网络安全PPT课件演示

contents

目录

01

CATALOGUE

网络安全概述

定义与重要性

定义

网络安全是指通过技术、管理和法律手段，保护计算机网络系统及其中的数据不受未经授权的访问、攻击、破坏或篡改的能力。

重要性

随着互联网的普及和数字化进程的加速，网络安全已成为国家安全、社会稳定和经济发展的重要保障。网络安全不仅关乎个人隐私和企业机密，还涉及到国家安全和社会稳定。

网络安全威胁类型

恶意软件

包括病毒、蠕虫、木马等，通过感染用户计算机或窃取用户信息来实施攻击。

网络钓鱼

通过伪造信任网站或电子邮件，诱骗用户输入敏感信息，如用户名、密码等。

拒绝服务攻击

通过大量无用的请求拥塞目标服务器，使其无法提供正常服务。

漏洞攻击

利用系统或应用程序中的漏洞，实施非法访问和数据窃取。

网络安全法律法规

1

《中华人民共和国网络安全法》

我国首部全面规范网络空间安全管理的基础性法律，明确规定了网络运营者、网络产品和服务提供者等的法律责任和义务。

2

《数据安全管理办法》

针对网络数据的安全管理制定了一系列措施，包括数据分类、备份恢复、加密等。

3

《个人信息保护法》

保护个人信息安全，规范个人信息的收集、使用和处理行为。

02

CATALOGUE

网络安全技术基础

加密技术与算法

对称加密

采用单钥密码系统的加密方法，同一个密钥可以同时用作信息的加密和解密。

混合加密

结合对称加密和非对称加密的优势，在保证安全性的同时提高加密和解密效率。

非对称加密

又称公钥加密，使用一对密钥来分别完成加密和解密操作，其中一个公开发布（即公钥），另一个由用户自己秘密保存（即私钥）。

防火墙原理及应用

防火墙定义

一种将内部网和公众访问网（如Internet）分开的方法，实际上是一种建立在现代通信网络技术和信息安全技术基础上的应用性安全技术。

防火墙功能

阻止未经授权的用户访问内部网络、允许合法用户安全地访问网络资源、记录并报告所有可疑的网络活动。

防火墙类型

包过滤防火墙、代理服务器防火墙、状态检测防火墙等。

入侵检测与防御系统

入侵检测系统（IDS）

通过对计算机网络或计算机系统中的若干关键点收集信息并对其进行分析，从中发现网络或系统中是否有违反安全策略的行为和被攻击的迹象。

入侵防御系统（IPS）

一种主动的、智能的入侵检测、防范、阻止系统，它不但能检测恶意攻击，还能实时阻断攻击，并对攻击源进行跟踪定位。

IDS与IPS的区别

IDS是旁路监听设备，对流量进行镜像监听，不直接对流量进行阻断；而IPS是串联接入设备，直接对流量进行阻断。

