



ESET NOD32 电力行业网络安全解决方案

高速动车组、地铁、路灯照明，小至居家电视机、冰箱、微波炉、手机，各类出行交通办公家电的正常运转都离不开“电”。庞大的电力输送高低压线路组成了电网。“电”就是在各省的电网中通过统一调配输送至千家万户的使用目的地。

国家电网中心作为重要的电力调度和管理机构，拥有先进的调度系统、通信系统和计算机系统，整个核心网络稳定运行，都需要计算机网络协同工作，网络安全防护不容忽视。

内外网隔离的电网调度覆盖多个地区、多个节点的网络，高性能办公电脑少则一两百数量，多则上千，不同部门的任务涉及发电、输电、配电、用电等环节。计算机网络管理员每天对于操作系统的故障整修、恢复、迁移、升级、补丁成了必修课，更重要的还有无法防备预料的计算机病毒入侵、爆发、资料保密。

电力行业计算机防安全防护涉及多方面：

- 1、 资料保密性：国家电力运作信息、千家万户的家庭资料属于高度机密。
- 2、 外源文件可靠性：电子公文、电子邮件、网络传真、便携笔记本。
- 3、 备份文件安全性：备份、共享的资料一旦感染病毒，所有访问者都将面临病毒威胁。
- 4、 集中管理统一性：终端操作系统安全漏洞检测、防病毒软件部署。

可见电网的“网”可以理解为两个网，一个是配电网，一个就是传递信息的互联网。仅传递信息的网就是庞大复杂且开放的网络体系，IT 管理人员必需第一时间知道工作站终端的运行情况，能够进行即时知悉、实时监控、统一部署、重点汇报的主动式管理。

XX 县电网中心现状：



这几年中不断加入新的工作终端，操作系统从 Windows98、2000，一直发展到了 XP、Vista、Win7。每天都需要通过访问共享的文件服务器、邮件服务器开展工作，所有检修监控和录入的数据都要在内部服务器做备份。公文、电邮、传真、即时通讯每一类数据都需要访问互联网。所有的威胁不单单从外部互联网入侵，局域网还面临着便携笔记本、智能手机、各类 USB 移动设备的内部渗透。所以电力行业在防护互联网的同时，还需有效防控内部系统。

病毒如何潜入？

悄悄地从互联网进来：

电子邮件：垃圾邮件、附件有宏病毒。

网络传真：文件被嵌入蠕虫漏洞病毒，如 PDF 阅读软件的漏洞。

即时通讯：钓鱼网址、虚假中奖链接

智能手机：垃圾短信、手机病毒

明目张胆打入内部：

移动磁盘：客户私密信息被复制走、蠕虫木马传播介质

共享公文：变种病毒、宏病毒、

便携笔记本：没有安装或升级防病毒软件、已经感染有病毒、随意接入局域网

系统漏洞：各种操作系统没有修复漏洞补丁，防病毒软件没有升级

县级单一电网防护方案：

对于地级市县一类小地方单一独立的电力网，可以在工作终端部署 ESET NOD32 防病毒软件，在共享文件、邮件服务器的 Windows/Linux 平台部署 ESET NOD32 服务器产品进行统一过滤防护。

ESET NOD32 的实时防护，对收取、下载到工作终端的文档、网络协议、网页内容进行监控，不论是浏览、运行、压缩、传送，都将在通过监控扫描确认安全后才能进行。

基于当今最高端的贝叶斯邮件过滤技术，部署在电力行业的邮件服务器中。所有收发的电邮信息，包括内容、地址、行为频率、附件过滤扫描后，工作站终端才能阅读。电网员工发送的邮件不仅要先通过本机 ESET NOD32 的安全扫描，还要由邮件服务器的 ESET NOD32 邮件防护引擎二次过滤确保万无一失后才能发送给省市级电网中心、用电客户。

开启 ESET NOD32 的可移动磁盘阻拦功能，无需借助第三方管理设备即可实现对 U 盘、移动硬盘、MP3 的拦截，任何读写操作都无法进行。但不会影响键盘、银行 U 盾、加密狗等系统应用层业务的 USB 设备插入工作。

