

# Silicon's blog

Menu

HOME KADENA SOLANA ETHEREUM BOT AUTOMATION  
PROXMOX NGINX PROXY MANAGER OTHERS CONTACT

Menu

## How to combine Nginx Proxy Manager with Cloudflare to access your websites/ web services securely

Posted on January 22, 2023 by Silicon

Sharing is Caring:



[The previous article](#) taught you how to install Nginx Proxy Manager using Docker Compose in Ubuntu 22.04.

Cloudflare provides a DNS proxy service which will hide your server IP address, adding an additional security layer to your website.

This article will teach you how to combine Nginx Proxy Manager with Cloudflare in order to access your internal web services via the Internet.

Prerequisite:

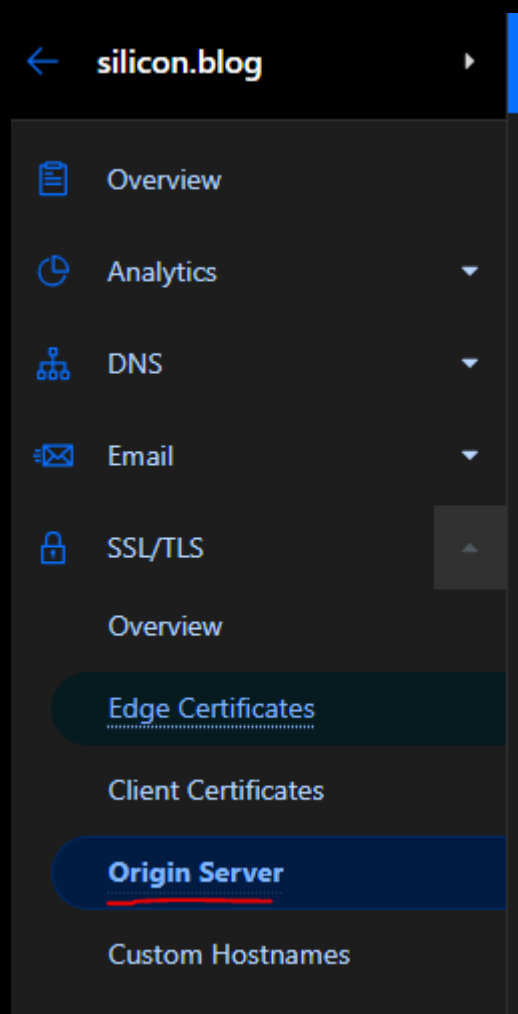
You have set up Nginx Proxy Manager on your system. Look at [my previous article](#) if you haven't set it up.

You have created a Cloudflare account.

You have changed your DNS from your registrar to Cloudflare.

You have a domain parked in the Active Zone on Cloudflare. You may visit [Freenom](#) to get a free domain if you don't have a paid one.

**Step 1:** Move to Original Server under your domain's SSL/TLS section.



Click the Create Certificate button.

## SSL/TLS

Origin Server

[Documentation](#)

### Origin Certificates

Generate a free TLS certificate signed by Cloudflare to install on your origin server.

Origin Certificates are only valid for encryption between Cloudflare and your origin server.

[Create Certificate](#)

Hosts

Expires On

**Step 2:** Change the expiration time of your certificate. I recommend you to choose a duration longer than 1 year; otherwise, you may need to replace your SSL certificate on Nginx Proxy Manager frequently.

## SSL/TLS

Origin Server

[Documentation](#)

[← Back](#)

### Origin Certificate Installation

Follow the steps below to install a certificate on your origin server.

**The first step in generating a certificate for your origin is creating a private key and a Certificate Signing Request (CSR).** You can provide your own CSR or we can generate a key and CSR using your web browser.

Generate private key and CSR with Cloudflare

Private key type

RSA (2048)

Use my private key and CSR

**List the hostnames (including wildcards) on your origin that the certificate should protect.** By default your origin certificate covers the apex of your domain (**example.com**) and a wildcard (**\*.example.com**). If there are others you wish to add, e.g., those not covered by the wildcard such as **one.two.example.com**, you can add them below.

Hostnames

\*.silicon.blog

silicon.blog

**Choose how long before your certificate expires.** By default your certificate will be valid for fifteen (15) years. If you'd like to decrease how long your certificate will be valid make a selection below.

