安全网络架构设计

崔宝江
北京邮电大学信息安全中心

目录

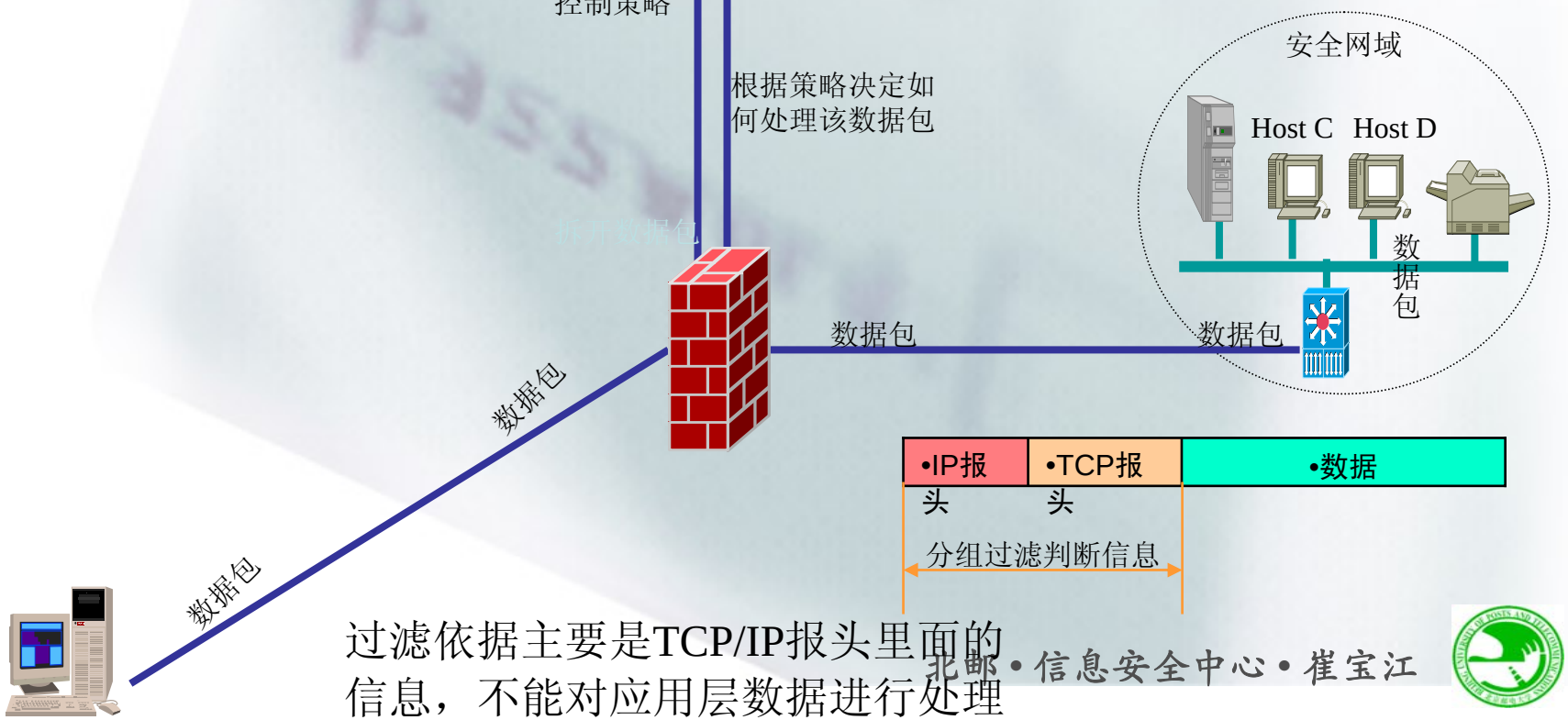
防火墙分类

- 根据保护对象分为：
  - 网络防火墙
  - 主机防火墙
- 根据防范技术分为：
  - 包过滤防火墙
  - 应用层代理
  - 全状态检测防火墙
  - 地址翻译防火墙

包过滤检查内容

•Source	•Destination	•Permit	•Protocol
•Host A	•Host C	•Pass	•TCP
•Host B	•Host C	•Block	•UDP

控制策略



过滤依据主要是TCP/IP报头里面的信息，不能对应用层数据进行处理

包过滤检查内容

- 数据包过滤一般要检查网络层的IP头和传输层的头：
  - IP源地址
  - IP目标地址
  - 协议类型（TCP包、UDP包和ICMP包）
  - TCP或UDP包的目的端口
  - TCP或UDP包的源端口
  - ICMP消息类型
  - TCP包头的ACK位
  - TCP包的序列号、IP校验和等

包过滤防火墙

服务方向	包方向	源地址	目标地址	包类型	源端口	目标端口	ACK
连接外部的telnet服务器	OUT	内部	外部	TCP	>1023	23	*
	IN	外部	内部	TCP	23	>1023	1
向外提供Telnet服务	IN	外部	内部	TCP	>1023	23	*
	OUT	内部	外部	TCP	23	>1023	1

