网络攻击与防御

刘智
西南石油大学 计算机科学学院
zhi.liu@swpu.edu.cn

第五章 网络安全防护系统

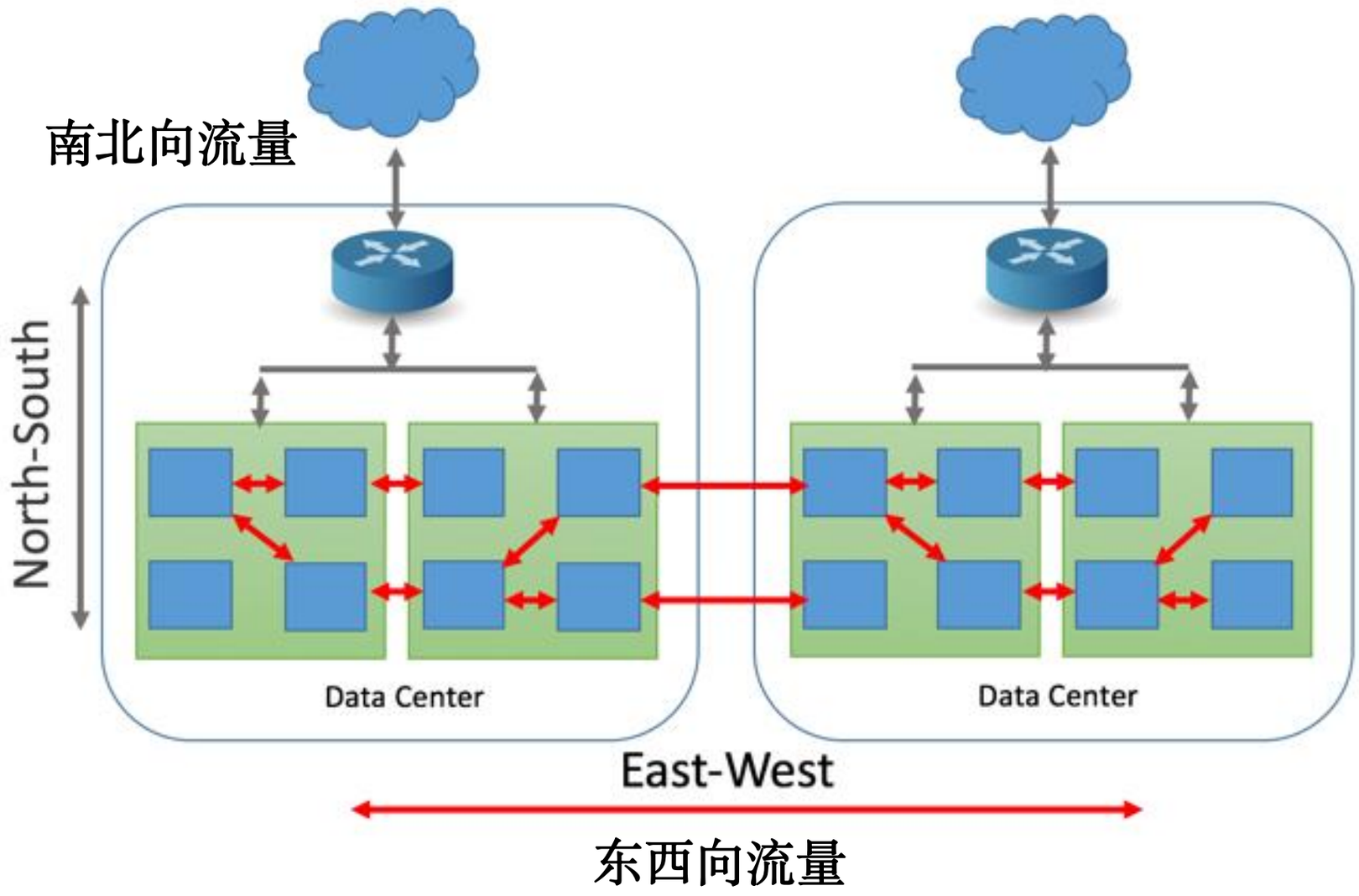
第一节 防火墙

本节内容与目标

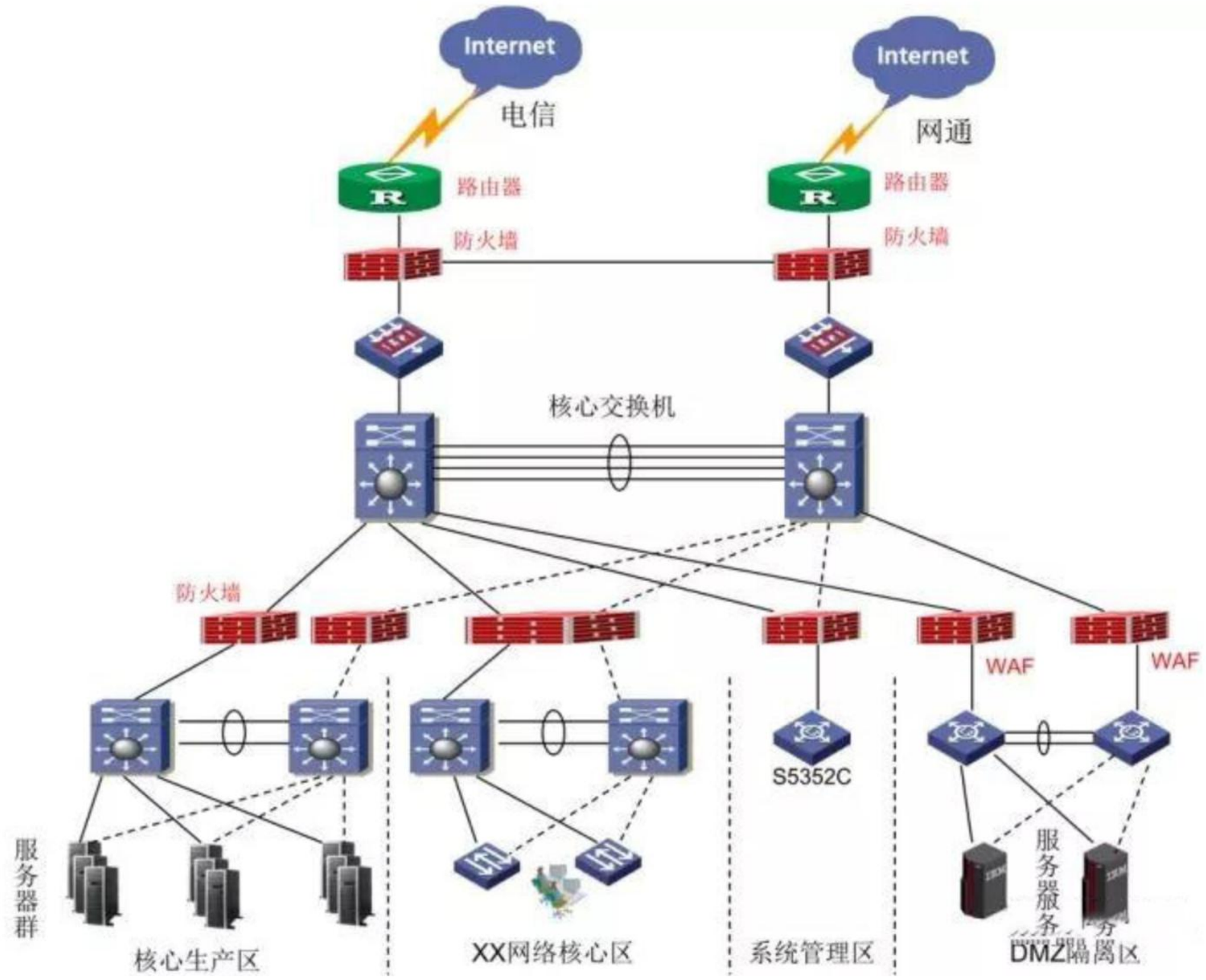
- 理解企业网络结构域划分
- 理解防火墙原理、部署防护、使用场景和优缺点

Zhi Liu, copy rights reserved

典型企业网络结构



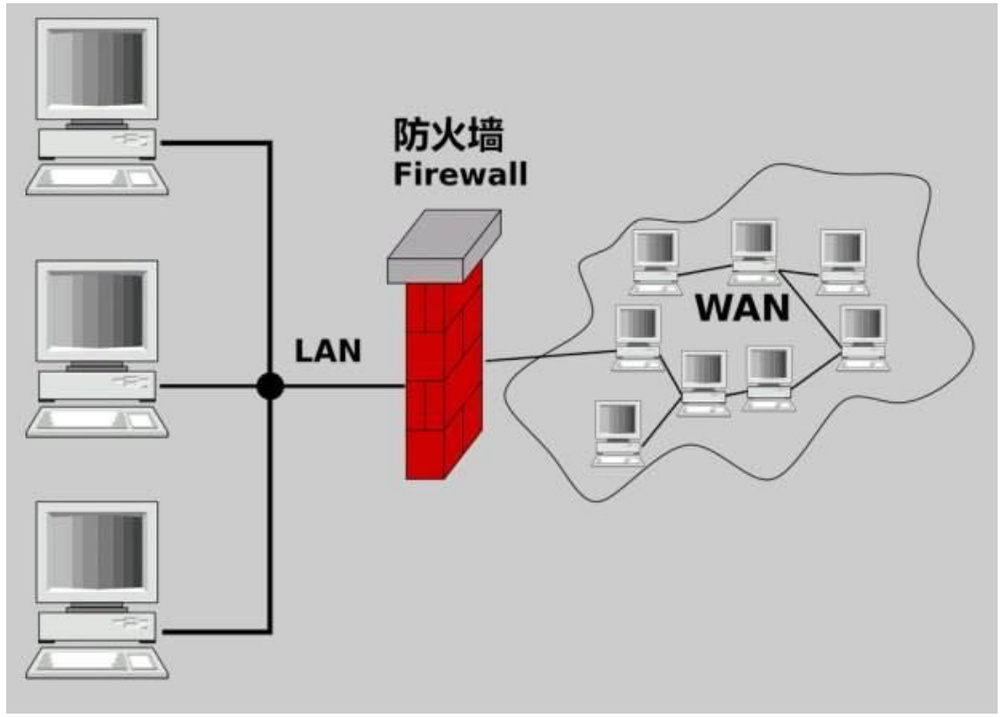
