

内网隧道搭建ksa工具-端对端-无需公网VPS做流量转发

原创

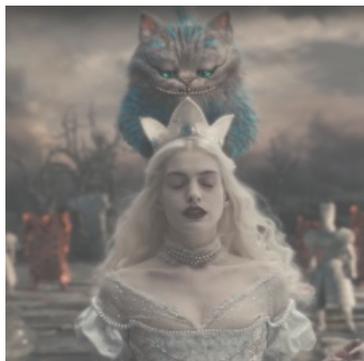
kuxing_admin 于 2021-11-08 12:29:11 发布 4292 收藏 1

分类专栏: [内网渗透](#) 文章标签: [linux macos](#) [运维](#) [网络安全](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: https://blog.csdn.net/weixin_42109829/article/details/121201936

版权



[内网渗透](#) 专栏收录该内容

8 篇文章 1 订阅

订阅专栏

1、前言

看雪安全接入 (KSA), 一款傻瓜式的一键接入私有网络的工具, 无论您在任何地点、任何时间、使用任何线路, 均可利用这一服务接入自己的私有设备。

KSA的服务端和客户端集成在一个可执行文件之中, 目前支持Windows、macOS和Linux平台, 支持x86/x64、arm(64)和mips(el), 树莓派和路由器都可以运行了!

