

知 V7防火墙SSL VPN 不同用户获取不同段地址访问不同内网IP资源典型案例 (WEB配置)

SSL VPN 张新姿 2021-01-11 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：如F5080、F5060、F5030、F5000-M等F5000、F5000-X系列的防火墙。

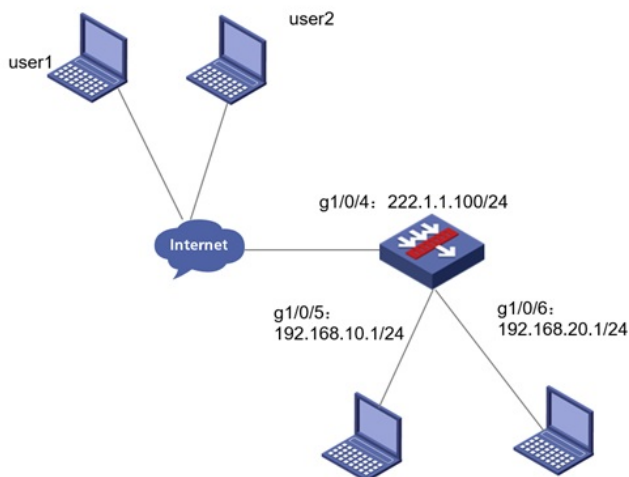
注：本案例是在F1000-C-G2的Version 7.1.064, Release 9323P19版本上进行配置和验证的。

1.2 配置需求及实现的效果

V7防火墙设备作为出口设备，外网PC通过inode软件拨SSLVPN，user1认证成功后可以访问内网192.168.10.0网段的资源。user2认证成功后可以访问内网192.168.20.0网段的资源。IP地址及接口规划如下表所示：

外网接口	公网地址/掩码	内网接口	内网地址/掩码
GE1/0/4	222.1.1.100/24	GE1/0/5	192.168.10.1/24
		GE1/0/6	192.168.20.1/24

2 组网图



配置步骤

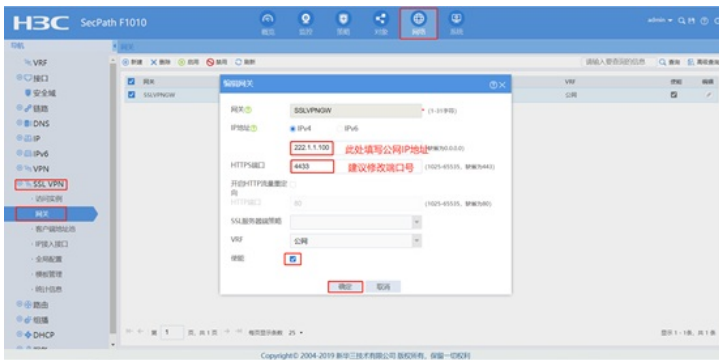
1 配置步骤

1.1 防火墙上网配置

防火墙上网配置请参考“2.2.2 防火墙外网使用固定IP地址上网配置方法”进行配置，本文只针对SSLVPN配置进行介绍。

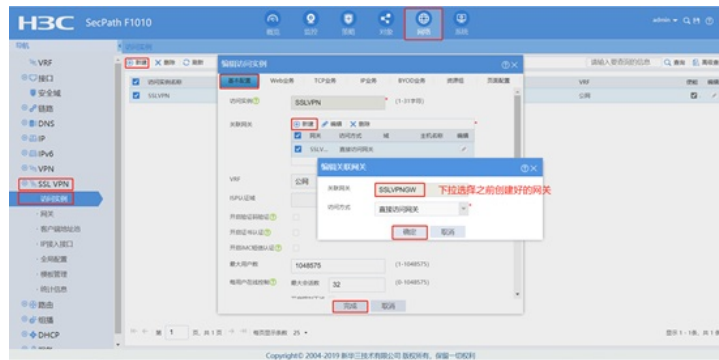
1.2 配置SSL VPN网关

#选择“网络”>“SSL VPN”>“网关”点击“新建”，IP地址填写防火墙1口地址222.1.1.1.00，端口号修改为443，缺省端口为443，443端口和https端口冲突。勾选“使能”选项点击“确认”完成配置

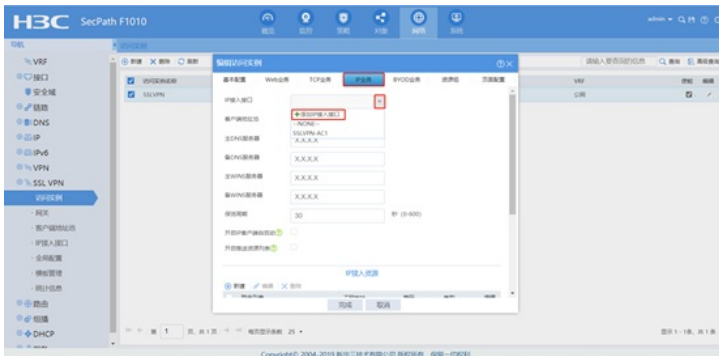


1.3 配置SSL VPN实例

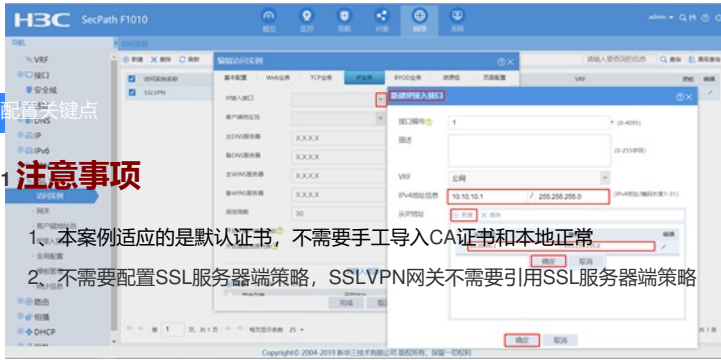
#选择“网络”>“SSL VPN”>“访问实例”中点击“新建”，在“关联网关”中点击“新建”，下拉选择上一步创建的SSL VPN网关，确定后点击“下一步”



#选择“IP业务”，然后下拉选择“添加IP接入接口”



#新建SSL VPN接口，接口编号为1，配置SSL VPN接口IP，IP地址不要和内网网段冲突，新建从IP地址，配置完成点击“确定”。



配置关键点

1 注意事项

- 1、本案例适应的是默认证书，不需要手工导入CA证书和本地正常
- 2、不需要配置SSL服务器端策略，SSLVPN网关不需要引用SSL服务器端策略