

# 企业信息内网的“大禹治水”

唐浩杰

(江苏省电力公司常州供电公司, 江苏省常州市局前街 27 号 213003)

**摘要:**对绝大多数人而言“网络防水墙”这一概念也许远不像“网络防火墙”那样被人们所熟知,在谈及信息安全时,我们更多的只是讨论来自外部的威胁、渗透与窃取,对于我们内部存在的一些隐患却往往视而不见。列宁曾经说过堡垒最容易从内部攻破,这句至理名言同样适用于信息安全。

水无色无味无形,无孔不入,像极了企业内部的信息安全隐患,明明存在却最容易被忽视,就好像我们常说的“灯下黑”一样,需要采取严密措施加以防范和控制。在企业信息化建设日益深入的今天,复杂的网络环境和信息数据安全等问题无一不困扰着无数的信息人,面对如此严峻的形势,“网络防水墙”的异军突起让原本尴尬的局面又有了新的突破,名不见经传的“网络防水墙”正成为信息安全市场一颗新星,冉冉升起。

**关键词:**网络防水墙;信息安全;网络控制;违规外联;弱口令

## 0 引言

谈到信息安全,我们首先想到的是病毒、黑客入侵等,然而更多时候引发的安全问题源自我们自身内部,俗话说的好:日防夜防、家贼难防。在企业内部人员通过计算机网络对信息资料的窥探与窃取会给企业造成可能无法估算和弥补的损失,而这也是影响企业信息网络安全的重要途径之一。从技术上讲,内部人员更容易辨识信息存储地,可以轻易的获得核心涉密资料;相对而言,黑客想要获取这些资料信息则比较困难,他们既要突破像防火墙、核心路由 ACL 策略等重重技术安全加固关卡,还要从海量的信息中找到他们所需要的有价值的信息,可谓是困难重重。

古有大禹治水造福百姓,在现在信息化网络高速发展的现代文明,为了保障企业内部信息安全,防止企业内部资料像洪水一样外泄,我们能不能效仿“大禹”通过一些技术手段来对网络起到监管治理的作用呢?接下来,就让我们来认识一下今天的主角—网络防水墙。

我们将通过以下几个方面来认识一下网络防水墙对于企业信息安全所发挥的重要作用与意义。

## 1 网络防水墙的工作原理

网络防水墙(注:后文中一律简称防水墙)是综合利用密码、访问控制和审计跟踪等技术手段,

对涉密信息、重要业务数据和技术专利等敏感信息的存储、传播和处理过程实施安全保护的软硬件系统。

从名称上,网络防火墙和防水墙是一对非常类似的名字。我们知道,防火墙通过软硬件隔离来防止外网对企业内网进行攻击,它被动地检查所有流过的网络数据包,以阻断违反安全策略的通信。

防火墙的工作都基于一个基本假设:它位于内外网的接入点,并且内外网间不存在其它旁路,正是基于这个假设,防火墙才成为内网的保护神。但是,很明显,对于内部的安全问题,防火墙无能为力。防水墙由此应运而生,它是一个内网监控系统,处于内部网络中,随时监控内部主机的安全状况。如果说防火墙是指防止外部威胁向内部蔓延的话,防水墙就是指防止企业内部信息的泄漏。可见,防水墙是对这样的内网管控系统非常形象的一种称呼。

### 1.1 防水墙主要由三层结构组成

#### 1.1.1 高层的用户接口层

以实时更新的内网拓扑结构为基础,提供系统配置、策略配置、实时监控、审计报告、安全告警等功能。

#### 1.1.2 低层的功能模块层

由分布在各个主机上的探测器组成。

#### 1.1.3 中层的安全服务层

从低层收集实时信息,向高层汇报或告警,并

记录整个系统的审计信息,以备查询或生成报表。  
在此结构上主要具有以下五大功能:

(1)信息泄漏防范,防止在内部网主机上,通过网络、存储介质、打印机等媒介,有意或无意的扩散本地机密信息;

