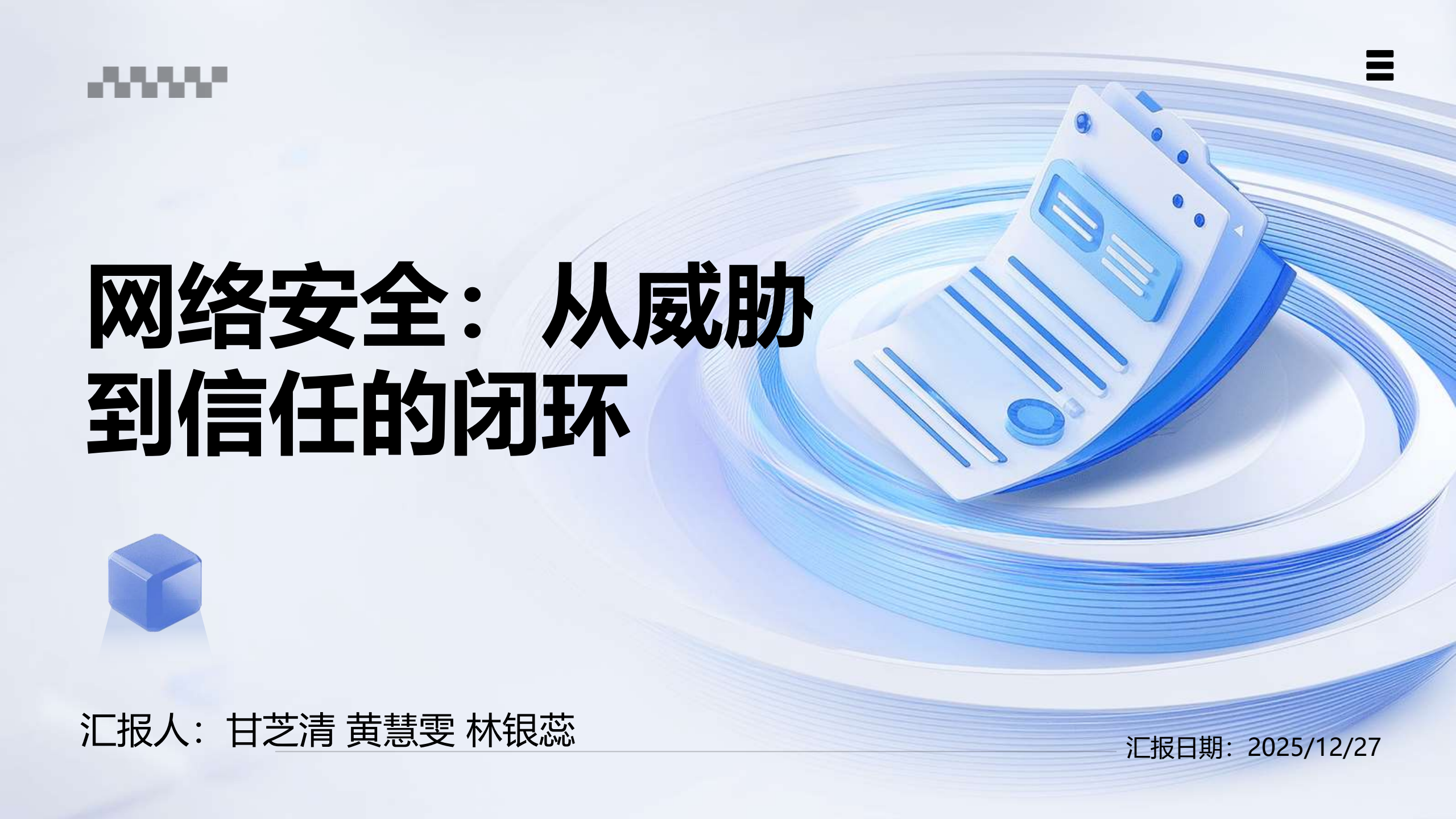
网络安全：从威胁到信任的闭环



汇报人：甘芝清 黄慧雯 林银蕊

汇报日期：2025/12/27

目录

CONTENTS

/ 01. 安全目标与威胁图谱

/ 02. 密码双体制：对称与非对称

/ 03. 信任凭证：签名与证书

/ 04. 边界与感知：防火墙IDS

/ 05. 协议级安全：SSL与IPsec

/ 06. 回顾与展望

安全目标与威胁图谱

01

CIA三角：安全通信的北极星

安全不是绝对状态，而是围绕三大核心目标的风险可控过程。

机密性

确保信息只被授权者访问，通过**加密**等技术实现。

完整性

保证信息在传输中未被篡改，通过**数字签名**等技术保证。

可用性

保障网络系统持续可用，通过**防火墙、IDS**等防御DoS攻击。

扩展目标包括**端点鉴别**与**运行安全性**，共同构成完整的信任体系。

威胁图谱：被动截获与主动篡改

被动攻击：静默的窃听者

核心行为：截获

目的：破坏**机密性**。

特点：不干扰系统，难以被察觉。

对策：重在**预防**，如数据加密。

主动攻击：直接的破坏者

核心行为：篡改、伪造、DoS

目的：破坏**完整性**与**可用性**。

特点：主动干扰，可被检测。

对策：重在**检测和恢复**。

密码双体制：对称与非对称

02

对称密钥：效率与规模的悖论

加密解密使用**同一把密钥**，高效但面临分发难题。

用户 A

密钥必须通过**安全信道**预先共享

用户 B

挑战： n个用户需要 n(n-1)/2 个密钥，管理复杂度呈指数级增长。

公钥密码：分发革命与性能代价

使用**一对密钥**（公钥和私钥），解决分发难题，但速度较慢。

私钥 (保密)

