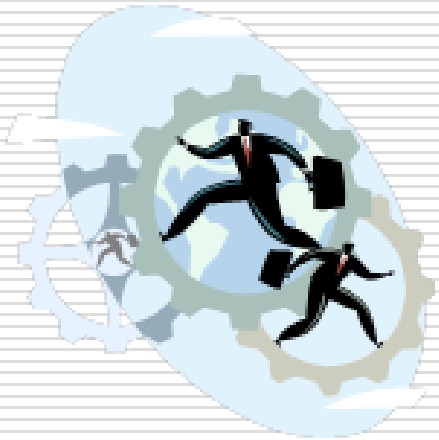


操作系统安全

1 系统安全概述

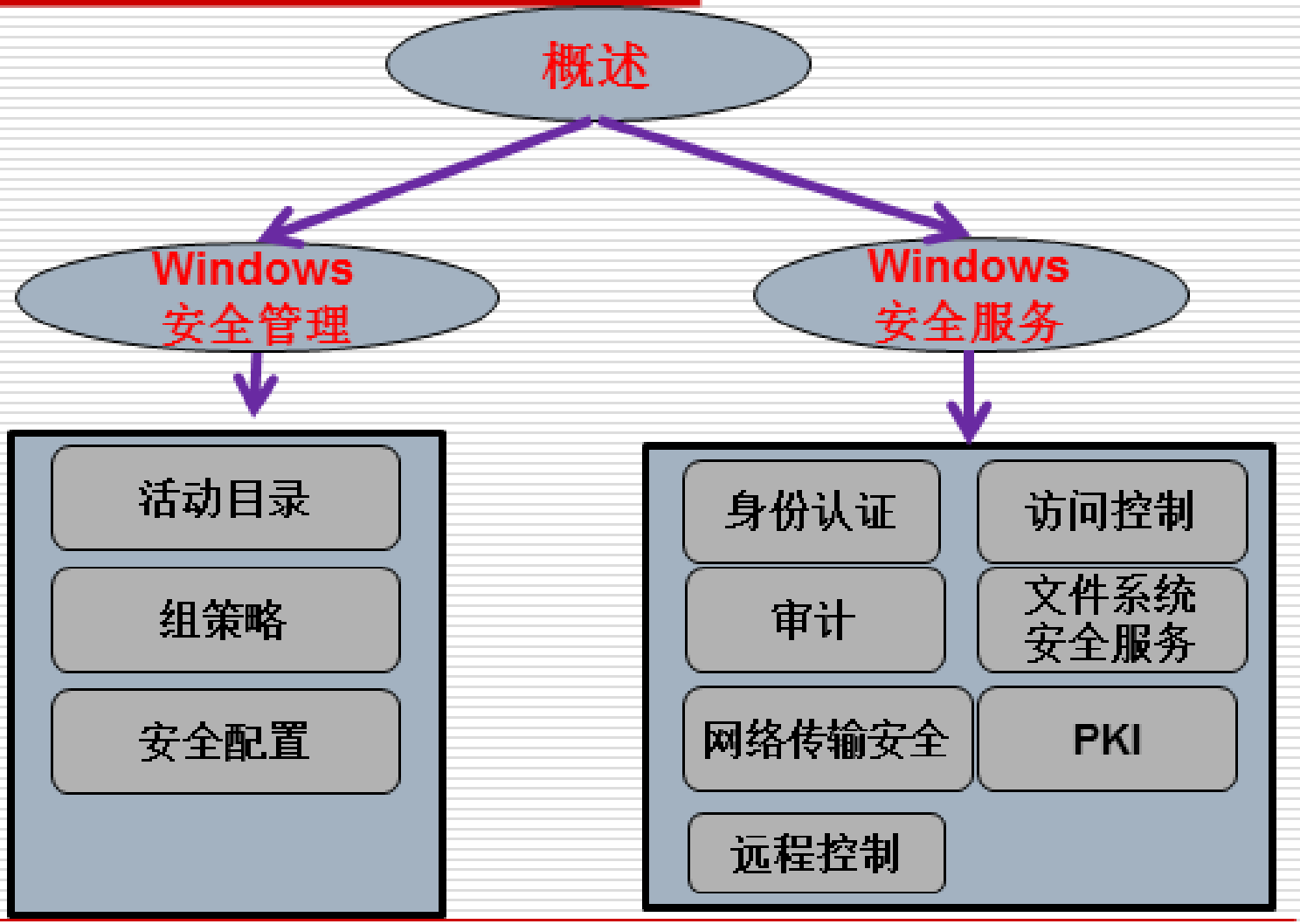
张爱娟

- 前导：网络安全，计算机网络
- 课程从计算机网络防御的角度，介绍了操作系统的安全原理和安全技术；

  目的在于理解分布式网络环境下的安全体系结构和构成组件，掌握具体的安全防御措施和技术，可以对系统及服务安全问题进行配置、分析与跟踪。示例以windows操作系统为主 。

- 总学时：48(讲课学时：40 实验学时：8)
- 参考

课程体系



2020/2/21

3

目录

- 系统安全概述
- Windows系统安全概述
- 活动目录
- 身份认证
- 访问控制
- 文件系统安全
- PKI
- 网络传输安全
- 应用层服务安全
- 组策略、审计及安全配置
- 本地安全

- 考核

50% 平时成绩（实验+作业）

50% 考试成绩

1 作业

名称	内容
活动目录	活动目录的搭建，测试和使用
组策略	账户策略、本地策略、公钥策略、软件限制策略，IP安全策略，软件设置，登陆脚本服务，远程安装服务和管理模版设置
认证、授权	身份认证、单点登录、分布式自主访问控制
PKI	PKI的搭建和使用，生成故障恢复代理证书,web服务器SSL认证证书
文件系统安全	NTFS权限、透明加密；磁盘阵列；数据恢复
VPN服务	设置VPN服务，并提供客户端上网服务

