

Forum:[Hack Forums](#)

Thread: [\[Warriors\] Create your own reverse Proxy](#)

guardian - December 29, 2020, 7:58 am

There are numerous situations, where a reverse proxy for your web server can be useful
It is pretty easy to setup, however, depending on your operation, you might need some additional configuration

We will set up an Nginx on our server with IP 5.206.xxx.xxx, which will act as a reverse proxy and pass our requests to 1.1.1.1 (Cloudflare App)

Installing Nginx

Code `apt -y install nginx`

After a successful installation of nginx, head over to the configuration file

Code `nano /etc/nginx/sites-enabled/default`

Search for location and remove the following line:`try_files $uri $uri/ =404;`

Then replace it with

Code `proxy_pass https://1.1.1.1`

Instead of 1.1.1.1 you could use another site as well, maybe your own site, in order to hide it's IP?
Or a site you always want to access with the servers IP? (NOTE: You will have to take care of the forwarded by header then, which would reveal your real IP)

Now let's test the configuration

Code `root@guardian:/etc/nginx/sites-available# nginx -t`

nginx: the configuration file /etc/nginx/nginx.conf syntax is ok

nginx: configuration file /etc/nginx/nginx.conf test is successful

Restart and reload nginx and we are ready to go :)

Code `systemctl restart nginx`

`systemctl reload nginx`

Now on to the test, our server IP should now show the contents of 1.1.1.1, when accessed and ...

It works! Our Nginx server now forwards all requests to 1.1.1.1

AeS0p - February 25, 2021, 10:37 pm

Great post! thanks friend!

duduch1995 - April 14, 2021, 5:54 pm

By doing this, does the server with the hidden ip (target server) not receive the attacks but the first one receive them?

Criptex - April 14, 2021, 5:58 pm

Very short and sweet tutorial. Thanks for sharing.

guardian - April 14, 2021, 11:06 pm

(Apr 14, 2021 05:54 PM)duduch1995 Wrote: [\[CITE\]](#) By doing this, does the server with the hidden ip (target server) not receive the attacks but the first one receive them?

This depends on the attacks and how the server is set up. What kind of attacks are you talking about? DDoS? Hacking?

duduch1995 - April 15, 2021, 3:16 am

(Apr 14, 2021 11:06 PM)guardian Wrote: [\[CITE\]](#) This depends on the attacks and how the server is set up. What kind of attacks are you talking about? DDoS? Hacking?

Im talking about DDoS Attacks yes

if for example I have a server that is DDoS protected and I do this method. Can he protect the other server?

thanks for your help

guardian - April 15, 2021, 3:46 am

(Apr 15, 2021 03:16 AM)duduch1995 Wrote: [\[CITE\]](#) Im talking about DDoS Attacks yes

if for example I have a server that is DDoS protected and I do this method. Can he protect the other server?

thanks for your help

Absolutely. But you have to do a little more, in order to protect it than simply setting up a reverse proxy. You can use a reverse proxy as a so called "load balancer". The load balancer basically spreads the requests across your cluster of servers. It is hard to down a well set up load balancer, because it simply does not handle 'heavy' requests. You should also configure it to filter requests somehow. Requests that the system receives that are detected as malicious, should not be forwarded to your back end. You can also use some kind of captcha on your reverse proxy, like cloudflare does. A solved captcha generates a new session that lets the user access the website through the reverse proxy.

But preventing DDoS is pretty much impossible, you can only make it harder. If someone has enough power and some good endpoint to attack, he will probably be able to do it. Just try to make it as hard as possible for them, so most script kiddies cannot afford downing your site. As long as you don't get in trouble with the big boys, you should be good.

Here is a short summarization of some basic DDoS prevention methods:

(I assume you are not building some super big project that will be at high risk for DDoS attacks)

- Build a server cluster that consists of multiple servers that have enough power to handle your requests and also a bit more, in case someone should be able to get through with their bots
- Use a reverse proxy as a load balancer, I recommend Nginx
- Configure a WAF (= Web Application Firewall) with Nginx, I recommend 'Naxsi'
- Maybe use some sort of captcha solution or have one ready that you activate in case of an attack,

it is not too hard to even code your own :)

- Use a super strict firewall on your back end server cluster, you can use the iptables command for that, only allow traffic that should be allowed, for instance: allow ssh connections so that you can connect to the server (I also recommend port knocking and using a non-common port for it, adds some extra security), allow traffic from and to your reverse proxy and localhost (i.e. for database stuff), this should be adapted, depending on your needs, the point is that your server should seem dead from the outside, because when someone finds out the IP of your server(s), they have more possible attack points for a DDoS

- Hiding your IP is important, because as I mentioned above, if someone finds out the true IP of your server and you did not set your firewall up correctly, they have a lot more options to attack you, so basically the reverse proxy would be pointless, maybe it would keep some skids away, but that is pretty much it, I already wrote a tutorial, about how someone can find the true IP behind cloudflare, this also applies for reverse proxies you set up on your own, maybe [check that out](#)

- Make sure to make the load requests can generate as small as possible, close database connections after the script is done, use prepared statements, load stuff from external sources ... list is endless, you have to find your way for that, as I don't know what kind of application you want to host

- Use some kind of filtering in your back end as well, even when using Naxsi or some other WAF on your front end, that way you have 2 instances checking the requests

- Make sure to log important stuff!! When a DDoS occurs and you are for some reason not able to defend yourself, you can view the log files and find out what you could have done to prevent it

