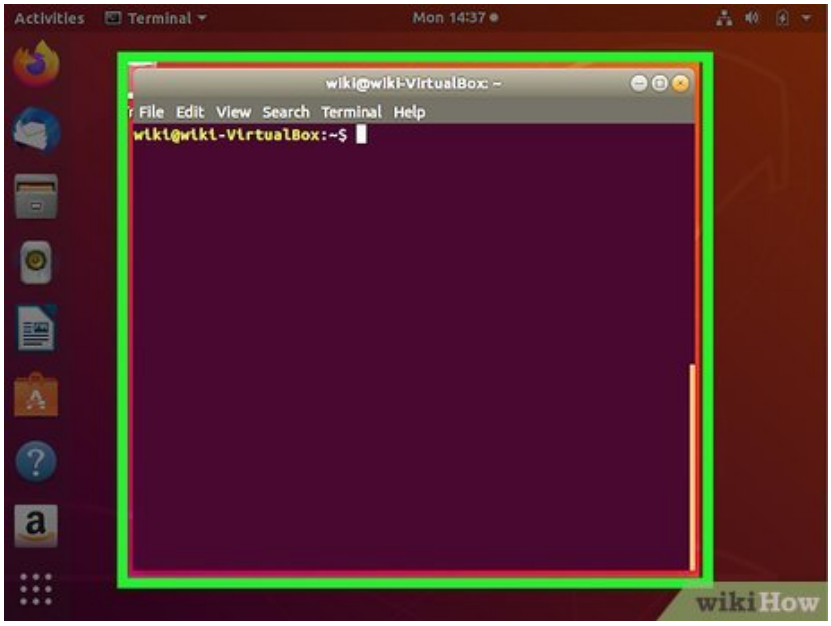
How to Open Ports in Linux Server Firewall

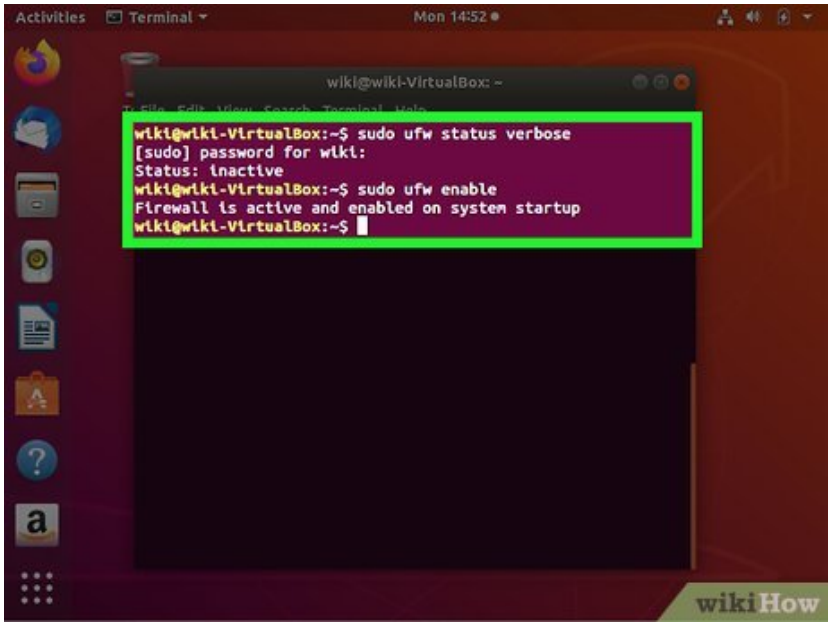
This wikiHow will teach you how to open ports in three popular Linux firewalls. If you're using a product like ConfigServer Firewall (CSF) or Advanced Policy Firewall (ADP), you can control open ports in the firewall's main configuration...