2、应用场景

你的vps网速过慢, 或者没有vps, 需要与目标主机搭建一个共同的网关, 然后可以互相访问。

下载链接

Linux客户端下载: KSA_0.80_linux.zip

https://aiminet.github.io/uploads/KSA_0.80_linux.zip

window客户端下载:

https://aiminet.github.io/uploads/KSA_0.80win_mac.zip

3、特点

简单、便捷:

配置简单; 秒连; 支持全终端; 驱动级的轻量化

安全、可靠:

双向TLS; 全局AES-256; 驱动级稳定性

4、使用教程

1、该软件的使用, 由系统来分类, 分为**window与mac系统** 和**linu系统**

2、然后该软件的使用需要创建一个服务端和客户端, 但该软件的服务端和客户端, 都是同一个程序运行的, 如图看下

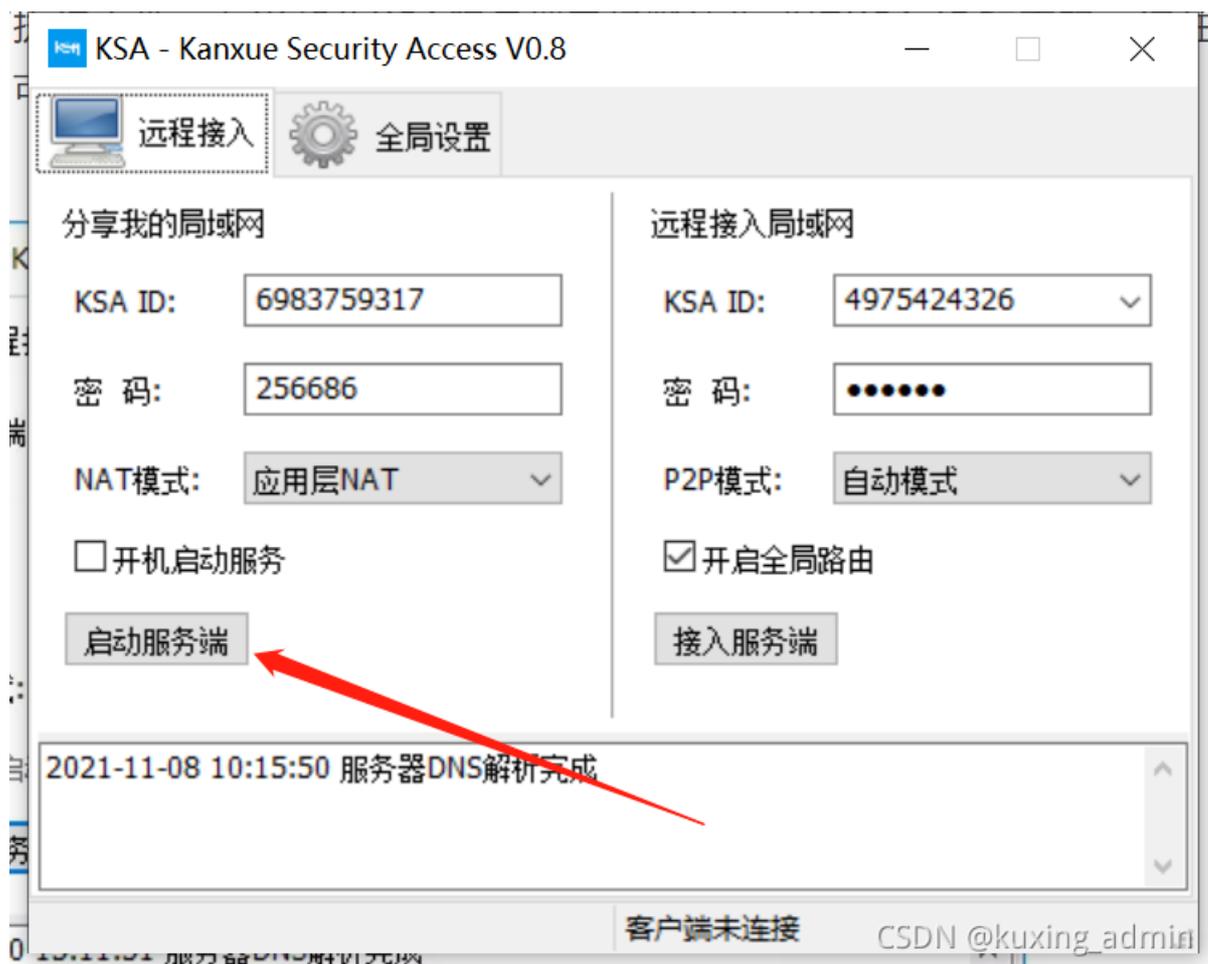
3、window 创建的服务端, linux主机能连接, linux主机创建的服务端, window主机也能连接, 不存在跨系统的限制。