包过滤防火墙优缺点

优点：

- 速度快，性能高
- 对用户透明

缺点：

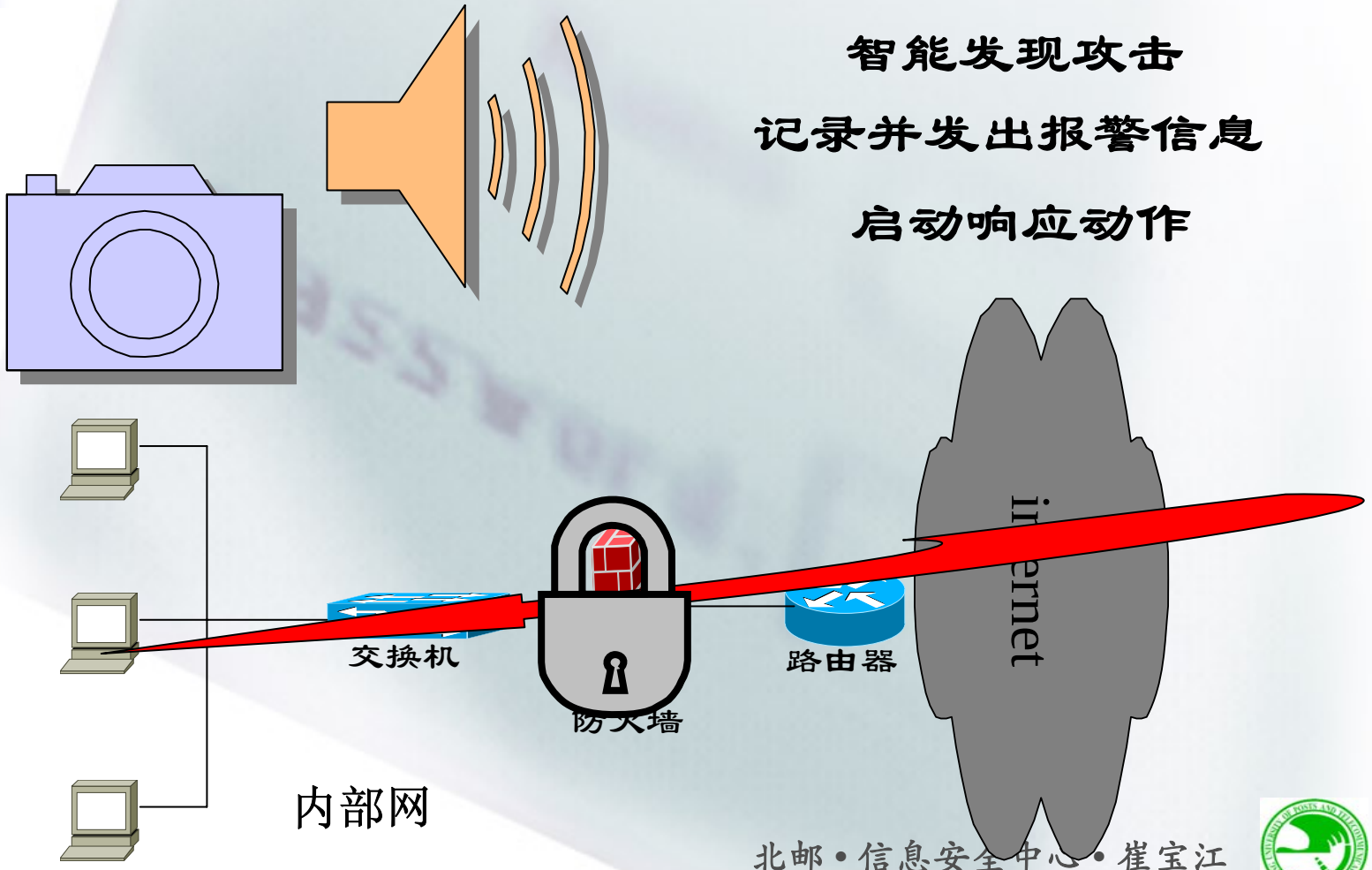
- 维护比较困难(需要对TCP/IP了解)
- 安全性低（IP欺骗等）
- 不提供有用的日志，或根本就不提供
- 不防范数据驱动型攻击
- 不能根据状态信息进行控制
- 不能处理网络层以上的信息
- 无法对网络上流动的信息提供全面的控制

