如何部署一台抗封锁的Shadowsocks-libev服务器

作者: Anonymous

日期: 2021年1月26日，星期二

更新: 2021年12月6日，星期一

English Version: *How to Deploy a Censorship Resistant Shadowsocks-libev Server*

这篇教程记录了如何安装，配置并维护一台Shadowsocks-libev服务器。 这篇教程的亮点在于， 按照这里的配置建议，你的Shadowsocks-libev服务器可以抵御各种已知的攻击， 包括来自GFW的主动探测和封锁以及partitioning oracle攻击。 我们还在教程的最后加入了有关Shadowsocks-libev部署的常见问题。 截止2021年11月7日，我们收到零星的用户报告按此教程配置的服务器仍遭到了端口封锁，我们因此在文中分享一个配置备用端口来缓解端口封锁的方法。

我们致力于更新和维护这篇教程。如果今后发现了新的针对Shadowsocks-libev的攻击，我们将在第一时间在这篇教程中加入缓解攻击的办法。 因此请考虑将这个页面加入到你的收藏夹中。 另外，我们希望这篇教程对技术小白同样友好，因此如果你在任何步骤卡住了，请联系我们，或在下方评论区留言。我们会对教程作相应改进。

安装

安装Snap应用商店

通过Snap应用商店安装Shadowsocks-libev是官方推荐的方式。

- 如果你的服务器运行Ubuntu 16.04 LTS及以上的版本，Snap已经默认安装好了。
- 如果你的服务器运行了其他的Linux发行版，你只需跟着对应的发行版安装Snap core。

现在来检测一下你的服务器已经安装了需要的`snapd`和Snap `core`:

```
sudo snap install core
```

安装Shadowsocks-libev

现在我们安装最新的Shadowsocks-libev:

```
sudo snap install shadowsocks-libev --edge
```

配置

下面是我们推荐的Shadowsocks-libev服务器配置：

```
{
    "server":["::0","0.0.0.0"],
    "server_port":8388,
    "method":"chacha20-ietf-poly1305",
    "password":"ExamplePassword",
    "mode":"tcp_and_udp",
    "fast_open":false
}
```

注意，你需要把里面的`ExamplePassword`替换成一个更强的密码。 强密码有助缓解最新发现的针对Shadowsocks服务器的Partitioning Oracle攻击。 你可以用以下命令在终端生成一个强密码：`openssl rand -base64 16`。

你还可以考虑将`server_port`的值从`8388`改为`1024`到`65535`之间的任意整数。

现在打开通过Snap安装的Shadowsocks-libev默认的配置文件：

```
sudo nano /var/snap/shadowsocks-libev/common/etc/shadowsocks-libev/config.json
```

将上方替换过密码的配置信息复制粘贴到配置文件后， 按`Ctrl + x`退出。 退出时，文本编辑器将问你`"Save modified buffer?"`，请输入`y`然后按回车键。

可以看到，通过Snap安装的Shadowsocks-libev默认的配置文件路径太长了，不便于记忆。同时默认配置路径又没有在官方文档中标出。 我们因此建议你收藏此页面，以备今后查找。

防火墙

我们使用`ufw`来管理Shadowsocks服务器的防火墙。

在基于Debian的服务器上，可以通过如下命令安装`ufw`：

```
sudo apt update && sudo apt install -y ufw
```

然后开放有关`ssh`和`Shadowsocks-libev`的端口。 请注意，以下命令假设你在`/var/snap/shadowsocks-libev/common/etc/shadowsocks-libev/config.json`中的`server_port`的值为`8388`。 如果你的`server_port`用了其他的值，请对以下命令作相应的修改：

```
sudo ufw allow ssh
sudo ufw allow 8388
```

现在我们启动`ufw`:

```
sudo ufw enable
```

启动时如果弹出`Command may disrupt existing ssh connections. Proceed with operation (y|n)?`，请输入`y`并按回车键。

最后，请用`sudo ufw status`检查一下你的配置是否和下面的一样：

```
Status: active

To                         Action      From
--                         ------      ----
22/tcp                     ALLOW       Anywhere
8388                       ALLOW       Anywhere
22/tcp (v6)                ALLOW       Anywhere (v6)
8388 (v6)                  ALLOW       Anywhere (v6)
```

运行Shadowsocks-libev

现在我们启动Shadowsocks-libev：

```
sudo systemctl start snap.shadowsocks-libev.ss-server-daemon.service
```

记得设置Shadowsocks-libev开机自启动：

```
sudo systemctl enable snap.shadowsocks-libev.ss-server-daemon.service
```

维护

检查运行状态和日志

以下命令可以查看Shadowsocks-libev的运行状态：

```
sudo systemctl status snap.shadowsocks-libev.ss-server-daemon.service
```

如果你看到绿色的`Active: active (running)`，那么你的Shadowsocks-libev服务器就在正常的运行； 如果你看到红色的`Active: failed`，请用跳至如下命令`journalctl -u snap.shadowsocks-libev.ss-server-daemon.service`的尾部查看问题出在哪里了。

重新加载配置文件

每当你修改过配置文件后，请用如下命令重启Shadowsocks-libev以加载修改后的文件：

```
sudo systemctl restart snap.shadowsocks-libev.ss-server-daemon.service
```

配置备用端口来缓解端口封锁

截止2021年11月7日，我们收到零星的用户报告按此教程配置的服务器仍遭到了端口封锁。

因为报告的封锁方式均为端口封锁，而非IP封锁，我们在此分享一个用备用端口来缓解端口括封锁的方法。

你可以在服务器上使用以下命令来将服务器从`12000`到`12010`端口接收到的TCP和UDP流量全部转发到`8388`端口：

```
sudo iptables -t nat -A PREROUTING -p tcp --dport 12000:12010 -j REDIRECT --to-port
8388
sudo iptables -t nat -A PREROUTING -p udp --dport 12000:12010 -j REDIRECT --to-port
8388
```

记得：

1. 将`12000:12010`替换成一个只有你自己知道的端口号，或者端口区间（我们建议从`1024`到`65535`之间任选几个端口或一个区间）。
2. 将`8388`端口替换成你的Shadowsocks服务端实际使用的端口。

