

Forum:[Hack Forums](#)

Thread: : [Looking for Someone to Assist with C2 Server Port Configuration Issue](#)

Simphiwe Macu - September 4, 2026, 10:37 am

Hello,

I am currently setting up a C2 server on a VPS and need assistance with a port-related issue preventing implant connections.

Current Setup:

- VPS IP: [YOUR_VPS_IP]
- C2 Framework: Metha (Python/Flask)
- Server is running and listening on port 5000 (HTTP)
- Port forwarding rule (iptables) is in place to redirect traffic from port 443 to port 5000
- The VPS provider has confirmed port 443 is open on their network firewall

Issue:

- Connections from my local computer to [https://\[YOUR_VPS_IP\]:443/api/v2/check](https://[YOUR_VPS_IP]:443/api/v2/check) are failing with Connection refused or ERR_CONNECTION_RESET
- Testing locally on the VPS with `curl -v http://127.0.0.1:5000/api/v2/check` returns `{"status":"no_data"}` – confirming the server itself is working correctly

What I've Tried:

- Verified the server is listening on 0.0.0.0:5000
- Confirmed iptables rule is active (tcp dpt:443 redir ports 5000)
- Generated SSL certificates and attempted to use socat as an SSL proxy
- Tested from both inside and outside the VPS

Request:

I need help diagnosing why external connections to port 443 are not reaching the server on port 5000. Please let me know if you require any additional details or logs.

Thank you

Shapeless - September 4, 2026, 11:15 am

so this is a classic issue i had this issue when i setup websocket connections over ssl, im almost sure this is your issue problem is 443 is https, and the backend you have is most likely http, you wrote it actually yourself

what you need is a reverse proxy and config it in nginx / caddy to be setup properly to send your data comprehensible to the flask backend.

Simphiwe Macu - September 4, 2026, 12:13 pm

Thanks I think you're right. I've been trying to hack it together with iptables and socat, but a proper reverse proxy is clearly the fix.

Do you have a quick nginx or Caddy config example that would proxy HTTPS on 443 to HTTP on 5000?

Appreciate it.

DramaKing - September 5, 2026, 8:15 am

The iptables rule seems like nonsense, but I don't know why socat didn't work. Regardless, a reverse proxy like Traefik is the way to go. Here's a YAML config:

Code # traefik.yml

entryPoints:

web:

address: :80

http:

redirections:

entryPoint:

to: websecure

scheme: https

permanent: true

observability:

accessLogs: true

metrics: true

tracing: false

websecure:

address: :443

services:

metha-c2-service:

loadBalancer:

servers:

- url: "http://127.0.0.1:5000" # Points to your app on port 5000

certificatesResolvers:

myresolver:

acme:

email: your-email@example.com

storage: acme.json

httpChallenge:

used during the challenge

entryPoint: webCode # dynamic.yml

http:

routers:

metha-c2-router:

rule: "Host(`://example.com`)" # Ensure this domain points to your server's public IP

entryPoints:

- "websecure"

service: "metha-c2-service"

tls:

certResolver: "myresolver"

services:

metha-c2-service:

loadBalancer:
servers:
- url: "http://127.0.0.1:5000"

Simphiwe Macu - September 5, 2026, 1:24 pm

Thanks bro for sharing the Traefik config — it looks like a clean way to handle SSL and routing to Metha on port 5000.

On the payload side, we're looking for a builder and crypter that can:

- Bypass Windows Defender and SmartScreen
- Support HTTPS callback to the server
- Allow PDF decoy binding (target opens a PDF while the .exe runs silently)
- Work with .exe or .vbs outputs

The PDF decoy is typically done by binding the payload with a real PDF using an injector, then applying a PDF icon and hiding the .exe extension.

If you have a working setup or can point us in the right direction, we'd appreciate it.

Thanks.

DramaKing - September 6, 2026, 5:29 am

(Sep 5, 2026 01:24 PM)Simphiwe Macu Wrote: [\[CITE\]](#) Thanks bro for sharing the Traefik config — it looks like a clean way to handle SSL and routing to Metha on port 5000.

On the payload side, we're looking for a builder and crypter that can:

- Bypass Windows Defender and SmartScreen
- Support HTTPS callback to the server
- Allow PDF decoy binding (target opens a PDF while the .exe runs silently)
- Work with .exe or .vbs outputs

The PDF decoy is typically done by binding the payload with a real PDF using an injector, then applying a PDF icon and hiding the .exe extension.

If you have a working setup or can point us in the right direction, we'd appreciate it.

Thanks.

That? Easy. Getting it to open with no file extension? Problem. Again, the payload will have to be built from scratch to your spec.

Simphiwe Macu - September 6, 2026, 9:36 am

You're right the payload needs a clean rebuild. I've tried, but it still doesn't connect. Server is reachable (curl works), but payload logs show nothing.

tokzhdanov - September 7, 2026, 11:01 am

Fill in your server's IP address and the times of failed connection attempts (in UTC time) — this makes it easier for them to match the records.