目录

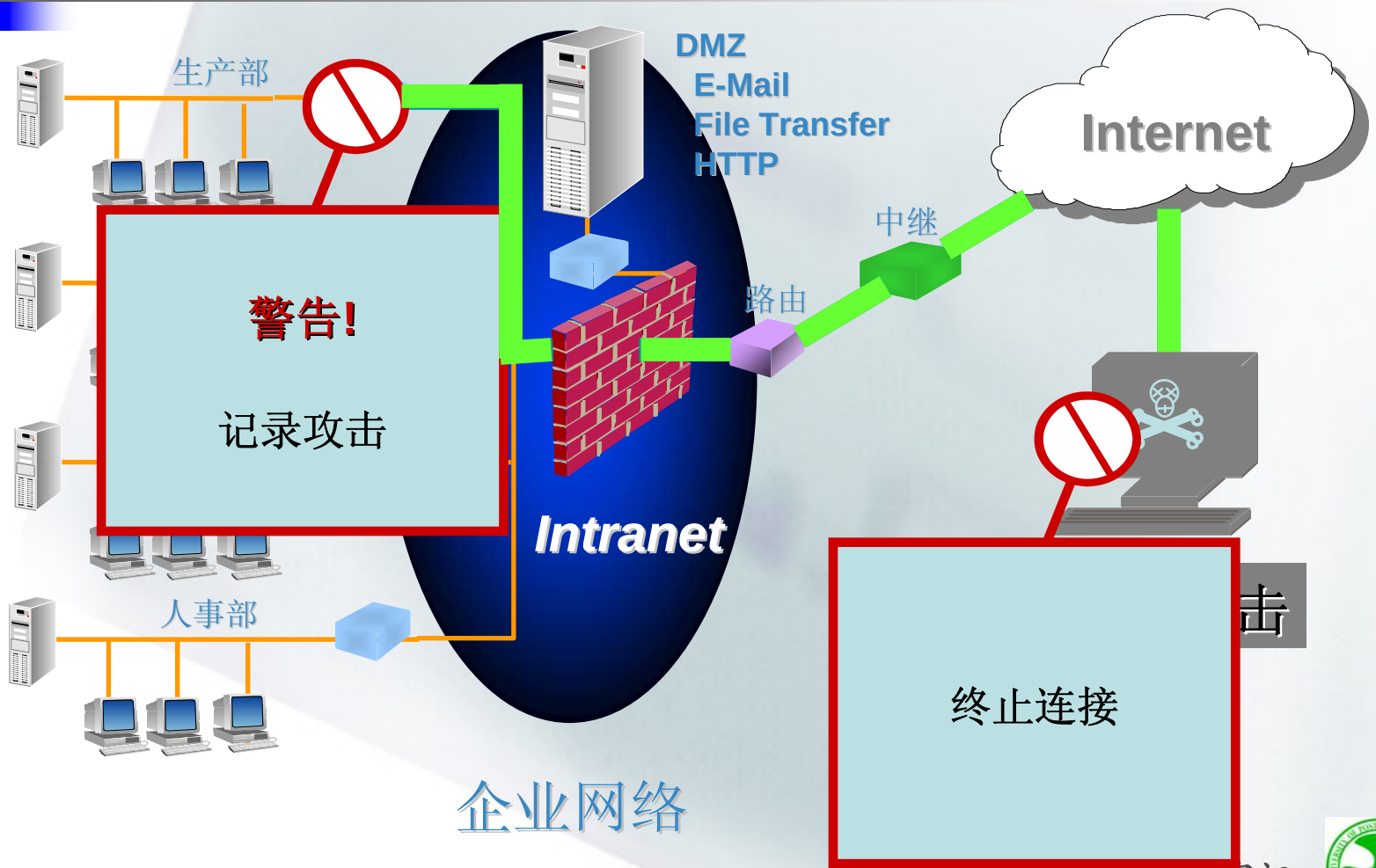
IDS

入侵检测系统（英文名称Intrusion Detection System或者称为IDS）工作在计算机网络系统中的关键节点上，通过实时地收集和分析计算机网络或系统中的信息，来检查是否出现违反安全策略的行为和遭到袭击的迹象，进而达到防止攻击、预防攻击的目的。

