电力信息网络安全的实现(上)

Implementation of Security of Power Information Networks (Upper Part)

摘　要： 本文描述了电力企业信息系统安全的现状，分析并构造了电力系统信息安全的体系结构和信息安全模型，提出了解决电力企业信息安全的总体实施方案，并就此论述了实际工作中取得的应用成果。

关键词： 信息 安全 解决

刘树吉　潘明惠　（沈阳辽宁省电力有限公司　110006）

1 引言

电力系统信息安全是电力系统安全运行和对社会可靠供电的保障，是一项涉及电网调度自动化、继电保护及安全装置、厂、站自动化、配电网自动化、电力负荷控制、电力市场交易、电力营销、信息网络系统等有关生产、经营和管理方面的多领域、复杂的大型系统工程。

随着Internet的迅速发展，信息安全问题面临新的挑战。电力系统信息安全问题已威胁到电力系统的安全、稳定、经济、优质运行，影响着“数字电力系统”的实现进程。研究电力系统信息安全问题，开发相应的应用系统，制定电力系统信息遭受外部攻击时的防范与系统恢复措施等信息安全战略，是当前信息化工作的重要内容。电力系统信息安全已经成为电力企业生产、经营和管理的重要组成部分。

2 电力系统信息安全目标及需求分析

2.1 辽宁电力信息网络系统现状

2.1.1 网络系统现状

辽宁电力信息网一个跨地区的大型企业信息网络系统，是国家电力信息网东北主节点，为国电东北公司、吉林、黑龙江省公司提供网络服务。，截止到目前，辽宁电力信息网络已经形成主干网、城域网、广域网三层网络结构，采用千兆以太网络技术组成信息主干网，城域网、广域网已连接省电力系统46个单位局域网、东北公司所属10个单位局域网。其中2Mbps以上连接25个单位。通过中国电信（4M）和吉通公司(4M)与Internet连接。

2.1.2 应用系统现状

辽宁电力信息主干网应用系统有：网络操作系统（DEC Unix、Alpha Windows NT V.11.5和Intel Windows NT V.4.0）；系统管理软件（CA Unicenter TNG 2.1）；数据库操作系统（Sybase Adaptive Server Enterprise 11.5）；网络服务软件（Netscape Suitespot Pro 3.6）；开发工具(Lotus Notes 4.51、Business Objects V4.1、MapInfor MapXSDK 4.5、Power Build Enterprise 7.0等)；30个管理信息系统；Cybercop Scanner安全检测系统；Sniffer网络协议分析系统；防病毒系统（NORTON Antivirus Enteriprise Solution 4.0）；数据备份与灾难恢复系统；网络安全监视系统等。

广域网中各单位的应用系统有：数据库操作系统（Sybase Adaptive Server Enterprise 11.5）；管理信息系统；Cybercop Scanner安全检测系统；防病毒系统（NORTON Antivirus Enteriprise Solution 4.0）等，如图1。

2.2 风险分析（需求分析）

随着Internet的迅速发展，信息安全问题面临新的挑战。计算机系统本身的脆弱性和通信设施的脆弱性共同构成了计算机网络的潜在威胁和脆弱性。一方面，计算机系统硬件和通信设施极易受到自然环境、自然灾害及人为的物理破坏；另一方面计算机系统的软件资源和数据信息极易受到非法的窃取、复制、篡改和毁坏等攻击；同时计算机网络系统的硬件、软件的自然损耗和自然失效等同样会影响系统的正常工作，造成系统的信息损坏、丢失和安全事故。

国家电力公司调度系统数据网络（SPDnet）的建设取得重大进展，国家电力数据网一级网络基本建成，覆盖了全国各网公司及部分省公司，二、三级网络工程正在实施中。

辽宁电力信息网络系统虽然有一些网络安全产品，但没有形成一个完整的信息安全体系。个别单位重基本建设，轻信息安全，网络结构不合理，缺乏网络安全观念，生产实时控制系统与管理信息系统、内部网络与外部网络没有采取有效的安全隔离措施，不能满足信息安全的要求。在信息安全方面缺少系统的网络安全体系，缺少有关信息安全的管理手段和防范措施，缺少故障时的恢复方法和策略，缺少网络实时安全监视手段。