2 综合的企业防御框架方案（我们学到的服务要有配置方案）

1 系统安全概述

1.1 安全威胁

1.2 安全防御

1.3 防御体系结构

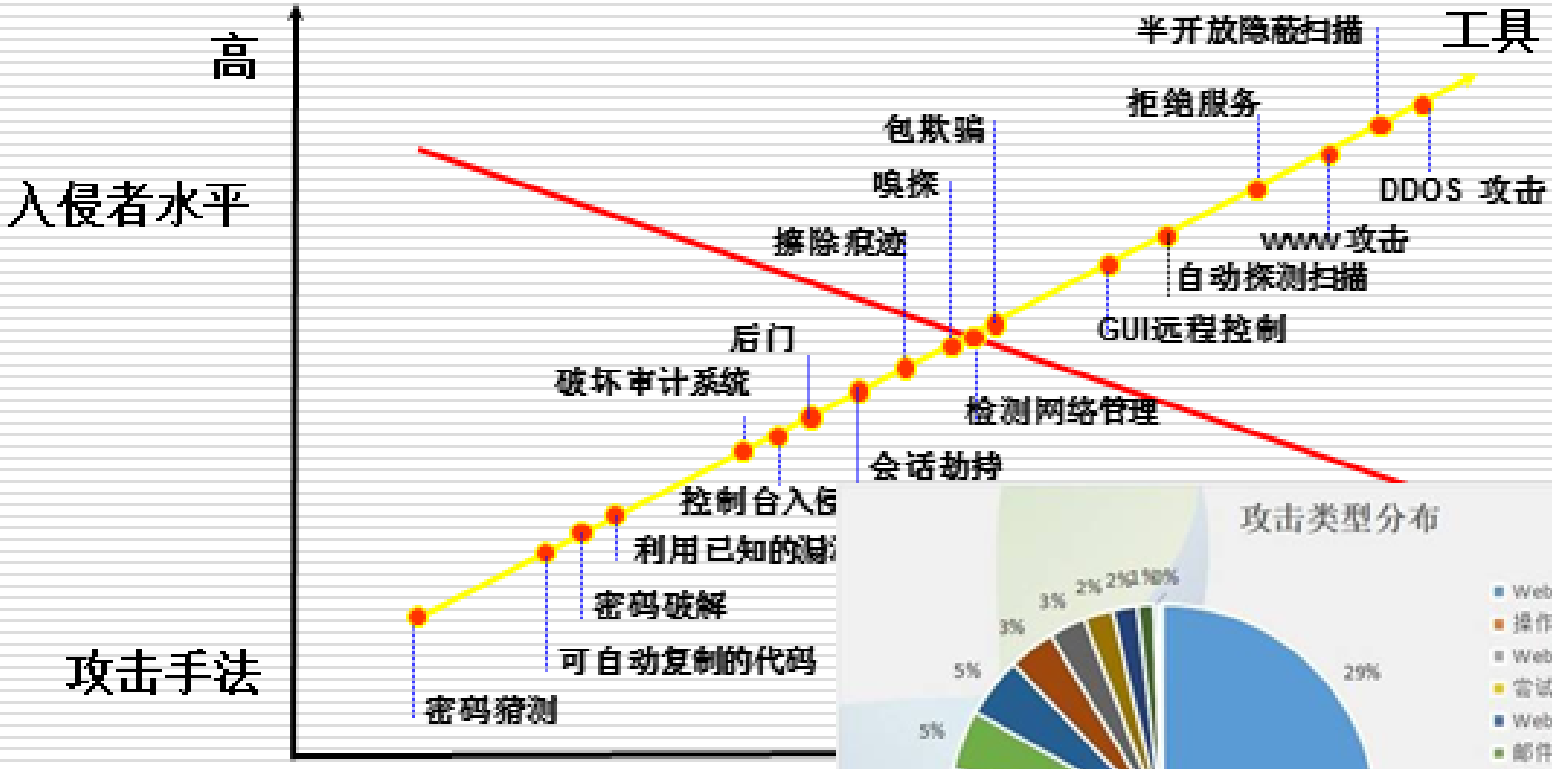
1.1 网络中存在的安全威胁

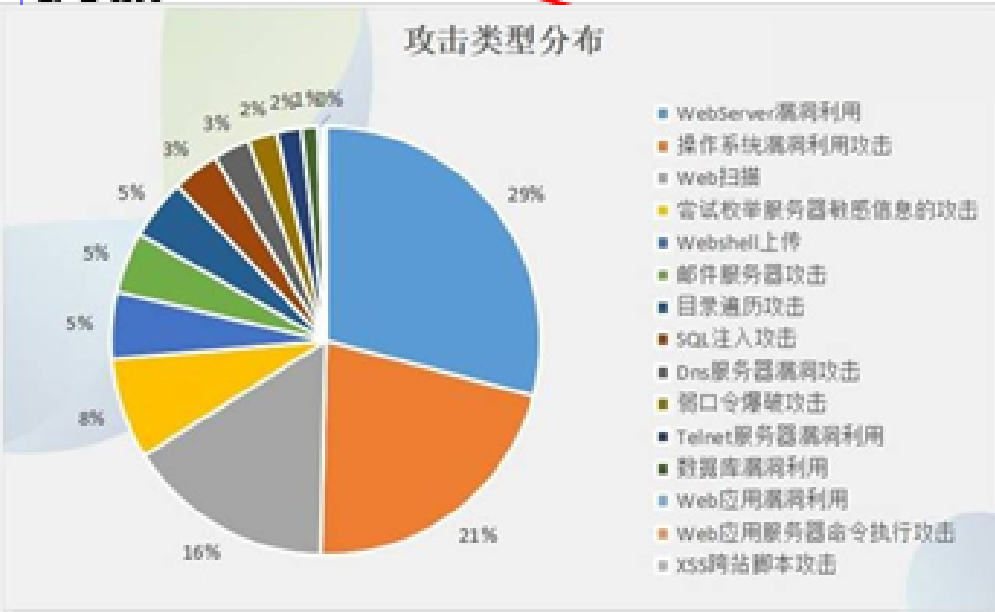
- 信息丢失，篡改，销毁
- 内部，外部泄密
- 部署不当：身份鉴别、访问控制、审计配置隐患，未安装程序补丁（未清除调试文件）。

- 计算机病毒，蠕虫，木马
- 不安全的直接对象引用、异常处理[过细、忽略泛化抛出]
- 后门，隐蔽通道[不完备的身份鉴别，会话管理，访问控制]
- 逻辑炸弹[不完备的业务逻辑验证]
- 缓冲区溢出
- SQL注入，跨站脚本攻击，跨站请求伪造[XSS, CSRF] 等。

- 拒绝服务攻击，篡改消息，伪造身份
- 流量、流向分析:数据嗅探

攻击方式发展


高
入侵者水平
攻击手法
工具
半开放隐蔽扫描
拒绝服务
包欺骗
嗅探
DDOS 攻击
擦除痕迹
www攻击
自动探测扫描
后门
GUI远程控制
破坏审计系统
检测网络管理
会话劫持
密码破解
可自动复制的代码
密码猜测


