内容分发网络技术在高校网络安全防护中的应用研究

李大盼

（河南经贸职业学院，河南 郑州 450003）

摘 要 本文针对高校校园网络面临的安全挑战，深入探讨了内容分发网络（CDN）技术的原理和优势，并将其与Web应用防火墙（WAF）相结合，提出了一种创新的网络安全解决方案。通过在校园网络中的实践应用和详细的数据统计分析,本文证明了该技术在提升网络访问速度、降低服务器负载、增强数据传输安全性方面的显著效果。

关键词 高校；网络安全；内容分发技术

中图分类号：TP393.08 **文献标志码**：A **文章编号**：2097-3365(2024)08-0031-03

信息技术的持续进步已将高校的教务管理、教学活动和科研工作带入了信息化时代。校园网络作为支撑这些活动的核心，其安全性和可靠性至关重要[1]。然而，校园网络在向互联网用户提供服务的过程中，不可避免地暴露于各种安全威胁之下，包括恶意攻击、数据泄露和网络诈骗等，这些风险对校园信息安全构成了巨大挑战[2]。为了有效防范这些风险，确保校园信息系统的安全性，本文提出了一种结合内容分发网络（CDN）技术和Web应用防火墙（WAF）的综合性安全解决方案。该方案不仅通过CDN技术优化了网络流量分配，提升了访问效率，而且利用WAF技术增强了对恶意请求的识别和防御能力。此外，本文还提出了一系列安全管理措施，构建一个多层次、全方位的安全防护体系。这些措施的实施，旨在全面提升校园网络的防御能力，保障高校信息化建设的顺利进行。

1 内容分发网络技术

1.1 技术简介

内容分发网络（CDN）作为一种高效的网络架构，其核心优势在于通过分布式的缓存服务器网络，实现资源的快速分发和访问。这种架构不仅减少了源服务器的负担，还通过智能路由和负载均衡技术，确保用户能够以最短的延迟获取所需内容。当用户发起请求时，CDN的全局负载均衡系统会评估用户的地理位置、网络状况以及服务器的负载情况，从而选择最优的缓存服务器来响应请求[3]。此外，CDN还具备强大的容错能力，即使某个节点发生故障，系统也能迅速切换到其他可用节点，保证服务的连续性和稳定性。这种智能调度和快速响应机制，使得CDN在处理大规模并发访问时，依然能够保持高效和稳定的表现。通过这种方式，CDN极大地提升了用户体验，尤其是在视频流媒体、在线游戏和大规模在线教育等对速度和稳定性要求极高的应用场景中，CDN的作用尤为显著。

1.2 基本工作原理

CDN，即内容分发网络，是一种通过将内容缓存到离用户更近的服务器上，来提高用户访问速度和网站可靠性的技术。其基本工作原理可以概括为以下几个步骤：

用户通过浏览器发起对特定网站的访问请求，该请求首先到达本地域名服务器（Local DNS Server）。

本地域名服务器检查缓存中是否已有该网站的访问记录。如果本地域名服务器缓存中没有记录，它会向上游的授权域名服务器（Authoritative DNS Server）发起查询请求。

授权域名服务器接收到查询请求后，会根据其配置的策略对访问地址进行解析。

授权域名服务器将解析得到的别名IP地址返回给本地域名服务器。这个别名IP地址指向的是CDN网络中的一个节点，该节点可能在地理位置上更靠近用户，从而减少数据传输的延迟。

本地域名服务器将解析得到的IP地址返回给用户，用户浏览器随后使用这个IP地址向CDN节点发起资源请求。

CDN节点接收到资源请求后，会根据缓存策略和内容的可用性，向用户发送请求的数据。如果节点上已有缓存的资源，它将直接提供服务；如果没有，节点会从原始服务器获取资源，然后再提供给用户。

通过这一系列的步骤，CDN能够确保用户即使在网络拥堵或者服务器负载较高的情况下，也能快速、稳定地获取所需内容。此外，CDN还能够提供额外的安全防护，比如DoS攻击防护，进一步提升网站的安全性和可靠性。

1.3 技术优势

由于节点部署广泛，可分摊处理流量，CDN技术极大地提高了静态资源的命中率，使得源站带宽压力大幅下降[4]。如果访问需跨运营商，由于域代码不同，数据往返速度会降低，影响用户访问。遇到此类情况，CDN会根据就近访问的原则，将用户请求就近分配到边缘节点，减少访问反应时间，提高访问效率，增强用户体验。互联网经常会攻击校园网络，占用源站资源，影响用户的正常使用。通过CDN技术，攻击被分散到各个节点，降低攻击影响，提升安全属性。

