基于计算机网络安全中的防火墙技术应用研究

汇报人：

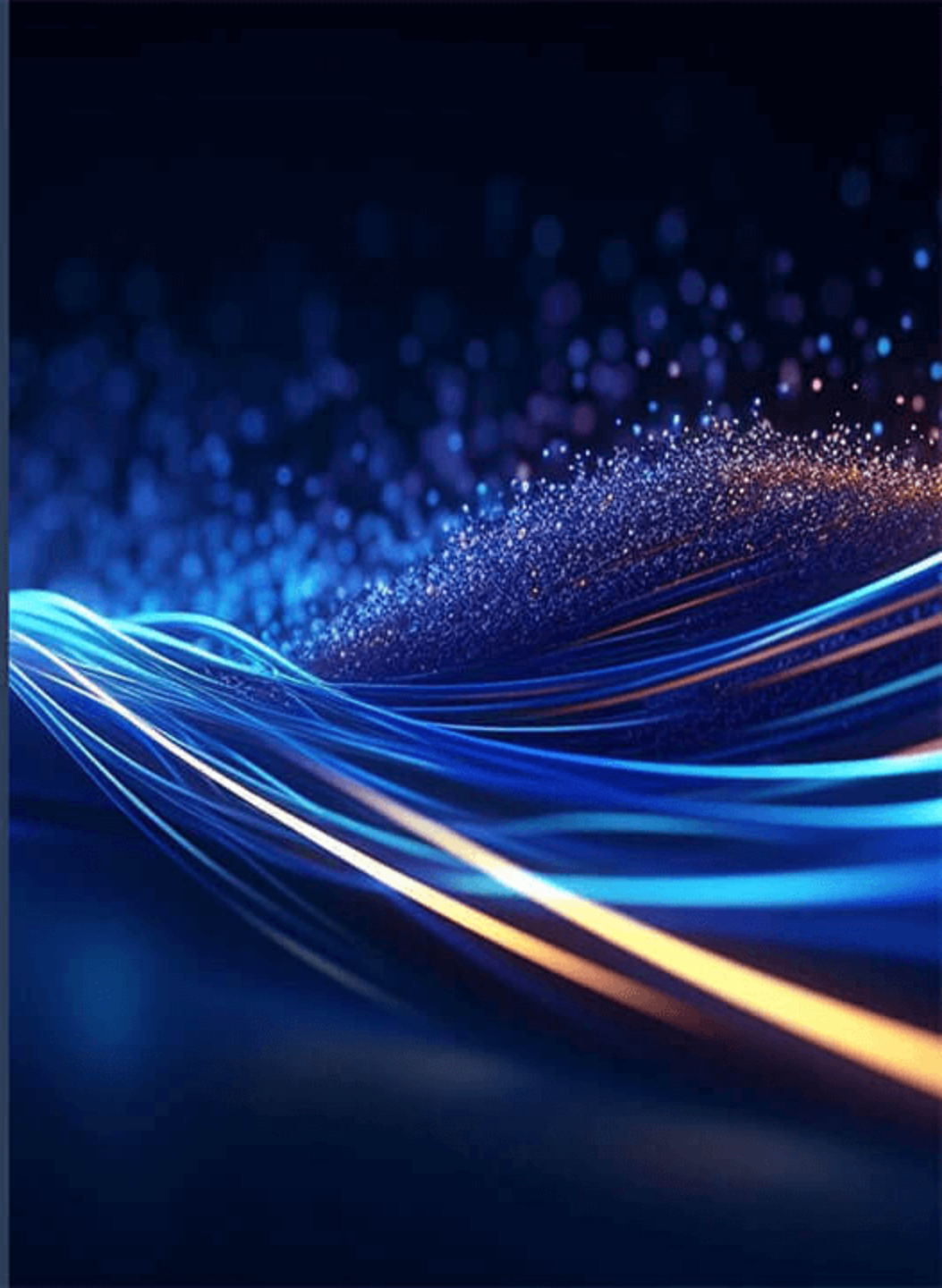
2024-01-26

contents

目录

01

防火墙技术概述



防火墙定义及作用

01

防火墙定义

防火墙是位于内部网络和外部网络之间的网络安全系统，它通过一系列安全策略和安全技术，对进出内部网络的数据流进行监控、过滤和审计，从而保护内部网络免受未经授权的访问和攻击。