攻击类型分布
29%
21%
16%
8%
5%
5%
5%
3%
3%
2%
2%
2%
WebServer漏洞利用
操作系统漏洞利用攻击
Web扫描
尝试枚举服务器敏感信息的攻击
Webshell上传
邮件服务器攻击
目录遍历攻击
SQL注入攻击
Dns服务器漏洞攻击
弱口令爆破攻击
Telnet服务器漏洞利用
数据库漏洞利用
Web应用漏洞利用
Web应用服务器命令执行攻击
XSS跨站脚本攻击

1.2 信息安全防御

- 网络空间安全
  - **网络攻击-Offense（威慑）**

    利用计算机网络中断、抵制、削弱或摧毁敌方计算机和网络中的信息，以及计算机和网络本身的活动
  - **网络利用-Exploitation（情报）**

    收集来自对方信息系统和网络的数据的网络活动
  - **网络防御-Defense（运维）**

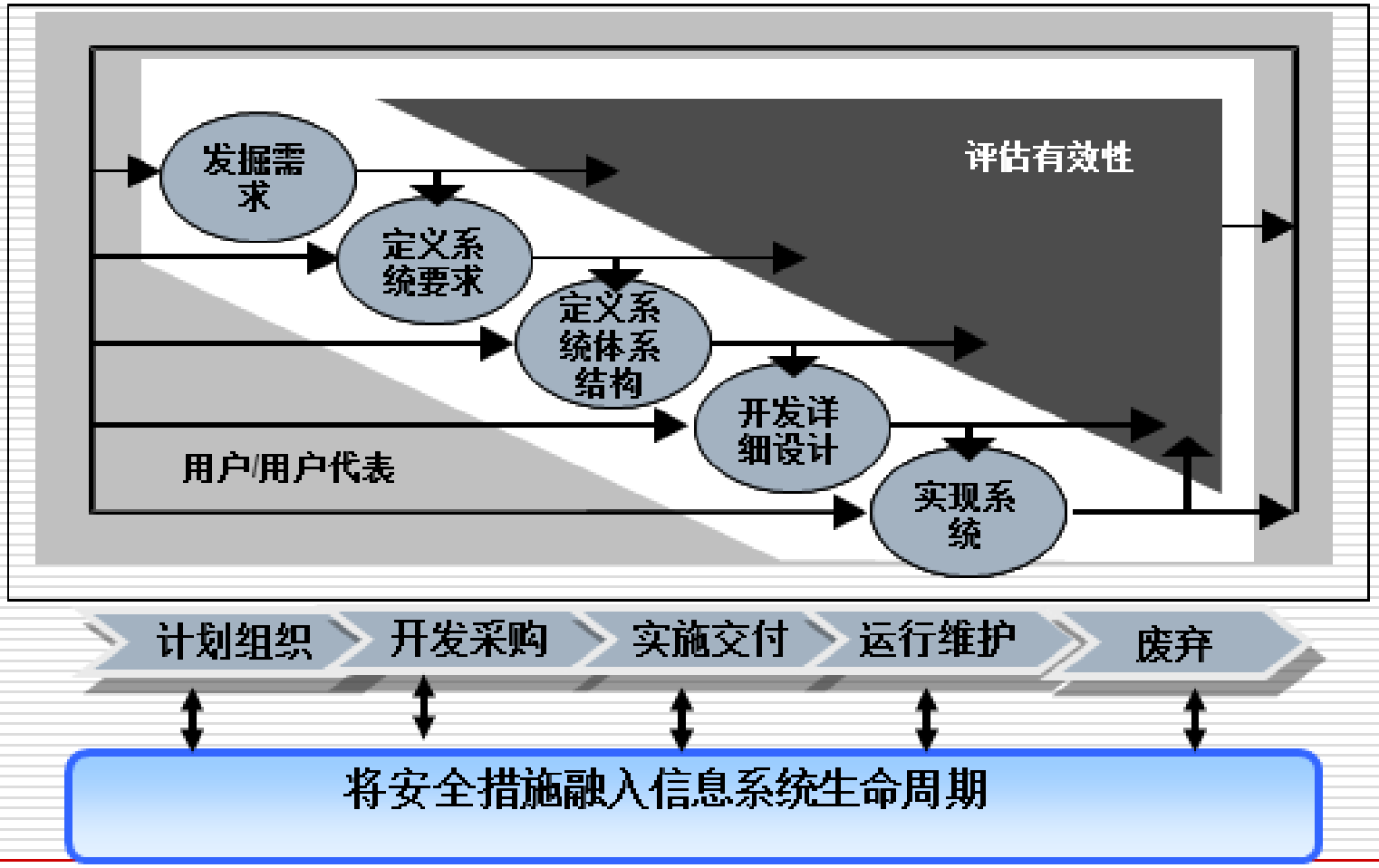
    保护信息、服务、计算机和网络免受扰乱或摧毁的措施，主要行动包括监视、检测和响应所有非法授权的计算机行动。

