防火墙通过Vlan实现内网多端口上网配置方法 （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

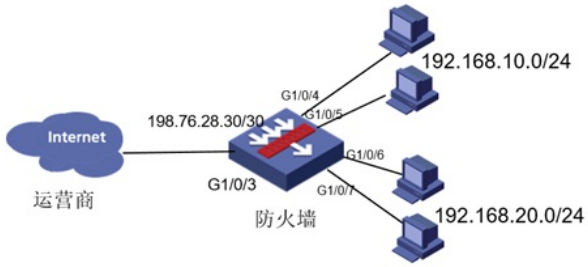
本案例适用于软件平台为Comware V7系列防火墙：如F1080、F1070、F5040、F5020等F10X0、F50X0系列的防火墙。

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3接口接入运营商，使用4接口到7接口连接内部网络，4接口和5接口使用192.168.10.0网段，6接口和7接口使用192.168.20.0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



配置步骤

1 配置步骤

1.1 配置互联网接口

#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

1.2 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

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 1作为192.168.10.0网段的网关

#创建VLAN1，配置VLAN1虚接口地址为192.168.10.1。

[H3C]vlan 1

[H3C-vlan1]quit

[H3C]interface Vlan-interface 1

[H3C-Vlan-interface1]ip address 192.168.10.1 24

[H3C-Vlan-interface1]quit

1.5 创建vlan 2作为192.168.20.0网段的网关

#创建VLAN2，配置VLAN2虚接口地址为192.168.20.1。

[H3C]vlan 2

[H3C-vlan2]quit

[H3C]interface Vlan-interface 2

[H3C-Vlan-interface2]ip address 192.168.20.1 24

[H3C-Vlan-interface2]quit

1.6 配置内网接口G1/0/4和G1/0/5

#配置内网接口为1/0/4接口和1/0/5接口为二层口，因为接口默认属于vlan1因此无需再将端口划分至vlan1中。

[H3C]interface GigabitEthernet 1/0/4

[H3C-GigabitEthernet1/0/4]port link-mode bridge
[H3C-GigabitEthernet1/0/4]quit
[H3C]interface GigabitEthernet 1/0/5
[H3C-GigabitEthernet1/0/5]port link-mode bridge
[H3C-GigabitEthernet1/0/5]quit
1.7 配置内网接口G1/0/6和G1/0/7
#配置内网接口为1/0/6接口和1/0/7接口为二层口，并且划分到VLAN2中
[H3C]interface GigabitEthernet 1/0/6
[H3C-GigabitEthernet1/0/6]port link-mode bridge
[H3C-GigabitEthernet1/0/6]port access vlan 2
[H3C-GigabitEthernet1/0/6]quit
[H3C]interface GigabitEthernet 1/0/7
[H3C-GigabitEthernet1/0/7]port link-mode bridge
[H3C-GigabitEthernet1/0/7]port access vlan 2
[H3C-GigabitEthernet1/0/7]quit
1.8 接口加安全域
#把G1/0/3接口加入“untrust”安全域
[H3C]security-zone name Untrust
[H3C-security-zone-Untrust] import interface GigabitEthernet1/0/3
[H3C-security-zone-Untrust]quit

#把G1/0/4到G1/0/7接口接口加入“trust”安全域，并且绑定VLAN 1-4094，VLAN虚接口也加入“trust”安全域。
[H3C]security-zone name Trust
[H3C-security-zone-Trust]import interface GigabitEthernet1/0/4 vlan 1 to 4094
[H3C-security-zone-Trust]import interface GigabitEthernet1/0/5 vlan 1 to 4094
[H3C-security-zone-Trust]import interface GigabitEthernet1/0/6 vlan 1 to 4094
[H3C-security-zone-Trust]import interface GigabitEthernet1/0/7 vlan 1 to 4094
[H3C-security-zone-Trust]import interface Vlan-interface1
[H3C-security-zone-Trust]import interface Vlan-interface2
[H3C-security-zone-Trust]quit
1.9 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

1.10 配置DHCP服务

[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

[H3C-dhcp-pool-1]quit

[H3C]dhcp server ip-pool 2

[H3C-dhcp-pool-2]network 192.168.20.0 mask 255.255.255.0

[H3C-dhcp-pool-2]gateway-list 192.168.20.1

[H3C-dhcp-pool-2]dns-list 114.114.114.114

[H3C-dhcp-pool-2]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。

1.11 保存配置

[H3C]save force

配置关键点

无