



珂儿吖

随笔- 36 文章- 0 评论- 70 阅读- 45万

博客园 首页 新随笔 联系 管理 订阅 XML

2021年8月						
日	一	二	三	四	五	六
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31	1	2	3	4
5	6	7	8	9	10	11

昵称：珂儿吖

园龄：4年

粉丝：416

关注：8

+加关注

最新随笔

- 1.企业级nosql数据库应用与实战-redis
- 2.Linux企业运维人员必备150个命令汇总
- 3.自动化运维工具——puppet详解（二）
- 4.自动化运维工具——puppet详解（一）
- 5.自动化运维工具——ansible详解（二）
- 6.自动化运维工具——ansible详解（一）
- 7.项目实战——企业级Zabbix监控实战（一）
- 8.实现基于tomcat集群会话保持
- 9.mysql实现高可用架构之MHA
- 10.实战项目——mysql主从架构的实现

积分与排名

积分 - 66714

排名 - 18124

SSH端口转发详解及实例

一、SSH端口转发简介

SSH会自动加密和解密所有SSH客户端与服务端之间的网络数据。但是，SSH还能够将其他TCP端口的网络数据通过SSH链接来转发，并且自动提供了相应的加密及解密服务。这一过程也被叫做“隧道”（tunneling），这是因为SSH为其他TCP链接提供了一个安全的通道来进行传输而得名。例如，Telnet，SMTP，LDAP这些TCP应用均能够从中得益，避免了用户名，密码以及隐私信息的明文传输。而与此同时，如果工作环境中的防火墙限制了一些网络端口的使用，但是允许SSH的连接，也能够将通过将TCP用端口转发来使用SSH进行通讯。

1.1 SSH端口转发的两大功能

- 加密SSH Client端至SSH Server端之间的通讯数据。
- 突破防火墙的限制完成一些之前无法建立的TCP连接。

二、本地转发

随笔分类

shell脚本(1)
vim(1)
xshell(1)
文本处理(2)
正则表达式(2)

随笔档案

2017年12月(7)
2017年11月(7)
2017年10月(4)
2017年9月(4)
2017年8月(11)
2017年7月(3)

阅读排行榜

1. 自动化运维工具——ansible详解
(一) (179493)
2. 自动化运维工具——puppet详解
(一) (76207)
3. SSH端口转发详解及实例(51731)
4. mysql实现高可用架构之MHA(36724)
5. 自动化运维工具——ansible详解
(二) (19341)
6. 项目实战——企业级Zabbix监控实战
(一) (15259)
7. 私人订制——属于你自己的Linux(9477)
8. 实战项目——mysql主从架构的实现(7387)
9. Linux企业运维人员必备150个命令汇总(6438)
10. 自动化运维工具——puppet详解
(二) (6261)

评论排行榜

1. 自动化运维工具——ansible详解
(一) (10)
2. mysql实现高可用架构之MHA(10)
3. SSH端口转发详解及实例(8)
4. 私人订制——属于你自己的Linux(5)
5. 企业级nosql数据库应用与实战-redis(4)

推荐排行榜

命令: -L

**localport:remotehost:remotehostport
sshserver**

说明: localport
号

本机开启的端口

remotehost

最终连接机器的

IP地址

remotehostport

转发机器的端口

号

sshserver

转发机器的IP地

址

选项: -f 后台启用

-N 不打开远程shell, 处于等待状态 (不加-N则直接登录进去)

-g 启用网关功能

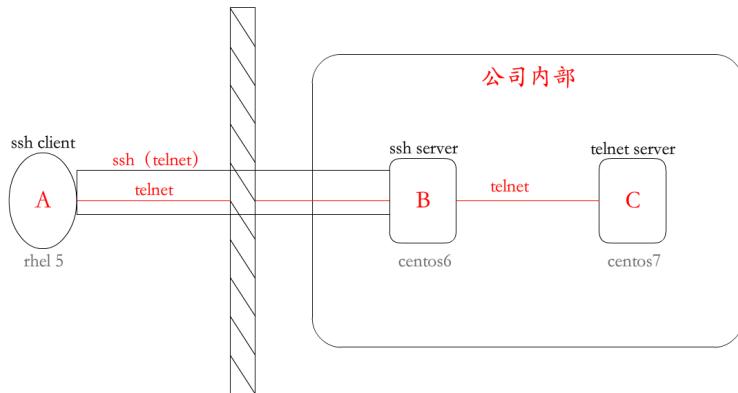
接下来, 我们通过实验来详细的说明一下如何实现本地转发:

实验一：实现SSH端口转发——本地转发

- 背景: 企业内部C服务器只允许telnet连接(23端口)访问, 不允许外部直接访问, B服务器是一个ssh服务器; 有一个用户需要从外部连接到企业内部的C服务器。
- 前提: 防火墙允许22端口进来(或者企业内部有一个堡垒机, ssh -t 通过堡垒机进去)。
- 原理: A用户通过ssh协议连接到B机器上, 再通过B机器做跳板, 连接至C机器。

1. 自动化运维工具——ansible详解
(一) (174)
2. 自动化运维工具——ansible详解
(二) (49)
3. 自动化运维工具——puppet详解
(一) (39)
4. 项目实战——企业级Zabbix监控实战
(一) (34)
5. SSH端口转发详解及实例(28)

- 机器：rhel5模拟A用户，centos6模拟B机器，centos7模拟C机器
- 图示如下：



- 实验步骤：

1) 模拟C机器不允许A用户连接，并且开启B机器的telnet服务端口23。

在centos7上输入以下口令：

```
iptables -A INPUT -s 192.168.191.55 -j REJECT
```

```
[root@centos7 ~]# iptables -A INPUT -s 192.168.191.55 -j REJECT
```

此时，从rhel5用ssh命令连接centos7，是拒绝的：

```
[root@centos7 ~]# ssh 192.168.191.77
ssh: connect to host 192.168.191.77 port 22: Connection refused
```

同时，我们还要开启7的telnet服务端口23：

```
systemctl start telnet.socket
```

用ss -ntl命令可以查看的服务端口是否已开启

```
[root@centos7 ~]# systemctl start telnet.socket
[root@centos7 ~]# ss -ntl
State Recv-Q Send-Q Local Address:Port Peer Address:Port
LISTEN 0 128 *:111 *:*
LISTEN 0 128 *:22 *:*
LISTEN 0 128 127.0.0.1:631 127.0.0.1:25
LISTEN 0 100 *:111 127.0.0.1:25
LISTEN 0 128 :::111 :::22
LISTEN 0 128 :::23 :::*
LISTEN 0 128 :::631 :::*
LISTEN 0 100 :::1:25 :::*
```

2) 开启端口转发 (telnet隧道)

首先，我们在5机器上确认已经开启的端口有哪些：

(root@el6) [~]# ss -ntl	Local Address:Port	Peer Address:Port
Recv-Q Send-Q		
0 0	127.0.0.1:2208	*
0 0	*:1111	*
0 0	127.0.0.1:631	*
0 0	127.0.0.1:22	*
0 0	*:825	*
0 0	127.0.0.1:2207	*
0 0	:::22	:::*

我们使用的端口是9527端口，从上图中我么已经看出，9527端口没有被占用，所以我们可以使用~

接着我们建立本地转发的隧道（5上输入以下命令）：

```
ssh -L 9527:192.168.191.77:23 -fN  
192.168.191.66
```

```
[root@rhel5 ~]# ssh -L 9527:192.168.191.77:23 -fN 192.168.191.66  
root@192.168.191.66's password:  
[root@rhel5 ~]# 已成功建立隧道，但是是后台运行  
[root@rhel5 ~]# |
```

在注用，我们可以

在这里，我们可以使用**ps aux**不查询后台运行的进程。也可以通过**ss -nt**查看接口连接情况：

```
[root@rhel6 ~]# ss -nt
State Recv-Q Send-Q
ESTAB      0      0
ESTAB      0     180
ESTAB      0      1
[root@rhel6 ~]#
```

```
[root@centos6 ~]# ss -nt
State      Recv-Q Send-Q          Local Address:Port          Peer Address:Port
ESTAB      0        0              192.168.191.66:22       connect()已经看到了有一个连接连接 192.168.191.55:42500
LISTEN    0        64             192.168.191.66:22       192.168.191.1:8960
[root@centos6 ~]#
```

3) 在rhel5上输入以下命令，用9527端口连接自己。

telnet 127.0.0.1 9527

```
[root@rhel5 ~]# telnet 127.0.0.1 9527] 进入通过9527端口连接自己
Trying 127.0.0.1...
Connected to localhost.localdomain (127.0.0.1).
Escape character is '^A'.
Kernel 3.10.0-514.17.x86_64 on an x86_64
Centos7 Login: keer [输入centos7的用户名和密码
Password:
Last login: Thu Sep 28 01:21:19 from ::ffff:192.168.191.66

[keer@centos7 ~]$
```

