F5000-X系列防火墙L2TP VPN的配置方法

L2TP VPN　zhiliao_FO3qD　2018-11-25 发表

组网及说明

1 配置需求及说明

1.1 适用的产品系列

本案例适用于软件平台为Comware V7系列防火墙：F100-X-G2、F1000-X-G2、F100-X-WiNet、F1000-AK、F10X0等。

注：本案例是在F100-C-G2的Version 7.1.064, Release 9510P08版本上进行配置和验证的。

1.2 配置需求及实现的效果

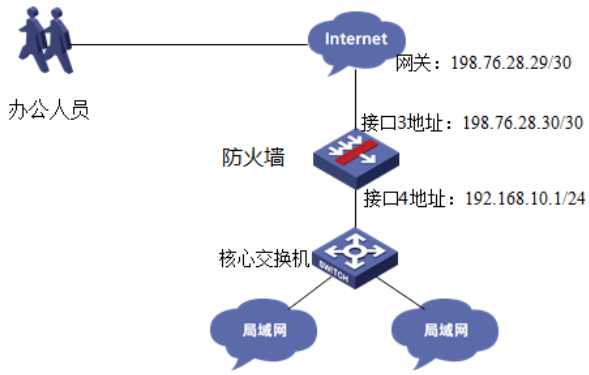
防火墙采用固定IP地址的方式部署在公司互联网出口，运营商提供的IP地址为198.76.28.30/30，网关为198.76.28.29，DNS地址为221.228.255.1。初步规划防火墙使用3接口接入运营商，使用4接口连接内部网络，内部网络使用192.168.10.0网段。

需求：

1）要求内网终端可以自动获取到地址并可以访问互联网。

2）公司外部办公人员需要通过拨号VPN连入公司内网。

2 组网图



配置步骤

3 配置步骤

3.1 配置外网接口

#将1/0/3设置为外网接口并设置IP地址。

<H3C>system-view

[H3C]interface GigabitEthernet 1/0/3

[H3C-GigabitEthernet1/0/3]ip address 198.76.28.30 255.255.255.252

[H3C-GigabitEthernet1/0/3]quit

3.2 配置内网接口

#配置内网接口为1/0/4接口并指定IP地址为192.168.10.1。

[H3C]interface GigabitEthernet 1/0/4

[H3C-GigabitEthernet1/0/4] ip address 192.168.10.1 255.255.255.0

[H3C-GigabitEthernet1/0/4] quit

3.3 配置NAT地址转换

#进入1/0/3接口配置NAT动态地址转换。

[H3C]interface GigabitEthernet 1/0/3

[H3C-GigabitEthernet1/0/3]nat outbound

[H3C-GigabitEthernet1/0/3]quit

3.4 配置到外网网关的静态路由

#配置默认路由到外网网关。

[H3C]ip route-static 0.0.0.0 0 198.76.28.29

3.5 建立VPN拨号账户

#创建本地PPP用户vpdnuser，设置密码为HelLo。

[H3C]Local-user vpdnuser class network

[H3C-luser-network-vpdnuser]password simple HelLo
[H3C-luser-network-vpdnuser]service-type ppp
[H3C-luser-network-vpdnuser]quit

3.6 开启L2TP功能

[H3C]l2tp enable

3.7 配置L2TP用户地址池

#创建用于给L2TP拨号用户分配地址的地址池。
[H3C] ip pool aaa 192.168.100.2 192.168.100.254
[H3C] ip pool aaa gateway 192.168.100.1

3.8 创建L2TP接口

#创建接口Virtual-Template1，PPP认证方式为CHAP，并使用地址池aaa为Client端分配IP地址。
[H3C]interface virtual-template 1
[H3C -Virtual-Template1]ppp authentication-mode chap domain system
[H3C -Virtual-Template1]ip address 192.168.100.1 24
[H3C-Virtual-Template1]remote address pool aaa
[H3C-Virtual-Template1]quit

3.9 创建L2TP组1

创建LNS模式的L2TP组1，配置隧道本端名称为LNS，指定接收呼叫的虚拟模板接口为VT1。
[H3C]l2tp-group 1 mode lns
[H3C-l2tp1]tunnel name LNS
[H3C-l2tp1]allow l2tp virtual-template 1
[H3C-l2tp1]undo tunnel authentication
[H3C-l2tp1]quit