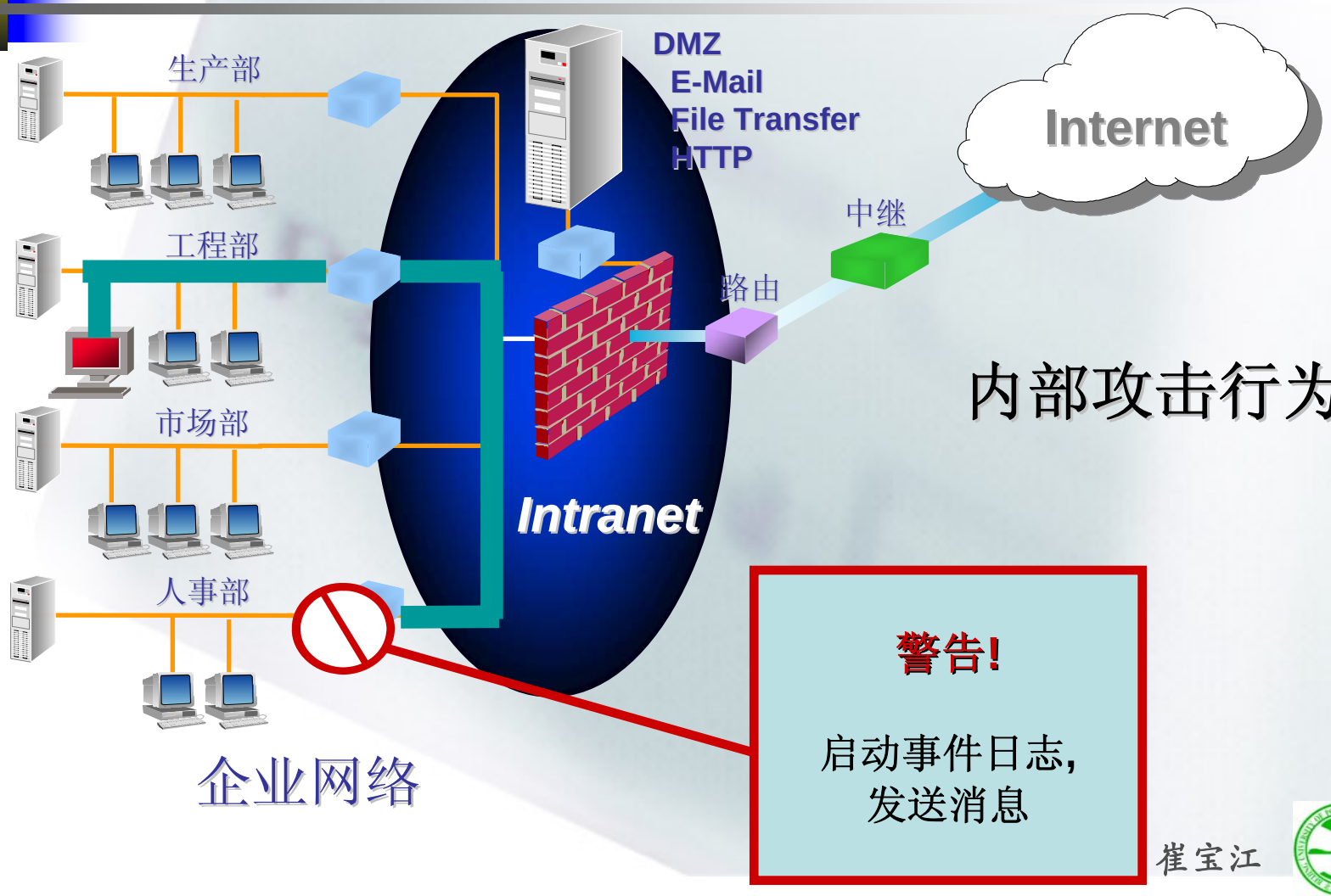
IDS的作用



IDS的作用



IDS的作用



崔宝江

NIDS

功能：

在网络关键点收集信息和分析，发现可疑行为。

缺陷：

能发现但难以阻止

FIREWALL & NIDS

功能互补，通过合理搭配部署和联动提升网络安全级别：

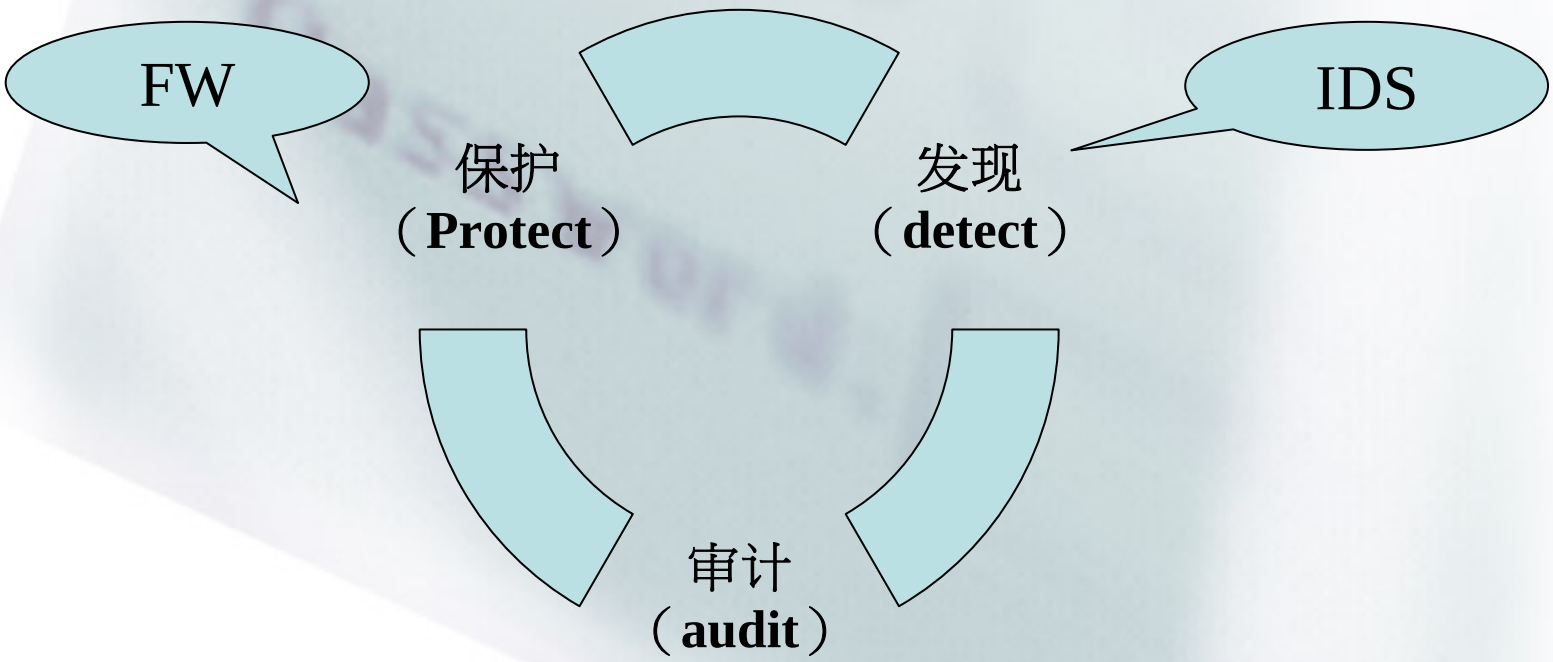
检测来自外部和内部的入侵行为和资源滥用

在关键边界点进行访问控制

攻击检测更新迅速，实时的发现和阻断

IDS&FIREWALL

- **相辅相成，在网络安全解决方案中承担不同的角色。**