03

CATALOGUE

操作系统与网络安全

Windows系统安全配置

关闭不必要的端口和服务

通过Windows防火墙或第三方软件关闭不必要的端口和服务，减少攻击面。

定期更新补丁

及时安装Windows系统补丁，修复已知漏洞，提高系统安全性。

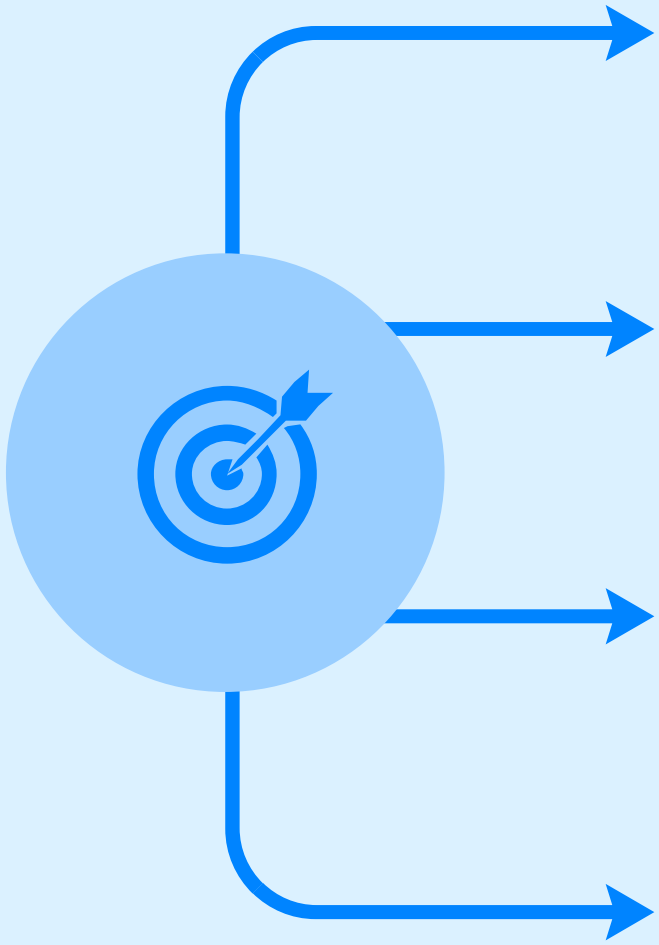
强化账户安全

设置强密码策略，定期更换密码，限制账户权限，防止账户被滥用。

配置安全审计策略

启用Windows事件日志记录功能，监控系统异常行为，及时发现潜在威胁。

Linux系统安全配置



最小化安装原则

仅安装必要的软件包和服务，降低系统复杂性，减少潜在的安全风险。

强化文件和目录权限

合理配置文件和目录权限，防止未经授权的访问和修改。

定期更新补丁

及时安装Linux系统补丁，修复已知漏洞，提高系统安全性。

配置防火墙和入侵检测系统

使用iptables或类似工具配置防火墙规则，限制网络访问；启用入侵检测系统，实时监控网络流量和事件，及时发现潜在威胁。

移动设备安全策略

设置强密码和锁屏图案

为移动设备设置强密码或复杂的锁屏图案，防止未经授权的访问。

限制应用程序权限

仔细审查应用程序权限请求，仅授予必要的权限，防止应用程序滥用权限。

定期更新操作系统和应用程序

及时安装操作系统和应用程序的更新补丁，修复已知漏洞，提高安全性。

启用远程擦除功能

启用远程擦除功能，一旦设备丢失或被盗，可以远程擦除设备上的数据，保护个人隐私。

04

CATALOGUE

网络通信安全

VPN技术原理及应用

01

VPN技术原理

通过在公共网络上建立专用网络，进行加密通讯，以保证数据的安全性和隐私性。

02

VPN技术应用

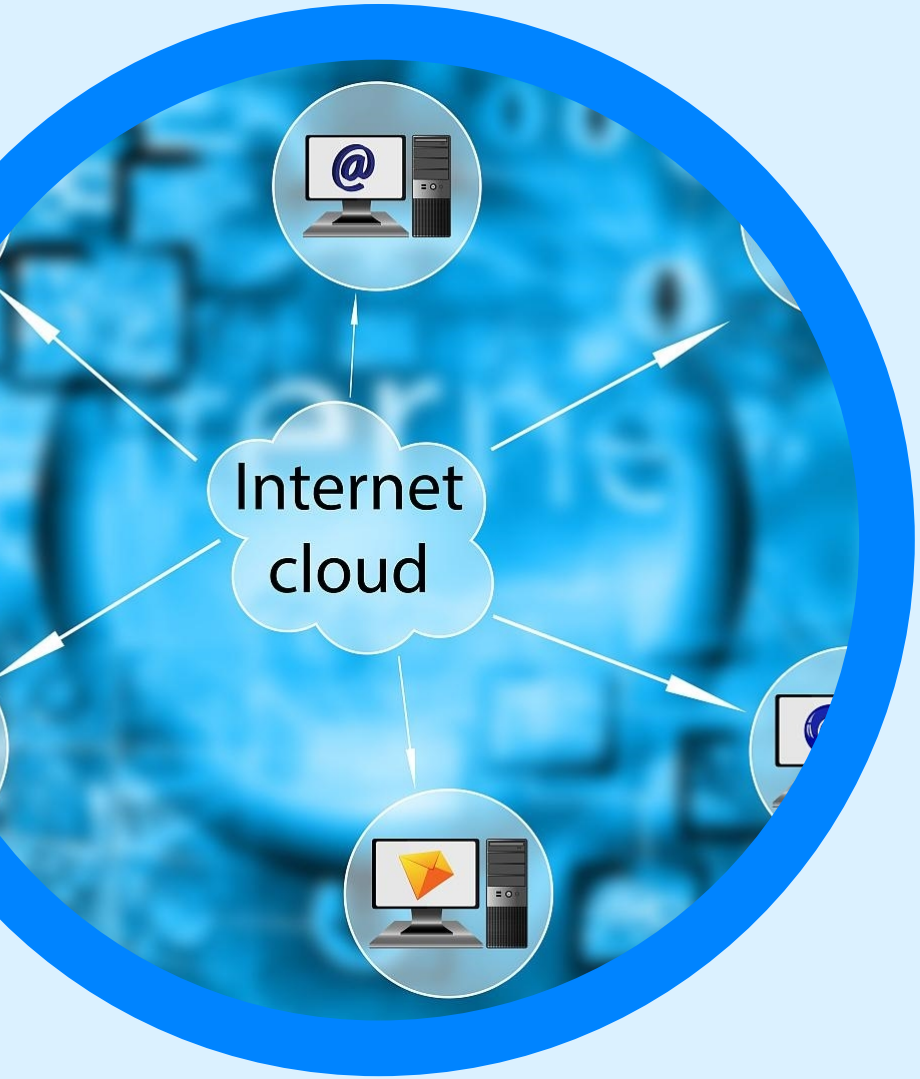
远程访问公司内部网络资源、保护敏感数据传输、绕过地域限制等。

03

VPN技术优缺点

优点包括安全性高、可远程访问等；缺点包括可能影响网络速度、需要额外配置等。

SSL/TLS协议分析



01

SSL/TLS协议作用

提供安全通信通道，确保数据在传输过程中的机密性、完整性和身份验证。

02

SSL/TLS协议工作流程

建立安全连接、服务器身份验证、客户端身份验证（可选）、协商加密套件和生成会话密钥等步骤。

03

SSL/TLS协议攻击与防护

可能遭受中间人攻击等威胁；防护措施包括使用强密码套件、定期更新证书等。