基于网络边界的安全防护研究

王　森

（中国地质调查局地球物理调查中心，河北 廊坊 065000）

摘　要　现代企事业单位高度依赖面对全球开放与互联互通的数据信息通信网络，而网络环境的安全是网络用户高度关注的问题。从某种意义上来说，互联网边界管理工作水平将影响到企事业单位的持续健康稳定发展。国家大力促进信息化网络化发展的时代背景下，我国大部分企事业单位在管理及办公方面已普及运用网络通信技术，通过各类业务网络可以进行信息之间的安全可靠传播与及时共享，促使工作效率得以有效提高。在企事业单位对网络进行运维管理服务过程中，很多关于本单位的内部信息都会录入到各类终端或存储服务器中，而单位内部网络环境面临网络安全威胁时就可能会导致机密信息的泄露，会影响一个单位的稳定安全发展。基于此，本文对企事业单位基于网络边界的安全防护问题进行了扼要分析，并提出了相应的运维管理措施，旨在对提高企事业单位网络环境的安全有所裨益。

关键词　网络边界安全防护　企事业单位　恶意攻击　防火墙技术　AC

中图分类号：TN915.08　　**文献标识码**：A　　**文章编号**：1007-0745(2022)12-0016-03

计算机网络由于其运行速度快，办公自动化程度高，因而在现代化办公中被广泛应用。但是由于网络具有开放性的特征，使得网络边界存在的安全隐患一直都无法得到彻底的解决。而如果企事业单位网络边界被攻破，不仅会致使本单位的基础信息遭受泄露风险，同时本单位的各种内部独有信息或是机密信息也会面临极大的风险，这将会严重损害个人及本单位的整体利益。所以，我们有必要加强企事业单位网络边界安全管理和运维工作，从建设管理制度再到实际操作执行，每一个环节都要有健全、完备的防护措施，只有这样，才能确保企事业单位内部信息、资料的安全性。

1 企事业单位安全管理与网络边界安全

从信息安全的角度来看，网络边界的安全不可能脱离明确的管理制度而单纯用技术去实现，其安全功能与扩展性能很大程度上决定了一个单位网络的可靠性与成熟度。

从根本上来说，技术最终是服务于管理的。在以往的管理实践当中发现，不少基层技术人员往往只是习惯用点对点的方式来对网络边界的安全（乃至整个单位信息资产的安全）进行外科式的、针对单个事件性的处理，却比较容易忽略技术与管理之间所存在的依存关系，这样就难以避免地陷入重技术而轻管理的思维模式，这是需要尤其注意的环节，网络安全是需要人防加技防的，而人防同样是重点[1]。

2 影响网络安全的主要因素

2.1 网络资源的共享性

资源共享是现代互联网最主要的作用，它包括软件共享、硬件共享及数据共享。所谓应用软件数据共享，是指在计算机网络内的所有使用者都能够实现共享计算机中的所有软件资源，包括各种语言程序、应用程序和服务程序。硬件数据共享，是指可在互联网进行的对数据处理资料、存储资源、输入输出资料等硬件资源的数据共享，尤其是对某些先进技术和贵重的电子设备，如巨型计算机、大容量的存储设备、画图仪、高分辨率的雷射印表机等的共享。数据共享是对网络范围内的数据共享。网络信息内容包罗万象，无所不有，可供每一位上网者查阅、咨询、下载。

2.2 网络的开放性

互联网是开放式的，能够随意使用，并且没有了时间与空间的约束，没有了地域间的距离限定，所有人都可以随意进入互联网，只要遵循规定的网络协议即可。同时，相对而言，在互联网上所有人都可以享受创作的自由，任何的信息流通都不受限制。网络平台的运行都是由所有使用者共同协调和决定，所以网络平台的每个使用者都是自由平等的，而正是由于这种开放性也使网络平台上的使用者之间不具有身份的界限，因为所有人入网就是用户。同时网络平台更是一个无国界的互联网虚拟自由王国，所有人都可以实现在网络平台上资讯的传递自由、用户的言论自由、

用户的使用自由 [2]。

2.3 网络系统设计的缺陷

实体的服务器和网络终端承载着一个单位的网络的基本构架。笔者在这里所谈论的是基于网络边界面临的安全问题，这是不同单位不同主体之间的信息交流，就像两个城邦之间需要具有护城河和城墙一样，但这又会导致信息传递、储存条件变得更加复杂。网络设计是指网络拓扑设计以及各种网络边界防护装置的建设计划。重要信息、各类网络操作系统等都可能直接产生安全隐患。一种正确的网络拓扑设计应该可以在节约资源的情况下带来很高的安全性，不当的网络拓扑设计将可能成为网络安全的潜在风险 [3]。

