

计算机网络架构的优化与安全性提升

张立波

(杭州市红十字会医院钱塘院区(杭州市第九人民医院) 杭州 310052)

摘要 在数字化时代,计算机网络承载着信息传输、商业交易、社交互动等关键功能。但随着网络攻击的日益频繁及数据泄露事件的不断增加,计算机网络的安全性问题变得尤为突出。文中探讨了如何通过优化架构设计与强化安全措施,如部署先进防火墙、入侵检测系统并实施访问控制,来应对复杂多变的网络威胁,提高了网络环境的安全性,为企业的持续发展提供了支撑。

关键词: 计算机;网络架构;网络安全

中图分类号 TN915.08

Optimization and Security Improvement of Computer Network Architecture

ZHANG Libo

(Hangzhou Red Cross Hospital Qiantang Campus (Hangzhou Ninth People's Hospital), Hangzhou 310052, China)

Abstract In the digital age, computer networks carry key functions such as information transmission, business transactions, and social interaction. However, with the increasing frequency of network attacks and the increasing number of data breaches, the security of computer networks has become particularly prominent. This paper explores how to optimize the architecture design and strengthen security measures, such as deploying advanced firewalls, intrusion detection systems, and implementing access control, to cope with complex and changeable network threats, improve the security of the network environment, and provide support for the sustainable development of enterprises.

Key words Computer, Network architecture, Network security

0 引言

在数字化时代,计算机网络被广泛应用于个人日常生活和企业运营,深刻地改变了人们的生活方式和工作模式。随着网络应用的广泛普及和技术的飞速发展,网络架构的复杂性和潜在的安全风险也日益凸显。网络架构的优化能有效提升网络性能,保障数据传输效率。通过合理设计网络拓扑,优化网络层次布局以及升级网络硬件设备,可以构建出高效灵活且健壮的网络架构,以应对日益增长的网络需求和挑战。

1 计算机网络架构

1.1 概述

网络架构是现代信息的基石^[1],其详细描述了网络的物理连接(如线缆、路由器、交换机等硬件设备的布局)及这些设备间如何通过逻辑规则相互协作,形成数据传输与信息共享的通路。网络架构包含了网络的拓扑结构,是各节点间的连接方式及形状(如星型环型和网状)。层次结构也是网络架构的一种,其将网络划分为核心层、汇聚层和接入

层,用于高效转发数据,以实现流量控制和安全隔离^[2]。

1.2 网络架构的基本层次

计算机网络架构分为应用层、传输层和网络层,可通过不同的功能进行共同协作,以实现数据的可靠传输和高效应用^[3]。

1.2.1 应用层的主要功能

应用层通过定义 HTTP(超文本传输协议用于网页浏览)、FTP(文件传输协议用于文件传输)、SMTP(简单邮件传输协议用于电子邮件发送)等各种网络应用协议,为用户提供丰富的网络服务。应用层负责将用户数据转换为适合网络传输的格式并在接收端进行反向转换,以确保数据的完整性和一致性。

1.2.2 传输层的主要功能

传输层位于应用层和网络层的中间^[4],负责在源端和目的端之间建立可靠的连接,以确保数据能准确无误地传输。由于网络层的数据传输单元大小有限,传输层需要将应用层传来的大数据块分割成较小的数据段进行传输,并在接收端将这些数据段重新组合成原始数据。

1.2.3 网络层的主要功能

网络层是计算机网络架构中的核心层次,其主要功能

作者简介:张立波(1994—),本科,助理工程师,研究方向为计算机管理。

包括路由选择与数据包转发、数据包封装与解封、逻辑地址分配与管理^[5]。网络层负责根据目标地址选择合适的路径,并将数据包从源节点传输到目的节点。通过使用各种路由算法来优化路径选择,可以确保数据包能准确地到达目标。网络层在传输数据包之前会将其封装成一定格式的数据包,添加必要的控制信息,并在接收端解封数据包,将其还原为原始数据,同时传递给上层进行进一步处理。

2 网络架构的优化

2.1 网络拓扑结构的优化

在规划网络架构时,需遵循一套明确的设计原则,以帮助网络工程师创建出能满足当前需求并具备未来发展潜力的网络系统。拓扑设计、层次化设计以及模块化设计是网络拓扑结构的3个重要原则^[6]。

(1)拓扑设计。网络拓扑指网络中设备之间的物理连接方式或逻辑组织形式。常见的网络拓扑包括星型环型和网状。星型拓扑结构(见图1)中的所有节点都连接到一个中心点,通常是交换机或路由器。星型拓扑具有简单易维护的优点,如即使某个节点(除中心节点外)发生故障也不会影响其他节点的通信。由于每个节点直接与中心设备相连,其可以实现较高的数据传输速度。环形拓补网络中的节点则通过点对点链接形成一个闭合环路。数据会沿着环传递直到到达目的地。环形网络的优点是可以通过冗余链路实现自愈能力,即当一条链路失败时,数据还可以绕过故障点继续传递。