2.3 辽宁电力信息系统安全目标

* 对网络安全现状作出正确判断、分析和采用有效措施对信息资源进行有效的保护。

* 较为准确地估计特定网络用户的风险，最大限度地提高系统的可用性，并把网络带

来的风险减低到可接受程度。

* 建立相应的控制风险的机制，并把这些机制容为一体形成防护体系。

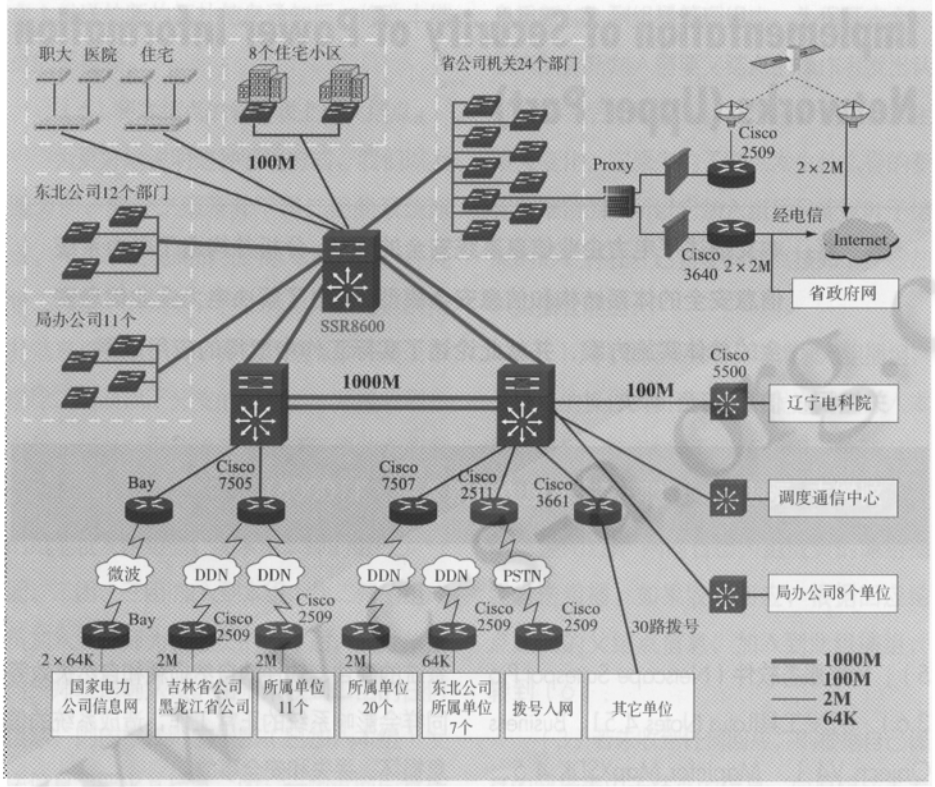

图 1 辽宁电力信息网主干网拓扑图

3 电力系统信息安全体系结构

网络安全体系是一个在网络系统内结合安全技术与安全管理，以实现系统多层次安全保证的应用体系。此体系结合网络、系统、用户、应用及数据方面的安全措施，对网络系统的使用实施统一的安全规划。从技术上和管理上解决网络的安全问题，主要以下五个层次里加强措施：网络的安全性、系统的安全性、用户安全性、应用程序的安全性和数据的安全性。如图2所示。

