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 IPv6 网络访问 IPv4 的互联网资源配置案例（WEB） 目录



# 1 配置需求或说明

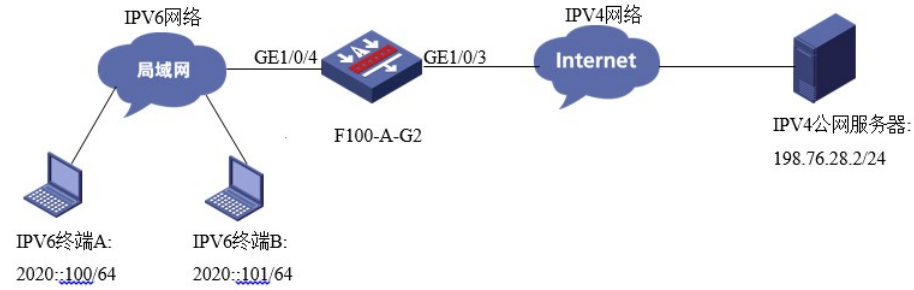
## 1.1 适用的产品系列

本案例适用于软件平台为 Comware V7 系列防火墙：F100-X-G2、F1000-X-G2、F100-WiNet、 F1000-AK、F10X0 等

注：本案例是在 F100-A-G2 的 Version 7.1.064, Release 9333P25 版本上进行配置和验证的。

## 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

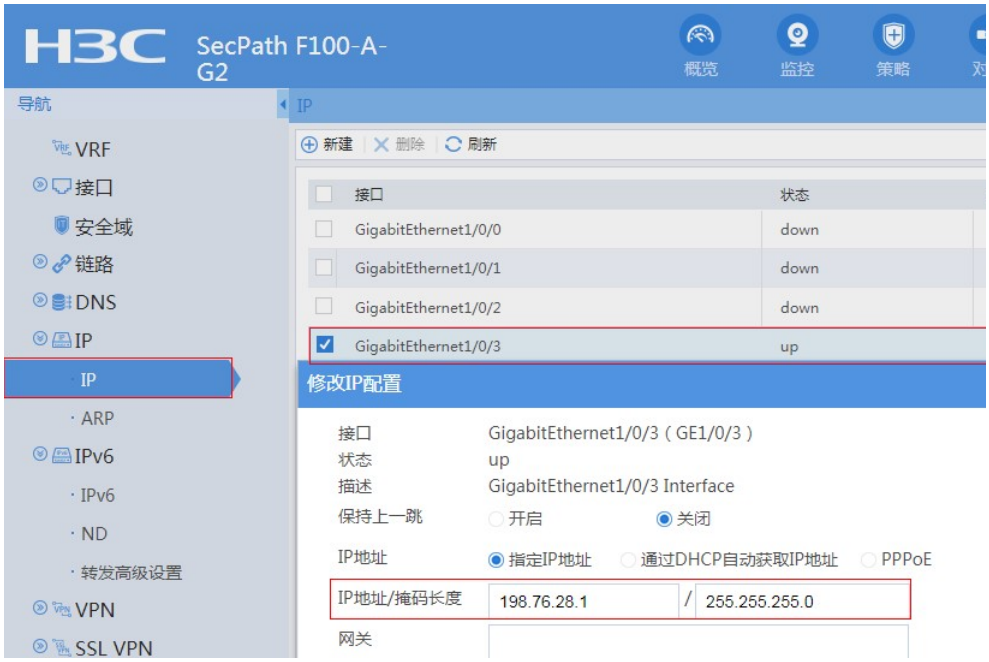
3 配置步骤

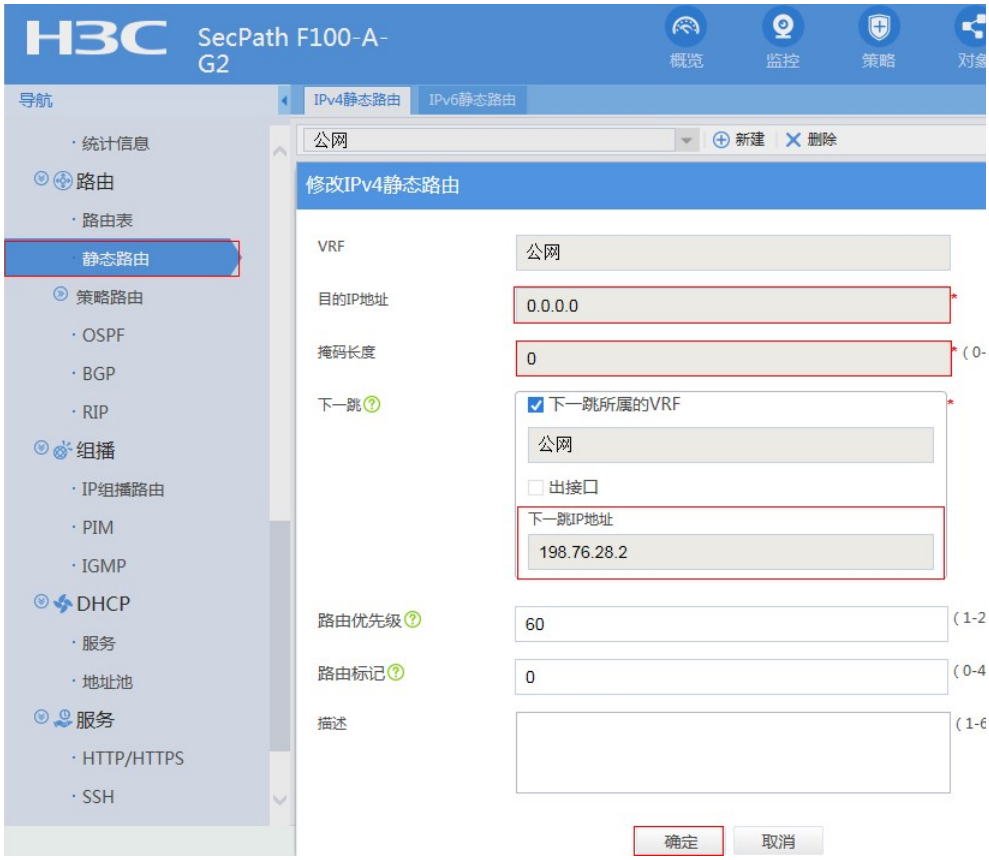
3.1 配置连接 IPV6 网络的 GE1/0/4 接口

#选择“网络”>“IPV6”选择 1/0/4 并点击编辑按钮为 GE1/0/4 接口配置 IPV6 地址。

