

浅谈调度内网二次系统安全监视平台建设

卓 倬

(宿迁供电公司, 江苏 宿迁 223800)

摘 要: 电力二次系统安全防护工作开展以来, 在地区调度和 200kV 及以上变电站部署了大量安全设备和系统, 但是缺乏对相关设备和系统进行集中管控和统计分析, 本文主要阐述了地级调度单位通过调度内网二次系统安全监视平台的建设, 有效的实现内网安全事件的集中收集和统一管理。

关键词: 纵向加密; 防火墙; IDS; 隔离装置

0 前言

随着计算机技术, 通信技术和网络技术的发展, 接入数据网络的电力控制系统越来越多。特别是随着电力改革的推进和电力市场的建立, 要求在调度中心、电厂及用户等之间进行的数据交换也就越来越多、电力二次系统已经成为电网运行控制不可须臾或缺的重要组成部分。然而随之而来的是计算机病毒、木马、黑客等恶意网络攻击的日益猖獗。

2000 年以来, 我国电网运行控制系统发生了多起信息安全事件, 严重影响电力系统安全稳定运行。因此, 2004 年电监会下发《电力二次系统安全防护规定》(第 5 号令), 2006 年电监会下发《电力二次系统安全防护方案》(第 34 号文) 及系列配套的安全防护方案, 制定了“安全分区、网络专用、横向隔离、纵向认证”的总体防护策略。

电力二次系统安全防护工作开展以来, 各级电网调度中心和变电站部署了大量安全设备和系统, 安全防护水平大幅提升, 但是相关设备和系统的运行状况和管理水平不高, 缺乏集中管控和统计分析手段, 系统管理员疲于应对。为此在国调中心的要求和指导下, 电力系统内部积极开展安全监视平台的研究与论证工作。

1 建设目标

电力二次系统安全监控平台通过对部署在横、纵向边界的电力专用和通用安全设备的运行情况和异常访问情况进行实时监视, 提高电力二次系统稳定运行水平, 提升电力二次系统安全防护体系的管控能力

1.1 总体目标

电力二次系统安全监控平台实施目标主要是实现内网安全事件的集中收集、统一管理。通过全方位的实时告警, 及时发现二次系统存在的异常和漏洞, 有利于故障的及时处理; 采集、存储大量翔实的运行数据, 实现安全设备运行状态检测, 为二次设备分析和资产管理提供精确的数据依据; 集成加密认证装置远程管理服务, 通管理报文以在线方式实现对纵向加密认证装置的实时监测和管理; 全方位保护关键业务, 为安全检查、安全评估提供方便的工具和手段。

1.2 监视范围

内网二次系统安全平台主要监视的设备包括省、地、县调、220kV 以上变电站部署的二次系统防护设备。主要包括纵向加密装置、防火墙设备、单比特正、反向隔离装置、漏洞扫描系统、入侵检测系统、防病毒系统等。

内网二次系统安全平台建设范围涉及省调、地调、县调及厂站的生产 I/II 区纵向边界防护; 涉及生产大区与信息大区区的横向互联防护, 以及各安全区内部的防护。如图 1 所示。

内网二次系统安全平台主要监视的设备主要分为电力专用安全设备和电力通用安全设备:

电力专用安全设备包括: 纵向认证加密装置、横向隔离装置。生产控制大区与广域网的纵向连接处的纵向加密认证装置主要关注隧道建立情况以及设备通信是否遵循已定义的安全策略情况。隔离装置主要关注策略的设置情况。

