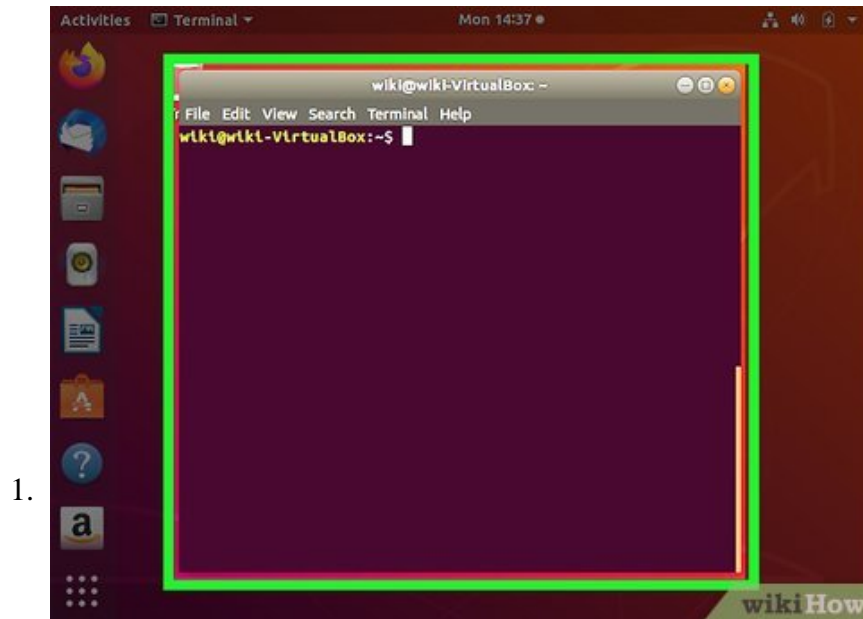


How to Open Ports in Linux Server Firewall

This wikiHow will teach you how to open ports in three popular Linux firewalls. If you're using a product like ConfigServer Firewall (CSF) or Advanced Policy Firewall (ADP), you can control open ports in the firewall's main configuration...

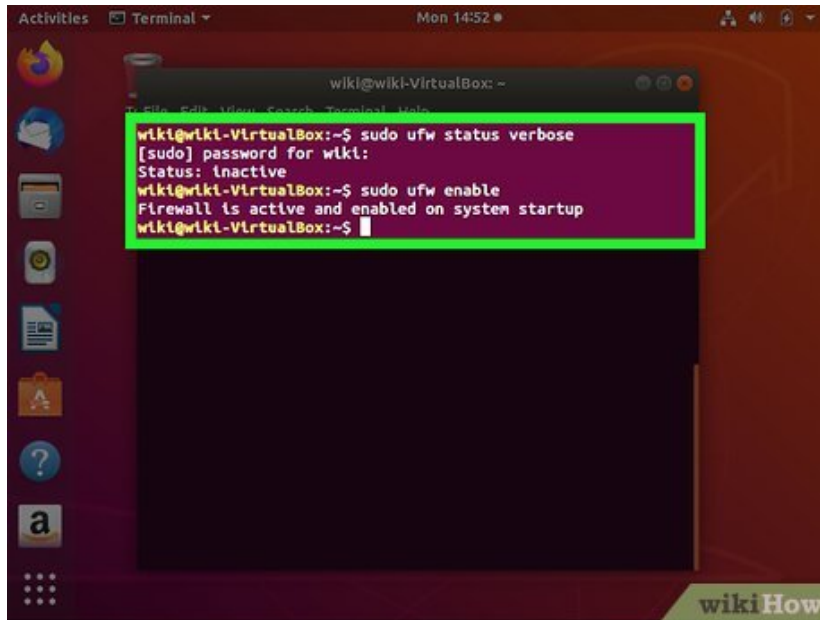
Method 1 of 3:

Using Uncomplicated Firewall for Ubuntu



Log in to your server. If you're using Ubuntu on your desktop, press `Ctrl + Alt + T` to open a terminal window.

2.