1.2 信息安全防御

- 信息安全防御体系构成的要素
  - 信息安全工程过程
  - 信息安全技术体系
  - 信息安全管理体系
  - 高素质的人员队伍

1.2 信息安全防御

科学的信息安全工程过程

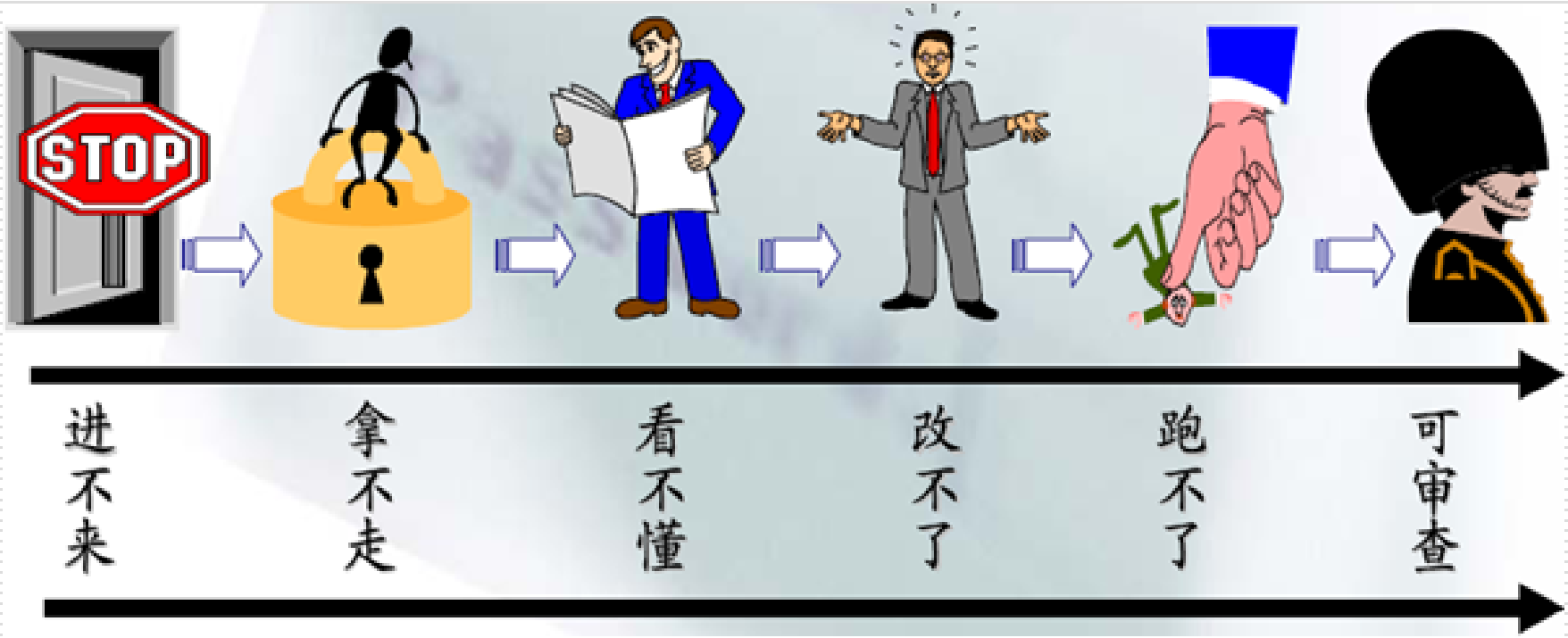


1.2 信息安全防御

- **信息安全“技管并重”的原则**
  - 信息安全的成败取决于两个因素：技术和管理。
  - 安全技术是信息安全的构筑材料，安全管理是真正的粘合剂和催化剂。
  - 对于信息安全，到底是技术，还是管理更重要？
    - 技管并重。

信息安全防御的目的

- 对非法使用达到如下控制目的：



认证服务　访问控制服务　机密性服务　完整性服务　非否认服务

安全防御服务

- 在计算机网络中，主要的安全防护措施被称作安全服务。目前主要有五种安全服务
  - **认证服务：**提供实体的身份的保证
  - **访问控制服务：**防止对资源的非授权使用，控制授权范围内的信息流向及行为方式。
  - **机密性服务：**对数据提供保护使之不被非授权地泄露，如VPN, 文件加密服务。
  - **完整性服务：**保护数据防止未授权的改变、删除或替代。
  - **非否认服务：**提供凭证，防止用户否认或抵赖已接收到相关的信息及实施的相关操作。

安全机制

实现以上安全服务的安全机制主要包括：

- **认证交换机制**
  - 证实主体身份。
- **访问控制机制：**
  - 对主体的身份和有关主体的信息进行认证，决定对其授权，防止非法访问和利用系统资源。
- **加密机制**
- **数字签名机制**
- **数据完整性机制**
  - 顺序检测、序列号、时间戳、密码检验和等。

安全机制

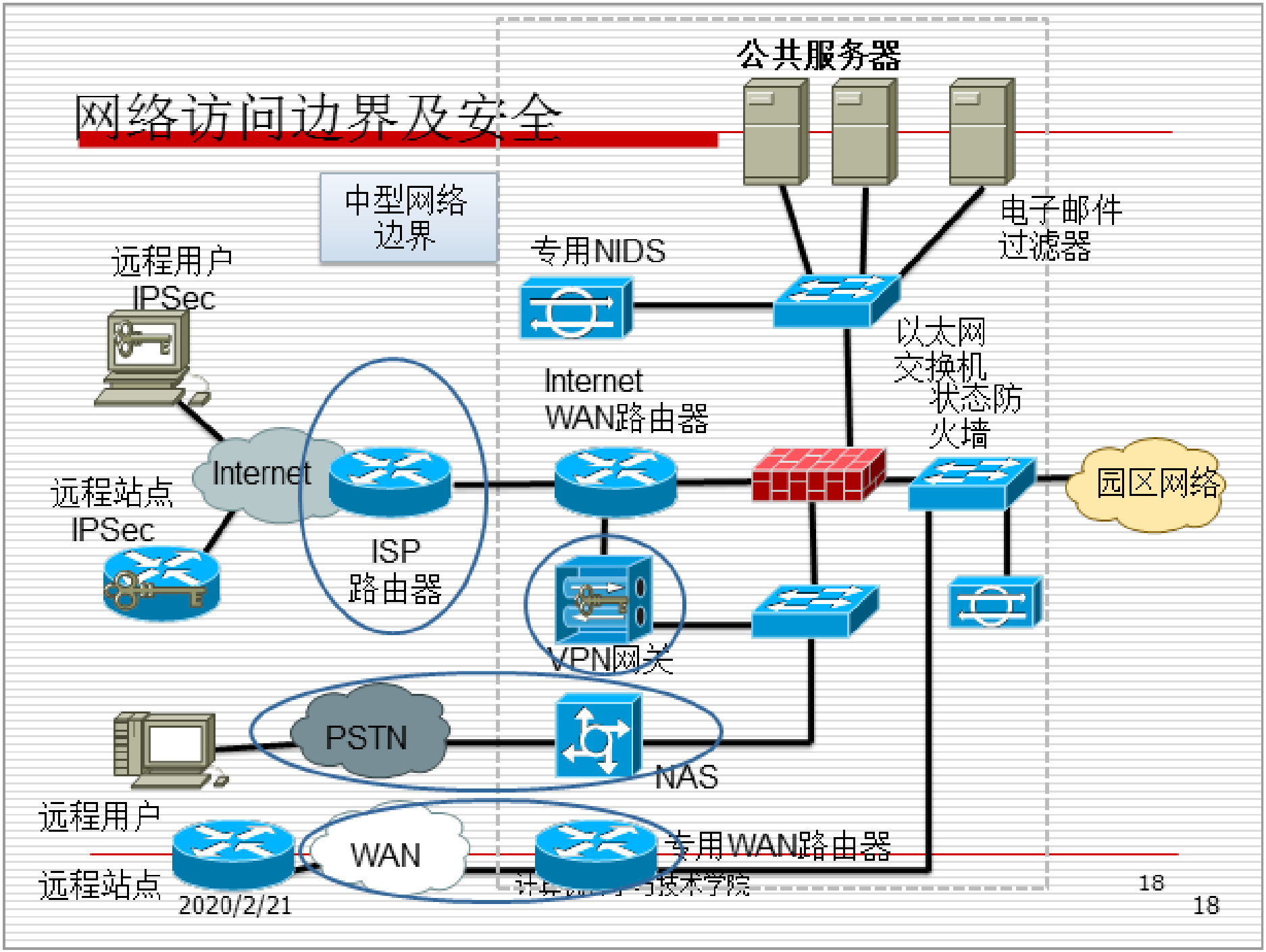
- **公证机制**

用于保证两个或更多个实体间通信数据的某种特性，如它的完整性、流/时间或目标等。由可信赖第三方TTP(Trusted Third Party)以可测试方式提供这类保证。

