

GSM 网关配置 SSH 反向连接

作用：使公司内网工作机透过公网服务器访问客户内网的 GSM 网关，以便调试

（一）服务器配置

Openvox-Wireless-Gateway

IP: 172.16.8.186

Port: SSH 12345, Web Port 80

Username: Web admin, SSH super

公网服务器

IP: 106.185.43.194

SSH Port: 22

SSH Username: root

工作机

IP: 172.16.8.180

（二）配置步骤

- 1) 端口映射（在 GSM 网关上进行操作）
1. 将网关上的 80 端口映射到公网服务器的 10241 端口

A. ssh -f -N -R 10241:localhost:80 root@106.185.43.194 -p 22

B. 需要输入公网服务器密码

2. 将网关上的 12345 端口映射到公网服务器的 10242 端口

A. ssh -f -N -R 10242:localhost:12345 root@106.185.43.194 -p 22

B. 需要输入公网服务器密码

```
root@Openvox-Wireless-Gateway:~# ssh -f -N -R 10241:localhost:80 root@106.185.43.194 -p 22
root@106.185.43.194's password:
root@Openvox-Wireless-Gateway:~#
root@Openvox-Wireless-Gateway:~# ssh -f -N -R 10242:localhost:12345 root@106.185.43.194 -p 22
root@106.185.43.194's password:
root@Openvox-Wireless-Gateway:~#
```

- 2) 配置公网服务器共享 SSH 隧道（在公网服务器上进行操作）
1. 编辑 /etc/ssh/sshd_conf: 设置 GatewayPorts yes

2. service iptables start

3. service sshd restart

```
[root@li754-194 ~]# vim /etc/ssh/sshd_config
[root@li754-194 ~]# service iptables start
[root@li754-194 ~]# service sshd restart
Stopping sshd: [ OK ]
Starting sshd: [ OK ]
[root@li754-194 ~]# netstat -ntpl
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:22             0.0.0.0:*               LISTEN      16790/sshd
tcp        0      0 0.0.0.0:1723           0.0.0.0:*               LISTEN      2290/pptpd
tcp        0      0 0.0.0.0:10241          0.0.0.0:*               LISTEN      16561/sshd
tcp        0      0 0.0.0.0:10242          0.0.0.0:*               LISTEN      16581/sshd
tcp        0      0 :::22                  :::*                     LISTEN      16790/sshd
tcp        0      0 :::10241                :::*                     LISTEN      16561/sshd
tcp        0      0 :::10242                :::*                     LISTEN      16581/sshd
[root@li754-194 ~]#
```

（三）使用 SSH 隧道

- 1) 从工作机透过公网服务器访问 GSM 网关（在内网工作机上进行操作）

访问 Web: 浏览器使用 106.185.43.194:10241 登陆, 输入 GSM 网关 Web端用户名和密码
访问 SSH: Xshell 使用 ssh 106.185.43.194 10242 登陆, 输入 GSM 网关 SSH 端用户名和密码

```
106.185.43.194:10242 - Xshell 4
新建 文件夹 重新连接 172.16.8.186:12345 2 106.185.43.194:22 3 106.185.43.194:10242 x
ssh://super@106.185.43.194:10242

Xshell for Xmanager Enterprise 4 (Build 0223)
Copyright (c) 2002-2013 NetSarang Computer, Inc. All rights reserved.

Type 'help' to learn how to use Xshell prompt.
Xshell:\> ssh super@106.185.43.194 10242

Connecting to 106.185.43.194:10242...
Connection established.
To escape to local shell, press 'Ctrl+Alt+J'.

sh: /usr/X11R6/bin/xauth: not found

BusyBox v1.4.2 (2014-07-09 10:37:25 CST) Built-in shell (ash)
Enter 'help' for a list of built-in commands.

|_| .----- .----- | |_| .----- .-----
|_| - | | - | - | | | | | | - | | -
|_| | | | | | | | | | | | | | | | |
|_| | | W I R E L E S S F R E E D O M

Openvox Wireless Gateway Technologies - Build in 2014-09-24 11:33:58
-----
root@Openvox-Wireless-Gateway:~# ifconfig eth0 | sed -n "2p" | awk '{print substr($2,1)}' | cut -d ':' -f 2
172.16.8.186
root@Openvox-Wireless-Gateway:~#
```

