StoneWall-2000 网络安全隔离设备（反向型）技术白皮书

中国电力科学研究院电网所

北京科东电力控制系统有限责任公司

目　　录

1 公司简介

1.1 中国电力科学研究院

•中国电力建立最早、专业最齐全的研究院，迄今已有 50 年历史；
•有科学院院士、工程院院士及许多电力系统著名专家；
•有研究生部、博士点及博士后流动站；
•形成许多品牌产品：如 CC-2000 调度自动化系统在中国网、省调度自动化系统占有率居全国第一，并荣获 2000 年国家科技进步一等奖；
•通过 ISO 9001（2000 版）的质量认证。

1.2 科东公司

北京科东电力控制系统有限责任公司(电网所)隶属于中国电力科学研究院，是一个专门从事电力系统自动化方面的技术开发、技术服务、技术咨询、技术培训及工程承包等工作的高新技术软件企业。注册资金 1000 万元。

1.2.1 技术力量

公司现有员工总数为 359 人。其中：专业技术人员 270 人，其中既有作为博士、硕士研究生导师、屡获国家级省市级嘉奖的著名老专家，也有获得博士、硕士学位具有丰富实践经验的中青年专家。所有技术人员具有大学本科以上学历。

从成立至今，科东公司已完成大小共几十项电网调度自动化系统工程。

电网所与国家电力公司科技环保部、调度通信中心一起完成了电力调度专用数据网络及电力二次系统安全防护的规划，并成功地申请了国家 863 计划；

电网所是国家电力二次系统安全防护专家组成员(王文博士、杨秋恒教授、高昆仑博士)，制定了《全国电力二次系统安全防护的总体方案》；

电网所是国家电力二次系统安全防护工作组成员(王文博士、杨秋恒教授、高昆仑博士)，对各地网省调度中心的二次系统安全防护方案进行评审，对各地网省调度中心的二次系统安全防护的实施情况进行了检查。

1.2.2 组织结构

科东公司实行董事会领导下的总经理负责制。由总经理、副总经理全面负责公司运营、技术工作，下设电网调度自动化、配电自动化、应用仿真、电力市场、技术开发、市场、销售、人事行政、质量管理、东北分公司、南方分公司等部门开展各项业务。

1.2.3 为您提供的服务

在电力二次系统安全防护领域竭诚为您提供以下服务：

电力二次系统网络安全防护方案的设计与实施；

电力专用网络安全设备系列产品，包括正向型、反向型隔离设备、纵向加密认证装置、加密装置管理系统、信息安全网络隔离装置、拨号加密认证装置、安全网关机、调度证书系统、数据库同步系统。

关于电力二次系统安全防护的咨询和培训。

2 StoneWall-2000 网络安全隔离设备（反向型）

2.1 开发背景

调度自动化系统等与当地的 MIS 系统或因特网之间直接互联（或无缝连接），对电网安全运行构成严重隐患。

2000-10-13 二滩电厂由于控制系统死机造成川渝电网大范围的停电事故，其中控制系统网络与办公自动化系统网络的直接互联就被认为是事故的一个可能因素；

国家电力公司科技环保部 2000 年科技攻关项目，是国家 863 项目—国家电网调度中心二次系统安全防护的子课题；

2001 年在国调试运行，并对设备进行多次改型、功能与性能完善；

2002 年 6 月，国家经贸委下发 30 号令；

2002 年 7 月通过公安部检验，并获得“网络安全隔离设备”的销售许可；

2002 年 9 月由国调、科技环保部在保密局组织了安全测试；

2002 年 9 月通过国家网络安全积极防御实验室检测；

2002 年 9 月通过解放军信息安全评测中心检测；

2002 年 9 月底，国调、科技环保部组织了安全技术评审，受到何德全、曲延文、吴世忠、杨有权、袁文恭等院士专家的好评；

2003 年 10 月 22 日 StoneWall-2000 网络安全隔离设备获得 实用新型专利 专利号 ZL 02 82484.7；

2003 年 11 月 15 日 StoneWall-2000 网络安全隔离设备(反向型) 全国第一个获得国家电力调度通信中心《关于电力专用安全防护设备的检测证明》；

2007 年 7 月对 StoneWall-2000 网络安全隔离设备（反向型）进行全面的升级改造。

2.2 概述

StoneWall-2000 网络安全隔离设备（反向型）是由中国电力科学研究院下属电网所-北京科东电力控制系统有限责任公司自主开发研制，具有物理隔离能力的网络安全设备，具有操作简便、高性能、高可靠性等特点。

StonewWall-2000 网络安全隔离设备（反向型）采用软、硬结合的安全措施，在硬件上使用双机结构通过安全岛装置进行通信来实现物理上的隔离；在软件上，采用综合过滤、访问控制、应用代理、双字节检查技术实现链路层、网络层与应用层的隔离。在保证网络透明性的同时，实现了对非法信息的隔离。

StoneWall-2000 网络安全隔离设备（反向型）配套软件，实现可信数据根据计划自动或手动地从外网到内网的传输，传输过程中，发送端程序对外网数据进行双字节转换及数字签名，报文在通过网络安全隔离设备前，网络安全隔离设备根据规则进行综合过滤，并对签名进行验证，对验证通过的报文再进行双字节检查，这样检查通过的报文才可以进入内网，以保证内网系统的安全，并保证在网络隔离的情况下可信数据能够进入内网。