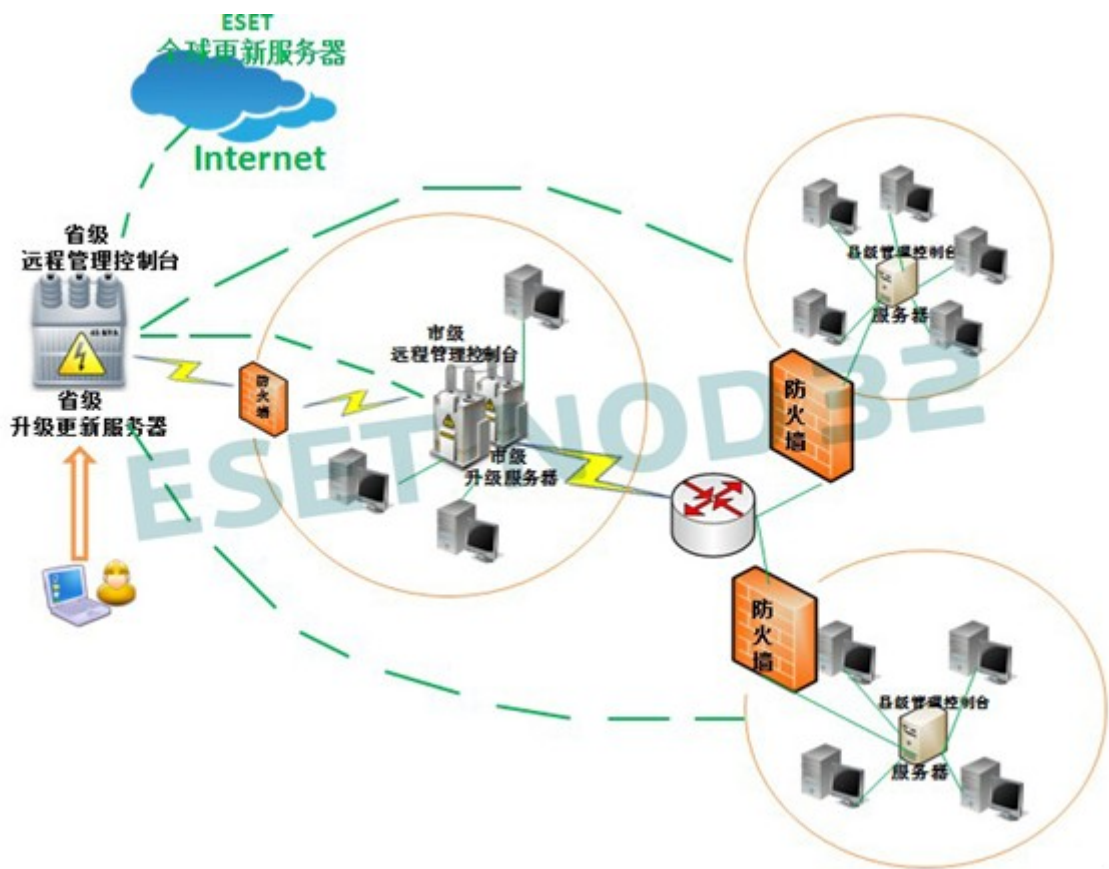


IT 管理员在服务器的远程管理控制台可监控本县电网工作终端防病毒软件防护状态、配置各项功能、统一升级病毒库，在电网调度工作的低峰时段定时启动磁盘扫描，丝毫不影响网络流量，或是低配置电脑的正常工作的。

超高压电网的工作，以一县或一市的能力根本无法开展，最小范围都是**省级网络、市级网络、县级网络**的三级级联架构组成。那么省级可以利用网络对市级、县级电网进行统一的防病毒产品部署、策略管理，状态监控。

庞大规模下的电网维护工作，每天派出的电力检修人员都是成百上千名。市县各地业务每天录入的数据集中管理面临的巨大威胁仍然是安全性。数据来源一旦出现纰漏，在任何一台服务器被共享后，受到威胁的不仅是一个县或市的办公网络，所有市级、县级网络，甚至全省电网的设备都将被蔓延的蠕虫、木马等病毒危害。

