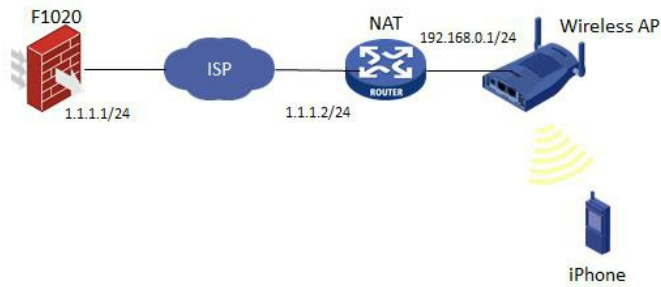


知 Comware V7平台FW与移动终端对接L2TP over IPSec配置案例

L2TP IPSec 幸启跃 2016-03-11 发表

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



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。

- 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

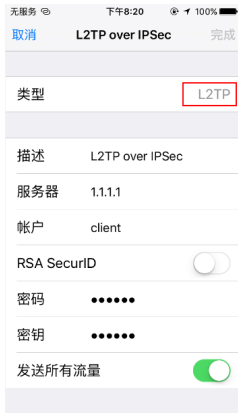
```
#
ip pool pool 10.1.1.2 10.1.1.10 //地址池
#
interface Virtual-Template1
 ppp authentication-mode pap
 remote address pool pool
 ip address 10.1.1.1 255.255.255.0
#
local-user client class network
 password cipher $c$3$0d64a2T9DdgR5wMufBCuNXFTiudDpvKZQ==
 service-type ppp
 authorization-attribute user-role network-operato
#
ipsec transform-set 1
 encapsulation-mode transport
 esp encryption-algorithm 3des-cbc
 esp authentication-algorithm md5
#
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 transform-set 6
 encapsulation-mode transport
```

```
esp encryption-algorithm aes-cbc-192
esp authentication-algorithm sha1
#
ipsec policy-template 1 1
transform-set 1 2 3 4 5 6 //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
local-identity address 1.1.1.1
match remote identity address 0.0.0.0 0.0.0.0
proposal 1 2 3 4 5 6
#
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 6
encryption-algorithm aes-cbc-192
dh group2
#
ike keychain 1
pre-shared-key address 0.0.0.0 0.0.0.0 key cipher $c$3$u+NQyrhBRDKT/m1ozccSLeUnk7xN1gnaF
w==
#
```

3、接口加入安全区域，并放通域间策略，在出口应用ipsec策略。

4、iPhone/Android配置

iPhone：



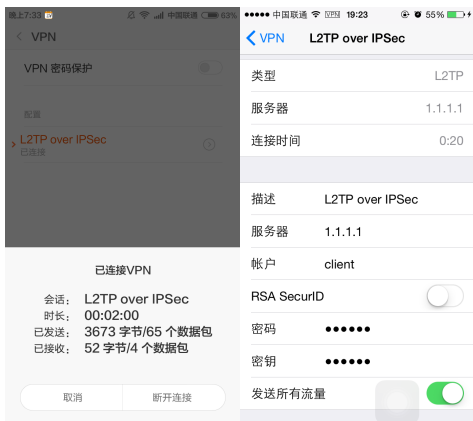
Android:



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。



5、验证



终端拨入VPN时，F1020 debug ike信息见附件。

#

ike profile 1

keychain 1

local-identity address 1.1.1.1

//ios最新的版本要配置local-identity address， 以前版

本不需要; android不需要配置

match remote identity address 0.0.0.0 0.0.0.0

proposal 1 2 3 4 5 6

#

综上, 建议在用手机和v7对接l2tp over ipsec的时候, ike profile下配置local-identity