基于主动积极防御协同的内网威胁感知技术研究与应用

汇报人：

2024-01-21

CATALOGUE

目录

01

CATALOGUE

引言

研究背景与意义

网络安全威胁日益严重

随着网络技术的快速发展，内网安全威胁日益增多，如恶意软件、内部泄露、高级持续性威胁等，对企业和组织的数据安全造成严重威胁。

传统防御手段存在局限性

传统的内网安全防护手段，如防火墙、入侵检测系统等，主要关注外部威胁的防御，对内部威胁的感知和应对能力有限。

主动积极防御协同的重要性

为主动应对内网威胁，需要研究基于主动积极防御协同的内网威胁感知技术，该技术能够实时监测内网环境，发现潜在威胁，并与现有防御手段协同工作，提升内网整体安全性。

国内外研究现状及发展趋势

国外研究现状

国外在内网威胁感知技术方面起步较早，已经形成了相对成熟的技术体系，如基于深度学习的恶意软件检测、基于网络流量的异常行为分析等。

国内研究现状

国内在内网威胁感知技术方面的研究相对较晚，但近年来发展迅速，已经在恶意软件检测、内部泄露预警等方面取得了一定成果。

发展趋势

未来内网威胁感知技术将更加注重实时性、智能化和协同性，利用人工智能、大数据等技术提升感知能力和应对效率。

研究内容、目的和方法

研究内容

本研究旨在研究基于主动积极防御协同的内网威胁感知技术，包括内网环境实时监测、潜在威胁发现、与现有防御手段协同工作等方面。

研究目的

通过本研究，期望能够提升内网整体安全性，有效应对内部威胁，保障企业和组织的数据安全。

研究方法

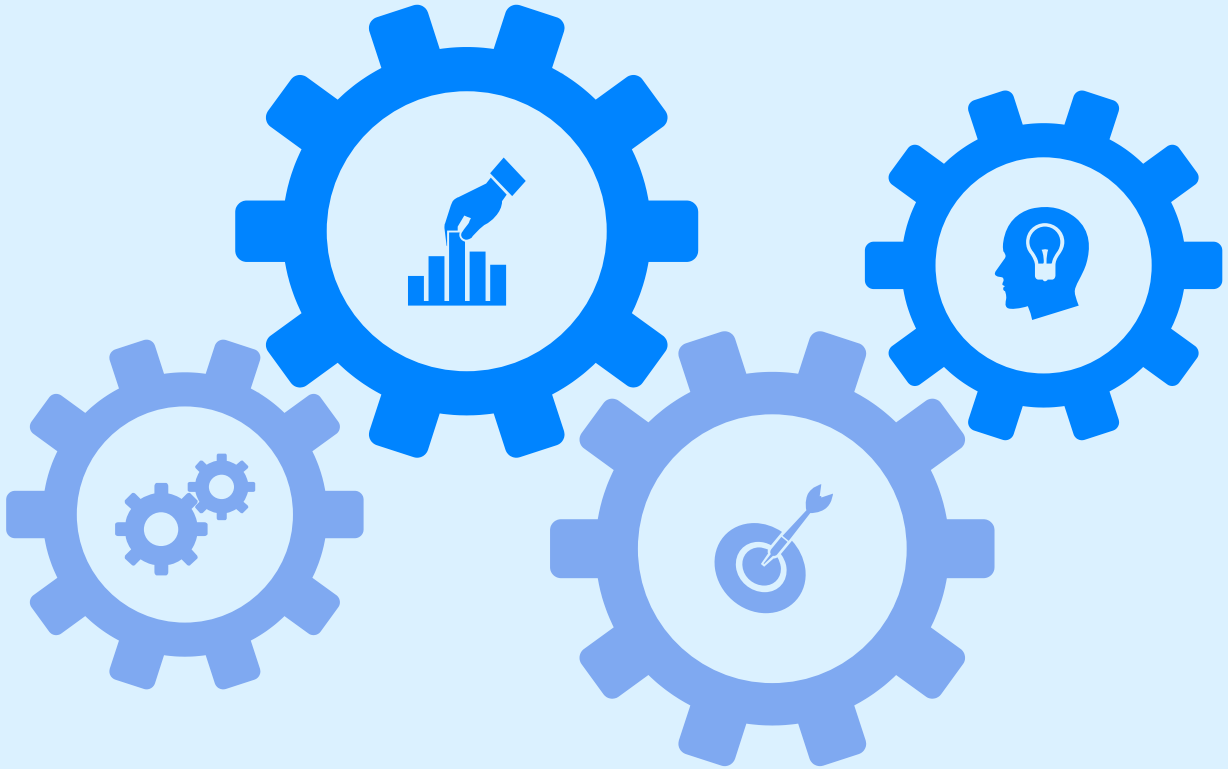
本研究将采用文献综述、理论分析、实验验证等方法进行研究。首先通过文献综述了解国内外研究现状及发展趋势；其次通过理论分析构建基于主动积极防御协同的内网威胁感知技术框架；最后通过实验验证所提技术的有效性和可行性。