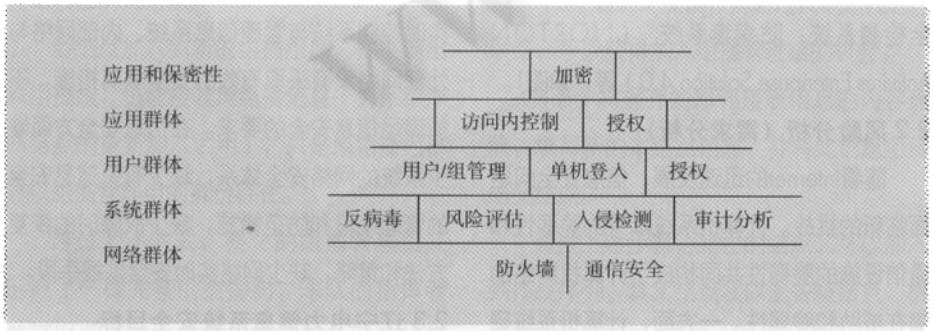

图 2 安全体系结构图

3.1 电力系统信息安全模型

归纳综合现有的一些安全体系模型后，我们提出电力系统信息安全模型，如图3所示。

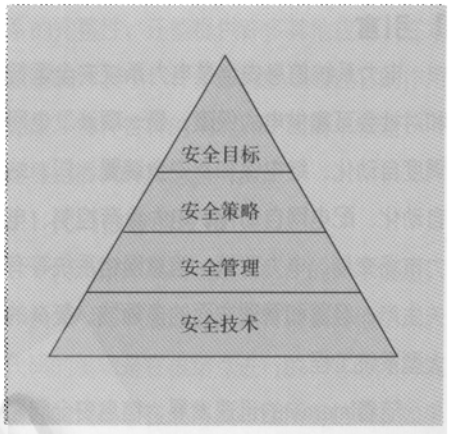

图 3 电力系统信息安全模型

3.2 网络的安全性

网络是信息系统里连接主机，用户机及其它电脑设备的基础，是公司业务系统正常运行的首要保证。从管理的角度看，网络可以分为内部网（Intranet）与外部网（Extranet）。网络的安全涉及到内部网的安全保证以及两者之间连接的安全保证。目前，使用比较广泛的网络安全技术包括防火墙、网络管理和通信安全技术。

3.3 系统的安全性

系统的安全管理围绕着系统硬件、系统软件及系统上运行的数据库和应用软件来采取相应的安全措施。系统的安全措施将首先为操作系统提供防范性好的安全保护伞，并为数据库和应用软件提供整体性的安全保护。在系统这一层，具体的安全技术包括病毒防范、风险评估、非法侵入的检测及整体性的安全审计。

3.4 用户的安全性

3.4.1 用户帐号的安全性

用户帐号无疑是计算机网络里最大的安全弱点。获取合法的帐号和密码是“黑客”攻击网络系统最常使用的方法。用户帐号的涉及面很广，包括网络登录帐号、系统登录帐号、数据库登录帐号、应用登录帐号、电子邮件帐号、电子签名、电子身份等。因此，用户帐号的安全措施不仅包括技术层面上的安全支持，还需在企业信息管理的政策方面有相应的措施。只有双管齐下，才能真

正有效地保障用户账号的保密性。从管理方面，企业可以采取的措施包括划分不同的用户级别、制定密码政策（例如密码的长度、密码定期更换、密码的组成等）、对职员的流动采取的必要措施以及对职员进行计算机安全的教育。从安全技术方面，针对用户账号完整性的技术包括用户分组的管理、惟一身份和身份认证。

3.4.2 用户分组管理

用户分组管理（User / Group Administration）是很多操作系统都支持的用户管理方法。对不同用户组的成员赋予不同的权限，设置相应的管理策略（Policy），使用户在网络和系统资源的使用上有不同的限制。

3.4.3 惟一身份

惟一身份（Single Sign - On）保证用户在企业计算机网络里任何地方都使用同一个用户名和密码。无论是登录网络、系统、数据库、还是应用，用户都只使用一个用户名。这样一来系统就能准确地确认用户并对用户的行为加以监控，在网络系统里对用户的信息访问进行统一管理。

3.4.4 身份认证

身份认证是对网络中的主体进行验证的过程，通常有三种方法验证主体身份。一是只有该主体了解的秘密，如口令、密钥；二是主体携带的物品，如智能卡和令牌卡；三是只有该主体具有的独一无二的特征或能力，如指纹、声音、视网膜或签字等。

3.5 应用程序的安全性

应用程序的安全性是为了确保专门的应用只能被授权的用户使用，专用的数据只能被专人访问。不同级别的用户在使用应用和访问数据时得到的权限也不同。使用控制与权限授予是这一道防线里较常用的两项技术。访问控制和用户授权。

