

Forum:[Hack Forums](#)

Thread: [Exposing Evilginx Locally via Cloudflare Tunnel \(Localhost Public HTTPS\)](#)

violontselos - March 11, 2026, 3:03 am

Evilginx Setup on Proxmox VM with Cloudflare - config.json and PKCS#8 Key Error

Hello everyone,

I am currently working on a project for educational purposes and would appreciate some guidance on a setup I am trying to build.

My Setup:

I have a mini PC running Proxmox.

I've created an Ubuntu VM on Proxmox (2GB RAM, 1 CPU, 20GB Disk).

I am trying to set up Evilginx within this VM.

The goal is to expose Evilginx to the internet through Cloudflare.

I am accessing the Proxmox host and the VM from my main computer via the local network.

I've run into a couple of issues where I'm not sure if I'm doing things correctly, and I'm also getting a specific error.

1. Doubts about config.json

I'm not entirely sure if I have configured my config.json file correctly for use with Cloudflare. Here is my current configuration:

JSON

```
{
  "blacklist": {
    "mode": "unauth"
  },
  "general": {
    "autocert": false,
    "bind_ipv4": "127.0.0.1",
    "dns_port": 53,
    "domain": "mydomain.site",
    "external_ipv4": "127.0.0.1",
    "https_port": 443,
    "ipv4": "",
    "unauth_url": "youtube.com/watch?v=dQw4w9WgXcQ"
  }
}
```

Is this configuration correct, especially the bind_ipv4 and external_ipv4 settings, when the intention is to use Cloudflare as a reverse proxy?

2. Private Key Parsing Error

I am encountering a problem with the private key I obtained from Cloudflare's Origin Server

SSL/TLS certificate. When I place the ca.key and ca.crt in the ~/.evilginx/crt/ directory, I get the following error upon starting Evilginx:

```
[09:07:36] [!!!] certdb: x509: failed to parse private key (use ParsePKCS8PrivateKey instead for this key format)
```

Here's the content of my ~/.evilginx/crt directory:

```
root@iakovos:~/.evilginx/crt# ls
```

```
ca.crt ca.key cert.csr email.txt sites
```

This error seems to suggest a format mismatch with the private key.

Questions:

Is this overall setup (Proxmox -> Ubuntu VM -> Evilginx -> Cloudflare) a viable way to achieve my goal?

Could someone provide step-by-step guidance on how to resolve the private key parsing error? Is there a conversion or regeneration step I am missing?

Can you offer any corrections or suggestions for my config.json to make it work correctly with Cloudflare?

Any help or pointers in the right direction would be greatly appreciated. Thank you in advance

DramaKing - March 11, 2026, 6:46 am

(Mar 11, 2026 03:03 AM)violontselos Wrote: [\[CITE\]](#) Evilginx Setup on Proxmox VM with Cloudflare - config.json and PKCS#8 Key Error

Hello everyone,

I am currently working on a project for educational purposes and would appreciate some guidance on a setup I am trying to build.

My Setup:

I have a mini PC running Proxmox.

I've created an Ubuntu VM on Proxmox (2GB RAM, 1 CPU, 20GB Disk).

I am trying to set up Evilginx within this VM.

The goal is to expose Evilginx to the internet through Cloudflare.

I am accessing the Proxmox host and the VM from my main computer via the local network.

I've run into a couple of issues where I'm not sure if I'm doing things correctly, and I'm also getting a specific error.

1. Doubts about config.json

I'm not entirely sure if I have configured my config.json file correctly for use with Cloudflare. Here is my current configuration:

JSON

```
{
  "blacklist": {
    "mode": "unauth"
```

```

},
"general": {
  "autocert": false,
  "bind_ipv4": "127.0.0.1",
  "dns_port": 53,
  "domain": "mydomain.site",
  "external_ipv4": "127.0.0.1",
  "https_port": 443,
  "ipv4": "",
  "unauth_url": "youtube.com/watch?v=dQw4w9WgXcQ"
}
}

```

Is this configuration correct, especially the bind_ipv4 and external_ipv4 settings, when the intention is to use Cloudflare as a reverse proxy?

2. Private Key Parsing Error

I am encountering a problem with the private key I obtained from Cloudflare's Origin Server SSL/TLS certificate. When I place the ca.key and ca.crt in the ~/.evilginx/crt/ directory, I get the following error upon starting Evilginx:

```
[09:07:36] [!!!] certdb: x509: failed to parse private key (use ParsePKCS8PrivateKey instead for this key format)
```

Here's the content of my ~/.evilginx/crt directory:

```

root@iakovos:~/.evilginx/crt# ls
ca.crt ca.key cert.csr email.txt sites

```

This error seems to suggest a format mismatch with the private key.

Questions:

Is this overall setup (Proxmox -> Ubuntu VM -> Evilginx -> Cloudflare) a viable way to achieve my goal?

Could someone provide step-by-step guidance on how to resolve the private key parsing error? Is there a conversion or regeneration step I am missing?

Can you offer any corrections or suggestions for my config.json to make it work correctly with Cloudflare?

Any help or pointers in the right direction would be greatly appreciated. Thank you in advance
You aren't writing to config.json manually, are you? And localhost is not an external address.

Why are you using Cloudflare certs? You just dumped everything you got into that directory, apparently without a thought for what Evilginx required. All I can tell you is that Cloudflare does not provide PKCS#8. ca.key is likely the CA public key. cert.csr is clearly the Certificate Signing Request. I don't think that you have a certificate or private key.

You can check for yourself by running cat on the files. The private key should start with —BEGIN PRIVATE KEY— and end with —END PRIVATE KEY—. Or you can try <https://decoding.info/digital-signature-verifier>

Oddly enough, the Let's Encrypt certs generated by Evilginx are stored as PKCS#1 denoted by -----BEGIN RSA PRIVATE KEY-----.