Certificate Validity

15 years

Cancel

Create

**Step 3:** Copy the text under Origin Certificate and create a file called cert.pem on your computer.



```
-----END PRIVATE KEY-----
```

to

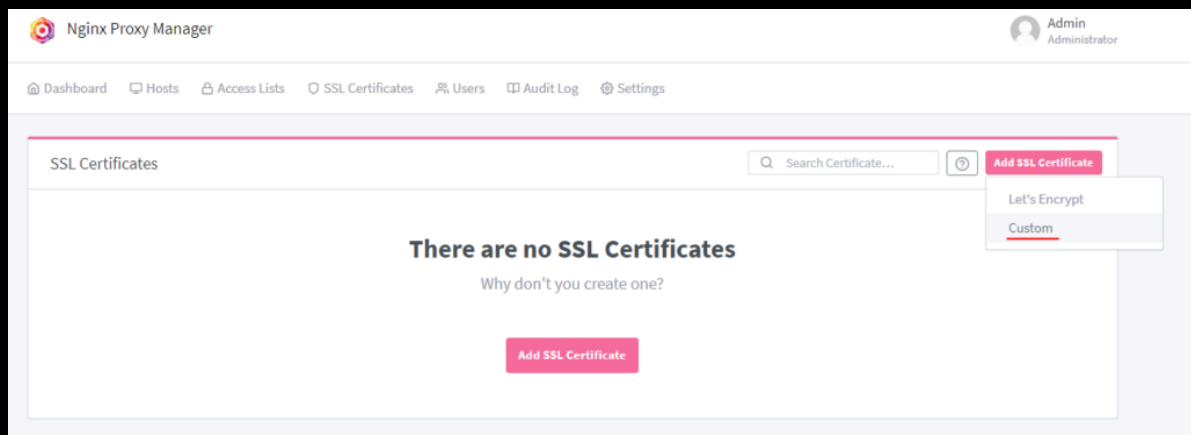
```
-----BEGIN RSA PRIVATE KEY-----
```

```
... ..
```

```
-----END RSA PRIVATE KEY-----
```

on your key.pem.

**Step 4:** Go back to Nginx Proxy Manager and go to the SSL Certificates section. Click the Add SSL Certificate button. Select "Custom".



Enter the name as your domain. Upload key.pem as Certificate Key and cert.pem as the certificate.

### Add Custom Certificate ✕

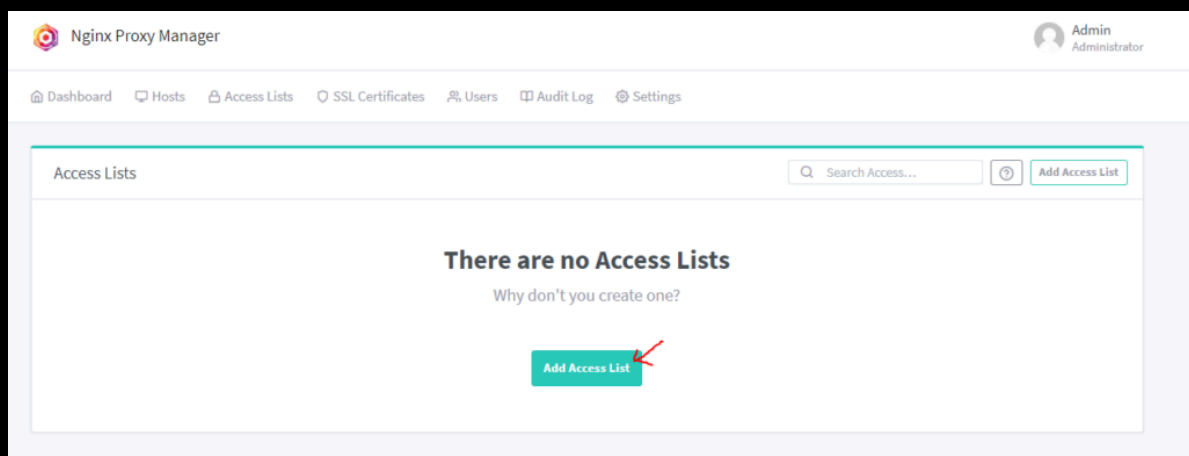
⚠ Key files protected with a passphrase are not supported.