2.3 基本功能

1) 完全满足《全国电力二次系统安全防护总体方案》标准要求，并通过公安部、国家电力调度通信中心、解放军信息安全评测中心的检测；
2) 实现两个安全区之间的非网络方式的安全的数据交换，并且保证安全隔离装置内外两个处理系统不同时连通；
3) 具有基于非对称加密算法数字签名和验证功能；
4) 通过对文本数据进行全角检查，进一步防毒；
5) 在配套软件的配合下，实现可信数据由外网到内网的自动或手动传输；
6) 自动传递的文件任务可定制，支持更新检查、增量发送；
7) 任务发送情况有日志记录，可随时查阅；
8) 支持多种工作模式：无 IP 地址透明工作方式（虚拟主机 IP 地址、隐藏 MAC 地址）、支持网络地址转换（NAT）、混杂工作模式，保证标准应用的透明接入；
9) 支持基于状态检测的 MAC、IP、传输协议、传输端口以及通信方向的综合报文过滤与访问控制；
10) 提供完备的日志审计功能，如时间、IP、MAC、PORT 等日志信息。对通过装置进入内网的应用数据及未通过装置而被丢失的应用数据进行完整的纪录，已备事后审计；
11) 具有报警功能，当发生非法入侵、装置异常、通信中断或丢失应用数据时，可输出报警信息；
12) 安全、方便的维护管理方式：基于证书的管理人员认证，图形化的管理界面。方便地对装置进行设置，监视和控制系统运行；
13) 支持地址绑定功能，可以有效阻止非法用户盗用合法用户的 IP 地址；
14) 支持双向地址转换功能，可以在保障自身网络安全的前提下向外提供服务；
15) 具有可定制的应用层解析功能，支持应用层特殊标记识别；
16) 提供基于硬件 WatchDog 的系统监视功能，保证系统连续稳定可靠运行；
17) 提供数据传输软件和 API 函数接口，方便用户进行二次系统安全隔离的改造。

2.4 设备特点

2.4.1 安全可靠

StoneWall-2000 建立在具有自主知识产权的安全操作系统基础上。通过对操作系统内核的大规模裁减，剔除不安全模块,大大加强了系统内核的安全性和抗攻击能力，而且操作系统固化在隔离设备中，避免了因操作系统故障而导致设备工作异常。

StoneWall-2000 网络安全隔离设备（反向型）功能比较全面，具有任务定制、文件名模式匹配、状态检测功能、地址绑定功能、双向地址转换功能、双机热备功能、日志审计功能等，而且由于 StoneWall-2000 网络安全隔离设备（反向型）使用透明接入方式，是一般用户在正常操作时感觉不到设备的存在,这样既不影响网络的工作效率,又保证了更高的安全性。

2.4.2 数字签名验证技术

签名应采用非对称加密算法，考虑加密强度的要求，统一要求采用 RSA 加密算法，然后用 RSA 公私钥对中的私钥对摘要数据进行加密，将密文做为签名附在数据后，反向型隔离设备在收到数据后，用相同公私钥对中的公钥对签名数据解密，对比计算出的摘要，完成对发送文件的验证。

2.4.3 双字节转换及检查技术

通过数字签名验证的文本报文，需要通过 StoneWall-2000 网络安全隔离设备（反向型）的双字节检查，才能最终进入内网，通过双字节检查，可以保证进入内网的数据为纯文本数据，而且这种文本数据中的脚本数据也是不能运行的全角数据，可以防止病毒进入内网。

2.4.4 硬件的数据流向控制

经过网络安全隔离设备（反向型）的数据流向控制是通过特有的硬件实现的硬控制，数据只能有外网流向内网，防止在安装反向隔离设备后为正向数据流动提供后门。

2.4.5 高强度的抗攻击能力

处于内网和外网通信唯一通路上的网络安全隔离设备（反向型）无形中成为黑客攻击的首要目标，要保护内网的安全，首先要保证网络安全隔离设备（反向型）具有较强的抗攻击能力，网络安全隔离设备（反向型）采用非 INTEL（及兼容）双微处理器，减少被病毒攻击的概率，采用自主版权的操作系统内核，取消所有网络功能，而且设备本身没有 IP 地址，使得黑客攻击无从下手。

2.4.6 高速稳定

StoneWall-2000 网络安全隔离设备（反向型）采用高速处理器，保证了硬件平台的高速运转，操作系统经过适当裁减和安全加固，保证了软件平台的稳定运行，再加上百兆以太网模块，这些条件保证了高速稳定的网络传输。

