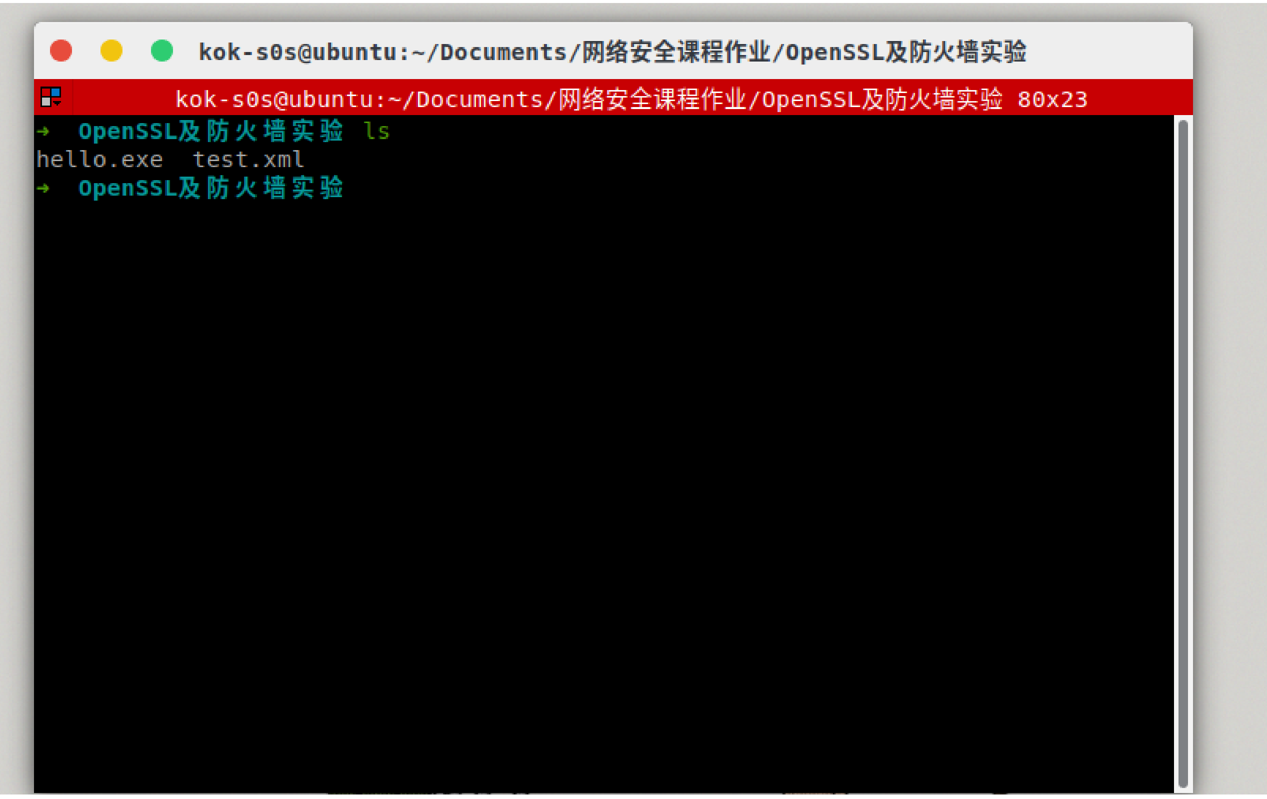
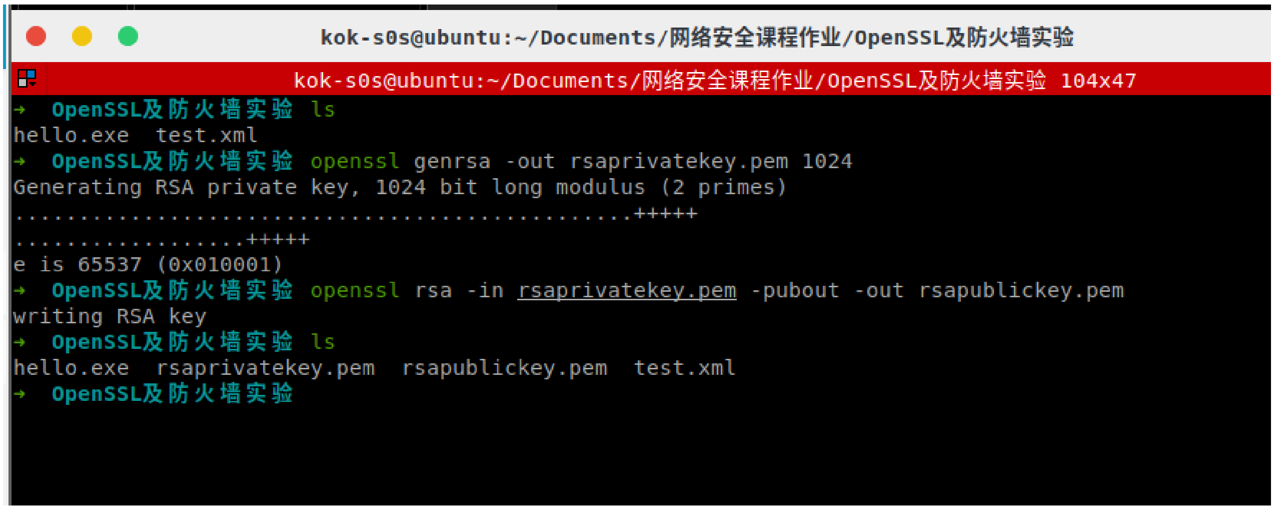
RSA



kok-s0s@ubuntu:~/Documents/网络安全课程作业/OpenSSL及防火墙实验
kok-s0s@ubuntu:~/Documents/网络安全课程作业/OpenSSL及防火墙实验 80x23

