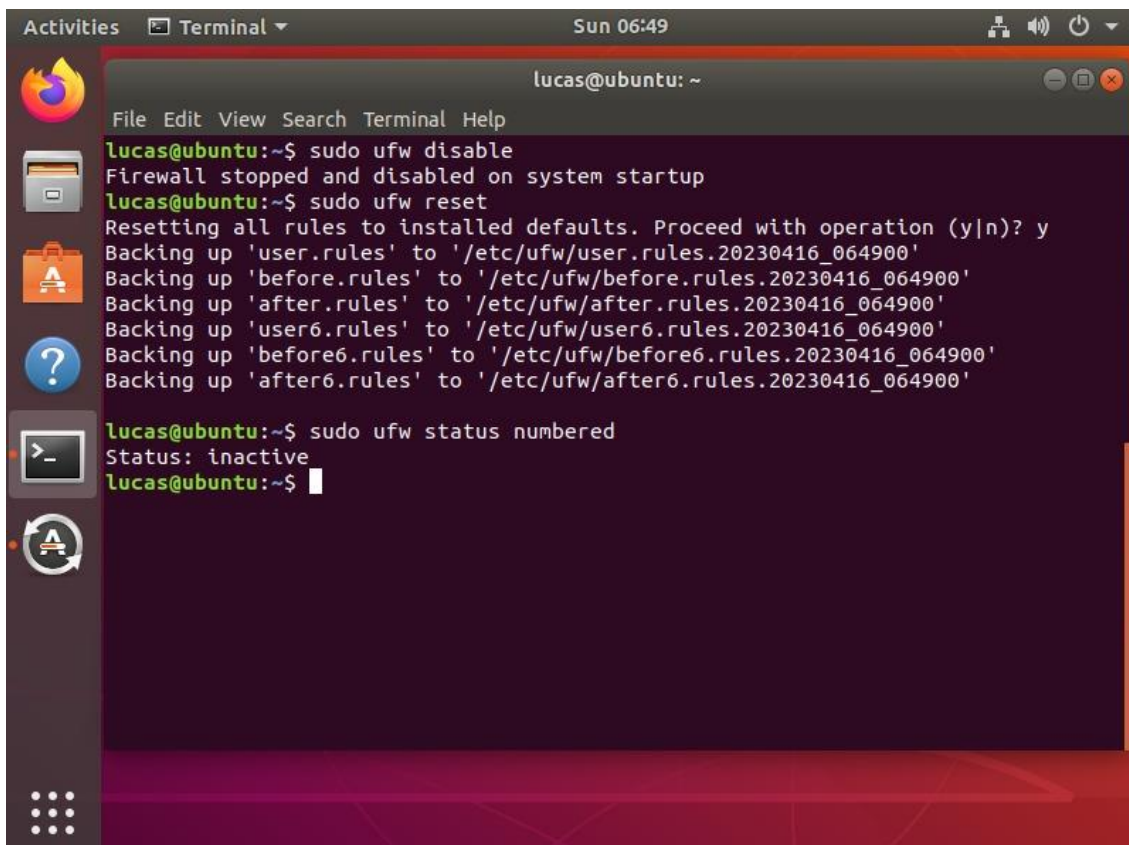
A terminal window titled 'Terminal' with the user 'lucas@ubuntu: ~'. The window shows the following commands and output:

```
lucas@ubuntu:~$ sudo ufw status numbered
Status: active

    To      Action      From
    --      -
[ 1] 56/tcp   DENY IN     Anywhere
[ 2] 300:310/tcp DENY IN     Anywhere
[ 3] 80/tcp    ALLOW IN    Anywhere
[ 4] Anywhere ALLOW IN     192.168.147.134
[ 5] 44       ALLOW IN     192.168.147.134
[ 6] 56/tcp (v6) DENY IN     Anywhere (v6)
[ 7] 300:310/tcp (v6) DENY IN     Anywhere (v6)
[ 8] 80/tcp (v6) ALLOW IN     Anywhere (v6)

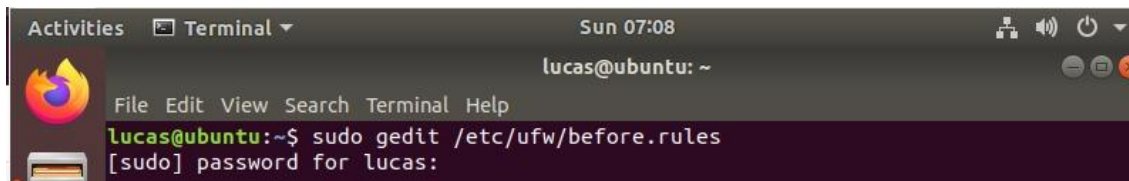
lucas@ubuntu:~$ sudo ufw delete 4
Deleting:
allow from 192.168.147.134
Proceed with operation (y|n)? n
Aborted
lucas@ubuntu:~$ sudo ufw delete 7
Deleting:
deny 300:310/tcp
Proceed with operation (y|n)? y
Rule deleted (v6)
lucas@ubuntu:~$
```

