电力系统实时监控网络安全解决方案讨论

张小卫

贵阳市南供电局　联系电话 0851-5898603 邮编: 550002

A discussion of the security solution for the SCADA systems in the power grid.

Xiaowei zhang
Guiyang South Power Supply Bureau

Abstracts: This essay describes the present status of the construction of SCADA systems in power industry, and analyzes the information security issues in this field. A set of feasible solution measures are proposed according to a practical instance. This essay also introduces the project of building a information security system for the SCADA system in Guiyang South Power Supply Bureau.

Keywords: SCADA System, information security

摘要：　本文通过分析近年来电力系统的实时监控系统的建设现状及由此而产生的系统网络安全问题,针对性的提出了一套可行的解决方案.并引用了贵阳市南供电局实时监控系统网络安全建设的方案为例子.

主题词：实时监控系统，网络安全

一：网络安全概述

近年来，电力企业生产和管理的信息化日新月异，包括计算机在内的各种数据采集终端、通信设备互联形成覆盖企业各个层次各个管理环节的综合性企业信息网络。从实际出发，计算机网络的规划设计中应当充分把握网络拓扑的可扩展性和相对稳定性，以及开放性和安全性因素之间协调关系。

从广义上说，网络安全性威胁包括了非法的外部网络攻击和侵入，以及各种病毒对系统和文件的感染。因此，对网络安全性的设计，应当根据网络的用途，结构及网络对安全性的要求来选取合适的网络安全设备和网络安全策略，选取合适的网络防病毒产品和策略。

一般，电力企业信息化包括了基础计算机网络建设，以及基于网络的各种信息管理和自动化应用系统建设。网络安全性主要就是对基础网络和应用提供安全性防护。在电力企业安全性策略设计中主要应基于以下原则：

（1）在系统安全性和开放性之间达到符合实际的折衷。既要保证各子网之间、外网和内网之间的合法访问和信息交换，又要保证内部系统和数据资源的安全；

（2）系统安全性的设计和实施，应保持现有网络拓扑结构的相对稳定，保护系统已有投资；

（3）满足电力企业生产系统高可靠性要求，具备系统容错和可靠性保障措施；

（4）在提供安全性和防病毒的同时，不应降低系统效率，满足电力生产自动化控制的实时性处理要求；

（5）满足系统各层次各环节的全生命周期的安全性需求，建立电力企业综合性立体的安全防御体系；

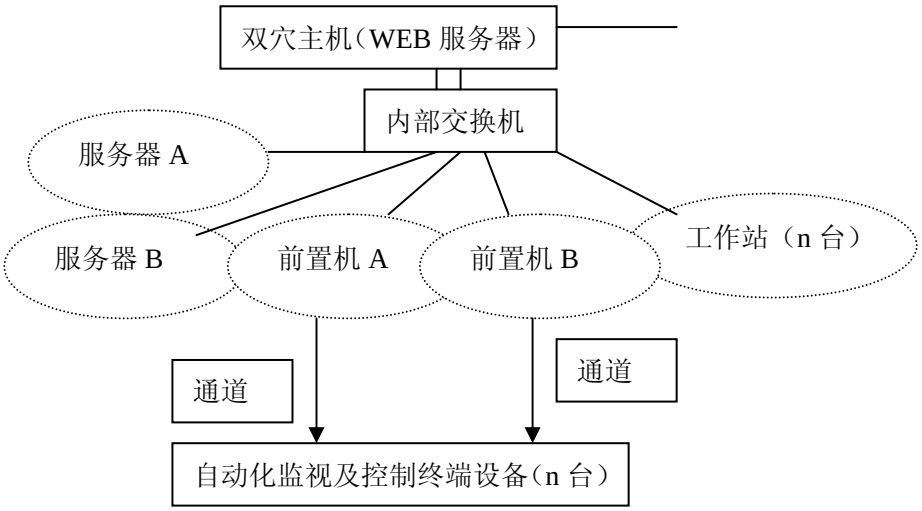
二、实时监控系统网络拓扑及安全建设现状（建设必要性）

目前，电力系统实时监控系统包括了变电站综合自动化系统、配网自动化系统、电能量管理系统、负荷监控系统、集控系统、调度自动化系统等分系统。

由于以上系统均属于与电力生产和用电密切相关的重要系统，实时性、安全性和可靠性要求高。一旦由于系统安全防范措施不足，而发生外部恶意侵入和攻击，或者外部无意识侵入情况下的误操作，或者病毒侵入发作，进而引起系统故障或事故，将造成系统或数据不可挽回的损失。四川二滩等地已经发生类似事件。并且，经过国家网络安全监测部门统计，网络受到威胁中来自于外部网络的占 60%，来自于内部网络的占 40%，而且几乎所有网络都受到过病毒的侵袭。因此，在电力实时监控环节建立相对独立的网络安全控制和管理机制，与全网之间形成局部隔离以保证上述系统安全性是十分必要的。这也是我国电力企业信息化现阶段的重要发展