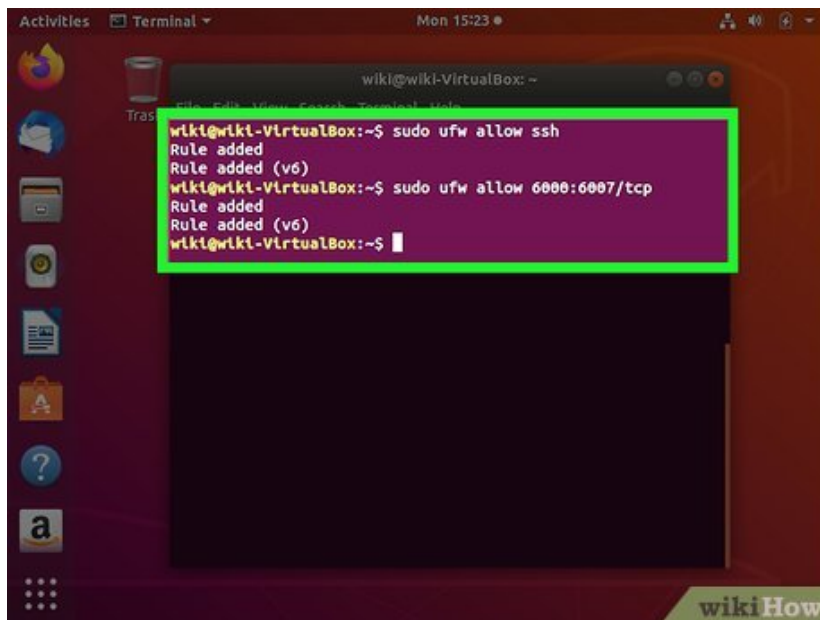
A terminal window titled 'wiki@wiki-VirtualBox: ~' is shown within a desktop environment. The terminal output is highlighted with a green box. It shows the command 'sudo ufw status verbose' being executed, followed by a password prompt '[sudo] password for wiki:'. The output indicates the firewall status is 'inactive'. Then, the command 'sudo ufw enable' is entered, resulting in the message 'Firewall is active and enabled on system startup'.

```
wiki@wiki-VirtualBox:~$ sudo ufw status verbose
[sudo] password for wiki:
Status: inactive
wiki@wiki-VirtualBox:~$ sudo ufw enable
Firewall is active and enabled on system startup
wiki@wiki-VirtualBox:~$
```

Type `sudo ufw status verbose` and press `?Enter`. If UFW is already running, you'll see a status message, as well as a list of any firewall rules (including opened ports) that already exist.^[1]

1. If you see a message that says *Status: inactive*, type `sudo ufw enable` at the prompt and press `?Enter` to start the firewall.

3.

A terminal window titled 'wiki@wiki-VirtualBox: ~' is shown within a desktop environment. The terminal output is highlighted with a green box. It shows the command 'sudo ufw allow ssh' being executed, followed by the output 'Rule added' and 'Rule added (v6)'. Then, the command 'sudo ufw allow 6000:6007/tcp' is entered, resulting in the output 'Rule added' and 'Rule added (v6)'.

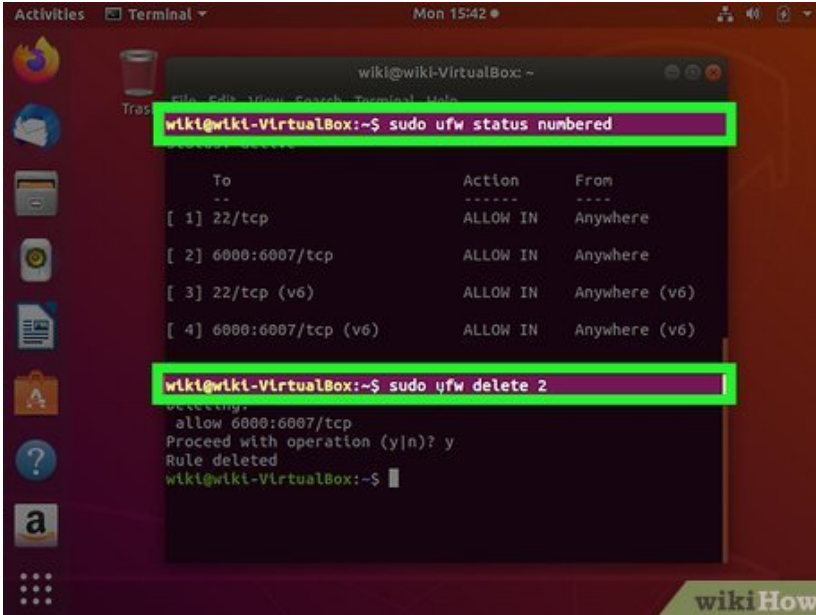
```
wiki@wiki-VirtualBox:~$ sudo ufw allow ssh
Rule added
Rule added (v6)
wiki@wiki-VirtualBox:~$ sudo ufw allow 6000:6007/tcp
Rule added
Rule added (v6)
wiki@wiki-VirtualBox:~$
```

