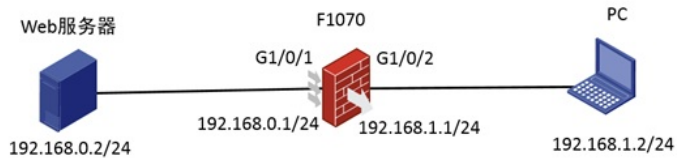


组网及说明

1. 组网需求:

Comware V7防火墙设备作为VPN总部, 电脑客户、移动终端通过中间跨越运营商网络拨入L2TP over IPSec VPN实现访问内网服务器的需求。

2. 组网图:



如图所示, 外网终端通过防火墙的接口2地址192.168.1.1拨号L2TP over IPSec VPN访问内网web服务器的资源。

配置步骤

1. 防火墙接口配置如下。

```
interface GigabitEthernet1/0/2
port link-mode route
ip address 192.168.1.1 255.255.255.0
ipsec apply policy 1
```

2. F1030 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 simple client
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
```

```

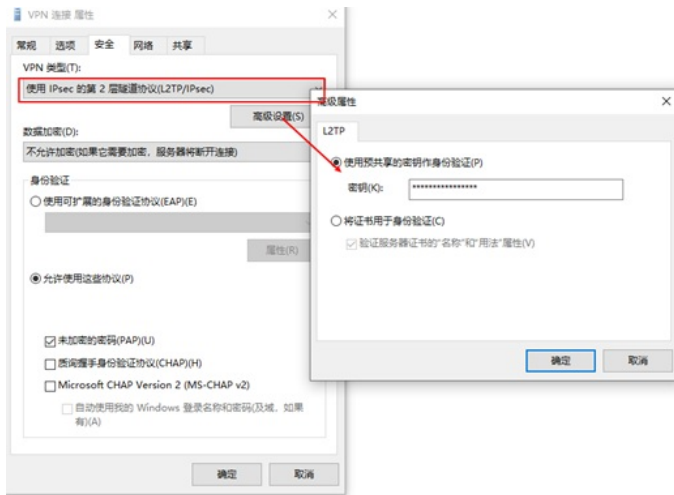
esp authentication-algorithm sha1
#
ipsec transform-set 5
encapsulation-mode transport
esp encryption-algorithm 3des-cbc
esp authentication-algorithm sha1
#
ipsec transform-set 6
encapsulation-mode transport
esp encryption-algorithm aes-cbc-192
esp authentication-algorithm sha1
#
ipsec policy-template 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 192.168.1.1
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 simple test
#

```

3. 物理口、Virtual-Template1接口加入安全区域，并放通域间策略。对于G1/0/2接口需要注意开放Untrust到Local的策略。对于Virtual-Template1接口，假设虚拟接口加入的是Untrust安全域，如果要访问内网资源，开放Untrust到Trust的安全策略。
4. window10电脑终端的配置
前面的步骤和W7一样，可以参考：<https://zhiliao.h3c.com/theme/details/104211>



...



或者点击网络和internet设置,从这里连接VPN

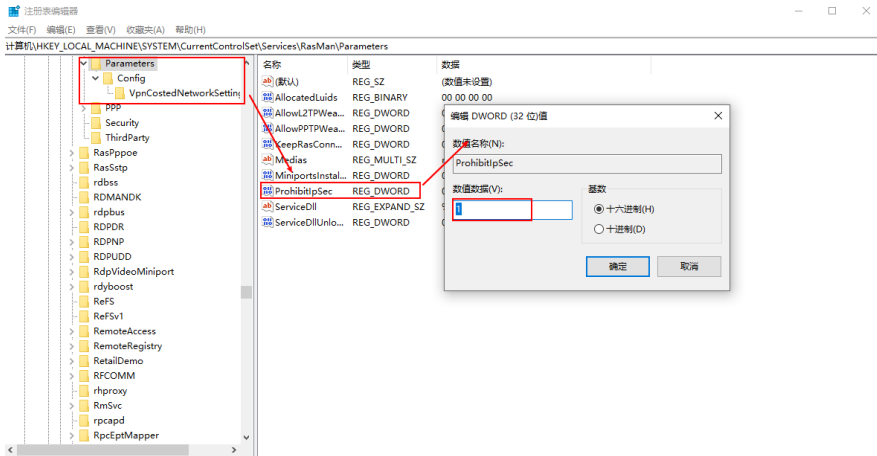
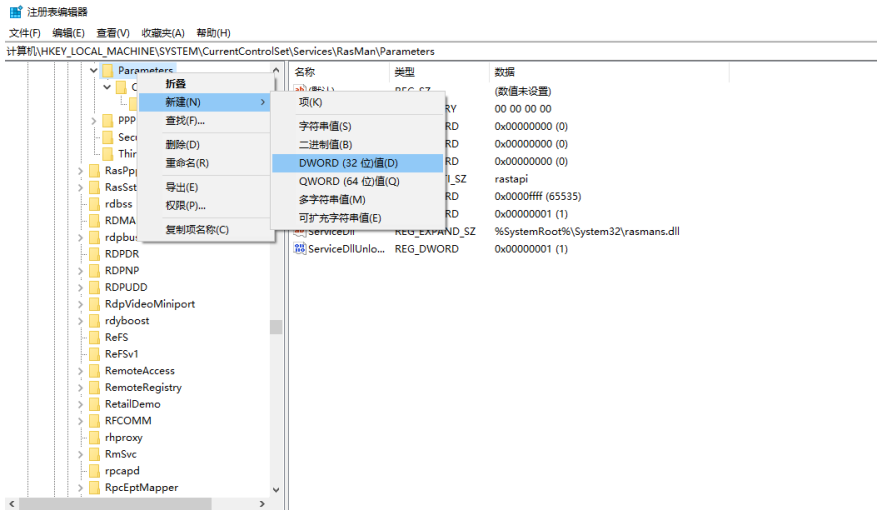


配置关键点

有点电脑注册表没有自动生成，这时候尽量都先新建下注册表

修改注册表

- 1、在“开始 > 运行”中，输入regedit命令，单击“确定”，进入注册表编辑器。
- 2、在“注册表编辑器”页面的左侧导航树中，选择“HKEY_LOCAL_MACHINE > SYSTEM > CurrentControlSet > Services > Rasman > Parameters”。
- 3、在菜单栏上选择“编辑 > 新建 > DWORD值”。
- 4、键入ProhibitIpSec，然后按“ENTER”。
- 5、右键单击ProhibitIpSec，选择“修改”，进入修改界面。
- 6、在“数值数据”框中键入1。
- 7、单击“确定”，并退出注册表编辑器。
- 8、重新启动该PC，使修改生效。



附件下载: W10拨号截图.rar