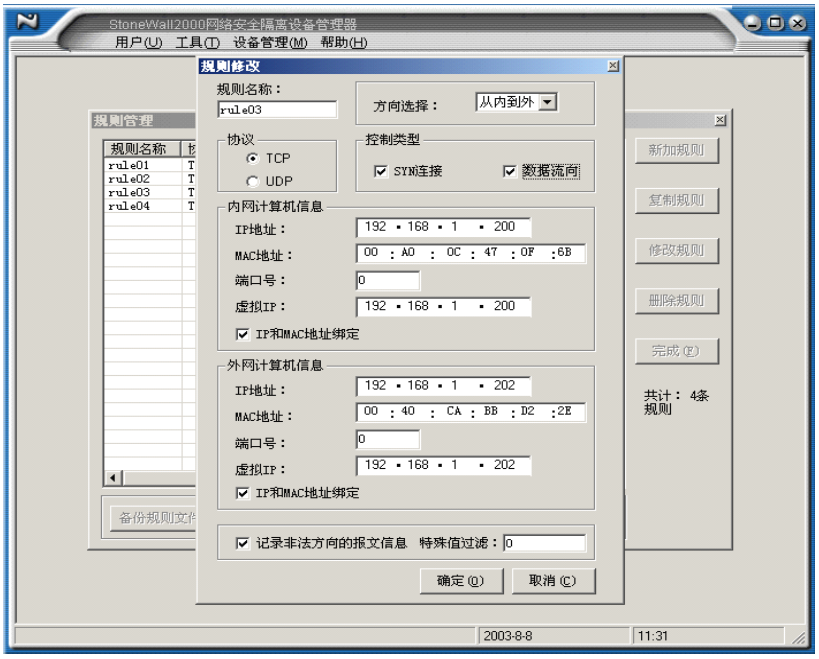
2.4.7 具有内外网络接口通信状态指示灯

StoneWall-2000 网络安全隔离设备（反向型）在前面板上提供电源指示灯、10M/100M 自适应网卡连接状态，传输速率指示灯，便于用户监控及故障诊断。

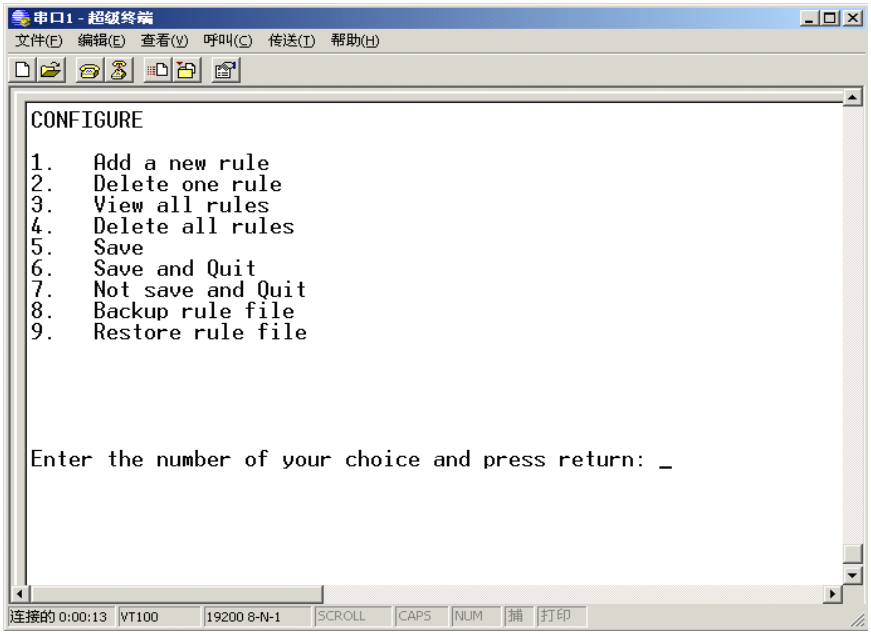
2.4.8 配置简单

StoneWall-2000 网络安全隔离设备（反向型）配置非常简便，对它的操作及设置都可以通过使用规则配置管理工具及配套文件传输程序实现。StoneWall-2000 网络安全隔离设备（反向型）提供了两种不同的规则配置管理工具：GUI 管理工具、CLI 管理工具，配套文件传输程序包括：文件发送端程序、文件接收端程序。

规则管理工具（GUI）是本产品的专用配套程序。该管理器具有界面友好直观、功能齐全、通俗易懂等特点，可以运行于 Microsoft Windows9X/Me/2000/XP 环境下。管理工具如下图所示：