3.10 配置外网接口、VT接口加入Untrust安全区域

#将1/0/3外网接口加入Untrust区域。
[H3C]security-zone name Untrust
[H3C-security-zone-Untrust]import interface GigabitEthernet 1/0/3
[H3C-security-zone-Untrust]import interface Virtual-Template 1
[H3C-security-zone-Untrust]quit

3.11 配置内网接口加入Trust安全区域

#将1/0/4内网接口加入Trust区域。
[H3C]security-zone name Trust
[H3C-security-zone-Trust]import interface GigabitEthernet 1/0/4
[H3C-security-zone-Trust]quit

3.12 配置安全策略将Trust到Untrust域内网数据放通

#创建对象策略pass。
[H3C]object-policy ip pass
[H3C-object-policy-ip-pass] rule 0 pass
[H3C-object-policy-ip-pass]quit
#创建Trust到Local域的域间策略调用pass策略。
[H3C]zone-pair security source Trust destination Untrust
[H3C-zone-pair-security-Trust- Untrust]object-policy apply ip pass
[H3C-zone-pair-security-Trust- Untrust]quit

3.13 配置安全策略将Trust到Local域、Local到Trust域数据全放通策略

#创建trust到Local域的域间策略调用pass策略。
[H3C]zone-pair security source Trust destination Local
[H3C-zone-pair-security-Trust-Local]object-policy apply ip pass
[H3C-zone-pair-security-Trust-Local]quit
#创建Local到trust域的域间策略调用pass策略。
[H3C]zone-pair security source Local destination Trust
[H3C-zone-pair-security-Local-Trust]object-policy apply ip pass
[H3C-zone-pair-security-Local-Trust]quit

3.14 配置安全策略将Untrust到Local域目的端口为UDP1701端口放通。

#创建服务对象1701用于匹配L2TP的UDP 1701端口。
[H3C]object-group service 1701

[H3C-obj-grp-service-1701]service udp destination eq 1701
[H3C-obj-grp-service-1701]quit
在对象策略中调用1701服务对象。
[H3C]object-policy ip 1701
[H3C-object-policy-ip-1701]rule pass service 1701
[H3C-object-policy-ip-1701]quit
#创建Untrust到Local域的域间策略调用1701服务对象策略。
[H3C]zone-pair security source Untrust destination Local
[H3C-zone-pair-security-Untrust-Local]object-policy apply ip 1701
[H3C-zone-pair-security-Untrust-Local]quit
#创建Local到Untrust域的域间策略调用1701服务对象策略。
[H3C]zone-pair security source Local destination Untrust
[H3C-zone-pair-security-Local-Untrust]object-policy apply ip 1701
[H3C-zone-pair-security-Local-Untrust]quit

3.15 配置安全策略将Untrust到trust访问内网资源的数据放通
#创建地址对象匹配到内网数据
[H3C]object-group ip address neiwang
[H3C-obj-grp-service-neiwang]network subnet 192.168.10.0 255.255.255.0
[H3C-obj-grp-service-neiwang]quit
在对象策略中调用到内网数据对象。
[H3C]object-policy ip neiwang
[H3C-object-policy-ip-neiwang]rule pass destination-ip neiwang
[H3C-object-policy-ip-neiwang]quit
#创建Untrust到Trust域的域间策略调用neiwang地址对象策略。
[H3C]zone-pair security source Untrust destination Trust
[H3C-zone-pair-security-Untrust-Trust]object-policy apply ip neiwang
[H3C-zone-pair-security-Untrust-Trust]quit

3.16 配置DHCP服务
#开启DHCP服务并指定动态下发的地址以及网关等参数。
[H3C]dhcp enable
[H3C]dhcp server ip-pool 1
[H3C-dhcp-pool-1]network 192.168.10.0
[H3C-dhcp-pool-1]gateway-list 192.168.10.1
[H3C-dhcp-pool-1]dns-list 221.228.255.1
[H3C-dhcp-pool-1]quit
注：DNS服务器地址优先设置当地运营商提供的DNS服务器地址，如果没有提供可以设置114.114.114.114或8.8.8.8等DNS服务器地址。