趋势。上海、东北、重庆、河北等地电力企业已经针对该问题进行了深入研究和规划，并建立了较为严密的网络安全体系。

一般,电力系统实时监控系统的局域网作为子网经过多级交换直接接入 MIS 网络。实时监控系统与 MIS 系统存在数据共享和交换，而实时监控系统的各功能子系统独立交换，内部独立编址。应用中主要操作系统包括 Windows 系列操作系统和 Unix 操作系统,主要通信协议包括 TCP/IP 协议、NETBEUI 协议和各种工业现场通信协议。目前典型的实时监控系统网络拓扑结构如下：



三．实施方案概述：

通过以上的网络拓扑图我们发现，各自动化控制系统目前在安全性上存在很大的隐患。

目前，各单位办公网络对外部广域网的安全机制一般已初步完成;随着内部公共网的建设和发展，局公共网对实时监控系统的安全已经形成了威胁，并且威胁在增大。如：公共网中的病毒感染实时监控系统的频率在增加；所谓的“hacker”对实时监控系统的”探访“等。

目前，仅仅依赖系统软件本身所提供的安全性手段和内网整体安全防范手段，而未采取防火墙技术，不足以防止来自于其它子网或外部网络的安全性威胁或病毒传播威胁，远远不能满足实时系统建设长期可靠安全发展的要求。

因此，我们认为应在各实时监控系统子网与内部公共网之间建立必要的网络安全保证机制，并在安全性的基础上来实现各系统之间与局公共网之间的数据共享和交换势在必行。

在具体实施中，可以采用防火墙、入侵监测系统 IDS 和网络防病毒工具，针对网络安全性漏洞分析和预防、非法入侵监测、入侵过滤和隔离、入侵处理和病毒查杀等安全性管理环节，建立覆盖安全性威胁和病毒的预防、监控、隔离、处理、记录等全生命周期阶段的综合性立体安全防御体系。

四、实时监控系统安全性措施建议

1． 防火墙原理和设计策略

1．1 防火墙原理

防火墙是位于两个信任程度不同的网络之间的软件或硬件设备的组合，它对两个网络之间的通信进行控制，通过强制实施统一的安全策略，防止对重要信息资源的非法存取和访问，以达到保护系统安全的目的。

其原理是监测并过滤所有内部网和外部网之间的信息交换。防火墙保护着内部网络的敏感数据不被窃取和破坏，并记录内外通信的有关状态信息日志，新一代的防火墙甚至可以阻止内部人员将敏感数据向外传输，还可以限制内部不同子系统之间互相访问，将局域网络放置于防火墙之后可以有效阻止来自外界的攻击。

1．2 防火墙的功能

（1）防火墙应具备的基本功能包括：

防火墙的设计策略应遵循安全防范的基本原则——“除非明确允许，否则就禁止”；

防火墙本身支持安全策略，而不是添加上去

的；

如果组织机构的安全策略发生改变，可以加入新的服务；

有先进的认证手段或有挂钩程序，可以安装先进的认证方法；

如果需要，可以运用过滤技术允许和禁止服务；

可以使用 FTP 和 Telnet 等服务代理，以便先进认证手段可被安装和运行在防火墙上；

拥有界面友好、易于编程的 IP 过滤语言，并可以根据数据包的性质进行包过滤，数据包的性质有目标和源 IP 地址、协议类型、源和目的 TCP/UDP 端口、TCP 包的 ACK 位、出站和入站网络接口等。

如果用户需要 NNTP（网络消息传输协议）、XWindow、HTTP 和 Gopher 等服务，防火墙应该包含相应的代理服务程序。

防火墙应该能够集中和过滤拨入访问，并可以记录网络流量和可疑的活动。此外，为了使日志具有可读性，防火墙应具有精简日志的能力。防火墙的强度和正确性应该可被验证，设计尽量简单，以便管理员理解和维护。