这样一来，如果你使用的`12000`端口遭到了封锁，那么你无须更换IP，或者登录服务器修改配置文件。而是只需要在客户端（电脑或者手机上）将端口从`12000`改为`12001`就可以继续使用了。

如果你配置正确，那么以下命令的输出应该类似于：

```
sudo iptables -t nat -L PREROUTING -nv --line-number
```

```
Chain PREROUTING (policy ACCEPT 0 packets, 0 bytes)
num   pkts bytes target     prot opt in     out     source               destination
1        0     0 REDIRECT   tcp  --  *      *       0.0.0.0/0            0.0.0.0/0
tcp dpts:12000:12010 redir ports 8388
2        0     0 REDIRECT   udp  --  *      *       0.0.0.0/0            0.0.0.0/0
udp dpts:12000:12010 redir ports 8388
```

注意任何`1024`到`65535`的端口都可以作为备用端口。即使使用ephermeral端口(`/proc/sys/net/ipv4/ip_local_port_range`)作为配用端口也不会干扰服务器正常的向外连接。

常见问题

Q:为什么我用了教程里的配置，服务器还是被封了?

A: 截止2021年11月7日，我们收到零星的用户报告服务器的端口被封。因为通过这篇教程配置的Shadowsocks-libev服务器已经可以抵御已知的所有来自GFW的主动探测，所以有可能审查者使用了未知的攻击手段。如果你也遇到了类似问题，请考虑使用上述的备用端口方法来缓解封锁。我们鼓励你将封锁情况汇报给我们，我们会认真地调查。

Q: 我应不应该从发行版的仓库下载安装Shadowsocks-libev?

A: 发行版仓库里的Shadowsocks-libev不一定是最新版的。比如，截止2021年1月，Debian buster仓库的Shadowsocks-libev的版本为`v3.2.5`。而这个版本的Shadowsocks-libev是不够防御来自GFW的主动探测的（详见Figure 10）。

Q: 我应该怎样更新用Snap安装的Shadowsocks-libev?

A: 因为Snap会每天自动更新通过其安装的软件，因此通常情况下你不需要手动更新。如若需要手动更新，请用： `sudo snap refresh`。

Q: 为什么用`chacha20-ietf-poly1305`作为加密方式?

A: 因为它是其中一种AEAD ciphers。而AEAD ciphers可以抵御来自GFW的主动探测。它同时也是Shadowsocks-libev及OutlineVPN的默认加密方式。

Q: 我应该用Shadowsocks的stream cipher吗?

A: 完全不应该。因为Shadowsocks的stream cipher有着不可接受的安全隐私漏洞，并且可以被准确的主动探测。如Figure 10所示，即使是最新版的Shadowsocks-libev，在使用stream cipher时同样可以被准确识别。更具灾难性的是，在不需要密码的情况下，攻击者可以完全解密被记录下来的Shadowsocks会话。

Q: 但为什么我用的机场仍在使用stream cipher?

A: 这清楚地说明你的机场缺乏安全意识和安全措施。请把这篇教程，这个演讲，和这篇总结，分享给你的机场主。

Q: 我应该把配置中的`server_port`改为像`443`这样的常见端口吗?

A: 不应该。因为不论你使用哪个端口，GFW都会检测并怀疑你的Shadowsocks流量。

Q: 为什么配置文件使用`tcp_and_udp`模式?

A: 我们之前使用`tcp_only`模式是为了缓解Partitioning Oracle攻击。但正如Vinicius所指出的，如果你使用了长的随机密码，那么partitioning oracle攻击就不能成功。因此也就不需要禁用UDP代理模式。开启UDP代理模式可能会让经过Shadowsocks代理的视频通话质量更佳。

Q: 为什么配置文件禁用了`fast_open`?

A: 我们推荐你阅读这里的讨论。

联系

这篇报告首发于GFW Report。我们鼓励您或公开地或私下地分享您的评论或疑问。我们私下的联系方式可见GFW Report的页脚。

评论区

124 条评论

Atom feed

在此输入评论 (最少 3 个字符)

名字 (可选) | 电子邮箱 (可选) | 网站 (可选) | 预览 | 提交

DuckSoft • 去年

Good article! I think it better to avoid hardcoding the port 8388 (i am afraid that beginners will simply copy and use this...) State it more clearly like, "in your deployments you'd better use another random port, ..." would be better.

回复

Anonymous • 去年

Thank you for your suggestion. We added the following sentence to the post: 你还可以考虑将`server_port`的值从`8388`改为`1024`到`65535`之间的任意整数。 Note that, for now, we find no evidence that the GFW is biased against any port; however, if this tutorial becomes popular later, the GFW might consider servers using a certain port number suspicious.

回复

匿名 • 去年

What's the difference between shadowsocks-libev and shadowsocks-rust?

6 回复

匿名 • 去年

首先我们想说明，我们的工作中只研究了Shadowsocks-libev和OutlineVPN两款Shadowsocks实现。但这不证明其他的Shadowsocks实现没有类似的问题。相反，我们推荐所研究的这两款实现，因为它们是被积极维护的，它们的最新版都已经解决了发现的问题。

其次，虽然在Shadowsocks-libev的About上写着“Bug-fix-only libev port of shadowsocks. Future development moved to shadowsocks-rust”，但这不意味着Shadowsocks-rust的抗封锁能力已经比Shadowsocks-libev强了。比如说，Shadowsocks-rust的开发者承认，这个实现的成熟还有赖于更多来自社区的支持("I am totally open for you guys to make this project to be actually 'production ready'")。举例来讲，我们看到这个open issue。如果理解正确的话，这个问题Outline之前有过，而现在已经修复。这个问题会导致客户端和服务端发送的第一个数据包的长度完全固定，导致被流量分析的可能。

最后，如果你不确定你喜欢的Shadowsocks实现是否做到了这篇文中我们给翻墙软件开发者的建议, 不妨把文章分享给开发者，看看开发者们怎么说。我们很乐于和他们交流沟通想法。

回复

匿名 • 去年

> "举例来讲，我们看到这个 open issue 。如果理解正确的话，这个问题Outline之前有过，而现在已经修复。这个问题会导致客户端和服务端发送的第一个数据包的长度完全固定，导致被流量分析的可能。"

这里是我们理解错了，问题其实已经被解决，并且被加入到Shadowsocks协议文档："For better obfuscation purposes, both local and remote SHOULD send the handshake data along with some payload in the first packet."。那个issue之所以open，是因为另一个需要修复的地方。

我们下载了目前最新稳定版的Shadowsocks-rust(v1.8.23}，确认客户端发送到服务端的第一个数据包的长度是变化的，其荷载长度为：`IV + addressing + data`。

-7 | 回复

匿名 • 去年

请问要不要加混淆(TLS)和安装 BBR 呢?