2.4 恶意攻击

恶意攻击是一个单位网络边界防护面临的大量极其危险的安全问题，匿名的攻击者利用其高超的技术手段及利用木马病毒、蠕虫病毒等手段通过一些不常用的、特殊的协议端口入侵单位内部的计算机及服务器，从而可以恶意篡改单位门户网站等或窃取单位内部信息，瘫痪内部网络，为单位造成损失。

2.5 人员网络安全意识淡薄

很多企事业单位的从业者依旧存在思想认知薄弱、网络安全防护警惕度不高的思想，极个别者对网络安全的重要性并没有进行正确认知，认为网络安全问题是网络管理员的分内之事，结果就会出现单位员工参与网络安全的积极性不高、保密意识不强、忽视出现的网络安全隐患的现象。久而久之，不仅会出现整个单位安全参与性不高的情况，而且还会给整个单位的安全发展留下诸多隐患。

3 传统的网络边界安全防护措施

3.1 构建完善的网络安全管理制度

企事业单位应建立与网络安全有关的制度，以明确网络安全参与者的职责和权利，并用来对网络参与者进行有效规范。指导单位互联网参与者根据自己单位的规定做好单位日常用网管理工作，为提高企事业单位安全管理水平打下了良好的现实基础。同时，将相关规定列入企事业单位每日网络安全管理检查重点事项，通过定期开展的安全检查结合个人自查工作，为企事业单位创造一个安全的、具备极强人防意识的、高效的上网环境。

3.2 防火墙技术

防火墙是指介于网络设备与服务器、网络群体终端与外部互联网之间，用于控制来自外部的匿名用户访问本地内局域网或控制本地局域网用户访问外部互联网的一类最基础的网络安全装置，是网络边界最外围的第一道屏障，所以说，如果不安装防火墙，每一个运行中的网络设备都是处在“裸奔状态”下的。因此在连接互联网之后，上网环境的安全性除要考虑各种病毒和操作系统的健康特性以外，更主要的是要防止匿名入侵者的非法攻击，而目前防范的安全措施也大多通过防火墙技术来实现。通过部署防火墙，可以使一个单位内部网络的稳定性获得很大的增强，并通过过滤策略减少风险。网站的安全策略也需要借助防火墙来加以加强，通过以防火墙为内核所组成的网络边界安全框架，能将所有可以访问的用户 IP、使用的端口、执行的网络进出策略进行精确的配置，并对所有的可能遭受到网络攻击的端口进行禁用。

3.3 上网行为管理技术（AC）

上网行为管理设备可以对内部员工的上网行为进行有效控制，在单位的网络边界上部署上网行为管理设备可以提高工作效率，有效降低非工作上网行为，保障网络资源的合理使用；同时能够减少安全风险，避免病毒、恶意代码给单位带来的潜在风险；提高网络的安全性，便于加强管理。部署上网行为管理设备适用于以下场景：

1. 接入安全场景。接入安全场景下可实现终端资产识别和分类管理、多方式的接入身份认证、终端安全状态检查、终端入网后行为审核、终端行为权限管控等，实现全流程的接入安全管控，帮助单位防范非法身份接入、病毒横向传播和越权访问行为等风险。

2. 业务行为安全场景。业务行为管理场景下，可实现自动识别梳理服务器和业务类型；业务访问和外联的深度审计；业务数据多维度分析，状态实时可视；智能识别大量下载、账号爆破等风险行为，异常事件及时告警。

3. 涉密风险分析场景。涉密风险分析场景下，对网络外发、终端外联、业务访问全方位审核和管控，并可通过关键字搜索、文件搜索、OCR 图片识别等方式追溯泄密行为记录，保障用户内部信息资产安全。

3.4 入侵检测技术

面对日渐加强的网络安全风险，作为对防火墙及其有益的补充，入侵检测系统可以协助安全系统迅速地发现网络攻击的产生原因，并扩展了网络系统管理者的安全管控能力（包含安全性评估、监控、进攻辨识和反应），进一步增强了网络安全基础架构的整体性。入侵检测技术、入侵检测方法很多，如采用专家管理系统的入侵检测技术、采用神经网络的入侵检测技术等。目前，一些入侵检测技术在应用层入侵分析中也已经应用。入侵检测通过进行下列工作来完成：（1）监控、分析数据和操作系统活动；（2）系统构造和弱

点的审计；（3）研究揭示已知入侵的行动方式，并向有关人员告警；（4）对不同行为类型的大数据分析；（5）研究重要用户的大数据，分析文档的安全性；（6）对应用的审核与研究，并发现重要用户违反安全策略的行为。目前的入侵检测系统的功能主要有：（1）对应用和网络行动的监控和分析；（2）网络设计及其脆弱性数据分析和审核；（3）异常行为模式的统计分析；（4）对信息系统和数据文件的安全性检测和评估；（5）操作系统的安全审核和控制；（6）对攻击方式的确定和应答，如断开连接、记录时间和告警等。可以有效地提升网络主机的操作系统安全和物理安全，为防火墙技术的发挥提供有力的基础保障[4]。