02

访问控制

通过配置安全策略，允许或拒绝特定用户或应用程序对内部网络的访问。

03

数据过滤

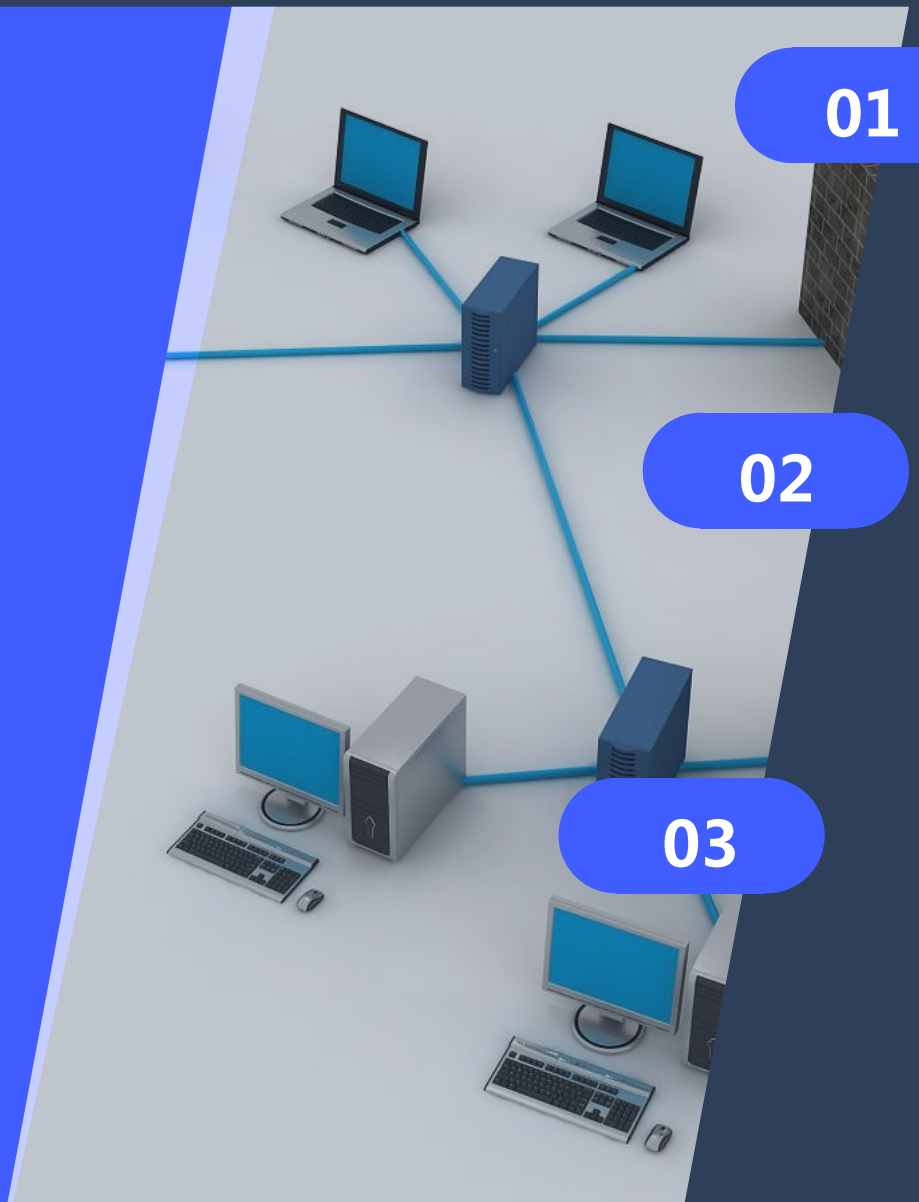
对进出内部网络的数据流进行深度检测和分析，过滤掉恶意代码和攻击流量。

04

日志审计

记录所有通过防火墙的数据流和用户行为，为安全审计和事件响应提供依据。

防火墙技术分类



01

包过滤防火墙

根据预先设定的规则，对进出内部网络的每个数据包进行检查和过滤。优点是处理速度快、对系统性能影响小；缺点是规则配置复杂，且无法有效应对应用层攻击。

02

代理服务器防火墙

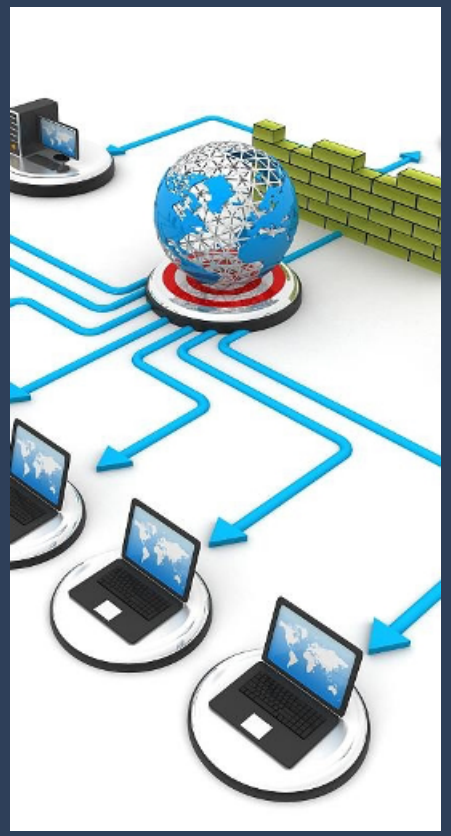
通过在内部网络和外部网络之间建立代理服务器，对应用层数据进行深度检测和分析。优点是安全性高、可应对应用层攻击；缺点是处理速度较慢、对系统性能影响较大。