- **路由控制机制**

为数据传送动态地或预先安排选定路由，通信系统可能检测主动或被动攻击，因此希望网络服务提供者建立经由不同路由的连接。类似地，数据可能载有某种安全标记指示由安全策略所禁止通行的某些网络或全连路。

- **业务流量填充机制**
  - 属于数据流的加密手段，防止业务量分析。数据流中嵌入一些虚假信息，来掩盖正常的通信特征，从而阻止对手企图使用流量分析，保护业务流的机密性。


网络访问边界及安全
公共服务器
中型网络
边界
电子邮件
过滤器
专用NIDS
远程用户
IPSec
以太网
交换机
Internet
WAN路由器
状态防
火墙
Internet
园区网络
远程站点
IPSec
ISP
路由器
VPN网关
PSTN
NAS
远程用户
WAN
专用WAN路由器
远程站点
2020/2/21
18

不同连通的首要问题：身份识别

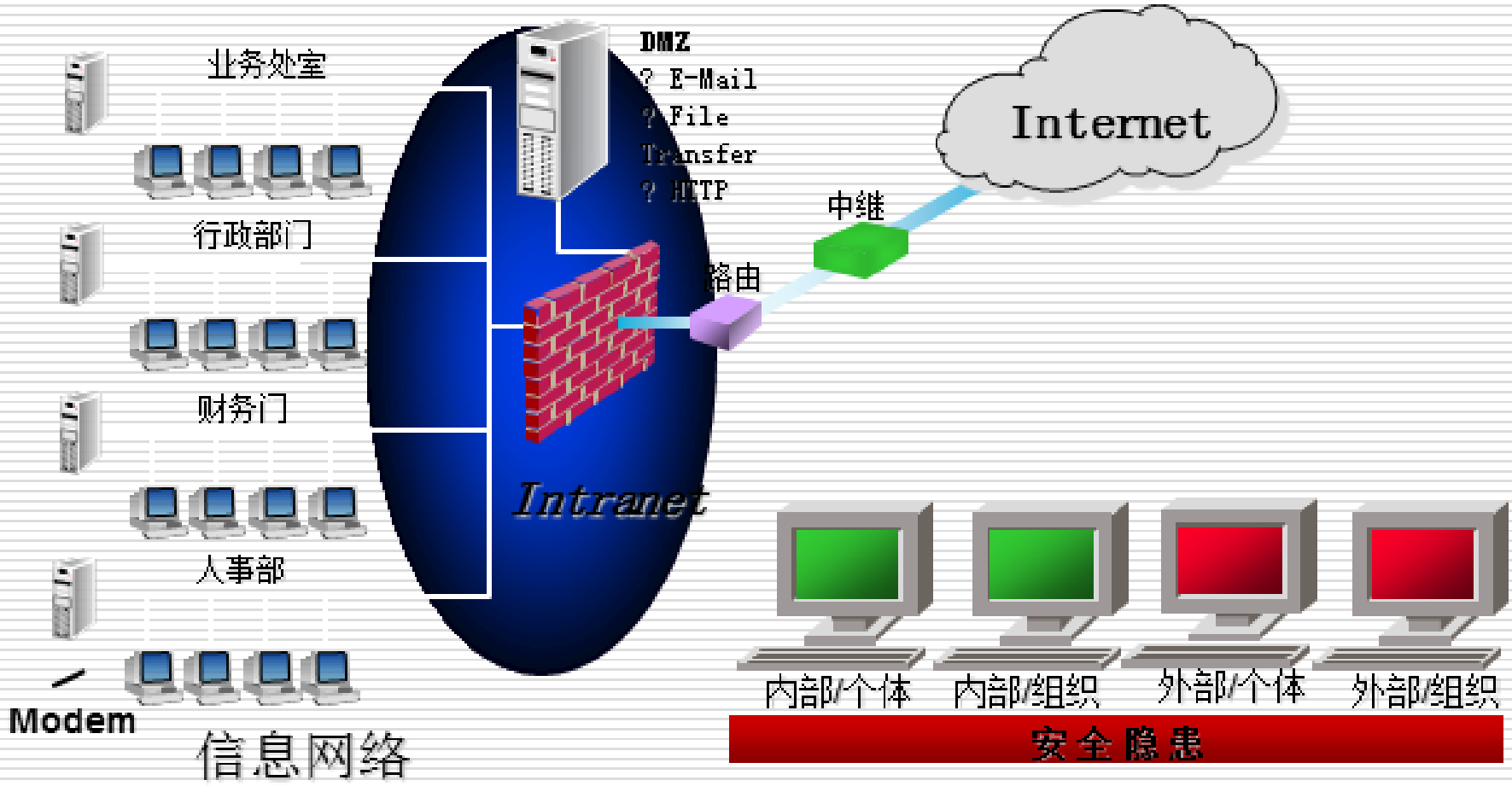
- 站点到站点VPN—与专用WAN链路类似，唯一的区别在于对流量的加密
  - 加密保护由隧道两端的可信设备执行
- 远程用户VPN—用户名/口令（更适宜用OTP (one-time password ），也可使用数字证书
- PSTN拨号—用户名和OTP认证，拨号使用一对专用网络访问服务器（NAS），然后通过防火墙。
- Internet WAN链路—从Internet进来的流量只通过IP地址识别。