Use `sudo ufw allow [port number]` to open a port. For example, if you want to open the SSH port (22), you'd type `kbd` and press `?Enter` to open the port. There's no need to restart the firewall, as the change will take effect immediately.^[2]

1. If the port you're opening is for a service listed in `/etc/services`, you just type the service's name instead of the port number. Example: `sudo ufw allow ssh`.
2. To open a specific range of ports, use the syntax `sudo ufw allow 6000:6007/tcp`, replacing `6000:6007` with the actual range. If the range is UDP ports, replace `tcp` with `udp`.

- To specify an IP address that can access the port, use this syntax: `sudo ufw allow from 10.0.0.1 to any port 22`. Replace `10.0.0.1` with the IP address, and `22` with the port you want to open to that address.

4.



```
wiki@wiki-VirtualBox:~$ sudo ufw status numbered

To Action From
---
[ 1] 22/tcp ALLOW IN Anywhere
[ 2] 6000:6007/tcp ALLOW IN Anywhere
[ 3] 22/tcp (v6) ALLOW IN Anywhere (v6)
[ 4] 6000:6007/tcp (v6) ALLOW IN Anywhere (v6)

wiki@wiki-VirtualBox:~$ sudo ufw delete 2
Deleting
allow 6000:6007/tcp
Proceed with operation (y/n)? y
Rule deleted
wiki@wiki-VirtualBox:~$
```

Delete firewall rules that aren't needed. Any ports that aren't specifically opened are blocked by default. If you open a port and decide you want to close it, use these steps:

- Type `sudo ufw status numbered` and press `?Enter`. This displays a list of all firewall rules, each beginning with a number to represent it in the list.
- Identify the number at the beginning of rule you want to delete. For example, let's say you want to remove the rule that opens port 22, and that rule is listed on line 2.
- Type `sudo ufw delete 2` and press `?Enter` to remove the rule at line 2.

Method 2 of 3:

Using ConfigServer Firewall

```
Ubuntu 18.04.2 LTS wiki tty1
wiki login: wiki
Password:
Last login: Mon Jan 13 08:48:53 UTC 2020 on tty1
Welcome to Ubuntu 18.04.2 LTS (GNU/Linux 4.15.0-74-generic x86_64)

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

System information as of Mon Jan 13 09:01:24 UTC 2020:

System load:  0.68           Processes:    87
Usage of /:   29.1% of 19.60GB Users logged in:  0
Memory usage: 3%           IP address for enp0s3: 10.0.2.15
Swap usage:  0%

181 packages can be updated.
31 updates are security updates.

wiki@wiki:~$ su_
```

1.