That is some basic stuff that you as an admin of a site should take care of to prevent DDoS. There is other stuff as well, but I don't want to make this post too long and I also don't know what kind of application we are talking about. Hope I could help you.

duduch1995 - April 15, 2021, 4:44 am

So thank you for all this information, so for my part I want to integrate a reverse proxy for a FiveM server, it is not a web server but a connection IP and a specific port so what I want is mainly that the attacks are redirected to the Anti DDoS of my dedicated server and that user connections can pass all that, my AntiDDoS protection already manages this basic system so what I was thinking is that I could use this system to protect my second server (Fivem server)

But in any case I will try to focus on all that I thank you in advance for this tutorial and for all these explanations it will help me a lot for my current project and subsequently in my future projects

guardian - April 15, 2021, 5:32 am

(Apr 15, 2021 04:44 AM)duduch1995 Wrote: [\[CITE\]](#) So thank you for all this information, so for my part I want to integrate a reverse proxy for a FiveM server, it is not a web server but a connection IP and a specific port so what I want is mainly that the attacks are redirected to the Anti DDoS of my dedicated server and that user connections can pass all that, my AntiDDoS protection already manages this basic system so what I was thinking is that I could use this system to protect my second server (Fivem server)

But in any case I will try to focus on all that I thank you in advance for this tutorial and for all these explanations it will help me a lot for my current project and subsequently in my future projects

This is a completely different scenario then. In this case the most important thing is your firewall and load balancer. Make sure to meticulously configure your firewall and reverse proxy. The stuff I told you about the firewall still applies. Only run necessary services and only allow those. Reject packets that are not received by a trusted source (i.e. your reverse proxy) and configure the reverse proxy to have some DDoS prevention going on. Don't forget to log, not too much, because this can also slow down the server, but essential stuff should be written to a log file.

Shadow_Cloud - April 16, 2021, 11:40 pm

[guardian](#) has made some really good points on preventing DDOS earlier, the one thing I'd like to

add is rate limiting by incoming IP on your proxy, you could detect an excessive amount of requests from a specific IP and either slow them down artificially or just drop the packets completely.

There's some really useful info on rate limiting here >
<https://www.nginx.com/blog/rate-limiting-nginx/>

In the case of the FiveM server (I don't really know anything about it) do you have a specific request to initiate the connection initially? Because you could potentially check for the expected value and drop anything else that's not established. Its not foolproof but it should help quite a bit.

darkhax0r - April 25, 2021, 12:51 pm

i got this error can anyone please solve this ?

```
nginx: [emerg] "proxy_pass" directive is not allowed here in /etc/nginx/sites-enabled/default:1
nginx: configuration file /etc/nginx/nginx.conf test failed
```

Payne - May 30, 2021, 12:09 am

Great post friend thank you so much

guardian - May 30, 2021, 6:59 am

(Apr 25, 2021 12:51 PM)darkhax0r Wrote: [\[CITE\]](#) i got this error can anyone please solve this ?

```
nginx: [emerg] "proxy_pass" directive is not allowed here in /etc/nginx/sites-enabled/default:1
nginx: configuration file /etc/nginx/nginx.conf test failed
```

Seems like you used the wrong config file.

\$(5)\$ - October 23, 2021, 4:12 pm

I love the way you properly formatted this tutorial with the code tags. It made it very easy to read and follow.

guardian - October 23, 2021, 10:14 pm

(Oct 23, 2021 04:12 PM)\$(5)\$ Wrote: [\[CITE\]](#) I love the way you properly formatted this tutorial with the code tags. It made it very easy to read and follow.
Thanks a lot! Glad you liked it and thanks for the feedback.

asad50 - October 28, 2021, 7:34 pm

Thank you for the method man, I will try it

guardian - October 28, 2021, 10:11 pm

(Oct 28, 2021 07:34 PM)asad50 Wrote: [\[CITE\]](#) Thank you for the method man, I will try it
Np, let me know if everything worked out.

helikai - October 29, 2021, 11:47 pm

Good post , thank you so much!

guardian - October 30, 2021, 12:11 am

(Oct 29, 2021 11:47 PM)helikai Wrote: [\[CITE\]](#) Good post , thank you so much!
Glad you liked it! What are you going to use your reverse proxy for?

Howmygoad - November 13, 2021, 1:20 pm

Thanks for sharing its helpful

guardian - November 14, 2021, 3:30 am

(Nov 13, 2021 02:20 PM)Howmygoad Wrote: [\[CITE\]](#) Thanks for sharing its helpful
Glad to hear that it helped you man.

jamoncito - November 26, 2021, 4:42 am

thanks I will give it a try

guardian - November 26, 2021, 5:54 am

(Nov 26, 2021 05:42 AM)jamoncito Wrote: [\[CITE\]](#) thanks I will give it a try
No problem man. Should you face any problems, feel free to post them in this thread & I will do my best to help you out.

JohanLiebert - November 28, 2021, 9:52 pm

this is great thanks for sharing

guardian - November 28, 2021, 10:30 pm

(Nov 28, 2021 10:52 PM)JohanLiebert Wrote: [\[CITE\]](#) this is great thanks for sharing
No problem, glad you liked it! Let me know, if you have any further questions.

The_Defiant_One - January 5, 2022, 10:27 am

Very informative tutorial buddy. Thanks for sharing!

SIM-4391894 - January 7, 2022, 8:17 pm

is this how the tor2web gateway service like onion.to and onion.ws created? @guardian

SkardeveosPALAIA - January 9, 2022, 8:56 am

high quality post. Appreciated