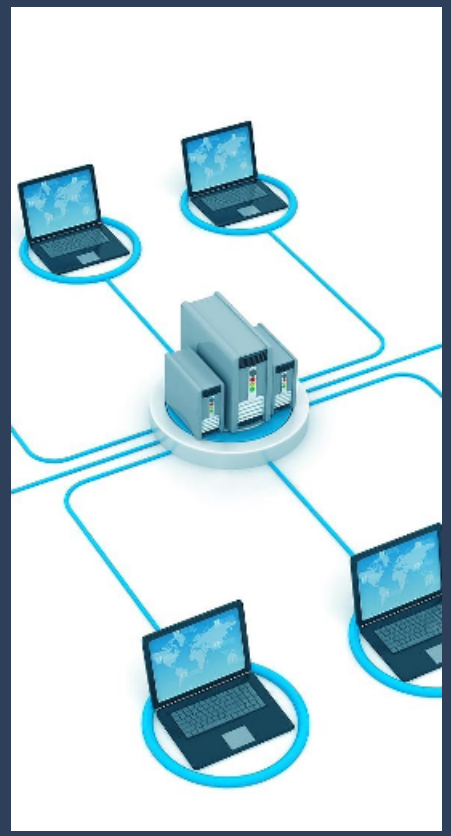
03

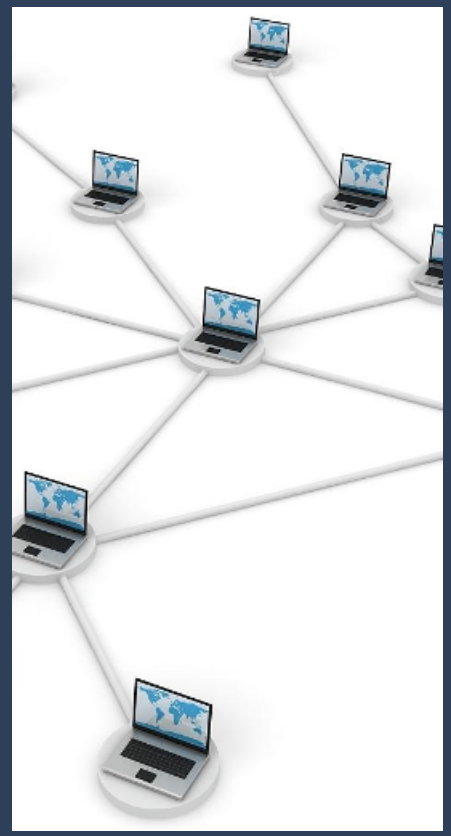
状态检测防火墙

结合包过滤和代理服务器技术的优点，对进出内部网络的数据流进行状态检测和分析。优点是安全性高、处理速度快；缺点是技术实现难度较大。

发展趋势与挑战







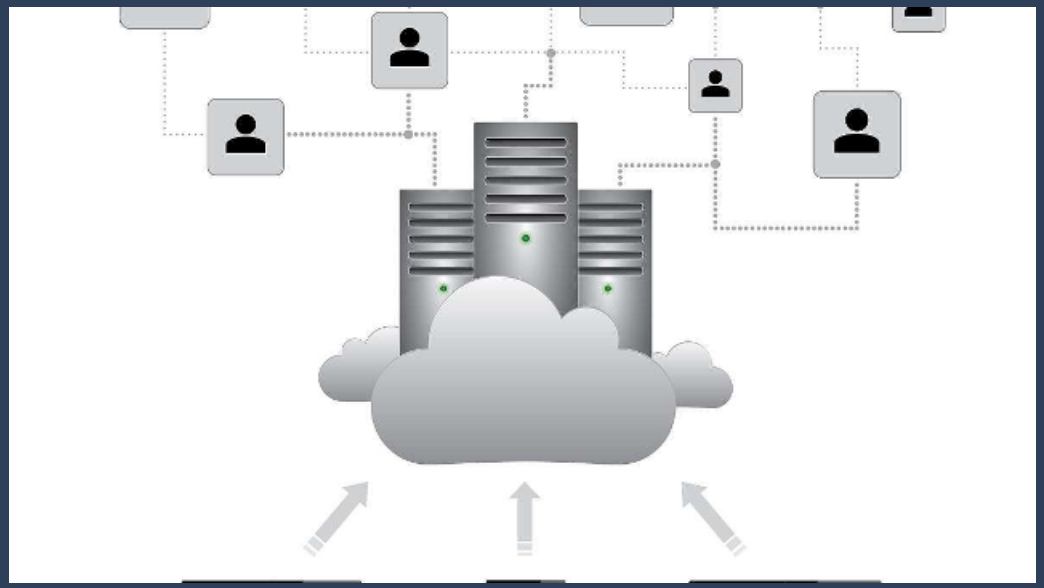
智能化

利用人工智能、机器学习等技术，提高防火墙的自适应能力和智能化水平。

云网支持

适应云计算、SDN等新型网络架构，提供云网环境下的安全防护能力。