2 内容分发网络技术应用

2.1 CDN构建方案

内容分发网络（CDN）的构建方案是确保网络高效、稳定运行的基础。在本节中，我们详细描述了CDN的构建流程。以下是对CDN构建方案的进一步补充：

在域名配置阶段，除了添加加速域名和输入网站备案号外，还需考虑域名的安全性和稳定性。同时，域名的DNS配置也需要进行优化，以支持快速的域名解析和故障转移。

在源站设置方面，除了基本的回源Host、协议、端口和地址设置外，还需要考虑源站的负载均衡和冗余设计。通过设置多个源站，可以在一个源站发生故障时，自动切换到其他源站，从而保证服务的连续性。

对于缓存规则的设置，除了主页缓存、文件名后缀和目录缓存外，还可以根据内容的更新频率和访问模式，定制更精细化的缓存策略。

最后，在用户请求重定向的过程中，除了将用户请求指向CNAME外，还可以通过智能DNS解析技术，根据用户的地理位置和网络状况，选择最佳的节点进行内容分发，从而进一步优化用户的访问体验。

2.2 保护源站服务器

保护源站服务器是CDN架构中的重要环节。在本节中，我们进一步阐述了在节点资源不足时，如何通过智能路由机制，将用户请求转发至源站服务器，从而避免用户直接访问源站，减轻源站的负载压力。以下是对保护源站服务器策略的进一步补充：

在节点资源不足的情况下，CDN系统可以通过智能算法，动态调整资源分配，确保用户请求能够快速得到响应。同时，CDN还可以通过内容预热机制，预先加载热门内容到节点，减少源站的访问压力[5]。

2.3 攻击预防

校园网络受到来自互联网的攻击对种多样，其中DDOS是一种常见的方式。DDOS发起攻击时，通过增大访问流量，占用网络带宽，当占用的带宽超过最大承受能力时，网络则会发生瘫痪。CDN将攻击分散到各节点，减轻被攻击的服务器的压力，给维护人员充足的时间进行修复。

2.4 CDN与WAF相结合

WAF能够按照既定的策略对网络系统进行防护，识别攻击、深度检测流经Web应用的流量[6]。与传统防火墙相比，WAF可对Web应用协议流量进行智能分析和实时监测识别，可以有效地解决各类问题，保护网络信息系统。

将CDN技术与WAF技术相结合，如图1所示，形成校园网络的安全防护系统。当黑客对校园网络发起攻击时，首先由FW抵挡低层攻击。对于DDOS攻击，则由CDN将其分散，减轻服务器压力。再通过WAF拦截剩余的少量DDOS攻击：WAF对用户请求进行扫描并校验网络包，再采用检测HTTP流量的方式将包含DDOS攻击的请求进行阻断。

3 应用结果

本文将CDN技术运用到校园网络，缓存加速校园网络的静态资源，以实现网络安全防护。为了分析CDN技术的应用效果，对校园网络进行用户分析、热门分析和用量分析。

（1）用户分析。校园网络管理员通过用户分析，可以统计访问运营商分布和用户区域分布等信息，并以此为依据，对回源节点位置进行分配调整，实现访问效率高效化，提升用户使用体验；（2）热门分析。校园网络管理员通过热门分析可以掌握热门回源URL和热门URL。当URL出现访问异常时，网络管理员可以及时的发现，并采取措施调整URL的访问策略；（3）用量分析。校园网络管理员通过用量分析能够查看源站的访问量、状态码、带宽和流量、用户请求数、CDN节点的回源情况、浏览量和字节命中率等信息。

为了了解运行情况，对2022年6月23日至6月29日校园网络的访问请求数、状态码、访问流量进行统计分析。当受到攻击时，CDN就会发出错误的相应状态码，通过WAF管理员对相应的IP进行封锁和阻断。