典型企业网络结构



http://www.bjruodianshigong.com/xinwendongtai/anfangzhishi/2019/1103/92.html

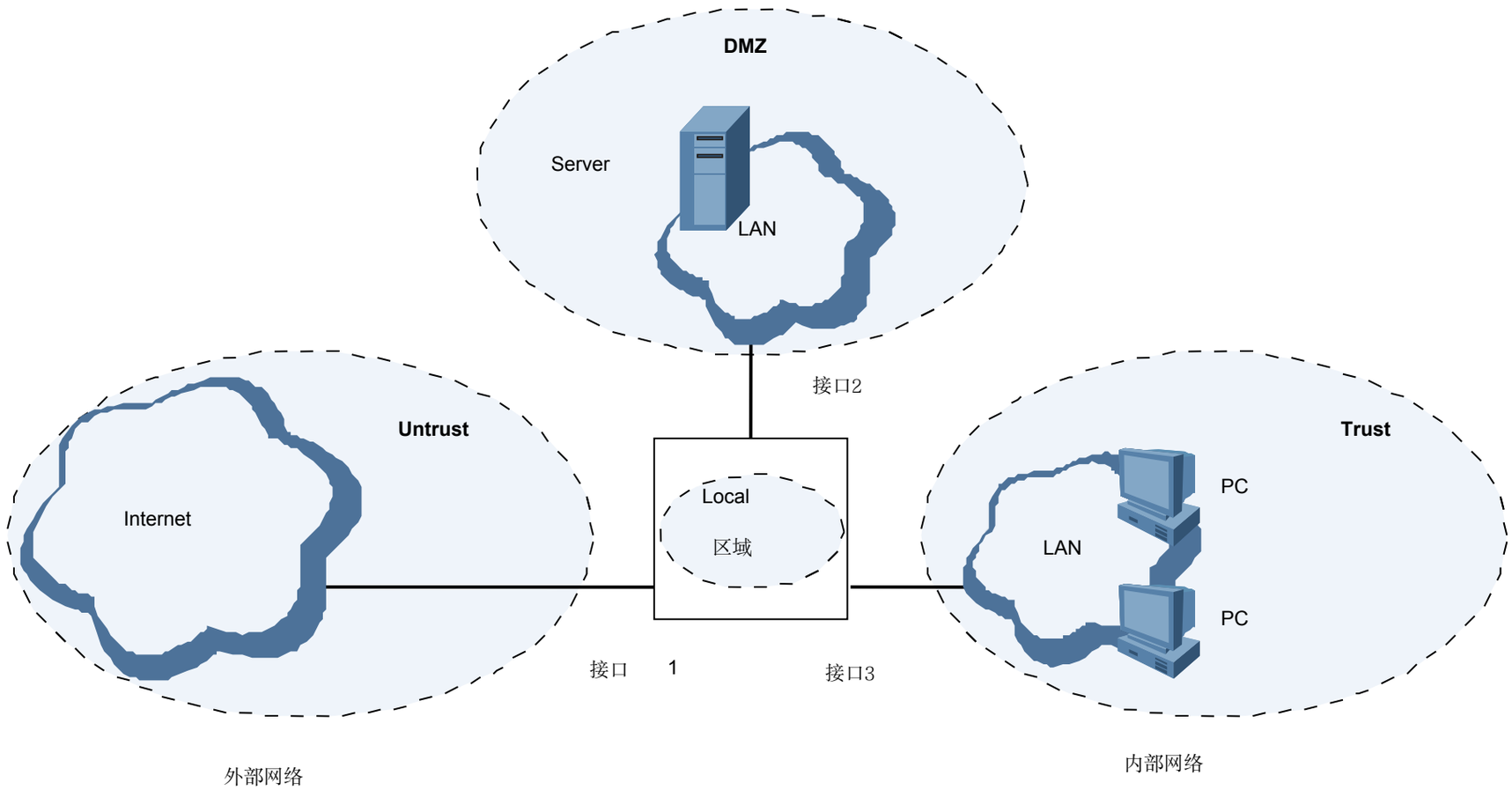
防火墙定义

- 防火墙(Firewall)是网络安全**第一道防线**，是位于**两个信任度不同的网络之间**（如企业内部网络和Internet之间）的安全设备，它对两个网络之间的通信进行控制，通过安全策略防止对重要信息资源的非法存取和访问以达到保护系统安全的目的。