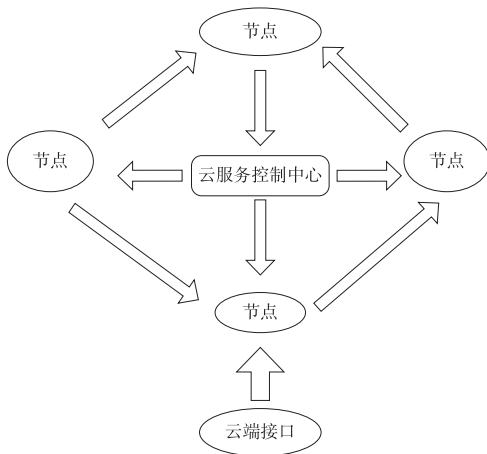


图1 星型拓扑结构

(2)层次化设计。层次化网络设计将网络分为核心层、汇聚层和接入层,其中每一层都有特定的功能,有助于提高网络的整体性能和可管理性。核心层作为网络的主干部分,主要负责高速转发大量数据流。核心层设备应具有高性能、低延迟和高可用性等特点,以保证数据包能在不同区域之间传输。汇聚层是接入层和核心层之间的桥梁,主要负责实现路由选择、访问控制等。接入层能将用户或设备接入网络,负责进行用户认证,保证端口安全,同时进行基

本的服务质量设置。

(3)模块化设计。模块化设计指将网络划分为独立的功能单元或模块,由每个模块负责部分具体的功能。其优点是当需要添加新功能或升级现有功能时只需修改或替换相应的模块,而不必对整个网络进行过大的改动。模块化设计简化了故障排查和修复过程,可以很容易地识别出哪个模块存在问题。当网络需要扩展时,设计人员还可以轻松地添加新的模块,而不会干扰现有的网络结构。

2.2 网络架构性能的优化

2.2.1 传输效率的优化

传输效率优化是一个多维度的过程,包括软硬件、协议、策略等多个方面的优化。在硬件层面,通过升级网络设备(如路由器、交换机),并采用支持高速传输的硬件接口,可以显著提升数据传输速度。在软件与协议层面,优化传输协议较为关键。例如,采用HTTP/2或HTTP/3等更新版本的协议,可通过头部压缩、多路复用、服务器推送等机制来提高数据传输效率。

2.2.2 资源的合理分配

在网络架构的优化过程中,合理分配资源能确保系统的高效运行。该过程涉及带宽、处理能力和存储资源等多个方面。带宽资源的分配需要根据不同业务的需求进行精细化调整。对于需要高带宽的业务,应优先分配足够的带宽资源,以确保数据传输的顺畅无阻。采用负载均衡、流量整形等管理技术,可以更有效地利用带宽资源,避免资源浪费和拥堵。利用虚拟化技术,可以将物理服务器的处理能力虚拟化,形成多个虚拟资源池,根据业务需求灵活分配资源。

2.2.3 流量的高效管理

通过流量管理,可以提高计算机网络的稳定性和高效性。计算机可通过对网络流量的实时监控,明确网络流量的来源、类型分布等信息,从而发现潜在的网络瓶颈或安全威胁。流量控制与限制能保证网络资源的公平分配和有效利用。通过设置合理的流量控制策略,可以有效避免某些应用或用户占用过多的网络资源,导致其他用户或应用的服务质量下降。例如,可以使用QoS(服务质量)技术为不同类型的数据流分配不同的带宽和优先级,以确保关键业务的顺畅运行。负载均衡技术可以将网络流量均匀地分配到多个服务器上,以减轻单一服务器的负载压力,提高整体的处理能力和容错性。这不仅可以提升用户的访问速度和体验,还可以降低服务器的故障风险。

2.3 可靠性增强

2.3.1 冗余设计

冗余设计是提升计算机网络架构可靠性的重要手段,主要通过多路径和双活数据中心进行维护。多路径设计可以在网络中配置多条逻辑路径,为数据传输提供多样化的通道。冗余路径可以在主路径发生故障时迅速接管通信任务,确保数据的连续传输,从而避免单点故障对网络服务产

生影响。双活数据中心则能从数据中心层面提升网络的可靠性。双活数据中心指两个或多个数据中心同时处于活动状态,共同承担业务服务。它们之间通过高速网络连接,以实现数据的实时同步和业务的无缝切换。当其中一个数据中心发生灾难性故障时,另一个数据中心能立即接管全部业务,确保服务的连续性和可用性。