3.6 数据的安全性

为保障数据的安全，常采用信息加密技术、数据完整性鉴别技术、防抵赖技术及数据备份及灾难恢复技术。

4 总体实施方案

完整的安全解决方案应该覆盖网络的各个层次，并且与安全管理相结合。

要建立一个安全的内部网，一个完整的解决方案必须从多方面入手。首先要加强主机本身的安全，减少漏洞；其次要用系统漏洞检测软件定期对网络内部系统进行扫描分析，找出可能存在的安全隐患；建立完善的访问控制措施，安装防火墙，加强授权管理和认证；加强数据备份和恢复措施；对敏感的设备和数据要建立必要的隔离措施；对在公共网络上传输的敏感数据要加密；加强内部网的整体防病毒措施；建立详细的安全审计日志等。本方案对主干网的有关安全问题进行全面解决，对广域网有关基层单位的漏洞检测系统、防病毒系统和与主干网相连的防火墙在本方案中统一购置，数据备份系统由于各单位实际应用情况不同，本方案只提出要求，各单位可根据本单位情况自行选择数据备份设备和系统。其中主干网总体解决方案结构见图4。

4.1 物理安全解决方案

对辽宁电力信息广域网系统连接的所有单位的机房、设备等进行全面安全检查，凡不符合GB50173－93《电子计算机机房设计规范》、GB2887－89《计算站场地技术条件》和GB9361－88《计算站场地安全要求》等国家标准的必须限期整改，使其达到国家标准。

4.2 网络系统安全解决方案

4.2.1主机安全解决方案

（1）安全漏洞扫描与实时入侵检测系统。在辽宁电力信息网络系统广域网连接的各单位安装网络安全漏洞扫描系统，如Internet 扫描器、数据库扫描器、系统扫描、实时的网络监视系统等来检验网络环境中的操作系统和网络设备的安全脆弱性，及时地发现网络环境中由于误配置等造成的潜在的、可被黑客利用的安全漏洞，并根据扫描结果向系统管理员提供周密可靠的安全性分析报告，由此可帮助防御网络环境下复杂的、未经授权的入侵和攻击行为，保证网络安全运行。安全漏洞扫描结构如图5所示。