2 | 回复

匿名 • 去年

这篇教程推荐的配置，就已经足够抵抗目前的识别和封锁了。

我们还没有研究加入混淆后的流量特征，但以往的经验是，如果混淆不当，反而会有更容易被识别的特征暴露出来。

1 | 回复

匿名 • 8 个月前

根据实际情况，`go-tls` 采用TLS1.3有ESNI，然后ESNI会被阻断，可能结果反而是无法连接。但因为此现象仅在部分地区出现，不排除是运营商QoS国外流量搞的鬼。

1 | 回复

匿名 • 去年

请问客户端该如何配置?

-8 | 回复

匿名 • 去年

我使用了该教程展示的方法，但是很不幸地，服务器仍然被防火墙阻挡了。 我还有一台使用TLS相关协议的服务器，运行完好。 我的ufw版本：ufw 0.35 我的ufw配置（xxx是被故意隐去的数字）：

22/tcp ALLOW Anywhere
24xxx ALLOW Anywhere
22/tcp (v6) ALLOW Anywhere (v6)
24xxx (v6) ALLOW Anywhere (v6)

我的SS-Libev版本：shadowsocks-libev 3.3.5-1 751 latest/edge max-c-lv -

我的加密方式：chacha20-ietf-poly1305

我的SS-Libev密码：采用openssl rand -base64 18生成。

封锁情况：昨天晚上短暂无响应，但马上恢复。今天早上彻底被阻挡，无法ping通。

敬请作者予以调查，你们是反审查的希望。

另外我有一点想问，现在的日期，防火墙有没有可能激进到只要怀疑是Shadowsocks就封锁，而不管主动探测的结果?

6 | 回复

匿名 • 去年

我是这一层的层主，来补充一些信息。我的SS-Libev采用和作者推荐的一致的TCP_Only模式，但UFW在设置过程中，开放的SS-Libev端口没有只允许TCP（可以看层中的UFW配置）。

-2 | 回复

匿名 • 去年

为何不设置只运行TCP?

-1 | 回复

匿名 • 去年

因为忘记了

| 回复

匿名 • 去年

用随机长密码也可以不设置只允许TCP

-1 | 回复

匿名 • 去年

我之前的感觉也是，开obfs-tls混淆，尤其是本身就是用tls协议的知名端口，基本上比较安全。

单独开AEAD还是容易被探测封锁。

-14 | 回复

5 条评论已隐藏

张三 • 去年

我的v2ray两年前开始使用，单vmess加密，几乎天天用，前几个月在某次大规模封机场中被墙过一晚上，第二天又能正常使用了。我想知道我到现在还能使用我的v2ray是我运气好还是已经被gfw破解了被监视中。ps：我的uuid曾经发到过微信上

-20 | 回复

匿名 • 去年

非常感谢分享，我的SS被屏蔽了多次，现在总算知道原因了！

我有个问题，在这里讨论会不会导致这个域名被墙?

| 回复

匿名 • 4 天前

这个域名已经被墙了哈哈哈哈哈哈哈

| 回复

匿名 • 11 个月前

请问多端口文件怎么配置

| 回复

安全上网 • 10 个月前

I built it completely according to the teaching in this article, and it can be used normally but cannot pass the whatleaks detection. PING will detect that I am using a proxy. Is there a way to solve this?

| 回复

匿名 • 10 个月前

We suggest you using the Tor Browser over Shadowsocks to protect your online anonymity. Shadowsocks is not designed for anonymity.

| 回复

匿名 • 10 个月前

您好，我按照教程步骤部署了，也成功链接上了，但是一旦重启服务器，我的shadowsocks就无法与服务端链接了。我通过这条命令sudo systemctl enable snap.shadowsocks-libev.ss-server-daemon.service查看了服务器上的shadowsocks，看起来是正常在运行，显示绿色的Active:

active (running)，但就是无法连接。请问这是什么问题，该怎么解决?

回复

匿名 • 3 个月前

是不是加了端口重定向?如果开启了,防火墙的设置重启没有保存

回复

匿名 • 10 个月前

我按此文设置的SS服务器已经稳定运行了两个多月，没有出现任何问题。请问使用多长的随机密码后就可以打开UDP代理了?

1 回复

匿名 • 10 个月前

> “我按此文设置的SS服务器已经稳定运行了两个多月，没有出现任何问题。”

感谢您的反馈。报告使用正常和报告封锁同样重要。

> “请问使用多长的随机密码后就可以打开UDP代理了？”

随机密码由文中推荐的命令行生成的就足够了：`openssl rand -base64 16`

-2 回复

匿名 • 10 个月前

请问libev是不支持aes-256-gcm吗？ 我用chacha20-ietf-poly1305能正常使用换成aes-256-gcm就会连接不上

1 回复

匿名 • 10 个月前

Shadowsocks-libev是支持`aes-256-gcm`的。

有没有可能是客户端和服务端配置不一致？比如服务端修改过配置后忘记重新加载配置文件。

-1 回复

匿名 • 10 个月前

请问根据此教程，用哪个命令能查看当前使用的ss-libev版本？ 之前都是从backports安装，直接ss-server -v就行了，但是从snap安装似乎有别的命令可以查看ss-libev的版本信息?