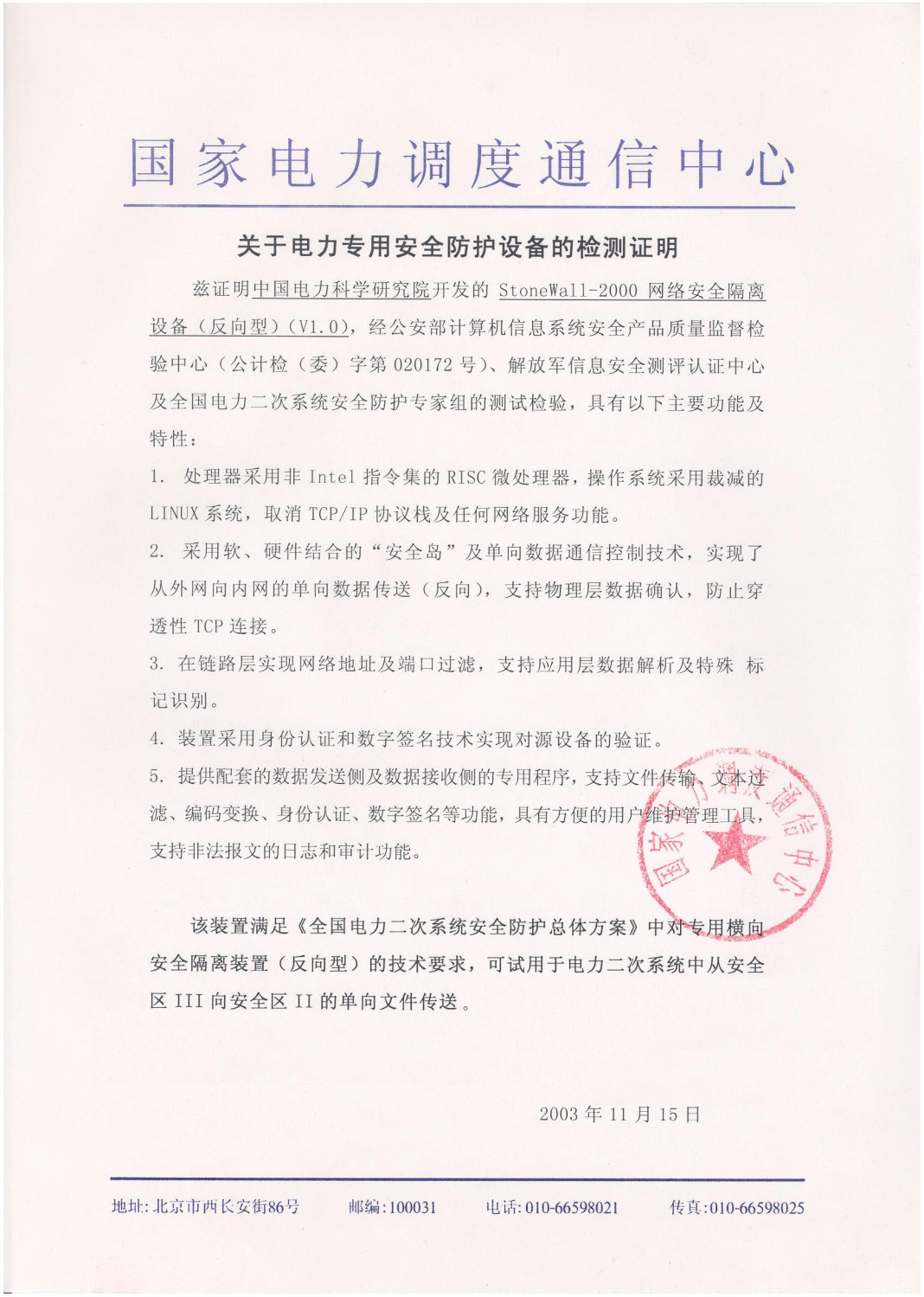


CLI 命令行方式是指使用设备提供的 Console 接口进行本地管理。该管理工具具有最高的安全级别，但相应的对管理员的要求比较高。管理工具的界面如下：


串口1 - 超级终端
文件(F) 编辑(E) 查看(V) 呼叫(C) 传送(T) 帮助(H)
CONFIGURE
1. Add a new rule
2. Delete one rule
3. View all rules
4. Delete all rules
5. Save
6. Save and Quit
7. Not save and Quit
8. Backup rule file
9. Restore rule file
Enter the number of your choice and press return: _
连接的 0:00:13
VT100
19200 8-N-1
SCROLL
CAPS
NUM
捕
打印

2.4.12 检测证明

国家电力调度通信中心的检测证明：



国家电力调度通信中心

关于电力专用安全防护设备的检测证明

兹证明中国电力科学研究院开发的 StoneWall-2000 网络安全隔离设备（反向型）（V1.0），经公安部计算机信息系统安全产品质量监督检验中心（公计检（委）字第 020172 号）、解放军信息安全测评认证中心及全国电力二次系统安全防护专家组的测试检验，具有以下主要功能及特性：

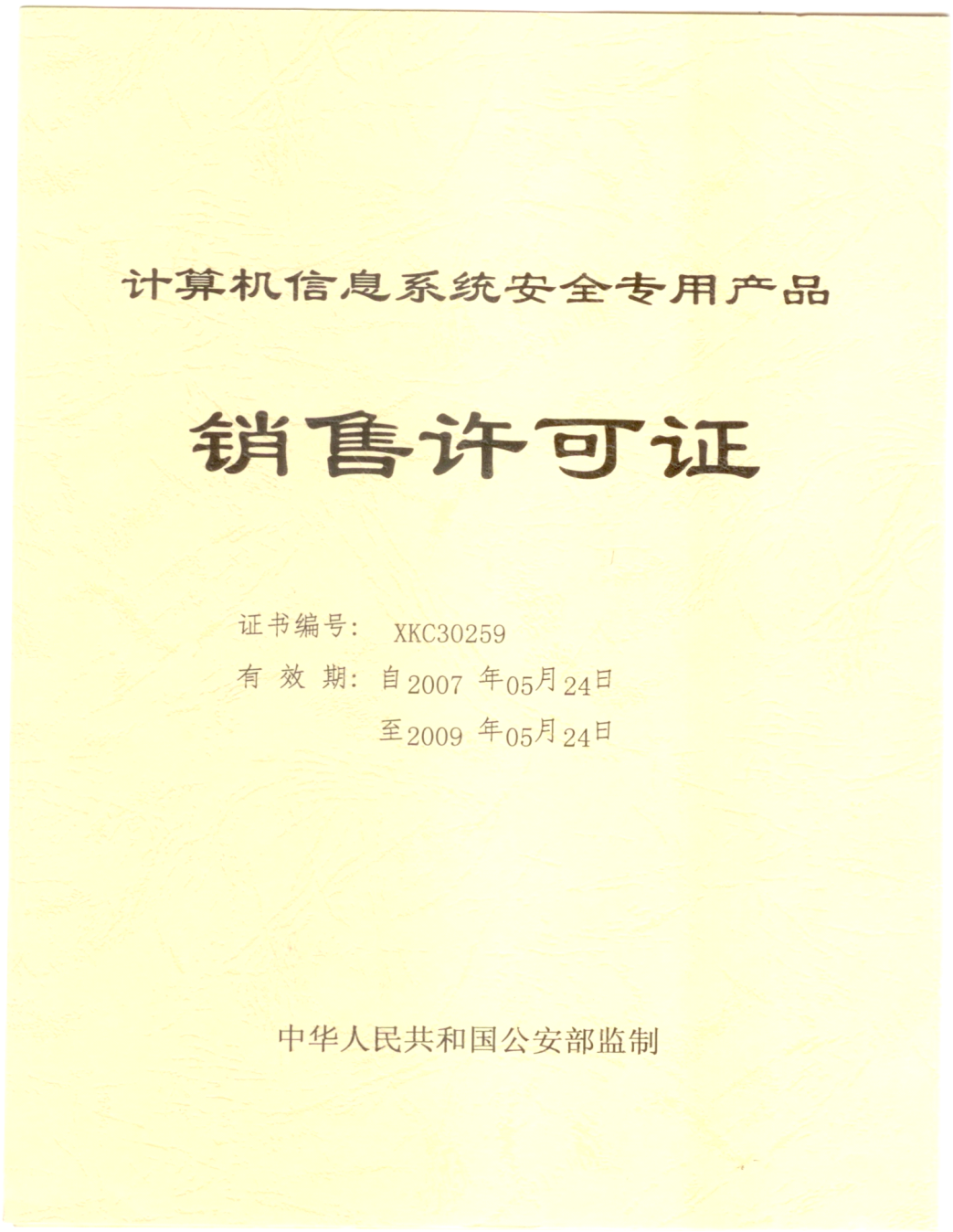
1. 处理器采用非 Intel 指令集的 RISC 微处理器，操作系统采用裁减的 LINUX 系统，取消 TCP/IP 协议栈及任何网络服务功能。
2. 采用软、硬件结合的“安全岛”及单向数据通信控制技术，实现了从外网向内网的单向数据传送（反向），支持物理层数据确认，防止穿透性 TCP 连接。
3. 在链路层实现网络地址及端口过滤，支持应用层数据解析及特殊 标记识别。
4. 装置采用身份认证和数字签名技术实现对源设备的验证。
5. 提供配套的数据发送侧及数据接收侧的专用程序，支持文件传输、文本过滤、编码变换、身份认证、数字签名等功能，具有方便的用户维护管理工具，支持非法报文的日志和审计功能。

