

知 某局点F100-C-A3-W WLAN无线用户互访不通经验处理案例

域间策略/安全域 孙轶宁 2024-06-30 发表

问题描述

防火墙配置WLAN无线功能后，发现无线用户互访不通。

过程分析

- 1、查看防火墙会话，发现没有这个无线用户的会话。
- 2、在设备上debug aspf packet，发现报文被丢弃了，报文接口为WLAN-BSS。
- 3、尝试在安全域中添加这个WLAN-BSS接口，发现防火墙上不存在这个接口。
- 4、WLAN-BSS接口是无线接口，在安全产品上是不可见的，所以无线用户互访被策略丢弃，目前只能将无线用户的地址对象组加入安全域（直接在安全域下面写地址段和掩码）。

```
security-zone name Trust
```

```
import ip 10.14.16.0 24
```

解决方法

WLAN-BSS接口是无线接口，在安全产品上是不可见的，所以无线用户互访被策略丢弃，目前只能将无线用户的地址对象组加入安全域（直接在安全域下面写地址段和掩码）。

```
security-zone name Trust
```

```
import ip 10.14.16.0 24
```