Log in to your server. If you're not logged in as the root user, you can `su` to root to adjust your configuration.

```
Ubuntu 18.04.2 LTS wiki tty1
wiki login: wiki
Password:
Last login: Mon Jan 13 13:26:26 UTC 2020 on tty1
Welcome to Ubuntu 18.04.2 LTS (GNU/Linux 4.15.0-74-generic x86_64)

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

System information as of Mon Jan 13 13:26:41 UTC 2020:

System load:  0.1           Processes:    89
Usage of /:   23.4% of 25.05GB Users logged in:  0
Memory usage: 3%           IP address for enp0s3: 10.0.2.15
Swap usage:  0%

 * Overheard at KubeCon: "microk8s.status just blew my mind".

https://microk8s.io/docs/commands#microk8s.status

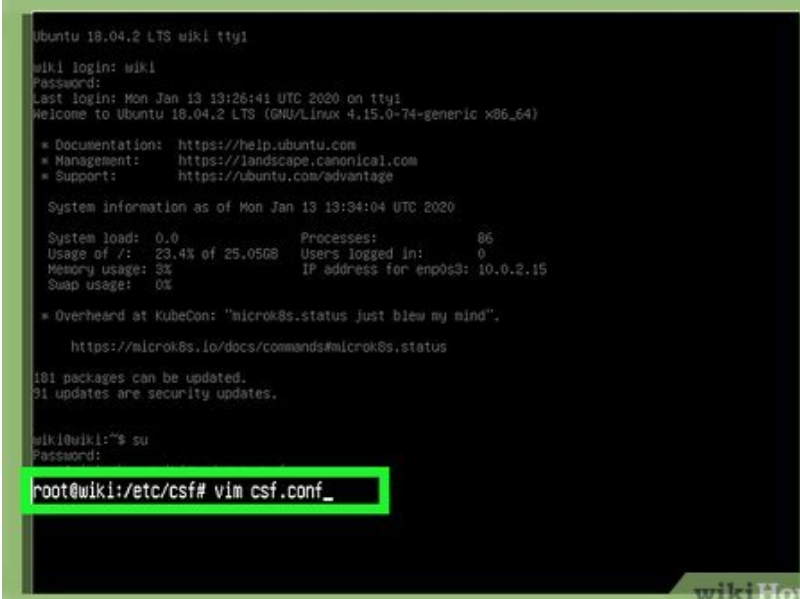
181 packages can be updated.
31 updates are security updates.

wiki@wiki:~$ su
root@wiki:/home/wiki# cd /etc/csf
```

2.

Go to directory that contains your CSF config file. The file is called `csf.conf`, and it's saved to `/etc/csf/csf.conf` by default.^[3] To do this, type `cd /etc/csf` and press `?Enter`.

3.



```
Ubuntu 18.04.2 LTS wiki tty1
wiki login: wiki
Password:
Last login: Mon Jan 13 13:26:41 UTC 2020 on tty1
Welcome to Ubuntu 18.04.2 LTS (GNU/Linux 4.15.0-74-generic x86_64)

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

System information as of Mon Jan 13 13:34:04 UTC 2020

System load:  0.0          Processes:      86
Usage of /:   23.4% of 25.05GB Users logged in:  0
Memory usage: 3%          IP address for enp0s3: 10.0.2.15
Swap usage:   0%

 * Overheard at KubeCon: "microk8s.status just blew my mind".
   https://microk8s.io/docs/commands#microk8s.status

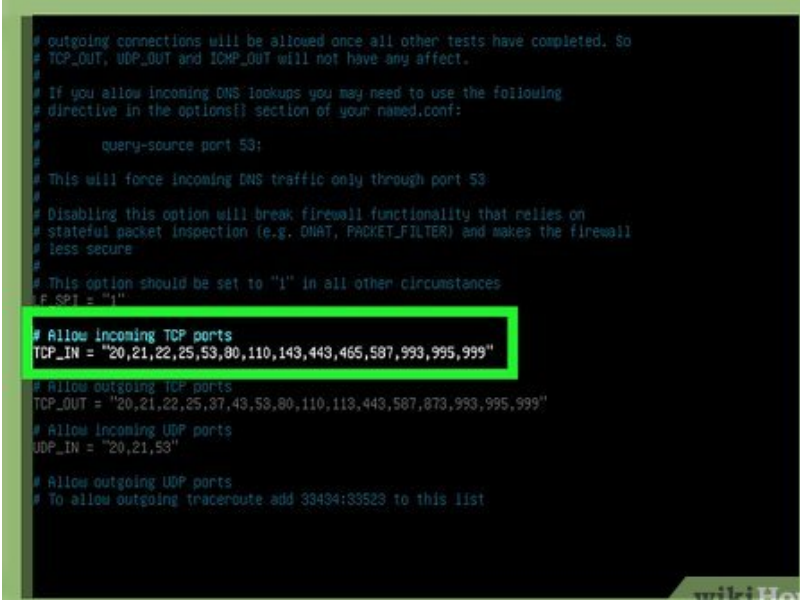
181 packages can be updated.
31 updates are security updates.

wiki@wiki:~$ su
Password:
root@wiki:/etc/csf# vim csf.conf_
```

Open `csf.conf` in a text editor. You can use any text editor you wish, such as vim or nano.