电力通用安全设备: 包括防火墙、防病毒和入侵检测系统。防火墙重点专注安全策略访问情况、防病毒主要监控病毒感染情况和入侵保护的入侵事件情况。

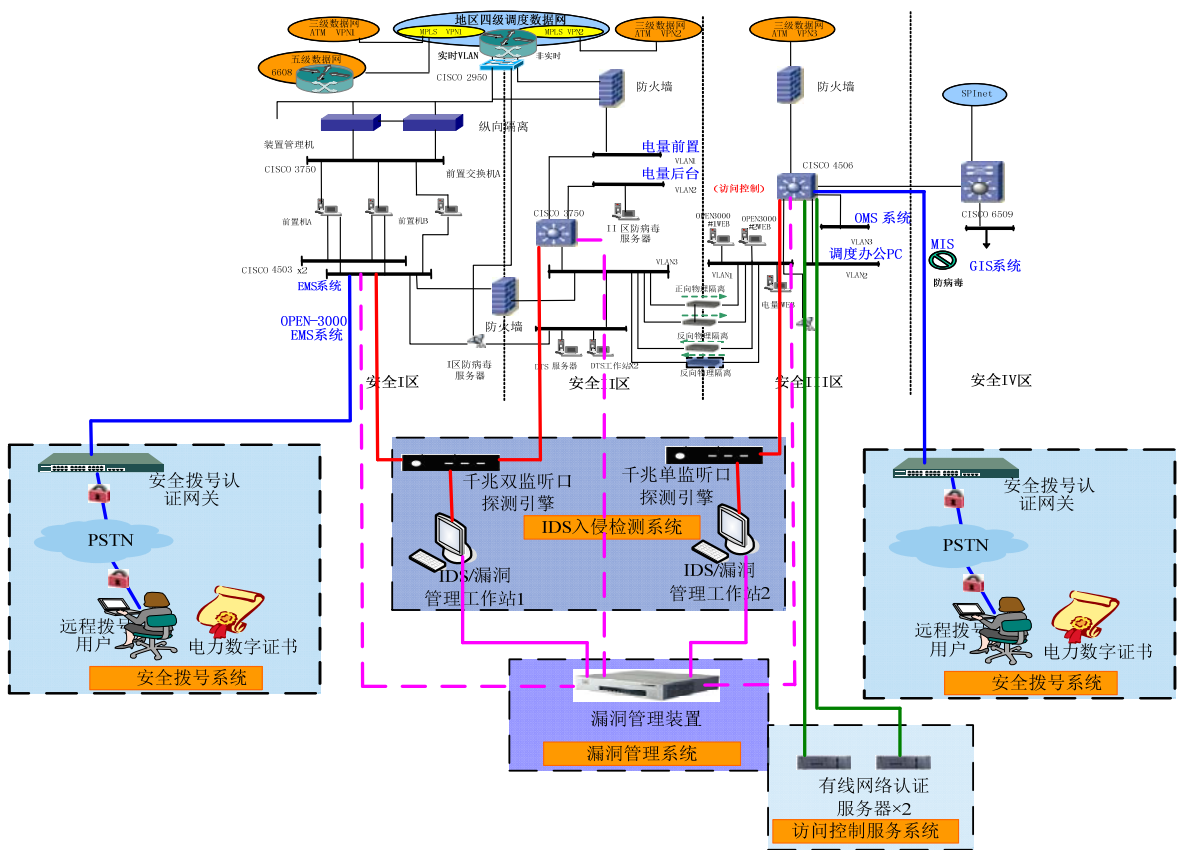


图 1 地级调度二次安全防护图

从图 2 可以看出目前的监控目标主要还局限于安全设备，以后可以把主机、网络、数据库、中间件和业务系统监控起来，并在基础数据监控的基础上做根源分析和影响分析。

目前实施的二次安全监视平台项目主要侧重调度主站端的二次安全防护设备（包括纵向加密、防火墙、IDS、防病毒服务器和隔离装置）和所辖区域 220kV 变电站（纵向加密和防火墙）的监视功能。

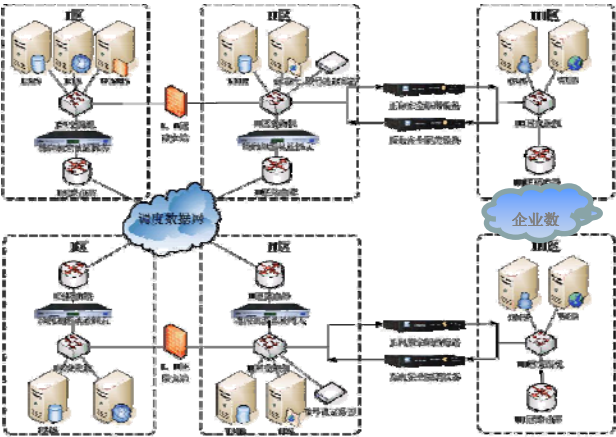


图 2 平台监控范围

2 平台架构及关键技术

2.1 平台架构

按照“统一部署、分级管理”要求，监视平台主要是实现上、下级调度中心安全监视平台的级联通信。根据策略制定原则，下级中心主动报送上级监视平台告警信息。如图 3 所示。

