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（命令行配置）

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。

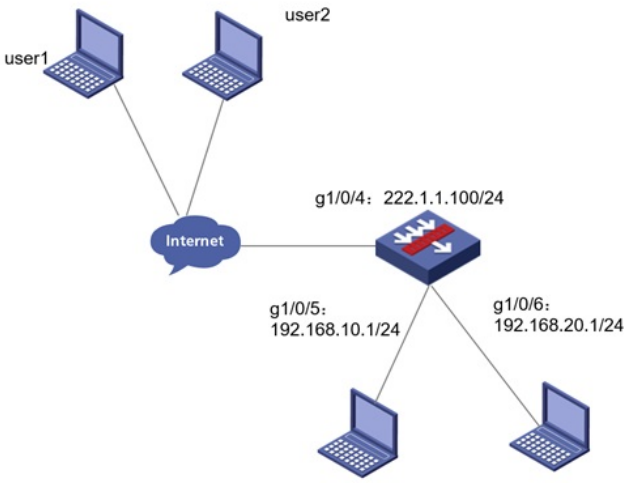
注：本案例是在F100-C-G2的version 7.1.064, Release 9333P35版本上进行配置和验证的。

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，认证成功后可以访问内网的资源。User1可以获取获取10.10.10.0/24网段的地址，访问192.168.10.0/24资源, User1可以获取获取20.20.20.0/24网段的地址，访问192.168.20.0/24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	192.168.10.0/24
		内网接口	内网地址/掩码
		GE1/0/6	192.168.20.0/24

2 组网图



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

#SSLVPN网关IP地址填写防火墙1口地址222.1.1.1.00，端口号修改为4433，缺省端口为443，443端口和https端口冲突，然后使能网关配置。

<H3C>sys

[H3C]sslvpn gateway SSLVPNGW

[H3C-sslvpn-gateway-SSLVPNGW]ip address 222.1.1.100 port 4433

[H3C-sslvpn-gateway-SSLVPNGW]service enable

[H3C-sslvpn-gateway-SSLVPNGW]quit

#创建SSL VPN AC接口1,配置接口IP为10.10.10.1/24

[H3C]interface SSLVPN-AC 1

[H3C-SSLVPN-AC1]ip address 10.10.10.1 255.255.255.0

[H3C-SSLVPN-AC1]ip address 20.20.20.1 255.255.255.0 sub

[H3C-SSLVPN-AC1]quit

#创建地址池名称为“SSLPOOL1”，指定IP地址范围为10.10.10.2——10.10.10.254

[H3C]sslvpn ip address-pool SSLPOOL 10.10.10.2 10.10.10.254

#创建地址池名称为“SSLPOOL2”，指定IP地址范围为20.20.20.2——20.20.20.254

sslvpn ip address-pool SSLPOOL2 20.20.20.2 20.20.20.254

#创建ACL 3998，允许SSL VPN用户访问的内网资源192.168.20.0/24网段

[H3C]acl advanced 3998

[H3C-acl-ipv4-adv-3998]rule permit ip destination 192.168.20.0 0.0.0.255

[H3C-acl-ipv4-adv-3998]quit

#创建ACL 3999，允许SSL VPN用户访问的内网资源192.168.10.0/24网段

[H3C]acl advanced 3999

[H3C-acl-ipv4-adv-3999]rule permit ip destination 192.168.10.0 0.0.0.255

[H3C-acl-ipv4-adv-3999]quit

1.3 配置SSL VPN实例

配置SSL VPN访问实例“SSLVPNSL”引用SSL VPN网关“SSLVPNGW”

[H3C] sslvpn context SSLVPN

[H3C-sslvpn-context-SSLVPN]gateway SSLVPNGW

#引用SSL VPN接口1

[H3C-sslvpn-context-SSLVPN] ip-tunnel interface SSLVPN-AC1

#引用SSL VPN地址池，掩码和dns

[H3C-sslvpn-context-SSLVPN]ip-tunnel address-pool SSLPOOL mask 255.255.255.0

[H3C-sslvpn-context-SSLVPN]ip-tunnel dns-server primary 114.114.114.114

#创建路由列表“NEIWANG1”，添加路由表项192.168.10.0/24

[H3C-sslvpn-context-SSLVPN] ip-route-list NEIWANG1

[H3C-sslvpn-context-SSLVPN-route-list-NEIWANG1] include 192.168.10.0 255.255.255.0

#创建路由列表“NEIWANG2”，添加路由表项192.168.20.0/24

[H3C-sslvpn-context-SSLVPN] ip-route-list NEIWANG2

[H3C-sslvpn-context-SSLVPN-route-list-NEIWANG2] include 192.168.20.0 255.255.255.0

创建SSL VPN策略组“SSLVPNZIYUAN”，引用路由列表“NEIWANG1”，配置ACL限制，只有通过ACL检查的报文才可以访问IP资源

[H3C-sslvpn-context-SSLVPN] policy-group SSLVPNZIYUANGROUP1

[H3C-sslvpn-context-SSLVPN-policy-group-SSLVPNZIYUAN]filter ip-tunnel acl 3999

[H3C-sslvpn-context-SSLVPN-policy-group-SSLVPNZIYUAN]ip-tunnel access-route ip-route-list NEIWANG1

创建SSL VPN策略组“SSLVPNZIYUAN”，引用路由列表“NEIWANG2”，配置ACL限制，只有通过ACL检查的报文才可以访问IP资源

[H3C-sslvpn-context-SSLVPN] policy-group SSLVPNZIYUANGROUP2

[H3C-sslvpn-context-SSLVPN-policy-group-SSLVPNZIYUAN]filter ip-tunnel acl 3998

[H3C-sslvpn-context-SSLVPN-policy-group-SSLVPNZIYUAN]ip-tunnel access-route ip-route-list NEIWANG2

[H3C-sslvpn-context-SSLVPN-policy-group-SSLVPNZIYUAN]ip-tunnel address-pool SSLPOOL2 mask 255.255.255.0

#启用该实例,用户绑定地址。

[H3C-sslvpn-context-SSLVPN-policy-group-SSLVPNZIYUAN]quit

[H3C-sslvpn-context-SSLVPN] user user2

[H3C-sslvpn-context-SSLVPN-user-user1] ip-tunnel bind address 20.20.20.2-20.20.20.10

[H3C-sslvpn-context-SSLVPN] service enable

[H3C-sslvpn-context-SSLVPN]quit

配置关键点

1.4 新建SSL VPN用户，关联SSLVPN资源组

1 注意事项

创建SSLVPN本地用户,配置用户名密码user1,服务类型sslvpn，引用之前创建的SSLVPN资源组1

[H3C]local-user user1 class network

[H3C-luser-network-user1]password simple user1

[H3C-luser-network-user1]service-type sslvpn

[H3C-luser-network-user1]authorization-attribute sslvpn-policy-group SSLVPNZIYUANGROUP1

[H3C-luser-network-user1]quit

#创建SSLVPN本地用户,配置用户名密码user2,服务类型sslvpn，引用之前创建的SSLVPN资源

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