4.1、window 和mac 使用教程

①-服务端配置

双击运行可执行文件，左半部分KSA服务端已经默认生成好KSA ID和密码，记住这个KSA ID和密码即可。点击启动服务开始运行服务端：



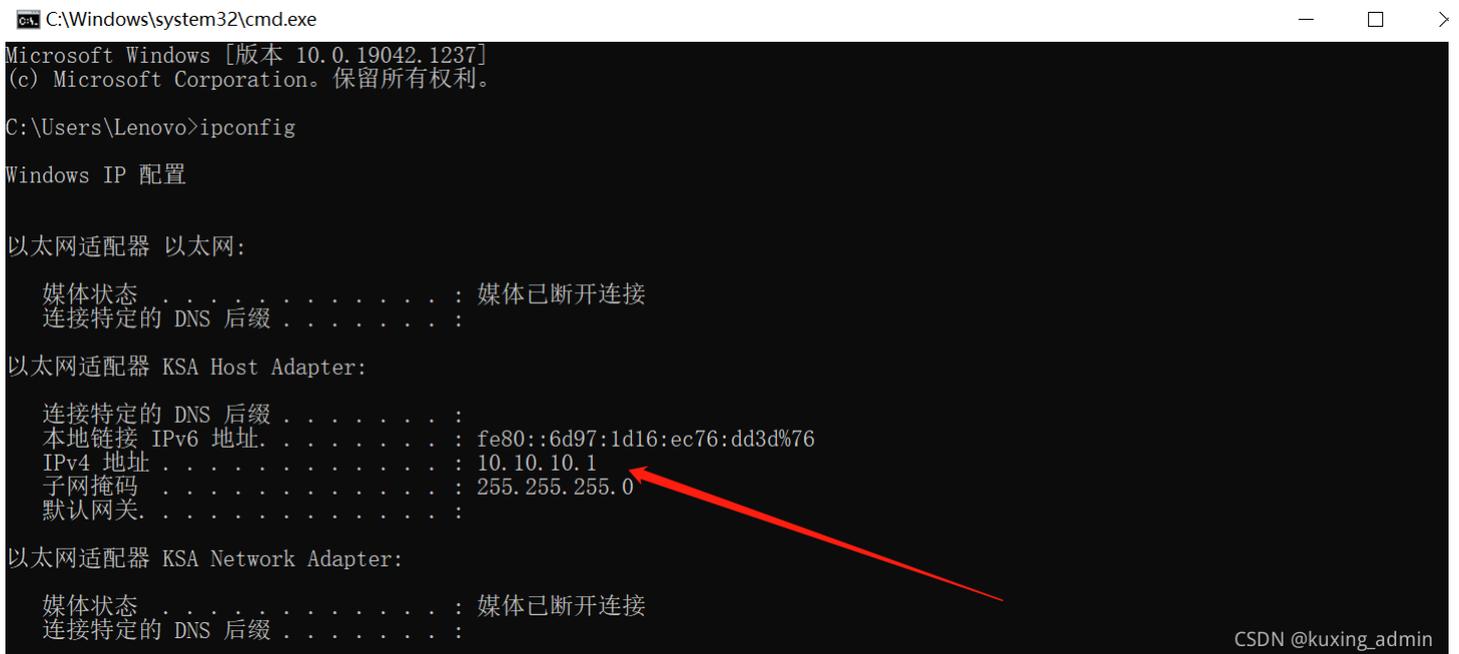
②-配置客户端

客户端的连接是需要在服务端上复制KSA ID 和密码两个参数。而且接入服务端需要先安装一个软件，点击安装即可。

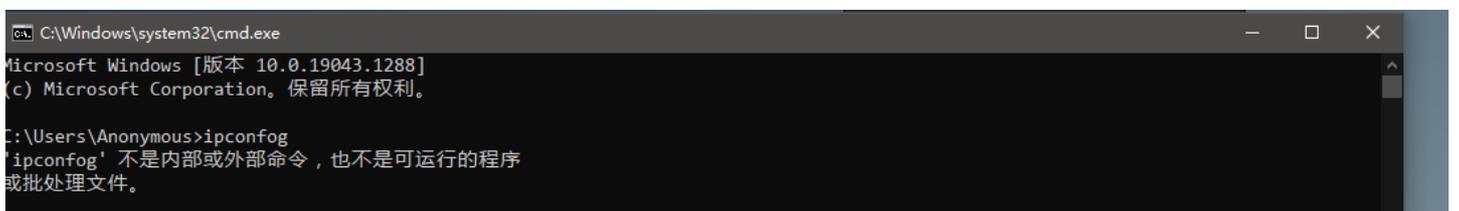


③-结果展示

这时候我们看服务端会出现一个 10.10.10.1的ipv4的地址



然后客户端会出现一个10.10.10.2 的ipv4的地址



```
C:\Users\Anonymous>ipconfig

Windows IP 配置

以太网适配器 KSA Network Adapter:

    连接特定的 DNS 后缀 . . . . . :
    本地链接 IPv6 地址. . . . . : fe80::ecca:1d29:7da1:afd4%31
    IPv4 地址 . . . . . : 10.10.10.2
    子网掩码 . . . . . : 255.255.255.0
    默认网关 . . . . . :

以太网适配器 Ethernet0:

    连接特定的 DNS 后缀 . . . . . : localdomain
```