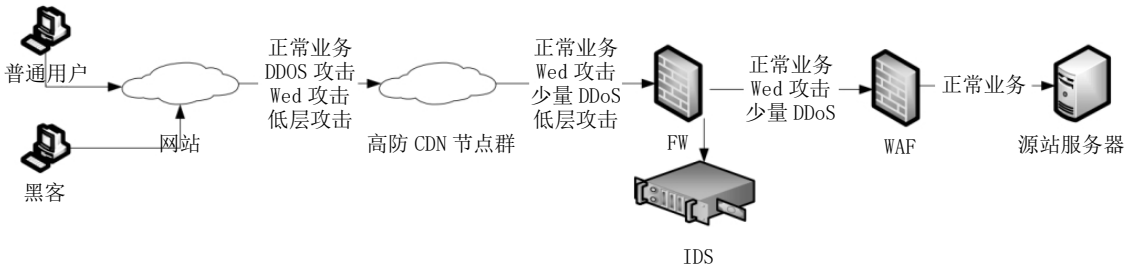

图 1 CDN 和 WAF 结合关系图

根据统计结果，6 月 23 日至 25 日的访问请求数约为 3 000 次，较为平稳，且访问时间较为固定。6 月 27 日时，访问请求数突然增加，这是由于网络选课开始。访问流量与访问请求数基本成正比。通过状态码统计结果，校园网络状态码主要为 2XX。由于 27 日的访问请求数激增，开始出现报错情况，3XX 较多，4XX 次之，5XX 最少。由此可知，虽然 URL 出现重定向问题，但校园网络仍然稳定运行，未受到严重影响，因此也不需要调整策略。

4 安全管理措施

除了采用 CDN 与 WAF 联合防护技术，本文还制定了相应的安全防护措施。

4.1 完善管理制度

结合学校实际情况，由分管领导主导、信息部门实施，制定相应的校园网络管理制度。该制度提出了校园网络安全管理的相关要求，明确了相应的责任，依据谁用谁负责、谁运维谁负责和谁主管谁负责的基本要求，建立管理体系。

4.2 开展安全运维服务

与安全服务公司签订运维服务协议，对校园网络进行安全运维和风险评估。此外，对信息资产开展安全加固、日志分析、安全巡查、扫描漏洞以及及时修复系统问题等维护。

4.3 闭环管理

保障条件、日常运行和技术防护是网络安全防护体系的三大方面。

1. 保障条件。除完善管理制度、开展安全运维服务外，还需加强人才培养和队伍建设、加固信息资产，编制切实可行的应急预案等，为校园网络的安全运行提供基本保障。

2. 技术防护层面。采用安全审计设备监测用户行为，例如：通过 Panabit 实现对用户的 DNS 管控、流量管理、HTTP 管控、连接数管理等；采用日志审计系统，对信息资产事件和安全设备进行统计，对校园网络行为进行监控。通过高防 CDN、防火墙、WAF 等针对 Web 服务器、IDS、IPS 等设备对上网流量进行监控管理。

3. 日常运行层面，网络管理员应加强预警监测，如遇问题，尽早进行处理，防止造成严重后果。并将问题向信息资产所属人员进行通报，对出现的问题及时整改，形成 PDCA 的闭环管理。

5 结论

1. 本文通过分析 CDN 的基本原理和技术优势，将 CDN 技术在校园网络安全防护中进行应用，明确了 CDN 构建方案、CDN 与 WAF 相结合模式。

2. 统计分析了 2022 年 6 月 23 日至 6 月 29 日校园网络的访问请求数、状态码、访问流量；通过这些数据，可以了解网络访问情况和运行情况，受到攻击时采取相应的措施。

3. 结合实际情况，制定了安全管理措施，包括：完善管理制度、开展安全运维服务和实行闭环管理。

参考文献：

[1] 王乐.基于WAF的高校信息系统HTTPS加密传输部署[J].网络安全技术与应用,2023(01):18-20.
[2] 张晶,李洪洋,张文婷,等.大数据背景下智慧校园网络数据安全研究[J].网络安全技术与应用,2023(01):76-77.
[3] 谢敏,于洪奇,杨征,等.浅析CDN技术及其在政务信息服务的应用实践:以自然资源部政务信息服务平台为例[J].自然资源信息化,2023(01):37-42.
[4] 何英,崔勇,罗巍.基于边缘CDN能力打造数字家庭终端ROM升级技术研究与实践[J].江西通信科技,2022(04):7-10.
[5] 王珏.基于数据挖掘的校园网络安全等级保护测评决策研究[J].电子技术与软件工程,2022(20):5-9.
[6] 张晓潮.校园网络的信息安全与体系结构优化分析[J].电子技术,2022,51(08):164-165.