3.2 配置连接 IPV4 网络的 GE1/0/3 接口

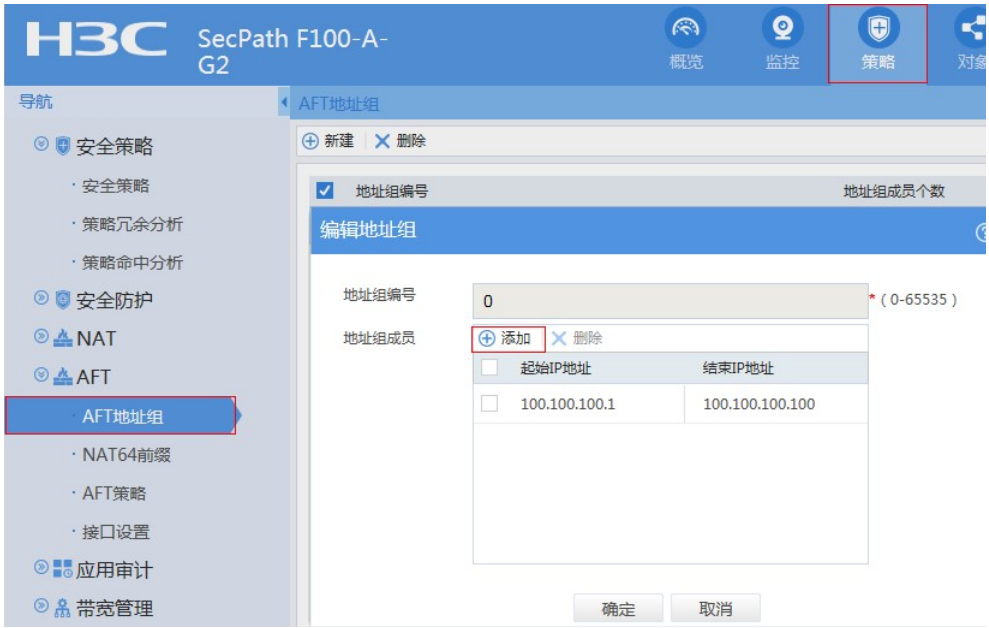
#在“网络”>“IP”选择 1/0/3 并点击编辑按钮为 GE1/0/3 接口配置 IPV4 地址。


H3C
SecPath F100-A-G2
概览
监控
策略
导航
VRF
接口
安全域
链路
DNS
IP
IP
ARP
IPv6
IPv6
ND
转发高级设置
VPN
SSL VPN
IP
新建
删除
刷新
接口
状态
GigabitEthernet1/0/0
down
GigabitEthernet1/0/1
down
GigabitEthernet1/0/2
down
GigabitEthernet1/0/3
up
修改IP配置
接口
GigabitEthernet1/0/3 ( GE1/0/3 )
状态
up
描述
GigabitEthernet1/0/3 Interface
保持上一跳
开启
关闭
IP地址
指定IP地址
通过DHCP自动获取IP地址
PPPoE
IP地址/掩码长度
198.76.28.1
/
255.255.255.0
网关