此时，我们可以查看一下centos6和centos7的连接情况：

```
[root@centos6 ~]# ss -nt
State      Recv-Q Send-Q
ESTAB      0      0
ESTAB      0      0
ESTAB      0      64
[root@centos6 ~]#
```

Local Address:Port	建立连接的端口	Peer Address:Port
192.168.191.66:22		192.168.191.55:42500
192.168.191.66:55120	rhel5通过centos7时生成的随机端口	192.168.191.77:23
192.168.191.66:22		192.168.191.1:8900

```
[root@centos7 ~]# ss -nt
State      Recv-Q Send-Q
ESTAB      0      52
ESTAB      0      0
ESTAB      0      0
[root@centos7 ~]#
```

Local Address:Port	建立连接的端口	Peer Address:Port
192.168.191.77:22		192.168.191.1:5900
::ffff:192.168.191.77:23	centos7上显示的是centos6通过23端口端口	::ffff:192.168.191.66:55118
192.168.191.77:23		

至此，我们已经实现了A用户在公司外部远程连接C机器的需求，接下来我们就来讲一讲实现过程：

data <- -> localhost:9527端口 <- ->
localhost:XXXXX (随机在客户端6开一个端口)
<- -> sshsrv:22 (通过ssh封装) <- ->
sshsrv:YYYYY (服务器解封装，开一个端口，代表telnet客户端) <- -> telnetsrv:23

用大白话来解释就是：当rhel5 (A用户) 连接自己的9527端口时，该请求自然会通过ssh协议封装发送给centos6 (B机器)，然后在centos6 (C机器) 上解封装，形成telnet流量，发送给centos7 (C机器)。

实验做完了，如果我们想要停止这个隧道，直接把后台的隧道进程杀死就可以了，命令如下：

```
killall ssh
```

```
[root@rhel5 ~]# killall ssh 关闭后台隧道
[root@rhel5 ~]# ss -nt
State      Recv-Q Send-Q
ESTAB      0      0
[root@rhel5 ~]#
```

Local Address:Port	建立连接的端口	Peer Address:Port
192.168.191.55:22		192.168.191.1:11442

我们的实验圆满完成ヽ(✿ﾟ▽ﾟ)ノ

三、远程转发

在我们实验一的场景下，首先要满足的是防火墙上必须打开22端口，但是在现实生活中，企业出于安全考虑，一般是不会打开防火墙，只允许出不允许进。所以，当防火墙的端口没有打开

的时候，我们要怎么办呢？这就要用到我们接下来要说的远程转发了：

命令：-R

sshserverport:remotehost:remotehostport
sshserver

说明： sshserverport 被转发机器开启
的端口号

remotehost 最终连接机器的
IP地址

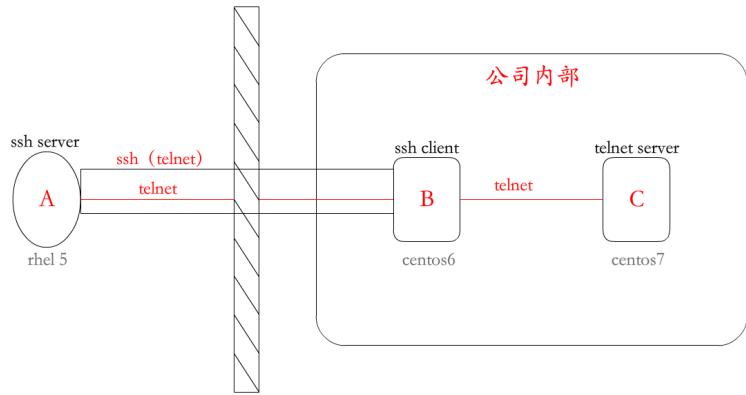
remotehostport 被转发机器的端
口号

sshserver 被转发机器的IP
地址

同样的，我们以实验来具体说明我们的远程
转发：

实验二、实现SSH端口转发——远程转发

- 背景：企业内部C服务器只允许telnet连接（23端口）访问，不允许外部直接访问，B服务器是一个ssh服务器；有一个用户需要从外部连接到企业内部的C服务器。
- 原理：B机器访问A用户，给A用户转发
- 机器：rhel5模拟A用户，centos6模拟B机器，centos7模拟C机器
- 图示如下：