5 - Desabilitando e redefinindo o UFW

A terminal window titled 'Terminal' with the user 'lucas@ubuntu: ~'. The terminal shows the execution of 'sudo ufw disable', which outputs 'Firewall stopped and disabled on system startup'. Then, 'sudo ufw reset' is executed, which prompts for confirmation to reset rules to defaults. After confirming with 'y', it backs up several rule files and then shows the status of UFW as 'inactive' when running 'sudo ufw status numbered'.

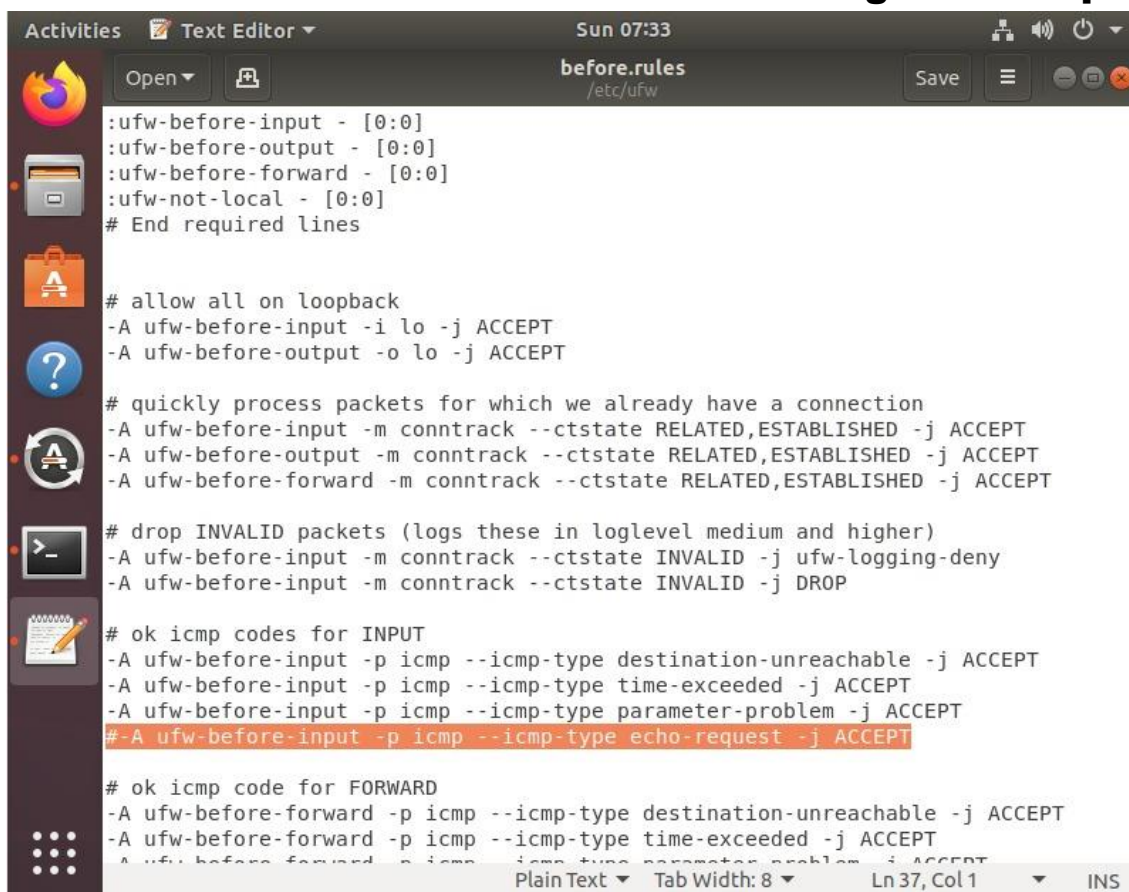
```
lucas@ubuntu: ~  
File Edit View Search Terminal Help  
lucas@ubuntu:~$ sudo ufw disable  
Firewall stopped and disabled on system startup  
lucas@ubuntu:~$ sudo ufw reset  
Resetting all rules to installed defaults. Proceed with operation (y|n)? y  
Backing up 'user.rules' to '/etc/ufw/user.rules.20230416_064900'  
Backing up 'before.rules' to '/etc/ufw/before.rules.20230416_064900'  
Backing up 'after.rules' to '/etc/ufw/after.rules.20230416_064900'  
Backing up 'user6.rules' to '/etc/ufw/user6.rules.20230416_064900'  
Backing up 'before6.rules' to '/etc/ufw/before6.rules.20230416_064900'  
Backing up 'after6.rules' to '/etc/ufw/after6.rules.20230416_064900'  
lucas@ubuntu:~$ sudo ufw status numbered  
Status: inactive  
lucas@ubuntu:~$
```

