

知 某局点comwareV7 FW基于应用的安全策略放通企业微信与钉钉不成功

域间策略/安全域 孔德飞 2022-11-10 发表

组网及说明

组网：

内网终端---核心SW---出口FW----公网

现场需求，现场需要通过基于应用的安全策略，放通企业微信 钉钉 以及腾讯会议

告警信息

不涉及

问题描述

问题现象：现场做过配置之后，发现钉钉拉不了群，腾讯会议打开空白

过程分析

分析过程

通过查看配置，发现现场没有放通基础应用

```
rule 4 name 1
```

```
action pass
```

```
logging enable
```

```
source-zone Trust
```

```
destination-zone Untrust
```

```
source-ip ACG_IP
```

```
application 钉钉
```

```
application 微信
```

```
application 企业微信
```

```
application 向日葵
```

```
application TeamViewer
```

```
application 腾讯会议
```

```
application 阿里邮箱
```

于是在rule4中添加如下应用

```
application http
```

```
application https
```

```
application dns
```

```
application general_tcp
```

```
application general_udp
```

```
application http_other
```

```
application tcp_other
```

```
application udp_other
```

添加之后，企业微信与钉钉都完全正常了，但是腾讯会议拉不了群

经过进一步分析，发现腾讯会议还必须放通“QQ, TimQQ, 腾讯网, 腾讯微云, 腾讯资源”这些资源，现场放通之后，正常

解决方法

需要注意的关键点：

1. 首先基础应用必须放通
2. 放通需要放通的应用，如果还有问题，特征库版本升级到最新，然后再测试，如果还是不行，那就新建一条策略，全放通，看一下是否正常，如果正常，一定是特征本身的问题导致，此时将以上分析过程，以及设备诊断，现场组网，现场现象，完整整理，拨打热线电话即可。