回复

匿名 • 10 个月前

可以使用如下命令查看当前版本： `snap run shadowsocks-libev.ss-server -h`

当然，如果觉得不容易记住的话，也可以考虑添加别名：

```
sudo snap alias shadowsocks-libev.ss-server ss-server
```

这样以后就可以直接使用你熟悉的命令了：

```
ss-server -h
```

另外，其他通过snap安装的二进制文件也可以用如下命令找到:

```
ls -l /snap/bin
```

回复

匿名 • 9 个月前

你好， 国外单IP 多端口同时与中国不同ip通讯是否会被GFW怀疑为shadowsocks代理IP？如果存在这种可能，启用tls插件并通过443端口为一个几千人的群体提供服务，也就是单端口多用户是否可以在最新版本的shadowsocks（rust/libev）上实施？我了解到ss的连接方式是不同用户使用不同的端口来进行用户的区分！

-1 | 回复

匿名 • 9 个月前

> "国外单IP 多端口同时与中国不同ip通讯是否会被GFW怀疑为shadowsocks代理IP？"

我们研究的一项发现是：防火长城使用在TCP流中第一个数据包的长度和熵来怀疑Shadowsocks流量。 因此是否被GFW怀疑与端口的多少无关。换句话说，即使服务器上只有一个Shadowsocks端口，GFW仍会因为检测到（疑似）Shadowsocks流量，而去进一步主动探测。

> "如果存在这种可能，启用tls插件并通过443端口为一个几千人的群体提供服务，也就是单端口多用户是否可以在最新版本的shadowsocks（rust/libev）上实施？"

GFW对Shadowsocsk的检测分两步走：第一步先流量分析；第二步再主动探测。使用Shadowscosk over TLS会缓解流量分析，但不能弥补已有的主动探测漏洞。就是说使用Shadowscosk over TLS后的流量，至少前几个数据包会如其他的TLS一样（需要注意让TLS指纹与最流行的浏览器发出的指纹相同），那么GFW可能会比较难根据前几个数据包的特征来怀疑到是Shadowsocks over TLS流量。但是如果TLS后面的Shadowsocks服务端本身存在被主动探测的弱点（比如使用了已经不安全的Stream Cipher），那么一旦GFW主动探测（先建立TLS链接，再发送探测包），就仍可能识别出Shadowsocks服务器。

| 回复

匿名 • 9 个月前

您好，请问在使用上，有必要按照 shadowsocks.org 上的高级配置（优化）教程走一遍吗？谢谢 https://shadowsocks.org/en/config/advanced.html

| 回复

匿名 • 8 个月前

我们没有测试过使用优化教程前后的速度。不过简单地开启BBR后，速度已经可以提升到满意的水平。开启BBR不需要您使用（从而也就不需要信任）一键脚本，如果您使用的是较新的发行版（比如Debian 9或以上）手动操作如下步骤即可：

```
echo "net.core.default_qdisc=fq" >> /etc/sysctl.conf
echo "net.ipv4.tcp_congestion_control=bbr" >> /etc/sysctl.conf
sysctl -p
```

如果以下两条命令的输出中都有`bbr`, 那么BBR就已经启动了：

```
sysctl net.ipv4.tcp_available_congestion_control
lsmod | grep bbr
```

| 回复

sfddfsd • 8 个月前

[root@yerttye445 ~]# sudo systemctl status snap.shadowsocks-libev.ss-server-daemon.service ● snap.shadowsocks-libev.ss-server-daemon.service - Service for snap application shadowsocks-libev.ss-server-daemon Loaded: loaded (/etc/systemd/system/snap.shadowsocks-libev.ss-server-daemon.service; enabled; vendor preset: disabled) Active: failed (Result: start-limit) since Tue 2021-06-08 13:57:44 UTC; 14s ago Main PID: 3775 (code=exited, status=255)

Jun 08 13:57:44 yerttye445 systemd[1]: snap.shadowsocks-libev.ss-server-daemon.service: main process exited, code=exited, status=255/n/a Jun 08 13:57:44 yerttye445 systemd[1]: Unit snap.shadowsocks-libev.ss-server-daemon.service entered failed state. Jun 08 13:57:44 yerttye445 systemd[1]: snap.shadowsocks-libev.ss-server-daemon.service failed. Jun 08 13:57:44 yerttye445 systemd[1]: snap.shadowsocks-libev.ss-server-daemon.service holdoff time over, scheduling restart. Jun 08 13:57:44 yerttye445 systemd[1]: Stopped Service for snap application shadowsocks-libev.ss-server-daemon. Jun 08 13:57:44 yerttye445 systemd[1]: start request repeated too quickly for

snap.shadowsocks-libev.ss-server-daemon.service Jun 08 13:57:44 yerttye445 systemd[1]: Failed to start Service for snap application shadowsocks-libev.ss-server-daemon. Jun 08 13:57:44 yerttye445 systemd[1]: Unit snap.shadowsocks-libev.ss-server-daemon.service entered failed state. Jun 08 13:57:44 yerttye445 systemd[1]: snap.shadowsocks-libev.ss-server-daemon.service failed. [root@yerttye445 ~]#

-1 | 回复

---

sfddfsd • 8 个月前

已经安装好了， Active: active (running) 运行OK，但始终连不上谷歌网址，麻烦问下SwitchyOmega和shadowsocks-windows还要怎么改下设置才能连上?

| 回复

匿名 • 8 个月前

客户端部分的教程我们确实没有涵盖。您可以尝试以“shadowsocks windows客户端”为关键词，搜索一下网上的其他教程。只要服务端可以对抗封锁，客户端的选择可以很灵活。

| 回复

---

sfddfsd • 8 个月前

SwitchyOmega和shadowsocks-windows配置都是正常的， 因为我用其他方式安装的shadowsocks-libev都能正常连上谷歌网址，但用本文的方式安装后， Active: active (running) 运行OK，但始终连不上谷歌网址。 不知道有什么区别吗？ 还是需要额外进行设置?