而且他们互相能ping通，就说明他们有共同的内网，能互相通信。

```
C:\Windows\system32\cmd.exe

以太网适配器 KSA Network Adapter:

    连接特定的 DNS 后缀 . . . . . :
    本地链接 IPv6 地址. . . . . : fe80::ecca:1d29:7da1:afd4%31
    IPv4 地址 . . . . . : 10.10.10.2
    子网掩码 . . . . . : 255.255.255.0
    默认网关 . . . . . :

以太网适配器 Ethernet0:

    连接特定的 DNS 后缀 . . . . . : localdomain
    本地链接 IPv6 地址. . . . . : fe80::9185:def3:fa19:10a3%11
    IPv4 地址 . . . . . : 192.168.47.130
    子网掩码 . . . . . : 255.255.255.0
    默认网关 . . . . . : 192.168.47.2

以太网适配器 蓝牙网络连接:

    媒体状态 . . . . . : 媒体已断开连接
    连接特定的 DNS 后缀 . . . . . :

C:\Users\Anonymous>ping 10.10.10.1

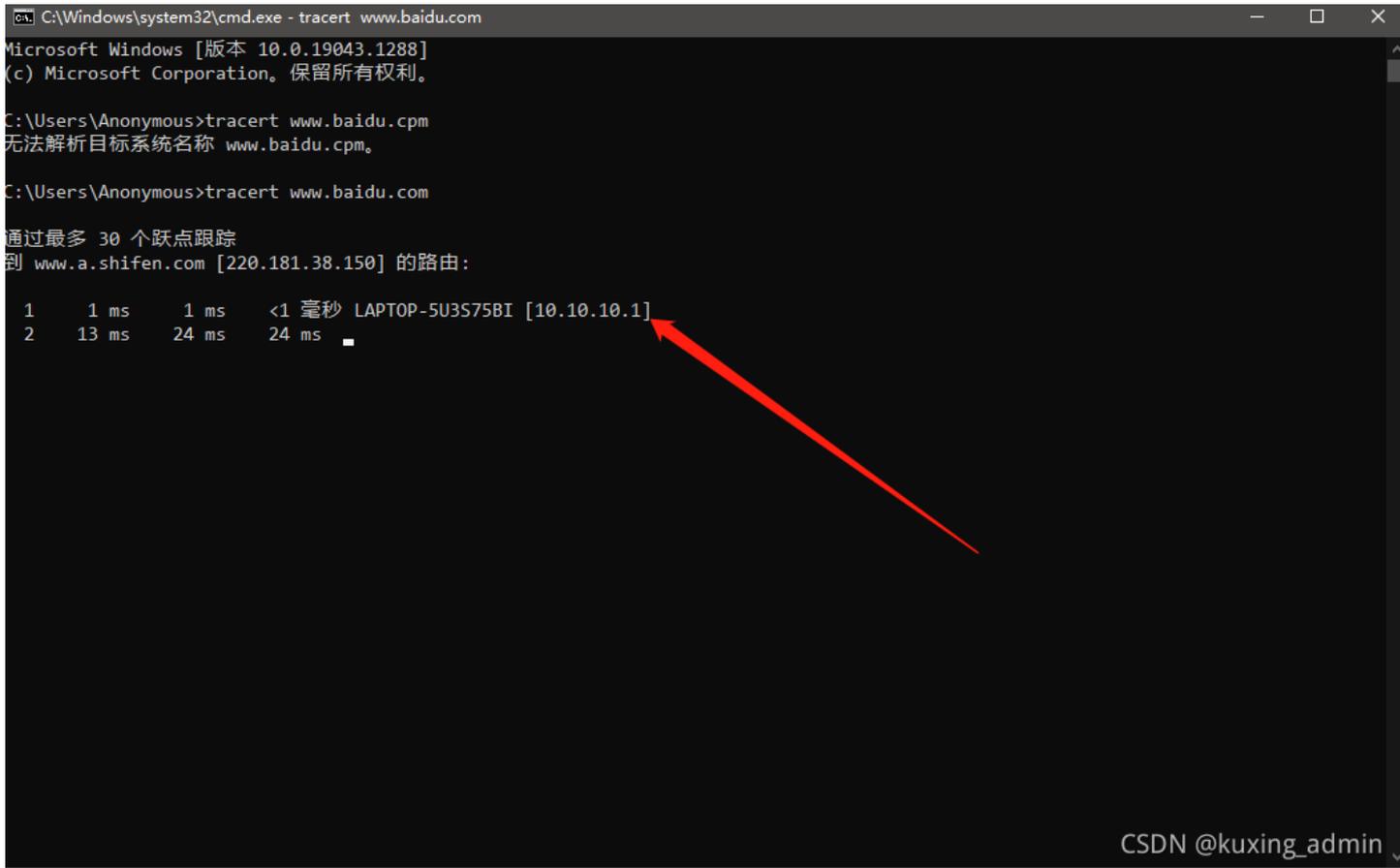
正在 Ping 10.10.10.1 具有 32 字节的数据:
来自 10.10.10.1 的回复: 字节=32 时间=1ms TTL=128
来自 10.10.10.1 的回复: 字节=32 时间<1ms TTL=128
来自 10.10.10.1 的回复: 字节=32 时间=2ms TTL=128
来自 10.10.10.1 的回复: 字节=32 时间=2ms TTL=128

10.10.10.1 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
    往返行程的估计时间(以毫秒为单位):
        最短 = 0ms, 最长 = 2ms, 平均 = 1ms

C:\Users\Anonymous>aaa
```