(2)系统用户管理,记录用户登录系统的信息,为日后的安全审计提供依据;

(3)系统资源安全管理,限制系统软硬件的安装、卸载,控制特定程序的运行,限制系统进入安全模式,控制文件的重命名和删除等操作;

(4)系统实时运行状况监控,通过实时抓取并记录内部网主机的屏幕,来监视内部人员的安全状况,威慑怀有恶意的内部人员,并在安全问题发生后,提供分析其来源的依据,在必要时,也可直接控制涉及安全问题的主机的 I/O 设备,如键盘、鼠标等;

(5)信息安全审计,记录内网安全审计信息,并提供内网主机使用状况、安全事件分析等报告。

综上所述,防水墙是对防火墙、VPN、入侵检测系统等多种安全设备,所提供安全服务的有效补充。对整体安全系统来说,它也是不可或缺的一环。

## 2 防水墙的体系结构

完整的防水墙系统由三部分组成:

- (1)防水墙服务器
- (2)防水墙控制台
- (3)防水墙客户端

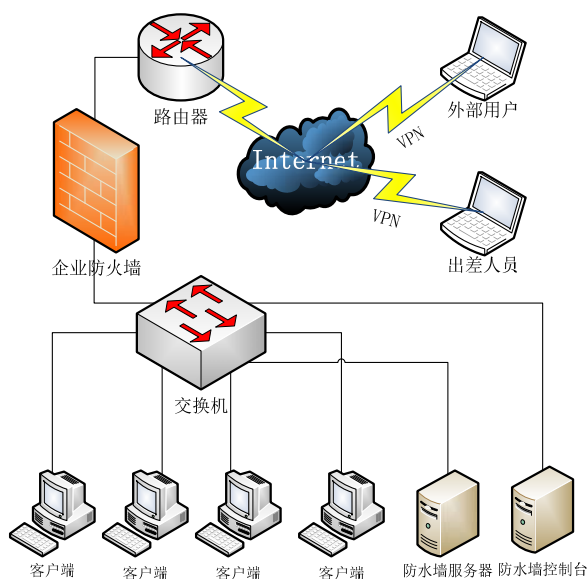


图 1 网络防水墙体系结构示意图

### 2.1 防水墙服务器

包括服务器端软件和支持数据库,是防水墙系统的核心部分。通过安全认证机制,建立与客户端的连接,实现对客户端系统的配置、策略制定下发推广、资产管理、操作审计等功能。

### 2.2 防水墙控制台

它是系统管理员、操作员、审计员等和防水墙系统交互的图形界面,实现系统管理、参数配置、策略管理和系统审计等功能。控制台采用分权分级的授权模式,严格限制对敏感信息的访问权限,以提高系统的安全性,保证信息安全。

### 2.3 防水墙客户端

它是隐藏于客户机内部的“安全哨兵”。它强制执行来自服务器的安全策略,根据安全策略监测客户端用户的行为。客户端软件采用了严密措施,防止本地用户自行卸载、关闭监后台控程序。

其中,防水墙控制台和客户端软件,可实时从服务器端获得最新版本,实现远程自动升级。

## 3 防水墙系统的设计理念

防水墙系统的设计理念是保护用户敏感信息不被非法外传、防止泄密事件发生,从而保证内部安全。它主要从以下五个方面来保障内网信息安全:

### 3.1 失泄密防护

信息外传途径主要有网络传输、移动存储带出和打印到纸介质文稿三种情况。防水墙系统针对这三种泄密途径都做了全面的防护,可以根据实际情况选择启用或禁用,还可选记录日志以备事后追踪。另外,防水墙系统还能够根据策略“启用”和“禁用”主机上可能造成泄密的外设接口,作为实施失泄密防护在硬件层次上的辅助手段。

### 3.2 文件安全服务

文件安全服务提供了对敏感文件的加解密安全防护,充分利用对称和非对称算法的优点对文件和密钥进行管理。为了保证敏感信息不被非法解读,防水墙系统使用了加密域的概念。加密域是一组防水墙系统用户的组合,每个文件在加密时均选择加密域,只有处于选择的域内的用户才能进行解密阅读。有效地防止了文件在传输途中可能造成的泄密,也防止了电脑丢失可能做成的泄密事件的发生。