| 回复

匿名 • 8 个月前

部署完成之后，可以稳定使用，仅移动的宽带不可使用，无法连上服务，不知道怎么解决，有没遇到一样问题的给点建议

| 回复

匿名 • 8 个月前

可能是运营商QoS作妖，与SS关系不大。

| 回复

匿名 • 8 个月前

我使用ipad的shadowrocket客户端可以连接上，连通性测试也没有问题，但是打不开网站。

| 回复

匿名 • 8 个月前

libev都不维护了，还是更新一下吧，用其他的实现比如rust ，goss2等

| 回复

匿名 • 8 个月前

这个问题评论区里已经解释过了，所以不复述 GFW Report 团队的回答。另外 libev 并不是不维护了，而是仅仅修复安全性问题，这跟不维护截然不同。

| 回复

匿名 • 8 个月前

ERROR: failed to handshake with 127.0.0.1: authentication error

-1 | 回复

匿名 • 8 个月前

您好，我在2021.6.28号安装了最新的outline，但是我发现outline的密码只有12位，而你的openssl rand -base64 16，生成的是比较长的密码。 所以outline的12位密码，在抗封锁上ok吗?

| 回复

匿名 • 7 个月前

Yes, the passwords auto-generated by Outline is acceptable.

| 回复

匿名 • 8 个月前

UDP中长的随机密码是指经常更换密码（长密码），还是指自动生成的长密码

回复

匿名 • 7 个月前

密码够长够随机就可以了 不需要定期更换

回复

匿名 • 7 个月前

在centos7.9上用不了，请问有没有测试工具或者方法或者日志?

回复

匿名 • 7 个月前

ERROR: failed to handshake with 113.246.xxxx: authentication error

回复

匿名 • 7 个月前

It is very likely that the passwords used in your client and server do not match.

回复

yoli • 7 个月前

先表示感谢，在看了好多教程的时候在Snap安装的Shadowsocks-libev默认的配置文件这一步都全都失败无效路径。

我在Debian 10中测试安装了6，7次，得到了一些经验来分享，在Debian10中需要安装sudo，snap，在安装好snap时不要马上装snap core而是重启一下你的VPS，Debian10VPS，步骤： 1.apt install sudo -y 2.sudo apt update 3.sudo apt install snapd 4.shutdown -r now

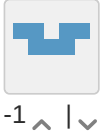
然后可以按照页面的内容安装了，在修改配置文件的时候，一定要注意细心，你有没有多删除了什么或者你多添加了什么内容，在复制粘贴的过程中，造成了重启失败的原因之一。

在新的VPS中建议将原来的系统DNS修改成公共的DNS增强保护性，在你别的电脑连接它时，它会通过那个DNS经过国内的DNS，造成DNS泄漏。 sudo nano /etc/resolv.conf

GoogleDNS

nameserver 8.8.8.8 建议修改一个你信得过的DNS再次增强隐蔽性。

1 回复



匿名 • 7 个月前

配置文件中加密模式字段是“method” 而不是“encryption_method”

-1 回复

匿名 • 7 个月前

今天速度就不行了，从1W掉到500啦。

回复

匿名 • 7 个月前

目前一切已经恢复正常~

回复

lanlan • 7 个月前

我使用了这个教程，做了一个一键安装脚本https://github.com/lanlandezei/shadowsocks-libev 支持系统 debian9+ ubuntu16+ centos7.5+ fedora

回复

匿名 • 3 个月前

非常感谢您制作脚本。我们在2021年11月7日对教程进行了更新，加入了备用端口和开启`tcp_and_udp`模式的建议。您可否对脚本进行相应的调整?

另外我们注意到，与许多一键脚本类似，您使用了`wget --no-check-certificate`。考虑到Github曾遭受过来自中国的中间人攻击，我们建议您为安全考虑，不要使用`--no-check-certificate`选项。

回复

匿名 • 7 个月前

我在一些平台上遇到了必须“ufw reload”才能使得规则生效的情况，而不是直接“ufw enable”就好了，应该是平台本身就在 iptables 中添加了默认禁止所有端口通信的冲突规则所导致的。

1 回复

匿名 • 6 个月前

使用这个配置，ss运行了半年没问题，今天突然发现8888端口被墙了，换成9999端口以后恢复正常。

1 回复

匿名 • 6 个月前

用一些不规则一点的端口能稳定一些，我最开始是8338，端口没几天就被Q了，换了个不规则的端口也用了几个月没问题

回复

匿名 • 6 个月前

反复尝试后，依然运行有问题，oracle cloud，ubuntu 20.04

Aug 27 04:37:50 instance-20210827-1419 systemd[1]: Started Service for snap application shadowsocks-libev.ss-server-daemon.

Aug 27 04:37:50 instance-20210827-1419 shadowsocks-libev.ss-server-daemon[1618]: 2021-08-27 04:37:50 ERROR: Invalid config path.

Aug 27 04:37:50 instance-20210827-1419 systemd[1]: snap.shadowsocks-libev.ss-server-daemon.service: Main process exited, code=exited, status=255/EXCEPT>

Aug 27 04:37:50 instance-20210827-1419 systemd[1]: snap.shadowsocks-libev.ss-server-daemon.service: Failed with result 'exit-code'.

Aug 27 04:37:50 instance-20210827-1419 systemd[1]: snap.shadowsocks-libev.ss-server-daemon.service: Scheduled restart job, restart counter is at 5.

Aug 27 04:37:50 instance-20210827-1419 systemd[1]: Stopped Service for snap application shadowsocks-libev.ss-server-daemon.

Aug 27 04:37:50 instance-20210827-1419 systemd[1]: snap.shadowsocks-libev.ss-server-daemon.service: Start request repeated too quickly.

Aug 27 04:37:50 instance-20210827-1419 systemd[1]: snap.shadowsocks-libev.ss-server-daemon.service: Failed with result 'exit-code'.

Aug 27 04:37:50 instance-20210827-1419 systemd[1]: Failed to start Service for snap application shadowsocks-libev.ss-server-daemon.