公钥 (公开)

优点

解决了密钥分发问题，公钥可公开，**n个用户仅需2n个密钥**。

缺点

算法复杂，**加解密速度远慢于对称加密**。

信任凭证：签名与证书

03

数字签名：手写签名的比特化

原始报文

报文摘要

数字签名

验证通过

核心特性：不可伪造、不可否认、报文完整性

发送方用其**私钥**对报文摘要“签名”，接收方用发送方**公钥**验证。任何改动都会使验证失败。

PKI与CA：公钥可信的链式锚点

通过数字证书和认证中心(CA)，为公钥世界建立中心化信任链。

信任链验证

任何信任根CA的用户，都可以用根CA的公钥验证中级CA的证书，进而信任用户A的公钥。信任是委托，一旦根私钥泄露，整个链将崩塌。

边界与感知：防火墙IDS

04

防火墙：网络边界的交通警察

外部网络（不可信）

防火墙

内部网络（可信）

分组过滤

基于IP、端口等规则过滤，简单高效。

状态检测

跟踪连接状态，动态过滤，更先进。

应用代理

作为通信中介，深度检查，安全性高。

入侵检测系统 (IDS)：网络的监控摄像头

基于特征的IDS

模式匹配

维护已知攻击“特征库”，通过匹配发现攻击。

优点：准确率高，误报少。

缺点：只能检测已知攻击。

基于异常的IDS

行为分析

建立“正常行为轮廓”，通过检测偏差发现攻击。

优点：可能发现未知攻击。

缺点：误报率高。

协议级安全：SSL与IPsec

05

SSL/TLS：应用透明的加密隧道

位于应用层与传输层之间，为上层数据提供安全保障，核心是**混合加密**。

核心应用：HTTPS (HTTP over SSL/TLS)

通过**握手协商**、**证书校验**、**对称加密传输**，实现服务器鉴别、数据加密和报文完整性。

IPsec：网络层的隐形护甲

在网络层提供安全服务，对上层协议透明，是构建**VPN**的核心技术。

传输模式

仅保护IP数据包的**载荷部分** (如TCP/UDP段)，适用于端到端主机通信。

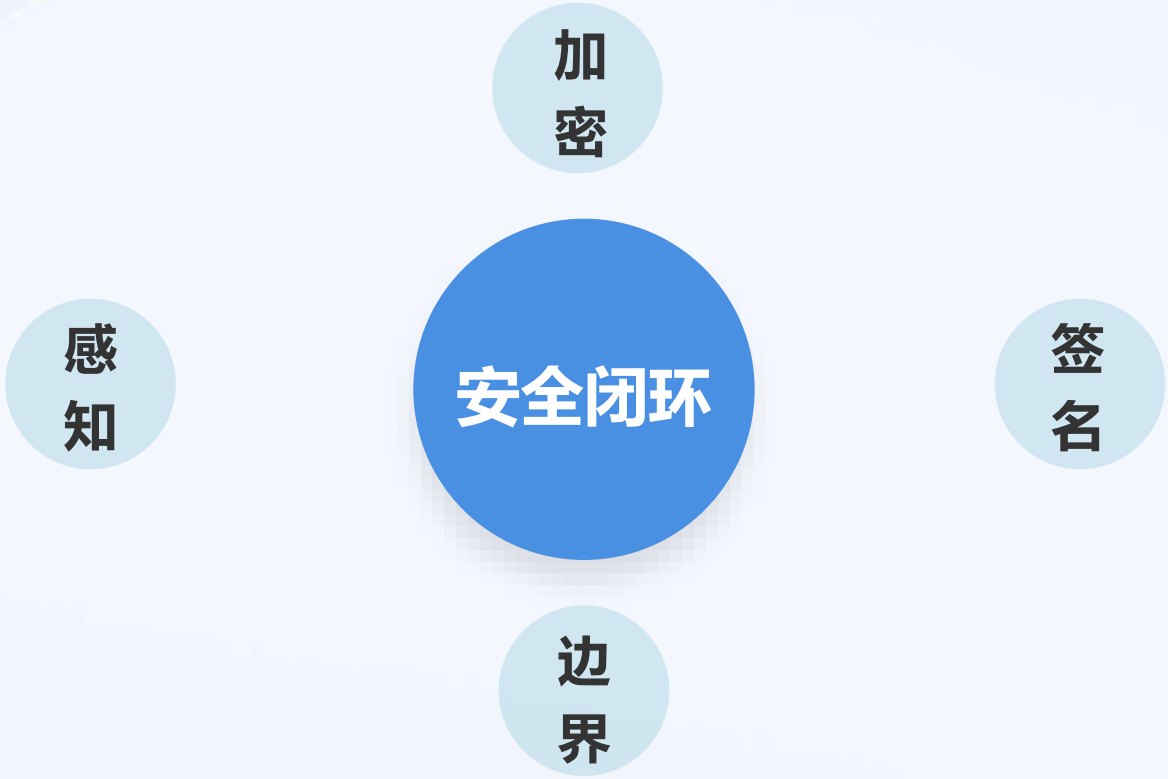
隧道模式

保护**整个原始IP包**，并将其封装在新的IP包中，适用于VPN网关场景。

回顾与展望

06

网络安全闭环：从加密到响应



安全是叠加与响应速度的艺术，需结合**加密、鉴别、访问控制、监控**等多种技术。

未来演进：零信任架构

“永不信任，持续验证”，打破传统边界，实现动态、精细化的安全控制。

身份　设备　环境　行为

核心原则

结合**微分段、最小权限、持续评估**，将安全从成本中心转化为信任竞争力。

THANK YOU FOR READING!

感谢您的观看

汇报人：甘芝清 黄慧雯 林银蕊

汇报日期：2025/12/27