如果开启全局路由，客户端的流量都会走服务端，所以客户端的出口ip会和服务端一样。





4.2、linux 使用教程

①-服务端配置

下载

```
wget https://aiminet.github.io/uploads/KSA_0.80_linux.zip
```

```
unzip KSA_0.80_linux.zip # 解压
cd KSA_0.80_linux #进入目录
```

解压之后，使用sudo chmod +x ksa*命令，给ksa软件添加可执行权限，然后启动即可。

安装

```
$ sudo chmod +x ksa*
$ sudo ./ksa_x64
```

服务端即会开启并运行，KSA ID和PSK都会出现。

也可以查看同目录下的ksa.log文件，启动日志已经写入到该文件中。

```
ubuntu@ubuntu-VirtualBox:~/Desktop/KSA_linux$ ls
ksa_arm          ksa_armhf_musl_so  ksa_mipsel_musl_so  ksa_x64_musl_so
ksa_arm64        ksa_armhf_uclib_so ksa_mipsel_uclib_so ksa_x86
ksa_arm64_musl   ksa_arm_musl_so    ksa_mips_musl_so    版本说明.txt
ksa_arm64_uclib_so ksa_arm_uclib_so  ksa_mips_uclib_so
ksa_armhf        ksa.conf           ksa_x64
ubuntu@ubuntu-VirtualBox:~/Desktop/KSA_linux$ sudo chmod +x ksa*
[sudo] password for ubuntu:
ubuntu@ubuntu-VirtualBox:~/Desktop/KSA_linux$ ls
ksa_arm          ksa_armhf_musl_so  ksa_mipsel_musl_so  ksa_x64_musl_so
ksa_arm64        ksa_armhf_uclib_so ksa_mipsel_uclib_so ksa_x86
ksa_arm64_musl   ksa_arm_musl_so    ksa_mips_musl_so    版本说明.txt
ksa_arm64_uclib_so ksa_arm_uclib_so  ksa_mips_uclib_so
ksa_armhf        ksa.conf           ksa_x64
ubuntu@ubuntu-VirtualBox:~/Desktop/KSA_linux$ sudo ./ksa_x64
KSA ID:1230319594
KSA PSK:003126
KSA SERVER:nat.kanxue.com
KSA LINK:UDP
KSA NAT MODE:KERNEL TUN
KSA SERVER START
ubuntu@ubuntu-VirtualBox:~/Desktop/KSA_linux$ cat *log
2019-07-03 16:50:56 KSA server start...
2019-07-03 16:50:57 KSA server 1230319594 10.0.0.0/24 started
2019-07-03 16:50:57 KSA server:nat.kanxue.com/47.102.223.17
2019-07-03 16:50:57 KSA conn:TLS CONN...
2019-07-03 16:50:57 KSA server:nat.kanxue.com udp mode:1 port:5000
2019-07-03 16:50:57 KSA conn:TLS CONN OK
2019-07-03 16:50:57 KSA NAT NIC:enp0s3 10.68.2.216
2019-07-03 16:50:57 KSA conn:SEVER CONN OK
2019-07-03 16:50:57 KSA tun dev:ksa_enp0s3 10.0.0.0/24
2019-07-03 16:50:57 KSA init nat 10.0.0.0/24 -> enp0s3
2019-07-03 16:50:57 on_netlink_ev_s:ksa_enp0s3_110d1 up
ubuntu@ubuntu-VirtualBox:~/Desktop/KSA_linux$
```