**Name \***

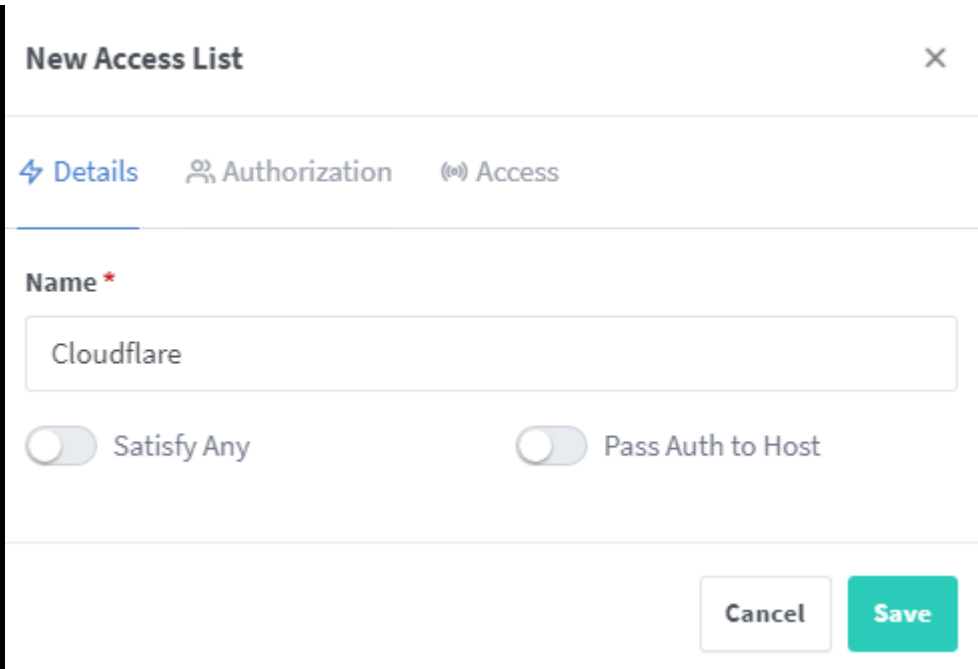
  
**Certificate Key \***   
**Certificate \***   
**Intermediate Certificate**

Click Save.

**Step 5:** Go to the Access Lists section on Nginx Proxy Manager. Click the Add Access List button.



Enter Cloudflare as Name.



**New Access List** ×

[↩ Details](#) [👤 Authorization](#) [🔊 Access](#)

**Name \***

Cloudflare

Satisfy Any  Pass Auth to Host

Click the Add button around 30 times.

Add Cloudflare IPs under the Access Section. You may visit this page for [the IP Ranges used by Cloudflare](#).

After entering any IP on the Access section, DO NOT CLICK the Add button again; otherwise, everything you input will be erased.

Press the Save button when everything is done.

