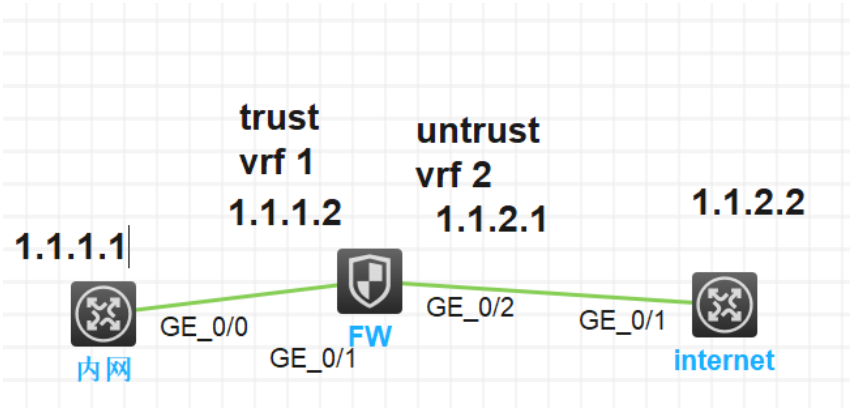
接口nat结合VRF案例

NAT VRF zhiliao_l9hSOv 2023-06-23 发表

组网及说明



1、防火墙1/0/2口做nat server将内网VPN 1内的PC 1.1.1.1映射为vpn2 内的公网接口地址 1.1.2.1，

2、内网VPN 1的PC1 1.1.1.1通过转换源地址访问公网 1.1.2.2 （在公网口 1/0/2 做nat outbound ）

问题描述

防火墙接口绑定vpn 实例，要实现接口vpn结合VRF

过程分析

1、防火墙安全策略放通

```
Security-policy ip
 rule 1 name 1
 action pass
 vrf 1   // 数据从绑定vpn实例的接口上来，写：vrf  vpn名称
 source-zone trust
 destination-zone untrust
 rule 2 name 2   （nat server 不匹配此策略）
 action pass
 vrf 2
 source-zone untrust
destination-zone trust
```

2、正常的路由要打通，数据上来后是查相关的vpn实例表。所以2边查找路由是都需要有相关的路由

此处简要写了2条缺省的 路由

```
 ip route-static vpn-instance 1 0.0.0.0 0 vpn-instance 2 1.1.2.2
 ip route-static vpn-instance 2 1.1.1.0 24 vpn-instance 1 1.1.1.1
```

查询相关的路由表项

```
[H3C]dis ip routing-table vpn-instance 1    // vpn实例 2 同理
 Destinations : 11 Routes : 11
 Destination/Mask  Proto    Pre     Cost      NextHop      Interface
0.0.0.0/0              Static      60      0           1.1.2.2          GE1/0/2
```

解决方法

1、通过nat outbound 转换，实现内网用户上网
interface GigabitEthernet1/0/2
 ip binding vpn-instance 2
 ip address 1.1.2.1 255.255.255.0
 nat outbound vpn-instance 2   // 数据从该口出，nat outbound 需要携带出接口 vpn-instance

2、通过nat outbound acl address-group ，实现内网部分用户访问公网/ 部分用户通过固定公网地址上网
通过acl 匹配内网用户
acl basic 2000
 rule 0 permit vpn-instance 1 source 1.1.1.1 0   // 写rule 规则时 数据从那个vpn 绑定的接口上来，需要带相关的 vpn-instance
相关接口nat outbound配置
interface GigabitEthernet1/0/2
 ip binding vpn-instance 2
 ip address 1.1.2.1 255.255.255.0
 nat outbound 2000 address-group 1 vpn-instance 2 // 数据从该口出，nat outbound 需要携带出接口 vpn-instance

3、通过公网地址间内网服务器映射出去
interface GigabitEthernet1/0/2
 ip binding vpn-instance 2
 ip address 1.1.2.1 255.255.255.0
 nat server global 1.1.2.1 vpn-instance 2 inside 1.1.1.1 vpn-instance 1
进行测试时： 1.1.2.2 ping 1.1.2.1 测试访问不通，通过debug nat packet 查看无回包命中
[H3C-GigabitEthernet1/0/2]undo na*Jun 23 13:02:46:626 2023 H3C NAT/7/COMMON: -COntext=1;
 PACKET: (GigabitEthernet1/0/2-in-config) Protocol: ICMP
 1.1.2.2:10985 -   1.1.2.1: 2048(VPN: 2) ------>
 1.1.2.2:10985 -   1.1.1.1: 2048(VPN: 1)
通过debug 查看 被安全策略拦截，无从untrust 到 trust 的策略， 匹配vpn-instance 1
*Jun 23 13:12:18:662 2023 H3C FILTER/7/PACKET: -COntext=1; The packet is denied. Src-ZOne=Untrust, D st-ZOne=Trust;If-In=GigabitEthernet1/0/2(3), If-Out=GigabitEthernet1/0/1(2); Packet Info:Src-IP=1.1. 2.2, Dst-IP=1.1.1.1, VPN-Instance=1,Src-Port=8, Dst-Port=0, Protocol=ICMP(1), Application=ICMP(22742),Terminal=invalid(0), ACL=none, Rule-ID=none.

在安全策略中添加一条测试成功 ,rule 2可删除
rule 3 name 3
 action pass vrf 1
 source-zone untrust
 destination-zone trust