某省烟草信息系统统一安全监控平台案例介绍

SOC 事业部

网御神州科技有限公司

1. 建设背景和用户需求

随着烟草行业计算机信息网络建设的不断发展、各类应用的不断深入，烟草行业的经营模式已经由传统模式逐渐向网络经济的模式转变。网络的开放性、互连性和共享性，以及随着网络上电子商务、网络电子银行等新业务的兴起，使得网络安全问题变得越来越重要。

某省烟草局（公司）信息系统上接国家局（公司）、下联各市县局（公司），实现互联互通，进行信息共享。该局（公司）网络整体结构是一个通过 DDN 连接的多级网络，并建有 Internet 出口，在网络每一级的节点上各有一个局域网，在多级网络上运行着综合业务系统、专卖系统、办公系统等，网络结构和应用系统十分复杂。网络内包含上百台应用服务器、众多的网络设备（包括路由器、交换机等）、安全设备（防火墙、IDS 等），以及多种不同的操作系统（主要有 Windows、AIX 等）。省局的网络不仅要保证与国家局、市县局的畅通，还要为客户提供快速、便捷的网络服务，网络管理人员的压力越来越大。目前，该局（公司）主要有以下问题：

1) 无法了解省局网络信息系统的整体运行状况
2) 网络出现故障后，不能及时诊断，影响业务进行

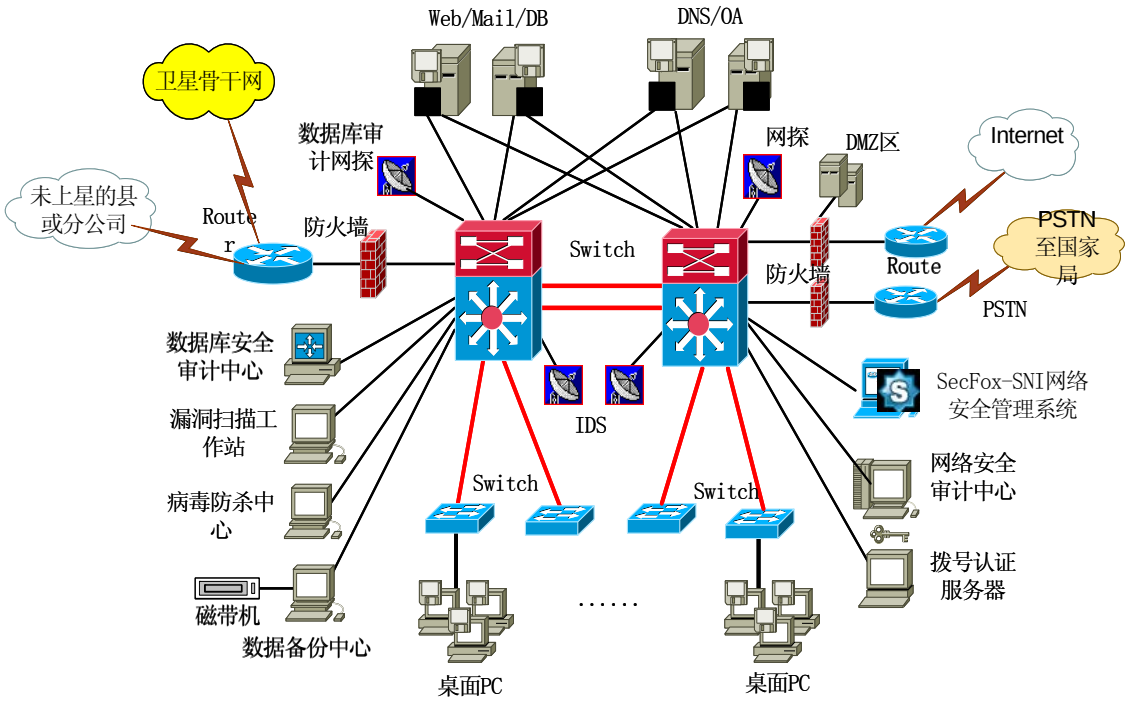
为了应对上述挑战，该局（公司）急需建立一个信息系统的统一监控平台，实现对全网安全和运行状态的整体态势把控。

2. 网御神州解决方案

针对用户的现状及需求，网御神州结合自己的产品，为用户提出了网络统一安全监控的解决方案：通过在网络中部署 SecFox 安全管理系统，对全网的网络设备、安全设备、主机、应用系统、中间件和数据库等的可用性指标进行监控，收集各种基础数据，全面的了解企业网络的运行状况，根据获取的监控参数和预定义的告警阈值决定是否告警和执行响应。