## IPv4

103.21.244.0/22

103.22.200.0/22

103.31.4.0/22

104.16.0.0/13

104.24.0.0/14

108.162.192.0/18

131.0.72.0/22

141.101.64.0/18

162.158.0.0/15

172.64.0.0/13

173.245.48.0/20

188.114.96.0/20

190.93.240.0/20

197.234.240.0/22

198.41.128.0/17

IPv6

2400:cb00::/32

2606:4700::/32

2803:f800::/32

2405:b500::/32

2405:8100::/32

2a06:98c0::/29

2c0f:f248::/32



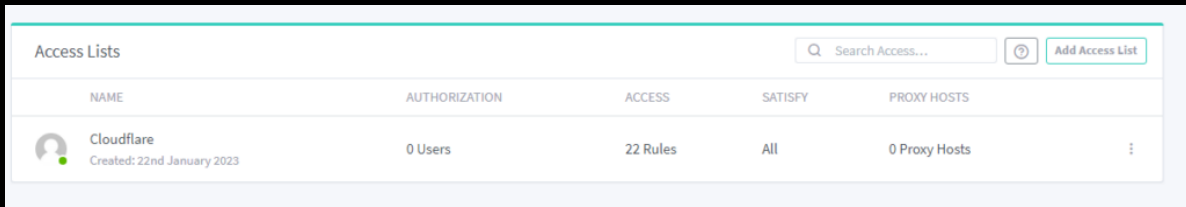
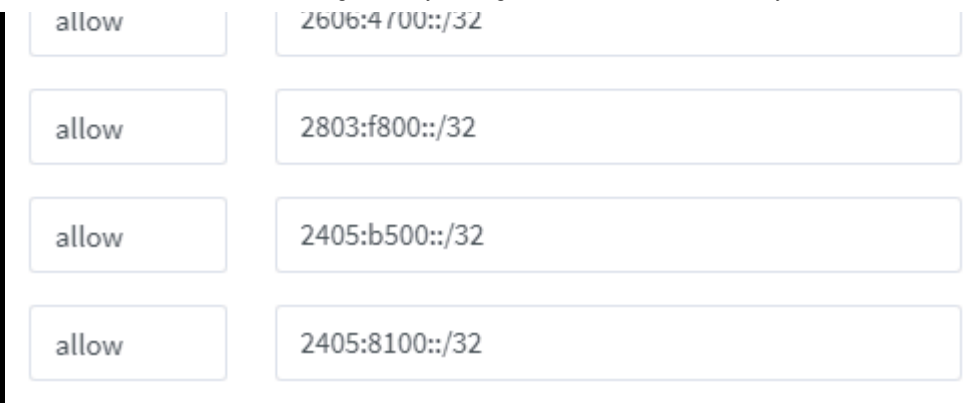
### Edit Access List



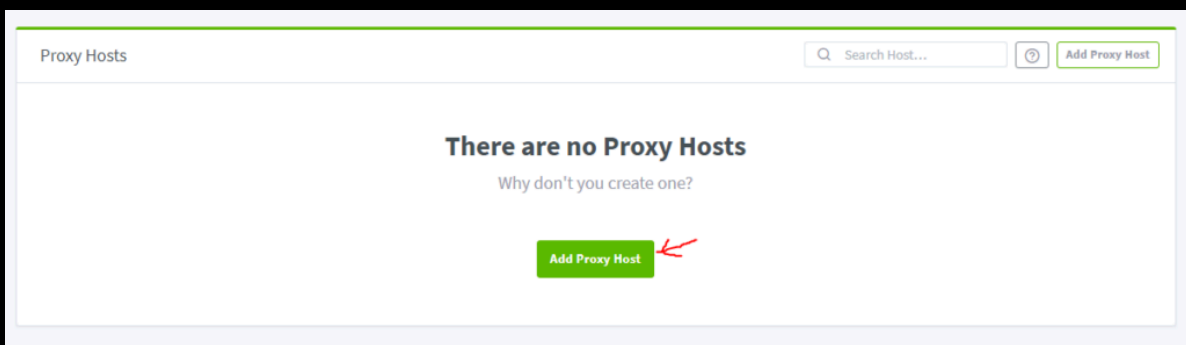
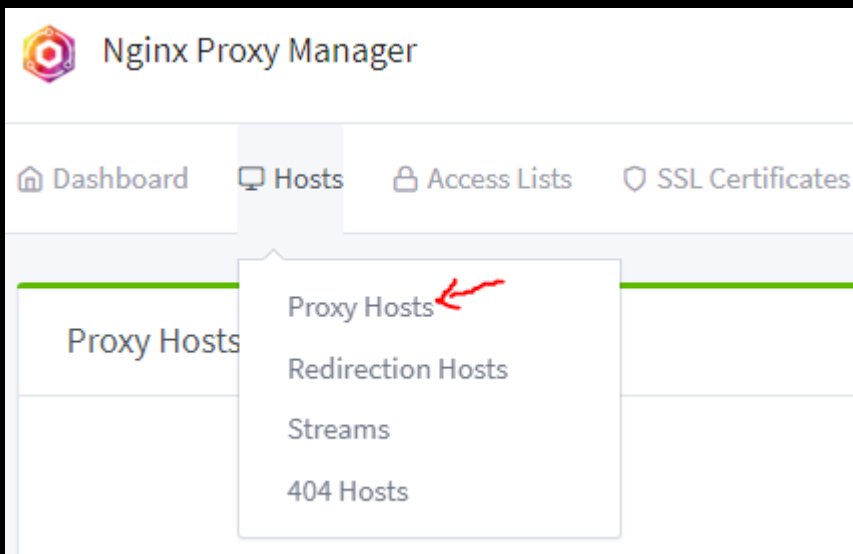
⚡ Details   🔑 Authorization   🔊 Access