（2）其它功能

支持地址转换，隐藏内部网络真正 IP，可以使黑客无法直接攻击内部网络；而且，可以让内部使用保留的 IP。

虚拟专用网络(VPN)可在防火墙与防火墙或移动的客户端之间对所有网络传输的内容加密，建立一个虚拟通道，以使两者可以安全且不受拘束地互相存取。

支持 QoS 和负载均衡，提供较好的通信服务质量和性能。

1.3 防火墙类型

按照防火墙技术原理来分，防火墙主要分为包过滤防火墙、应用级网关和状态检测防火墙三种。

包过滤式防火墙检查所有通过的信息包中的 IP 地址，并按照系统管理员所给定的过滤规则进行过滤。如果防火墙设定某 IP 地址的站点为不适宜访问的话，从这个地址来的所有信息都会被防火墙屏蔽掉。其优点是它对于用户来说是透明的，处理速度快而且易于维护，但不支持入侵者的攻击记录，且配置繁琐。包过滤可阻止外部对私有网络的访问，却不能记录内部访问，也不能鉴别不同的用户和防止 IP 地址盗用。

应用级网关比单一的包过滤更为可靠，而且会详细地记录所有访问状态信息。但是它会使访问速度变慢，不允许用户直接访问网络，而且应用级网关需要对每一个特定的 Internet 服务安装相应的代理服务软件，用户不能使用未被服务器支持的服务，对每一类服务要使用特殊的客户端软件。

状态监测防火墙具有非常好的安全特性，使用在网关上执行网络安全策略的软件模块，称之为监测引擎。监测引擎在不影响网络正常运行的前提下，采用抽取有关数据的方法对网络通信的各层实施监测，抽取状态信息，并动态地保存起来作为以后执行安全策略的参考。监测引擎支持多种协议和应用程序，并可以很容易地实现应用和服务的扩充。与前两种防火墙不同，当用户访问请求到达网关的操作系统前，状态监视器要抽取有关数据进行分析，结合网络配置和安全规定做出接纳、拒绝、身份认证、报警或给该通信加密等处理动作。其优点是：一旦某个访问违反安全规定，就会拒绝该访问，并报告有关状态作日志记录；支持监测无连接状态的远程过程调用（RPC）和用户数据报（UDP）之类的端口信息。但会降低网络速度，配置也较复杂。

防火墙与普通代理服务器最大不同在于防火墙专门为了保护网络安全而设计，而一个好的防火墙不但应该具备包括检查、认证、警告、记录的功能，并且能够为使用者可能遇到的困境，事先提出解决方案，如 IP 不足形成的 IP 转换的问题，信息加密/解密的问题。

按照实现方式来分，防火墙产品可分为硬件防火墙、软件防火墙和标准服务器防火墙。硬件防火墙主要采取基于 ASIC 芯片的方式实现，软件防火墙主要基于网络处理器方式实现。一般，前者处理效率较高，而后者灵活性较好且可编程。标准服务器防火墙基于专用安全操作系统实现。

指标	软件防火墙	硬件防火墙	标准服务器防火墙
安装	复杂	简单	简单
安全性	高	较高	高
性能	依赖硬件平台	高	高
管理	简单	较简单	简单
成本	低	高	低
扩展性	高	低	高
配置灵活性	高	低	高
价格	低	高	较高

从上面比较可以看出，我们应侧重于选择硬件防

火墙或标准服务器防火墙。

未来，防火墙不仅能够保护内部网络安全，且应具有更为优良的整体性能。这包括地址转换和加密算法的处理效率。防火墙应支持 VPN 和可扩展的内驻应用层代理，且便于安装和管理，集成防病毒和防黑客攻击的功能。总之，未来的防火墙将会具有高度安全性、高透明性和高网络性能。

2. 防火墙配置方案

网络安全性防范是指针对网络外的非授权访问、假冒和拒绝服务等安全性威胁采取的预防、监测、过滤、隔离和处理等措施。根据我所安全性实际需求，我们提出可供选择的网络安全性措施和实施方案（拓扑结构图如下）：

现代网络安全性保证的主要手段就是采用防火墙技术和入侵检测技术 IDS。防火墙技术主要实现对安全性威胁的实时监测、过滤、隔离和紧急处理。入侵检测技术主要实现对网络安全脆弱性进行检测，找出网络安全漏洞，提出增强安全性的建议和策略，起到负责管理员进行网络系统安全管理和安全性预防的作用

