

组网及说明

1 配置需求及说明

1.1 适用的产品系列

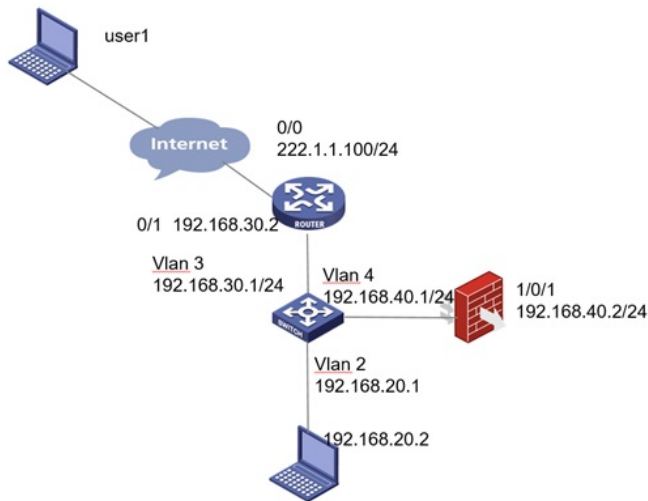
本案例适用于软件平台为Comware V7系列防火墙：本案例适用于如F1080、F1070、F5040、F5020等F10X0、F50X0系列的防火墙。

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

路由器设备作为出口设备，防火墙旁挂，外网PC通过inode软件拨SSLVPN，认证成功后可以访问内网的资源。

2 组网图



配置步骤

1 配置步骤

1.1 路由器配置

设置路由器出0口地址222.1.1.100，配置nat outbound,以及针对内部的提供服务的端口号修改为14433，缺省端口为443，443端口和https端口冲突，然后配置nat server映射对应的端口

```
[H3C]interface GigabitEthernet0/0
[H3C-GigabitEthernet0/0]ip address 222.1.1.100 255.255.255.0
[H3C-GigabitEthernet0/0] nat outbound
[H3C-GigabitEthernet0/0] nat server protocol tcp global 222.1.1.100 14443 inside 192.168.40.2
14443
```

设置路由器内网接口地址为192.168.30.2

```
[H3C]interface GigabitEthernet0/1
[H3C-GigabitEthernet0/1] ip address 192.168.30.2 255.255.255.0
[H3C-GigabitEthernet0/1]
```

路由器设置针对内网的网段路由：

```
[H3C] ip route-static 0.0.0.0 0 222.1.1.200
[H3C] ip route-static 192.168.0.0 16 192.168.30.1
```

1.2 配置交换机和防火墙以及路由器互联

#配置策略路由保证内网的数据可以上送到防火墙设备

```
[H3C]acl ad 3000
[H3C-acl-ipv4-adv-3000] rule 10 permit ip source 192.168.20.0 0.0.0.255 destination 10.10.10.0 0.0.0.255
[H3C-acl-ipv4-adv-3000]quit
[H3C]policy-based-route aaa permit node 10
[H3C-pbr-aaa-10] if-match acl 3000
[H3C-pbr-aaa-10] apply next-hop 192.168.40.2
[H3C-pbr-aaa-10]quit
```

#配置对应的ip地址和调用策略路由

```
[H3C]interface Vlan-interface2
[H3C-Vlan-interface2] ip address 192.168.20.1 255.255.255.0
[H3C-Vlan-interface2] ip policy-based-route aaa
[H3C-Vlan-interface2]quit
[H3C]interface Vlan-interface3
[H3C-Vlan-interface3] ip address 192.168.30.1 255.255.255.0
[H3C-Vlan-interface3]quit
[H3C]interface Vlan-interface4
[H3C-Vlan-interface4] ip address 192.168.40.1 255.255.255.0
[H3C-Vlan-interface4]quit
```

#配置相应的路由

```
[H3C] ip route-static 0.0.0.0 0 192.168.30.2
```

1.3 配置防火墙静态路由

#配置相应的路由

```
[H3C] ip route-static 0.0.0.0 0 192.168.40.1
```

1.4 配置SSL VPN网关

#SSLVPN网关IP地址填写防火墙1口地址192.168.40.2，端口号修改为14433，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 192.168.40.2 port 14433
[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]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 192.168.20.0 0.0.0.255
[H3C-acl-ipv4-adv-3999]quit
```

1.5 防火墙配置SSL VPN实例

配置关键点

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

```
[H3C-sslvpn-context-SSLVPN]
1 注意事项
[H3C-sslvpn-context-SSLVPN]gateway SSLVPNGW
```

#引用SSL VPN接口1
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

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

#引用SSL VPN地址池，掩码和dns

3、交换机上需要将对应的流量通过策略路由形式引到防火墙进行处理，以免数据来回路径不一致

```
[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“NEIWANG”，添加路由表项192.168.20.0/24

```
[H3C-sslvpn-context-SSLVPN] ip-route-list NEIWANG
```