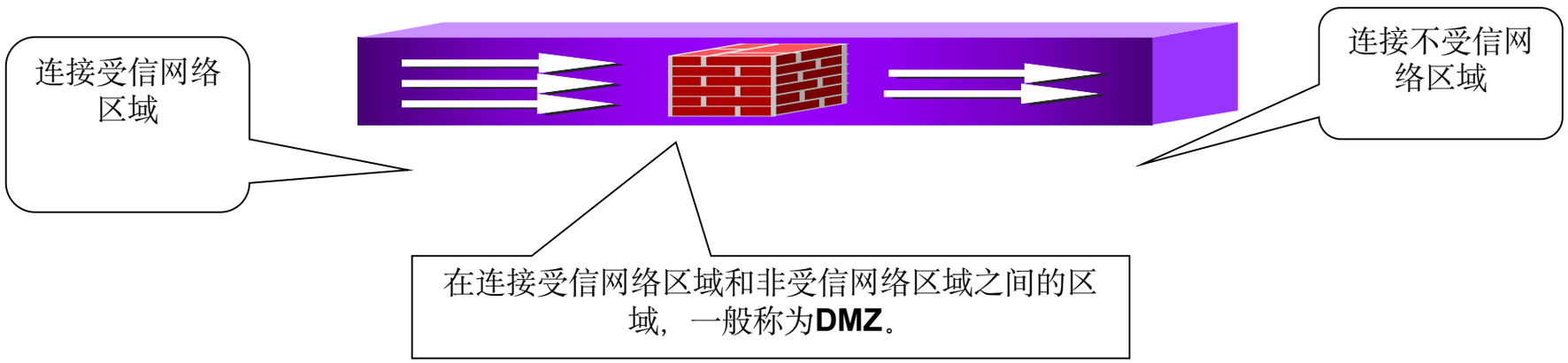
安全域划分

- Trust信任域
- Untrust非信任域
- **DMZ**

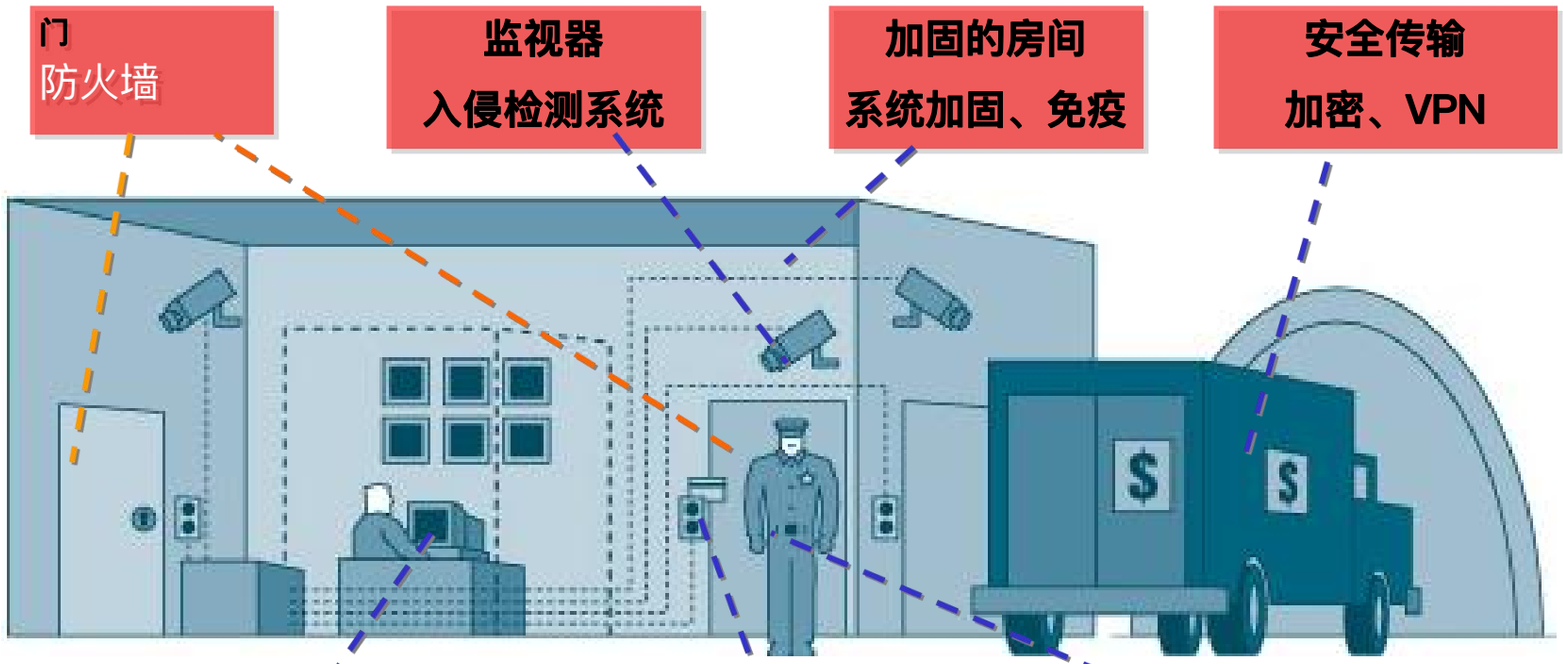


防火墙特点

- 内部和外部网络之间(南北向)所有网络数据都必须经过防火墙。
- 只有符合安全策略的数据流才可以通过防火墙。
- **防火墙是一种串联设备，具有阻断能力**
- **通常部署在南北向关键位置**



