防火墙内网使用二层口上网配置方法（命令行）

二层转发 张新姿 2020-12-14 发表

组网及说明

1 配置需求及说明

1.1 适用的产品系列

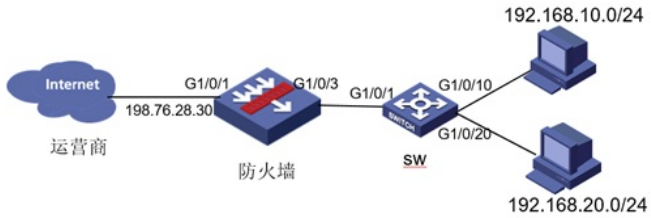
本案例适用于软件平台为Comware V7系列防火墙：如F1000-A-G2、F1000-S-G2、F100-M-G2、F100-S-G2等F1000-X-G2、F100-X-G2系列的防火墙。

注：本案例是在F100-C-G2的ersion 7.1.064, Release 9333P30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1接口接入运营商，使用3接口连接内网二层交换机，电脑接到交换机10口可以获取192.168.10.0网段地址上网，接到交换机20口可以获取192.168.20.0网段地址上网。

2 组网图



配置步骤

1 配置步骤

1.1 配置外网接口

#将1/0/1设置为外网接口并设置IP地址。

<H3C>system-view

[H3C]interface GigabitEthernet 1/0/1

[H3C-GigabitEthernet1/0/3]ip address 198.76.28.30 255.255.255.252

[H3C-GigabitEthernet1/0/3]quit

1.2 配置NAT地址转换

#进入1/0/1接口配置NAT动态地址转换。

[H3C]interface GigabitEthernet 1/0/1

[H3C-GigabitEthernet1/0/3]nat outbound

[H3C-GigabitEthernet1/0/3]quit

1.3 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

1.4 创建VLAN虚接口，配置对应网关地址

#创建VLAN 10，VLAN 20

[H3C]vlan 10

[H3C-vlan10]qu

[H3C]vlan 20

[H3C-vlan20]qu

#创建VLAN虚接口，配置地址

[H3C]int vlan 10

[H3C-Vlan-interface10]ip add 192.168.10.1 24

[H3C-Vlan-interface10]qu

[H3C]int vlan 20

[H3C-Vlan-interface20]ip add 192.168.20.1 24

[H3C-Vlan-interface20]qu

1.5 配置内网接口G1/0/3

#配置内网接口为1/0/3接口二层trunk口，放通所有VLAN

[H3C]int g1/0/3

[H3C-GigabitEthernet1/0/3]port link-mode bridge

[H3C-GigabitEthernet1/0/3]port link-type trunk

[H3C-GigabitEthernet1/0/3]port trunk permit vlan all

[H3C-GigabitEthernet1/0/3]qu

1.6 接口加安全域
#把G1/0/1接口加入“untrust”安全域
[H3C]security-zone name Untrust
[H3C-security-zone-Untrust] import interface GigabitEthernet1/0/1
[H3C-security-zone-Untrust]quit

#把G1/0/3接口接口加入“trust”安全域，并且绑定VLAN 1-4094
[H3C]security-zone name Trust
[H3C-security-zone-Trust]import interface GigabitEthernet1/0/3 vlan 1 to 4094
#把VLAN虚接口加入“trust”安全域
[H3C]security-zone name Trust
[H3C-security-zone-Trust] import interface Vlan-interface10
[H3C-security-zone-Trust] import interface Vlan-interface20
[H3C-security-zone-Trust]quit
1.7 配置安全策略将Trust到Untrust域内网数据放通
#创建内网地址的对象组
[H3C]object-group ip address neiwang
[H3C-obj-grp-ip-neiwang] security-zone Trust
[H3C-obj-grp-ip-neiwang] 0 network subnet 192.168.10.0 255.255.255.0
[H3C-obj-grp-ip-neiwang] 10 network subnet 192.168.20.0 255.255.255.0
[H3C-obj-grp-ip-neiwang] quit

#配置安全策略将trust到untrust域中内网访问外网的数据放通
[H3C]security-policy ip
[H3C-security-policy-ip] rule 0 name trust-untrsut
[H3C-security-policy-ip-0-trust-untrsut] action pass
[H3C-security-policy-ip-0-trust-untrsut] source-zone Trust
[H3C-security-policy-ip-0-trust-untrsut] destination-zone Untrust
[H3C-security-policy-ip-0-trust-untrsut] source-ip neiwang
[H3C-security-policy-ip-0-trust-untrsut]quit
1.8 配置DHCP服务
[H3C]dhcp enable
[H3C]dhcp server ip-pool 10
[H3C-dhcp-pool-10]network 192.168.10.0 mask 255.255.255.0
[H3C-dhcp-pool-10]gateway-list 192.168.10.1
[H3C-dhcp-pool-10]dns-list 114.114.114.114
[H3C-dhcp-pool-10]quit
[H3C]dhcp server ip-pool 20
[H3C-dhcp-pool-20]network 192.168.20.0 mask 255.255.255.0
[H3C-dhcp-pool-20]gateway-list 192.168.20.1
[H3C-dhcp-pool-20]dns-list 114.114.114.114
[H3C-dhcp-pool-20]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。

1.9 配置安全策略将Trust到Local域、Local到Trust域数据全放通策略
[H3C]security-policy ip
[H3C-security-policy-ip] rule 1 name DHCP
[H3C-security-policy-ip-1-DHCP] action pass
[H3C-security-policy-ip-1-DHCP] source-zone Trust
[H3C-security-policy-ip-1-DHCP] source-zone Local
[H3C-security-policy-ip-1-DHCP] destination-zone Trust
[H3C-security-policy-ip-1-DHCP] destination-zone Local
[H3C-security-policy-ip-1-DHCP] quit
1.10 保存配置
[H3C]save force
1.11 交换机端配置
#创建vlan
<H3C>system-view
[H3C]vlan 10
[H3C-vlan10]quit
[H3C]vlan 20
[H3C-vlan20]quit

#将连接路由器的接口切换成trunk口，并放通所有vlan
[H3C]interface GigabitEthernet 1/0/1
[H3C-GigabitEthernet1/0/1]port link-type trunk
[H3C-GigabitEthernet1/0/1]port trunk permit vlan all
[H3C-GigabitEthernet1/0/1]quit
#将连接PC1和PC2接口划分到相应的vlan中
[H3C]interface GigabitEthernet 1/0/10
[H3C-GigabitEthernet1/0/10] port access vlan 10
[H3C-GigabitEthernet1/0/10] interface GigabitEthernet 1/0/20
[H3C-GigabitEthernet1/0/20] port access vlan 20
#保存配置
[H3C]save force

配置关键点

无