

某公司升级防火墙后网络不通

问题描述:

某公司拓扑如下。核心为两台100F，与交换机运行ospf发现路由。将100f版本从12xx升级到1625版本后，发现pc无法访问服务器。

解决方案:

经检查，1625版本默认启用了TCP首包检查机制。如果首包没有从防护墙过，那么防火墙的规则是丢弃其他后续报文。而该网络中存在很多来回路径不一致的情况。

需要将首包检查关闭，命令如下：

```
Firewall session aging-time 260 （260为特殊值，关闭首包检查）
```