Method 1 of 3:

Using Uncomplicated Firewall for Ubuntu

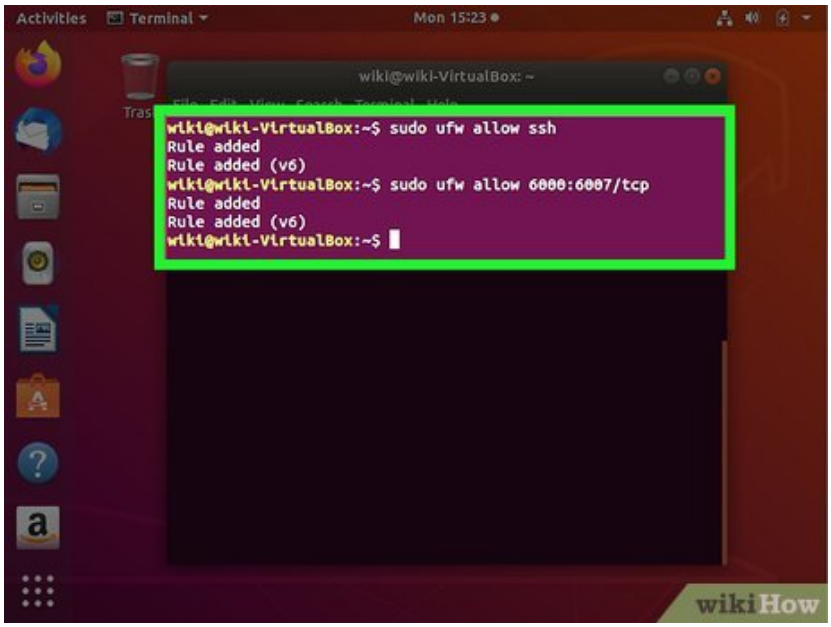
1. 

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

2. 

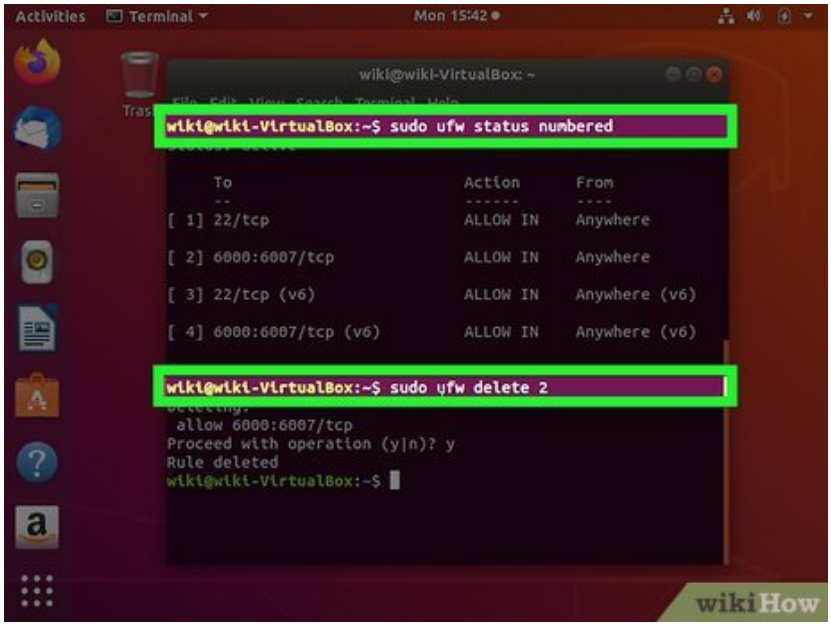
Type `sudo ufw status verbose` and press ? Enter. If UFW is already running, you'll see a status message, as well as a list of any firewall rules (including opened ports) that already exist.[1]

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. 

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`.