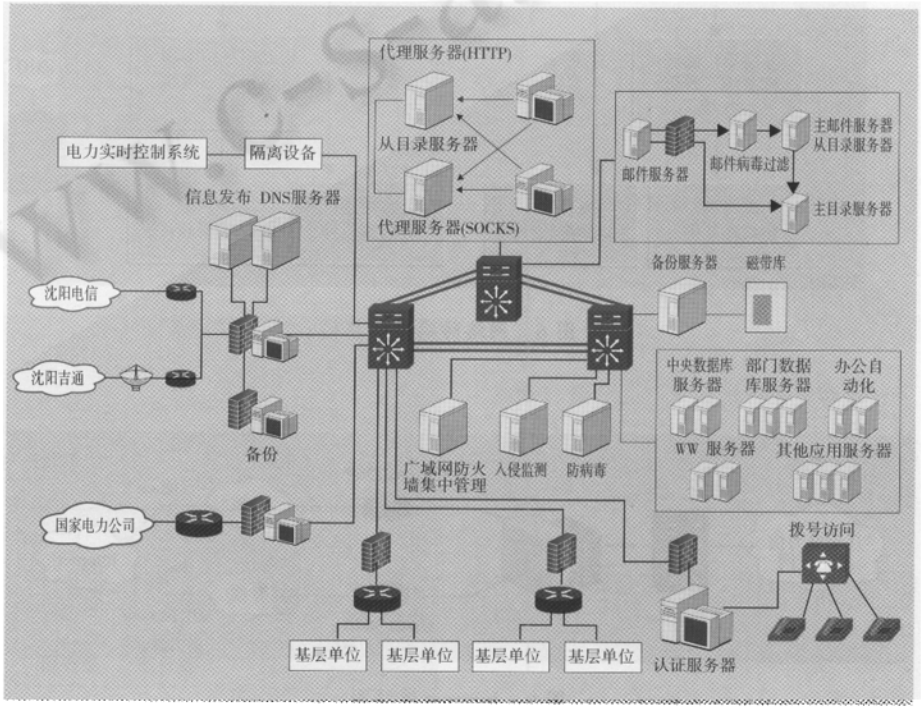

图 4 总体解决方案结构图

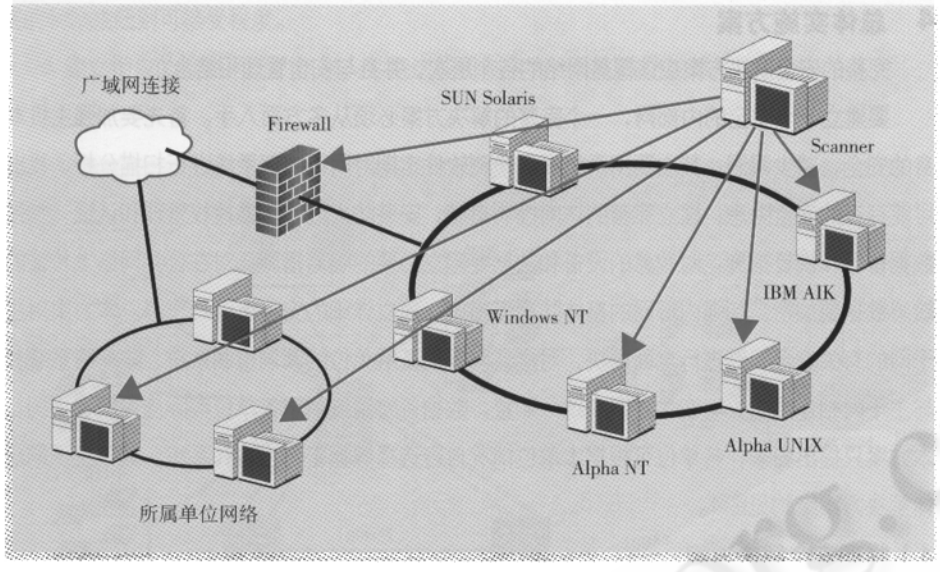

图 5　安全漏洞扫描结构

（2）网络防病毒系统。建立辽宁电力信息网络防病毒系统，构造一个整体的、全方位的、无缝的、功能强大的防病毒体系(如图6，图7所示)，保护企业免遭来自企业外部和企业内部病毒的威胁，从根本上杜绝病毒的发作和传播，有效的保护企业的内部资源。