#### IP Address Whitelist/Blacklist via [Nginx HTTP Access](#)

allow	103.21.244.0/22
allow	103.22.200.0/22
allow	103.31.4.0/22
allow	104.16.0.0/13
allow	104.24.0.0/14
allow	108.162.192.0/18
allow	131.0.72.0/22
allow	141.101.64.0/18
allow	162.158.0.0/15
allow	172.64.0.0/13
allow	173.245.48.0/20
allow	188.114.96.0/20
allow	190.93.240.0/20
allow	197.234.240.0/22
allow	198.41.128.0/17
allow	2400:cb00::/32
..	.....



**Step 6:** Move to the Proxy Hosts section on the Nginx Proxy Manager. Click the Add Proxy Host button.



**Step 7:** Enter your domain name and press Tab to save.

Select HTTP or HTTPS as your Scheme.

Enter your Forward Hostname / IP and Forward Port.

Change the Access List to Cloudflare.

Do not click the block common exploits button at this moment. You must ensure you can access your website before turning it on.

For some web services, such as code-server, you may need to turn on Websockets Support. By default, it is turned off.

**New Proxy Host** [X]

Details Custom locations SSL Advanced

**Domain Names \***

silicon.blog

**Scheme \*** **Forward Hostname / IP \*** **Forward Port \***

https wordpress 8443

Cache Assets  Block Common Exploits

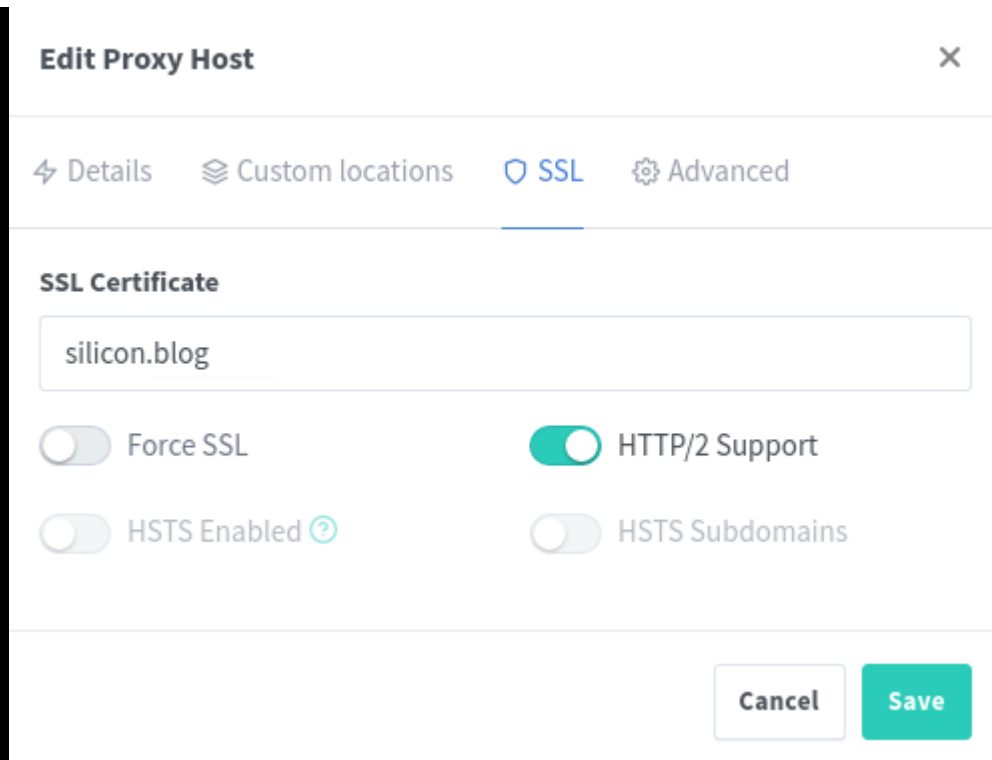
Websockets Support

