MSR与Android、IOS移动终端建立L2TP over IPSec VPN典型配置案例

IPSec VPN L2TP VPN 程咪 2019-10-31 发表

问题描述

MSR与Android、IOS移动终端建立L2TP over IPSec VPN典型配置案例

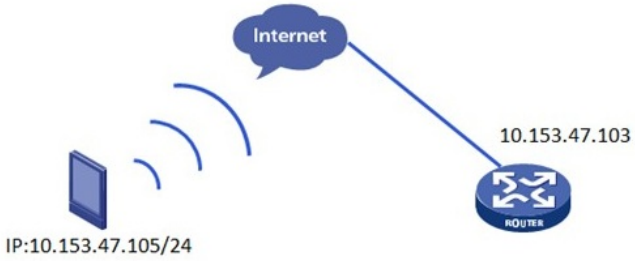
解决方法

组网需求：

随着智能终端的普及，，Android 和 苹果的IOS操作系统占有电子市场的绝大份额。越来越多的客户希望利用这些手持终端设备与防火墙直接建立VPN连接，从而访问公司内部网络资源。本案例用于指导网络工程师对上述组网需求进行配置。

组网图：

移动终端通过无线与MSR三层可达，路由可达，中间不允许经过nat设备。



设备版本

Android：MIUI V5 、原生安卓4.0

IOS版本：IOS 6 IOS 7

MSR版本：2209P37

配置步骤：

1、设备开启L2TP 功能，配置好虚模板地址以及相应的地址池，创建用户123，密码123

```
#
 l2tp enable
#
domain system
ip pool 1 192.168.13.200 192.168.13.250
#
local-user 123
 password cipher 123
 service-type ppp
#
l2tp-group 1
 undo tunnel authentication
 allow l2tp virtual-template 0
#
interface Virtual-Template0
 ppp authentication-mode chap domain system
 ppp ipcp remote-address forced
 remote address pool 1
 ip address 192.168.13.1 255.255.255.0
#
```

2、针对安卓手机配置IPSec：

```
#
ike proposal 1
 encryption-algorithm aes-cbc 256
```

```
 dh group2
 sa duration 28800
#
ike peer android
 exchange-mode aggressive
 proposal 1
 pre-shared-key cipher 123456789
 id-type name
 remote-name aaa
 local-name rt1
 nat traversal
#
ipsec proposal 1
 encapsulation-mode transport
#
ipsec policy-template android 1
 ike-peer android
 proposal 1
#
ipsec policy phone 1 isakmp template android
#
interface GigabitEthernet0/0
 port link-mode route
 ip address 10.153.47.103 255.255.255.0
 ipsec policy phone
#
```

3、安卓客户端的配置：

名称：随便起

类型：L2TP/IPSEC PSK

服务器地址：LNS的外网地址

IPSec标示符：aaa

预共享密钥：123456789

4、针对IOS 用户的IPSec配置：

```
#
ike proposal 2
 encryption-algorithm 3des-cbc
 dh group2
 authentication-algorithm md5
 sa duration 3600
#
ike peer ios
```

```
 proposal 2
 pre-shared-key cipher 456123
 local-address 10.153.47.103
 nat traversal
#
ipsec proposal 2
 encapsulation-mode transport
 esp authentication-algorithm sha1
 esp encryption-algorithm aes 128
#
ipsec policy-template ios 1
 ike-peer ios
 proposal 2
#
ipsec policy phone 2 isakmp template ios
#
interface GigabitEthernet0/0
 port link-mode route
 ip address 10.153.47.103 255.255.255.0
 ipsec policy phone
#
```

5、IOS客户端的配置：

描述：随便写
服务器：LNS公网口地址
账户：123
密码：123
密钥：456123

注意事项：

1 经过抓包分析出安卓手机和ios系统对IPSec协商的一些参数
2 本案例中Android客户端与IOS客户端均是动态获取IP地址。
3 Android和IOS终端均没有找到使能nat穿越的设置选项，所以在本案例的基础上设备之间添加个NAT转换设备，则无法拨入成功。如果客户的移动终端是3G的，使用私网IP地址上网的，可能无法拨入成功。此问题是终端不能开启nat穿越功能导致。
4 测试MSR软件版本为2209P37，创建IPSec安全提议的命令仍然是 ipsec proposal。现场实际环境如果是23xx以上版本，可自行修改一下IPSec对应的安全提议参数。