2.3.2 容错机制

容错机制是确保系统在面对故障时能持续提供服务的关键,主要由故障转移与自动恢复两类机制组成。故障转移机制可以在检测到系统或组件故障时自动将业务或数据流从故障点转移到备用资源上,以迅速响应故障并减少服务中断,保障业务的连续性。自动恢复机制则能在故障被排除后自动将业务恢复到正常状态,涉及故障的检测、修复及系统状态验证等多个环节。通过自动化工具和技术,系统能实时监控自身状态,在检测到潜在问题时立即触发恢复流程。

2.3.3 维护与监控

通过实施全面的维护策略和高效的监控机制,可以及时发现潜在问题,并采取相应措施进行干预,避免故障的发生,提高系统可靠性和用户体验。软件层面的维护主要包括操作系统、数据库及应用程序的更新与补丁,以修复已知漏洞,提升系统的安全性与稳定性。监控机制可通过部署监控工具,实时监控网络架构中的各个组件,以收集并分析日志信息和安全事件。例如,通过监控网络流量,可以及时发现异常流量模式,预防DDoS攻击;通过监控数据库性能,可以预测并避免因资源瓶颈而导致的服务延迟。

3 提升计算机网络架构安全性的策略

3.1 实施网络分段

实时网络分段可以显著提升计算机网络架构的安全性。该策略能通过动态地了解网络流量、用户行为或安全威胁的变化,即时调整网络分段布局,从而快速响应并隔离潜在的安全风险。实时网络分段具有动态性和智能性特点。传统的静态网络分段往往难以应对快速变化的安全威胁,而实时网络分段则通过集成先进的监控和分析工具,能实现对网络环境的实时监控与分析。当监控系统检测到异常流量或未授权访问的安全威胁时,就会自动触发网络分段调整机制,迅速隔离受影响的区域,防止威胁进一步扩散。

3.2 强化访问控制

强化访问控制可通过精细化的权限管理策略来降低安全风险。强化访问中包含最小权限原则、零信任网络架构以及基于角色的访问控制(RBAC)等策略。最小权限原则

强调“按需分配”,能有效减少因权限过度分配而引发的安全漏洞,且鼓励权限的精细化管理,使得权限分配更加合理和高效。在零信任网络中,不存在默认的信任关系,所有用户和设备都必须经过严格的身份验证和授权才能访问网络资源。基于角色的访问控制(RBAC)会根据用户的角色和职责来分配访问权限,确保每个用户只能访问其职责范围内的资源。

3.3 部署防火墙和安全设备

在计算机网络架构中部署防火墙、入侵检测与防御系统(IDPS)、安全网关等安全设备,能有效抵御来自内外部各种安全威胁。防火墙是第一道防线,负责检查传入和传出的流量。其能通过设定规则对进出网络的数据包进行过滤,阻止未经授权的访问和恶意流量。入侵检测与防御系统(IDPS)采用深度包检测(DPI)和行为分析技术,能有效分析并识别潜在的安全威胁。一旦发现异常行为或恶意攻击,IDPS就能立即触发警报并采取相应的防御措施,从而有效遏制安全威胁的扩散。安全网关可利用加密技术对传输中的数据进行加密和解密处理,确保数据的机密性和完整性。通过安全网关,企业可以在不安全的网络环境中传输敏感数据,如客户信息、财务报表等。

4 结语

随着信息技术的快速发展,构建一个既高效又安全的网络架构已成为企业信息化建设的核心任务。通过优化网络架构,可以实现资源的合理配置和高效利用,显著提升企业的业务处理能力和响应速度。为加强网络安全防护,可采取多种技术手段和管理措施,实施强化访问控制策略,以有效抵御内外部的安全威胁,保护企业数据资产的安全性和完整性。

参考文献

- [1] 陆玉贵. 基于计算机技术的网络信息安全体系架构设计研究[J]. 国际教育学, 2024, 2(7): 103-105.
- [2] 李静. 基于计算机技术实现信息安全体系架构设计[J]. 信息技术与信息化, 2024(3): 188-191.
- [3] 程曦. 企业计算机网络的安全架构设计与优化分析[J]. 集成电路应用, 2024, 41(2): 226-227.
- [4] 李明, 赵明莉, 张亦姝. 容错计算机系统架构设计[J]. 信息技术与信息化, 2023(6): 118-121.
- [5] 郑文娟. 基于云计算技术的计算机实验平台架构设计[J]. 无线互联科技, 2023, 19(2): 99-102.
- [6] 徐文伟, 张磊, 陈乐. 云数据中心网络架构与技术[M]. 人民邮电出版社: 华为网络技术系列, 2022.