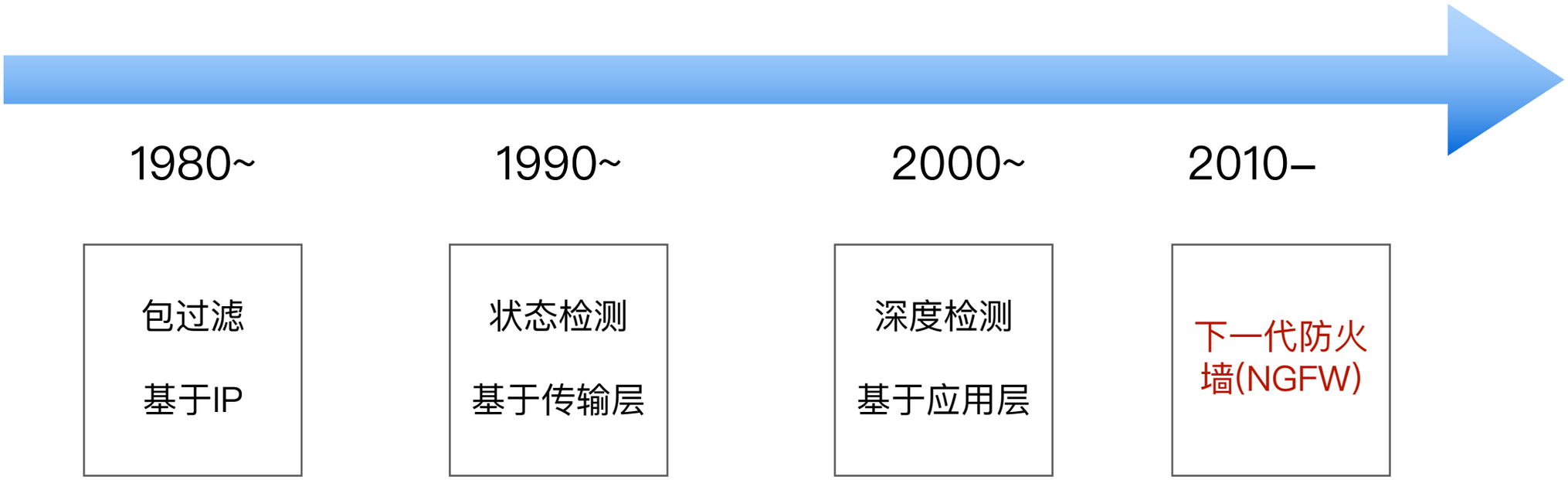
防火墙在安全体系位置



防火墙类型

- 个人防火墙
  - 通过软件实现的防火墙，如Windows自带防火墙、Linux的iptables
- 普通硬件防火墙
  - 传统x86和操作系统实现的防火墙
- 专属硬件防火墙
  - 专属硬件和操作系统实现的防火墙

防火墙技术演进

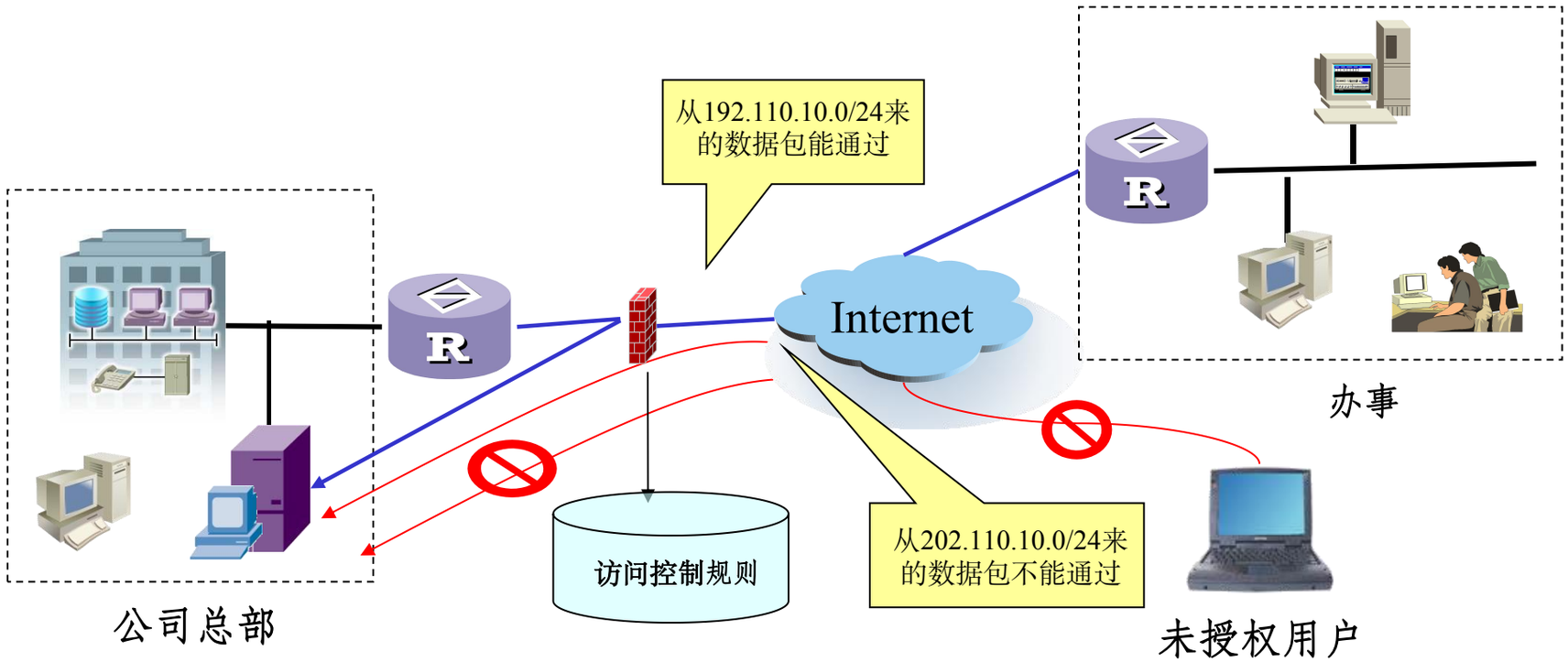


防火墙技术原理

- 包过滤防火墙(Packet Filtering)
  - 利用特定规则过滤数据包(packet)，通过IP源地址、目的地址、源端口和目的端口等信息过滤。
- 状态监测防火墙 (Stateful inspecting)
  - 动态记录和维护各个连接(session)的状态，对其进行网络访问控制和安全攻击检测。
- 下一代防火墙(NGFW)
  - 融合DPI技术，提供灵活网络访问控制和强大攻击检测的下一代防火墙，通常具备安全检测与阻断、NAT、VPN等多种功能。