CSDN @kuxing_admin

服务端成功启动后，运行ifconfig命令可以查看到KSA向系统中添加的虚拟网卡。

```
ubuntu@ubuntu-VirtualBox:~/Desktop/KSA_linux$ ifconfig
enp0s3  Link encap:Ethernet  HWaddr 08:00:27:9b:c6:b0
        inet addr:10.68.2.216  Bcast:10.68.255.255  Mask:255.255.0.0
        inet6 addr: fe80::7316:1297:bc5e:4188/64  Scope:Link
        UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
        RX packets:871998 errors:0 dropped:0 overruns:0 frame:0
        TX packets:203324 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1000
        RX bytes:178543386 (178.5 MB)  TX bytes:19220286 (19.2 MB)

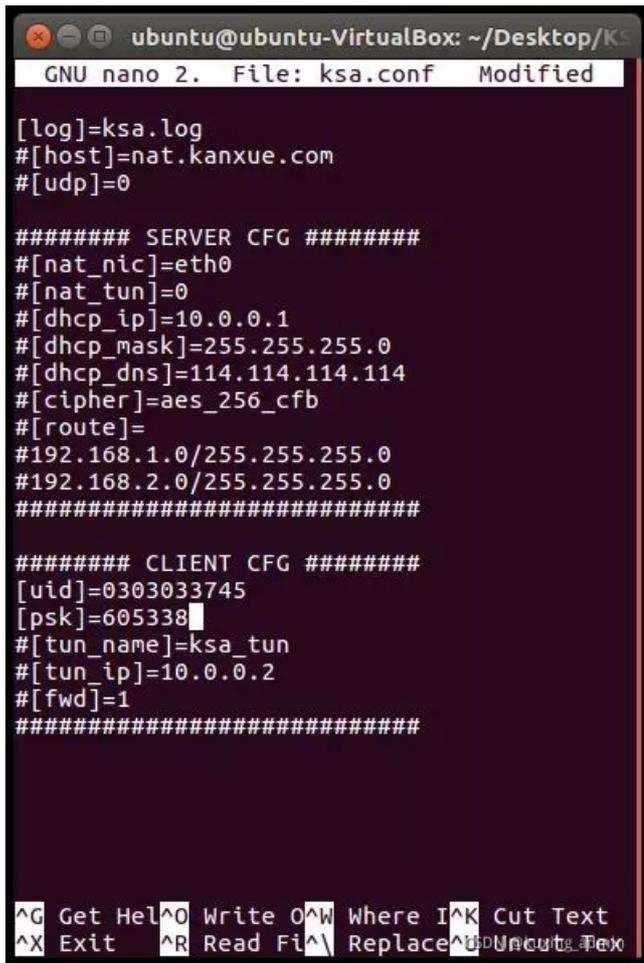
ksa_enp0s3 Link encap:UNSPEC  HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
        inet addr:10.0.0.1  P-t-P:10.0.0.1  Mask:255.255.255.0
        inet6 addr: fe80::56b4:cb8e:a11f:72e1/64  Scope:Link
        UP POINTOPOINT RUNNING NOARP MULTICAST  MTU:1400  Metric:1
        RX packets:0 errors:0 dropped:0 overruns:0 frame:0
        TX packets:234 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:500
        RX bytes:0 (0.0 B)  TX bytes:31368 (31.3 KB)

lo      Link encap:Local Loopback
        inet addr:127.0.0.1  Mask:255.0.0.0
        inet6 addr: ::1/128  Scope:Host
        UP LOOPBACK RUNNING  MTU:65536  Metric:1
        RX packets:287 errors:0 dropped:0 overruns:0 frame:0
        TX packets:287 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1000
        RX bytes:29214 (29.2 KB)  TX bytes:29214 (29.2 KB) CSDN @kuxing_admin
```

② 客户端配置

首先请确保没有任何ksa的进程在执行，有则先关闭。可以使用ps aux |grep ksa命令来查找，并使用sudo kill -pid-来杀死进程。

然后打开ksa.conf文件：配置好KSA ID和PSK，并取消[uid]和[psk]前方的#号，使其生效。最终效果如下图：



```
ubuntu@ubuntu-VirtualBox: ~/Desktop/KSA
GNU nano 2. File: ksa.conf Modified

[log]=ksa.log
#[host]=nat.kanxue.com
#[udp]=0

##### SERVER CFG #####
#[nat_nic]=eth0
#[nat_tun]=0
#[dhcp_ip]=10.0.0.1
#[dhcp_mask]=255.255.255.0
#[dhcp_dns]=114.114.114.114
#[cipher]=aes_256_cfb
#[route]=
#192.168.1.0/255.255.255.0
#192.168.2.0/255.255.255.0
#####

##### CLIENT CFG #####
[uid]=0303033745
[psk]=605338
#[tun_name]=ksa_tun
#[tun_ip]=10.0.0.2
#[fwd]=1
#####

^G Get Help ^O Write Out ^W Where I Am ^K Cut Text
^X Exit ^R Read File ^\ Replace Text ^U Undo ^T Exit
```