6 - comando para editar arquivo before.rules do firewall

A terminal window titled 'Terminal' with the user 'lucas@ubuntu: ~'. The terminal shows the execution of 'sudo gedit /etc/ufw/before.rules', which prompts for the user's password.

```
lucas@ubuntu: ~  
File Edit View Search Terminal Help  
lucas@ubuntu:~$ sudo gedit /etc/ufw/before.rules  
[sudo] password for lucas:
```

7 - identificando e comentando com # regra de icmp



```
:ufw-before-input - [0:0]
:ufw-before-output - [0:0]
:ufw-before-forward - [0:0]
:ufw-not-local - [0:0]
# End required lines

# allow all on loopback
-A ufw-before-input -i lo -j ACCEPT
-A ufw-before-output -o lo -j ACCEPT

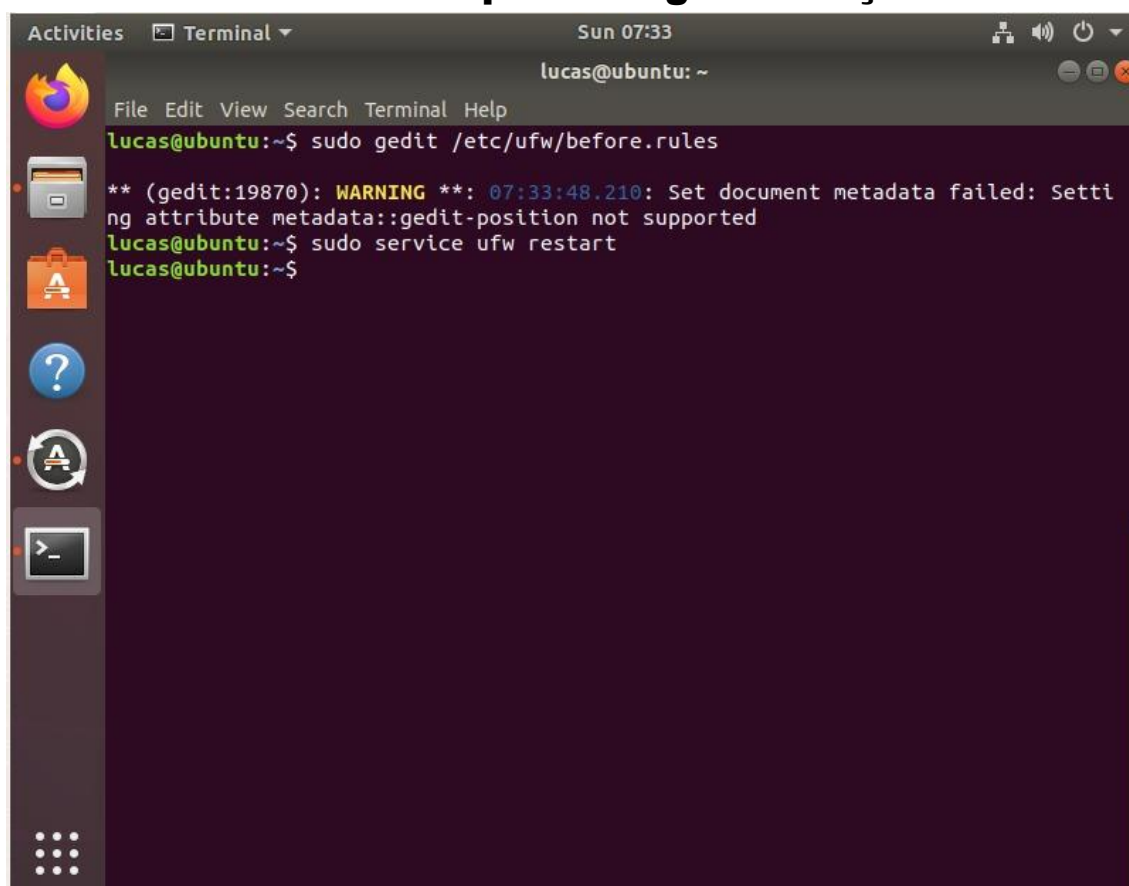
# quickly process packets for which we already have a connection
-A ufw-before-input -m conntrack --ctstate RELATED,ESTABLISHED -j ACCEPT
-A ufw-before-output -m conntrack --ctstate RELATED,ESTABLISHED -j ACCEPT
-A ufw-before-forward -m conntrack --ctstate RELATED,ESTABLISHED -j ACCEPT

# 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

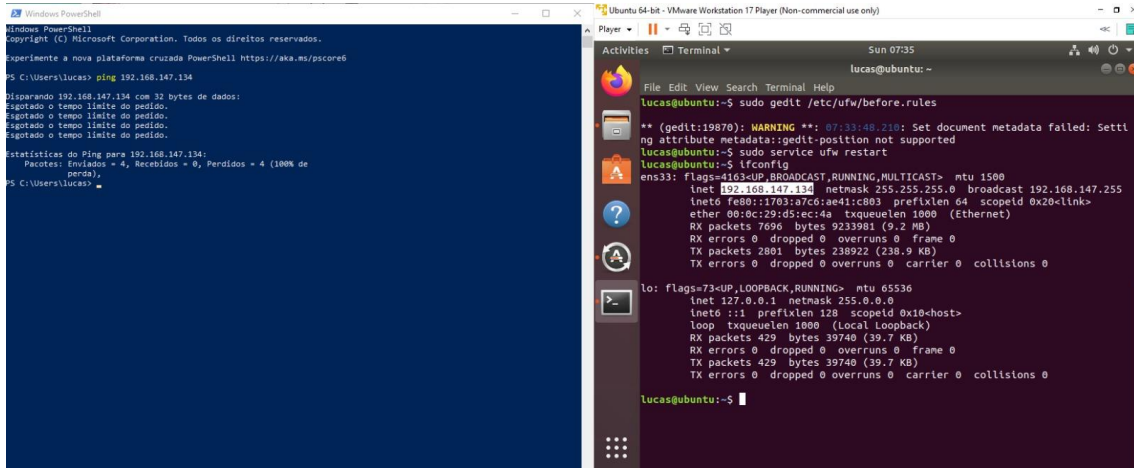
# ok icmp code for FORWARD
-A ufw-before-forward -p icmp --icmp-type destination-unreachable -j ACCEPT
-A ufw-before-forward -p icmp --icmp-type time-exceeded -j ACCEPT
-A ufw-before-forward -p icmp --icmp-type parameter-problem -j ACCEPT
```