**Access List**

Cloudflare

Cancel Save

**Step 8:** Add your domain's SSL certificate to the SSL section. It is optional to enable HTTP/2 Support.



**Edit Proxy Host** ✕

↩ Details 📁 Custom locations 🛡 SSL ⚙ Advanced

**SSL Certificate**

silicon.blog

Force SSL  HTTP/2 Support

HSTS Enabled ?  HSTS Subdomains

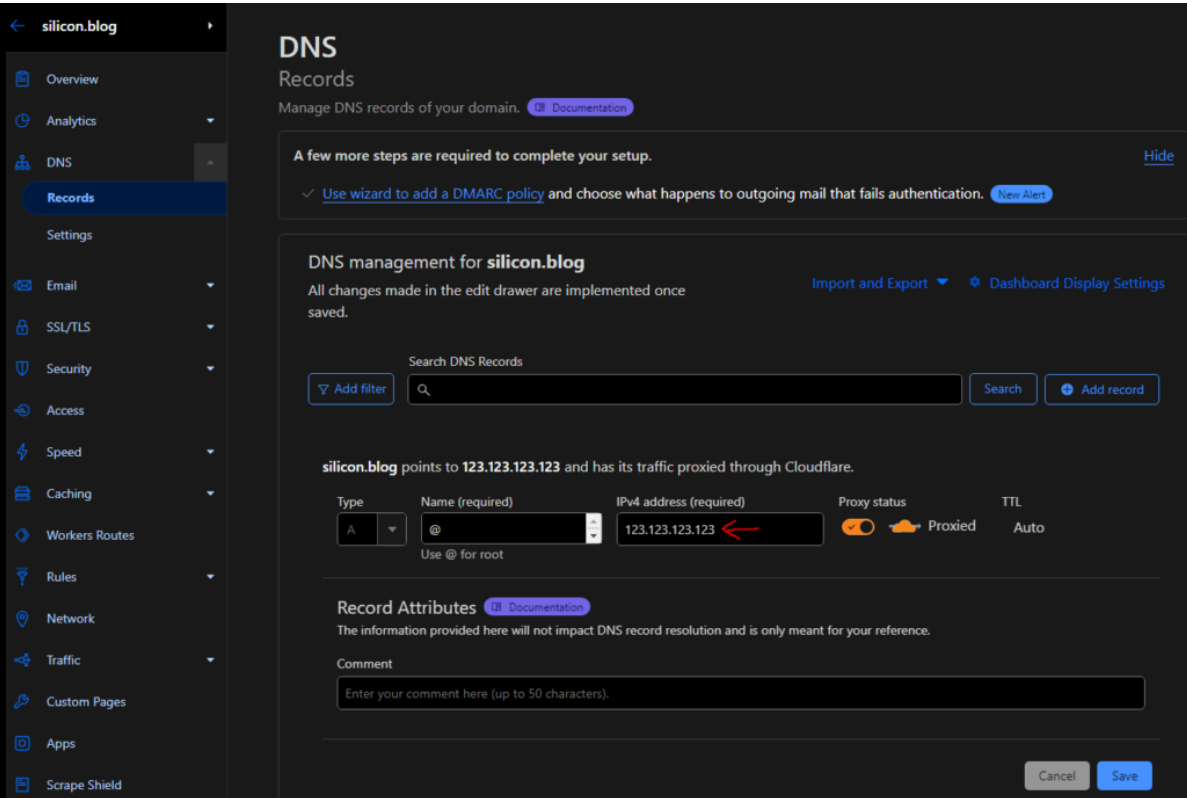
Cancel Save

**Step 9:** Go back to your Cloudflare dashboard.

Add an A record to your domain if you are using a static IP.

Instead, if you are using a dynamic IP address and you want to use a DDNS. Create a CName record.

Remember to turn on the Proxied option. Click the save button to take effect. It may take at most 1 day to update your DNS record worldwide.



**Step 10:** Ensure you have forwarded port 80/443 to Nginx Proxy Manager on your router/ switch. Since different brands will have different configurations, you may need to Google it and set it up yourself.

If you are using Oracle Cloud, remember to configure your firewall to allow incoming traffic by

```
sudo iptables -I INPUT -j ACCEPT
sudo su
iptables-save > /etc/iptables/rules.v4
exit
```

If you can access your domain after a few hours, congratulations, you successfully combined Nginx Proxy Manager with Cloudflare!