### 3.3 运行状况监测

对受控主机，监控其历史运行状况。包括：用户删除文件、系统服务，屏幕截取等记录，方便系统管理员查看管理。是计算机安全保密的有效措施之一。

### 3.4 系统资源管理

系统资源管理功能用于收集受控主机上的软硬件信息，并上传至服务器作为初始资源信息备份。系统管理人员可以随时获得所管理部门的主机的系统资源信息。完整的系统资源管理信息包括：系统信息、硬件信息、用户和组等信息。

### 3.5 扩展身份认证

接管身份认证。如果接管 Windows 身份认证，只需输入合法的防水墙用户名和强口令（数字+字母+符号 长度满 8 位）即可登录 Windows 系统。

## 4 防水墙构筑信息安全保密解决方案

防水墙系统的主要功能，对系统内部进行如下几方面防护，可以最大限度的保障系统的安全。

### 4.1 身份验证机制

用户身份的鉴别和防护，是保证计算机系统安全的第一道防线，众多失泄密事件都是由于用户身份认证的不严格而引起的。

防水墙系统提供了自身的身份验证系统，用户要登录到防水墙客户端时，除需要提供操作系统用户名和口令外，还需要提供防水墙用户名和口令，用户口令长度为 8 位以上的数字、字母加符号的组合，确保不发生弱口令事件，保证了口令的安全性与可靠性，同时口令的验证与存放均使用哈希函数中的 MD5 算法，有效防止暴力破解。

### 4.2 访问控制体系

完善的访问控制体系应包括控制单位内部员工的访问操作，即采取主动的方式，尽可能多的封锁住各种可能造成失泄密的渠道，防止由于内部员工的有意或无意的操作，造成泄密事件的发生。

防水墙系统提供了三种访问控制体系，基本涵盖可能造成泄密的各种途径：

#### 4.2.1 网络访问控制

可以有效的控制终端用户的网页浏览、网上文件上传下载、Email 控制、Modem 拨号、Telnet、网络共享等网络操作。

#### 4.2.2 接口控制

可对计算机的 USB 接口、1394 接口、串口、并口等 10 种外设接口进行控制，使终端用户无法使用相应接口的硬件设备，所控制的 10 种接口基本涵盖所有可能造成失泄密的情况。

#### 4.2.3 打印机控制

对系统内部用户使用打印机进行控制，可根据需要设定禁止使用、自由使用记录日志、自由使用记录影像等不同程度的策略。

### 4.3 “违规外联”控制

不难看出，通过上面讨论的“网络访问控制”和“接口控制”，可以严密防止单位内部“违规外联”情况的发生。因为通过禁止网络访问或通过禁止可能访问网络的外设接口，就有效地控制了“违规外联”。

### 4.4 设备密级标识

信息是分密级的。在一个合格的安全体系中，不同密级的信息必须保存在不同的位置或不同的存储介质上，这样可以最大限度保障信息的安全。为此，需要将网络体系中所有的计算机系统、可移动介质设置为不同的密级，用以存放相应密级的数据，只有具备相关权限的人员才能对涉密信息进行访问。

防水墙系统提供专门的授权模块，对计算机终端或移动存储介质等设定相应的密级标识。不同密级的计算机执行不同密级的策略，接受不同程度的管理监控。在防水墙系统中，密级标识从低到高级分别为：普通、秘密、机密、绝密。而密级标识本身使用加密等措施进行有效存储。

### 4.5 移动存储介质的有效管理

存储介质（如 USB 盘、移动硬盘等）作为企业核心机密和敏感信息的载体，实现对它们安全、有效的管理是保证企业信息安全的重要手段。防水墙系统提供了可信移动存储介质管理功能，通过将移动存储介质划分密级、加密存储等技术手段，可以有效防止移动存储介质在计算机上跨密级使用。可信移动存储管理功能是对设备密级标识的充分应用，防水墙系统的可信移动存储功能中的密级访问控制包括：