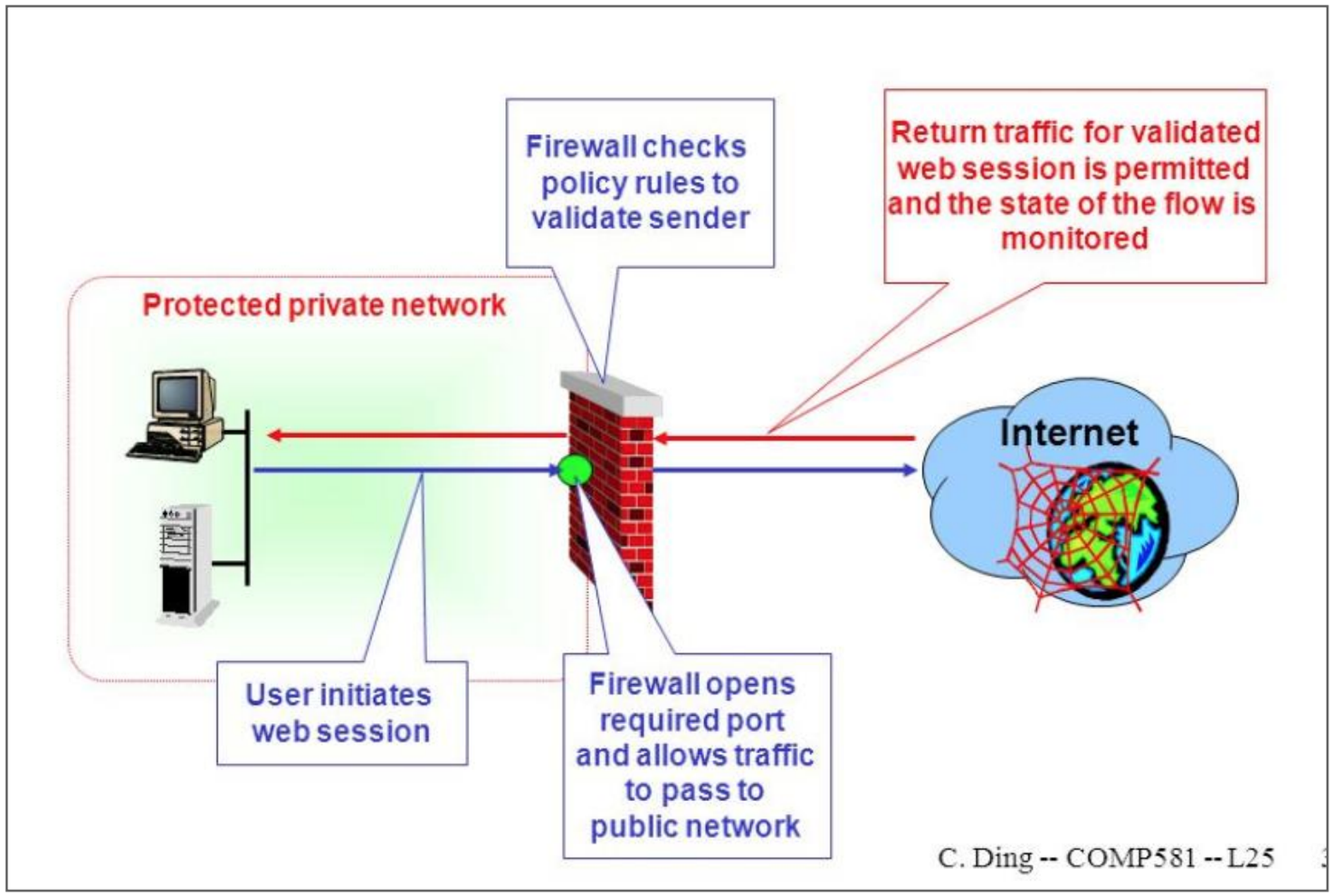
包过滤防火墙

- 对数据包(packet)进行检测



状态监测防火墙

- 对网络流(flow)进行分析和检测

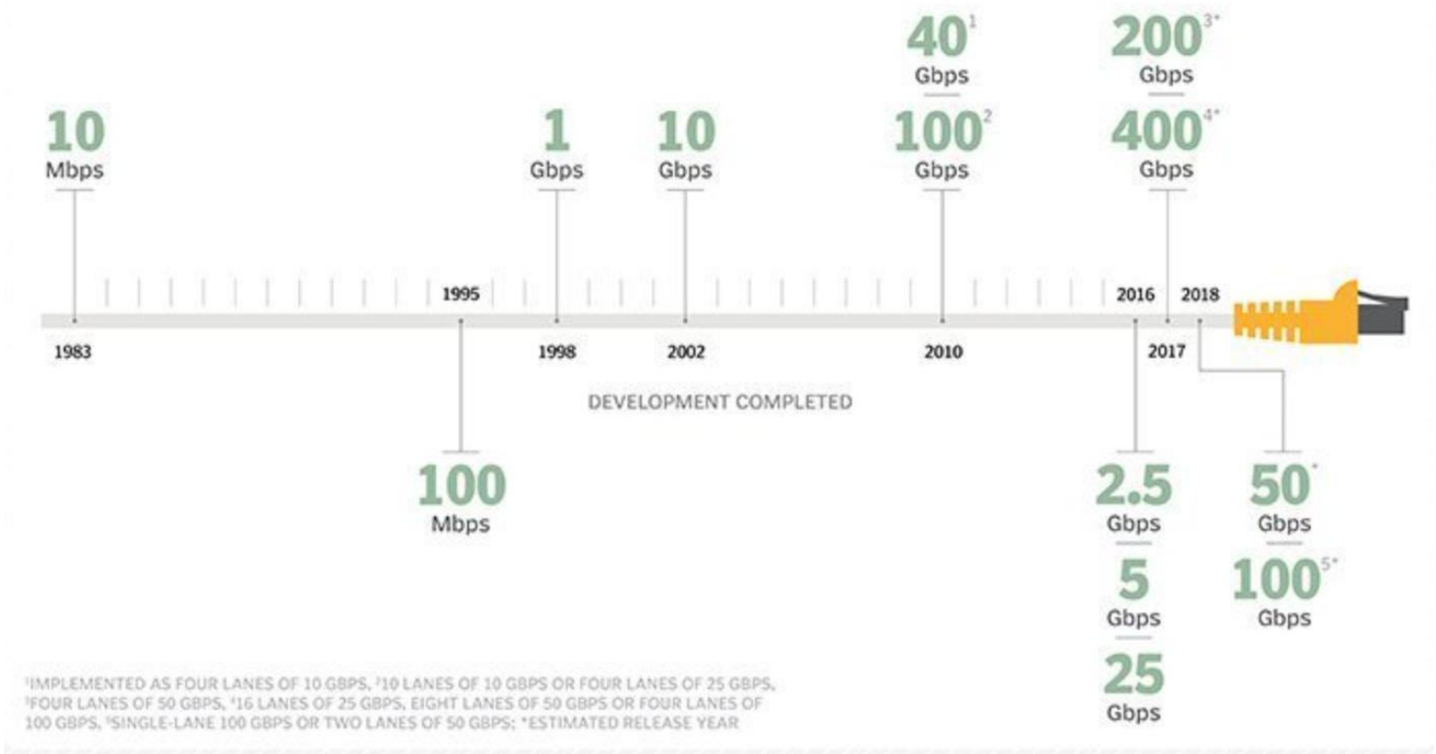


下一代防火墙

- 网络能力
  - 不依赖端口的协议识别
  - 深度流量分析
  - VPN能力
- 安全能力
  - 集成IDS/IPS功能
  - 与其它安全解决方案整合
  - **加密流量分析**