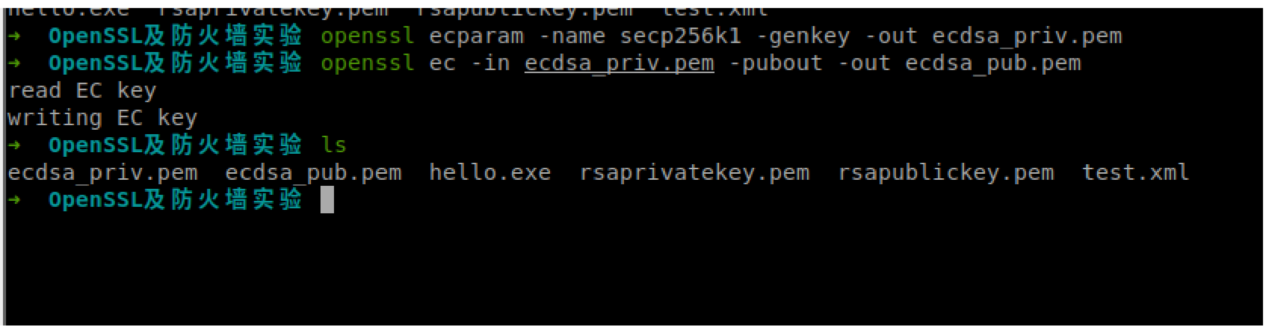
```
→ OpenSSL及防火墙实验 ls
hello.exe  test.xml
→ OpenSSL及防火墙实验
```

自己签发一对RSA和ECDSA公私钥



kok-s0s@ubuntu:~/Documents/网络安全课程作业/OpenSSL及防火墙实验
kok-s0s@ubuntu:~/Documents/网络安全课程作业/OpenSSL及防火墙实验 104x47

```
→ OpenSSL及防火墙实验 ls
hello.exe  test.xml
→ OpenSSL及防火墙实验 openssl genrsa -out rsaprivatekey.pem 1024
Generating RSA private key, 1024 bit long modulus (2 primes)
...............................................+++++
..................+++++
e is 65537 (0x010001)
→ OpenSSL及防火墙实验 openssl rsa -in rsaprivatekey.pem -pubout -out rsapublickey.pem
writing RSA key
→ OpenSSL及防火墙实验 ls
hello.exe  rsaprivatekey.pem  rsapublickey.pem  test.xml
→ OpenSSL及防火墙实验
```

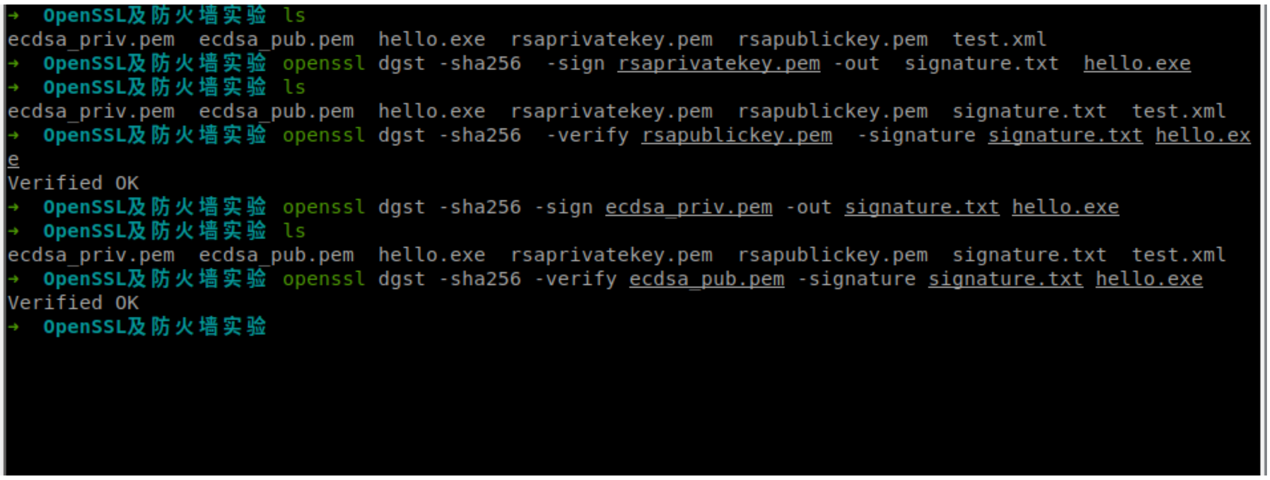


```
hello.exe  rsaprivatekey.pem  rsapublickey.pem  test.xml
→ OpenSSL及防火墙实验 openssl ecparam -name secp256k1 -genkey -out ecdsa_priv.pem
→ OpenSSL及防火墙实验 openssl ec -in ecdsa_priv.pem -pubout -out ecdsa_pub.pem
read EC key
writing EC key
→ OpenSSL及防火墙实验 ls
ecdsa_priv.pem  ecdsa_pub.pem  hello.exe  rsaprivatekey.pem  rsapublickey.pem  test.xml
→ OpenSSL及防火墙实验
```