8 - reiniciando UFW para a regra começar a valer

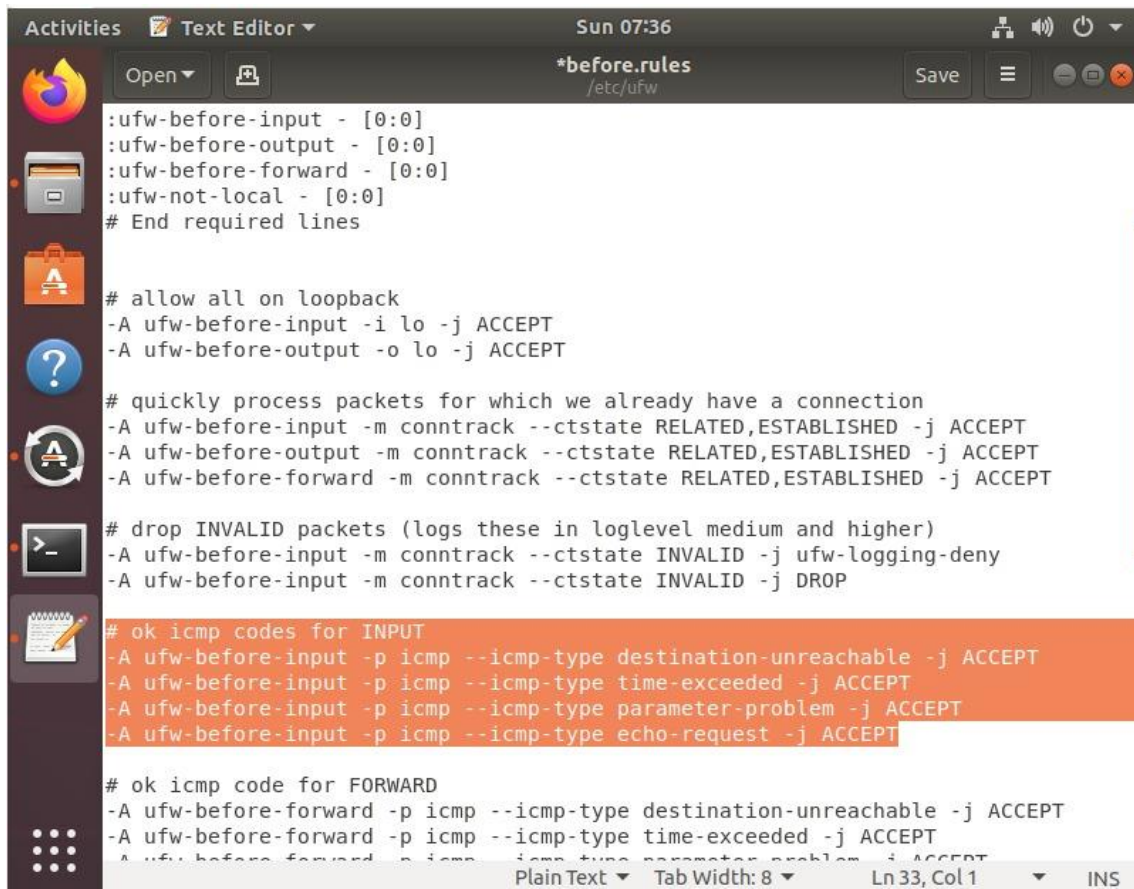


```
lucas@ubuntu: ~
File Edit View Search Terminal Help
lucas@ubuntu:~$ sudo gedit /etc/ufw/before.rules
** (gedit:19870): WARNING **: 07:33:48.210: Set document metadata failed: Setting attribute metadata::gedit-position not supported
lucas@ubuntu:~$ sudo service ufw restart
lucas@ubuntu:~$
```