1. To open `csf.conf` in vim, type `vim csf.config` and press `?Enter`.

4.



```
# outgoing connections will be allowed once all other tests have completed. So
# TCP_OUT, UDP_OUT and ICMP_OUT will not have any affect.
#
# If you allow incoming DNS lookups you may need to use the following
# directive in the options[] section of your named.conf:
#
#     query-source port 53;
#
# This will force incoming DNS traffic only through port 53
#
# Disabling this option will break firewall functionality that relies on
# stateful packet inspection (e.g. DNAT, PACKET_FILTER) and makes the firewall
# less secure
#
# This option should be set to "1" in all other circumstances
# F SPI = "1"

# Allow incoming TCP ports
TCP_IN = "20,21,22,25,53,80,110,143,443,465,587,993,995,999"

# Allow outgoing TCP ports
TCP_OUT = "20,21,22,25,37,43,53,80,110,113,443,587,873,993,995,999"

# Allow incoming UDP ports
UDP_IN = "20,21,53"

# Allow outgoing UDP ports
# To allow outgoing traceroute add 33434:33523 to this list
```

Add an incoming port to the `TCP_IN` list. TCP ports. Once you have the file open, you will see `TCP_IN` and `TCP_OUT` sections. The `TCP_IN` section lists open inbound TCP ports separated by commas. The ports are in numerical order to make things easy, but it's not required that the ports you stick to the order. You can add ports to the end of the sequence, just separate them with commas.

1. For example, let's say you want to open port 999, and the current open ports are `20, 21, 22, 25, 53, 80, 110, 143, 443, 465, 587, 993, 995`.
2. After adding port 999 to the list, it will look like this: `20, 21, 22, 25, 53, 80, 110, 143, 443, 465, 587, 993, 995, 999`.
3. To get into insertion/typing mode in vim, press the `i` key on the keyboard.

```
# outgoing connections will be allowed once all other tests have completed. So
# TCP_OUT, UDP_OUT and ICMP_OUT will not have any affect.
#
# If you allow incoming DNS lookups you may need to use the following
# directive in the options[] section of your named.conf:
#
#     query-source port 53;
#
# This will force incoming DNS traffic only through port 53.
#
# Disabling this option will break firewall functionality that relies on
# stateful packet inspection (e.g. DNAT, PACKET_FILTER) and makes the firewall
# less secure
#
# This option should be set to "1" in all other circumstances
LF_SPI = "1"

# Allow incoming TCP ports
TCP_IN = "20,21,22,25,53,80,110,143,443,465,587,993,995,999"

# Allow outgoing TCP ports
TCP_OUT = "20,21,22,25,37,43,53,80,110,113,443,587,873,993,995,999"

# Allow incoming UDP ports
UDP_IN = "20,21,53"

# Allow outgoing UDP ports
# To allow outgoing traceroute add 33434:33523 to this list
```

5.

Allow outgoing TCP to the `TCP_OUT` list. Just as you did with the incoming port, add any outbound TCP ports you'd like to open to the `TCP_OUT` list.



6.

Save your changes and exit the file. Follow these steps to save and exit the file:

1. Press the `Esc` key.
2. Type `:wq!`.
3. Press `Enter`.

```
# Allow incoming TCP ports
TCP_IN = "20,21,22,25,53,80,110,143,443,465,587,993,995,999"

# Allow outgoing TCP ports
TCP_OUT = "20,21,22,25,37,43,53,80,110,113,443,587,873,993,995,999"

# Allow incoming UDP ports
UDP_IN = "20,21,53"

# Allow outgoing UDP ports
# To allow outgoing traceroute add 39434:39523 to this list
UDP_OUT = "20,21,53,113,123,873,6277,24441"

# Allow incoming PING. Disabling PING will likely break external uptime
# monitoring
ICMP_IN = "i"

# Set the per IP address incoming ICMP packet rate for PING requests. This
# rate limits PING requests which if exceeded results in silently rejected
# packets. Disable or increase this value if you are seeing PING drops that you
# do not want
#
# To disable rate limiting set to "0", otherwise set according to the Intables

root@wiki:/etc/csf# service csf restart_
```

7.

