

Table Of Contents

Table Of Contents ..... 1

How Do I Configure Nginx To Block IPs? ..... 2

    How Do I Deny All and Allow Only Intranet/LAN IPs? ..... 3

    How Do I Customize HTTP 403 Forbidden Error Messages? ..... 3

        See also: ..... 3

        References: ..... 3

[Home](#) > [Faq](#) > [Nginx](#)

## Nginx Block And Deny IP Address OR Network Subnets

Posted by [Vivek Gite](#) <[vivek@nixcraft.com](mailto:vivek@nixcraft.com)>

How do I block or deny access based on the host name or IP address of the client visiting website under nginx web server?

Nginx comes with a simple module called `ngx_http_access_module` to allow or deny access to IP address. The syntax is as follows:

```
deny IP;
deny subnet;
allow IP;
allow subnet;
# block all ips
deny    all;
# allow all ips
allow   all;
```

Note rules are checked in the order of their record to the first match.

## How Do I Configure Nginx To Block IPs?

Edit `nginx.conf` file, enter (note my nginx path is set to `/usr/local/nginx/`, replace this according to your setup):

```
# cd /usr/local/nginx/conf/
# vi nginx.conf
```

Add the following line in http section:

```
## Block spammers and other unwanted visitors  ##
include blockips.conf;
```

Save and close the file. Finally, create `blockips.conf` in `/usr/local/nginx/conf/`, enter:

```
# vi blockips.conf
```

Append / add entries as follows:

```
deny 1.2.3.4;
deny 91.212.45.0/24;
deny 91.212.65.0/24;
```

Save and close the file. Test the config file, enter:

```
# /usr/local/nginx/sbin/nginx -t
```

Sample outputs:

```
the configuration file /usr/local/nginx/conf/nginx.conf syntax is ok
configuration file /usr/local/nginx/conf/nginx.conf test is successful
```

Reload the new config, enter:

```
# /usr/local/nginx/sbin/nginx -s reload
```

## How Do I Deny All and Allow Only Intranet/LAN IPs?

Edit config file as follows:

```
location / {
    # block one workstation
    deny    192.168.1.1;
    # allow anyone in 192.168.1.0/24
    allow   192.168.1.0/24;
    # drop rest of the world
    deny    all;
}
```

Granted access to network 192.168.1.0/24 with the exception of the address 192.168.1.1.

## How Do I Customize HTTP 403 Forbidden Error Messages?

Create a file called error403.html in default document root, enter:

```
# cd /usr/local/nginx/html
# vi error403.html
```

```
<html>
<head><title>Error 403 - IP Address Blocked</title></head>
<body>
Your IP Address is blocked. If you this an error, please contact webmaster with your IP at
</body>
</html>
```

If SSI enabled, you can display the client IP easily from the html page itself:

```
Your IP Address is <!--#echo var="REMOTE_ADDR" --> blocked.
```

Save and close the file. Edit your nginx.conf file, enter:

```
# vi nginx.conf

# redirect server error pages to the static page
error_page 403 /error403.html;
location = /error403.html {
    root    html;
}
```

Save and close the file. Reload nginx, enter:

```
# /usr/local/nginx/sbin/nginx -s reload
```

See also:

- [Nginx Shell Script To Block Spamhaus Lasso Drop Spam IP Address](#) <sup>[2]</sup>

References:

- [nginx wiki](#)

4000+ howtos and counting! Want to read more Linux / UNIX howtos, tips and tricks? Subscribe to our [daily email](#) newsletter or [weekly newsletter](#) to make sure you don't miss a single tip/tricks. Alternatively, subscribe via [RSS/XML](#) feed.

Article printed from Frequently Asked Questions About Linux / UNIX: <http://www.cyberciti.biz/faq/>

URL to article: <http://www.cyberciti.biz/faq/linux-unix-nginx-access-control-howto/>

URLs in this post:

[1] Image: <http://www.cyberciti.biz/faq/category/nginx/>

[2] Nginx Shell Script To Block Spamhaus Lasso Drop Spam IP Address: <http://bash.cyberciti.biz/web-server/nginx-shell-script-to-block-spamhaus-lasso-drop-spam-ip-address/>

---

Copyright © 2006-2010 [nixCraft](http://www.cyberciti.biz/). All rights reserved. This print / pdf version is for personal non-commercial use only. More details <http://www.cyberciti.biz/tips/copyright>.