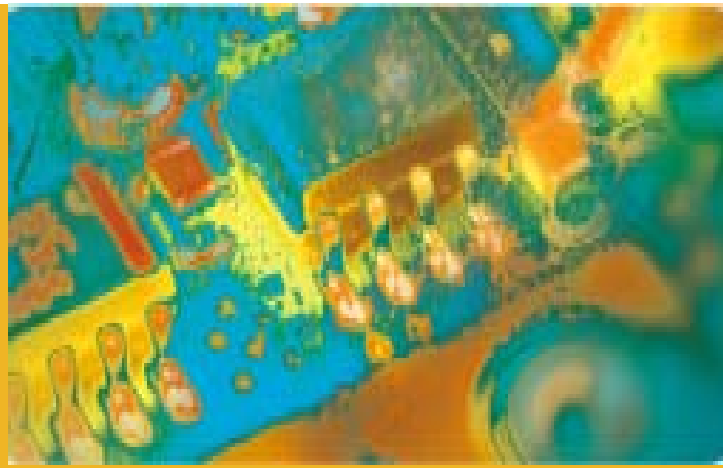
温州大學
WENZHOU UNIVERSITY

网络性能测试与分析



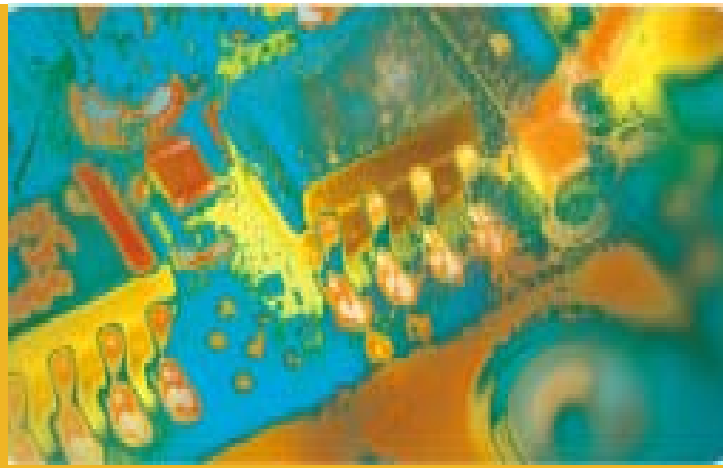
http://network.wzu.edu.cn

http://www.spirent.com

beetleking@163.com

温州大學
WENZHOU UNIVERSITY

第六章 网络安全性能测试



http://network.wzu.edu.cn

http://www.spirent.com

beetleking@163.com

本章教学提要

■教学目标：

✓了解网络安全的概念

✓了解网络安全的常用技术

✓了解拒绝服务攻击的常用方法

✓掌握网络安全性能的技术指标

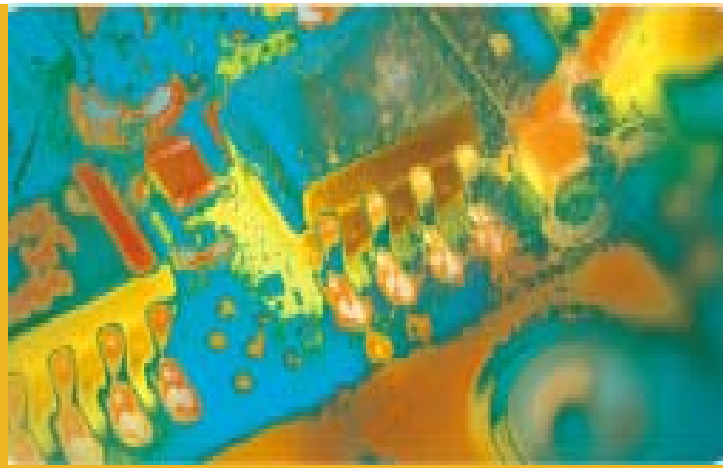
✓掌握网络安全性能测试的基本方法

●教学难点/重点：网络安全的性能技术指标、网络安全的测试方法

●教学时数：理论4学时

温州大學
WENZHOU UNIVERSITY

第一节　网络安全测试的必要性



本节关注问题

1、网络安全的重要性

- 网络安全威胁的不断增加
- 威胁网络安全的技术手段日趋复杂，并且表现出高度的多样性

2、对企业而言：

- 网络安全是风险与收益平衡的结果
- 网络安全是网络的功能和脆弱性折衷的结果