Type `service csf restart` and press `? Enter`. This restarts the firewall and opens the new ports.

1. To deny a port, re-open the file, delete the port, save the file, and then re-start the firewall.

Method 3 of 3:

Using Advanced Policy Firewall

```
Ubuntu 18.04.2 LTS wiki tty1
wiki login: wiki
Password:
Last login: Mon Jan 13 08:48:53 UTC 2020 on tty1
Welcome to Ubuntu 18.04.2 LTS (GNU/Linux 4.15.0-74-generic x86_64)

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

System information as of Mon Jan 13 09:01:24 UTC 2020

System load:  0.68      Processes:    87
Usage of /:   29.1% of 19.68GB  Users logged in:  0
Memory usage: 3%        IP address for enp0s3: 10.0.2.15
Swap usage:   0%

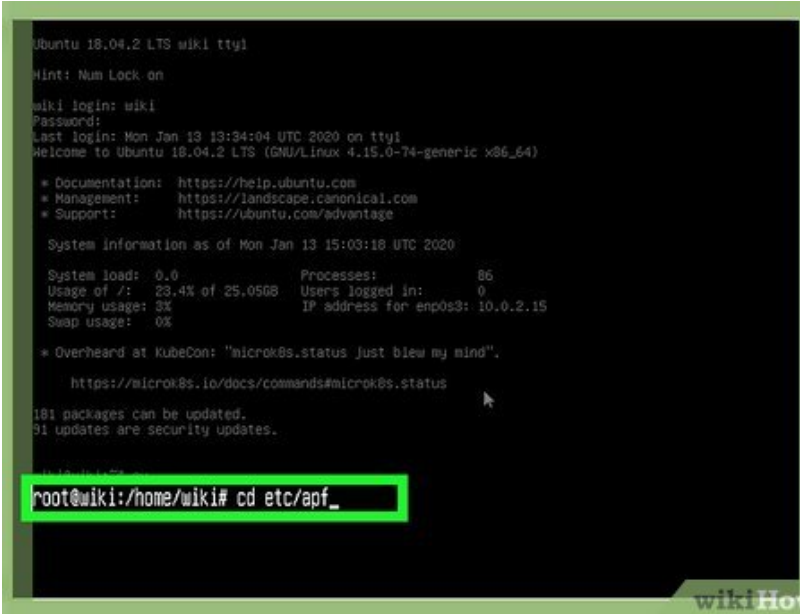
181 packages can be updated.
31 updates are security updates.

wiki@wiki:~$ su_
```

1.

Log in to your server. If you're not logged in as the root user, you can `su` to root to adjust your configuration.