- 实验步骤：

1) 模拟C机器不允许A用户连接，并且开启B机器的telnet服务端口23。

在centos7上输入以下口令：

```
iptables -A INPUT -s 192.168.191.55  
-j REJECT
```

[root@centos7 ~]# iptables -A INPUT -s 192.168.191.55 -j REJECT

此时，从rhel5用ssh命令连接centos7，是拒绝的：

[root@rhel5 ~]# ssh 192.168.191.77
ssh: connect to host 192.168.191.77 port 22: Connection refused

同时，我们还要开启7的telnet服务端口23：

systemctl start telnet.socket

用**ss -ntl**命令可以查看的服务端口是否已开启

```
[root@centos7 ~]# ss -ntl
State Recv-Q Send-Q Local Address:Port Peer Address:Port
LISTEN 0 128 *:111 *:*
LISTEN 0 128 *:22 *:*
LISTEN 0 128 127.0.0.1:631 127.0.0.1:25
LISTEN 0 100 :::111 :::*
LISTEN 0 128 :::22 :::*
LISTEN 0 128 :::23 :::*
LISTEN 0 128 :::631 :::*
LISTEN 0 100 :::1:25 :::*
```

端口已经开启

2) 开启隧道转发 (telnet隧道)

这一次，由于防火墙完全关闭，外部的设备连接不进来，所以我们要通过B机器去连接A用户

的机器，因此，我们的开启隧道命令要在B机器
(centos6) 上运行：

首先，我们要确定一下centos6上开启了哪
些端口：

```
[root@centos6 ~]# ss -nt
State      Recv-Q Send-Q
LISTEN     0          128
LISTEN     0          128
LISTEN     0          128
LISTEN     0          100
LISTEN     0          100
[root@centos6 ~]#
```

然后，我们选择一个没有被开启的端口开启
隧道，进行实验：

```
[root@centos6 ~]# ssh -q 9527 192.168.191.55 [密钥校验失败的隧道命令
Trying connect to 192.168.191.55 (192.168.191.55) port 9527: Connection failed.
RSA key fingerprint is 26:91:3c:65:33:c6:39:7b:e0:f6:47:s7:22:ae:98:de.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.191.55' (RSA) to the list of known hosts.
root@192.168.191.55's password:
[root@centos6 ~]#
```

同样的，在这里，我们可以使用ps aux来
查询后台运行的进程。也可以通过ss -nt查看
接口连接情况：

```
[root@rhel5 ~]# ss -nt
State      Recv-Q Send-Q
ESTAB     0          0
ESTAB     0          0
[root@rhel5 ~]#
```



```
[root@centos6 ~]# ss -nt
State      Recv-Q Send-Q
ESTAB     0          64
ESTAB     0          0
[root@centos6 ~]#
```

3) 在rhel5上输入以下命令，用9527端口连接自
己：

telnet 127.0.0.1 9527

```
[root@rhel5 ~]# telnet 127.0.0.1 9527
Trying 127.0.0.1...
Connected to localhost.localdomain (127.0.0.1).
Escape character is '^A'.
Kernel 3.10.0-514.17.x86_64 on an x86_64
centos/ login: keen [输入centos的用户名和密码]
Password: Last Login: Thu Sep 28 01:21:19 from ::ffff:192.168.191.66
[keer@centos7 ~]$
```

此时，我们可以查看一下centos6和centos7
的连接情况：

```
[root@centos6 ~]# ss -nt
State      Recv-Q Send-Q
ESTAB     0          64
ESTAB     0          0
ESTAB     0          0
[root@centos6 ~]#
```



```
[root@centos7 ~]# ss -nt
State      Recv-Q Send-Q
ESTAB     0          52
ESTAB     0          0
[root@centos7 ~]#
```

至此，我们已经实现了A用户在公司外部远程连接C机器的需求，接下来我们就来讲一讲实现过程：

```
data <- -> sshsrv:9527端口 <- ->
sshsrv:22 (通过ssh封装) <- ->
localhost:XXXXX (随机在客户端6开一个端口)
<- -> localhost:YYYYY (服务器解封装, 开一个端口, 代表telnet客户端) <- ->
telnetsrv:23
```

用大白话来解释就是：当rhe15 (A用户) 连接自己的9527端口时，该请求自然会通过ssh协议封装发送给centos6 (B机器)，然后在centos6 (C机器) 上解封装，形成telnet流量，发送给centos7 (C机器)。