- 在开放的互联网环境中，绝对安全的网络是不存在的

3、网络安全是4~7层测试的关注点

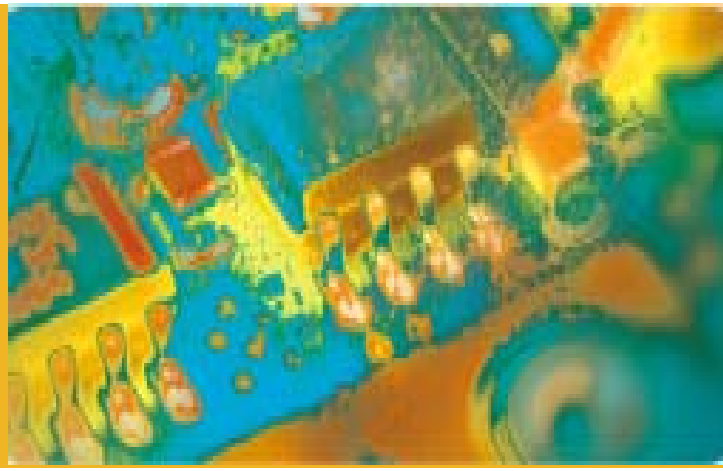
1、了解具有安全部署的网络在面对不安全因素时的性能表现，以及网络是否具备一定的响应机制和恢复机能，以确保业务的正常开展

2、提供网络安全防护产品的测试评估，

通过网络安全测试，能够准确地衡量防火墙、IDS和IPS系统的真实性能，从而帮助生产厂商改进产品、提供可信度高的宣传数据，帮助用户更深入真实地了解产品性能，为网络安全系统的设计和部署提供更有价值的参考。

温州大學
WENZHOU UNIVERSITY

第二节　网络安全概述



- 网络的物理安全
- 网络拓扑结构安全
- 网络系统安全
- 应用系统安全
- 网络管理的安全
- 本章关注：网络入侵(Network Intrusion)

网络入侵(Network Intrusion)

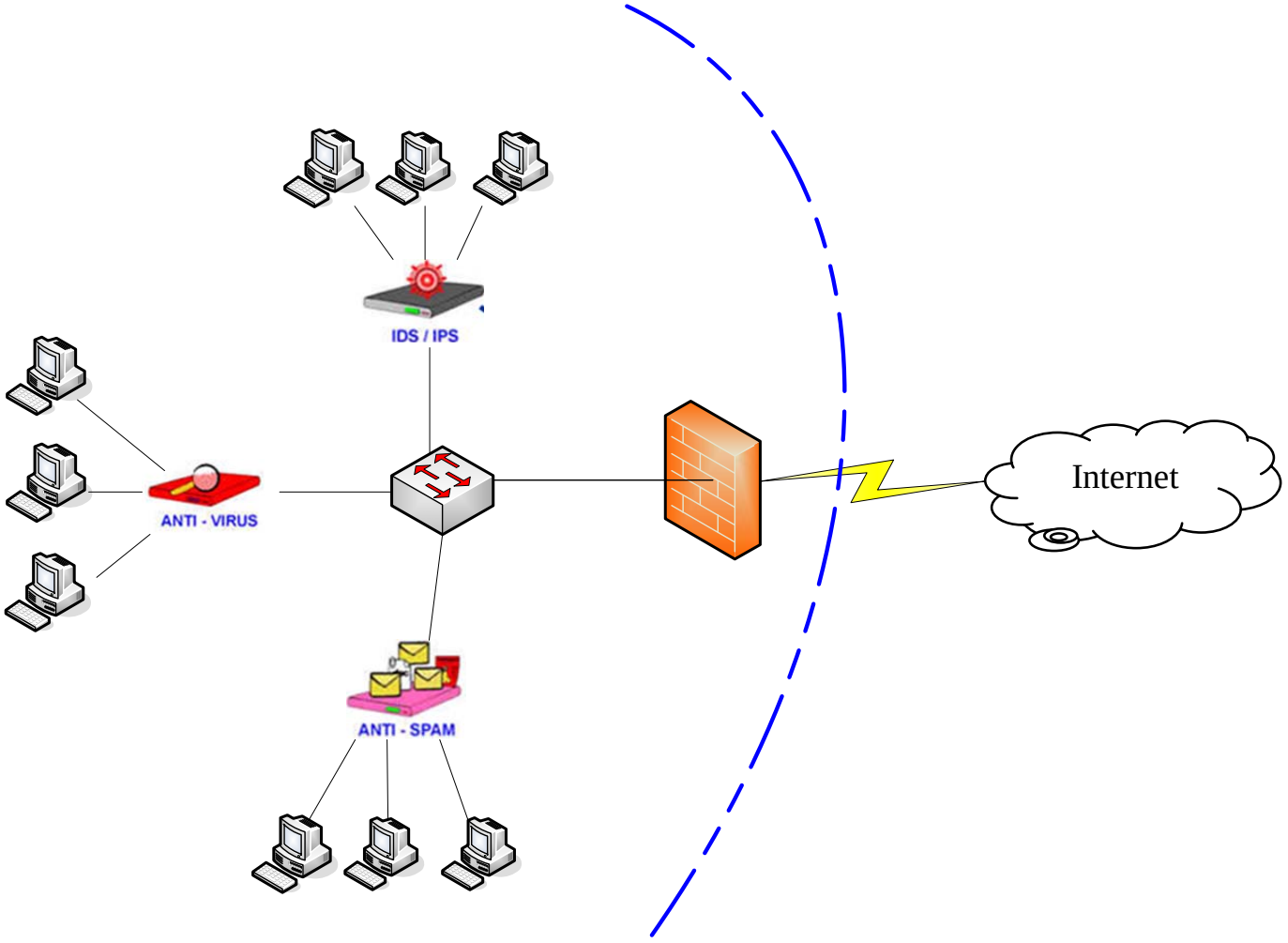
- 网络存取攻击
  - ✓通过非法途径获得网络中的资源使用权限或者利用网络从事非法攻击活动，如非法侵入企业内部网络获取商业机密信息等
- 资源消耗攻击
  - ✓攻击者通过某种手段扰乱或者阻止网络系统为用户提供正常服务，如通过DoS攻击方式致使Web服务器瘫痪等
- 根据现实网络应用中经常遇到的网络安全问题，又将其细分为以下几类：