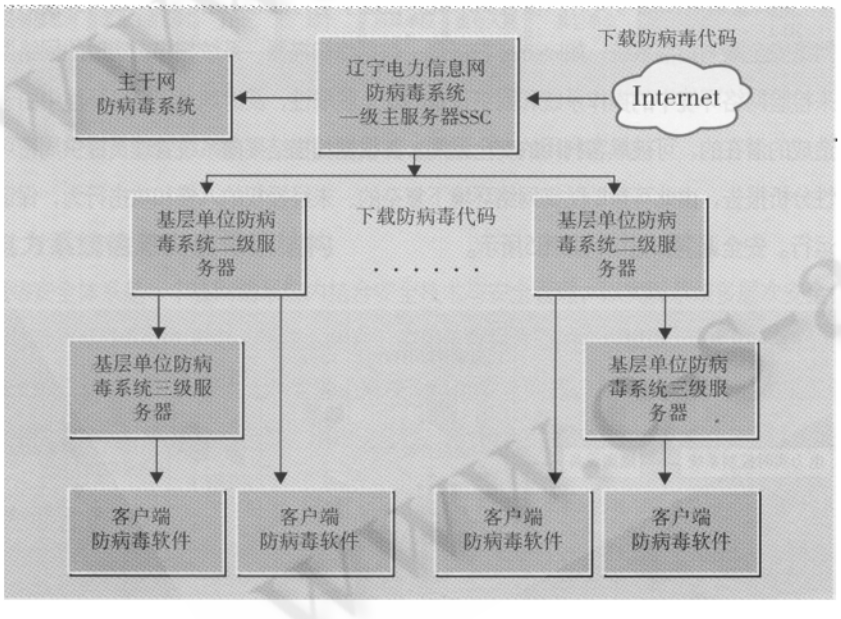

图 6　网络防病毒体系

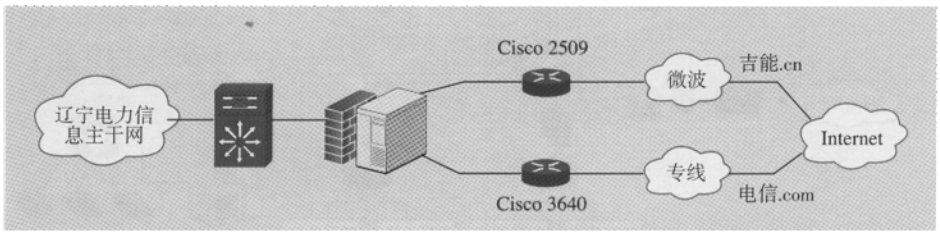

图 9　Internet 连接图

主干网具体配置如图8所示。各单位可自行配置。

（3）数据备份与恢复系统。采用先进数据备份和灾难恢复技术，在本地和异地建立区域数据备份中心，保证数据因系统或误操作造成损坏或丢失后，可及时在本地实现数据的恢复或当发生地域性灾难（地震、火灾等自然灾害）时，可及时在本地或异地实现数据及整个系统的灾难恢复。

各发电厂和供电公司要根据其应用的特点及具体需求，制定相应的备份策略，选择适当的备份设备和系统，自行筹建数据备份中心。

辽宁电力信息网主干网要建立1-2个可抵抗地震、火灾等毁灭性自然灾难的备份与恢复中心，保证整个公司系统在出现不可预见的毁灭性灾难时，可在短时间内恢复信息服务。具体条件是异地数据备份中心的单位与主干网连接带宽必须在100M bps以上。主干网数据备份中心结构(见图8)。

4.2.2 Internet访问安全方案

辽宁电力信息网与Internet连接是通过两台路由器分别连接中国电信和吉通，每台路由器连接带宽为4Mbps，利用两个高速串口，每个串口2M bps，如图9所示。

工作方式为：在代理服务器中，人工设置访问路径，发现访问.com 结尾的出网流量，将其送至同中国电信相连的软件防火墙上出网；发现访问.cn结尾的出网流量，将其送至同吉通相连的软件防火墙上出网。解决方案见图10。

辽宁电力信息网广域网连接的有关单位如因工作需要，在本地设有Internet接口的要选择适当的安全设备和系统，保证网络的安全，以免通过局域网进入主干网或其他单位局域网，造成危害。