这类广域网环境必须进行一体化管理，实现省级电网 IT 管理员在自己办公桌前远程统一管理市县成百上千的服务器、工作终端。



省级电网：如果已经有 SQL、Oracle 一类的数据库，那么只需要部署 ESET NOD32 的远程管理控制台。这一控制台能够管辖不限数量市、县各类服务器、客户端的防病毒软件工作状态、系统漏洞、病毒库升级、防火墙设置、电邮过滤等。

ESET NOD32 提供的 MS Exchange 邮件服务器，Linux 文件、邮件服务器，VMWARE 虚拟化技术的全线防护功能调配都能集成在这个控制台完成。

每小时一次的病毒库升级检测，体积在 100K 左右，对网络流量几乎能忽略不计。



市级电网：通过部署一套二级远程管理控制台，实现对县级电网工作终端的管理，或是提供病毒库镜像升级服务。并且纳入到省级电网一级控制台的管理中。

县级工作终端：只需在内部共享服务器中下载 ESET NOD32 安装包双击鼠标就能自动配置完成安装。任何功能配置都可由本地网络管理员或市级管理员通过策略配置完成。也就是电网员工不需要培训学习如何使用防病毒软件，一切高效防护都是在静默运行中。

工作终端的病毒库升级无需连接到外部互联网，可以到市级电网的二级控制台服务器升级，也可以到省级电网的一级控制台服务器升级。每次升级体积在 100K 左右，不会造成网络堵塞。

ESET NOD32 对 Windows 全系操作系统提供支持 Windows98、XP、2000、2003、Vista、Win7。智能手机、MAC 苹果操作系统同时提供系列防护产品。

国家电网触角伸及全国各地，也就形成了不同网络组成的一个广域网，在安全防护上不能仅停留在空洞的流程和概念上， ESET NOD32 的五大管理策略就能融合在呼叫中心企业现有的网络基础中进行远程中央管理。

