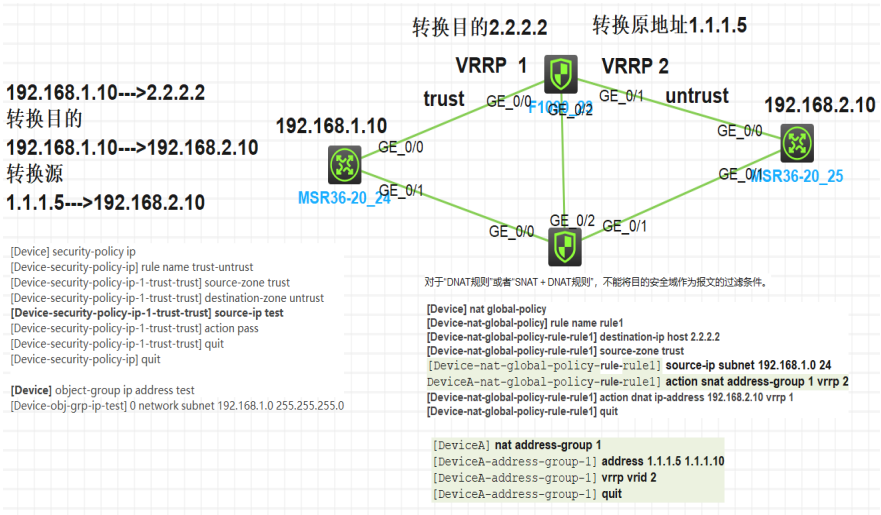
防火墙rbm主备结合vrrp 全局nat 单方向既转换源地址又转换目的地址

双机热备 VRRP NAT Super_King 2023-12-20 发表

组网及说明



配置步骤

防火墙配置rbm主备,参考官网案列

内网地址192.168.1.10--->2.2.2.2转换目的192.168.1.10--->192.168.2.10再转换源1.1.1.5--->192.168.2.10

防火墙是ｒｂm主备结合ｖｒｒｐ组网：

全局ｎａｔ配置：

对于“DNAT规则”或者“SNAT＋DNAT规则”，不能将目的安全域作为报文的过滤条件。

```
[Device] nat global-policy
[Device-nat-global-policy] rule name rule1
[Device-nat-global-policy-rule-rule1] destination-ip host 2.2.2.2
[Device-nat-global-policy-rule-rule1] source-zone trust
[Device-nat-global-policy-rule-rule1] source-ip subnet 192.168.1.0 24
DeviceA-nat-global-policy-rule-rule1] action snat address-group 1 vrrp 2
[Device-nat-global-policy-rule-rule1] action dnat ip-address 192.168.2.10 vrrp 1
[Device-nat-global-policy-rule-rule1] quit
[DeviceA] nat address-group 1
[DeviceA-address-group-1] address 1.1.1.5 1.1.1.10
[DeviceA-address-group-1] vrrp vrid 2
[DeviceA-address-group-1] quit
```

安全策略配置：

```
[Device] security-policy ip
[Device-security-policy-ip] rule name trust-untrust
[Device-security-policy-ip-1-trust-trust] source-zone trust
[Device-security-policy-ip-1-trust-trust] destination-zone untrust
[Device-security-policy-ip-1-trust-trust] source-ip test
[Device-security-policy-ip-1-trust-trust] action pass
[Device-security-policy-ip-1-trust-trust] quit
[Device-security-policy-ip] quit

[Device] object-group ip address test
[Device-obj-grp-ip-test] 0 network subnet 192.168.1.0 255.255.255.0
```

配置关键点

对于“DNAT规则”或者“SNAT＋DNAT规则”，不能将目的安全域作为报文的过滤条件。

要结合ｖｒｒｐ编号：

```
DeviceA-nat-global-policy-rule-rule1] action snat address-group 1 vrrp 2
[Device-nat-global-policy-rule-rule1] action dnat ip-address 192.168.2.10 vrrp 1
```

测试的ｎａｔ的ｄｅｂｕｇ

```
RBM_P<H3C>*Dec 20 00:45:54:605 2023 H3C NAT/7/COMMON: -COntext=1;
 PACKET: (GigabitEthernet1/0/0-in-config) Protocol: ICMP
    192.168.1.10:11021 -         2.2.2.5: 2048(VPN:     0) ------>
    192.168.1.10:11021 -     192.168.2.10: 2048(VPN:     0)
```

```
*Dec 20 00:45:54:606 2023 H3C NAT/7/COMMON: -COntext=1;
 PACKET: (GigabitEthernet1/0/1-out-config) Protocol: ICMP
    192.168.1.10:11021 -    192.168.2.10: 2048(VPN:    0) ------>
        1.1.1.10:    4 -    192.168.2.10: 2048(VPN:    0)
*Dec 20 00:45:54:606 2023 H3C NAT/7/COMMON: -COntext=1;
 PACKET: (GigabitEthernet1/0/1-in-session) Protocol: ICMP
    192.168.2.10:    4 -        1.1.1.10:    0(VPN:    0) ------>
    192.168.2.10:11021 -    192.168.1.10:    0(VPN:    0)
*Dec 20 00:45:54:606 2023 H3C NAT/7/COMMON: -COntext=1;
 PACKET: (GigabitEthernet1/0/0-out-session) Protocol: ICMP
    192.168.2.10:11021 -    192.168.1.10:    0(VPN:    0) ------>

        2.2.2.5:11021 -    192.168.1.10:    0(VPN:    0)
```