Comware V7平台FW与移动终端对接L2TP over IPSec配置案例

L2TP VPN IPSec VPN 程咪 2019-10-31 发表

问题描述

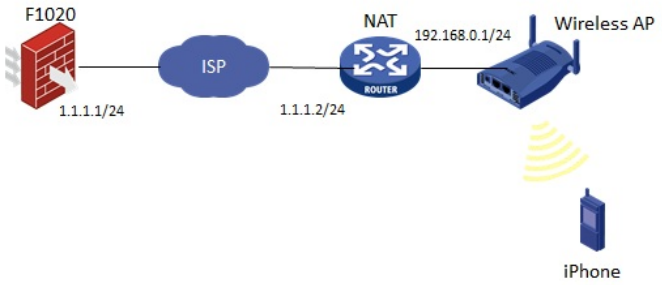
Comware V7平台FW与移动终端对接L2TP over IPSec配置案例

解决方法

一、 组网需求：

Comware V7防火墙设备作为VPN总部，客户通过移动终端iPhone/Android拨入，中间跨越运营商nat。

二、 组网图：



如图所示，F1020通过G1/0/1与NAT设备G0/1相连，NAT设备下挂一台无线AP，iPhone/Android通过AP接入网络，自动获取地址。由于终端地址不固定，总部F1020采用模板方式建立IPSec。

三、 配置步骤：

1、NAT上配置基本上网所需的NAT及路由功能即可，此处略，AP配置同略。

2、F1020 L2TP/IPSec相关配置

```
#
l2tp enable
#
ip pool pool 10.1.1.2 10.1.1.10            //地址池
#
interface Virtual-Template1
 ppp authentication-mode pap
 remote address pool pool
 ip address 10.1.1.1 255.255.255.0
#
local-user client class network
 password cipher $c$3$0od64a2T9DdgR5wMufBCuNXFTiudDpvKZQ==
 service-type ppp
 authorization-attribute user-role network-operato
#
ipsec transform-set 1
 encapsulation-mode transport
 esp encryption-algorithm aes-cbc-192
 esp authentication-algorithm sha1
#
ipsec transform-set 2
 encapsulation-mode transport
 esp encryption-algorithm aes-cbc-128
 esp authentication-algorithm sha1
#
ipsec transform-set 3
 encapsulation-mode transport
 esp encryption-algorithm aes-cbc-256
 esp authentication-algorithm sha1
#
ipsec transform-set 4
 encapsulation-mode transport
 esp encryption-algorithm des-cbc
 esp authentication-algorithm sha1
#
```

```
ipsec transform-set 5
 encapsulation-mode transport
 esp encryption-algorithm 3des-cbc
 esp authentication-algorithm sha1
#
ipsec policy-template 1 1
 transform-set 1 2 3 4 5   //不确定终端的提议类型，这里设置多个
 ike-profile 1
#
ipsec policy 1 1 isakmp template 1
#
l2tp-group 1 mode lns
 allow l2tp virtual-template 1
 undo tunnel authentication
#
 l2tp enable
#
ike profile 1
 keychain 1
 match remote identity address 0.0.0.0 0.0.0.0
 proposal 1
#
ike proposal 1
 encryption-algorithm 3des-cbc
 dh group2
 authentication-algorithm md5
#
ike keychain 1
 pre-shared-key address 0.0.0.0 0.0.0.0 key cipher $c$3$u+NQyrhBRDKT/m1ozccSLeUnk7xN1gnaFw==
#
```

3、接口加入安全区域，并放通域间策略

4、iPhone/Android配置

iPhone：

Android：

连接时会弹出用户名/密码界面，此时输入设备上配置的local-user。


晚上7:29
中国联通
64%
连接到L2TP over IPSec
用户名
client
密码
••••••
取消
连接
*
1
2
3
#
4
5
6
+
7
8
9
-
返回
0
符号

5、验证


晚上7:33
中国联通
63%
VPN
VPN 密码保护
配置
L2TP over IPSec
已连接
已连接VPN
会话： L2TP over IPSec
时长： 00:02:00
已发送： 3673 字节/65 个数据包
已接收： 52 字节/4 个数据包
取消
断开连接


中国联通
VPN
19:23
55%
VPN
L2TP over IPSec
类型 L2TP
服务器 1.1.1.1
连接时间 0:20
描述 L2TP over IPSec
服务器 1.1.1.1
帐户 client
RSA SecurID
密码 ••••••
密钥 ••••••
发送所有流量