


YOUR LOGO

防火墙技术：网络安全的坚 固盾牌

▶▶▶ 2024 ◀◀◀

主讲人：郑冬贤

时间：2024



CONTENTS

目录

1. 防火墙的基本概念及工作基本原理

3. VPN技术及其应用

2. 第三方防火墙的应用

YOUR LOGO

Part 01

防火墙的基本概念及工作 基本原理

防火墙的定义与作用

防火墙的工作原理主要基于包过滤、代理服务和状态检测等技术。包过滤是最基本的防火墙技术，它在网络层对数据包进行检查，根据数据包的源 IP 地址、目的 IP 地址、端口号、协议类型等信息，与预设的访问控制列表

(ACL) 进行比对，决定是否允许数据包通过。例如，如果 ACL 中设置禁止外部网络访问内部特定服务器的某一端口，当外部数据包的目的地址为该服务器且端口号匹配时，防火墙就会直接丢弃该数据包，阻止连接建立。

防火墙的网络安全作用

防火墙位于内部网络与外部网络之间，根据安全策略监控、过滤和控制网络流量，阻止未经授权访问。

防火墙保护内部网络免受攻击和入侵，防止内部敏感信息泄露。

防火墙的工作原理



包过滤技术

包过滤技术检查数据包头部信息，与ACL 比对，决定是否放行，适用于基础的访问控制。



代理服务技术

代理服务在应用层控制网络连接，代理服务器代替客户端发起请求，进行深入检查和过滤。



状态检测技术

状态检测技术结合包过滤和代理服务，跟踪网络连接状态，提高防火墙效率和安全性。

YOUR LOGO

Part 02

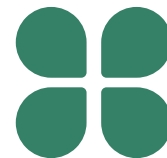
第三方防火墙的应用

第三方防火墙的优势



卡巴斯基安全软件的多层防护

卡巴斯基提供网络流量过滤、反病毒、反恶意软件等高级安全功能，灵活设置安全级别和规则。



诺顿网络安全特警的智能防护

诺顿防火墙智能识别和阻止网络攻击，管理家庭网络中的智能设备，防止成为入侵跳板。

第三方防火墙的隐私保护功能

防止个人信息非法收集

诺顿防火墙具备隐私保护功能，阻止广告商追踪用户上网行为，保护用户隐私安全。

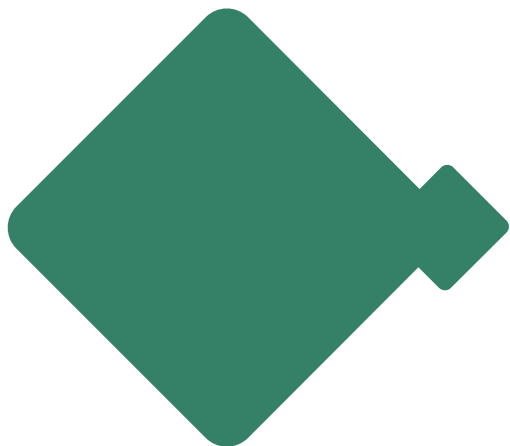


YOUR LOGO

Part 03

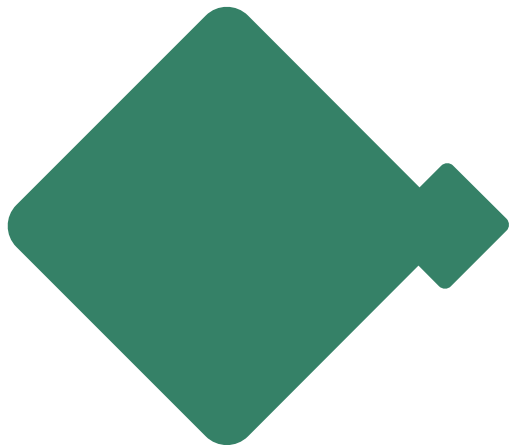
VPN技术及其应用

VPN的定义与主要应用场景



企业远程办公的VPN应用

VPN技术通过加密和隧道技术，实现企业员工远程安全访问内部资源，保障数据传输的保密性和完整性。



个人用户VPN应用

个人用户使用VPN绕过地域限制访问网站，但需遵守中国法律法规，确保合法合规的网络行为。

VPN与防火墙技术的配合



构建全面的网络安全保障

防火墙与VPN技术相互配合，为网络安全提供全面保障，保护内部网络免受攻击，为远程访问提供安全通道。

在个人用户方面，VPN 也有广泛的应用。例如，在访问一些受到地域限制的网站或服务时，用户可以使用 VPN 连接到其他地区的服务器，绕过地域限制，获取所需的信息。但需要注意的是，在中国，未经电信主管部门批准，不得自行建立或租用专线（含虚拟专用网络 VPN）等其他信道开展跨境活动。个人使用 VPN 应当遵守国家法律法规，确保合法合规的网络行为。

防火墙技术和 VPN 技术相互配合，为网络安全提供了全面的保障。防火墙保护内部网络免受外部攻击，VPN 则为远程访问和数据传输提供了安全通道，两者共同构建了一个安全、可靠、灵活的网络环境，使得我们能够在享受网络带来的便利的同时，确保我们的信息资产和网络活动的安全。随着网络技术的不断发展，防火墙和 VPN 技术也将持续演进，以应对日益复杂多变的网络安全挑战。

YOUR LOGO

谢谢大家

▶▶▶ 2024 ◀◀◀

主讲人：郑冬贤

汇报时间：2024