

403 Forbidden

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](#)

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（**NAT**全局策略方式命令行）

目录

1 配置需求及说明

1.1 适用的产品系列

1.2 配置需求及实现的效果

2 组网图

3 配置步骤

3.1 配置外网接口

3.2 配置内网接口

3.3 配置NAT地址转换

[3.4 配置外网接口加入Untrust安全区域](#)

[3.5 配置内网接口加入Trust安全区域](#)

[3.6 安全策略配置](#)

[3.7 配置DHCP服务](#)

[3.8 保存配置](#)

1 配置需求及说明

1.1 适用的产品系列

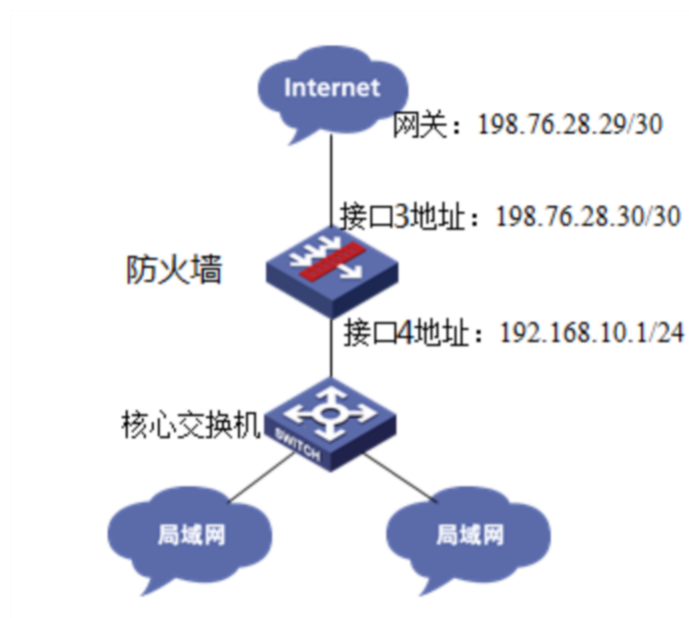
本案例适用于F1000-AI-X系列防火墙。

注：本案例是在HCL V3.01的F1090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

#配置NAT全局策略，实现从**trust**安全域到**untrust**安全域的源地址转换，转换方式为**easy-ip**。

```
[H3C]nat global-policy
[H3C-nat-global-policy]rule      name
easy_ip
[H3C-nat-global-policy-rule-
easy_ip]source-zone Trust
[H3C-nat-global-policy-rule-
easy_ip]destination-zone Untrust
[H3C-nat-global-policy-rule-
easy_ip]action snat easy-ip
[H3C-nat-global-policy-rule-
easy_ip]quit
[H3C-nat-global-policy]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

创建安全策略并放通local到trust和trust到local的安全策略（用于DHCP获取地址）以及trust到untrust的安全策略（用于上网）。放通local和untrust之间的安全策略用于外网口获取IP地址。

```
[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]
```

```

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
[H3C-security-policy-ip]rule          20
name dhcp
[H3C-security-policy-ip-20-dhcp]
action pass
[H3C-security-policy-ip-20-dhcp]
source-zone local
[H3C-security-policy-ip-20-dhcp]
source-zone untrust
[H3C-security-policy-ip-20-dhcp]
destination-zone local
[H3C-security-policy-ip-20-dhcp]
destination-zone untrust
[H3C-security-policy-ip-20-dhcp]
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
```