

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

防火墙外网使用固定IP地址方式上网配置方法（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 配置到外网的缺省路由](#)

[3.5 配置外网接口加入Untrust安全区域](#)

[3.6 配置内网接口加入Trust安全区域](#)

[3.7 安全策略配置](#)

[3.8 配置DHCP服务](#)

[3.9 保存配置](#)

1 配置需求及说明

1.1 适用的产品系列

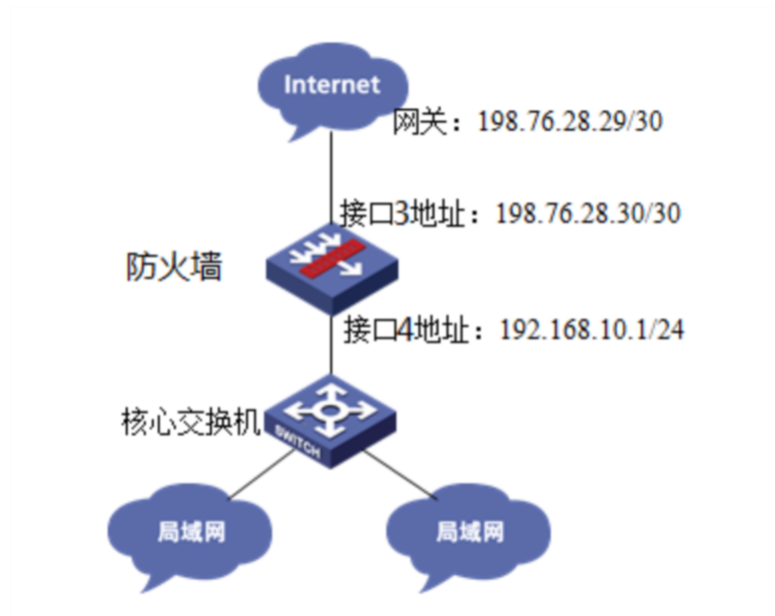
本案例适用于F1000-AI-X系列防火墙。

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

将防火墙部署在互联网出口，使用固定IP地址线路接入互联网。运营商提供的IP地址为198.76.28.30/30，网关为198.76.28.29，DNS地址为114.114.114.114。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



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              198.76.28.30
255.255.255.252
[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 配置到外网的缺省路由

#配置默认路由，下一跳为外网网关地址。

```
[H3C]ip    route-static    0.0.0.0    0
198.76.28.29
```

3.5 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
```

3.6 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
```

3.7 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）。

```
[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

```

3.8 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。

3.9 保存配置

```
[H3C]save force
```