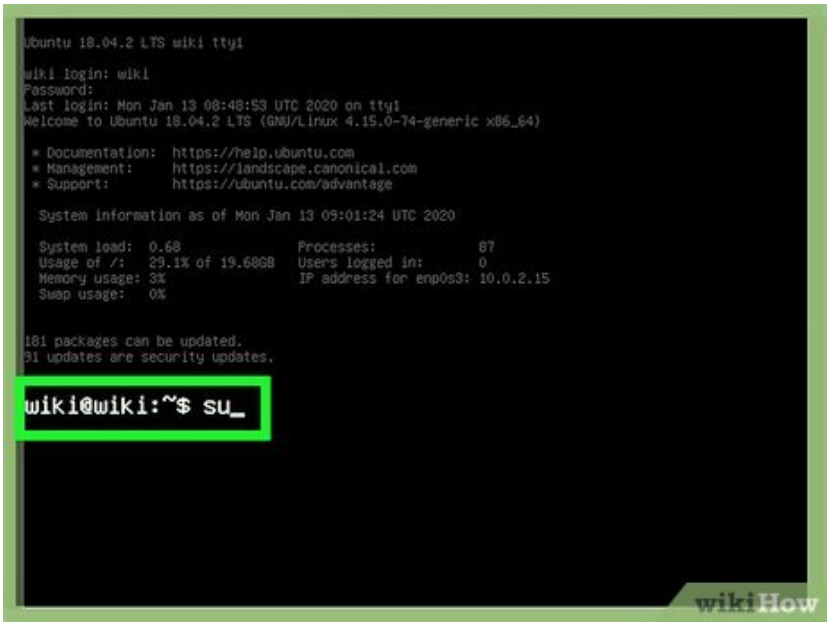
3. To specify an IP address that can access the port, use this syntax: `sudo ufw allow from 10.0.0.1 to any port 22`. Replace `10.0.0.1` with the IP address, and `22` with the port you want to open to that address.
4. 

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:

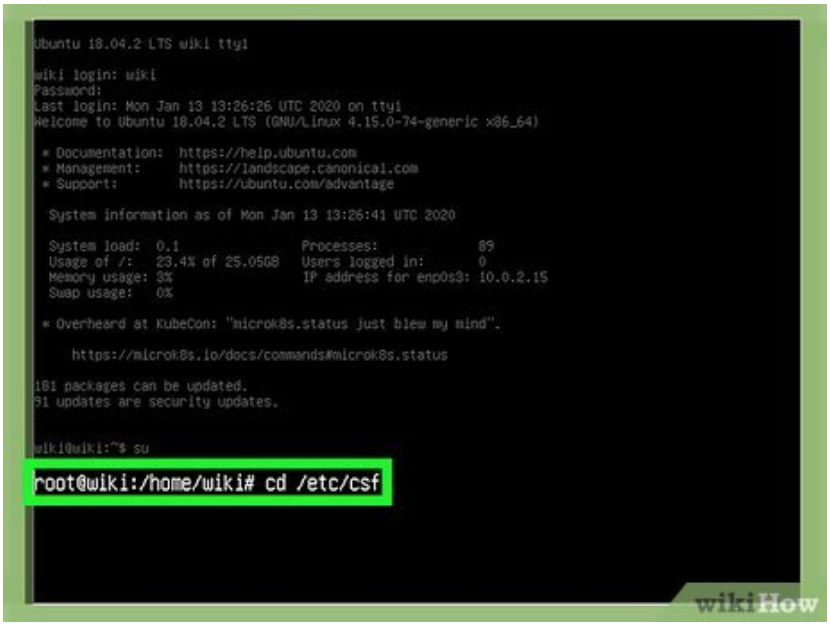
1. Type `sudo ufw status numbered` and press ? Enter. This displays a list of all firewall rules, each beginning with a number to represent it in the list.
2. Identify the number at the beginning of rule you want to delete. For example, let's say you want to remove the rule that opens port 22, and that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

Method 2 of 3:

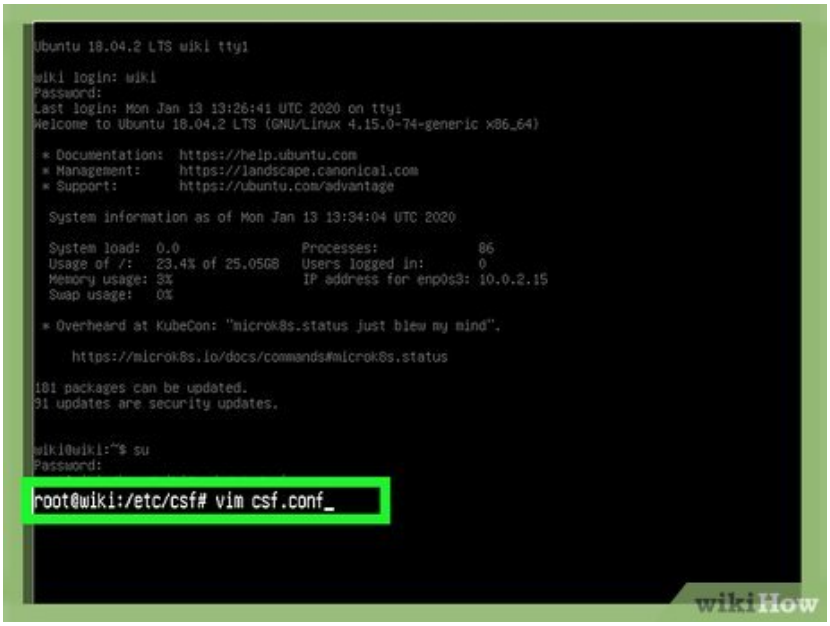
Using ConfigServer Firewall

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.

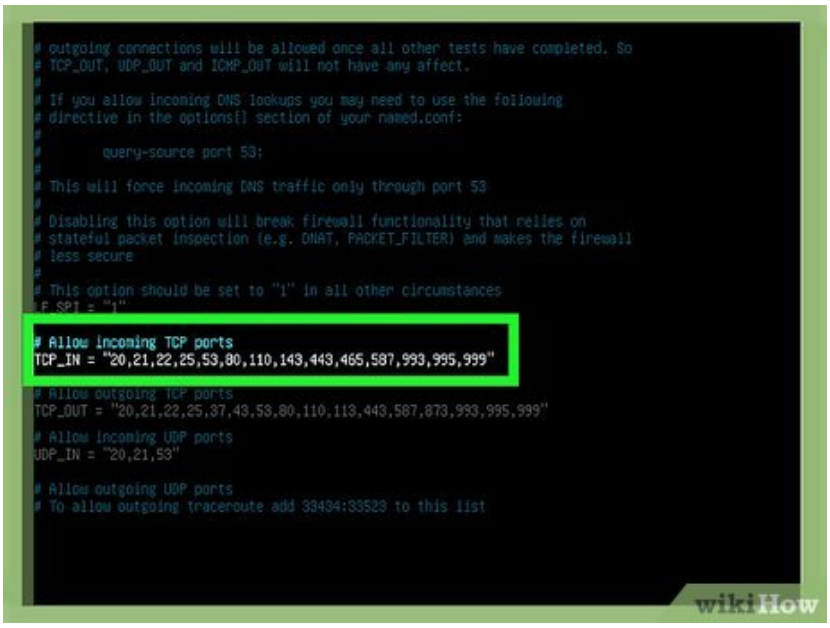
2. 

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. 

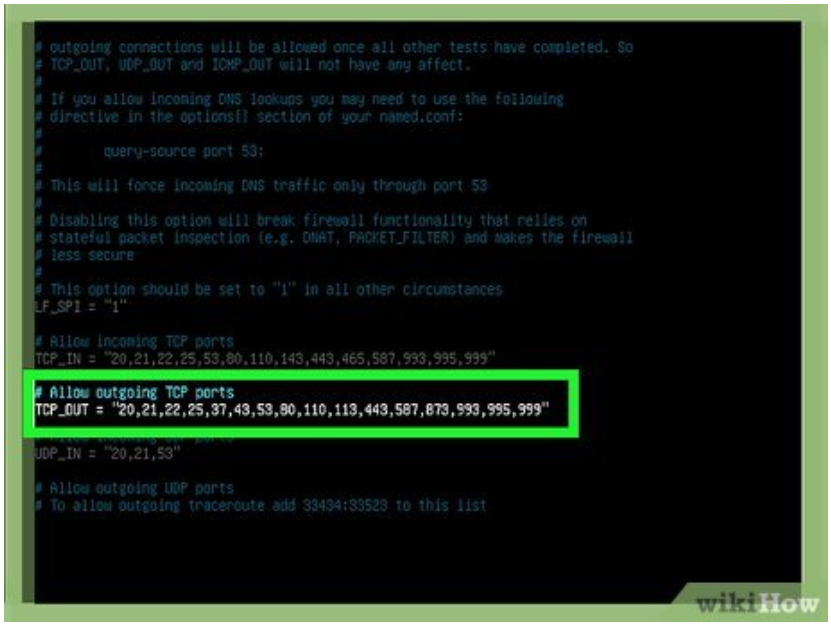
Open `csf.conf` in a text editor. You can use any text editor you wish, such as vim or nano.