实验做完了，如果我们想要停止这个隧道，直接把后台的隧道进程杀死就可以了，命令如下：

```
killall ssh
```

```
[root@rhe15 ~]# killall ssh 关闭后台隧道
[root@rhe15 ~]# ss -nt
State      Recv-Q   Send-Q      Local Address:Port          Peer Address:Port
ESTAB      0          0          ::ffff:192.168.191.55:22  ::ffff:192.168.191.1:11442
[root@rhe15 ~]#
```

我们的实验圆满完成ヽ(✿ﾟ▽ﾟ)ノ

四、动态转发

众所周知，我国有一个功能强大的防火墙，用来避免我们访问谷歌等外国的部分网站，嗯。。。FQ的方法有很多，相信大家不比小编懂得少，所以我们就不一一举例说明了。接下来，小编就给大家说一说如何通过ssh转发技术实现FQ~

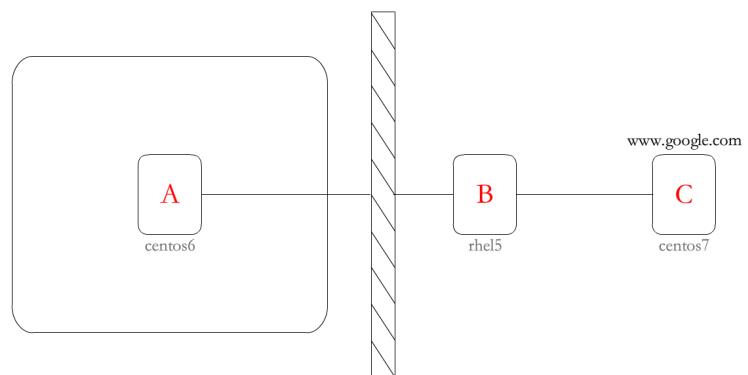
这里，就要用到我们的动态转发技术了：

当用firefox访问internet时，本机的1080端口做为代理服务器，firefox的访问请求被转发到sshserver上，由sshserver替之访问internet。

接下来，我们还是以实验进行说明：

实验三、实现SSH端口转发——动态转发

- 背景：模拟Google的服务器C不允许国内网站A直接访问，B服务器是国外的一个小型的学习用的服务器；国内网站A可以访问国外学习服务器B；实现国内网站A访问模拟Google服务器C。
- 原理：国内网站A通过ssh协议连接到国外学习服务器B上，再通过国外学习服务器B做跳板，连接至Google服务器C。
- 机器：centos6模拟国内网站A，rhel5模拟国外学习服务器B，centos7模拟Google服务器C
- 图示如下：



- 实验步骤：

- 1) 在模拟google服务器C上搭建一个网页，从互联网上访问centos7时，页面显示"Welcome to

www.google.com"

命令如下：

```
[root@centos7 ~]# cd /var/www/html/  
[root@centos7 html]# vim index.html  
<h1> Welcome to www.google.com </h1>
```

编写完文件以后，记得重启一下httpd服务：

```
[root@centos7 html]# systemctl restart httpd
```

2) 模拟Google服务器C不允许国内网站A连接

在centos7上输入以下命令：

```
[root@centos7 ~]# iptables -A INPUT  
-s 192.168.191.66 -j REJECT
```

此时，我们来测试一下centos6和rhel5能否访问centos7，命令为：

```
curl 192.168.191.77 或 links  
192.168.191.77
```

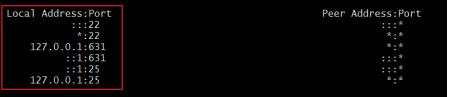
```
[root@rhel5 ~]# curl 192.168.191.77  
<h1> Welcome to www.google.com </h1>  
  
[root@centos6 ~]# curl 192.168.191.77  
curl: (7) couldn't connect to host
```

可以看出，rhel5可以连接到centos7，但是centos6不能连接到centos7。我们现在的需求就是希望centos6可以借助于rhel5访问centos7，方法也很简单，接下来就给大家说一说。

3) 动态端口转发

首先，我们在6机器上确认已经开启的端口有哪些：

```
[root@centos6 ~]# ss -ntl
State Recv-Q Send-Q
LISTEN 0 128
LISTEN 0 128
LISTEN 0 128
LISTEN 0 128
LISTEN 0 100
LISTEN 0 100
[root@centos6 ~]#
```