Check out [this article](#) on self-hosting a WordPress and reverse proxy it with Nginx Proxy Manager.

Have a look of [this article](#) for how to hide your HTTP/HTTPS on the public Internet using Cloudflare Tunnel with Nginx Proxy Manager.

If you want more advanced techniques, try to [configure Nginx Proxy Manager for load balancing](#) or [configure Nginx Proxy Manager to create a failover WordPress server on cPanel](#).

## 16 thoughts on “How to combine Nginx Proxy Manager with Cloudflare to access your websites/ web services securely”



**W Yoder says:**

April 13, 2023 at 9:11 pm

Excellent document! Thank you very much for putting this together for us, it worked perfectly on the first try for me 😊

One minor comment is that after you create the SSL cert using the key downloaded from Cloudflare, you need to specify that certificate as the SSL certificate in the proxy host that is created in steps 7 & 8, otherwise Cloudflare will give you an Invalid Certificate error when you try to hit your domain.

Thanks again for this information, it was excellent and as you say, very quick to get up and running.

[Reply](#)



**Silicon says:**

April 16, 2023 at 3:27 pm

Dear Yoder,

Thanks for your comment. 😊

It seems that I missed 1 image in this post. I will update it later.

Btw, I found an issue with Nginx Proxy Manager after version 2.9.19. You may have issues when you try to handshake with a website involved in TLSv1.3 (You can confirm it by `curl -k`

"https://your\_internal\_service\_ip:443" -H 'Host: your\_service\_public\_domain\_name' -http1.1). I have not found a workaround yet. You may need to downgrade to NPM v2.9.19 if you have similar issues.

[Reply](#).



**Rob says:**

May 15, 2023 at 6:14 pm

Did you ever figure out a workaround to the handshake problem with tls1.3?

[Reply](#).



**Silicon says:**

May 16, 2023 at 12:01 pm

Dear Rob,

Thanks for your comment.

Are you trying to combine Headscale with Cloudflared (Cloudflare Tunnel) and Nginx Proxy Manager? If that is the case, I think the issue is on the Cloudflare side. They claim they have enabled WebSockets for Cloudflare Tunnel, but even though I tried the same configuration with Apache / Nginx, Headscale still could not work. I could not register any devices through Headscale. Eventually, I gave Cloudflare Tunnel up. I exposed my 443 port and proxied the WebSockets through Cloudflare (combing with NPM). Everything works properly now.

However, be careful to not violate the ToS of Cloudflare. If you have high traffic proxied by Cloudflare through WebSockets with non-HTML contents, they may temporarily suspend your domain until you change it back to non-Proxied.

#### 2.8 Limitation on Serving Non-HTML Content

The Service is offered primarily as a platform to cache and serve web pages and websites. Unless explicitly included as a part of a Paid Service purchased by you, you agree to use the Service solely for the purpose of serving web pages as viewed through a web browser or other functionally equivalent applications and rendering Hypertext Markup Language (HTML) or other functional equivalents. Use of the Service for

serving video (unless purchased separately as a Paid Service) or a disproportionate percentage of pictures, audio files, or other non-HTML content, is prohibited.

If that is not the case, you may give v2.9.18 or v2.9.19 a try. It seems everything is fine on that version. Or you may have a look at this link:

<https://github.com/NginxProxyManager/nginx-proxy-manager/issues/2822>. It seems Jebabin solved that issue on v2.10.2.

[Reply](#)



**Rob says:**

May 16, 2023 at 3:57 pm

Appreciate the reply. I'm actually not trying to use Cloudflare Tunnels in this case. I followed the guide you presented, plus the comment about setting the CF Origin Cert as the Cert for the Proxy Host. When I activate the Proxy Host with all the settings I get a 403 Forbidden (Openresty) Error. If I switch back to the default Public Access List it works fine. I'm struggling to figure out what is causing the error. If you happen to have any ideas it would be greatly appreciated. Thanks again for the reply!

[Reply](#)



**Silicon says:**

May 18, 2023 at 3:43 am

Dear Rob,

It may be related to your internal firewall settings.

