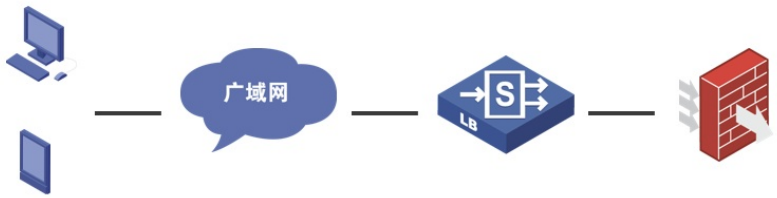
L2TP over IPSec结合iNode客户端与移动终端拨号典型配置

L2TP over IPSec VP　iNode　吴川云　2021-08-31 发表

组网及说明



出口为LB，将防火墙地址做了静态映射； L2TP over IPSec做在内网的防火墙上；属于内网地址映射和拨号认证的场景。

配置步骤

FW侧配置：

```
ipsec policy-template 1 1
transform-set 3 4 5 7 8 9     //  3 4 5为传输模式，匹配手机端；7 8 9为隧道模式，匹配PC iNODE
local-address XXXX
ike-profile 1
reverse-route dynamic   //添加反向路由引入的命令，向终端发送全0默认路由
#
ike profile 1
keychain 1
local-identity fqdn LNS
match remote identity user-fqdn LAC    //  匹配手机端配置的LAC标识符
match remote identity fqdn LAC          //   匹配PC iNODE 端 的标识符
match remote identity address 0.0.0.0 0.0.0.0    // 匹配手机端不配置ipsec标识符的情形
proposal 1 2 3 4 5 6

#
ipsec transform-set 3
 encapsulation-mode transport
 esp encryption-algorithm aes-cbc-128
 esp authentication-algorithm sha1
#
ipsec transform-set 4
 encapsulation-mode transport
 esp encryption-algorithm aes-cbc-256
 esp authentication-algorithm sha1
#
ipsec transform-set 5
 encapsulation-mode transport
 esp encryption-algorithm 3des-cbc
 esp authentication-algorithm sha1
#
ipsec transform-set 7
 esp encryption-algorithm aes-cbc-192
 esp authentication-algorithm sha1
#
ipsec transform-set 8
 esp encryption-algorithm 3des-cbc
 esp authentication-algorithm sha1
#
ipsec transform-set 9
 esp encryption-algorithm aes-cbc-256
 esp authentication-algorithm sha1

#
ike proposal 1
 encryption-algorithm aes-cbc-128
 dh group2
 authentication-algorithm md5
#
ike proposal 2
 encryption-algorithm 3des-cbc
 dh group2
 authentication-algorithm md5
#
ike proposal 3
 encryption-algorithm 3des-cbc
 dh group2
#
ike proposal 4
```

encryption-algorithm aes-cbc-256
dh group2
#
ike proposal 5
dh group2
#
ike proposal 10
encryption-algorithm aes-cbc-192
dh group2

移动端：

0.0.0.0 key cipher c3$cLvXGmVl9pDX6==

配置关键点

经过测试，安卓手机端系统自带的l2tp over ipsec 标识身份信息的类型为user-fqdn，PC iNODE标识身份信息类型为fqdn。因此在配置ike profile中对端身份时需要同时配置两种类型。另外iNODE上需要配置为NAT穿越，因此ipsec模式只能使用隧道模式，而安卓手机默认是隧道模式。 因此在ipsec模板中要同时调用两种模式的transform set。

•名称应该写LNS
•类型选L2TP/IPSEC PSK
•服务器地址填公网地址XXXX
•ipsec表示符选填，可以填LAC
•预共享秘钥与防火墙上pre-share-key一致 保存后用防火墙上建的local-user用户密码登陆即可。

PC iNode客户端侧：iNODE配置如下，IPSec服务器为公网映射出的地址，LNS服务器为内网真实地址，注意勾选NAT穿越。

总结：

1、对于设备部署在内网，出口为其他路由器，外网已把L2tp 和IPsec 端口都做了映射，配置完成之后，发现终端使用iNODE 无法拨号成功，提示建立隧道或会话失败，需在iNODE填写正确的地址；即IPSec地址为公网地址，LNS的地址为内网地址；

2、安卓手机端系统自带的l2tp over ipsec 标识身份信息的类型为user-fqdn，PC iNODE标识身份信息类型为fqdn。因此在配置ike profile中对端身份时需要同时配置两种类型。另外iNODE上需要配置为NAT穿越，因此ipsec模式只能使用隧道模式，而安卓手机默认是隧道模式。协商问题及时调整参数；