我们使用1080端口，从上图中我么已经看出，1080端口没有被占用，所以我们可以使用~

接着我们建立动态转发的隧道（6上输入以下命令）：

```
ssh -D 1080 -fN 192.168.191.55
```

```
[root@centos6 ~]# ssh -D 1080 -fN 192.168.191.55
root@192.168.191.55's password: 登录成功但是后台运行
[root@centos6 ~]#
[root@centos6 ~]#
```

在这里，我们可以在rhe15上查看到centos6的连接：

```
[root@rhe15 ~]# ss -nt
State Recv-Q Send-Q
ESTAB 0 0
ESTAB 0 0
[root@rhe15 ~]#
```

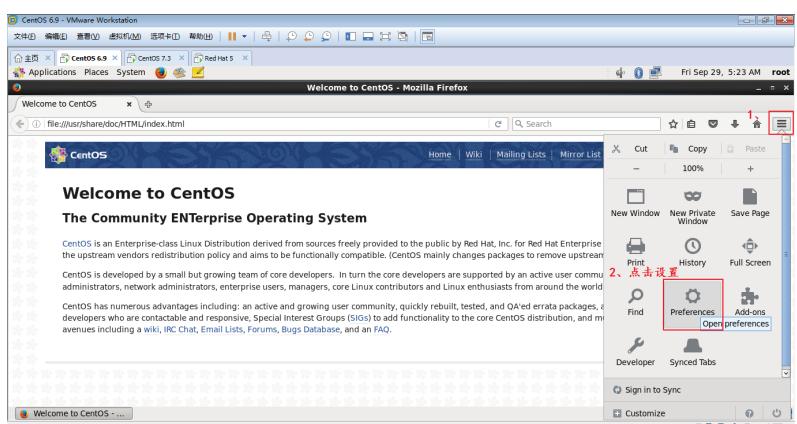


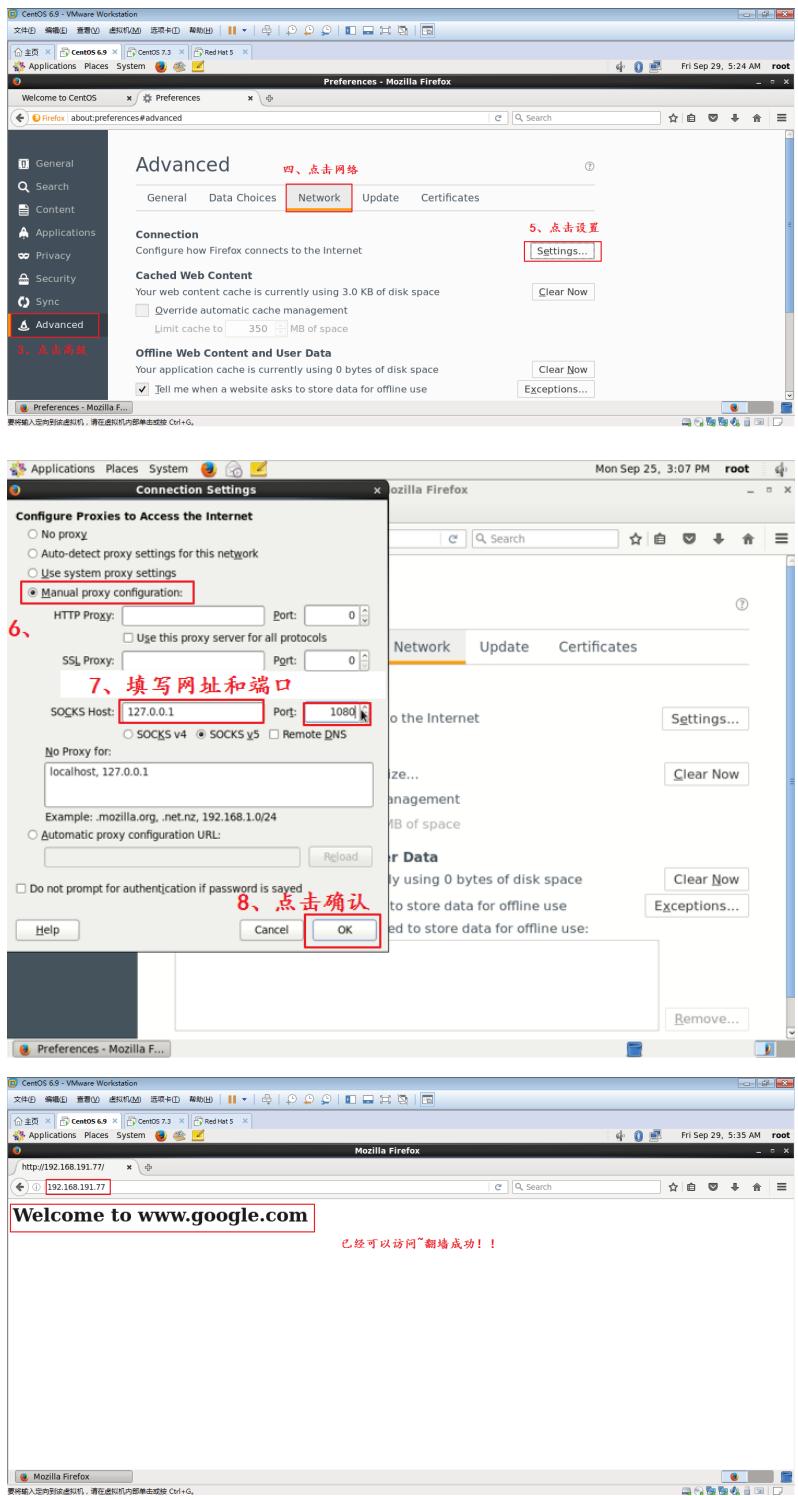
4) 设置代理rhe15访问centos7，命令如下（在centos6上输入）：

```
curl --socks5 127.0.0.1:1080
http://192.168.191.77
```

```
[root@centos6 ~]# curl --socks5 127.0.0.1:1080 http://192.168.191.77
<html>Welcome to www.google.com </html> | 现在的centos6已经可以访问到centos7的网站
[root@centos6 ~]#
```