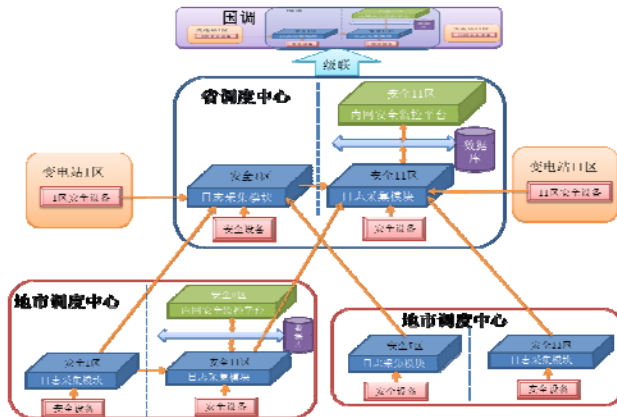


图 3 平台结构

2.2 日志规范

目前地区调度使用的二次系统安全防护设备种

类多样, 主要的类型如表 1 所示。

表 1 二次系统安全防护主要设备类型

安全设备类别	厂商	型号
地调加密认证装置	南瑞	千兆
地调防火墙	东软	NetEye
	天融信	NGFW
地调横向隔离装置	南瑞	Syskeeper
地调防病毒系统	瑞星	IBM
		DELLPowerEdge
地调入侵检测系统	Neusoft	NetEye IDS
220kV 变电站纵向加密认证装置	南瑞	NETKEEPER
220kV 变电站防火墙	东软	neteve

依照国家电力调度通信中心颁布的电力二次系统安全监控日志规范，各厂家安全设备必须遵照电力行业专用标准来实现上传二次监视平台的日志类型。

2.3 日志格式

为了规范各厂家设备上传的日志内容，规定了安全监控日志格式的定义：

<告警级别><空格>告警时间<空格>设备名称<空格>设备类型<空格>内容描述

告警级别：紧急、重要、次要、通告。

告警时间: 格式为 YYYY-MM-DD HH:MM:SS, 其中 YYYY 表示年份, MM 为月份, DD 是日期。MM 为月份, DD 是日期。24 小时制, 有效值为 (00-23), MM 和 SS 的值的范围为(00-59)。月、日、时、分、秒各 2 个字符, 小于 10 时十位应补 0。

设备名称：标识产生告警事件的主机名字或者是主机 IP 地址。

设备类型：主要设备类型如表 2 所示。

表 2 主要设备类型

FW	防火墙
IDS/IPS	入侵检测/保护系统
FID	横向正向隔离装置
BID	横向反向隔离装置
VEAD	纵向加密认证装置
SVR	服务器
AV	防病毒系统
SDIAL	安全拨号服务器
MP	安全监视平台

内容描述：主要格式为<日志类型><空格><日志子类型><空格><内容>。

3 平台构建

3.1 硬件准备

安装两台采集服务器，并接入机房 KVM 系统（如果没有的话需要安装两台显示器和两套键盘和鼠标），并准备多条网线。考虑到走线的方便，设备选择安装在二次安防设备的机柜内。

3.2 网络结构

采集服务器配置了两块网卡，分别连接内网的前置网段和主网端，实现对所有设备的监控。总体网络结构如图4所示，确定采集机所连接的网络能与二次安防设备通信（包括与省调通信的路径以及IDS、防病毒、防火墙和隔离装置的连接情况）

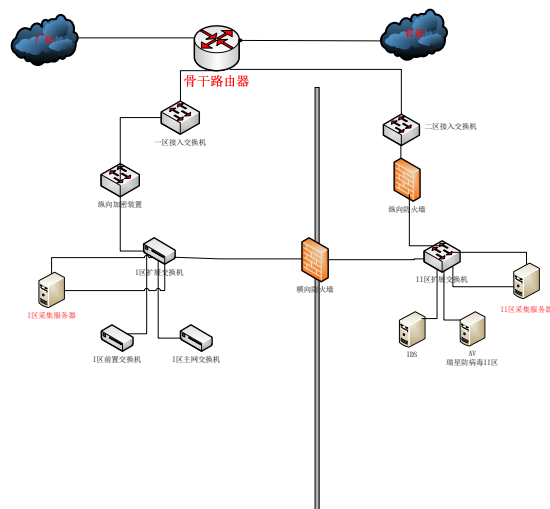


图 4 网络结构

3.3 硬件配置

配置地调端纵向加密装置，在与省公司的隧道上配置相应的策略。

配置地调端防火墙,配置相应的地址转换策略。

配置一二区采集机的网卡，配置完成并重启网卡服务后不仅要能从地调能 ping 通省调的相应 IP 地址，还要使从省调能 ping 通地调的相应 IP 地址，如果有一方不通，还需要与地调人员联系。