不同连通的首要问题：身份识别

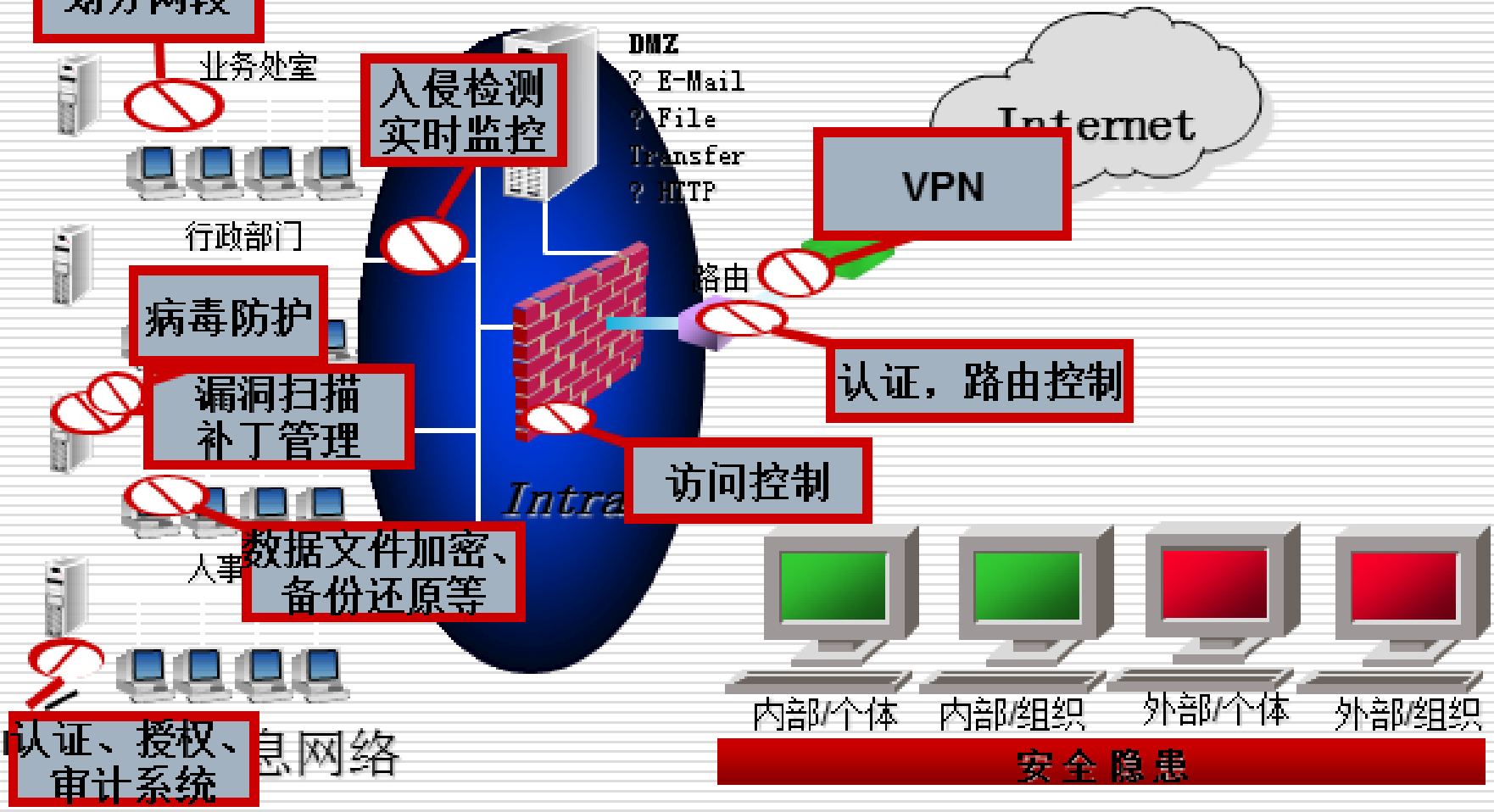
- 专用WAN链路—可使用任何身份识别技术
  - 在网络级别—IP地址
  - 在应用级别—用户名/口令,等
- 公共服务器—根据应用程序不同，需要对用户有额外的身份识别要求
  - 基本Web服务器—接收来自有效地IP地址并且通过防火墙的所有请求（如果服务器必须识别连接方的身份，可以通过HTTPS连接实现）