该装置满足《全国电力二次系统安全防护总体方案》中对专用横向安全隔离装置（反向型）的技术要求，可试用于电力二次系统中从安全区 III 向安全区 II 的单向文件传送。

2003 年 11 月 15 日

地址：北京市西长安街86号 邮编：100031 电话：010-66598021 传真：010-66598025

销售许可证：



计算机信息系统安全专用产品

销售许可证

证书编号： XKC30259

有 效 期： 自2007 年05月24日

至2009 年05月24日

中华人民共和国公安部监制

中国电力科学研究院：

根据公安部《计算机信息系统安全专用产品检测和销售许可证管理办法》及有关规定，经审查，准许你单位生产的（代理）网络安全隔离设备 StoneWall-2000----------安全专用产品进入市场销售，特发此证。

公安部公共信息网络安全监察局
计算机信息系统安全专用产品管理专用章

2007 年 05 月 24 日

公安部检验报告：

报告编号：公计检 060172

检验报告

样品名称 网络安全隔离设备

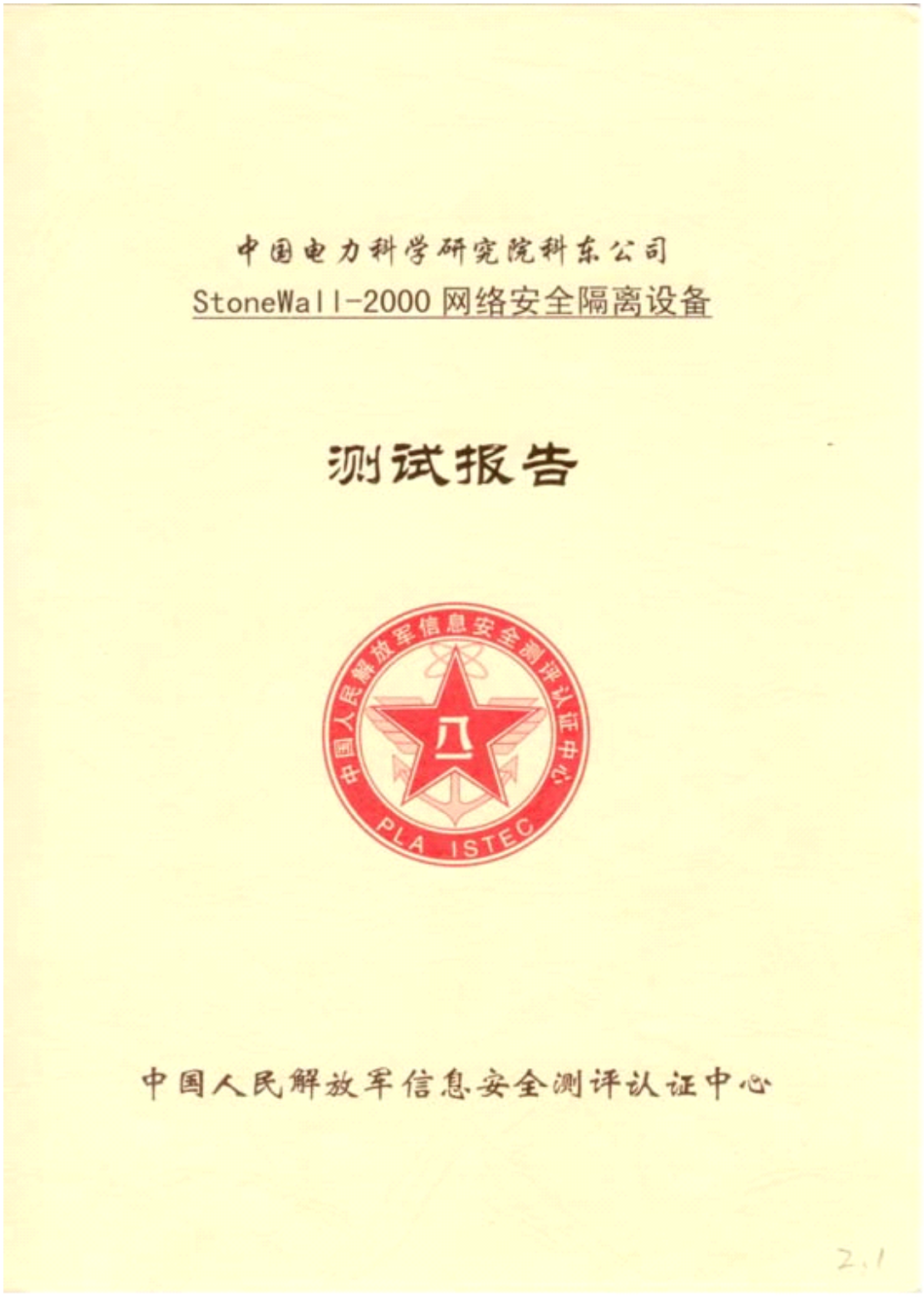
型号规格 StoneWall-2000

受检单位 中国电力科学研究院

检验类别 委托检验

公安部计算机信息系统安全产品质量监督检验中心

解放军总参的测试报告：


中国电力科学研究院科东公司

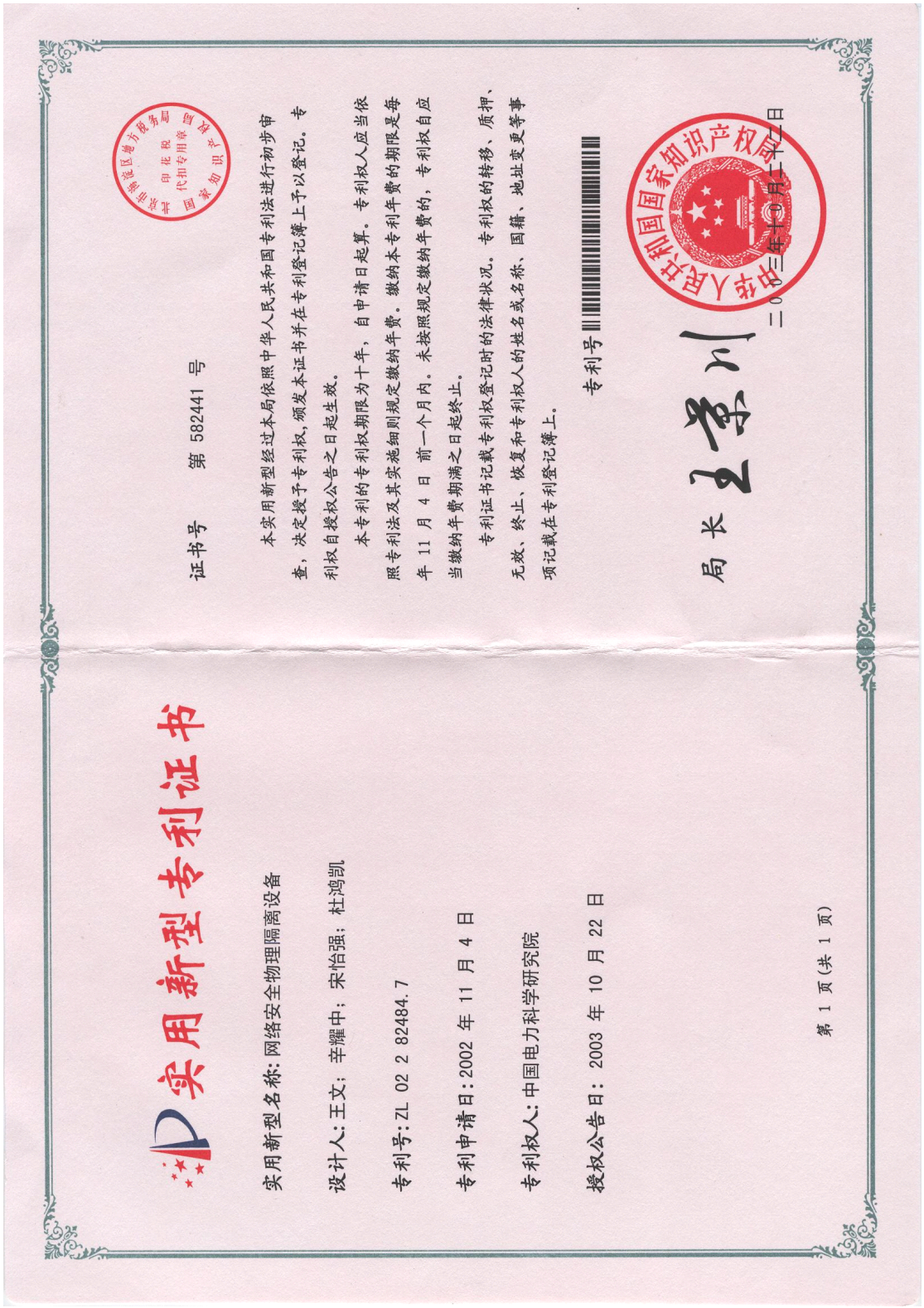
StoneWall-2000 网络安全隔离设备

测试报告

中国人民解放军信息安全测评认证中心

2.1

专利证明：



实用新型专利证书

实用新型名称：网络安全物理隔离设备

设计人：王文；辛耀中；宋怡强；杜鸿凯

专利号：ZL 02 2 82484.7

专利申请日：2002 年 11 月 4 日