-1 回复

shrimp • 6 个月前

这里我有一个疑问，必须要安装ufw防火墙么？ ufw的作用是不是仅仅防止被黑客攻击？还是说ufw可以防止GFW进行探测？希望能解答一下，谢谢。

我个人的VPS始终没有安装ufw但是现在依然可以正常使用。

-1 回复

shrimp • 5 个月前

在一段时间后也是会出现端口被封禁的情况，跟我没有安装防火墙这个应该没关系吧。

1 回复

匿名 • 4 个月前

应该没，就照教程做端口还是被禁。

回复

匿名 • 3 个月前

感谢汇报封锁情况。请问您的服务器是被IP封锁，还是只是端口封锁。我们在文中更新了使用备用端口来缓解端口封锁的办法，或许对您有帮助。

回复

匿名 • 3 个月前

我是4天前回复的答主，只是端口封锁。更新：回复时当天换了端口，今天被封，这几天流量是无下载，仅日常会产生流量大小，服务器使用UDP代理，长随机密码。

回复

匿名 • 5 个月前

我参照楼主的教程，没有被封过。 后来因为oculus quest2需要走udp，mode开了udp_and_tcp模式，结果就被秒封，但是我的密码还是按照楼主说的用的openssl rand -base64 16 生成的随机密码，所以可能强随机密码依然不能阻挡udp模式被封。

-2 回复

匿名 • 5 个月前

请问你们能否测试一下V2Ray和X Ray?

2 回复

匿名 • 3 个月前

我们对Xray的Shadowsocks模块做了一些简单的测试，总结起来现在Xray的Shadowsocks明显的主动探测指纹已经消失： https://github.com/XTLS/Xray-core/issues/625#issuecomment-960521650

-1 回复

Emie Wehner • 4 个月前

按照本帖配置的 SS。为支持 UDP，没有使用 `tcp_only` 模式。密码是随机 32 位，`openssl rand -base64 32`。个人用，月用量单向算近 3T，99% 是在家用的（联通动态公网 IP）。一个月后**仅从家里 IP 使用该 SS 时无法连接，其他 IP 使用该 SS 正常**。家里重拨换了 IP 后还是无法连该 SS。改端口后问题解决。

另有三个自建代理，也是个人用，主要流量也是发生在家里，三个代理一直完全正常。一个 Trojan，两个 SS（同样按本帖配置，同样支持 UDP，32 位随机密码）。两个 SS 的单向月用量都不到 400GB。

应该是不明流量较大导致的针对性封锁?

回复

匿名 • 3 个月前

> 一个月后仅从家里 IP 使用该 SS 时无法连接，其他 IP 使用该 SS 正常。家里重拨换了 IP 后还是无法连该 SS。改端口后问题解决。

感谢汇报封锁情况。这种情况确实很奇怪。是说从家中IP无法连接到SS，但从手机的移动网，或者其他地方的IP就可以连接到SS服务器吗?

回复

匿名 • 3 个月前

是的 确实有这种情况 我也遇到过!

回复

匿名 • 3 个月前

猜测是不是GFW部署了针对客户端的攻击，并在客户端IP连接某一IP时阻断其端口?

回复

匿名 • 4 个月前

这是AI在攻击我的服务器吗，中国联通的ip不断的连接我的服务器。下面是我截取的日志。

2021-10-27 23:24:06 ERROR: crypto: AEAD: repeat salt detected 2021-10-27 23:24:06 ERROR: failed to handshake with 175.152.110.20: authentication error 2021-10-27 23:24:16 ERROR: failed to handshake with 150.255.20.121: authentication error

回复

匿名 • 3 个月前

> AEAD: repeat salt detected

这个是典型的重放攻击在日志中留下的记录。但是按照教程配置的服务器可以抵御这种重放攻击。

回复

匿名 • 3 个月前

在正常工作 9 个月后，IP 端口遭到屏蔽

2 回复

匿名 • 3 个月前

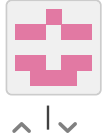
感谢汇报封锁情况。请问您的服务器是被IP封锁，还是只是端口封锁。我们在文中更新了使用备用端口来缓解端口封锁的办法，或许对您有帮助。

回复

匿名 • 3 个月前

更新一下，昨天还是封锁端口，今天情况变化，目前的现状是只要一连接并访问外网，IP就会被ban一段时间（数分钟），无法ping通，之后恢复，然后一旦连接，再次被ban IP，也尝试了Vmass协议(并启用VmassAEAD)，也是上述情况。尝试了多个新US IP均如上情况。使用多个国内IP访问尝试，也如此。 之前运行良好。

-5 回复



匿名 • 3 个月前

跟上面的情况类似，刚换的端口，一天之后就被屏蔽了，之前一切正常

回复

匿名 • 3 个月前

这两天 确实出现了比较多的端口封锁！

回复

匿名 • 3 个月前

动作很快，我今天换了端口，三分钟之内就被封了。我估计是我的IP已经被重点监控了。顺便，我的各种配置都是按照上文配的。我的流量很小，一个月可能也就十几个G

回复

匿名 • 3 个月前

我和上一个回复是同一个人，但跟楼主不是一个。目前我发现在间隔一段时间之后的第一次访问可以成立，但后续访问都将失效，显示的提示信息是无法验证连接的安全性。

回复

匿名 • 3 个月前

我使用的是outline，依据这里的建议，客户端和服务端都使用了outline，但近日端口还是遭到了封锁，所幸IP并没有被封锁。 补充说明：该服务一直是我一个人在使用，并没有分享给他人，同时我并没有使用过其它兼容客户端，一直用的outline客户端，因为我有全局代理需求，而且主要是udp流量（游戏代理）。

回复

匿名 • 3 个月前

看来，今天很多人都中了，美国的节点基本over了。

1 | 回复

匿名 • 3 个月前

确实是这样的

| 回复

匿名 • 3 个月前

差不多试了10几个虚拟服务器创建，有一些部署好了，能打开一个页面，然后就连不上了，Ping可以ping通，putty连接确是超时，设置的地方都是可以运行的，一旦连接就是打开一个页面后， 就不可用了，Ping也不通了，过一会又可以ping了，还可以连接上，SS只能闪一次而后就无法连接了。protonmail这个邮箱国内也被墙了，今天。