（1）高密级移动存储介质不能在低密或者普通计算机上使用；

（2）涉密移动存储介质不能在非涉密计算机上使用

（3）低密级移动存储不能（或者只读）在高

密级计算机上使用

(4) 非授权的移动存储介质不能在涉密计算机上使用

(5) 即使密级相同,也只能在用户或者计算机得到许可的情况下才能够使用

防水墙系统中的“可信移动存储介质管理系统”充分利用信息保密、访问控制、审计等技术手段,对企业移动存储设备实施安全保护,使企业信息资产、涉密信息不能通过移动存储设备非法泄漏,用技术的手段,真正实现移动存储设备信息安全的“五不”原则,即:进不来、拿不走、读不懂、改不了、走不脱。

“进不来”,是指外部的移动存储介质拿到单位内部来不能用;“拿不走”是指单位内部的存储介质拿出去使不了;“读不懂”是指只有授权的人才能解密阅读,任何未经授权的人打不开其中的文件,这意味着即使存储介质丢失也不会造成泄密;“改不了”是指其中的信息篡改不了;“走不脱”是指系统具有事后审计功能,对违反策略的行为和事件可以跟踪审计。

#### 4.6 安全审计

防水墙系统具有“事前预防、事中控制、事后审计”三大特征,在信息保密的各个阶段实施对敏感信息的强有力的保护。防水墙系统提供的“黑匣子”和“审计平台”,能够快速对出现的安全事件进行审计。所谓“黑匣子”,是指安装于防水墙客户端、用于记录用户操作的加密文件系统,假如发生泄密事件,具有“安全官”(系统最高使用权限,如保密委员会授权的人员)权限的用户可以从控制台导入泄密主机“黑匣子”,使用防水墙黑匣子分析仪对其进行分析,以追究泄密责任。审计平台主要针对历史性的数据库备份文件和日志文件进行对应审计,进行更全面的问题追责。

从上面的介绍可以看出,防水墙系统的受控主机集合构成了一个相对独立的“内部安全体系”,有时我们也称其为“防水墙系统安全域”。域内的主机

是受到防水墙策略的严格控制的,这些主机的用户行为是受到监控的,其泄密后果是可以追查和审计的。

#### 4.7 非法主机控制

以上六种防护措施均是针对“防水墙安全域”内部用户的。对于接入到“防水墙安全域”中的外部主机(如用户很容易地将笔记本电脑接入到“防水墙安全域”中)如果它没有安装防水墙客户端软件,不接受防水墙系统的监控,会对企业的安全体系造成破坏,造成失泄密事件的发生。防水墙系统的“网络巡逻员”可以对连接到网络中没有安装防水墙的“非法”主机进行检测,及时报告非法主机的接入,并可根据策略对其进行报警与阻断。

### 5 结论

网络防水墙作为目前国内日趋成熟的企业内网信息安全管控系统,政府机关、军工企业、涉密的企事业单位,通过应用部署该系统,都能很好的满足内网信息安全防护的需要,切实降低信息泄密的风险,同时又提高了单位的工作效率,具有良好的应用效果。目前上千家用户的实践经验表明:基于防水墙系统构筑信息保密安全体系和解决方案,是切实可行的,是新时期保密工作的有力武器。

#### 参考文献:

- [1] 中软通用产品研发中心“内部信息泄漏的守护神&中软防水墙”[Z].
- [2] 陈尚义,周显敬,吕巍.可信移动介质解决方案[Z].中软,2005(30):25-26.
- [3] 上海山网安 防水墙系统技术白皮书[Z].
- [4] 北京北信源软件股份有限公司.内网安全管理系统解决方案白皮书[Z].

#### 作者简介:

唐浩杰(1981-),男,江苏常州人,经济员,从事信息系统检修维护工作,E-mail: donald\_tj@qq.com.