专利权人：中国电力科学研究院

授权公告日：2003 年 10 月 22 日

证书号 第 582441 号

本实用新型经过本局依照中华人民共和国专利法进行初步审查，决定授予专利权，颁发本证书并在专利登记簿上予以登记。专利权自授权公告之日起生效。

本专利的专利权期限为十年，自申请日起算。专利权人应当依照专利法及其实施细则规定缴纳年费。缴纳本专利年费的期限是每年 11 月 4 日 前一个月内。未按照规定缴纳年费的，专利权自应当缴纳年费期满之日起终止。

专利证书记载专利权登记时的法律状况。专利权的转移、质押、无效、终止、恢复和专利权人的姓名或名称、国籍、地址变更等事项记载在专利登记簿上。

专利号

局长

二〇〇三年十〇月二十二日

第 1 页(共 1 页)

科技进步奖：

国家电网公司

科学技术进步奖

获奖证书

获奖项目：StoneWall-2000网络安全隔离设备

获奖等级：三等

获 奖 者：马 骁

奖励年度：2004年

发证机构：国家电网公司

证书号：20043107-G03

2.5 型号

StoneWall-2000 网络安全隔离设备（反向型）

2.6 系统组成

设备（硬件）：是一个高速稳定的硬件平台和安全加固的操作系统的完美结合体。

配置管理工具（软件）：StoneWall-2000 网络安全隔离设备（反向型）提供了两种管理工具：GUI 和 CLI。用于对隔离设备的配置和管理。

配套应用程序（软件）：文件发送端程序，文件接收端程序。

2.7 接口配置

内网：

网络接口：10/100BaseTX	2 个
CONSOLE 接口：RJ45，115200-8-N-1	1 个
扩展串口：	2 个

外网：

网络接口：10/100BaseTX	2 个
CONSOLE 接口：RJ45，115200-8-N-1	1 个
扩展串口：	2 个
电源插座	2 个
电源开关	2 个

