原创

# open***下的配置文件与iptables优化

往事_Jim_遗 关注 2016-08-18 15:44:15 27269人阅读 0人评论

最近公司里的***服务器宕机了，恢复后发现***拨不通了，开始还以为是ISP封堵了端口，结果后面检查了下并没有后面就检查下服务器上的路由表和iptables也没有问题啊怎么回事，后来利用wif连接电脑检查了下客户端的路由表就发现问题了，因此就对open***的配置文件以及iptables做了一次优化，这里就不多说open***的安装部署了，想必在网上都可以找到很多的教程，虽然麻烦点但是总体来说还是不太难的以前安装的时候有参考过http://fengwan.blog.51cto.com/508652/1404435、http://ylw6006.blog.51cto.com/470441/1009004/等文章。

先说下open***的server.conf优化，这里建议使用tap桥接模式，它会创建一个以太网隧道，可以省得再去添加路由表，缺点就是不能在移动设备中使用，广播包会散发到虚拟网络中，可能极大消耗流量

```
[root@test conf]# cat server.conf
local 192.168.168.253#***服务器需要监听的ip，如果有外网尽量用外网
port 1194
proto udp#尽量用udp端口，保证远程桌面等服务的连接，如果只是传文件就用tcp，客户端要和服务端一
dev tap#tap模式
ca /usr/local/open***/easy-rsa/keys/ca.crt
cert /usr/local/open***/easy-rsa/keys/server.crt
key /usr/local/open***/easy-rsa/keys/server.key
dh /usr/local/open***/easy-rsa/keys/dh2048.pem
tls-auth /usr/local/open***/easy-rsa/keys/ta.key 0#在生成证书的时候生成ta.key用于防御DOS、
#要注意的是服务器上是 0 客户端是1，两个文件必须一样，不然就连不上
server 10.8.0.0 255.255.255.0#给客户端分配的IP地址段，tap模式下一般是服务是10.8.0.1作为网关
ifconfig-pool-persist /usr/local/open***/conf/ipp.txt#设置客户端ip地址池
push “redirect-gateway def1 bypass-dhcp”#自动推送客户端上的网关 及DHCP，这是优化的关键
push "dhcp-option DNS 114.114.114.114"#推送一些通用DNS，当然也可已加上服务器上的DNS
push "dhcp-option DNS 8.8.8.8"
client-to-client
duplicate-cn
keepalive 10 120
comp-lzo
max-clients 100
persist-key
tls-server#使用TLS加密传输，本端为Server，Client端为tls-client
persist-tun
verb 3
status /usr/local/open***/log/open***-status.log
log /usr/local/open***/log/open***.log
mute 20#相同信息的数量，如果连续出现 20 条相同的信息，将不记录到日志中
auth-user-pass-verify /usr/local/open***/conf/checkpsw.sh via-env#这个脚本到处都可以下下载
client-cert-not-required
script-security 3 system
```

windows下的client.o***配置文件

```
client
dev tap
proto udp
remote xx.xx.xx.xx 1194
```

```
resolv-retry infinite
redirect-gateway def1#让客户端发起的所有IP请求都通过Open×××服务器
nobind
persist-key
persist-tun
ca ca.crt
cert client.crt
key client.key
auth-user-pass
remote-cert-tls server
tls-auth ta.key 1#ta.key
tls-client#TLS加密传输
ns-cert-type server
comp-lzo
verb 3
mute 20
```

iptables里优化如下

```
[root@test conf]# vi /etc/sysconfig/iptables
*nat
:PREROUTING ACCEPT [45:3684]
:POSTROUTING ACCEPT [1:92]
:OUTPUT ACCEPT [1:92]
#-A POSTROUTING -s 10.8.0.0/24 -d 192.168.168.0/24 -o eth0 -j MASQUERADE
-A POSTROUTING -s 10.8.0.0/24 -d 192.168.168.0/24 -o eth0 -j SNAT --to-source 192.168.168.
#如果是静态ip就用这条以节省系统开销，如果是动态公网ip用上面的MASQUERADE伪装,nat表就做这些
COMMIT
*filter
:INPUT ACCEPT [0:0]
-A OUTPUT -m state --state INVALID -j DROP
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [278:27552]
-A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
-A INPUT -i lo -j ACCEPT
-A INPUT -p icmp -j ACCEPT
-A INPUT -s 192.168.168.0/24 -d 192.168.168.253 -i eth0 -p tcp -m state --state NEW -m tcp
-A INPUT -i eth0 -p udp -m state --state NEW -m udp --dport 1194 -j ACCEPT
-A INPUT -j REJECT --reject-with icmp-host-prohibited
COMMIT
[root@test conf]# /etc/init.d/iptables restart
```

如此open***优化完毕



open*** server.conf ***

0 收藏 分享

上一篇：linux硬盘SMART检查 下一篇：open***中push “re...

往事_Jim_遗

225篇文章，112W+人气，4粉丝

关注