具体而言，主要有以下四种：

方案一：双宿主机网关配置（如图 1）

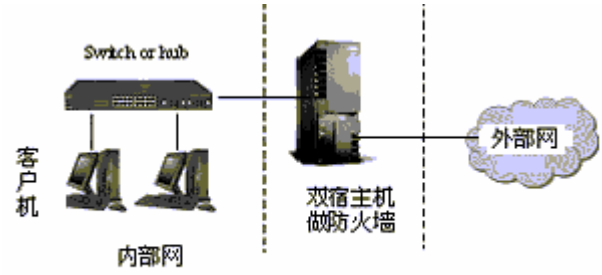


图 1 双宿主机网关

该方案下，只需在目前双穴主机上加装软件防火墙即可。此方案成本相对较低，但是一旦入侵者夺取该主机控制权，则会造成极大的安全性隐患。该主机也就只具备路由的功能了。

方案二：双宿堡垒主机

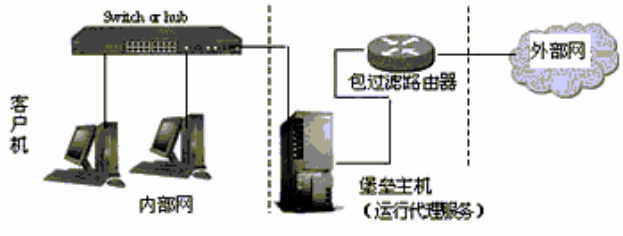


图 2 屏蔽主机网关（双宿堡垒主机）

该方案中双宿主机加装入侵检测系统，包过滤路由即包过滤防火墙。在包过滤路由器上设置过滤规则。主机则是外部唯一可访问到的主机。所有内部向外部的访问也必须通过该主机。

方案三：屏蔽子网

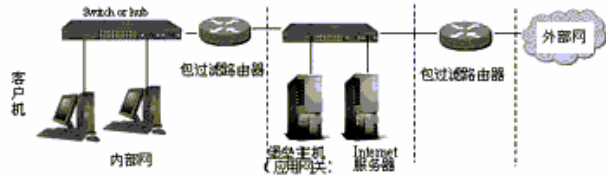


图3 屏蔽子网防火墙

在本子网与其它子网之间建立屏蔽子网。两个包过滤路由器放在子网的两端，在子网内构成一个“缓冲地带”。可根据需要在屏蔽子网中安装堡垒主机，为内部网络和外部网络的互相访问提供代理服务，但是来自两网络的访问都必须通过两个包过滤路由器的检查。这种结构的防火墙安全性能高，具有很强的抗攻击能力，但需要的设备多，造价高。由于防火墙技术和产品种类众多，我们对防火墙技术和产品分类，以及在选择防火墙产品时应考虑的因素进行了分析。

3. 防火墙产品选择

目前，比较著名的主流标准服务器防火墙产品主要有：checkpoint Firewall-1、CyberGuard Firewall、Cisco PIX。根据安全性、高效性、配置便利性、管理难易度、可靠性和可扩展性等因素考虑，我们认为选择 checkpoint Firewall-1 或 Cisco PIX 产品较为合适。低端产品还有东方龙马硬件防火墙、清华紫光 NETCURE UF350 防火墙等国产产品。

当然，在具体选型时，还应考虑同时支持用户连接数、跨平台、支持协议数量、支持端口数和类型等因素。

五、实时监控系统网络防病毒措施建议

1. 系统网络防病毒的必要性

随着电力企业信息化程度不断提高，病毒的威胁和所造成的损失也越来越大。在网络开放互联的基础上，病毒的特征和传播方式也层出不穷。电力生产和运营系统也饱受病毒侵害之苦，为了降低病毒威胁和可能造成的损失，我们必须建立符合系统特点的全方位立体网络防病毒体系。

