某局点SecPath F100-C-A3-W(V7)无线用户互访不通的处理经验案例

ASPF 域间策略/安全域 丁佳欣 2020-11-09 发表

组网及说明

不涉及。

问题描述

现场配置F100-C-A3防火墙wlan无线功能后，发现内网用户连接无线后无法互访，收到反馈后我们立即展开分析 。

过程分析

1、 终端无线用户二层无法互访，首先我们检查防火墙安全域及安全策略配置。如下：

```
security-zone name Trust
import interface Vlan-interface1
import interface Ethernet1/0/0 vlan 1
import interface GigabitEthernet1/0/4 vlan 1
import interface GigabitEthernet1/0/5 vlan 1
import interface GigabitEthernet1/0/6 vlan 1
#
security-policy ip
rule 0 name trust-untrust
  action pass
  counting enable
 source-zone Trust
  source-zone Local
  source-zone Untrust
  destination-zone Untrust
  destination-zone Trust
  destination-zone Local
```

已经将无线业务vlan及绑定的接口均加入了安全域并已放通，检查安全域和策略配置暂时未发现问题。

2、 无线终端互访时进行debug，进一步分析无法互访的原因：

（debugging ip packet acl；debugging ip info acl ； debugging aspf packet acl；debugging security-policy packet ip acl)

Debug打印信息如下：

```
*Oct 23 11:46:45:905 2020 H3C ASPF/7/PACKET: The packet was dropped by ASPF for nonexistent zone pair. Src-ZOne=-, Dst-ZOne=-;If-In=WLAN-BSS1/0/2(136), If-Out=WLAN-BSS1/0/2(136), VLAN-In=1, VLAN-Out=1; Packet Info:Src-IP=10.14.16.3, Dst-IP=10.14.16.100, VPN-Instance=none, Src-Port=1, Dst-Port=2048. Protocol=ICMP(1).
```

通过debug信息我们可知无线用户互访的流量由于不存在的域间实例被aspf丢弃了，接口是WLAN-BSS接口。

3、被策略丢弃，那应该如何放通策略呢？于是后续进一步确认到，对于WLAN-BSS接口，它是无线接口，在安全产品上不可见，所以无线用户互访被策略丢弃，目前的解决办法就是将无线用户的地址对象组加入安全域当中做策略放通以实现无线用户的互访。

解决方法

将无线用户互访地址加入安全域并做放通后可以互访。

```
security-zone name Trust
import interface Vlan-interface1
import interface Ethernet1/0/0 vlan 1
import interface GigabitEthernet1/0/4 vlan 1
import interface GigabitEthernet1/0/5 vlan 1
import interface GigabitEthernet1/0/6 vlan 1
import ip 10.14.16.0 24    //增加配置将无线用户互访的地址加入到安全域
```

并且放通同域之间的安全策略后问题得到解决。