Q1

对一个exe文件生成签名/验签

RSA && ECDSA



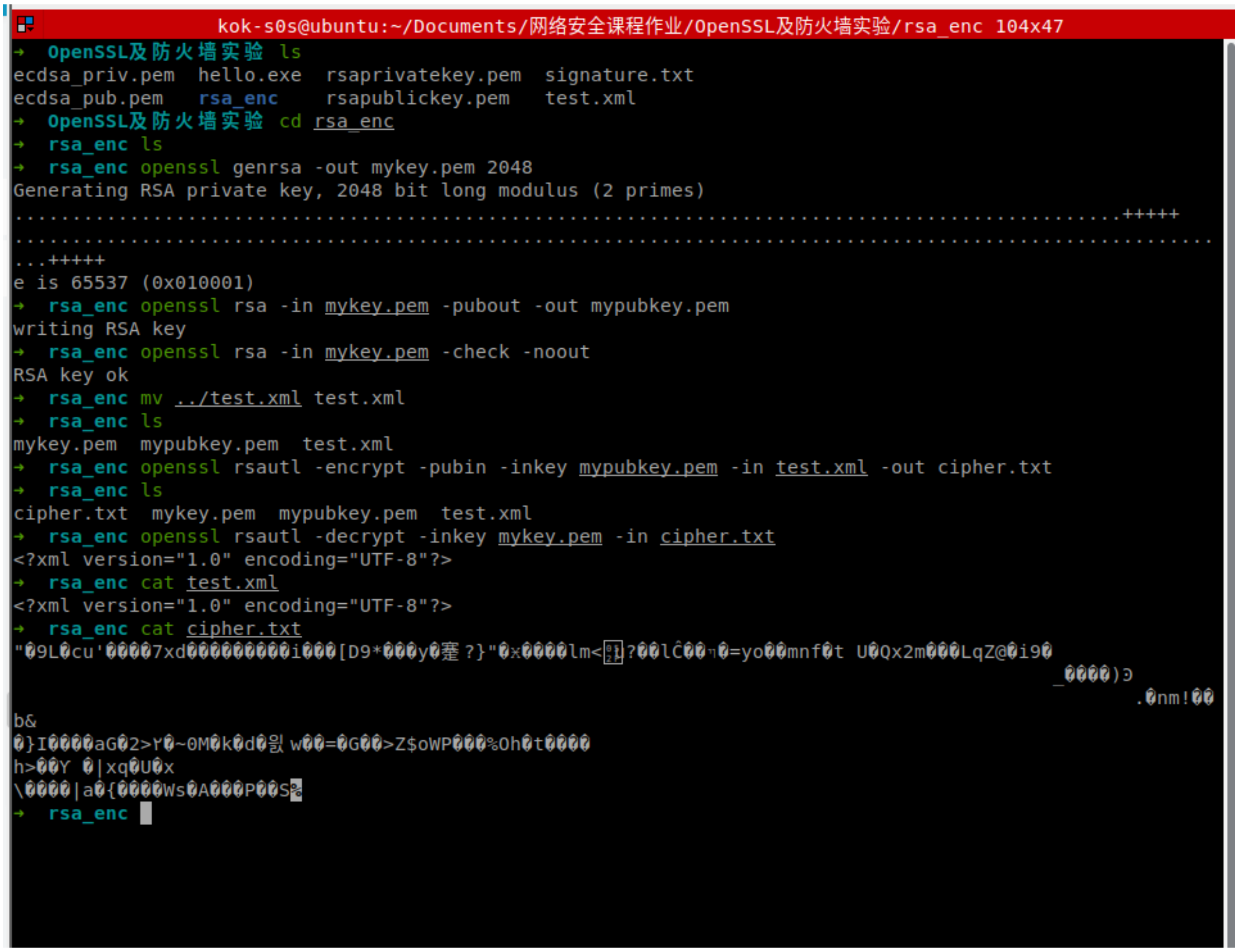
```
➜  OpenSSL及防火墙实验 ls
ecdsa_priv.pem  ecdsa_pub.pem  hello.exe  rsaprivatekey.pem  rsapublickey.pem  test.xml
➜  OpenSSL及防火墙实验 openssl dgst -sha256  -sign rsaprivatekey.pem -out  signature.txt  hello.exe
➜  OpenSSL及防火墙实验 ls
ecdsa_priv.pem  ecdsa_pub.pem  hello.exe  rsaprivatekey.pem  rsapublickey.pem  signature.txt  test.xml
➜  OpenSSL及防火墙实验 openssl dgst -sha256  -verify rsapublickey.pem  -signature signature.txt hello.ex
e
Verified OK
➜  OpenSSL及防火墙实验 openssl dgst -sha256 -sign ecdsa_priv.pem -out signature.txt hello.exe
➜  OpenSSL及防火墙实验 ls
ecdsa_priv.pem  ecdsa_pub.pem  hello.exe  rsaprivatekey.pem  rsapublickey.pem  signature.txt  test.xml
➜  OpenSSL及防火墙实验 openssl dgst -sha256 -verify ecdsa_pub.pem -signature signature.txt hello.exe
Verified OK
➜  OpenSSL及防火墙实验
```

