



How to limit SSH (TCP port 22) connections with ufw on Ubuntu Linux

last updated August 18, 2017 in [Debian / Ubuntu](#), [Iptables](#), [Linux](#), [Ubuntu Linux](#)

How do I limit ssh connection attempts using UFW (Uncomplicated Firewall) on Ubuntu or Debian Linux server?



UFW means [Uncomplicated Firewall](#). It defaults on Ubuntu and can be installed on other Linux distros such as Arch Linux, Debian and more. It is nothing but a front-end for managing a Netfilter firewall. It provides a command line interface and aims to be uncomplicated and easy to use.

```
Status: active
Logging: on (low)
Default: deny (incoming), allow (outgoing), deny (routed)
New profiles: skip

To Action From
--
22/tcp LIMIT IN Anywhere
22/tcp (v6) LIMIT IN Anywhere (v6)
```

UFW rate limit on Ubuntu server

Adblock detected 🙄

My website is made possible by displaying online advertisements to my visitors. I get it! Ads are annoying but they help keep this website running. It is hard to keep the site running and producing new content when so many people block ads. Please consider donating money to the nixCraft via [PayPal/Bitcoin](#), or become a [supporter using Patreon](#).

Rate limiting with ufw

You can add limit rule. Currently only IPv4 is supported. With this syntax you can deny connections from an IP address that has attempted to initiate 6 or more connections in the last 30 seconds. This option is very useful for services such as sshd.

Syntax

The syntax is pretty simple:

```
## ufw limit ssh various usage ##
ufw limit ssh

ufw limit ssh/tcp

ufw limit ssh comment 'Rate limit for openssh serer'

### if sshd is running on tcp port 2022 ####
ufw limit 2022/tcp comment 'SSH port rate limit'
```

The above rules are useful for protecting against brute-force login attacks. When a limit rule is used, ufw will normally allow the connection but will deny connections if an IP address attempts to initiate six or more connections within thirty seconds. Once setup you can verify it with the following command:

```
$ sudo ufw limit ssh/tcp comment 'Rate limit for openssh serer'
$ sudo ufw status
```

Sample outputs:

```
Status: active
```

To	Action	From	
--	-----	----	
22/tcp	LIMIT	Anywhere	# Rate limit for
22/tcp (v6)	LIMIT	Anywhere (v6)	# Rate limit for

The actual rules are as follows in iptables:

```
-A ufw-user-input -p tcp -m tcp --dport 22 -m conntrack --ctstate NEW -m recent --set
-A ufw-user-input -p tcp -m tcp --dport 22 -m conntrack --ctstate NEW -m recent --update --seconds 30 --hitcount 6
-A ufw-user-input -p tcp -m tcp --dport 22 -j ufw-user-limit-accept
```

Please note that the new ssh rule will then replace the previous ssh rule.

This entry is **5 of 9** in the **Uncomplicated Firewall (UFW)** series. Keep reading the rest of the series:

1. [How to install UFW firewall on Ubuntu 16.04 LTS server](#)

2. [How to open ssh.port using ufw on Ubuntu/Debian Linux](#)
3. [How to configure ufw to forward port 80/443 to internal server hosted on LAN](#)
4. [How to block an IP address with ufw on Ubuntu Linux server](#)
5. How to limit SSH (TCP port 22) connections with ufw on Ubuntu Linux
6. [How To: Ubuntu Linux Firewall Open Port Command Using UFW](#)
7. [How to open DNS.port 53 using ufw on Ubuntu/Debian Linux](#)
8. [Set Up a Firewall with UFW on Ubuntu 18.04](#)
9. [How to delete a UFW firewall rule](#)

SHARE ON

[Facebook](#)[Twitter](#)

Posted by: Vivek Gite

The author is the creator of nixCraft and a seasoned sysadmin, DevOps engineer, and a trainer for the Linux operating system/Unix shell scripting. Get the **latest tutorials on SysAdmin, Linux/Unix and open source topics** via [RSS/XML feed](#) or [weekly email newsletter](#).

 3 comment

Jouni "rautamiekka" Järvinen January 25, 2017 at 10:48 am

It's harder but directly commanding `iptables` is better since you can make precise rules while UFW only in the general direction.

PGF January 30, 2017 at 1:54 pm

It is simpler, but it gives you far less fine control than iptables.

Stephan January 31, 2017 at 4:31 pm

But what if the IP changes then the attacker can still attempt to connect to the server. Why not just not use the default port, configure SSH on another port.

Still, have a question? Get help on our forum!

Tagged as: [ufw command](#), [Easy](#).



@2000-2019 nixCraft. All rights reserved.

[PRIVACY](#)

[TERM OF SERVICE](#)

[CONTACT/EMAIL](#)

[DONATIONS](#)

[SEARCH](#)