5) 在图形化界面，在centos6上的firefox浏览器设置代理：





我们的实验圆满完成ヽ(✿ﾟ▽ﾟ)ノ

作者：珂儿吖

出处：<http://www.cnblogs.com/keerya/>

本文版权归作者和博客园共有，欢迎转载，但未经作者同意必须保留此段声明，且在文章页面明显位置给出原文连接，否则保留追究法律责任的权利。

大家写文都不容易，希望尊重劳动成果哟~

标签: ssh

[好文要顶](#)[关注我](#)[收藏该文](#)

珂儿吖

关注 - 8

粉丝 - 416

[+加关注](#)

28

[推荐](#)

2

[反对](#)[« 上一篇：私人订制——属于你自己的Linux](#)[» 下一篇：Linux上mysql的安装与配置](#)

posted on 2017-09-29 20:58 珂儿吖 阅读(51734) 评论(8) [编辑](#) [收藏](#) [举报](#)

[刷新评论](#) [刷新页面](#) [返回顶部](#) 登录后才能查看或发表评论，立即[登录](#) 或者[逛逛](#) 博客园首页

【推荐】百度智能云2021普惠上云节：新用户首购云服务器低至0.7折

【推荐】阿里云云大使特惠：新用户购ECS服务器1核2G最低价87元/年

【推荐】大型组态、工控、仿真、CAD\GIS 50万行VC++源码免费下载!

【推广】园子与爱卡汽车爱宝险合作，随手就可以买一份的百万医疗保险



编辑推荐：

- DDD领域驱动及落地方案
- CSS 奇思妙想 | 使用 resize 实现强大的图片拖拽切换预览功能
- 浅谈 C# 取消令牌 CancellationTokenSource
- 记一次 .NET 某WMS仓储打单系统 内存暴涨分析
- 神奇的 SQL 之别样的写法 —— 行行比较

最新新闻：

- 一站式云超算平台北鲲云完成新一轮融资 (2021-08-19 18:50)
- 声网发布全链路加速FPA为互联网增加QoS保障 (2021-08-19 18:38)
- 腾讯Q2财报会议，高管解读：行业监管、税率、游戏业务发展 (2021-08-19 18:37)
- Facebook发布了一份关于News Feed中浏览量最高内容的报告 (2021-08-19 18:26)
- 美国官方曝网络摄像头大漏洞 超 8300 万台设备受影响 (2021-08-19)

18:20)

» [更多新闻...](#)

Copyright © 2021 珂儿吖

Powered by .NET 5.0 on Kubernetes