防火墙主要功能指标

- 吞吐量：以bps作为单位，如10Gbps
- 每秒钟处理的包数(PPS, Pakcet Per Second)
- 新建连接数、并发连接数



以太网速率

https://searchstorage.techtarget.com/photostory/450419695/Speeds-of-storage-networking-technologies-rise-as-flash-use-spikes/2/High-speed-Ethernet-standards-offer-implementation-choices

防火墙优缺点

- 优点
  - 具有较强阻断能力
  - 功能较为丰富
- 缺点
  - 难以防御内部威胁(东西向流量)
  - 难以检测新型攻击
  - 高速网络下的性能瓶颈

本节内容与目标

- 理解企业网络结构域划分
- 理解防火墙原理、部署防护、使用场景和优缺点

课后延伸与作业

- 使用Windows或Linux防火墙，对其进行测试
- 阅读防火墙产品白皮书，了解主要指标

第五章 网络安全防护系统

第二节 入侵检测系统

本节内容与目标

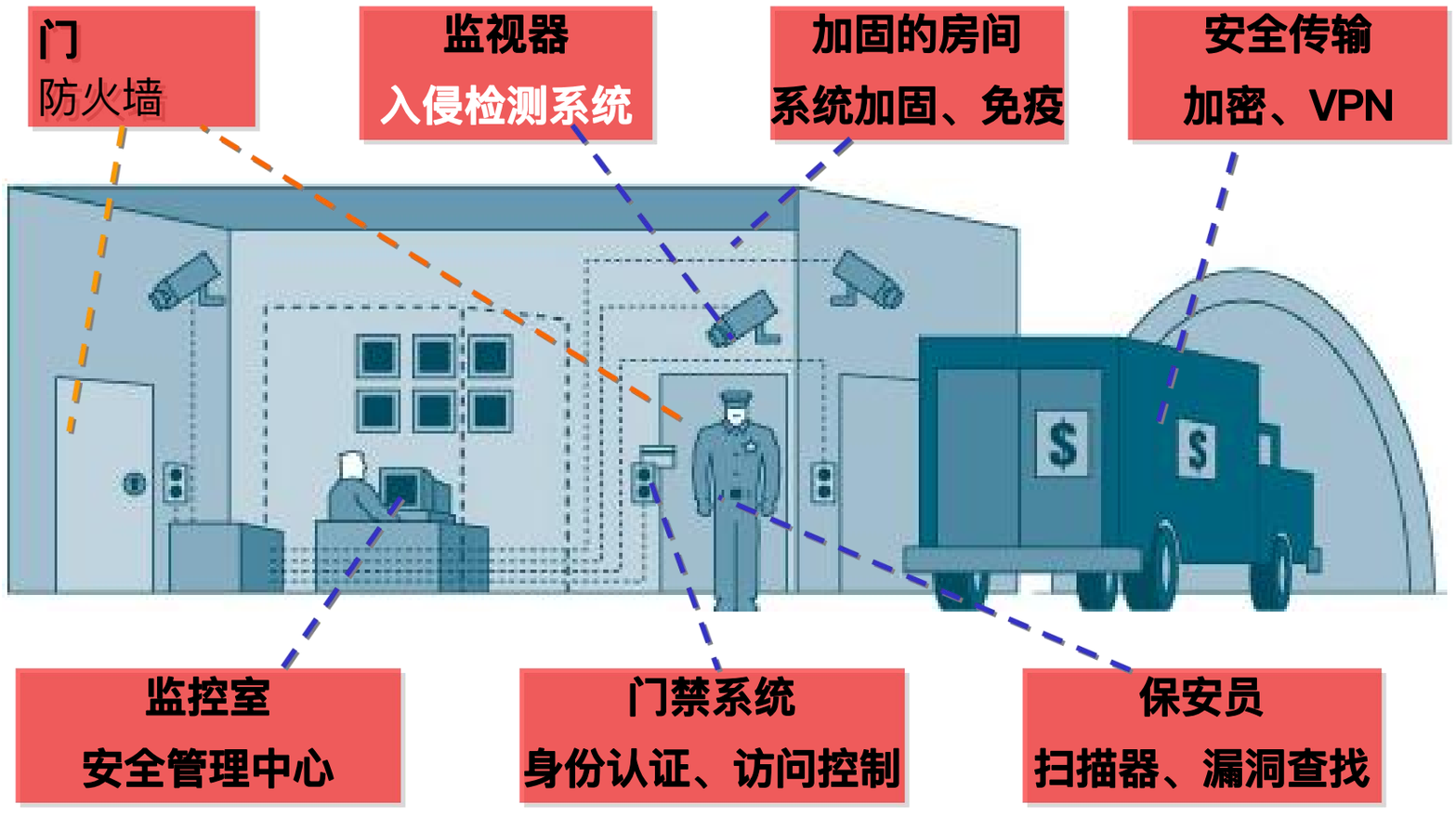
- 了解IDS工作原理，能分析IDS和防火墙区别
- 理解IDS规则匹配方法。

入侵检测系统概述

- “通过对网络或计算机系统中若干**关键点**信息收集并对其分析，发现网络或系统中**是否有违反安全策略的行为或遭到攻击的痕迹**。是一种动态网络检测技术，对攻击行为进行**分析**。”
- 使用场景
  - 内部威胁防护(东西向)
  - 增强南北向安全防护

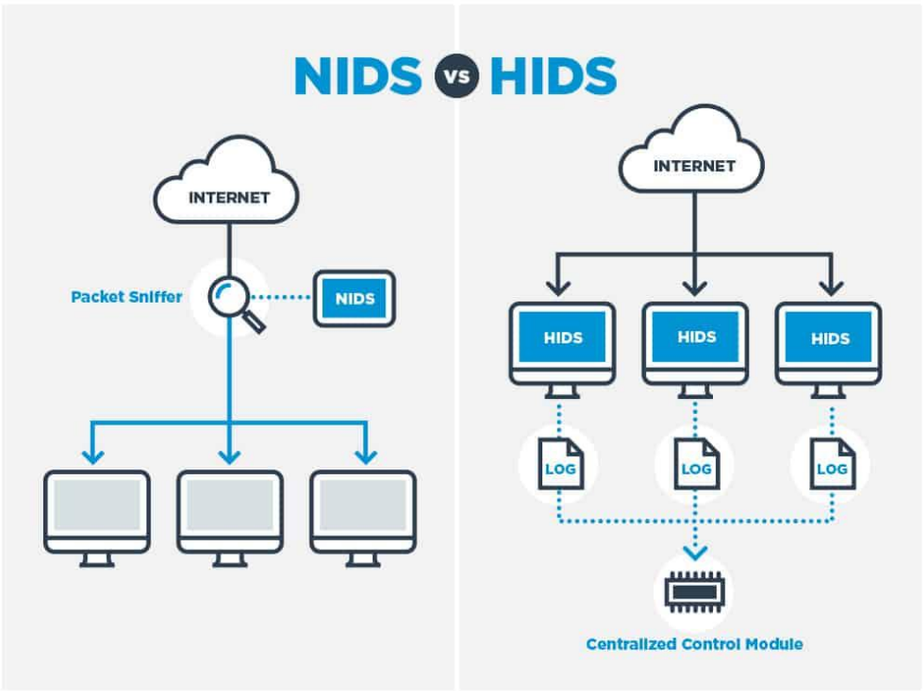
Zhi Liu, copy rights reserved

IDS在安全体系结构的位置



入侵检测系统分类

- **网络入侵检测(NIDS)**
  - **部署在网络中的入侵检测系统，以网络流量作为输入。**
- **主机入侵检测(HIDS)**
  - **部署在主机的入侵检测系统，以主机活动作为输入。**