发展趋势与挑战



- 零信任安全：基于零信任安全理念，构建以身份为中心的动态访问控制体系。

发展趋势与挑战

高性能需求

随着网络带宽和数据量的不断增长，防火墙需要具备更高的处理能力和性能。

应用层攻击防护

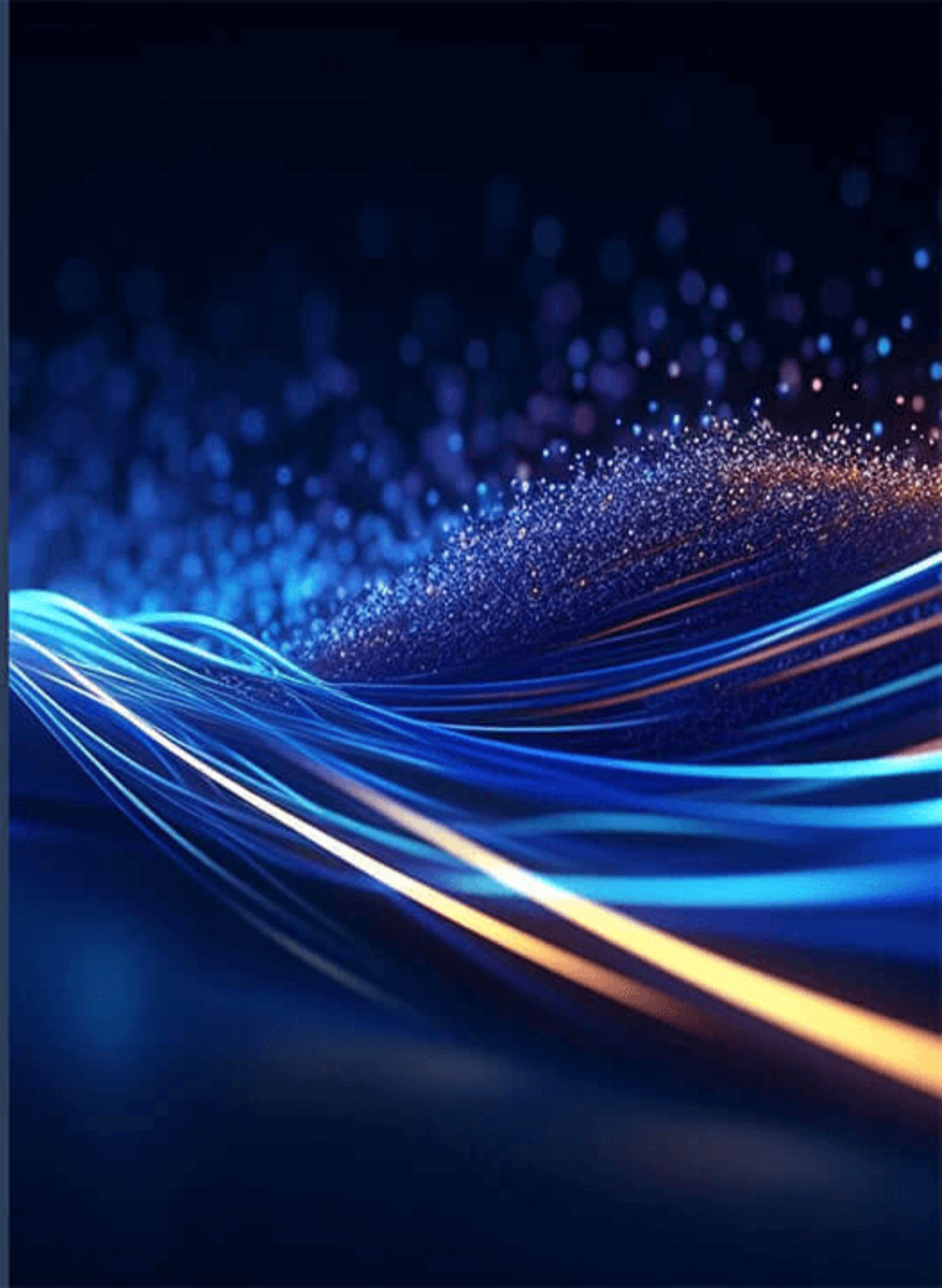
针对应用层攻击的防护技术需要不断完善和创新。

安全策略管理

如何制定合理且有效的安全策略，降低误报率和漏报率，是防火墙技术面临的挑战之一。

02

计算机网络安全现状及威胁分析



计算机网络安全现状

01