flag1 flag, 2003-6-3

IDS和扫描器的关系

- IDS和扫描器都是简化管理员的工作，发现网络中的问题

扫描器是完全主动式安全工具，能够了解网络现有的安全水平

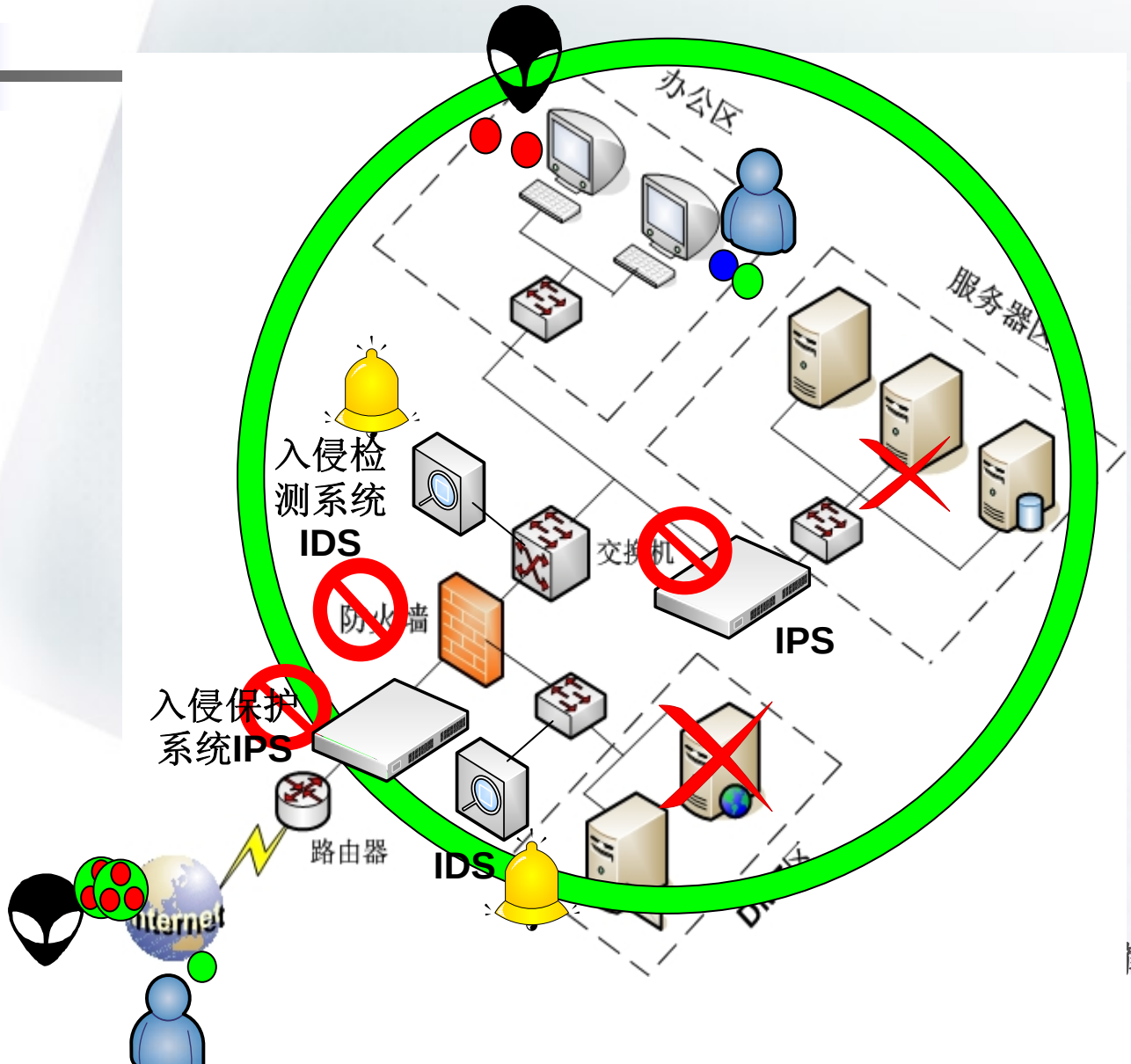
IDS是相对被动式安全工具，能够了解网络中即时发生的攻击

目录

IPS

- 背景：
  - 防火墙不能有效检测并阻断夹杂在正常流量中的攻击代码
  - IDS由于旁路部署，无法阻断攻击，亡羊补牢，侧重安全状态监控
- IPS的优点
  - 串联在线部署，主动防御，实时阻断攻击
  - 实现内容和应用层的拦截