1.3信息安全防御体系结构框架

1、常见企业网络体系：



进一步完善的信息安全技术体系

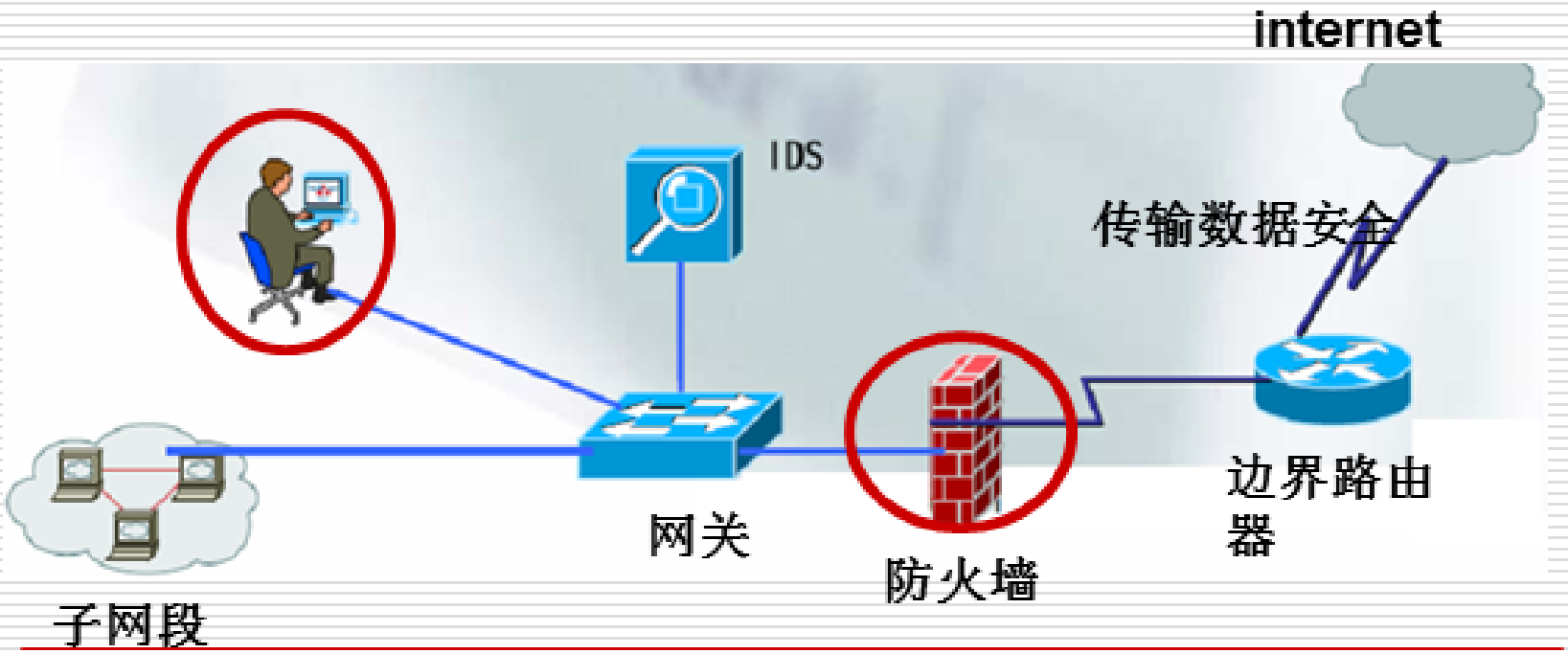


网络流数据安全

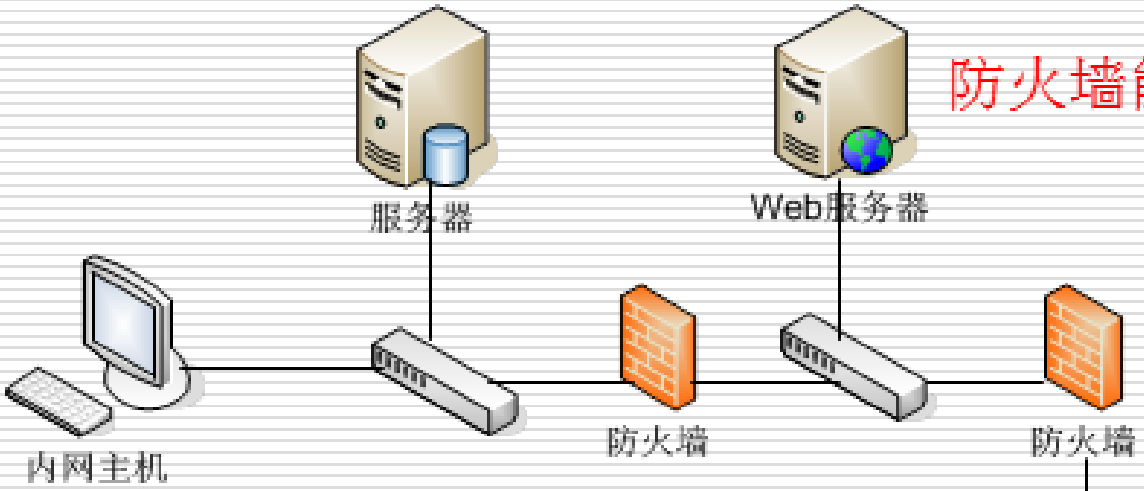
静态应用数据安全

应用程序级安全(认证、授权、审计)

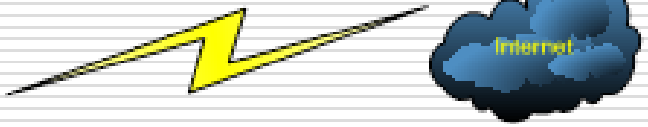
操作系统级安全(认证、授权、审计、数据安全、防病毒、漏洞管理、部署管理)