Try to add your public IP/32 to the whitelist first.

Then give your internal IP /24 (let's say 192.168.1.0/24) a try.

If you use Docker to host your web service, add 172.17. 0.0/16 to the whitelist.

Let me know if the above IP ranges solve your issue. 😊

By the way, I have created other tutorials related to Nginx Proxy Manager starting from scratch. I could not find any issue with the Cloudflare filter.

The only time I encountered a 403 issue was when I used the wrong scheme (using HTTP on an HTTPS site).



[Reply](#)

---



**Horst says:**

December 5, 2023 at 3:40 pm

Great post but I still have the problem that the website still gives me the 1000 (DNS points to prohibited IP) Cloudflare Error and I don't know why I did everything according to the tutorial

[Reply](#)

---



**Silicon says:**

January 9, 2024 at 7:02 pm

Hello Horst, Sorry for the late reply. I was taking a vacation for a whole month.

Probably you are pointing to a server protected by cloudflare (Cloudflare IP) causing error 1000.

Have you tried to point your dns record to another IP (origin server's IP)?

[Reply](#)

---



**Infinimonster says:**

January 28, 2024 at 10:38 pm

Hello, thanks for this post. I currently try to containerize an own php application and everything went good so far.

Now my issue is, that i get the error "521: Webserver down" aka "Connection Refused" when i have cloudflare proxy enabled. If i disable cloudflare proxy everything works fine but disabeling it, isn't what i want as users can just do an DNS lookup on the domain to find out the real server ip and then potentially DDOS my Site....

I would appriciate it if anyone can help me. Telegram:  
[@Infinimonster](#)

[Reply](#)

---



**Silicon says:**

February 1, 2024 at 7:33 pm

Dear Infinimonster,

Have you tried to whitelist the cloudflare IP on your local .htaccess file and nginx proxy manager?

Also, try to set you domain's SSL/TLS encryption mode to FULL on Cloudflare if you set it to Full (strict).

[Reply](#).



**Coad says:**

February 3, 2024 at 3:37 am

Dear Silicon,

Thank you for these god sent blogs.

I've followed your steps and encounter the 403 Forbidden issue if I use the Cloudflare access list.

No issue if change the access list you publicly accessible.

Do you have any ideas what could be the cause?

Thank you

[Reply](#).



**Silicon says:**

February 4, 2024 at 6:38 pm

Dear Coad,

Cloudflare updated their ipv6 list on 28th Sep 2023. You may need to add 2405:b500::/32 to your nginx proxy manager's whitelist.

Your domain should be proxied. Is your domain being proxied by Cloudflare?

Let me know if you need any help.

[Reply](#).



**Coad says:**

February 10, 2024 at 7:58 pm

Dear Silicon,

- 2405:b500::/32 was added.
- domain being proxied

No clue. getting 403. But I think it's fine to use it publicly.

[Reply](#)



**Silicon says:**

February 10, 2024 at 8:00 pm

Dear Coad,

1. Try to disable Browser Integrity Check on your Cloudflare domain dashboard first.

<https://community.cloudflare.com/t/api-403-after-enabling-cloudflare/108078>

2. Try to add

proxy\_hide\_header X-Powered-By;

on your Nginx Proxy Manager's Advanced section.

3. If it doesn't work, also try to add

proxy\_ssl\_server\_name on;

proxy\_ssl\_name \$proxy\_host;

on your Nginx Proxy Manager's Advanced section.

What's your Nginx Proxy Manager version?

If none of these methods work, it may relate to the version of your Nginx Proxy Manager.

I am using v2.9.19.

[Reply](#)



**Kenneth says:**

May 2, 2024 at 3:50 am

I have done everything write but the certificate says Your connection to this site isn't secure, any idea how to solve this?

[Reply](#)



**Silicon says:**

May 3, 2024 at 3:53 am

Dear Kenneth,

Try to go to your Cloudflare domain configuration page -> SSL/TLS -> Overview -> set SL/TLS encryption mode to full and see if the error message disappears.

Regards,  
Silicon

[Reply](#)

---

## Leave a Reply

COMMENT \*

NAME \*

EMAIL \*

WEBSITE

The reCAPTCHA verification period has expired. Please reload the page.

Post Comment

©2024 Silicon's blog