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

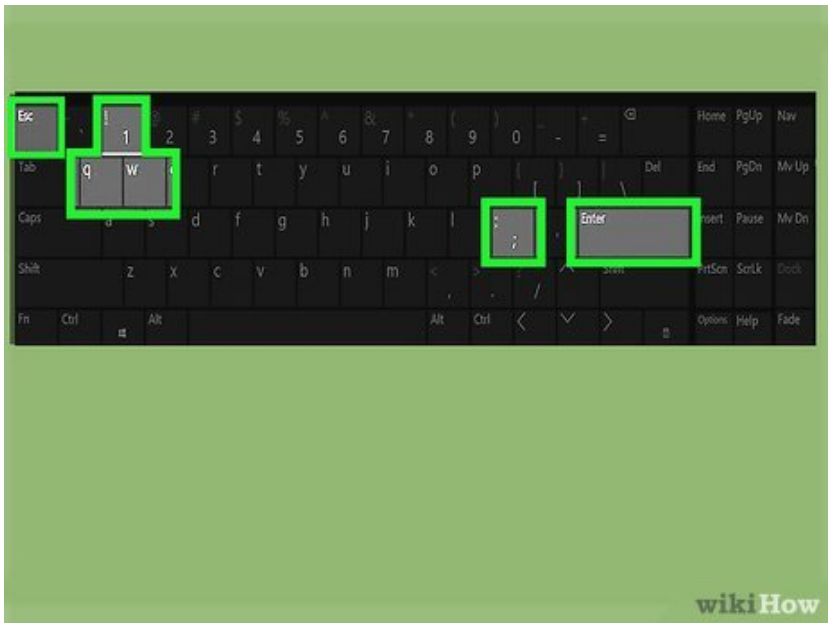
4. 

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.

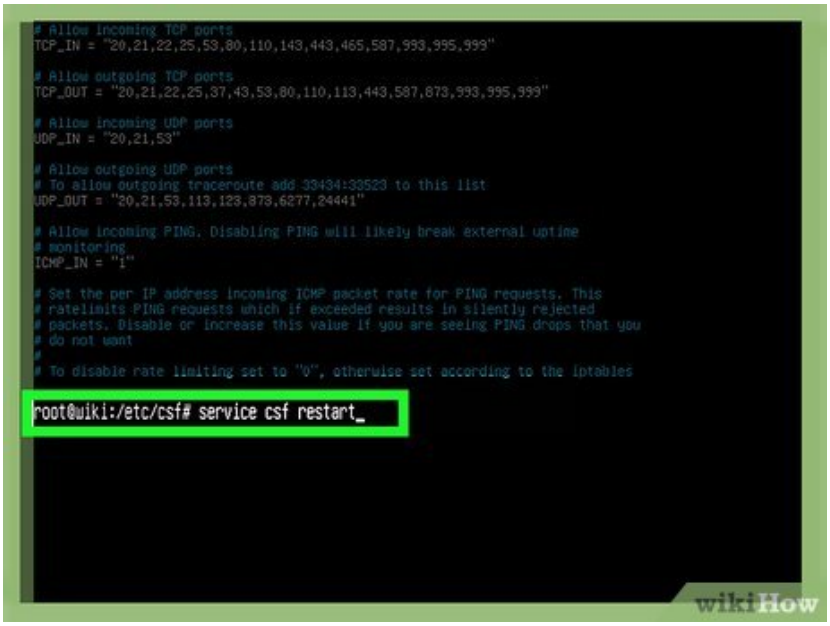
5. 

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.

