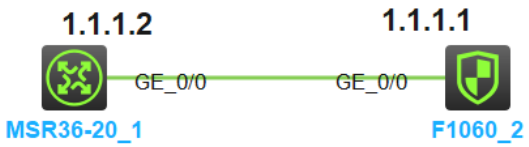
防火墙OSPF明细的安全策略如何配置

域间策略/安全域 OSPF 罗书鹏 2023-12-21 发表

组网及说明



告警信息

无

问题描述

防火墙和trust区域路由器建立OSPF邻居，由于条件限制，无法直接放通local和trust之间any的策略，如何添加明细策略建立OSPF

过程分析

建立OSPF邻居一般双向放通LOCAL和对应设备的IP地址，service 需要放通ospf协议。但还是不通，查询手册有说明：

广播（Broadcast）类型：当链路层协议是Ethernet、FDDI时，缺省情况下，OSPF认为网络类型是Broadcast。在该类型的网络中，通常以组播形式（OSPF路由器的预留IP组播地址是224.0.0.5；OSPF DR/BDR的预留IP组播地址是224.0.0.6）发送Hello报文、LSU报文和LSAck报文；以单播形式发送DD报文和LSR报文。

同时debugging security-policy packet ip 可以看到有报文被deny，目标地址是组播的224.0.0.5，

Dec 21 10:03:33:164 2023 H3C FILTER/7/PACKET: -COntext=1; The packet is denied. Src-ZOne=Trust, Dst-ZOne=Local;If-In=GigabitEthernet1/0/0(1), If-Out=NULL0(1283); Packet Info:Src-IP=1.1.1.2, Dst-IP=224.0.0.5, VPN-Instance=,Src-Port=0, Dst-Port=0, Protocol=OSPFIGP(89), Application=invalid(0),Terminal=invalid(0), ACL=none, Rule-ID=none

*Dec 21 10:05:43:953 2023 H3C FILTER/7/PACKET: -COntext=1; The packet is denied. Src-ZOne=Local, Dst-ZOne=Trust;If-In=InLoopBack0(1284), If-Out=GigabitEthernet1/0/0(1); Packet Info:Src-IP=1.1.1.1, Dst-IP=224.0.0.5, VPN-Instance=,Src-Port=0, Dst-Port=0, Protocol=OSPFIGP(89), Application=invalid(0),Terminal=invalid(0), ACL=none, Rule-ID=none.

解决方法

除去正常业务需要放通的单播地址，建立OSPF的安全策略主要配置如下：

（# abc地址对象组配置

```
object-group ip address abc
 0 network host address 224.0.0.5
 10 network host address 224.0.0.6
)
```

（# 策略部分：

```
security-policy ip
 rule 1 name a
  action pass
  source-zone local
  source-zone trust
  destination-zone local
  destination-zone trust
  source-ip-host 1.1.1.1
  source-ip-host 1.1.1.2
  destination-ip abc
  service ospf
)
```

```
[H3C-security-policy-ip]dis ospf peer

        OSPF Process 1 with Router ID 192.168.0.1
            Neighbor Brief Information

 Area: 0.0.0.0
```

Router ID	Address	Pri	Dead-Time	State	Interface
1.1.1.2	1.1.1.2	1	36	Full/BDR	GE1/0/0