SecFox 安全管理系统采用集中、非代理式的监控方式，模拟系统管理员操作的方式采集数据，这样就无需在被监控对象上安装任何代理软件，实施和维护都非常简便。对不同的监控对象设置不同的监控频率，以进一步降低监控系统对网络正常运行的影响。系统能够对监控对象进行分组，同时提供网络拓扑图和分类拓扑，方便网络管理员更直观地了解网络设备的运行状况。系统采用基于角色的权限管理机制，通过设置适当的管理权限，使得多名管理员各司其职、共同完成管理工作。

网御神州 SecFox 安全管理系统部署简单，只需要选择一台合适的服务器，确保被监控网络 IP 可达，一次性将软件系统安装好即可使用。系统实施无需修改现有的网络拓扑环境，无需另外安装数据库或者 WEB 服务器等附加系统，无需在被监控设备上安装代理或者探针。



SecFox 安全管理系统部署示意图

3. 应用效果

目前项目已经实施完毕，并成功上线。该局（公司）使用网神 SecFox 安全管理系统有效实现了对业务系统的全面监控。监控对象和内容概述如下：

设备类型	监控对象	数量（台）	监控内容简述
交换机	Cisco 6509	32	监控 CPU/内存利用率、接口流量等，确保设备正常运行、监控异常流量
	华为 6506		
路由器	Cisco 7200	28	监控设备接口信息、IP 地址和接口流量信息。确保设备正常运行、监控异常流量
	Cisco 3745		
	Cisco 2811		
	Cisco2611		
防火墙	东软	32	监控防火墙的设备属性和参数、运行状态、网络接口流量。确保设备正常运行、监控异常流量
IDS	东软	15	监控 IDS 的基本运行参数。确保设备正常运行
主机	IBM AIX	62	监控 CPU 使用情况、内存使用情况、进程状况(消耗 cpu 资源 top10、指定的进程)、磁盘使用情况、网络状况、文件系统空间使用情况、系统错误日

			志（是否有 Errpt 输出），等等。确保系统本身及其上面运行的业务正常运行
	MS Windows 各型操作系统	54	监控 CPU 利用率、内存利用率、进程状况(消耗 cpu 资源 top10、指定的进程)、网络状况、磁盘利用率，等等。确保系统本身及其上面运行的业务正常运行
数据库	IBM DB2	60	监控数据库请求的连接时间、连接情况、代理情况、事务情况、排序情况、分配表空间大小、空闲表空间大小、表空间空闲比例、缓冲区统计、死锁数，等等。确保系统本身及其上面运行的业务正常运行
中间件	IBM WebSphere	60	监控中间件系统的 JVM、Serverlet、线程池、EJB、JDBC 等的状态和运行参数。确保系统本身及其上面运行的业务正常运行

安全监控平台上线后，各级管理员在一个界面就可以了解全网各类设备的运行状况，并可以在设备发生故障前进行预警，一旦发生故障，迅速定位，极大地提高了管理员的网络监控预警能力和事故响应处理速度。系统支持多种方式的报警，从短信、邮件到电话响铃。系统还能够实现与网络及安全设备进行联动，对于显著的安全问题直接进行阻断和策略变更。

目前，系统运行一切良好。在网神 SecFox 安全管理系统的协助下，极大地提高了该局（公司）管理人员日常工作的自动化程度和运维保障水平，保证了全网业务的连续性，也再次印证了网御神州在安全管理领域的强大实力。

关于网御神州

网御神州科技（北京）有限公司（www.legendsec.com）是集技术研发、平台管理、综合服务于一体的高科技信息安全方案、产品及服务提供商。 公司成立以来，以满足客户需求为中心，以自主研发为重心，不懈努力、积极进取，取得了丰硕的技术成果以及傲人的市场份额。据赛迪顾问 2007-2008 年中国信息安全产品市场研究年度报告显示，网御神州已跃居国内防火墙市场第二、SOC 市场第一，以最快的成长速度成为国内信息安全产业的中坚力量。

欲获取更多信息，请即联系网御神州科技（北京）有限公司

全国统一热线服务电话：010-87002000（7×24 小时）

E-mail：service@legendsec.com（5×8 小时）

网站地址：www.legendsec.com

网神安全管理博客地址：http://blog.sina.com.cn/legendsec

传真：010-62972896

通信地址：北京市海淀区上地信息产业基地开拓路 7 号先锋大厦 2 段 1 号

邮政编码：100085