3.17 保存配置
[H3C]save force

4 VPN客户端配置
4.1 Windows 7电脑拨号配置
#点击电脑右下角电脑图标，选择“打开网络和共享中心”选项。

#点击“设置新的连接或者网络”。

#点击“连接到工作区”。

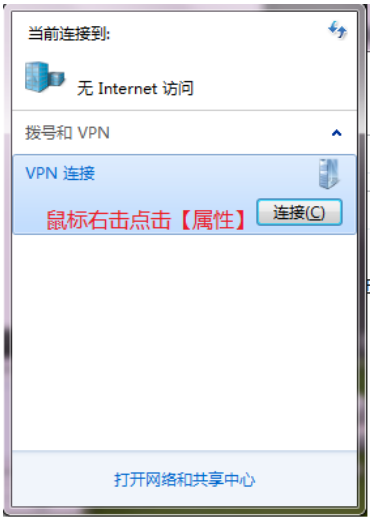
#选择“使用我的Internet连接（VPN）”。

#点击“我将稍后设置Internet连接”

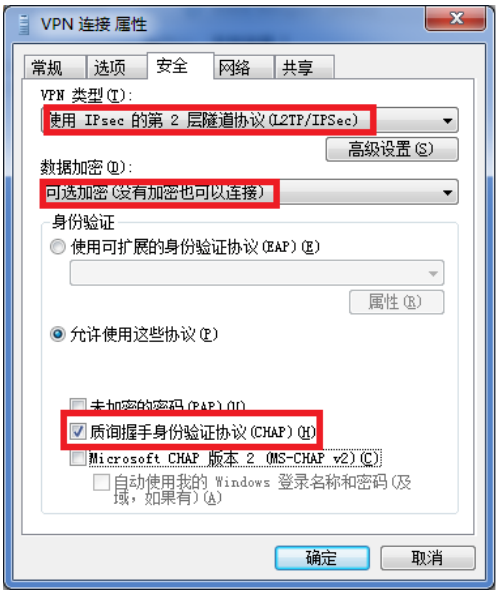
#“Internet地址”置防火墙外网接口的IP地址。

#设置用于VPN拨号的用户名和密码

#再次单击电脑桌面右下角的电脑图标，鼠标右击点击“属性”按钮。



#在“安全”页签中选择VPN类型为“使用IPsec的第2层隧道协议（L2TP/IPSEC）”,数据加密选择“可选加密”，允许协议选择“质询握手身份验证协议（CHAP）”。

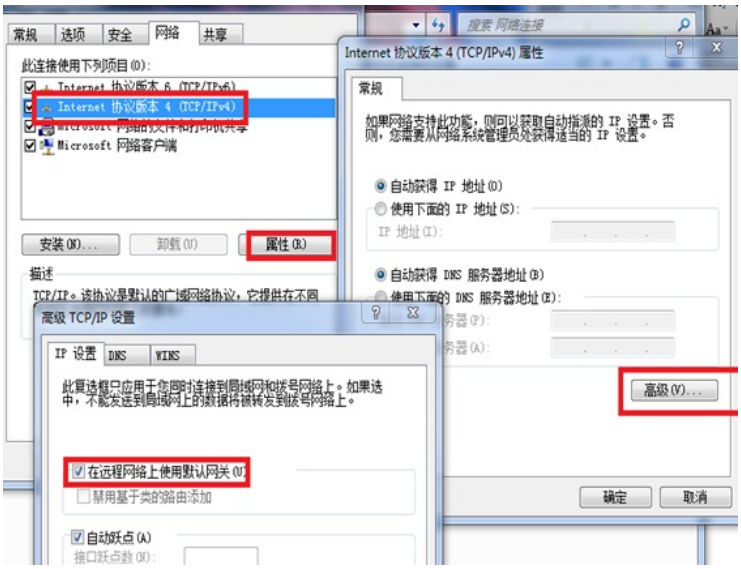


4.2 Windows 7电脑拨号常见问题

4.2.1 连接VPN后无法连接外网

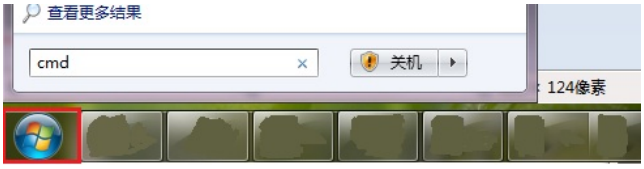
#VPN拨号成功后会在电脑路由表中生成一条到VPN网关的默认路由，其优先级高于电脑自身网关的默认路由。如果即想访问VPN又想上网请参考下面配置。

去掉“在远程网络上使用默认的网关”勾选。



#在电脑添加到对端内网的明细路由。

#打开电脑命令提示图窗口，输入CMD命令。



#增加目的地址为192.168.10.0（防火墙内网地址段），掩码为255.255.255.0，网关地址为192.168.100.1的路由。

配置关键点