一、策略管理

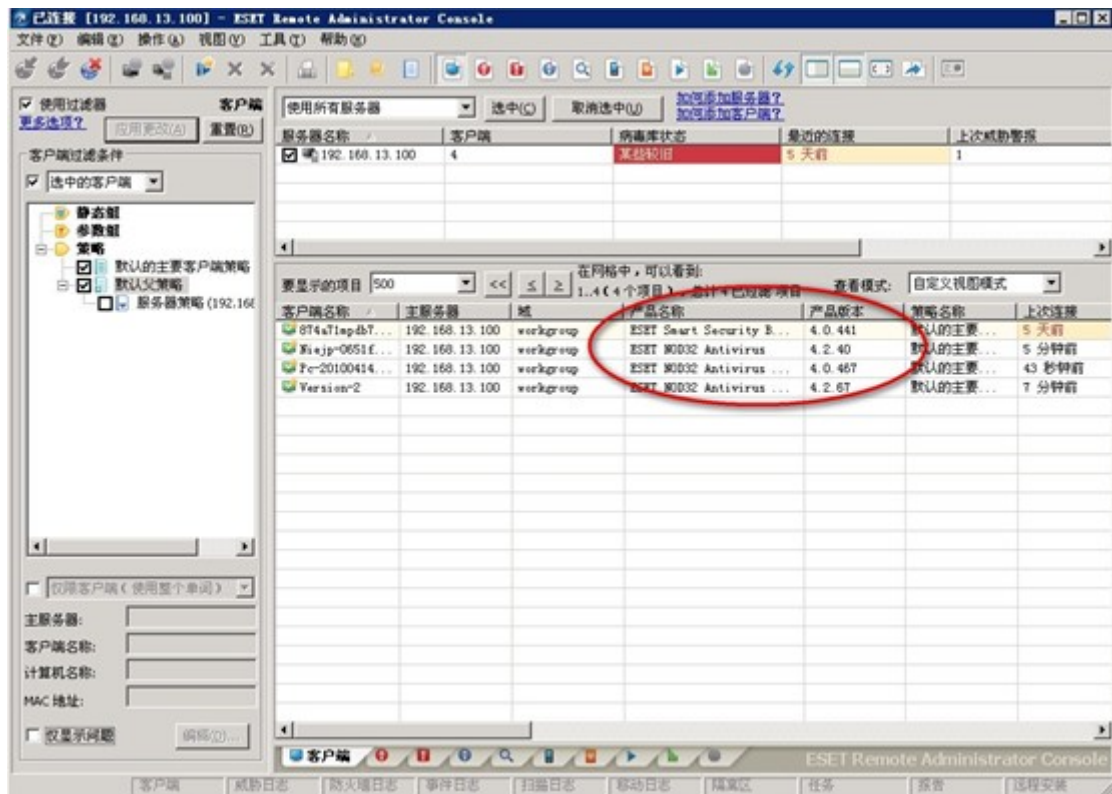
网络准入控制

电力电网行业在淘汰旧电脑的同时，也会增加新的电脑，或是业务人员进进出出带的便携笔记本。在配置了 ESET NOD32 NAC 网络准入控制基础上，网络交换机将会检测接入局域网的电脑有没有安装 ESET NOD32 防病毒产品。如果没有安装将执行拒绝访问策略，拒绝此计算机接入工作网络，实现电力网络任一端点不合格终端设备的排斥，杜绝外来威胁。

强制策略配置

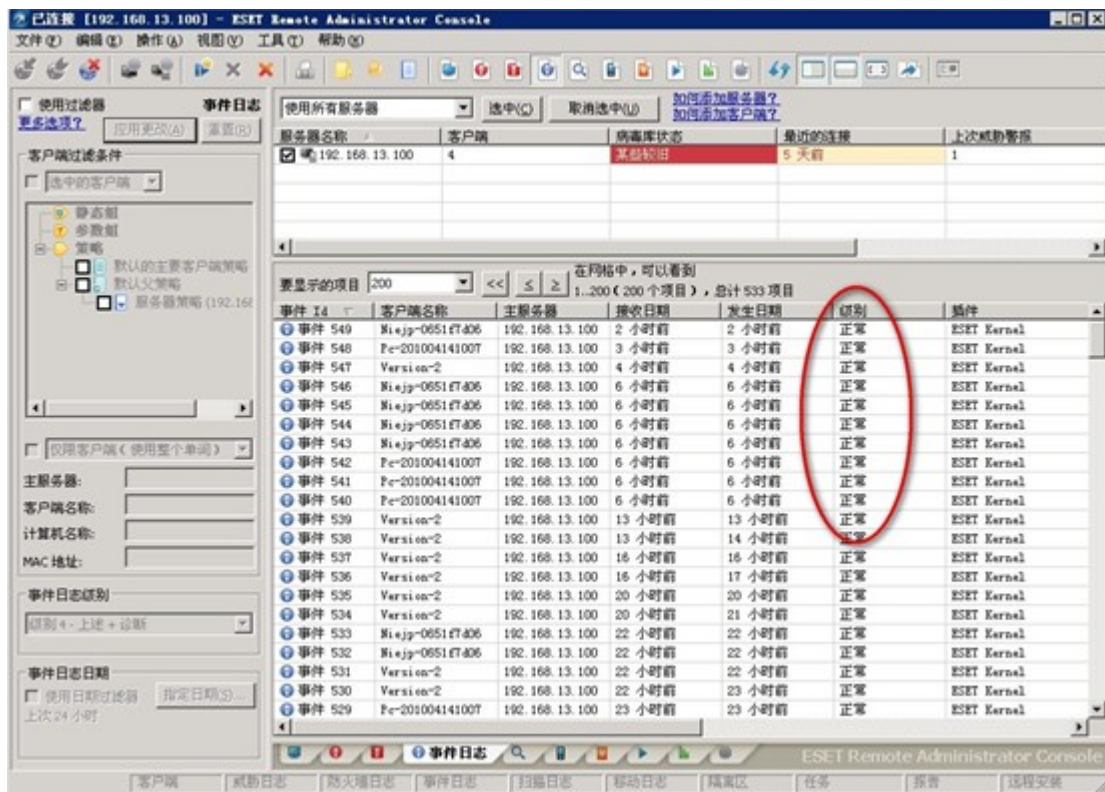
凡是进入内部工作局域网的计算机，检测到安装了 ESET NOD32 后，将会被强行变更所属网段的防病毒功能配置。如市级 A 的员工出差到了市级 B，B 的防病毒配置是根据当地情况而设置的，所以 A 员工的 ESET NOD32 就会被自动修改为 B 的设置。当出差员工回到市级 A 后，ESET NOD32 匹配网络防护策略后会再次自动修改回 A 地的防护设置。