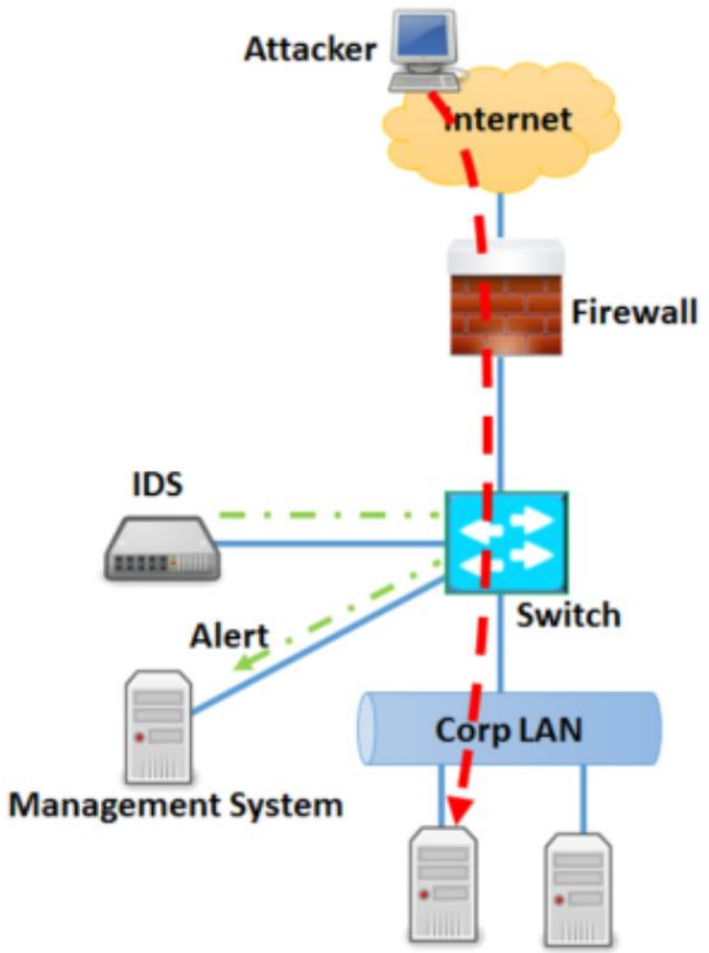


NIDS部署

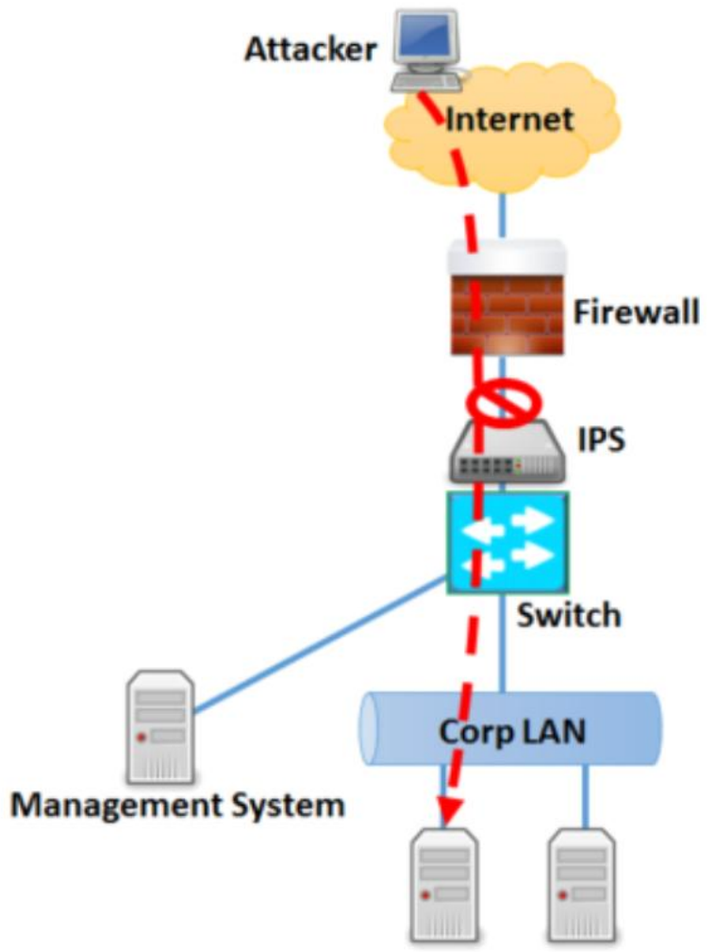
- 通常通过**端口镜像(mirror port)**从交换机引流
- IDS不具备阻断能力
- IPS为入侵防御系统，具备阻断能力

