**How to install and configure ufw**

To install and configure ufw (Uncomplicated Firewall) on a Ubuntu system, follow these steps:

Install ufw:

**sudo apt-get update**

**sudo apt-get install ufw**

Check the status of the firewall:

**sudo ufw status**

Enable the firewall:

**sudo ufw enable**

To allow incoming traffic on a specific port, for example, port 80 for HTTP:

**sudo ufw allow 80/tcp**

To allow incoming traffic for a specific service, for example, OpenSSH:

**sudo ufw allow ssh**

To deny incoming traffic for a specific port:

**sudo ufw deny 80/tcp**

To delete a rule:

**sudo ufw delete allow 80/tcp**

To reset the firewall to its default state:

**sudo ufw reset**

To disable the firewall:

**sudo ufw disable**

Remember to always be cautious when modifying firewall rules as it can potentially impact the security and connectivity of your system.

**How to see all allowed in ufw**

To see all the allowed incoming traffic rules in ufw, use the following command:

**sudo ufw status numbered**

This will show a numbered list of all the active incoming firewall rules, including the rule number, the rule action (ALLOW or DENY), the protocol (tcp, udp, icmp, etc.), the source IP address, and the destination port. For example:

Status: active

To Action From

-- ------ ----

22/tcp ALLOW Anywhere

80/tcp ALLOW Anywhere

22/tcp (v6) ALLOW Anywhere (v6)

80/tcp (v6) ALLOW Anywhere (v6)

You can use the rule number to delete a specific rule using the command sudo ufw delete [rule\_number].

How to specify particuler address

To allow incoming traffic from a specific IP address or network to your system using ufw, use the following syntax:

**sudo ufw allow from [IP\_ADDRESS] to any port [PORT\_NUMBER]**

For example, to allow incoming traffic on port 80 from the IP address 192.168.1.100, use the following command:

sudo ufw allow from 192.168.1.100 to any port 80

Similarly, to allow incoming traffic on port 22 from the subnet 192.168.1.0/24, use the following command:

sudo ufw allow from 192.168.1.0/24 to any port 22

Note that the to any part of the command specifies that the incoming traffic is allowed to any destination on the system, not just a specific one. You can also specify a specific destination IP or hostname if needed.