网络安全事件频发

随着互联网的普及和技术的进步，网络安全事件不断增多，包括黑客攻击、病毒传播、网络钓鱼等。

02

数据泄露风险加大

企业和个人数据泄露事件屡见不鲜，涉及个人隐私、商业机密等重要信息。

03

恶意软件泛滥

恶意软件数量不断增长，通过各种手段传播并窃取用户信息，造成重大损失。

网络攻击手段与特点

社交工程攻击

利用人的心理弱点，通过伪造身份、诱骗等方式获取敏感信息。

分布式拒绝服务攻击（DDoS）

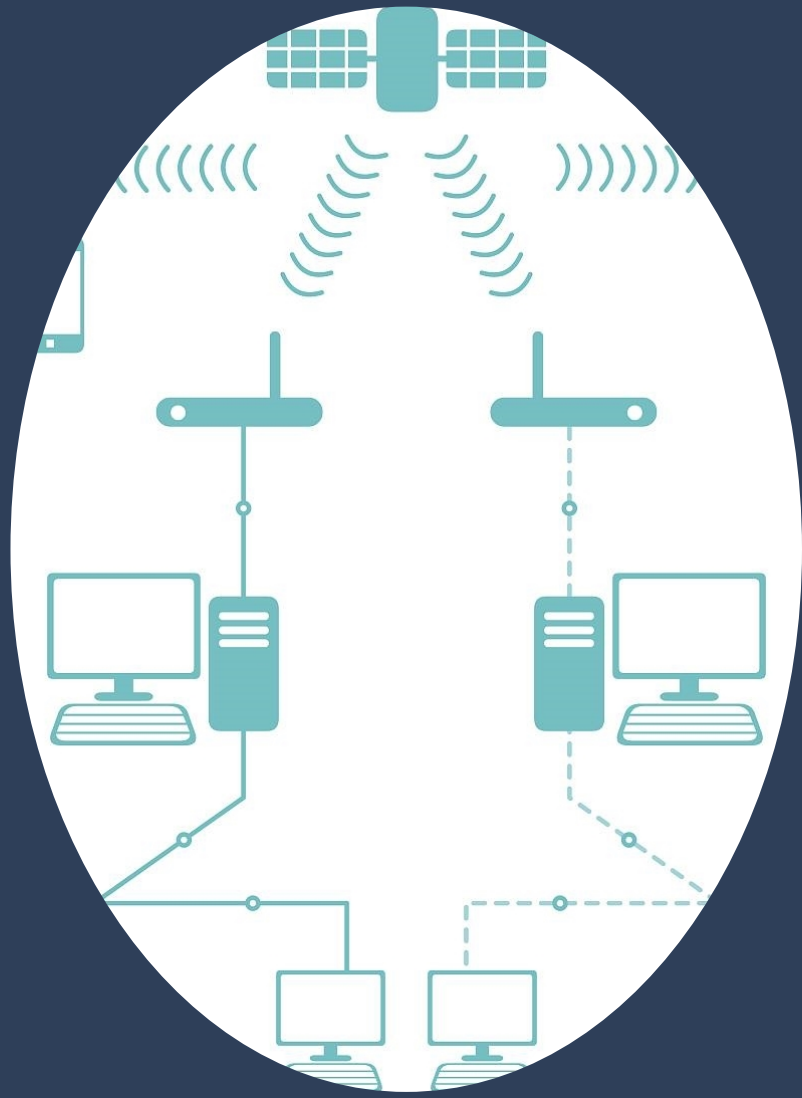
通过大量请求拥塞目标服务器，使其无法提供正常服务。