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，路由的目的地址为 0.0.0.0、掩码长度为 0、下一跳地址为 198.76.28.2。




3.4 创建 AFT 地址池

#在“策略”>“AFT”>“AFT 地址组”中新建 AFT 地址组，起始地址与结束地址分别为 100.100.100.1-100.100.100.100。

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。 #在 “对象” ACL”> IPV6”>“ “ 中新建 ACL 编号为 2000 的基本 ACL 并匹配源 IPV6 地址为 2020::/64。

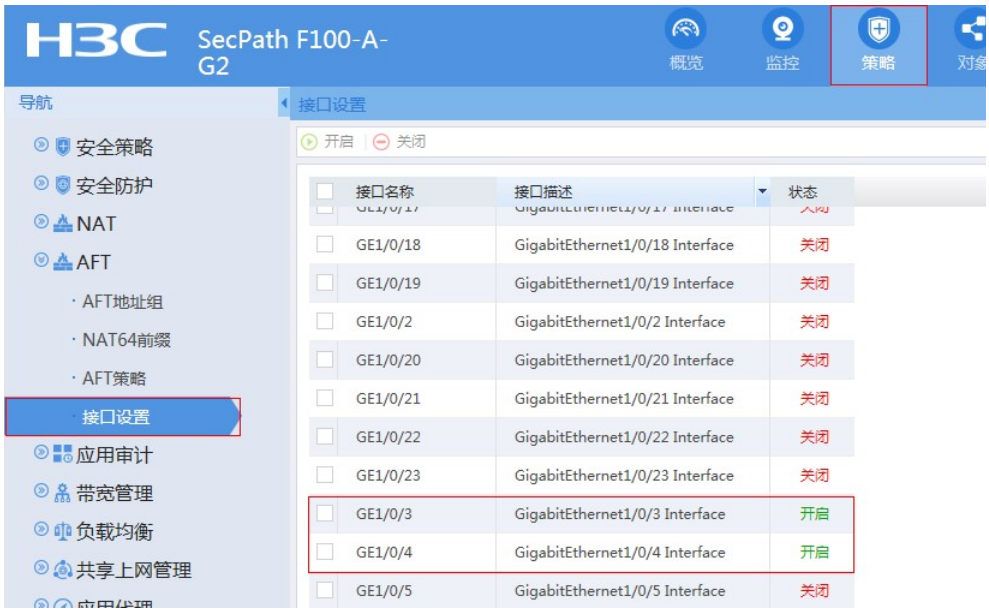


3.6 创建 AFT 转换策略

#在“策略”>“AFT”>“AFT 策略”中点击新建，将刚才创建的 ACL 与 AFT 地址池绑定。

3.7 配置 NAT64 前缀

#在“策略”>“AFT”>“NAT64 前缀”中点击新建，IPV6 前缀为 2019::、NAT64 前缀长度为 96。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。

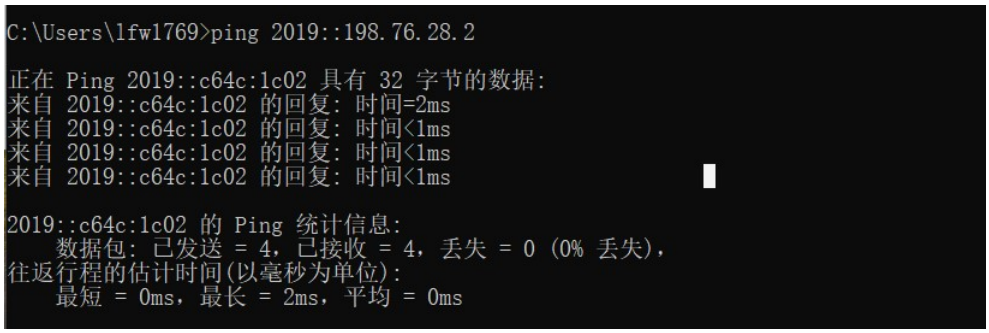

3.8 在 IPV4 与 IPV6 接口都开启 AFT 转换功能

#在“策略”>“AFT”>“接口设置”中点击 1/0/3 与 1/0/4 关闭按钮，将两个接口的 AFT 状态切 换为开启状态。

3.9 安全域及安全策略配置

#在“网络”>“安全域”中将 1/0/3 加入 untrust 安全域、将 1/0/4 加入 trust 安全域，如下图所示：




#在“策略”>“安全策略”中新建源安全域为 any、目的安全域为 any 的安全策略，如下图所示： 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；

3.10 保存配置

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： <H3C>debugging aft packet ipv6 <H3C>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。 在 WEB 界面中“监控”>“会话列表”中可以查看到当前会话信息： 1、IPV6 发起方的会话信息：

2、IPV4 发起方的会话信息：

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： <H3C> 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。