**电力系统网络安全监测装置常见问题及对策**

余 轲[1]，于艺盛[2]

1. 国网湖南省电力有限公司检修公司，湖南省长沙市 410000；2.国网湖南省电力有限公司检修公司，湖南省长沙市 410000）

摘 要：网络安全给电网带来的挑战日益激烈，网络安全监测装置通过对异常操作和异常状态进行监控，确保电力系统网络安全。本文以东方电子DF1911S网络安全监测装置为例，对调试过程中常出现的问题进行总结并提出来相应的对策，提高网络安全装置的调试效率。

关键词：网络安全监测装置；单电源；对时异常；证书错误

1 前言

随着科技的发展，电力系统的安全稳定运行面临的挑战日渐加剧。近年来，国际上网络安全事件频发，乌克兰大面积停电事件、美国东部互联网服务瘫痪、勒索病毒全球爆发相继发生。电力监控系统作为关键信息基础设施，具有覆盖范围广、系统复杂、实时性强、安全要求高等特点，一直以来都是网络攻击的首选目标①。为加强对电力系统的网络安全监测、保障电网运行的安全稳定②，网络安全监测装置陆续被安装使用。本文以东方电子DF-1911S网络安全监测装置为例，提出调试过程中常见问题及解决方案。

2 网络安全监测装置

网络安全监测装置具备安全分析与告警功能，对运行过程中监视到非法访问、操作时产生的安全事件进行实时监视并形成告警、对运行过程中监视到运行异常进行实时监视并形成告警、对监视对象的硬件状态异常进行实时监视并形成告警，安全监测装置采集及分析得到的告警，上传至网安全管理平台。

3 常见问题及解决方案

东方电子自主研发的DF-1911S网络安全监测装置属于II型网络安全监测装置，主要用于厂站端。在变电站端，主要对防火墙、正向隔离装置、反向隔离装置、交换机、纵向加密装置进行监测。网络安全监测装置在调试的过程中常出现的问题有：单电源运行、对时异常、证书不匹配等。

3.1 单电源运行

网络安全监测装置采用两路电源独立供电，同时支持两路直流电源和两路交流电源，任何一路回路电源中断均不会造成装置故障或重启。虽然一路电源供电可使设备正常运行，但如果该电源出现失电情况，设备将无法进行工作，因此当发生单电源运行情况时，立即处理，防止设备失电而无法工作。

如图1所示，DF-1911S网络安全监测装置正面对于电源有两个指示灯，分别对应电源1和电源2。当两路电源同事正常运行时，指示灯亮绿灯；当两路电源其中一路电源失电时，对应电源指示灯亮红色。出现告警信息后，应对电源模块进行检查，测量对应电源电压是否为正常电压值，如不正常则进行更换。



图1 DF-1911S

3.2 对时异常

服务器与网络安全监测装置主机服务器之间如采用的对时方式不一致，会产生对时异常的告警。电力系统要求各设备具有高度的时间同步性，因此对时系统的可靠运行是电力系统运行的重要保障③。网络安全监测装置有两种对时方式④：NTP对时、GPS对时。两种对时方式相差8小时。

当发生对时异常时，存在两种原因。一种是网络安全监测装置主机服务器超前8小时，一种是网络安全监测装置主机服务器滞后8小时。根据不同的情况，可采用下列两个方法解决：

（1）sudocp/usr/share/zoneinfo/GMT+0/etc/localtime

（2）sudocp/usr/share/zoneinfo/Asia/Hong-Kong/etc/localtime

3.3 证书异常

在配置网络安全监测装置时，需要导入设备证书、主站证书、平台证书。设备证书与主站证书须正确且一致，平台证书与主站证书必须正确且一致的情况下，网络安全监测装置才能正常工作，设备证书与主站证书、平台证书与主站证书任何一个出现错误或不一致都将导致相关业务隧道通讯不正常，网络安全监测装置对于相关业务管理不上。

证书异常可以从报文中查看。当报文的第7位为“91”时，表示设备证书与主站证书不一致；当报文的第7位为“92”时，表示平台证书与主站证书不一致。

表1 报文第7位所示内容

|  |  |
| --- | --- |
| 报文第7位数值 | 证书异常原因 |
| 91 | 设备证书与主站证书不一致 |
| 92 | 平台证书与主站证书不一致 |

根据报文所示内容，检查相对应的证书是否一致，证书类型的选择是否正确。

4 结束语

自动化系统和网络通信迅速发展带动了电力系统自动化程度的迅速提升，与此同时也带来了网络安全等问题。网络安全监测装置通过对运行设备产生的异常操作进行监控，为电力系统安全稳定的运行建立了一道安全防线。本文对东方电子DF1911s网络安全监测装置调试过程中常见的问题进行归纳总结，并提出解决方案，为该型号网络安全设备的调试带来便利。

参考文献：

【1】华敏. [智能电网中网络安全的关键性技术与应用研究](https://kns.cnki.net/kcms/detail/detail.aspx?filename=SDDZ201410023&dbcode=CJFQ&dbname=CJFD2014&v=" \t "https://kns.cnki.net/KCMS/detail/kcmstarget)[J].  信息技术与信息化. 2014(10)

【2】崔颖. [探究网络安全技术于网络安全运维中的应用](https://kns.cnki.net/kcms/detail/detail.aspx?filename=WLAQ201603014&dbcode=CJFQ&dbname=CJFD2016&v=" \t "https://kns.cnki.net/KCMS/detail/kcmstarget)[J].  网络安全技术与应用. 2016(03)

【3】郑华 电力系统内基于NTP协议的对时网络异常情况处理研究[M] 中国电力出版社，2004：211-227．

【4】 张红,王志强,陈前斌,陈伟 [NTP协议及其在电信网络中的应用](https://kns.cnki.net/kcms/detail/detail.aspx?filename=JSJY2004S1010&dbcode=CJFQ&dbname=CJFD2004&v=" \t "https://kns.cnki.net/kcms/detail/frame/kcmstarget)[J]. 计算机应用2004(S1)