Q2

对一个xml文件进行加密/解密

DSA算法只能进行签名，不能用于加密解密

RSA加解密



```
kok-s0s@ubuntu:~/Documents/网络安全课程作业/OpenSSL及防火墙实验/rsa_enc 104x47
→  OpenSSL及防火墙实验 ls
ecdsa_priv.pem  hello.exe  rsaprivatekey.pem  signature.txt
ecdsa_pub.pem   rsa_enc    rsapublickey.pem   test.xml
→  OpenSSL及防火墙实验 cd rsa_enc
→  rsa_enc ls
→  rsa_enc openssl genrsa -out mykey.pem 2048
Generating RSA private key, 2048 bit long modulus (2 primes)
.............................................................................................+++++
.........................................................................................................
...+++++
e is 65537 (0x010001)
→  rsa_enc openssl rsa -in mykey.pem -pubout -out mypubkey.pem
writing RSA key
→  rsa_enc openssl rsa -in mykey.pem -check -noout
RSA key ok
→  rsa_enc mv ../test.xml test.xml
→  rsa_enc ls
mykey.pem  mypubkey.pem  test.xml
→  rsa_enc openssl rsautl -encrypt -pubin -inkey mypubkey.pem -in test.xml -out cipher.txt
→  rsa_enc ls
cipher.txt  mykey.pem  mypubkey.pem  test.xml
→  rsa_enc openssl rsautl -decrypt -inkey mykey.pem -in cipher.txt
<?xml version="1.0" encoding="UTF-8"?>
→  rsa_enc cat test.xml
<?xml version="1.0" encoding="UTF-8"?>
→  rsa_enc cat cipher.txt
"�9L�cu'����7xd����������i���[D9*���y�蹇?}"�x����lm<�?��lĈ��¬�=yo��mnf�t U�Qx2m���LqZ@�i9�
                                                                                                         _����)϶
                                                                                                                .�nm!��
b&
�}I����aG�2>ϒ�~0M�k�d�읬 w��=�G��>Z$oWP���%0h�t����
h>��Y �|xq�U�x
\����|a�{����Ws�A���P��S%
→  rsa_enc
```