纵深防御体系的安全管理需求



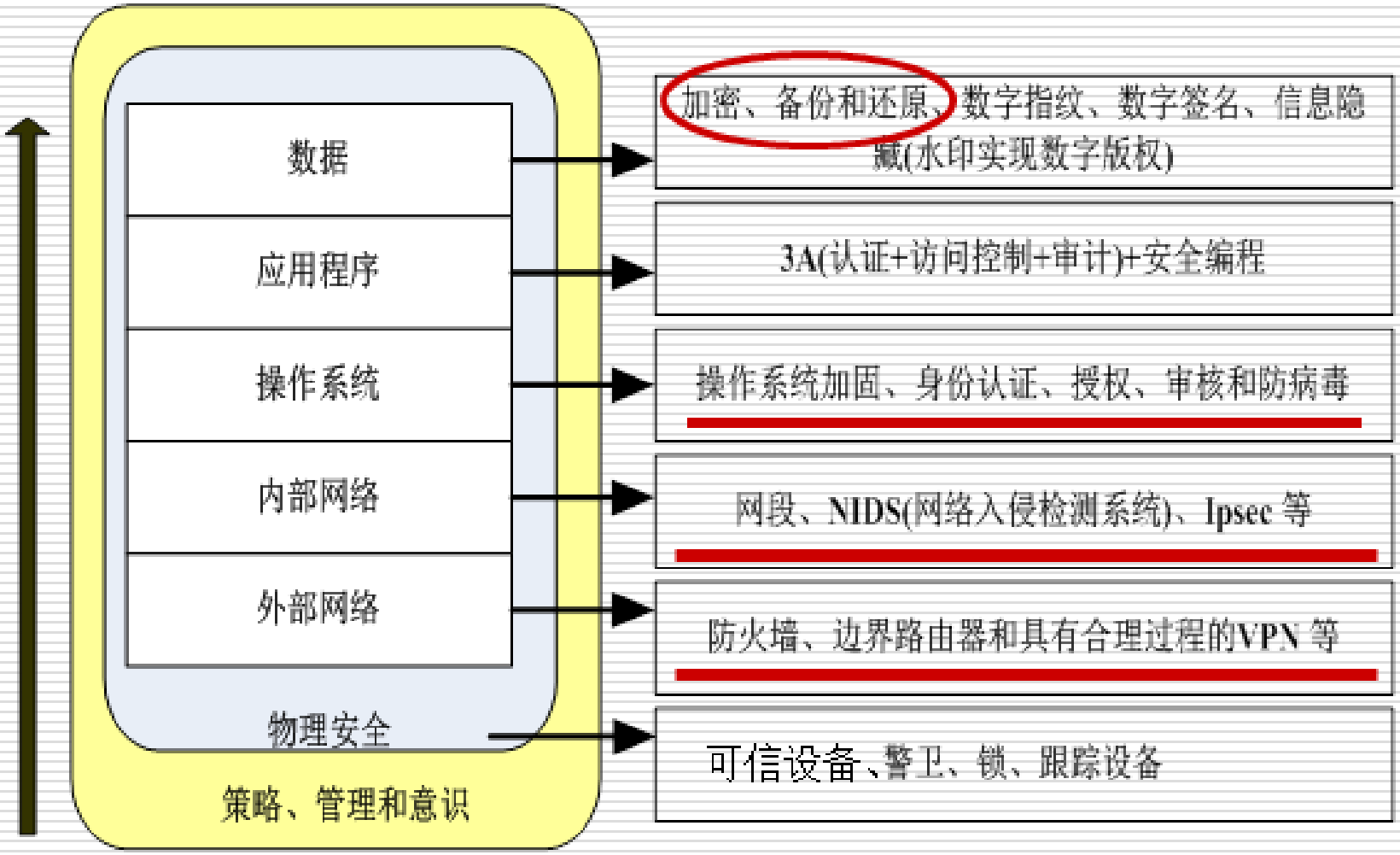
防火墙能解决这样的问题吗？

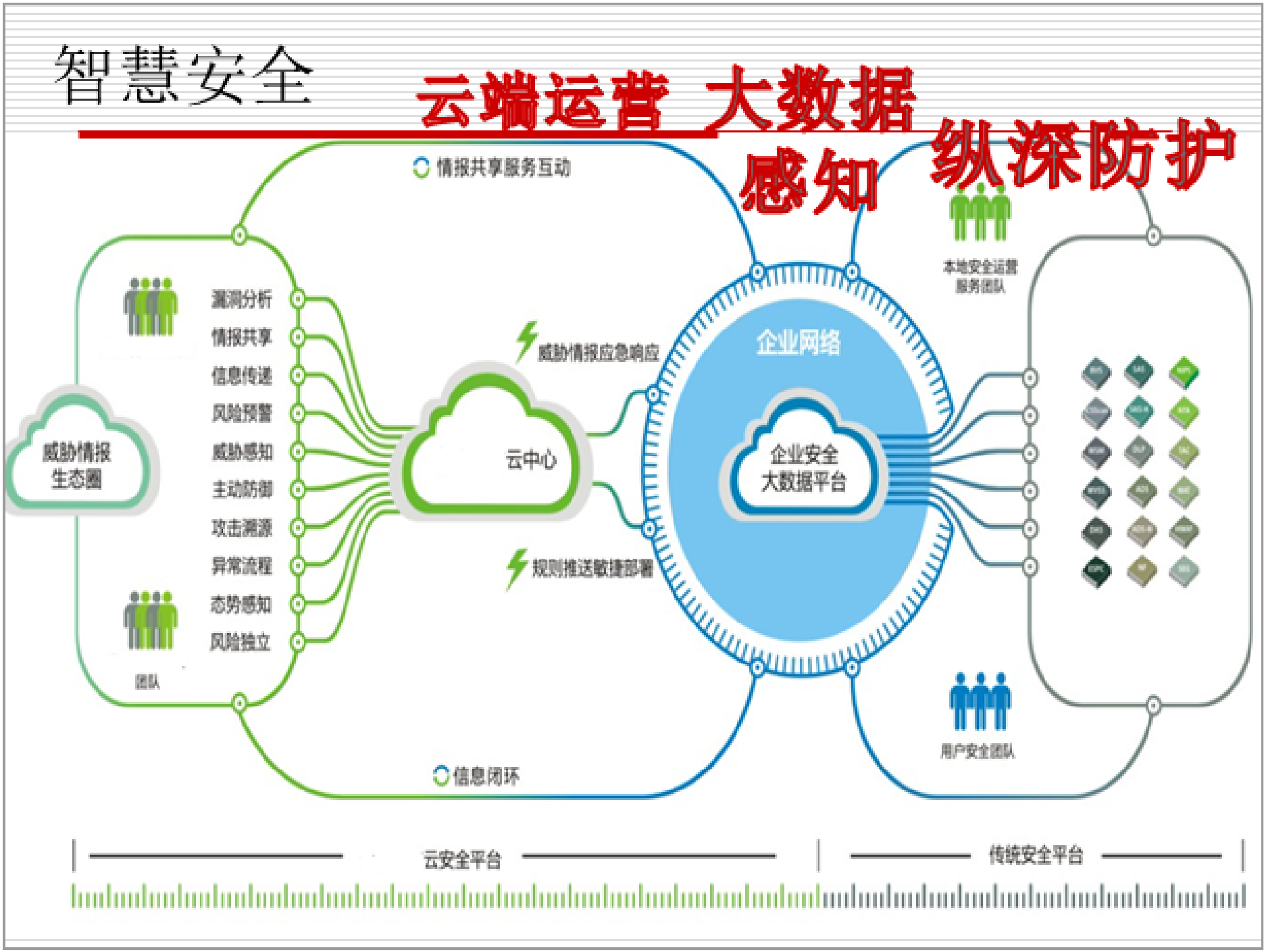


WO!3G

精心设计的网络防御体系，因违规外连形同虚设

1.3信息安全分层防御体系




智慧安全
云端运营 大数据
感知 纵深防护
情报共享服务互动
威胁情报
生态圈
漏洞分析
情报共享
信息传递
风险预警
威胁感知
主动防御
攻击溯源
异常流程
态势感知
风险独立
团队
云中心
威胁情报应急响应
规则推送敏捷部署
企业网络
企业安全
大数据平台
本地安全运营
服务团队
用户安全团队
信息闭环
云安全平台
传统安全平台

小结

- 安全威胁介绍
- 信息安全防御概述
- 纵深防御体系结构：由物理层、外部网络、内部网络、操作系统层、应用程序层、数据层的安全服务及 策略和管理组成。

课程中的实验环境

环境配置

- 需要分布式网络环境，因此最少应该有三个独立的操作系统，而且三个操作系统可以通过以太网通信
- 利用虚拟机搭建分布式平台或者利用实验室平台搭建分布式平台

虚拟机软件VMware

- 常用VMware和Virtual PC
- VMware：多平台虚拟软件
- 在多平台下测试代码和漏洞非常有用。
- 在VMware虚拟系统上感染了恶意软件不会影响到宿主机器，可以通过加载快照文件恢复被感染了的虚拟系统

安装&配置VMware虚拟机

- VMWare的常用的是两种联网方式：

（1）Used Bridged networking

- 虚拟机操作系统的IP地址可设置成与主机操作系统在同一网段，虚拟机操作系统相当于网络内的一台独立的机器，网络内其他机器可访问虚拟机上的操作系统，虚拟机的操作系统也可访问网络内其他机器。

（2）User network address translation（NAT）

- 实现主机的操作系统与虚拟机上的操作系统的双向访问。但网络内其他机器不能访问虚拟机上的操作系统，虚拟机可通过主机操作系统的NAT协议访问网络内其他机器。

配置VMware虚拟机

- 待安装的操作系统，其中有3台需安装windows server 2003或更高版本的2008,2012,2016,2019 server版。
- 另外一台虚拟机上可安装客户机，xp/win7/win10 都可以，如果想装服务器版本也可以 。

- 信息安全实验室网站
  - 202.119.201.219
  - 操作系统安全子模块