这个省级电网的所有电脑操作系统都使用了备份还原技术，也就是俗称的一键还原。这是不影响工作效率下解决系统故障最快速的方法。但还原的系统最常见问题是：大量系统漏洞、防病毒软件没升级。这两年危害最大的 ARP 病毒、Configur 变种蠕虫就是利用系统漏洞扩散感染。在 ESET NOD32 的组策略环境下，这些现象的修复都会被强制要求执行，无需二次手工操作。



二、实时监控

某一工作终端在规定时间内没有及时升级病毒库，或是防护功能异常，都会在远程管理控制台实时呈现。对不同分公司的服务器可以通过分类、分组、分部门查阅，有病毒威胁的、系统有隐藏漏洞的客户端等等，都能在远程管理控制台一眼尽收。



三、集中管理

市级、县级电网的服务器监控情况，通过级联架构的通信方式实时反馈到省级电网的一级远程管理控制台。中央 IT 管理员可以自定义不同市级县级的防护策略。对可疑文件统一收集分析提交。经常出差外勤检修的移动笔记本用户，设置成复合认证更新，在工作网络之外也能连接入 ESET 全球服务器升级病毒库、模块。即使离线环境下无法升级病毒库，高级启发式的 ESET ThreatSense 引擎也可对计算机提供全方位防护。

集中部署市级、县级电网的网段策略，如限制某个源 IP 段访问某个目的 IP 的黑名单策略，或是只允许某个源 IP 段访问某个目的 IP 段的白名单策略。

四、任务管理

在 7 x 24 小时的输电配电监控工作制下，网络管理员无法预测每一地级市县成千上万的工作终端什么时候才打开电脑工作，防病毒软件的各项功能也就不可能逐一检查部署。这就需要具备主动式分发任务功能。



全网扫描计划、漏洞检测、防火墙等所有防护功能的开启或定制，ESET NOD32 通过主动式任务下发或事件触发机制自动执行，随时能查看各项任务的执行进度。一个工作终端可能在当前是下班关机状态，那么管理员下发的任务将在它下一次开机后主动接收并执行。依据各网段客服高低峰电话时段设置定时执行，实现最优化配置。

电网的工作由于会接触到重要机密的内部信息文件，可采用 ESET NOD32 的 USB 移动设备阻拦功能实现。在操作系统的软件层使用强制手段消除工作终端的信息泄漏隐患。

五、报表管理

省市县每一级地区面临的威胁都不同，如何提取扩散最广的病毒类型进行统计分析制定解决方案很重要。不同威胁、不同网段的报表可以由控制台生成 HTML、CSV 等多图表形式。并且周期性自动生成并邮件发送。

基于以上 ESET NOD32 的统一管理策略，整个电力广域网工作环境下的电脑将纳入形成高度受控终端的“主动式终端安全”体系范围内。自定义的各项不同策略，以自动执行方式协同静默工作，每一策略项目都可实时查阅、下载、复制、分发。

电力行业是国家的重点基础行业，关系国计民生，电力网络的计算机系统安全，需要完成对电力内部网、文件服务器、邮件服务器、计费服务器、数据库系统、配电系统的安全管理。电力的复杂性已经是一个大型的数据采集、中转、通信中心，对各类设备的安全功能、性能都要环环相扣设置，并进行实时、预警监控。