2.



```
Ubuntu 18.04.2 LTS wiki tty1
Hint: Num Lock on
wiki login: wiki
Password:
Last login: Mon Jan 13 13:34:04 UTC 2020 on tty1
Welcome to Ubuntu 18.04.2 LTS (GNU/Linux 4.15.0-74-generic x86_64)

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

System information as of Mon Jan 13 15:03:18 UTC 2020:

System load: 0.0          Processes: 86
Usage of /: 23.4% of 25.0GB Users logged in: 0
Memory usage: 3%        IP address for enp0s3: 10.0.2.15
Swap usage: 0%

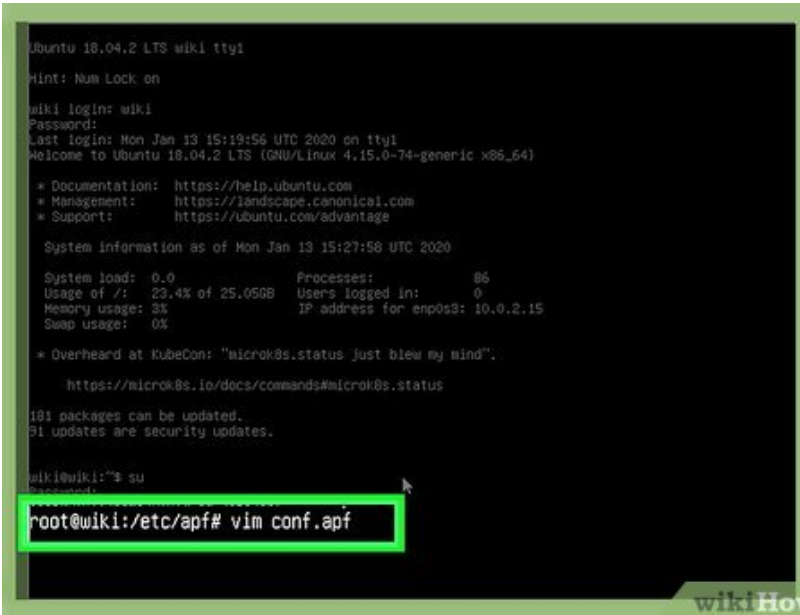
 * Overheard at KubeCon: "microk8s.status just blew my mind".
   https://microk8s.io/docs/commands#microk8s.status

181 packages can be updated.
91 updates are security updates.

wiki@wiki:~$
root@wiki:/home/wiki# cd /etc/apf_
```

Go to the directory that contains your APF config file. The file you're looking for is called `conf.apf`, and it'll be in `/etc/apf` by default.^[4] Type `cd /etc/apf` to enter that directory.

3.



```
Ubuntu 18.04.2 LTS wiki tty1
Hint: Num Lock on
wiki login: wiki
Password:
Last login: Mon Jan 13 15:19:56 UTC 2020 on tty1
Welcome to Ubuntu 18.04.2 LTS (GNU/Linux 4.15.0-74-generic x86_64)

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

System information as of Mon Jan 13 15:27:58 UTC 2020:

System load: 0.0          Processes: 86
Usage of /: 23.4% of 25.0GB Users logged in: 0
Memory usage: 3%        IP address for enp0s3: 10.0.2.15
Swap usage: 0%

 * Overheard at KubeCon: "microk8s.status just blew my mind".
   https://microk8s.io/docs/commands#microk8s.status

181 packages can be updated.
91 updates are security updates.

wiki@wiki:~$ su
Password:
root@wiki:/etc/apf# vim conf.apf
```

Open `conf.apf` in a text editor. You can use any text editor you wish, such as vim or nano.

1. To open `conf.apf` in vim, you'd type `vim conf.apf` and press `?Enter`.

4.

```
HELPER_FTP="1"
HELPER_FTP_PORT="21"
HELPER_FTP_DATA="20"

# Configure inbound (Ingress) accepted services. This is an optional
# feature: services and customized entries may be made directly to an ip's
# virtual net file located in the vnet/ directory. Format is comma separated
# and underscore separator for ranges.
#
# Example:
# IG_TCP_CPORTS="21,22,25,53,80,443,110,143,6000,7000"
# IG_UDP_CPORTS="20,21,53,123"
# IG_ICMP_TYPES="3,5,11,0,30,8"

# Common inbound (Ingress) TCP ports
IG_TCP_CPORTS="20,21,22,25,53,80,110,143,443,465,587,993,995,999"

# Common inbound (Ingress) UDP ports
IG_UDP_CPORTS=""

# Common ICMP inbound (Ingress) types
# 'internals/icmp.types' for type definition: 'all' is wildcard for any
IG_ICMP_TYPES="3,5,11,0,30,8"

# Configure outbound (egress) accepted services. This is an optional
# feature: services and customized entries may be made directly to an ip's
# virtual net file located in the vnet/ directory.
#
# Outbound (egress) filtering is not required but makes your firewall setup
# complete by providing full inbound and outbound packet filtering. You can
# toggle outbound filtering on or off with the EGF variable. Format is comma
```

Add inbound ports to the `IG_TCP_CPORTS` list. Once you have the file open, you will see `IG_TCP_CPORTS` and `EG_TCP_CPORTS` sections. The `IG_TCP_CPORTS` section lists open inbound ports separated by commas. The ports are listed in numerical order to make things easy, but it's not required to stick with it. You can add ports to the end of the sequence, just separate them with commas.