02

CATALOGUE

内网威胁感知技术概述

内网威胁定义及分类



定义

内网威胁是指在企业或组织内部网络中，由于内部人员恶意行为、系统漏洞、病毒传播等原因，对网络和信息系统造成的潜在或实际危害。

分类

内网威胁可分为内部人员恶意行为、内部系统漏洞、病毒和恶意软件传播、内部网络攻击等类型。

传统内网安全防护措施及局限性

传统防护措施

包括防火墙、入侵检测系统、反病毒软件等，主要关注外部威胁的防御。

局限性

传统防护措施对内网威胁的感知能力有限，无法有效应对内部人员恶意行为、系统漏洞等威胁，且容易产生误报和漏报。

基于主动积极防御协同的内网威胁感知技术原理

原理

基于主动积极防御协同的内网威胁感知技术，通过实时监测内网中的网络流量、系统日志、用户行为等信息，运用大数据分析、机器学习等技术手段，实现对内网威胁的精准感知和快速响应。

VS

技术特点

该技术具有主动性、协同性、精准性和快速响应等特点，能够主动发现潜在威胁，协同各类安全设备进行联动防御，精准定位威胁源头并快速处置。

03

CATALOGUE

关键技术研究

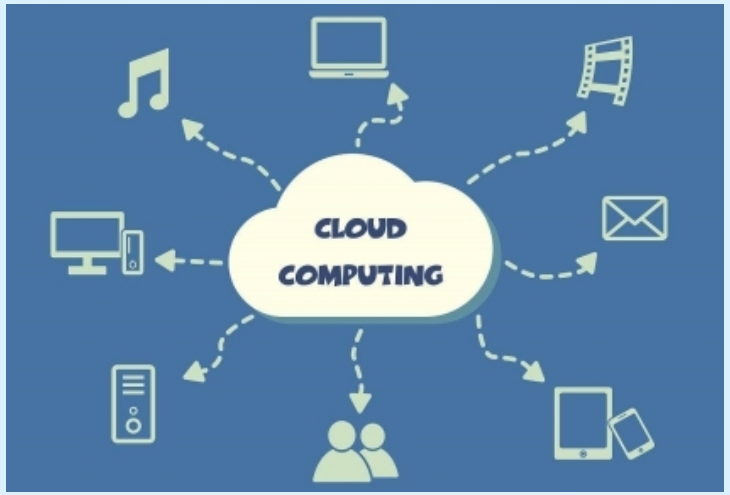
深度包检测技术

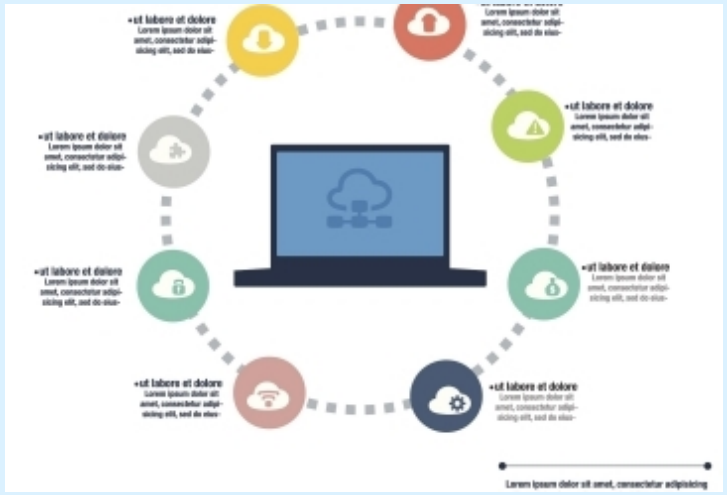
深度包检测（Deep Packet Inspection，DPI）技术是一种基于网络数据包内容的检测技术，通过对网络数据包进行深度解析和检测，可以识别出网络中的恶意流量和威胁行为。

DPI技术可以检测网络数据包中的应用层协议、端口号、IP地址等信息，同时还可以对数据包内容进行深度解析，如检测恶意代码、病毒、木马等。

DPI技术可以应用于防火墙、入侵检测系统、网络监控等场景中，实现对网络威胁的精准识别和防御。

行为分析技术





行为分析技术是一种基于网络行为特征的检测技术，通过对网络中的主机、设备、应用等的行为进行分析和建模，可以识别出网络中的异常行为和威胁行为。

行为分析技术可以检测网络中的流量、连接、会话等行为特征，同时还可以结合机器学习、深度学习等技术进行智能分析和预测。

行为分析技术可以应用于网络安全管理、风险评估、威胁预警等场景中，实现对网络威胁的全面感知和快速响应。

流量异常检测技术

流量异常检测技术是一种基于网络流量特征的检测技术，通过对网络中的流量数据进行实时监测和分析，可以识别出网络中的异常流量和威胁行为。

流量异常检测技术可以检测网络中的流量大小、流向、流速等特征，同时还可以结合统计分析、时间序列分析等技术进行深度挖掘和预测。

流量异常检测技术可以应用于网络性能管理、故障排查、安全防御等场景中，实现对网络威胁的及时发现和处置。