1、常见的网络安全问题

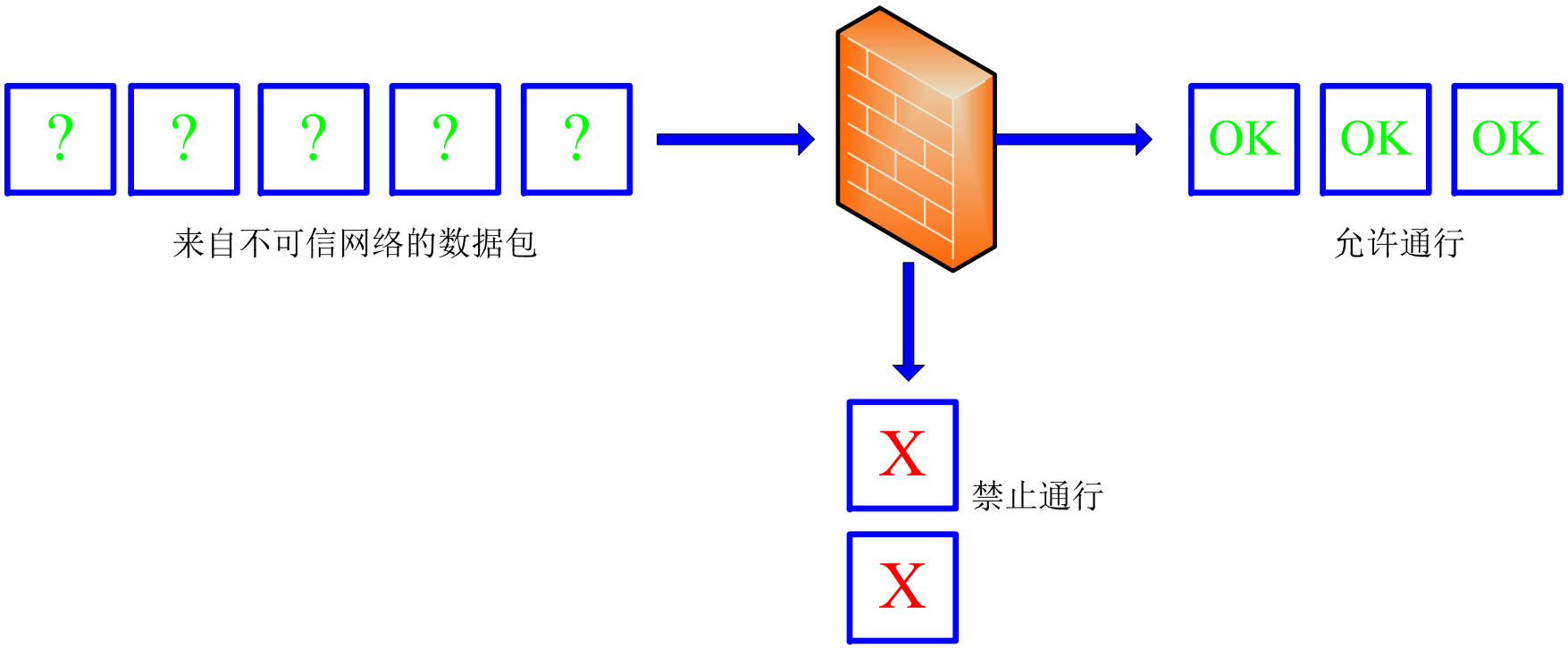
- 非法入侵
- 计算机病毒
- 分布式拒绝服务攻击