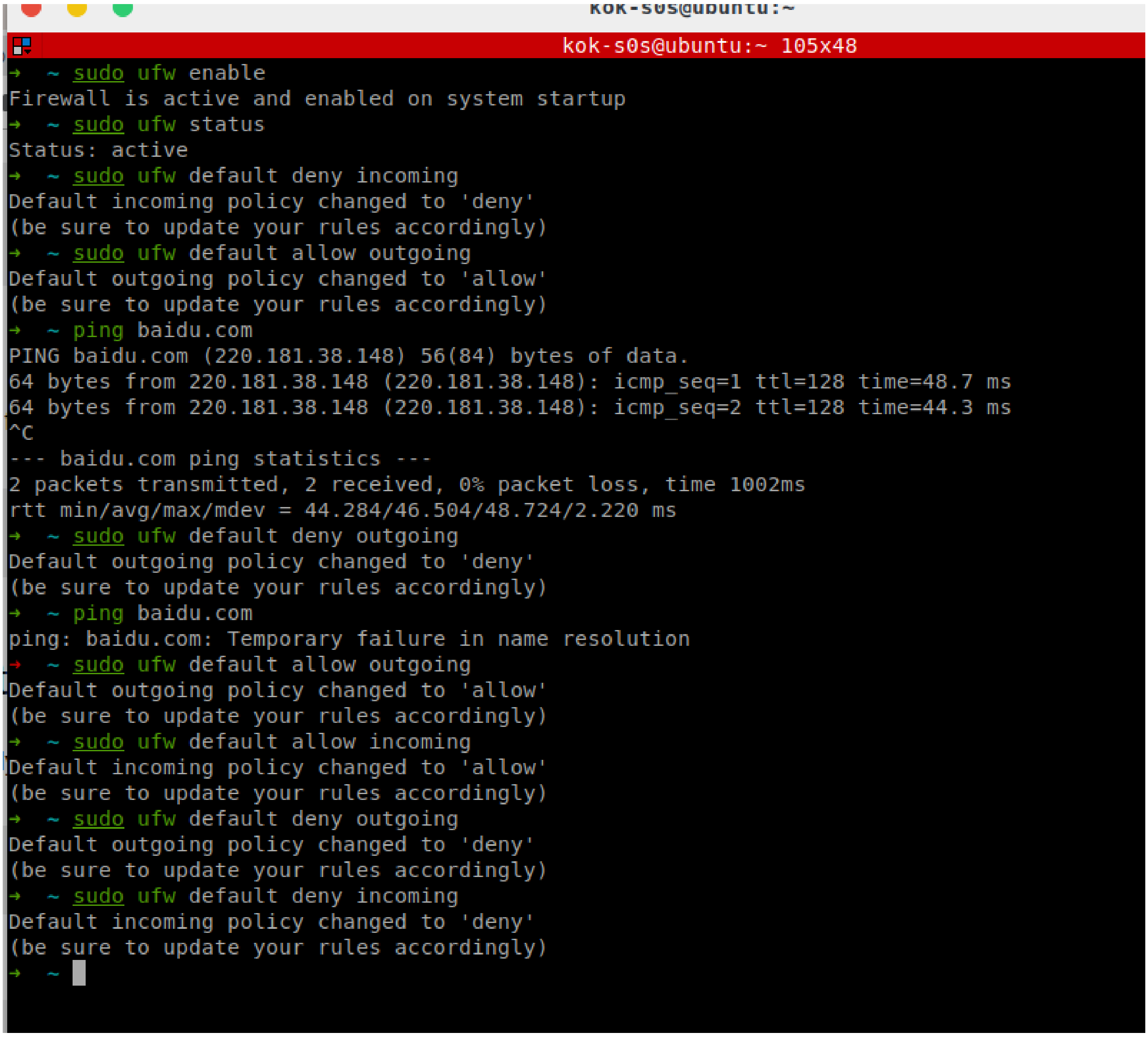
防火墙

系统：Ubuntu20.04

工具：gufw，ufw

task：

- 外部用户不可以访问内部
- 内部用户只可以访问外部80端口

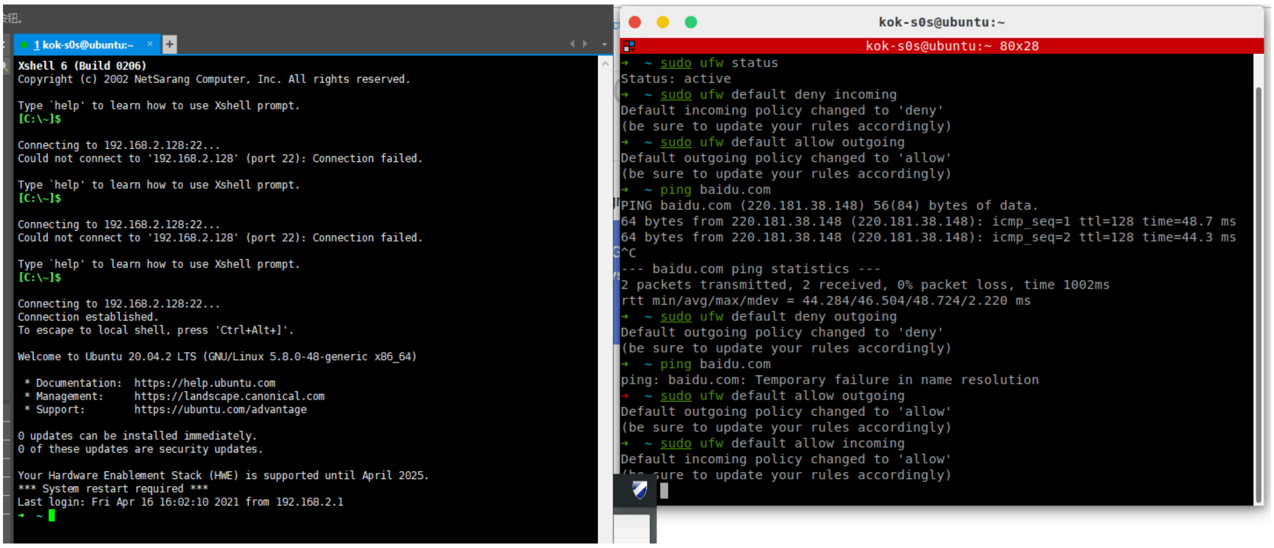


```
➜  ~ sudo ufw enable
Firewall is active and enabled on system startup
➜  ~ sudo ufw status
Status: active
➜  ~ sudo ufw default deny incoming
Default incoming policy changed to 'deny'
(be sure to update your rules accordingly)
➜  ~ sudo ufw default allow outgoing
Default outgoing policy changed to 'allow'
(be sure to update your rules accordingly)
➜  ~ ping baidu.com
PING baidu.com (220.181.38.148) 56(84) bytes of data.
64 bytes from 220.181.38.148 (220.181.38.148): icmp_seq=1 ttl=128 time=48.7 ms
64 bytes from 220.181.38.148 (220.181.38.148): icmp_seq=2 ttl=128 time=44.3 ms
^C
--- baidu.com ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1002ms
rtt min/avg/max/mdev = 44.284/46.504/48.724/2.220 ms
➜  ~ sudo ufw default deny outgoing
Default outgoing policy changed to 'deny'
(be sure to update your rules accordingly)
➜  ~ ping baidu.com
ping: baidu.com: Temporary failure in name resolution
➜  ~ sudo ufw default allow outgoing
Default outgoing policy changed to 'allow'
(be sure to update your rules accordingly)
➜  ~ sudo ufw default allow incoming
Default incoming policy changed to 'allow'
(be sure to update your rules accordingly)
➜  ~ sudo ufw default deny outgoing
Default outgoing policy changed to 'deny'
(be sure to update your rules accordingly)
➜  ~ sudo ufw default deny incoming
Default incoming policy changed to 'deny'
(be sure to update your rules accordingly)
➜  ~ 
```