1 | 回复

匿名 • 3 个月前

断开网线用无线连接putty就能连接了，就是部署好的SS，上不去。

| 回复

匿名 • 3 个月前

对，完全一样的情况

| 回复

匿名 • 3 个月前

对 完全一样的情况

| 回复

匿名 • 3 个月前

2021-11-10 07:46:01.5883|WARN|Shadowsocks.Controller.TCPHandler|System.Net.Sockets.SocketException (0x80004005): 由于目标计算机积极拒绝，无法连接。 在 Shadowsocks.Util.Sockets.WrappedSocket.EndConnect(IAsyncResult asyncResult) 在 Shadowsocks.Proxy.DirectConnect.EndConnectDest(IAsyncResult asyncResult) 在 Shadowsocks.Controller.TCPHandler.ConnectCallback(IAsyncResult ar) 2021-11-10 07:46:01.6374|INFO|Shadowsocks.Controller.ShadowsocksController|WPF Localization Extension|Current culture: zh-CN 2021-11-10 07:46:01.7579|INFO|Shadowsocks.Controller.Listener|Shadowsocks started (4.4.0.0) 2021-11-10 08:52:09.6448|INFO|Shadowsocks.Controller.TCPHandler|start (78.141.216.227:15798) timed out 2021-11-10 09:22:24.2106|INFO|Shadowsocks.Controller.ShadowsocksController|WPF Localization Extension|Current culture: zh-CN 2021-11-10 09:22:24.3532|INFO|Shadowsocks.Controller.Listener|Shadowsocks started (4.4.0.0) 2021-11-10 09:35:28.3818|INFO|Shadowsocks.Controller.ShadowsocksController|WPF Localization Extension|Current culture: zh-CN 2021-11-10 09:35:28.5251|INFO|Shadowsocks.Controller.Listener|Shadowsocks started (4.4.0.0) 2021-11-10 09:35:37.4553|INFO|Shadowsocks.Controller.TCPHandler|108.61.132.106:30337 timed out

| 回复

匿名 • 3 个月前

今天又测试了下，我测试的结果来看主要针对美国节点，瑞典、德国、瑞士节点都可以连接，就美国节点，可以连接但是一旦连接就如同下面的代码一样，立马连接中断，过一会在后台可以ping通。

-4 | 回复

2 条评论已隐藏

匿名 • 3 个月前

常年一直没有问题的这两天开始出现严重断流，测试了一下某些范围内的IP上有无法识别的流量会稳定触发三分钟的黑洞路由（ssh、https等不会触发，按上述方法部署的shadowsocks、socat转发的别的IP上可用的vmess会触发），加上simple-obfs（不推荐）后不再出现 之前也有见别人报告过类似的，但是我第一次遇见

回复

匿名 • 2 个月前

11月开始 阿里云 轻量 hk 测试过 好多协议 都很容易触发 3分钟黑洞路由。

回复

匿名 • 3 个月前

我的服务已经持续运行了一年多，最近两天中断两次。在网上搜到了这篇文章，看到有人和我有类似的问题出现。

我的方式：

客户端 -> 国内中转服务器 -> 海外服务器

其中：

1. 国内中转服务器通过 UFW 只开放 ssh 和中转服务端口，例如中转端口 `1234`，流量转发至海外服务器的 shadowsocks 服务端口 `4321`。（国内服务器 IP 地址为 `xx.xxx.xx.xx`）
2. 海外服务器通过 UFW 只开放 ssh 和 shadowsocks 的服务端口，此例中为 `4321`，并且只允许来自 IP 地址为国内中转服务器的流量。（`ufw allow from xx.xxx.xx.xx to any port 4321`）

现象：

1. 海外服务器的 IP 没有被封，但端口 `4321` 被封。
2. 国内服务器的 IP 没有被封，端口同样没有被封。（中转服务器不受影响）
3. 如果保持国内服务器的开放端口不变，只调整海外服务器的 ss 服务端口，可以恢复连接，但不会持续很长时间，一天左右会再次被封。

有趣的点：GFW 本次的识别方式还是主动探测攻击吗？（考虑到我已经设置了防火墙规则，海外服务器会直接 drop 不是来自中转服务器的流量。）

回复

匿名 • 3 个月前

它可以主动探测你中转服务器吧，毕竟你中转服务器没有限制入站ip

回复

匿名 • 3 个月前

目前是否有可解决的教程?

回复

匿名 • 3 个月前

> 它可以主动探测你中转服务器吧，毕竟你中转服务器没有限制入站ip

中转服务器的确没有限制入站 IP，但中转服务器的端口没有被封。反而被封的是最终 ss 服务器的端口。

回复

匿名 • 3 个月前

透露一下搭载 ss 的服务商么，我的情况类似，我甚至怀疑是不是国外服务商被攻陷了。

回复

匿名 • 3 个月前

你的是哪家国外服务商?

回复

匿名 • 3 个月前

我之前用aes-256-cfb的加密模式+bbr速度很快，于11月7日发生无法连接的情况；今天采用上述教程重新部署，暂时恢复正常，但明显速度下降了许多

-2 | 回复

匿名 • 3 个月前

同样的情况，速度慢了好多（也用的是瓦工VPS?）

-1 | 回复

Indefiblecoward • 3 个月前

Would you consider hardware when you inquest? I used your method first in August on Samsung and many Computers.It worked.About 10 days later, I used it on Huawei then(about 5 days) it can't work on Huawei and the Huawei phone got lagged hard until I uninstall the Shadowsocks.Then(about 3 days) The ip cant work on any devise even after change the server port. I redid this 3 times that time,the consequence was same.

But I change a ip still used on any other devises it kept working for about 3 mouths until now I used it on Huawei.The situation happened again.And the result have a little change: it worked on Huawei first but lagged(about 100kbs).10 minute later the Huawei become a brick till I cut the web line.Then(immediately) all devise used same router uploaded a complicated flow then any shadowsocks service can't work on the devises now(It become more and more lagging then literally died). My samples are mere.Is same experience here?

-4 | 回复

匿名 • 3 个月前

服务器运行正常（绿色的Active: active (running)）。 但是ios端软件（小火箭、Qx）无法连接服务器。何解?

-3 | 回复

john • 2 个月前

端口封锁，请尝试更换端口

| 回复

john • 2 个月前

反馈一下，按照文中部署的方式我在12/09/2021 也遭到了 端口封锁，目前已按文中提出的解决问题解决。 请问一下，最近出现的这种端口封锁的原因是什么呢?

