F10X0/F50X0系列防火墙外网使用DHCP方式上网配置方法（命令行）

DHCP　zhiliao_FO3qD　2018-11-25 发表

组网及说明

1 配置需求及说明

1.1 适用的产品系列

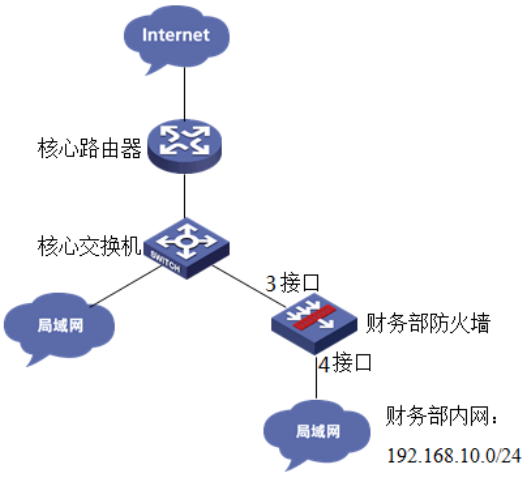
本案例适用于如F1080、F1070、F5040、F5020等F10X0、F50X0系列的防火墙

注：本案例是在F100-C-G2的Version 7.1.064, Release 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



配置步骤

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。

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 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

3.7 配置安全策略将Trust到Local域、Local到Trust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

3.8 配置安全策略将Untrust到Local域、Local到Untrust域DHCP流量放通策略

#创建服务对象DHCP用于匹配DHCP的UDP 67、68端口。

[H3C]object-group service DHCP

[H3C-obj-grp-service-DHCP]service udp destination range 67 68

[H3C-obj-grp-service-DHCP]quit

#在对象策略中调用DHCP服务对象。

[H3C]object-group service DHCP

[H3C-object-policy-ip-DHCP]rule pass service DHCP

[H3C-object-policy-ip-DHCP]quit

#创建Untrust到Local域的域间策略调用DHCP服务对象策略。

[H3C]zone-pair security source Untrust destination Local

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

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

#创建Local到Untrust域的域间策略调用DHCP服务对象策略。

[H3C]zone-pair security source Local destination Untrust

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

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

3.9 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。

3.10 保存配置

[H3C]save force

配置关键点