在省地两边都能 ping 通对方后，需要维护人员在路由器、防火墙开通部分网络端口。

4 平台使用

4.1 平台界面

平台的维护界面使用 web 浏览，登陆到系统主界面如图 5 所示。

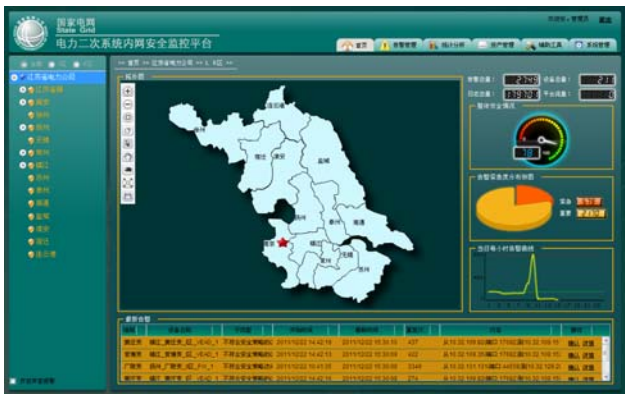


图 5 平台主界面

4.2 运维模块

对于地调运维人员来说手工维护的主要有资产管理模块、告警模块和相关的配置模块。当地调接入新变电站后，需配置变电站节点信息，并在资产管理页面进行添加资产操作，完成添加后可以在资产管理模块中查看 CPU、内存、告警、流量曲线等来验证设备已经成功接入系统。如图 6 所示。



图 6 设备基础信息界面

- a) 查看 CPU、内存列的数据，如果有数据，说明接通了，设备能接受到 cpu，内存数据了，没有 cpu，内存的话，可以点击详情按钮，进入详情界面。如图 7 所示。
- b) 这里有告警量，如果有告警量的话，说明设备接入成功了。如图 8 所示。
- c) 没有告警的话，可以看看流量，如果有流量折线图也说明接通了。如图 9 所示。
- d) 没有流量，就只有看 cpu，内存曲线了有显

示曲线也说明接通了。

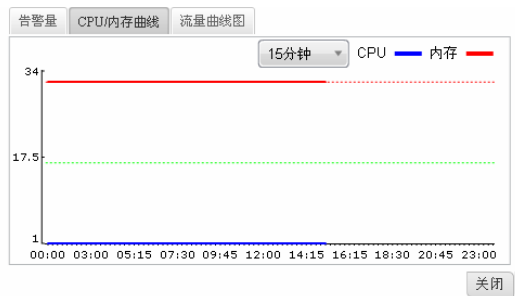


图 7 内存曲线界面



图 8 告警量主界面

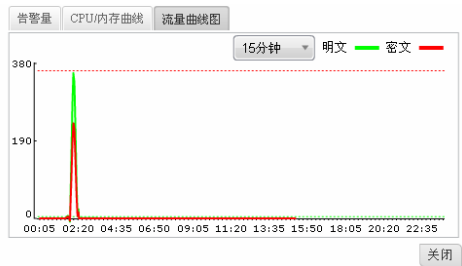


图 9 流量曲线图

5 结束语

内网安全监视平台的实施，规范了防护体系的建设，实现了防护效果的统一性，对电力系统的二次安全防护工作具有重要意义，提升了电力二次系统安全防护体系的管控能力。

参考文献：

[1] 张惠刚.变电站综合自动化原理与系统[M].北京:中国电力出版社,2004.
[2] 张永健.电网监控与调度自动化[M].北京:中国电力出版社,2004.

作者简介：

卓 倬 (1984-), 女, 江苏宿迁人, 助理工程师, 主要从事自动化系统运维工作。