

Forum:[Hack Forums](#)

Thread: [How to bypass strict dpi firewall](#)

raspito - August 9, 2024, 9:34 pm

I'm trying to get around a Fortigate firewall that's doing some serious SSL inspection. It basically pretends to be the recipient, decrypts the traffic, checks it out, and then re-encrypts it before sending it on. I managed to get the root certificate through some means (let's just say it wasn't easy), so I know what's going on with the traffic.

Here's what I've tried so far:

Psiphon: Works pretty well! I noticed that when using Psiphon, my traffic is encrypted and passes through without any issues. However, I'm not 100% sure why it's working so smoothly, and I want to explore other options that might be more reliable or faster.

SOCKS over HTTPS: I got this working, but it was glitchy. Sometimes the connection would drop or become unstable, so it's not really reliable for me.

Now, I'm considering a few other tools and would love some advice on which might work best and why. Here are the options I'm looking at:

Hysteria2
wstunnel
stunnel
httptunnel
obfsproxy
OpenVPN using HTTPS
Trojan
SoftEther

Given that the Fortigate is doing SSL MITM stuff, which of these tools do you think would be the most reliable for getting around this kind of inspection? I'm especially interested in knowing if any of these options might work as well as or better than Psiphon, and why SOCKS over HTTPS was so glitchy. Basically the Fortigate pretends to be the recipient, decrypts the traffic, re encrypts it with its own certificate, then sends it to the client. When I go into Wireshark while using Psiphon I just see TLSv1.2 and TCP traffic. I'd love to know which of these would work, which wouldn't, and why. Also can I use a self signed certificate?

P.S: I encountered a weird thing 2 days ago. I tried using stunnel to access a remote website on port 1194 that wasn't forwarded and for some reason it said it was blocked, even though the server was unblocked and I could access it fine from my home computer. I was connected to 127.0.0.1:29988 which took that traffic sending it out to the remote server on port 443 and then forwarded to port 1194. I'm guessing it's because I was using a self signed certificate but not sure. Any help would be appreciated, sorry this is a long question.

shadowcrow - August 13, 2024, 3:17 am

Have you tried tunnelshell with fragmented packets?

diabloshulu - November 4, 2024, 1:53 am

It seems, we have the same problem.

Let me introduce the problems I am currently encountering.

The target is a server hosted by cloudflare, using IPS firewall interception, and all ports do not allow direct IP access?

my thoughts:

1.Find all server sources ?(to complete)

2.Traffic analysis with packet capture,Find the real host behind the defense and log in by IP

So, the advice I can give you is to try to find more information hidden behind the host and then send it out.

raspito - November 11, 2024, 8:00 am

(Nov 4, 2024 02:53 AM)diabloshulu Wrote: [\[CITE\]](#) It seems, we have the same problem.

Let me introduce the problems I am currently encountering.

The target is a server hosted by cloudflare, using IPS firewall interception, and all ports do not allow direct IP access?

my thoughts:

1.Find all server sources ?(to complete)

2.Traffic analysis with packet capture,Find the real host behind the defense and log in by IP

So, the advice I can give you is to try to find more information hidden behind the host and then send it out.

Finally got it working with trojan-go its fast and low ping.