2.8 接口规范

网络接口：10/100BaseTX
CONSOLE 接口：RJ45，115200-8-N-1

2.9 电气性能

a) 电源
可应用 220V 和 110V 电压。
b) 环境规范
运行温度：0℃ -- 40℃
操作湿度：10% -- 90%@40 摄氏度，非冷凝

2.10 参考的安全规范和标准

UL 1950

EN 41003
AS/NZS 3260
AS/NZS 3548 Class A
CSA Class A
FCC Class A
EN 60552-2
VCCI(ClassII)

2.11 抗干扰性

IEC-1000-4-2 （ESD）
IEC-1000-4-3 （辐射敏感性）
IEC-1000-4-4 （电快速瞬变）
IEC-1000-4-5 （电涌）
IEC-1000-4-6 （谐波）

2.12 几何及物理特性

尺寸：标准 1U 机箱

2.13 安全机理

2.13.1 具有专利的物理结构和安全岛技术

StoneWall-2000 网络安全隔离设备（反向型）使用双机结构，通过连接双机的非网络设备而实现的安全岛技术将受保护网络从物理上隔离开来。

StoneWall-2000 网络安全隔离设备（反向型）通过开关切换及数据缓冲设施来进行数据交换。开关的切换使得在任何时刻两个网络没有直接连通，而数据流经网络安全隔离设备（反向型）时 TCP/IP 协议被终止，防止了利用协议进行攻击，在某一时刻网络安全隔离设备（反向型）只能连接到一个网络。

StoneWall-2000 网络安全隔离设备（反向型）作为代理从外网的网络访问包中抽取出数据然后通过数据缓冲设施转入内网，完成数据中转。在中转过程中，网络安全隔离设备（反向型）会对抽取的数据报文的 IP 地址、MAC 地址、端口号、连接方向实施综合过滤控制，然后对通过上述过滤的报文进行签名验证，对验证通过得报文进行双字节检查或二进制校验，只有满足上述所有要求的报文才可以通过网络安全隔离设备（反向型）。由于网络安全隔离设备（反向型）采用了独特的开关切换机制，因此，在进行检查时网络实际上处于断开状态，只有通过严格检查的数据才有可能进入内网，**即使黑客强行攻击了网络安全隔离设备（反向型），由于攻击发生时内外网始终处于物理断开状态，黑客也无法进入内网**。

网络安全隔离设备（反向型）在实现物理隔断的同时允许可信网络和不可信网络之间的数据和信息的安全交换。由于网络安全隔离设备（反向型）仅抽取合法数据交换进内网，因此，内网不会受到网络层的攻击，这就在物理隔离的同时实现了数据的安全交换。

2.13.2 安全的硬件及操作系统

StoneWall-2000 网络安全隔离设备（反向型）**采用非 INTEL 指令系统（及兼容）的 RISC 微处理器、采用双嵌入式计算机及安全岛技术，**减少受攻击的概率，实现两个安全区之间的非网络方式的单向数据传输；

设备固化了精简的、安全的 linux 操作系统，将嵌入式 Linux 内核进行了裁剪。**内核中只包括用户管理、进程管理、和 Socket 编程接口，裁剪掉 TCP/IP 协议栈和其它不需要的所有系统服务**，提高了系统安全性和抗攻击能力，保证了系统安全的最大化；

2.13.3 数据包的综合过滤技术

StoneWall-2000 网络安全隔离设备（反向型）对于数据包要进行 IP/MAC/PORT 的综合过滤，只有满足条件的数据包才可以通过隔离设备；

通过综合报文过滤与访问控制、表示层与应用层数据完全单向传输、应用层解析、日志审计和报警功能，能够抵御除 DoS 以外的已知的网络攻击。

2.13.4 数字签名验证技术

通过综合过滤的报文，需要通过 StoneWall-2000 网络安全隔离设备（反向型）的数字签名验证，才有可能可以通过隔离设备进入内网，这种数字签名采用非对称数字加密技术，可以防止非法用户假冒合法用户向内网发送文件。

2.13.5 双字节检查技术

通过数字签名验证的报文，需要通过 StoneWall-2000 网络安全隔离设备（反向型）的双字节检查，才能最终进入内网，通过双字节检查，可以保证进入内网的数据为纯文本数据，而且这种文本数据中的脚本数据也是不能运行的全角数据，可以防止病毒进入内网。

2.13.7 状态检测技术

状态检测技术：基于隔离设备所维护的状态表的内容转发或拒绝数据包的传送，比普通的包过滤有着更好的网络性能和安全性。普通包过滤使用的过滤规则是静态的。而采用状态检测技术的隔离设备在运行过程中一直维护着一张状态表，这张表记录了从受保护网络发出的数据包的状态信息，然后隔离设备根据状态表内容对返回受保护网络的数据包进行分析判断，这样，只有响应受保护网络请求的数据包才被放行。

2.13.8 高可用技术

StoneWall-2000 网络安全隔离设备（反向型）内置硬件 Watchdog，保证系统软件的可靠运行。**支持双机热备，互为备用的两台设备中任何一台出现故障，另一台设备自动接替其工作，保证提供不间断的网络服务；支持双电源，在工作的时候,有一个电源作为主电源供电,一个作为辅电源作备份，实现了主备电源的在线无缝切换**，有效地提高整个电源工作的可靠性及延长整个系统的平均无故障工作时间，通过采用以上技术，提高设备的持续运行能力，提供更高的可用性；

2.13.9 地址绑定技术

隔离设备具有地址绑定技术，可以通过建立起来的合法 IP 地址和 MAC 地址的对应关系识破非法用户盗用合法 IP 的阴谋，并拒绝该连接请求。

2.13.10 双向网络地址转换技术

为了达到可以让不同网段两个网络通过隔离设备通信的目的，在隔离设备上采用网络地址转换功能模块，当 NAT 代表内部网络与外部网络建立连接时，它使用自定义的 IP 地址。在受保护的内部网络里，当一个 TCP/IP 请求被送往隔离设备时，NAT 模块将源 IP 地址替