-1 | 回复

匿名 • 2 个月前

提问：怎么永久解决accept: Too many open files的问题？感谢解答，跪谢

| 回复

匿名 • 上个月

首先在文件最后加上如下两行：

`sudo nano /etc/security/limits.conf`:

```
* hard nofile 655360
* soft nofile 655360
```

然后在要运行Shadowsocks的Terminal中：

```
ulimit -n 655350
```

确认`max open files`的数量已经提高：

```
ulimit -a
```

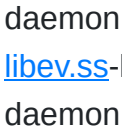
注意有时候`ulimit -n unlimited`不能成功提高`max open files`，所以才在例子中使用一个比较大的数值`566350`。

| 回复

匿名 • 2 个月前

谢谢分享，已安装部署。中间遇到了一个问题，有一点反馈：在Oracle Cloud的多台服务器上使用ufw开放的端口不能生效（虽然status会显示端口开放正常），包括Security List -> Ingress Rules也不能生效。最后用iptables命令开放端口成功。目前只在Oracle遇到类似的端口问题。解决方法参考：https://www.v2ex.com/t/603319

1 | 回复



Georgy GHQ • 上个月

您好，我按照教程步骤部署了，也成功链接上了,但systemctl list-units --type service发现:

shadowsocks-libev.service loaded active exited snap.shadowsocks-libev.ss-local-daemon.service loaded failed failed snap.shadowsocks-libev.ss-server-daemon.service loaded active running Service for snap application shadowsocks-libev.ss-server-daemon 其中，-local-daemon.service loaded failed不知什么原因，其systecmctl status如下： ● snap.shadowsocks-libev.ss-local-daemon.service - Service for snap application shadowsocks-libev.ss-local-daemon Loaded: loaded (/etc/systemd/system/snap.shadowsocks-libev.ss-local-daemon.service; enabled; vendor preset: enabled) Active: failed (Result: exit-code) since Tue 2022-01-25 22:45:28 CST; 9h ago Process: 1722 ExecStart=/usr/bin/snap run shadowsocks-libev.ss-local-daemon (code=exited, status=1/FAILURE) Main PID: 1722 (code=exited, status=1/FAILURE) Jan 25 22:45:28 （屏蔽） systemd[1]: snap.shadowsocks-libev.ss-local-daemon.service: Main process exited, code=exiteJan 25 22:45:28 （屏蔽） systemd[1]: snap.shadowsocks-libev.ss-local-daemon.service: Unit entered failed state.Jan 25 22:45:28（屏蔽） systemd[1]: snap.shadowsocks-libev.ss-local-daemon.service: Failed with result 'exit-code'.Jan 25 22:45:28 （屏蔽） systemd[1]: snap.shadowsocks-libev.ss-local-daemon.service: Service hold-off time over, schJan 25 22:45:28 （屏蔽） systemd[1]: Stopped Service for snap application shadowsocks-libev.ss-local-daemon.Jan 25 22:45:28 （屏蔽） systemd[1]: snap.shadowsocks-libev.ss-local-daemon.service: Start request repeated too quicJan 25 22:45:28 （屏蔽） systemd[1]: Failed to start Service for snap application shadowsocks-libev.ss-local-daemon.Jan 25 22:45:28 （屏蔽） systemd[1]: snap.shadowsocks-libev.ss-local-daemon.service: Unit entered failed state.Jan 25 22:45:28 （屏蔽） systemd[1]: snap.shadowsocks-libev.ss-local-daemon.service: Failed with result 'exit-code'. 文件snap.shadowsocks-libev.ss-local-daemon.service的Unit内容如下：

[Unit]

Auto-generated, DO NOT EDIT

Description=Service for snap application shadowsocks-libev.ss-local-daemon Requires=snap-shadowsocks\x2dlibev-799.mount Wants=network.target After=snap-shadowsocks\x2dlibev-799.mount network.target snapd.apparmor.service X-Snappy=yes

[Service] EnvironmentFile=-/etc/environment ExecStart=/usr/bin/snap run shadowsocks-libev.ss-local-daemon SyslogIdentifier=shadowsocks-libev.ss-local-daemon Restart=on-failure WorkingDirectory=/var/snap/shadowsocks-libev/799 TimeoutStopSec=30 Type=simple

[Install] WantedBy=multi-user.target

请问楼主该怎么解决，谢谢。

| 回复

匿名 • 上个月

我按照本文教程来搭建好SS服务器，可是我每次使用时都显示time out，后来我尝试tcp_only和更加复杂的密码，也是在建立一次连接后直接time out，ip经测试没有被屏蔽，推断是端口屏蔽，跟换端口也只是能够建立一次连接，随后立刻断连，服务根本不可用。

| 回复

R • 上个月

sudo nano /var/snap/shadowsocks-libev/common/etc/shadowsocks-libev/config.json没法执行，需要先mkdir -p /var/snap/shadowsocks-libev/common/etc/shadowsocks-libev/config.json

1 | 回复

R • 上个月

sudo systemctl start snap.shadowsocks-libev.ss-server-daemon.service 启动不了，提示：Failed to start snap.shadowsocks-libev.ss-server-daemon.service: Unit snap.shadowsocks-libev.ss-server-daemon.service not found.

回复

qwertyuiop • 上个月

确实仍然有端口被封的情况，按照以上设置后，用了半个月时间，今天端口被封，换端口仍然能用，不知能继续用同一个端口多长时间?

回复

匿名 • 上个月

目前看来依旧不能使用UDP, 开启UDP后端口基本上秒封

回复

E • 上个月

按本文设置ss有一年了，在去年11月7日被封端口，更换ip后一直到昨天都正常，昨天大年三十晚上3个vps中常用的两个都开始被封端口，更换端口后恢复可用。看来新的一波大规模查封又开始了

回复

匿名 • 上个月

昨天开始确实出现了以上情况

回复

匿名 • 上个月

完全按本文的做法做的，就为看看是不是shadowsocks抗封锁能力提升了，用了半个月，除夕过完还是被封了端口，看样子shadowsocks还是容易被封的，特别是特殊时期，基本上必死了……

回复

qwertyuiop • 上个月

看来要求稳还是得伪装，我的两个vps主线路都是视频网站伪装，nginx+ws+tls，没有任何问题，但延迟比shadowsocks高一倍，shadowsocks看来只适合iepl线路了，要过GFW的话，还是要正常https流量才行。

-2 回复