配置完成之后，运行sudo ./ksa_x64来启动即可。启动成功之后，可以在ifconfig中看到ksa的虚拟网卡。

```
ubuntu@ubuntu-VirtualBox:~/Desktop/KSA_linux$ nano *conf
ubuntu@ubuntu-VirtualBox:~/Desktop/KSA_linux$
ubuntu@ubuntu-VirtualBox:~/Desktop/KSA_linux$
ubuntu@ubuntu-VirtualBox:~/Desktop/KSA_linux$
ubuntu@ubuntu-VirtualBox:~/Desktop/KSA_linux$ sudo ./ksa_x64
KSA SERVER:nat.kanxue.com
KSA LINK:UDP
ubuntu@ubuntu-VirtualBox:~/Desktop/KSA_linux$
ubuntu@ubuntu-VirtualBox:~/Desktop/KSA_linux$ ifconfig
enp0s3      Link encap:Ethernet  HWaddr 08:00:27:9b:c6:b0
            inet addr:10.68.2.216  Bcast:10.68.255.255  Mask:255.255.0.0
            inet6 addr: fe80::7316:1297:bc5e:4188/64 Scope:Link
            UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
            RX packets:881549 errors:0 dropped:0 overruns:0 frame:0
            TX packets:204789 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:1000
            RX bytes:179864672 (179.8 MB)  TX bytes:19422338 (19.4 MB)

ksa_tun     Link encap:UNSPEC  HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
            inet addr:10.10.10.2  P-t-P:10.10.10.2  Mask:255.255.255.0
            inet6 addr: fe80::2b0d:70bb:3e8d:1e71/64 Scope:Link
            UP POINTOPOINT RUNNING NOARP MULTICAST  MTU:1400  Metric:1
            RX packets:0 errors:0 dropped:0 overruns:0 frame:0
            TX packets:1 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:500
            RX bytes:0 (0.0 B)  TX bytes:48 (48.0 B)

lo         Link encap:Local Loopback
            inet addr:127.0.0.1  Mask:255.0.0.0
            inet6 addr: ::1/128 Scope:Host
            UP LOOPBACK RUNNING  MTU:65536  Metric:1
            RX packets:346 errors:0 dropped:0 overruns:0 frame:0
            TX packets:346 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:1000
            RX bytes:33454 (33.4 KB)  TX bytes:33454 (33.4 KB) CSDN @kuxing_admin
```

可以尝试ping一下服务端检测连接是否成功:

```
ubuntu@ubuntu-VirtualBox:~/Desktop/KSA_linux$ ping 10.10.10.1
PING 10.10.10.1 (10.10.10.1) 56(84) bytes of data.
64 bytes from 10.10.10.1: icmp_seq=1 ttl=64 time=0.796 ms
64 bytes from 10.10.10.1: icmp_seq=2 ttl=64 time=0.690 ms
64 bytes from 10.10.10.1: icmp_seq=3 ttl=64 time=0.646 ms
64 bytes from 10.10.10.1: icmp_seq=4 ttl=64 time=0.650 ms
64 bytes from 10.10.10.1: icmp_seq=5 ttl=64 time=0.659 ms
^C
--- 10.10.10.1 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4090ms
rtt min/avg/max/mdev = 0.646/0.688/0.796/0.058 ms
ubuntu@ubuntu-VirtualBox:~/Desktop/KSA_linux$ CSDN @kuxing_admin
```

③-扩展

这里运行 ksa_x64 程序是因为 我的系统是x64，可通过 `uname -a` 来查看主机自己的系统是什么版本。

5、注意事项

- 1、远程接入分为 P2P 直连和 NAT 中转两种模式。
- 2、KSA 会优先选择 P2P 直连的模式，在该模式下服务端与客户端直接连接，速度快，不限量。
- 3、在 P2P 尝试失败的情况下，KSA 会启用 NAT 中转模式，在该模式下服务端与客户端之间的连接会经过看雪服务器中转，所有流量使用 AES-256-CFB 模式全局加密，看雪服务器不会保存流量、也无法解密。

4、在NAT中转模式，由于看雪服务器资源有限，会进行一定的限速限量措施，内测阶段会根据流量进行动态调整，恕不另行告知。

6、引用

看雪安全接入(KSA)，支持远程接入内网！

https://mp.weixin.qq.com/s/dXzfBJwVTDN-x_PYF3xLCQ