1. For example, let's say you want to open port 999, and the current open ports are `20, 21, 22, 25, 53, 80, 110, 143, 443, 465, 587, 993, 995`.
2. After adding port 999 to the `IG_TCP_CPORTS` list, it will look like this: `20, 21, 22, 25, 53, 80, 110, 143, 443, 465, 587, 993, 995, 999`.
3. To get into insertion/typing mode in vim, press the `i` key on the keyboard.

5.

```
# separated and underscore separator for ranges.
#
# Example:
# EG_TCP_CPORTS="21,25,80,443,43"
# EG_UDP_CPORTS="20,21,53"
# EG_ICMP_TYPES="all"

# Outbound (egress) filtering
EGF="0"

# Common outbound (egress) TCP ports
EG_TCP_CPORTS="20,21,22,25,53,80,110,443,443,465,587,993,995,999"

# Common outbound (egress) UDP ports
EG_UDP_CPORTS="20,21,53"

# Common ICMP outbound (egress) types
# 'internals/icmp.types' for type definition: 'all' is wildcard for any
EG_ICMP_TYPES="all"

# Configure user-id specific outbound (egress) port access. This is a more
# granular feature to limit the scope of outbound packet flows with user-id
# conditioning. Format is comma separated and underscore separator for ranges.
# This is NOT A FILTERING FEATURE, this is an ACCESS CONTROL feature. That
# means EG_TCP_UID and EG_UDP_UID are intended to ALLOW outbound access for
# specified users, not DENY.
#
# Format: EG_[TCP|UDP]_UID="uid:port"
# Example:
# Allow outbound access to destination port 22 for uid 0
# EG_TCP_UID="0:22"
```

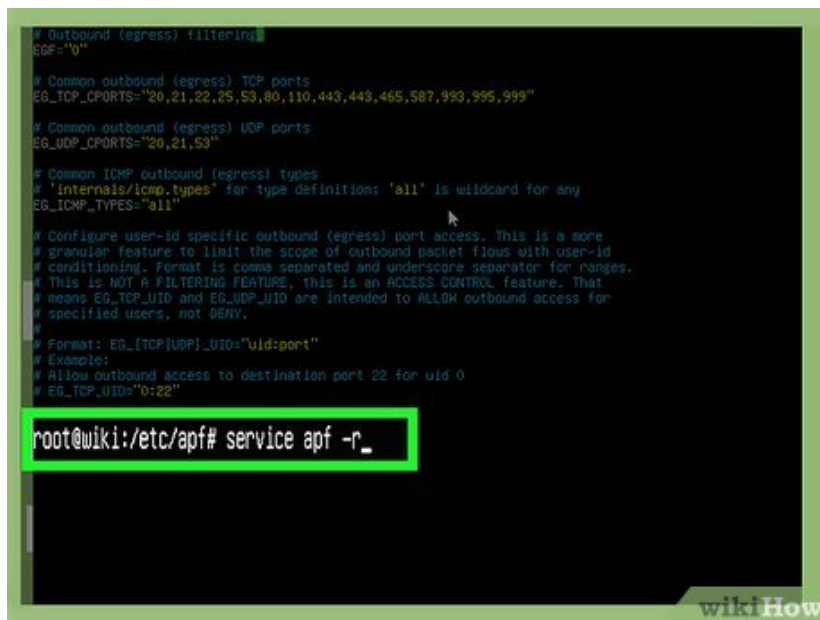
Allow outbound ports to the `EG_TCP_CPORTS` list. Just as you did with the incoming port, add any outbound TCP ports you'd like to open to the `EG_TCP_CPORTS` list.



6.

Save your changes and exit the file. Follow these steps to save and exit the file:

1. Press the `Esc` key.
2. Type `:wq!`.
3. Press `?Enter`.



7.

Type `service apf -r` and press `?Enter`. This restarts the APF firewall and opens the new ports.

1. To deny a port, re-open the file, delete the port, save the file, and then re-start the firewall.

You finished reading the article "**How to Open Ports in Linux Server Firewall**" edited by the [TipsMake](#) team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.