换为自定义的 IP 地址。当外部网络的应答返回到隔离设备时，NAT 将应答的目标地址字段替换为最初建立 TCP/IP 请求的的内部网络计算机结点的 IP 地址。

因为外部网络的计算机结点也有可能主动发送 TCP/IP 连接请求给内部网络，所以外部网络的计算机必须知道内部网络的计算机的 IP 地址，因此，对于 NAT 的设计采用的是静态地址分配机制，就是说 NAT 为内部网络的计算机结点绑定了一个固定的 IP 地址（虚拟的 IP 地址）。

2.13.11 日志审计及实时报警

可以实时监控数据通信状况，对非法的数据包进行信息记录和浏览，方便管理员及早发现问题。支持日志集中存储和管理的 SYSLOG 机制。

StoneWall-2000 网络安全隔离设备（反向型）提供实时的报警输出功能，用户可以通过串口，获得系统的实时报警信息，报警格式遵循 SYSLOG 规范，便于用户收集、分析及综合利用。

2.13.12 高强度的抗攻击能力

通过特殊的硬件结构和加固的操作系统的内核以及隔离设备本身没有 IP 地址，使得隔离设备本身的抗攻击能力的强度极高，黑客对设备的攻击无从下手。

2.14 数据传输过程描述

专用安全隔离装置（反向）用于从安全区 III 到安全区 I/II 传递数据，是安全区 III 到安全区 I/II 的唯一一个数据传递途径。专用安全隔离装置（反向）集中接收安全区 III 发向安全区 I/II 的数据，进行签名验证、内容过滤、有效性检查等处理后，转发给安全区 I/II 内部的接收程序具体数据传输过程如下：

1. 安全区 III 用户端应用程序首先调用接口函数（半角变全角，签名，如果是小文件则用隔离装置公钥加密，大文件仅签名），将明文文件转变成密文文件。
2. 安全区 III 用户端通过 TCP（FTP）等协议将密文文件传输到安全区 III 应用网关（即外网网关）
3. 在安全区 III 应用网关上运行反向隔离设备发送端的配套程序，以 UDP 协议将密文文件发送到隔离设备的外网侧。
4. 隔离设备外网侧接收 UDP 报文，将整个文件收完后，调用接口函数（小文件解密，验签，E 文本内容检查，全角检查）通过检查后，将解密文件传输到设备的内网侧。
5. 设备内网侧采用 UDP 协议将文件传输到安全区 II 应用网关上（即内网网关）。
6. 内网网关通过 TCP（FTP）等协议将带有签名的文件传输到安全区 II 用户端。
7. 用户端应用程序对带有签名的文件入库时，先进行验签，然后将全角转换成半角存储到数据库中。

注：

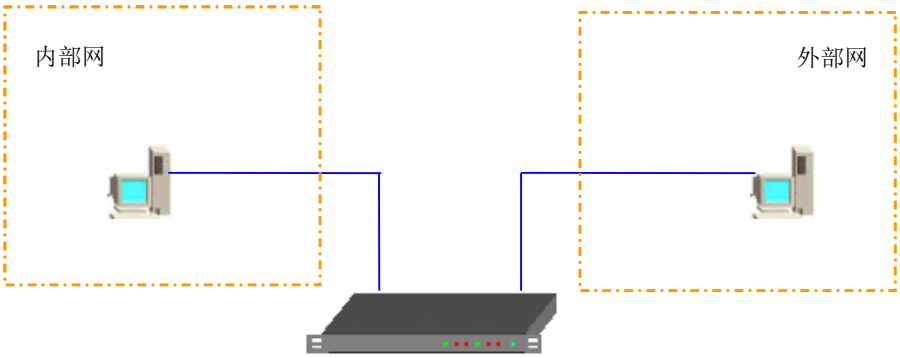
1) Windows 下采用 USB key 进行 RSA 保护，非 windows 操作系统可用 p12 证书;

2) 编码转换和私钥加密,Hash 等函数可由第三方提供或用户自己开发;
3) USB key 证书和本端 E 语言模板要发布到反向给隔离装置;

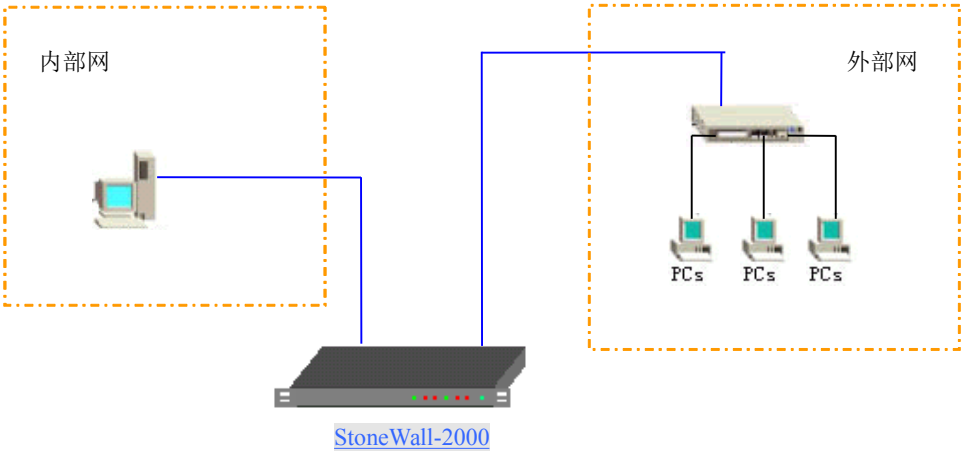
2.15 典型应用

StoneWall-2000 网络安全隔离设备（反向型）的应用可分为比较典型的三种：

2.15.1 计算机和计算机主机之间



2.15.2 计算机网络和计算机主机之间



2.15.3 计算机网络和计算机网络之间