一般，计算机网络包括网络服务器和网络节点

站。计算机病毒在网上的传播方式包括：

病毒直接从有盘站拷贝到服务器中；

病毒先传染工作站，在工作站内存驻留,等运行网络盘内程序时再传染给服务器；

病毒先传染工作站，在工作站内存驻留，在运行时直接通过映像路径传染到服务器；

如果远程工作站被病毒侵入，病毒也可以通过通讯中数据交换进入网络服务器中；

在网络环境下，网络病毒除了具有可传播性、可执行性、破坏性、可触发性等计算机病毒的共性外，还具有新的特点：

感染速度快：病毒可以在网络中通过网络通信机制进行迅速扩散；

扩散面广：由于病毒在网络中扩散非常快，扩散范围很大，能迅速传染局域网内所有计算机，甚至跨网段传染到其它子网和广域网；

传播的形式复杂多样：计算机病毒在网络上一般是通过“工作站-服务器-工作站”的途径进行传播的，但传播的形式复杂多样；

难于彻底清除：企业网络中，只要有一台工作站未能消毒干净，就可能使整个网络重新被病毒感染，甚至刚刚完成清除工作的一台工作站就有可能被网上另一台带毒工作站所感染；

破坏性大：网络上病毒将直接影响网络的工作，轻则降低速度，影响工作效率，重则使网络崩溃，破坏服务器信息，严重破坏生产运营；

综上所述，网络防病毒是我所各自动化系统正常健康运行的必须选择。

2．网络防病毒策略设计

跟据网络防病毒需求实际情况,我们应制定和实施“层层设防、集中控制、以防为主、防杀结合”的全方位立体网络防病毒策略。具体而言，如下：将 PC 防病毒与网络防病毒系统相结合,建立分级管理机制,采用分布式管理和集中管理相结合的管理模式，同时采用统一的防病毒策略和防病毒管理制度。管理中心可以在中心控制台对全网客户端防病毒配置进行管理和控制。各客户端可动态更新病毒代码库。

3． 网络防病毒产品选购

网络防病毒产品分为三大类：软件、硬件和与防火墙集成。硬件产品效率高，但灵活性差。软件产品灵活性和可配置特性高。我们倾向于选择网络防病毒软件产品。

目前主要的主流网络防病毒产品包括冠群金辰的 Kill、Symantec 的 Norton、趋势科技产品。以下是对其主要指标的比较：

指标	Kill	Norton	趋势
软/硬件	软/硬件	软件	软件
支持代理模式接入	支持	支持	支持
单服务器接入	支持	支持	支持
客户端大小	28M	15M	37M
支持推送、WEB 和 MS UNC	支持	支持	支持
可检测病毒类型	病毒、木马、蠕虫、恶意 javapplet 和 ActiveX	各种已知和未知病毒	多于 76000
扫描压缩文件类型	多种压缩格式及不限层次的压缩文件扫描	对各压缩格式具有实时防护	支持
定时/实时/子定义扫描清除	支持	支持	支持
特征对比和行为判断	支持	NAVEX 专利技术	支持
Email 病毒扫描	支持	支持邮件服务器和客户端查杀	支持
Internet 下载/内存扫描	支持	支持	支持
启发式扫描	支持	BloodHound 专利	支持
告警报告	支持	实时告警，定期执行报告	支持
邮件内容过滤	支持	支持内容字典自定义	支持
URL 封堵	支持	支持自定义 url 列表	支持
反垃圾邮件	支持	支持	支持
跨平台支持	支持	Dos、windows、linux 等	支持
远程锁定配置	支持	支持	支持
远程修改配置	支持	可从集中控制台修改客户端配置	支持
设置不同策略/管理权限	支持	支持	支持

设置反病毒域和权限	支持	支持	支持
平台支持	邮件过滤支持所有平台，反病毒支持 windows、unix 、 linux 、 Mac 、 netware	Dos、windows	Windows 、Solaris、AIX、linux、OS/2
自动发现成员	支持，能广播发现客户端	专门控制台工具	支持
容错均衡集群能力	支持	支持	不支持集群
并发用户数	无限制，根据 OS 定	取决于服务器硬件	支持
病毒库全升级	支持	网站全升级包	支持
病毒库增量升级	支持，满足低带宽要求	支持	支持
支持 HTTP、FTP 和 UNC 升级	支持	支持	支持
资质	获得公安部许可证、军用许可证、通过 VIRUS BULLETIN 100%、ICSA 认证	获得公安部认证、VB100%、Westcostlab、ICSA 认证	公安部认证、ICSA 认证

六、其它

在引入防火墙、入侵检测和网络防病毒技术手段后，更重要的是根据实际发展的安全性需求和反病毒需求，基于产品或工具平台制定完善的安全性策略，并制定切实可行的安全性和反病毒管理制度。这样，系统的安全性和反病毒才有了切实和全面的保障。