3.5 网闸

网闸全称叫做安全隔离与信息交换系统。由于对两台单独的内部主机系统都采用了网闸加以分隔，使系统之间并不具备互相通讯的物理链接、逻辑连接和消息传递模式，不具备直接依据协议实现的信息交流功能，而只是以数据文件方法实现的无协议摆渡。这样，网闸在物理上隔绝、抑制了对内网之间有着潜在入侵可能性的任何连接，从而使得外界攻击者无法直接进入、攻击或摧毁内网，从而保证了内部主机的安全性。

3.6 及时进行系统升级和系统改造

要经常性的采用目前最贴合现实的、最先进的技术，及时进行系统升级和系统改造，扩宽网络平台范围。及时维护和更新系统，及时补漏，提升抵御非法入侵和各类病毒的安全能力。

3.7 提高人员网络安全意识

在日常网络安全管理工作中，要进行安全教育、技术培训等工作，使每个员工都意识到安全保密工作的重要性，并提高保密意识，增强操作能力，以减少或防止人员在日常工作过程中发生的各种安全事故。

4 网络边界防护技术架构和防护办法

网络边界防护安全系统的基本架构应先由安全系统架构阶段转入被动防护，然后到主动防御阶段。一个企事业单位网络安全的基础就是单位网络安全系统架构，它能够反映单位网络结构是否牢固，被动防御是通过消耗匿名攻击者的攻击资源和增加其进攻时间的手段，而主动防护则是对被动防御功能的补充，用以抵御更加复杂的高级威胁。概括起来就是，在面临未知威胁下的网络边界防护系统里，要在保证网络结构坚固的基础上，进一步延长防御纵深，同时不断增强监测、分析与响应能力。建立完整的边界安全防护系统框架，需要通过采用各种技术手段同时结合增加硬件与各种安全功能的方法，才可以建立起高效的防御系统。网络边界安全防御系统框架在功能结构上，主要包括了网络边界端的接入管理和网络边界安全防护。利用防火墙和上网行为管理设备建立了身份验证的体系，用于实现对设备和认证用户的边界接入、隔离控制；利用数字签名和访问控制等技术，实现对用户访问权限的管理并避免了伪造、否认、冒充等问题；每个进出网络边界的数据流经过整个体系的各类安全设备的监控与管理，以此达到边界内外数据的安全可控交换。

联动防御，消耗攻击者资源：网络边界安全防御有时候之所以不能产生应有的成效，就是因为传统的边界防护技术只是采用静态特征的方法加以防御，而对于日益革新的入侵技术与手段则会变得有点力不从心。若能在网络边界上增强各类威胁检测的手段与精度，就能够做到提高入侵的进攻难度。目前，不断革新换代的防火墙技术增加了关于应用识别、数据鉴别、信息辨别、威胁鉴别、资产辨别、地址鉴别的功能，这些措施也极大地增强了防火墙自身的安全水平，可看作是增加了网络边界的城防的作用。但仅仅具有基本的防御能力显然是不足的，所以仍需依托整个防护系统框架的同时继续加深战略纵深防护体系，也就是增加了更多的检测威胁手段，并利用了多种安全产品、设备之间的协作联动，以及利用威胁情报等外部的能力，通过围绕防火墙技术提升了整个系统的安全防护能力，如此就组成了一个新的、可以更大幅度消耗攻击资源的大纵深网络边界安全防护体系。

5 结语

综上所述，互联网是企事业单位工作中不能替代的工具，但因为互联网具有非常大的开放性，使用互联网会涉及信息技术、硬件、安全管理和法规制度等多个领域，所以网络边界的安全管理是一个非常繁复的系统工程，不只是依靠防火墙、杀毒软件等软件防护，还需要加强人员的防护意识，做好链路维护与管理工作，形成有效的安全体系，从而打造一个便捷、安全的网络系统，提升企事业单位管理效率，促进企事业单位健康稳定发展。

参考文献：

[1] 赵朔，潘桉卿 . 新型网络边界防护技术研究 [J]. 信息通信 ,2017(08):57-58.
[2] 刘伟 . 浅谈计算机网络边界安全的防护和管理 [J]. 通讯世界 ,2020,27(03):212-213.
[3] 杨功彬，赵凤芹 . 浅析事业单位计算机网络安全维护工作 [J]. 黑龙江科技信息 ,2016(19):174.
[4] 许雪礼 . 计算机网络边界安全防护与管理策略探讨 [J]. 探索科学 ,2020(06):197.