

组网及说明

1 配置需求及说明

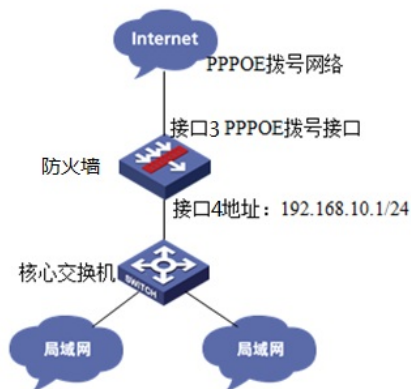
1.1 适用的产品系列

本案例适用于如F1000-AK180、F1000-AK170等F1000-AK系列的防火墙。

配置需求及实现的效果

将防火墙部署在互联网出口，使用PPPOE拨号方式接入互联网。运营商提供的拨号账号为：hz123456，密码为：123456。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，要求内网终端可以自动获取到地址并可以访问互联网。

2 组网图



配置步骤

2.1 配置外网接口

将1/0/3设置为外网接口并设置拨号连接。

配置拨号访问组1以及对应的拨号访问控制条件。

```
system-view
```

```
[H3C]dialer-group 1 rule ip permit
```

```
# 在Dialer1接口上使能共享DDR。
```

```
[H3C]interface dialer 1
```

```
[H3C-Dialer1]dialer bundle enable
```

```
# 将Dialer1接口与拨号访问组1关联。
```

```
[H3C-Dialer1]dialer-group 1
```

```
# 配置Dialer1接口通过协商获取IP地址。
```

```
[H3C-Dialer1]ip address ppp-negotiate
```

```
[H3C-Dialer1]ppp ipcp dns admit-any
```

```
[H3C-Dialer1]ppp ipcp dns request
```

```
# 配置PPPoE Client工作在永久在线模式。
```

```
[H3C-Dialer1]dialer timer idle 0
```

```
# 配置本地以CHAP方式认证时发送的CHAP用户名和密码和以PAP方式认证时发送的CHAP用户名和密码
```

```
[H3C-Dialer1]ppp chap password simple 123456
```

```
[H3C-Dialer1]ppp chap user hz123456
```

```
[H3C-Dialer1]ppp pap Local-user hz123456 password simple 123456
```

```
[H3C-Dialer1]tcp mss 1024
```

```
[H3C-Dialer1]quit
```

```
# 配置PPPoE会话与1/0/3端口绑定。
```

```
[H3C]interface GigabitEthernet 1/0/3
```

```
[H3C-GigabitEthernet1/0/3]pppoe-client dial-bundle-number 1
```

```
[H3C-GigabitEthernet1/0/3]quit
```

2.2 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
```

配置NAT地址转换

#进入Dialer 1拨号接口配置NAT动态地址转换。

```
[H3C]interface dialer 1
```

```
[H3C-Dialer1]nat outbound
```

```
[H3C-Dialer1]quit
```

2.3 配置到外网的缺省路由

#配置默认路由，指向拨号的虚接口dialer 1。

```
[H3C]ip route-static 0.0.0.0 0 dialer 1
```

2.4 配置外网接口加入Untrust安全区域

#将1/0/3、Dia1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 dialer 1
```

```
[H3C-security-zone-Untrust]quit
```

2.5 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
```

2.6 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Untrust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
```

2.7 配置安全策略将Trust到Local域、Local到Trust、Local到Untrust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
```

#创建Local到Untrust域的域间策略调用pass策略。

```
[H3C]zone-pair security source Local destination Untrust
```

```
[H3C-zone-pair-security-Local-Untrust]object-policy apply ip pass
```

```
[H3C-zone-pair-security-Local-Untrust]quit
```

2.8 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 mask 255.255.255.0
```

```
[H3C-dhcp-pool-1]gateway-list 192.168.10.1
```

```
[H3C-dhcp-pool-1]dns-list 114.114.114.114 8.8.8.8
```

```
[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。

2.9 保存配置

```
[H3C]save force
```