如何防御攻击？



内容管理

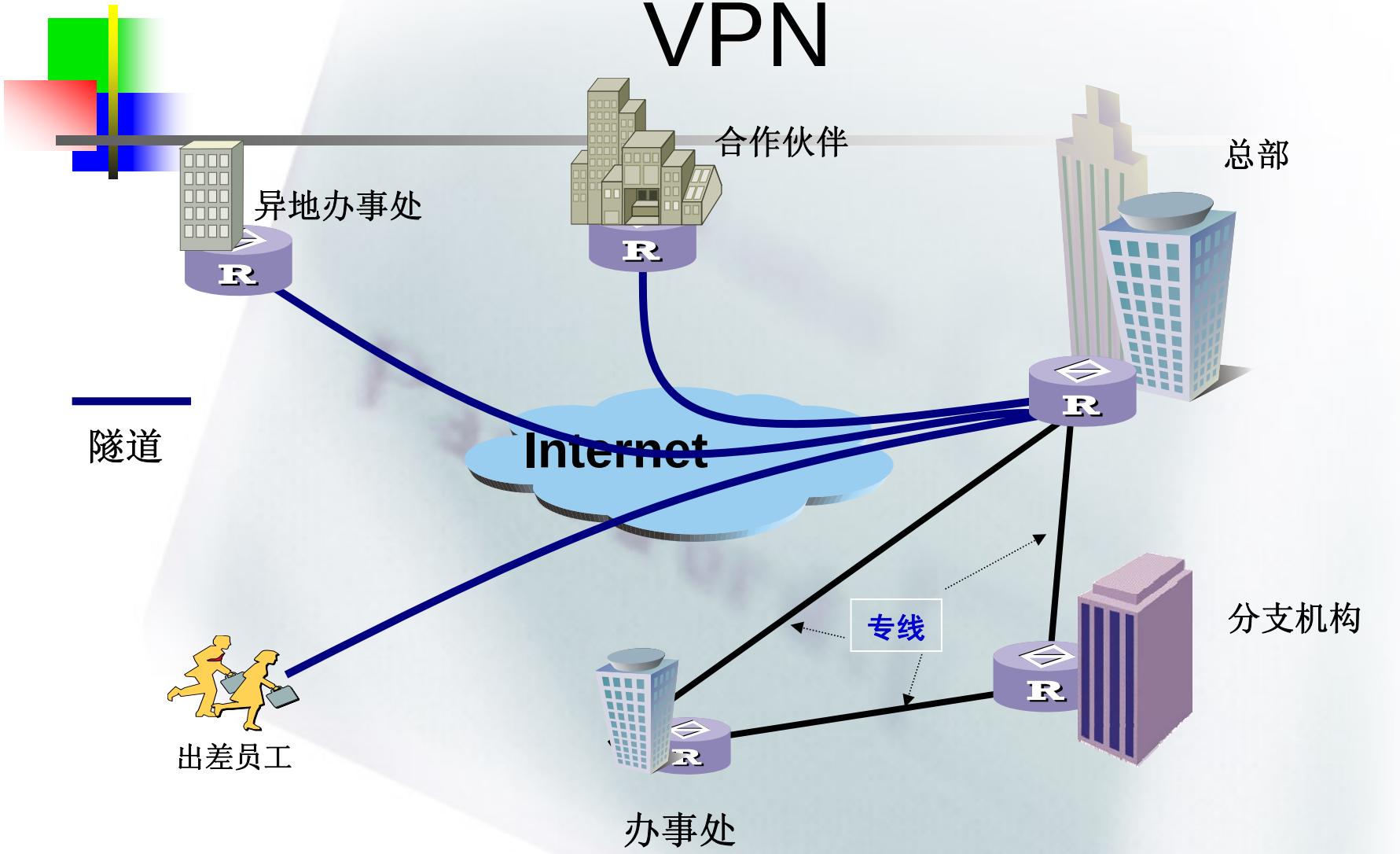
- 能够基于行为、时间、IP地址等多种条件组合，灵活控制用户上网行为，包括IM即时通讯、P2P下载、在线视频、网络流媒体及网络游戏等行为
- 对IM即时通讯、P2P下载等行为提供内容监控，及时发现恶意行为并进行阻断
- 全面抵御木马后门、广告软件、恶意程序等间谍软件功能，对间谍软件的通信和传播进行拦截并阻止对这些恶意程序的下载
- 支持审计功能，可以记录网络的通信报文，并解码回放，支持HTTP、SMTP、FTP、Telnet、POP3协议

目录

一. VPN概述

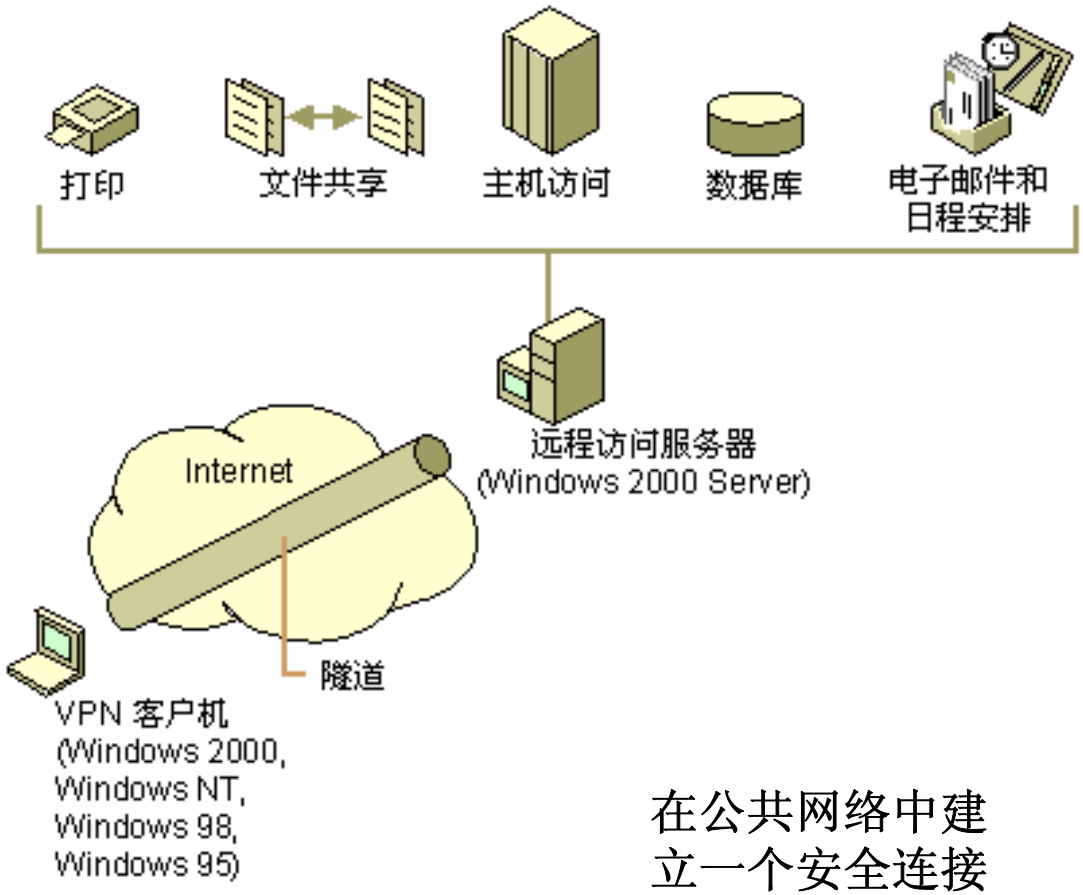
- 专用网的特点：
  - 封闭的用户群
  - 安全性高
  - 服务质量保证