测试外部用户能否访问该主机

Xshell链接

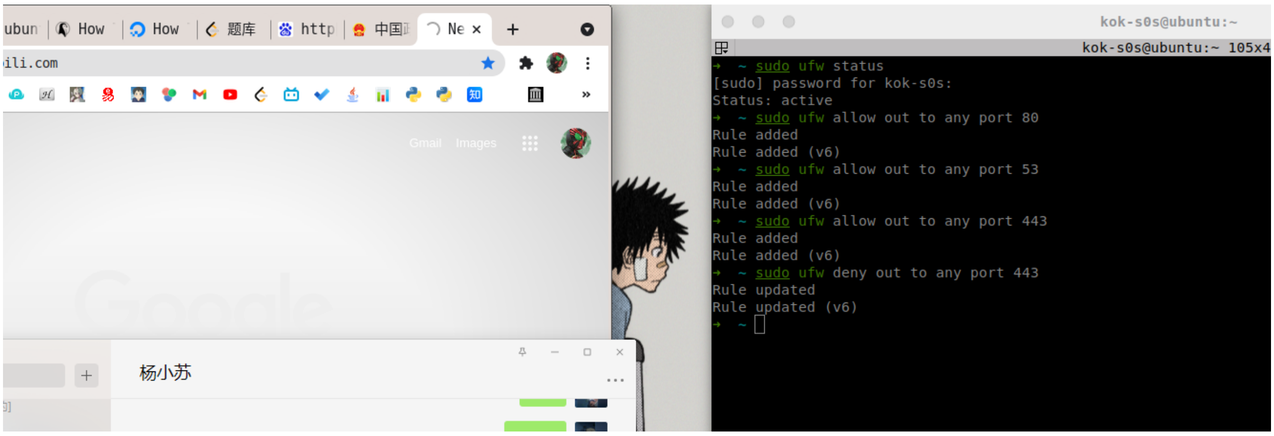
将 `Incoming` 和 `Outgoing` 都 `deny` 后，使用Xshell进行访问连接，连接失败。



```
Xshell 6 (Build 0206)
Copyright (c) 2002 NetSarang Computer, Inc. All rights reserved.

Type `help' to learn how to use Xshell prompt.
[C:\~]$

Connecting to 192.168.2.128:22...
Could not connect to '192.168.2.128' (port 22): Connection failed.

Type `help' to learn how to use Xshell prompt.
[C:\~]$

Connecting to 192.168.2.128:22...
Could not connect to '192.168.2.128' (port 22): Connection failed.

Type `help' to learn how to use Xshell prompt.
[C:\~]$

Connecting to 192.168.2.128:22...
Connection established.
To escape to local shell, press 'Ctrl+Alt+]'.

Welcome to Ubuntu 20.04.2 LTS (GNU/Linux 5.8.0-48-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

0 updates can be installed immediately.
0 of these updates are security updates.

Your Hardware Enablement Stack (HWE) is supported until April 2025.
*** System restart required ***
Last login: Fri Apr 16 16:02:10 2021 from 192.168.2.1
➜  ~ 
```

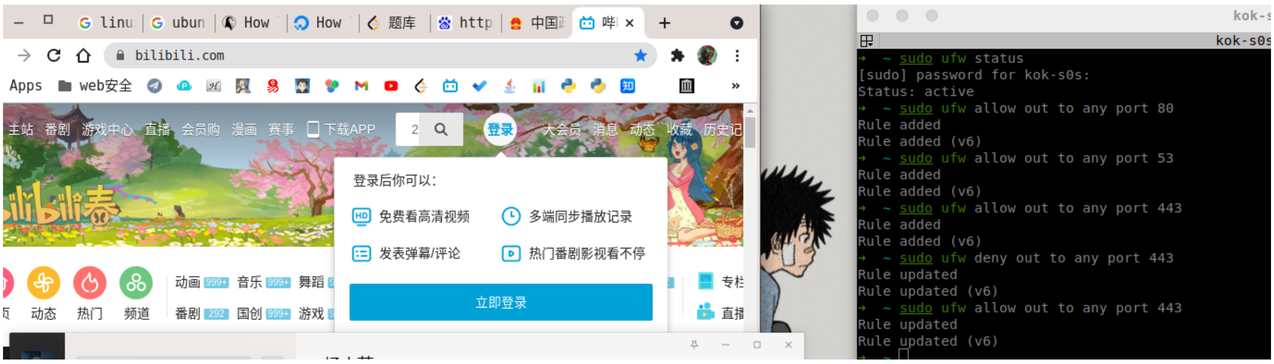
```
➜  ~ sudo ufw status
Status: active
➜  ~ sudo ufw default deny incoming
Default incoming policy changed to 'deny'
(be sure to update your rules accordingly)
➜  ~ sudo ufw default allow outgoing
Default outgoing policy changed to 'allow'
(be sure to update your rules accordingly)
➜  ~ ping baidu.com
PING baidu.com (220.181.38.148) 56(84) bytes of data.
64 bytes from 220.181.38.148 (220.181.38.148): icmp_seq=1 ttl=128 time=48.7 ms
64 bytes from 220.181.38.148 (220.181.38.148): icmp_seq=2 ttl=128 time=44.3 ms
^C
--- baidu.com ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1002ms
rtt min/avg/max/mdev = 44.284/46.504/48.724/2.220 ms
➜  ~ sudo ufw default deny outgoing
Default outgoing policy changed to 'deny'
(be sure to update your rules accordingly)
➜  ~ ping baidu.com
ping: baidu.com: Temporary failure in name resolution
➜  ~ sudo ufw default allow outgoing
Default outgoing policy changed to 'allow'
(be sure to update your rules accordingly)
➜  ~ sudo ufw default allow incoming
Default incoming policy changed to 'allow'
(be sure to update your rules accordingly)
```