- 2) 关闭 SSH 隧道 (在 GSM 网关上进行操作)
使用 ps 命令查找ssh 相应的端口转发进程, 使用 kill 命令将其杀掉

```
4107 root      420 S      ssh -f -N -R 10241:localhost:80 root@106.185.43.194 -
4110 root      408 S      ssh -f -N -R 10242:localhost:12345 root@106.185.43.19
4112 root      500 S      dropbear -p 12345
4113 root      464 S      -ash
4124 root      368 R      ps -ef
root@Openvox-Wireless-Gateway:~# kill 4107 4110
root@Openvox-Wireless-Gateway:~#
```

- 3) 关闭监听的端口 (在公网服务器上进行操作)
使用 lsof 命令查找监听端口的进程, 使用 kill 命令将其杀掉

```
[root@li754-194 ~]# lsof -i :10241
COMMAND PID USER  FD  TYPE  DEVICE  SIZE/OFF  NODE NAME
sshd     973  root   7u   IPv4  4394862      0t0  TCP *:10241 (LISTEN)
sshd     973  root   8u   IPv6  4394863      0t0  TCP *:10241 (LISTEN)
[root@li754-194 ~]# kill 973
[root@li754-194 ~]# netstat -ntpl
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      16790/sshd
tcp        0      0 0.0.0.0:1723            0.0.0.0:*               LISTEN      2290/pptpd
tcp        0      0 :::22                  :::*                   LISTEN      16790/sshd
[root@li754-194 ~]#
```

(四) SSH 无密码登陆

1. 使用 ssh-keygen 生成公钥和私钥 (一路回车, 可以不输入任何信息)
2. 使用 ssh-copy-id 将公钥拷贝到公网服务器, 需输入一次公网服务器密码
3. 以后便可无需密码连接公网服务器

```
[~]# rm -rf /root/.ssh/*
[~]# ssh-keygen → 生成公钥和私钥
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /root/.ssh/id_rsa.
Your public key has been saved in /root/.ssh/id_rsa.pub.
The key fingerprint is:
4d:22:20:d2:91:8b:a0:43:f0:5f:76:53:7c:18:2d:eb root@server88
The key's randomart image is:
+--[ RSA 2048 ]-----+
|+.oo. .o+ |
|+.o. . .+ o |
|+... + + .+ |
|+ .. o o =. |
| . . S.. |
| . E |
| |
| |
+-----+
[~]# ssh-copy-id root@172.16.8.199 -p 22 → 拷贝公钥到远端服务器
The authenticity of host '172.16.8.199 (172.16.8.199)' can't be established.
ECDSA key fingerprint is 6f:a7:66:ce:cf:80:52:4d:78:db:83:51:37:14:86:fe.
Are you sure you want to continue connecting (yes/no)? yes
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter out any that are already installed
/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you are prompted now it is to install the new keys
root@172.16.8.199's password: → 远端服务器密码

Number of key(s) added: 1

Now try logging into the machine, with: "ssh -p '22' 'root@172.16.8.199'"
and check to make sure that only the key(s) you wanted were added.

[~]# ssh -f -N -R 50000:localhost:80 root@172.16.8.199 -p 22 → 无密码访问
[~]#
```

（五）SSH 反向连接自动重连

1. 使用 autossh

```
autossh -M 20241 -f -N -R 10241:localhost:80 root@106.185.43.194 -p 22
-M port[:echo_port], port 为监听端口, 默认的 echo_port=port+1
autossh 通过 port 和 echo_port 监听 ssh 状态, 从 port 发送数据, echo_port 接收数据
```

注: 在 CentOS 上测试, 无数据流经过时, 5-6 分钟连接失效, 但进程仍在