VPN



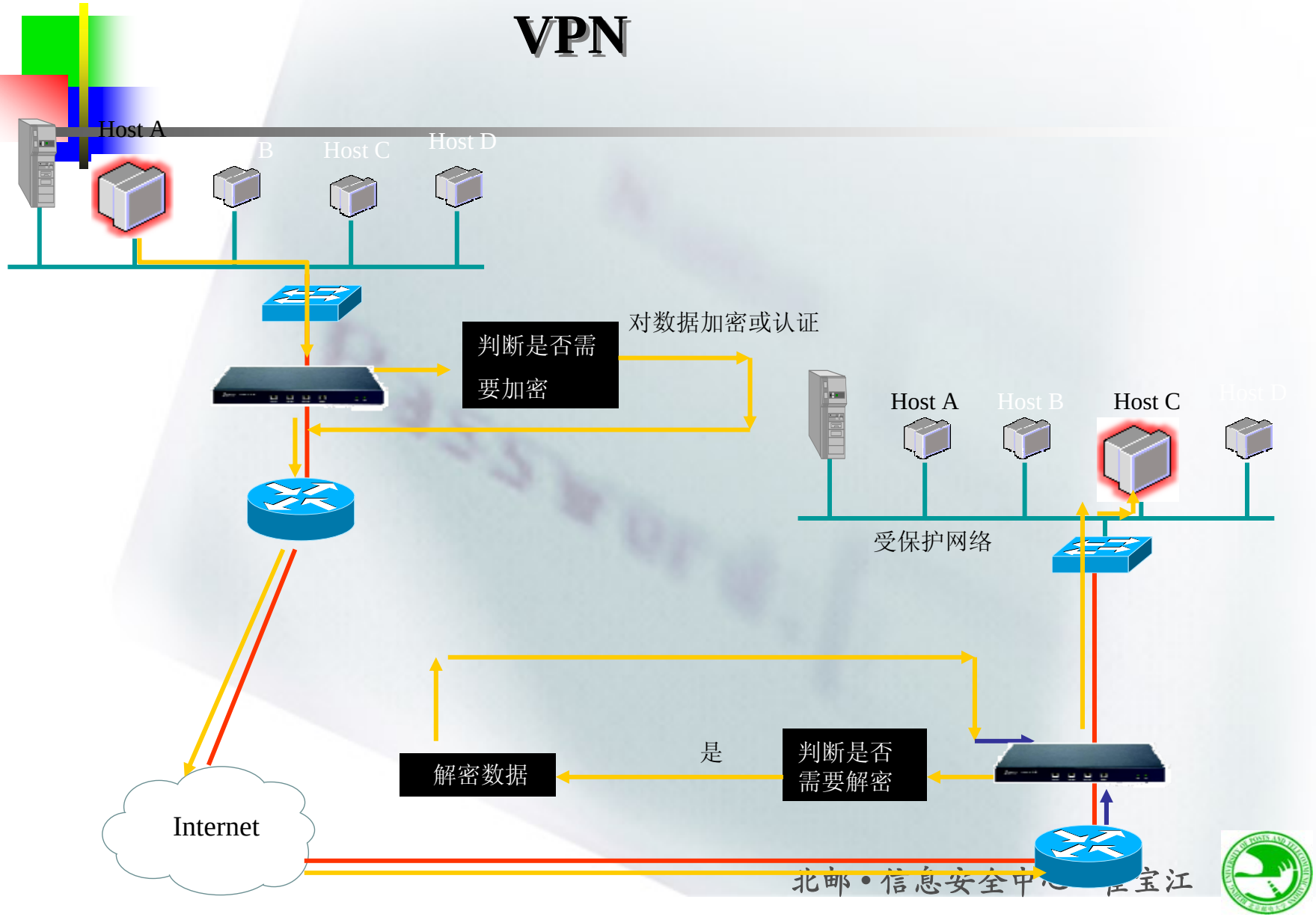
一. VPN概述

- VPN概述
  - 功能
    - 加密数据
    - 身份认证
    - 完整性检验
  - 优点
    - 成本低
    - 结构灵活



在公共网络中建立一个安全连接

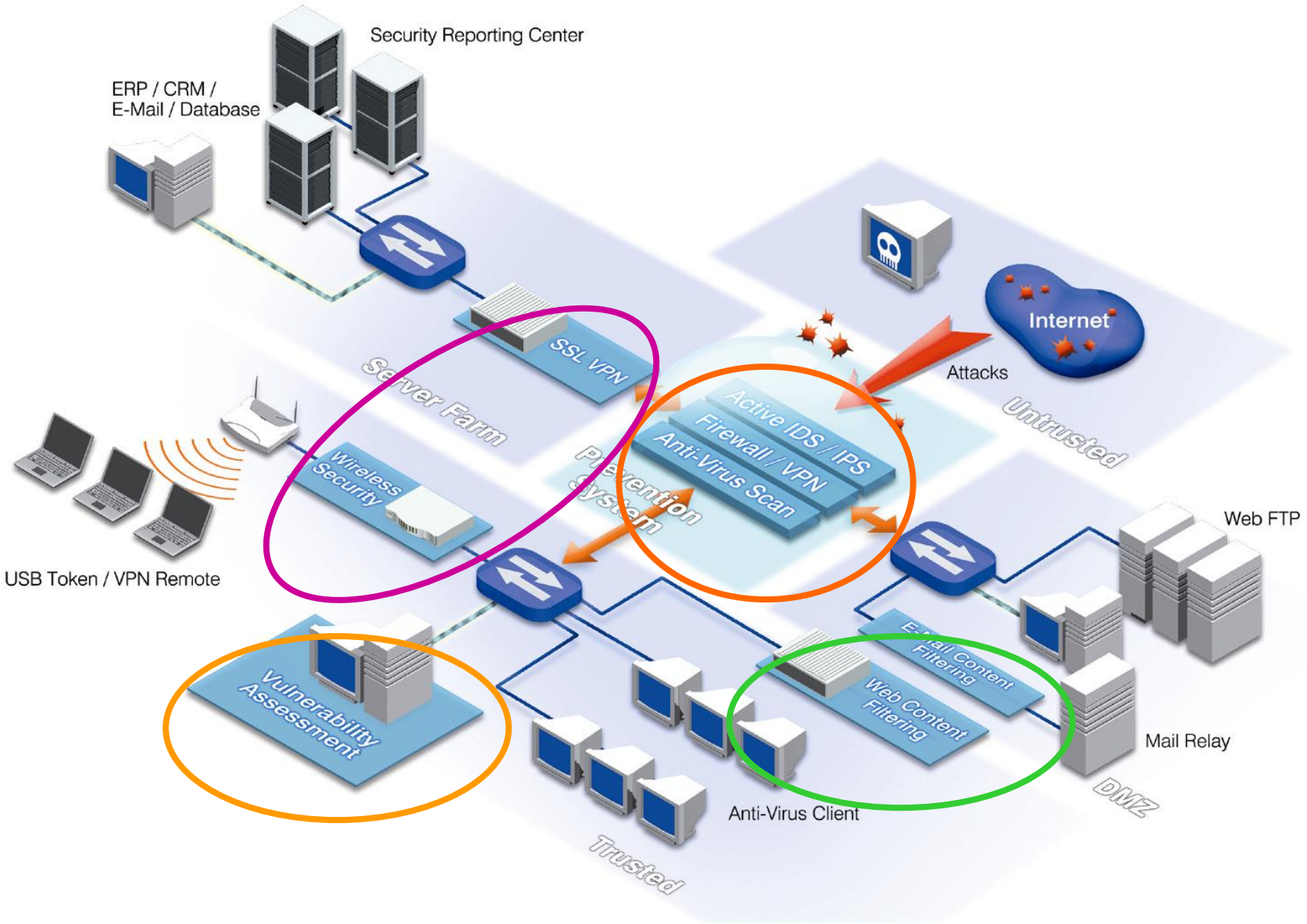
VPN



目录

网络安全基本组件

- 防火墙/虚拟专用网 (Firewall/VPN)
- 入侵防护系统 (Intrusion Prevention System)
- 病毒网关 (Application Anti-Virus gateway)
- 漏洞评估 (Vulnerability Assessment)
- SSL VPN网关 (SSL VPN Gateway)
- 无线安全网关 (Wireless Security Gateway)
- 网页内容过滤 (Web Content Filtering)
- 电子邮件内容过滤 (E-Mail Content Filtering)


Security Reporting Center
ERP / CRM /
E-Mail / Database
SSL VPN
Server Farm
Internet
Attacks
Untrusted
Active IDS / IPS
Firewall / VPN
Anti-Virus Scan
Prevention System
Wireless Security