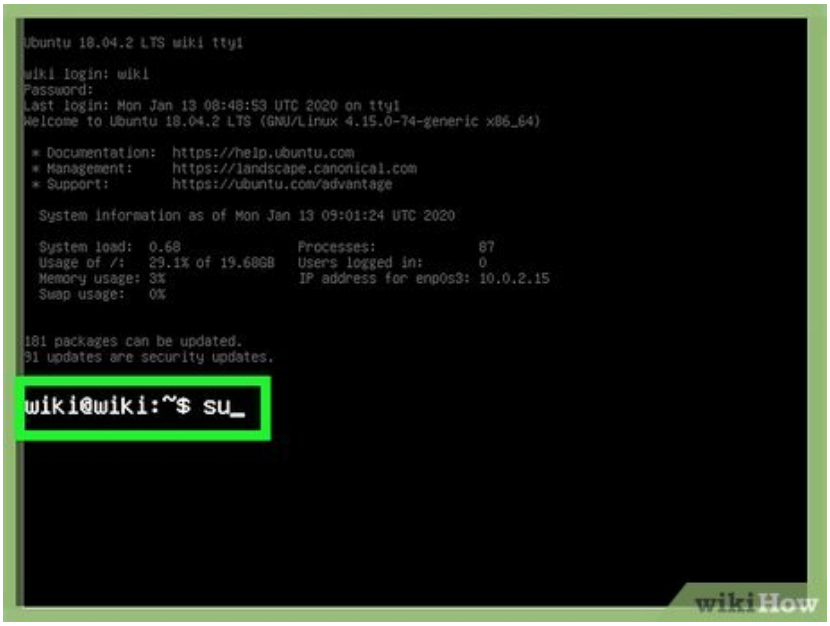
7. 

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

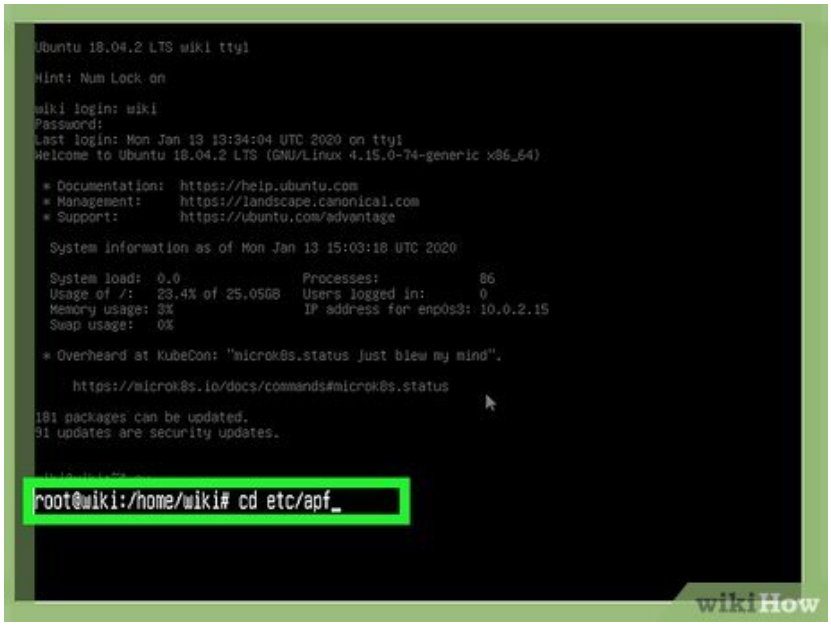
1. To deny a port, re-open the file, delete the port, save the file, and then re-start the firewall.

Method 3 of 3:

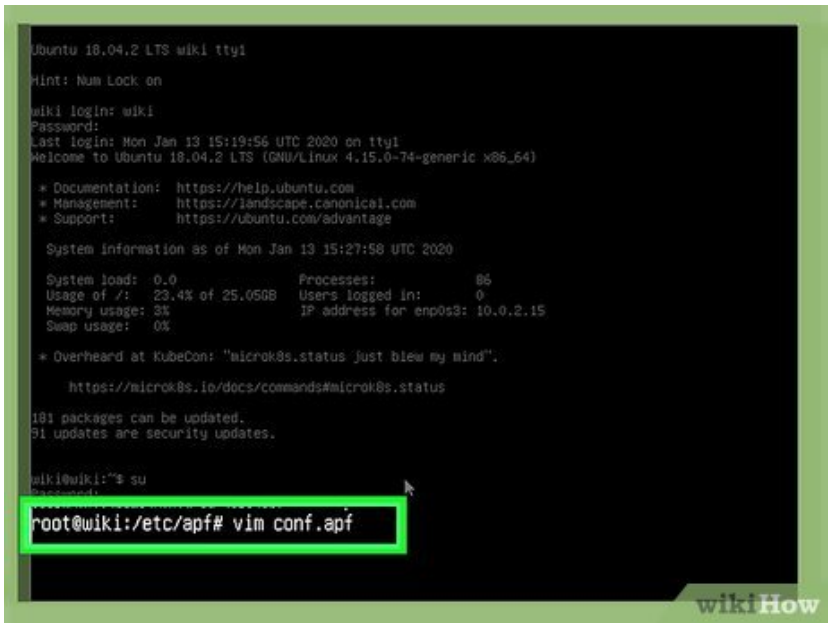
Using Advanced Policy Firewall

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.

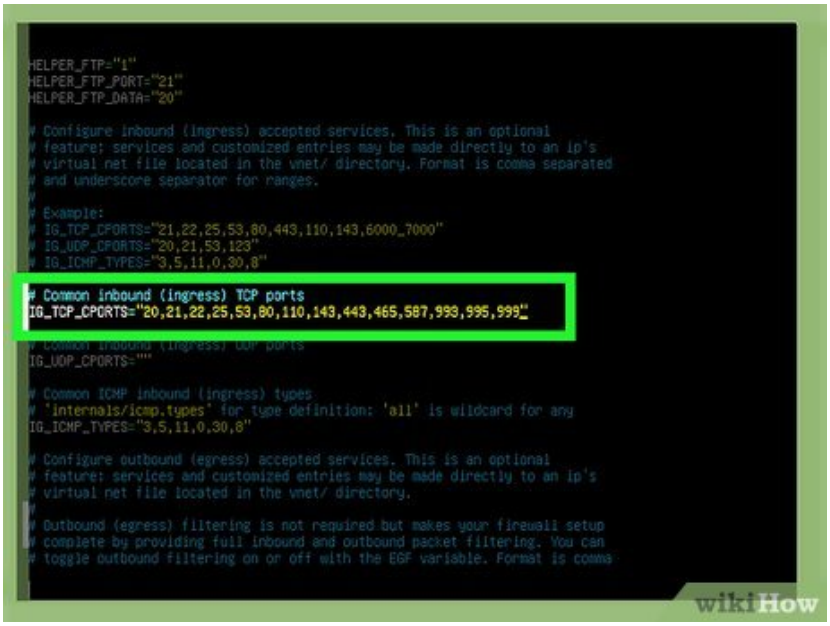
2. 

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. 

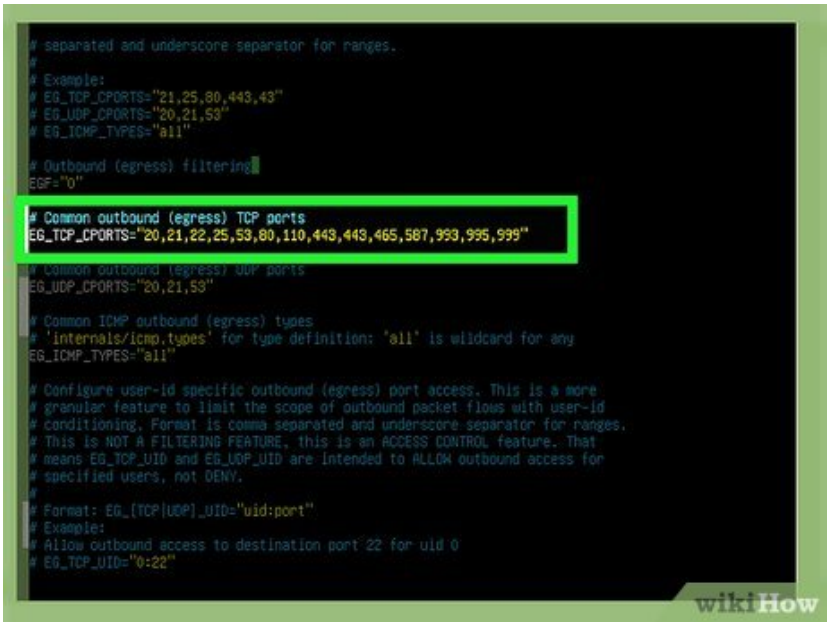
Open `conf.apf` in a text editor. You can use any text editor you wish, such as vim or nano.