恶意代码攻击

包括病毒、蠕虫、木马等，通过感染用户系统窃取信息或破坏系统功能。

零日漏洞攻击

利用尚未公开的漏洞进行攻击，具有极高的隐蔽性和危害性。



典型案例分析

1

WannaCry勒索病毒

利用Windows系统漏洞进行传播，加密用户文件并索要赎金，造成全球范围内的巨大损失。

2

NotPetya网络攻击

伪装成勒索病毒，实则具有更强的破坏力，不仅加密文件还破坏系统引导记录，导致系统无法启动。

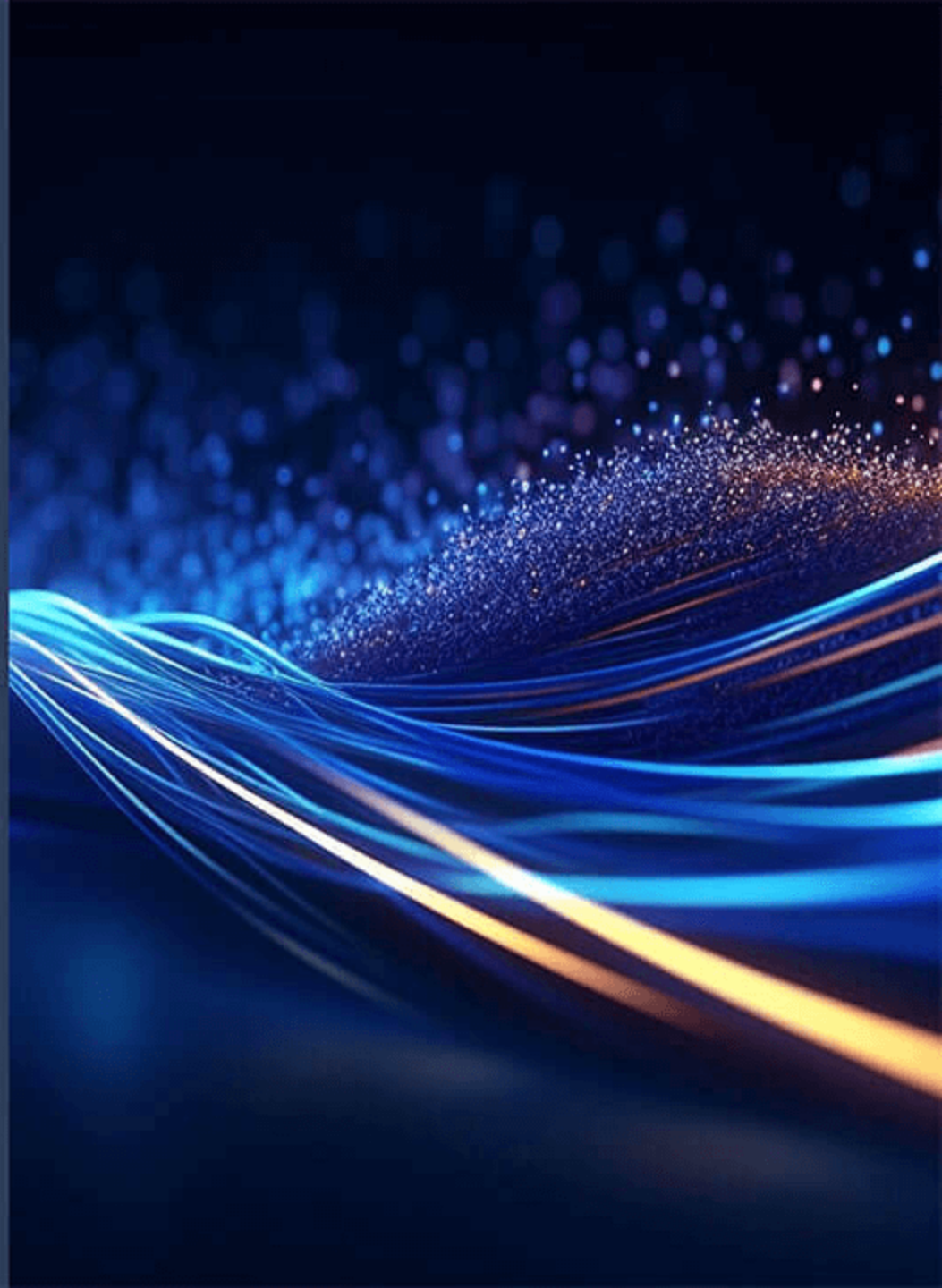
3

Equifax数据泄露事件

黑客利用漏洞入侵Equifax公司系统，窃取大量用户个人信息，包括姓名、地址、社保号等敏感信息。

03

防火墙技术在计算机网络安全中应用



访问控制策略制定与实施

01

制定严格的访问控制策略

根据网络的安全需求和业务规则，制定访问控制列表（ACL），明确允许或拒绝特定IP地址、端口号、协议类型的网络访问。

02

实施基于角色的访问控制（RBAC）

针对不同用户或用户组分配不同的网络访问权限，确保只有授权用户能够访问敏感资源。

03

强化身份认证机制

采用多因素身份认证方式，如用户名/密码、数字证书、动态口令等，提高用户身份认证的安全性。