USB Token / VPN Remote
Web FTP
Vulnerability Assessment
Web Content Filtering
Mail Relay
DMZ
Anti-Virus Client
Trusted

结束语

- 个人方面：提高警惕，避免End-User端的攻击
  - 在网络中（特别是一些论坛中），尽量避免泄漏本单位信息，如单位名称和EMAIL地址等。
  - 不要随便执行文件
  - 不要随便打开陌生的电子邮件
  - 不要连接到未知网站
  - 不要随意打开未知的URL
  - 密码不要太简单
  - 关闭文件共享
  - 不要使用系统默认值
  - 安装防病毒软件，并经常更新
  - 定期更新系统补丁

结束语

- 主机方面
  - 定期进行漏洞扫描
  - Integrity Check (ex. Tripwire、MD5Sum)
  - 确认每一个在执行的Service用途
  - 确认每一个在执行的Process用途
  - 确认每一个监听端口的用途，以及建立连接程序的用途。(netstat、fport、TCPView)
  - 定期更新防病毒软件规则
  - 确认安装最新的Service Pack及补丁程序

结束语

- 网络方面
  - 定期进行漏洞扫描
  - 限制一般User，不可在内部网络上进行漏洞扫描
  - 使用防火墙，防止外部对内部的扫描
  - 流量监控
  - 连接监控
  - 使用IDS，防止来自内部的攻击
  - 定期检查系统Log

Q & A