IDS和IPS部署

Intrusion Detection System

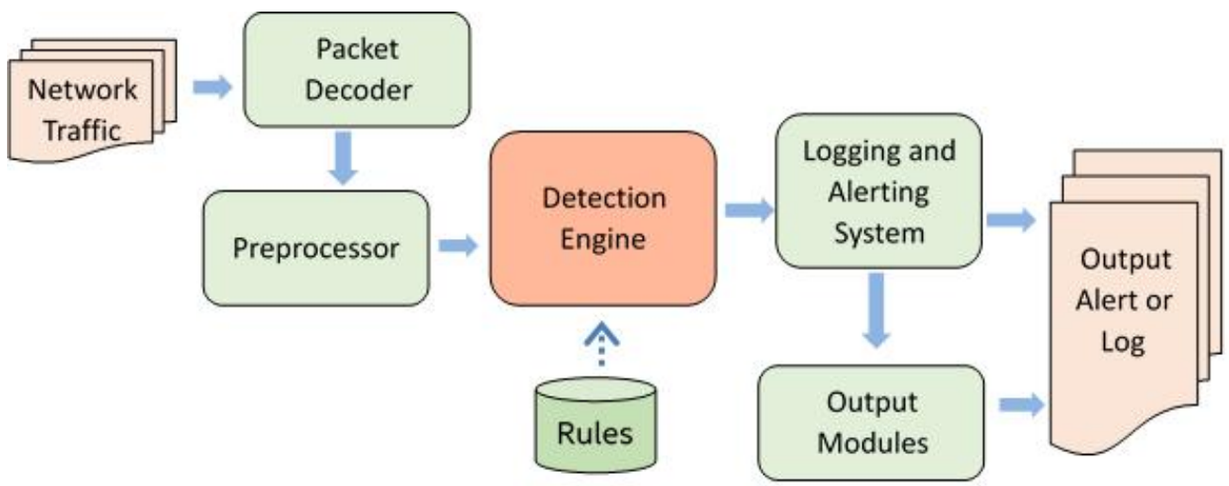


Intrusion Prevention System



IDS工作原理

- 主要组件
  - 数据包解码、协议解析
  - 攻击检测引擎、规则库
  - 输出



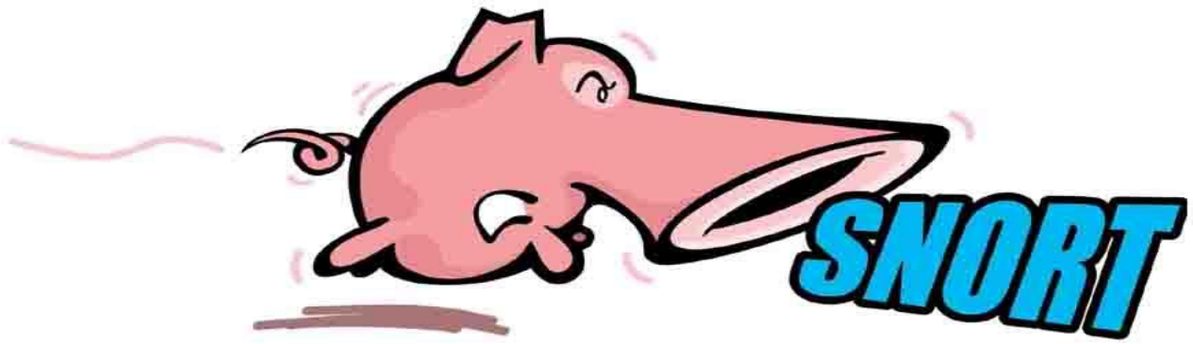
https://software.intel.com/en-us/articles/hyperscan-and-snort-integration

规则匹配

- 原理
  - 将**流量数据**与**已知规则**进行比较，发现违反安全策略的攻击行为。
- 优点
  - 技术成熟，但误报和漏洞率高。
- 缺点
  - 随着攻击库不断增大系统**性能下降**
  - 需要不断进行**升级规则库**实现对新攻击检测。

Snort介绍

- 业界知名开源IDS系统
- 使用场景
  - 轻量级
  - 跨平台，移植性强
  - 开源(GPL协议)



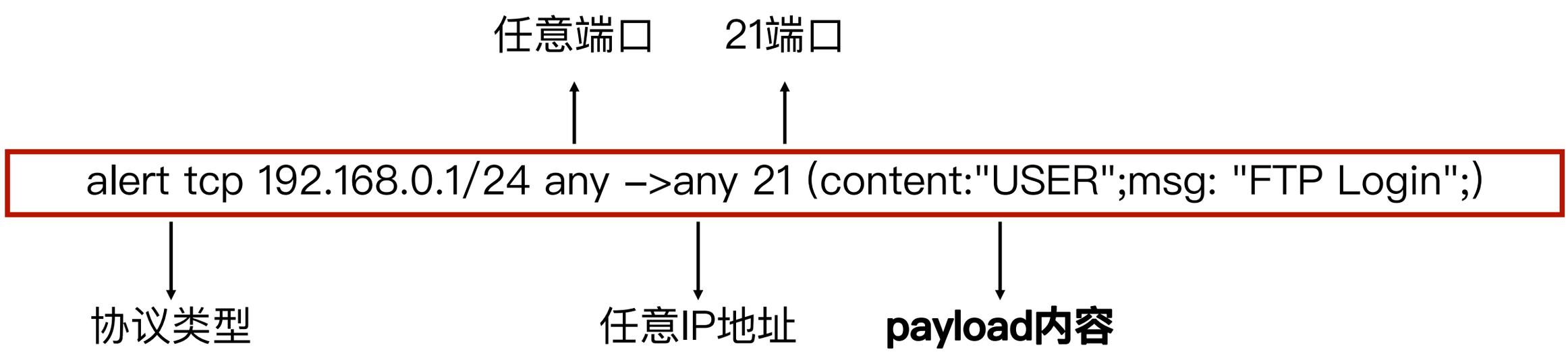
Snort设计

- 性能
  - 使用**Libpcap**采集网络流量(~100Mbps)
- 规则
  - 基于**规则**的检测引擎
- 灵活性
  - 灵活的插件编写

规则(rules)

- 实时检测引擎将规则与流量数据实时匹配
- 可检测多种攻击
  - 扫描，缓冲区溢出, exploit, shell code, 木马等
- 规则具有良好描述性和可读性

Snort规则例1



在192.168.0.1/24网段主机发起的TCP网络连接中，如果目标端口为21，并且payload包含“user”，则发出警报“ FTP登陆”

Snort规则例2

规则头部	规则选项
Alert tcp 1.1.1.1 any -> 2.2.2.2 any	(flags: SF; msg: “SYN-FIN Scan”;)
Alert tcp 1.1.1.1 any -> 2.2.2.2 any	(flags: S12; msg: “Queso Scan”;)
Alert tcp 1.1.1.1 any -> 2.2.2.2 any	(flags: F; msg: “FIN Scan”;)

常见匹配算法

- 模式匹配引擎是IDS核心
- 常见匹配算法
  - 单模匹配：KMP、AC
  - 多模匹配：AC_BM
  - 硬件级模式匹配：HyperScan(Intel)

“Hyperscan是一款来自于Intel的**高性能的正则表达式匹配库**。它是基于x86平台以PCRE为原型而开发的。大量高效算法及IntelSIMD*指令的使用实现了Hyperscan的高性能匹配。Hyperscan适用于部署在诸如DPI/IPS/IDS/FW等场景中，还支持和开源IDS/IPS产品Snort和Suricata 集成，使其应用更加广泛。”

规则维护与升级

- Snort自带部分规则，但较为陈旧
- 规则主要由安全研究人员维护

IDS优缺点

- 优点
  - 旁路接入、部署简单，不影响业务
  - 产品较为成熟
- 缺点
  - 难以检测新型攻击
  - 误报和漏报较高
  - 无法阻断攻击

IDS发展趋势

- 高速网络流量分析
- 结合DPI技术实现更细粒度的检测
- 提升安全规则准确性
- 基于ML/AI的异常检测

防火墙与IDS比较

- 技术原理
  - 都使用了协议识别和解析技术
  - 都利用规则匹配检测攻击
- 使用场景
  - 防火墙提供网络和安全两部分能力，通常部署在南北向流量关键位置
  - IDS仅有安全检测能力，为旁路设备(不具备阻断能力)

本节小结

- IDS
  - 掌握技术原理、使用场景和部署模式
  - 了解规则匹配主要技术使用
  - 理解防火墙与入侵检测区别

课后延伸与作业

- 安装Zeek，分析其产生的日志(conn.log, ssl.log)