F1000-X-G2/F100-X-G2系列防火墙IPv6网络访问IPv4的互联网资源配置案例（命令行）

NAT 田威 2020-04-01 发表

组网及说明

1 配置需求或说明

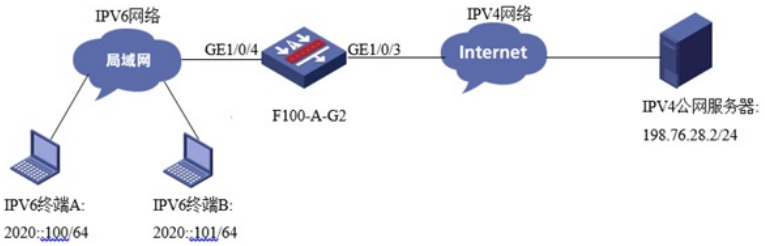
1.1 适用的产品系列

本案例适用于如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。

1.2 配置需求及实现的效果

某公司内部网络已经全部升级为IPV6，但是外网仍然使用运营商IPV4的网络。为实现内网IPV6用户上网需要使用防火墙AFT功能将IPV6地址转换为IPV4进行互联网访问；

2 组网图



配置步骤

3 配置步骤

3.1 配置连接IPV6网络的GE1/0/4接口

#将连接IPV6网络的1/0/4接口配置IPV6地址2020::1/64并作为内网IPV6主机的网关。

system-view

[H3C] interface GigabitEthernet1/0/4

[H3C-GigabitEthernet1/0/4]ipv6 address 2020::1 64

[H3C-GigabitEthernet1/0/4]undo ipv6 nd ra halt

[H3C-GigabitEthernet1/0/4 quit

3.2 配置连接IPV4网络的GE1/0/3接口

#将连接IPV4网络的1/0/3接口配置IPV4地址198.76.28.1/24用于连接IPV4互联网，并开启1/0/3接口的NAT转换功能。

system-view

[H3C] interface GigabitEthernet1/0/3

[H3C-GigabitEthernet1/0/3]ip address 198.76.28.1 255.255.255.0

[H3C-GigabitEthernet1/0/3] quit

3.3 配置IPV4网络的路由指向运营商网关

#配置路由指向运营商网关198.76.28.2.

[H3C]ip route-static 0.0.0.0 0 198.76.28.2

3.4 创建AFT地址池

#创建AFT地址池用于IPV6源地址转换为IPV4地址；

system-view

[H3C] aft address-group 0

[H3C-aft-address-group-0] address 100.100.100.1 100.100.100.100

[H3C-aft-address-group-0] quit

3.5 创建访问控制列表（选配）

#为实现只有2020::的主机可以访问IPV4网络，需要添加ACL将2020::的主机过滤出来，网内其他IPV6主机仍使用IPV6网络访问IPV6互联网；如果内网IPV6地址全部需要转换为IPV4地址访问IPV4网络则这步可以忽略不做。