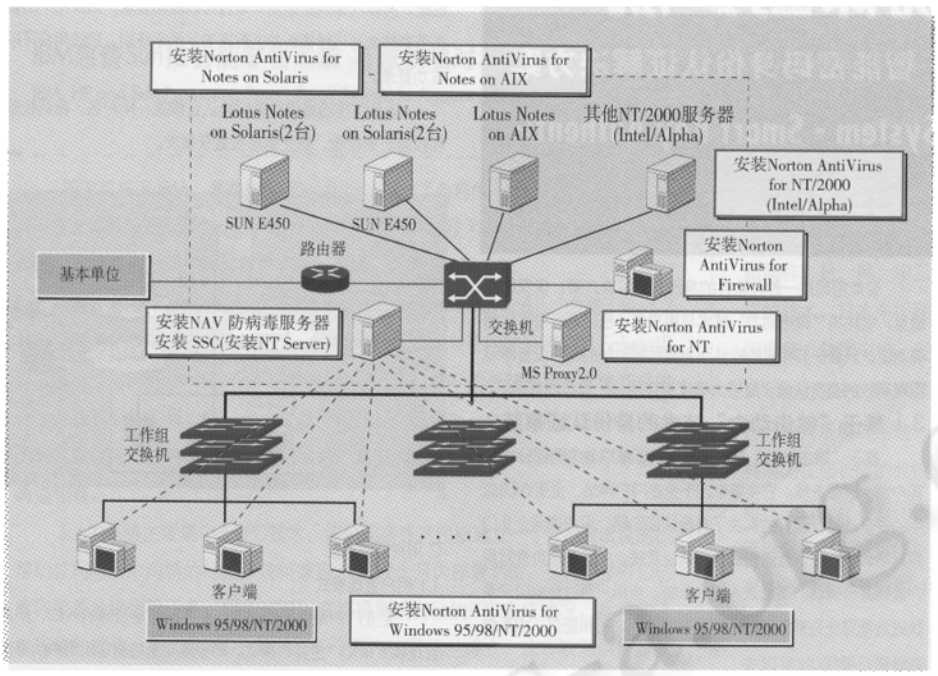

图 7　网络防病毒配置图

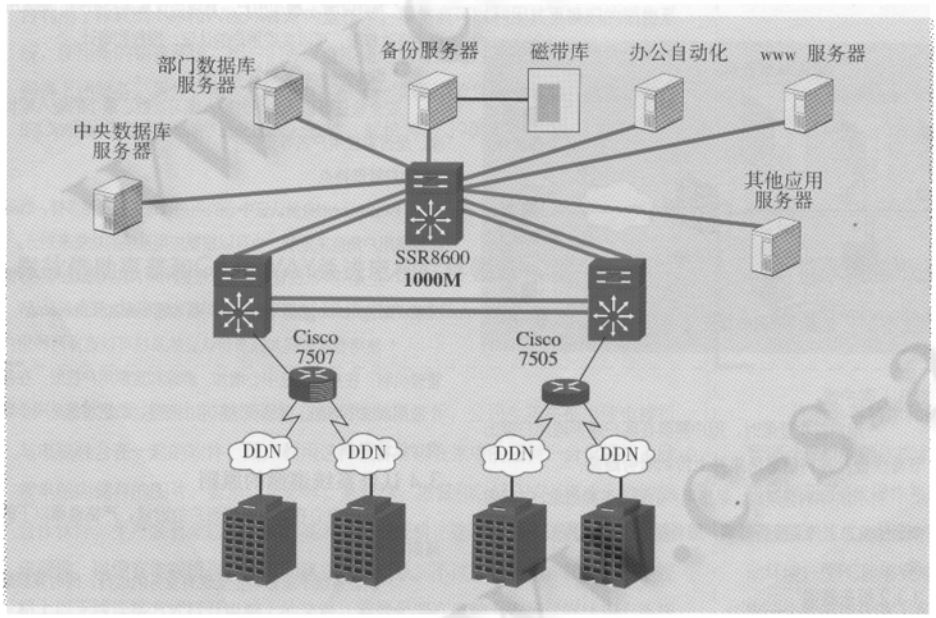

图 8　主干网异地数据备份中心

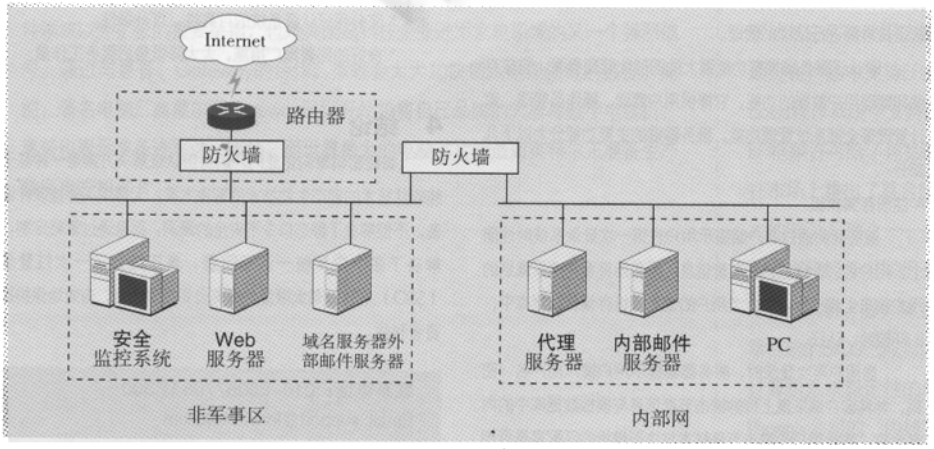

图 10　Internet 访问安全结构图