本电子书由CyberArticle制作。点击这里下载CyberArticle。注册版本不会显示该信息。 删除广告

防火墙外网使用DHCP方式上网配置方法（命令行）

目录

1 配置需求及说明

1.1 适用的产品系列

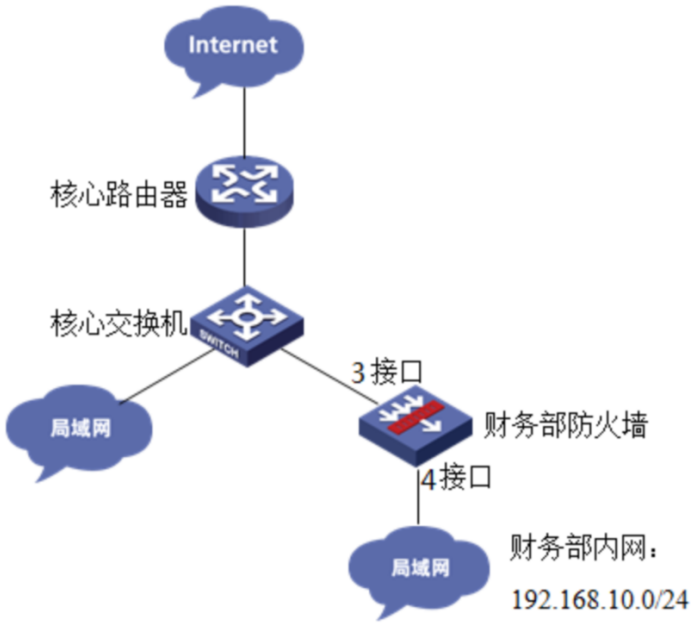
本案例适用于软件平台为Comware V7系列防火墙：F100-X-G2、F1000-X-G2、F100-X-WiNet、F1000-AK、F10X0等。

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

将防火墙部署在公司核心网络下为财务部门提供网络安全防护，要求防火墙使用3接口自动获取公司内网地址，4接口连接财务部为财务部用户动态下发192.168.10.0网段地址。在对公司原有网络影响最小的情况下实现财务部电脑可以主动访问防火墙以外的网络，防火墙以外的网络不能主动访问财务部电脑的需求。

2 组网图



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
dhcp-alloc
[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 配置外网接口加入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]quit
```

3.5 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
```

3.6 安全策略配置

防火墙目前版本存在两套安全策略，请在放通安全策略前确认设备运行那种类型的安全策略？以下配置任选其一。

1. 通过命令“display cu | in security-policy”如果查到命令行存在“security-policy disable”或者没有查到任何信息，则使用下面策略配置。

```
[H3C]display cu | in security-policy
 security-policy disable
```

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
```

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
```

#创建Untrustl到Loca域的域间策略调用pass策略。

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

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

2. 通过命令“display cu | in security-policy”如果查到命令行存在“security-policy ip”并且没有查到“security-policy disable”，则使用下面策略配置。

```
[H3C]display cu | in security-policy
security-policy ip
```

创建安全策略并放通local到trust和trust到local的安全策略。

```
[H3C]security-policy ip
[H3C-security-policy-ip]rule 10 name test
[H3C-security-policy-ip-10-test]action
pass
[H3C-security-policy-ip-10-test]source-
zone local
[H3C-security-policy-ip-10-test]source-
zone Trust
[H3C-security-policy-ip-10-test]source-
zone Untrust
[H3C-security-policy-ip-10-test]
destination-zone local
[H3C-security-policy-ip-10-test]
```

```
destination-zone Trust
[H3C-security-policy-ip-10-test]
destination-zone Untrust
[H3C-security-policy-ip-10-test]quit
```

3.7 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。

3.8 保存配置

```
[H3C]save force
```