测试内部用户只能通过80端口访问外部



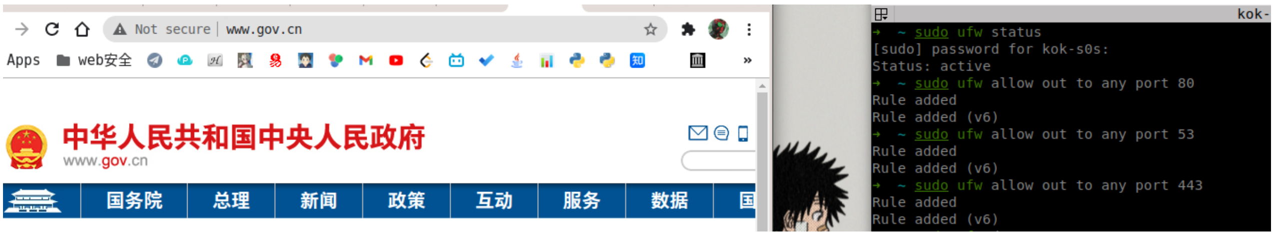
```
➜  ~ sudo ufw status
[sudo] password for kok-s0s:
Status: active
➜  ~ sudo ufw allow out to any port 80
Rule added
Rule added (v6)
➜  ~ sudo ufw allow out to any port 53
Rule added
Rule added (v6)
➜  ~ sudo ufw allow out to any port 443
Rule added
Rule added (v6)
➜  ~ sudo ufw deny out to any port 443
Rule updated
Rule updated (v6)
➜  ~
```

先将 `HTTP:80` ， `HTTPS:443` ， `DNS:53` 端口都开放，连接再将 `443` 端口关闭，访问B站 `https://bilibili.com` 失败，浏览器显示一直是加载状态。


bilibili.com
主站 番剧 游戏中心 直播 会员购 漫画 赛事 下载APP
登录 大会员 消息 动态 收藏 历史记
登录后你可以：
免费看高清视频
多端同步播放记录
发表弹幕/评论
热门番剧影视看不停
立即登录
动态 热门 频道
动画 音乐 舞蹈 番剧 国创 游戏

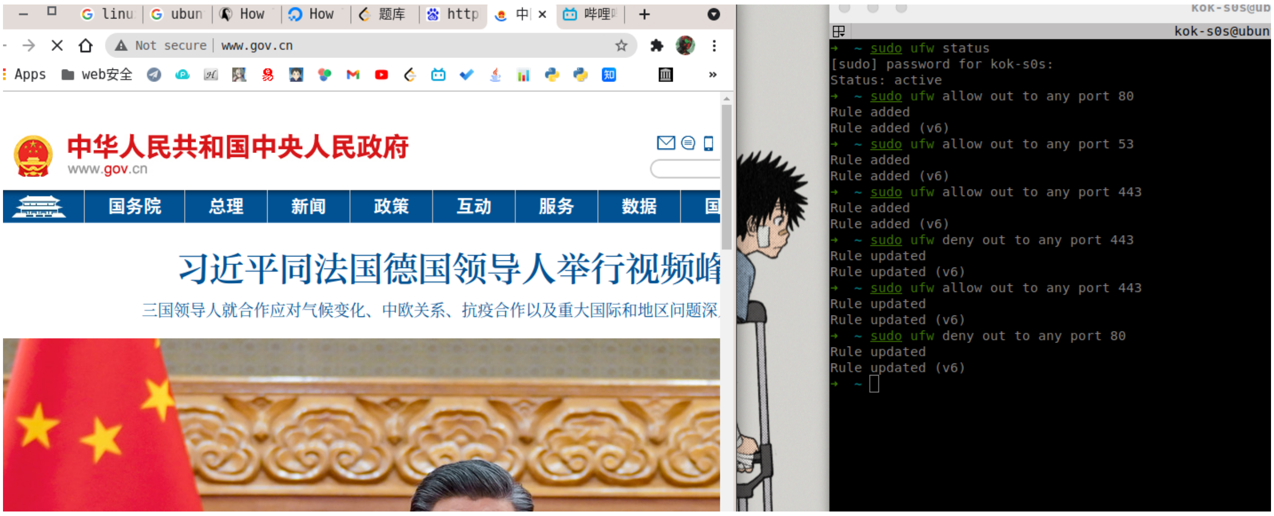
```
➜  ~ sudo ufw status
[sudo] password for kok-s0s:
Status: active
➜  ~ sudo ufw allow out to any port 80
Rule added
Rule added (v6)
➜  ~ sudo ufw allow out to any port 53
Rule added
Rule added (v6)
➜  ~ sudo ufw allow out to any port 443
Rule added
Rule added (v6)
➜  ~ sudo ufw deny out to any port 443
Rule updated
Rule updated (v6)
➜  ~ sudo ufw allow out to any port 443
Rule updated
Rule updated (v6)
```