[H3C]acl ipv6 basic 2000

[H3C-acl-ipv6-basic-2000]rule permit source 2020:: 64

[H3C-acl-ipv6-basic-2000]quit

3.6 创建AFT转换策略

#将ACL与AFT地址池绑定。

[H3C]aft v6tov4 source acl ipv6 number 2000 address-group 0

3.7 配置NAT64前缀

#配置NAT64前缀，此前缀用于IPV6终端访问此前缀+IPV4地址，设备根据此前缀将IPV6目的地址转换为IPV4目的地址。

[H3C]aft prefix-nat64 2019:: 96

3.8 在IPV4与IPV6接口都开启AFT转换功能

#开启接口的AFT转换功能

[H3C] interface GigabitEthernet1/0/3

[H3C-GigabitEthernet1/0/3] aft enable

[H3C-GigabitEthernet1/0/3]quit

[H3C] interface GigabitEthernet1/0/4

[H3C-GigabitEthernet1/0/4] aft enable

[H3C-GigabitEthernet1/0/4]quit

3.9 安全域及安全策略配置

#安全域配置：将1/0/3加入untrust安全域、将1/0/4加入trust安全域。

[H3C]security-zone name untrust

[H3C-security-zone-Untrust]import interface GigabitEthernet 1/0/3

[H3C-security-zone-Untrust]quit

[H3C]security-zone name trust

[H3C-security-zone-Trust]import interface GigabitEthernet 1/0/4

[H3C-security-zone-Trust]quit

#由于本章内容重在展示AFT效果，因此IPV4及IPV6安全策略为全放通状态；

[H3C]security-policy ipv6

[H3C-security-policy-ipv6]rule 0 name pass

[H3C-security-policy-ipv6-0-pass]action pass

[H3C-security-policy-ipv6-0-pass]quit

[H3C-security-policy-ipv6]quit

[H3C]security-policy ip

[H3C-security-policy-ip]rule 0 name pass

[H3C-security-policy-ip-0-pass]action pass

[H3C-security-policy-ip-0-pass]quit

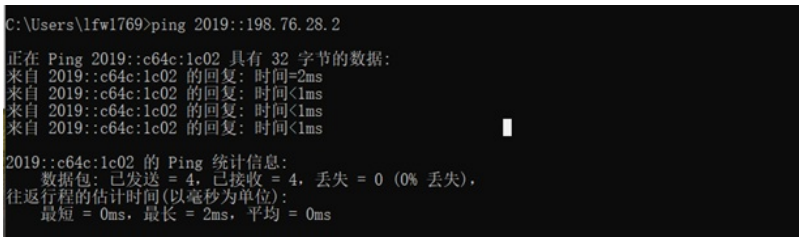
[H3C-security-policy-ip]quit

3.10 保存配置

[H3C]save force

3.11 结果测试

#使用IPV6终端访问IPV4终端结果：



#设备侧debug AFT信息：

debugging aft packet ipv6

debugging aft packet ip

[H3C-aft-address-group-0]*Nov 13 10:15:57:424 2019 H3C AFT/7/COMMON: -COntext=1;

PACKET: (GigabitEthernet1/0/4) Protocol: ICMPv6

2020::adc1:6213:6160:67a8/1 - 2019::c64c:1c02/32768(VPN:0) ------>

100.100.100.44/1 - 198.76.28.2/2048(VPN:0)

*Nov 13 10:15:57:425 2019 H3C AFT/7/COMMON: -COntext=1;

PACKET: (GigabitEthernet1/0/3) Protocol: ICMP

198.76.28.2/1 - 100.100.100.44/0(VPN:0) ------>

2019::c64c:1c02/1 - 2020::adc1:6213:6160:67a8/33024(VPN:0)

可以看到当设备收到2019::198.76.28.2的数据时会将后面的IPV4地址转换为16进制的2019::c64c:1c02，然后再将源地址转换为AFT地址池中的地址。

配置关键点

3.12 注意事项

1、防火墙从什么版本开始支持IPV6?

防火墙从R9323P15之后的版本才能完全支持IPV6相关功能，在使用IPV6前一定要确认目前防火墙版本在9323P15版本后；

2、如果将AFT地址池中的地址从100.100.100.1-100.100.100.100网段变更为 198.76.28.1（1/0/3接口公网地址）会出现什么现象?

如果将地址池中的地址变为接口公网地址，如下所示：

system-view

[H3C] aft address-group 0

[H3C-aft-address-group-0] address 198.76.28.1 198.76.28.1

[H3C-aft-address-group-0] quit

Debug AFT信息如下：

[H3C-GigabitEthernet1/0/3]*Nov 13 10:15:21:498 2019 H3C AFT/7/COMMON: -COntext=1;

PACKET: (GigabitEthernet1/0/4) Protocol: ICMPv6

2020::adc1:6213:6160:67a8/1 - 2019::c64c:1c02/32768(VPN:0) ------>

198.76.28.1/2 - 198.76.28.2/2048(VPN:0)

*Nov 13 10:15:21:499 2019 H3C AFT/7/COMMON: -COntext=1;

PACKET: (GigabitEthernet1/0/3) Protocol: ICMP

198.76.28.2/2 - 198.76.28.1/0(VPN:0) ------>

2019::c64c:1c02/1 - 2020::adc1:6213:6160:67a8/33024(VPN:0)

发现AFT直接会将数据的源地址转换为了198.76.28.1，这样1/0/3接口也就不需要配置NAT地址转换了。

-