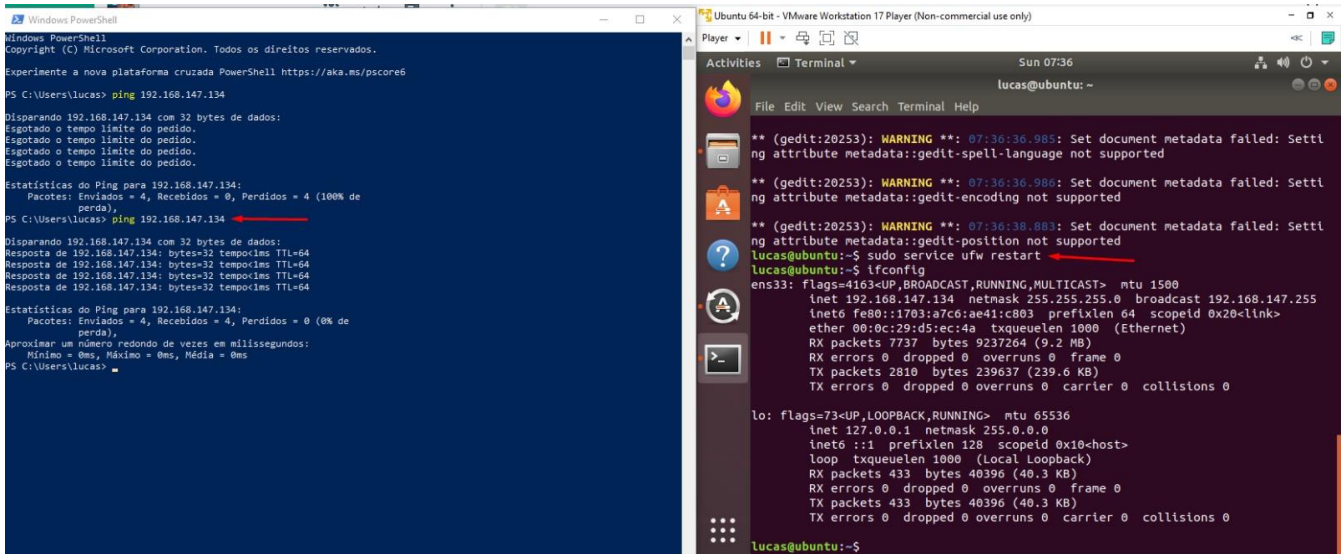

9 - testando ping bloqueado



10 - descomentando regra para ping para voltar a funcionar



11 - reiniciando ufw e testando com ping desbloqueado e funcionando



The image shows two terminal windows side-by-side. The left window is a Windows PowerShell terminal running a ping command to 192.168.147.134. The right window is an Ubuntu terminal running 'ifconfig' and 'sudo service ufw restart'. The 'ifconfig' output shows the 'ens33' interface is up and running with an IP of 192.168.147.134. The 'ufw restart' command shows several warnings about metadata but successfully restarts the service.

```
Windows PowerShell
Copyright (C) Microsoft Corporation. Todos os direitos reservados.

Experimente a nova plataforma cruzada PowerShell https://aka.ms/pscore6

PS C:\Users\lucas> ping 192.168.147.134

Disparando 192.168.147.134 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 192.168.147.134:
    Pacotes: Enviados = 4, Recebidos = 0, Perdidos = 4 (100% de perda)
PS C:\Users\lucas> ping 192.168.147.134

Disparando 192.168.147.134 com 32 bytes de dados:
Resposta de 192.168.147.134: bytes=32 tempo<ms TTL=64
Resposta de 192.168.147.134: bytes=32 tempo<ms TTL=64
Resposta de 192.168.147.134: bytes=32 tempo<ms TTL=64
Resposta de 192.168.147.134: bytes=32 tempo<ms TTL=64

Estatísticas do Ping para 192.168.147.134:
    Pacotes: Enviados = 4, Recebidos = 4, Perdidos = 0 (0% de perda)
    Aproximar um número redondo de vezes em milissegundos:
        Mínimo = 0ms, Máximo = 0ms, Média = 0ms
PS C:\Users\lucas>
```

```
lucas@ubuntu: ~
Sun 07:36

** (gedit:20253): WARNING **: 07:36:36.985: Set document metadata failed: Setting attribute metadata:gedit-spell-language not supported
** (gedit:20253): WARNING **: 07:36:36.986: Set document metadata failed: Setting attribute metadata:gedit-encoding not supported
** (gedit:20253): WARNING **: 07:36:38.883: Set document metadata failed: Setting attribute metadata:gedit-position not supported
lucas@ubuntu:~$ sudo service ufw restart
lucas@ubuntu:~$ ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
    inet 192.168.147.134  netmask 255.255.255.0  broadcast 192.168.147.255
    inet6 fe80::1703:a7c6:ae41:c803  prefixlen 64  scopeid 0x20<link>
    ether 00:0c:29:d5:ec:4a  txqueuelen 1000  (Ethernet)
    RX packets 7737  bytes 9237264 (9.2 MB)
    RX errors 0  dropped 0  overruns 0  frame 0
    TX packets 2810  bytes 239637 (239.6 KB)
    TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

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 433  bytes 40396 (40.3 KB)
    RX errors 0  dropped 0  overruns 0  frame 0
    TX packets 433  bytes 40396 (40.3 KB)
    TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lucas@ubuntu:~$
```

Comando para instalar: `sudo apt-get install ufw`