我将 `443` 端口再次开放，此时浏览器加载完毕，我能够正常访问 `https` 网站。


Not secure | www.gov.cn
中华人民共和国中央人民政府
www.gov.cn
国务院 总理 新闻 政策 互动 服务 数据

```
➜  ~ sudo ufw status
[sudo] password for kok-s0s:
Status: active
➜  ~ sudo ufw allow out to any port 80
Rule added
Rule added (v6)
➜  ~ sudo ufw allow out to any port 53
Rule added
Rule added (v6)
➜  ~ sudo ufw allow out to any port 443
Rule added
Rule added (v6)
```

然后这个 `80` 端口开启后，我是能正常访问 `http` 网站。



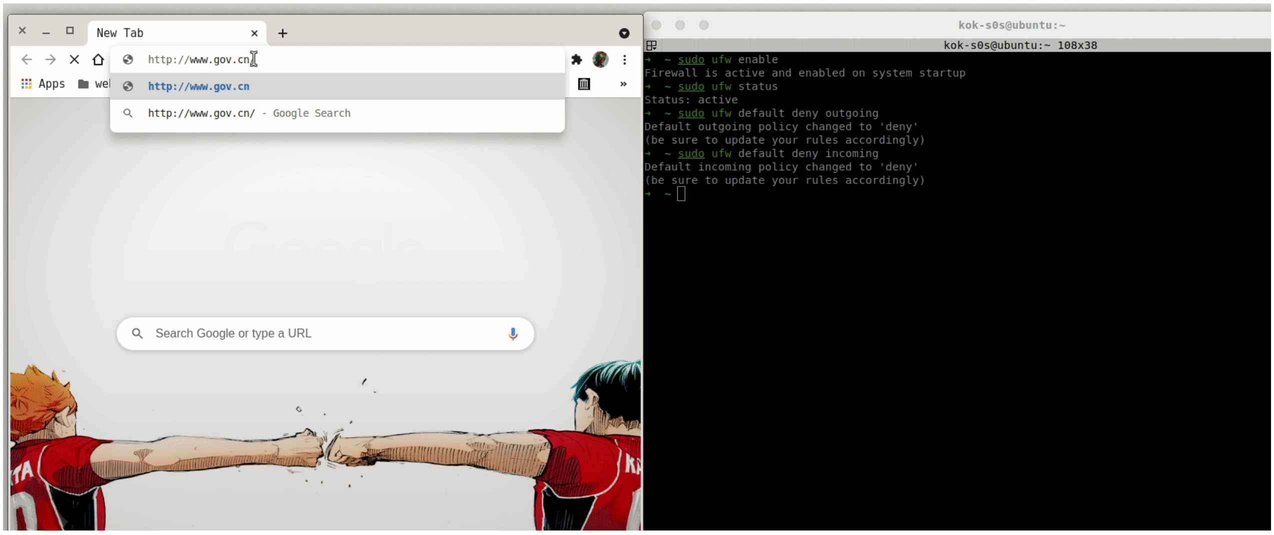
习近平同法国德国领导人举行视频峰

三国领导人就合作应对气候变化、中欧关系、抗疫合作以及重大国际和地区问题深

```
kok-s0s@ubun
→  ~ sudo ufw status
[sudo] password for kok-s0s:
Status: active
→  ~ sudo ufw allow out to any port 80
Rule added
Rule added (v6)
→  ~ sudo ufw allow out to any port 53
Rule added
Rule added (v6)
→  ~ sudo ufw allow out to any port 443
Rule added
Rule added (v6)
→  ~ sudo ufw deny out to any port 443
Rule updated
Rule updated (v6)
→  ~ sudo ufw allow out to any port 443
Rule updated
Rule updated (v6)
→  ~ sudo ufw deny out to any port 80
Rule updated
Rule updated (v6)
→  ~ 
```

我再把 `80` 关了，刷新是一直在加载的状态。

具体演示效果



New Tab
http://www.gov.cn
http://www.gov.cn
http://www.gov.cn/ - Google Search
Apps
Search Google or type a URL

```
kok-s0s@ubuntu:~
kok-s0s@ubuntu:~ 108x38
→  ~ sudo ufw enable
Firewall is active and enabled on system startup
→  ~ sudo ufw status
Status: active
→  ~ sudo ufw default deny outgoing
Default outgoing policy changed to 'deny'
(be sure to update your rules accordingly)
→  ~ sudo ufw default deny incoming
Default incoming policy changed to 'deny'
(be sure to update your rules accordingly)
→  ~ 
```