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

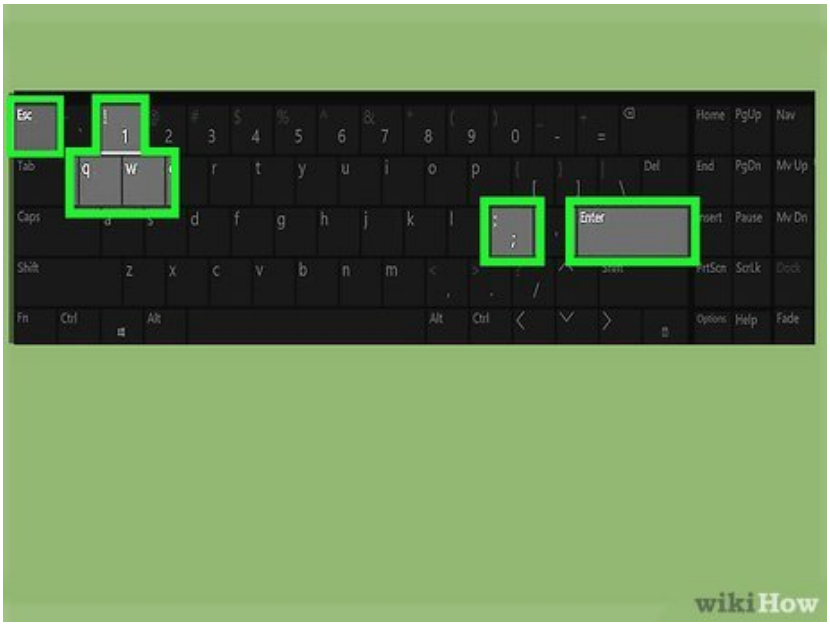
4. 

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.

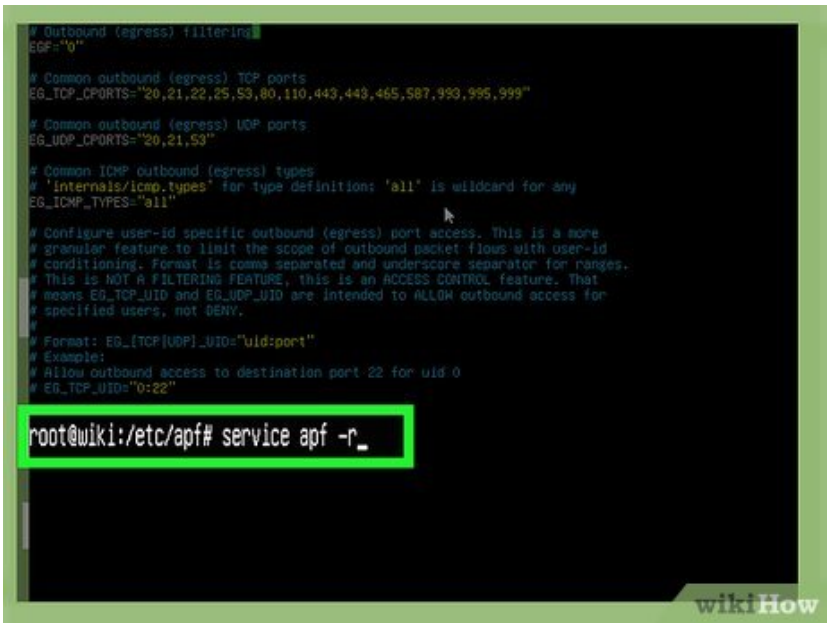
5. 

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 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.