- 信息截获

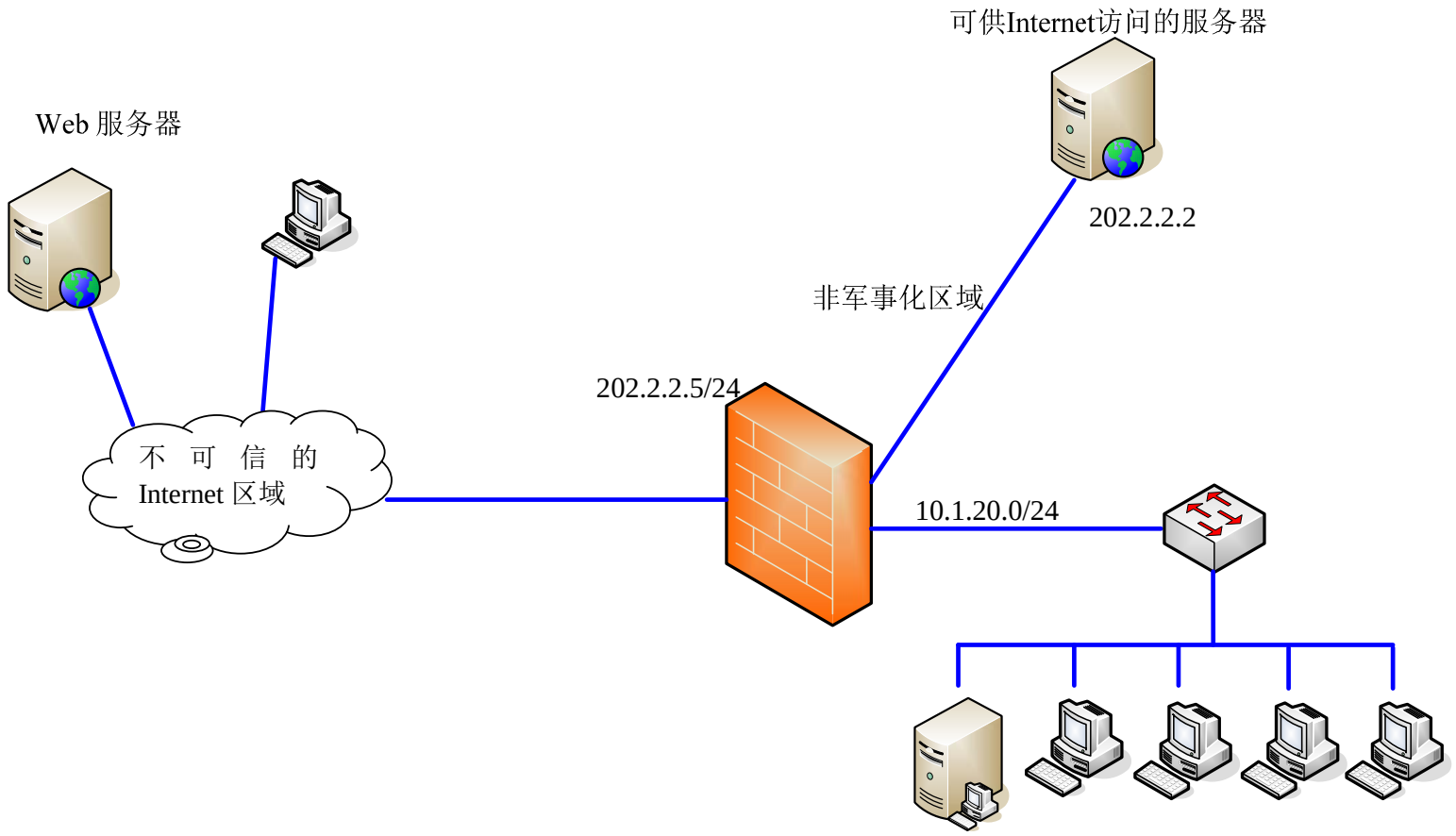
2、常见的网络安全技术

网络安全防护拓扑图

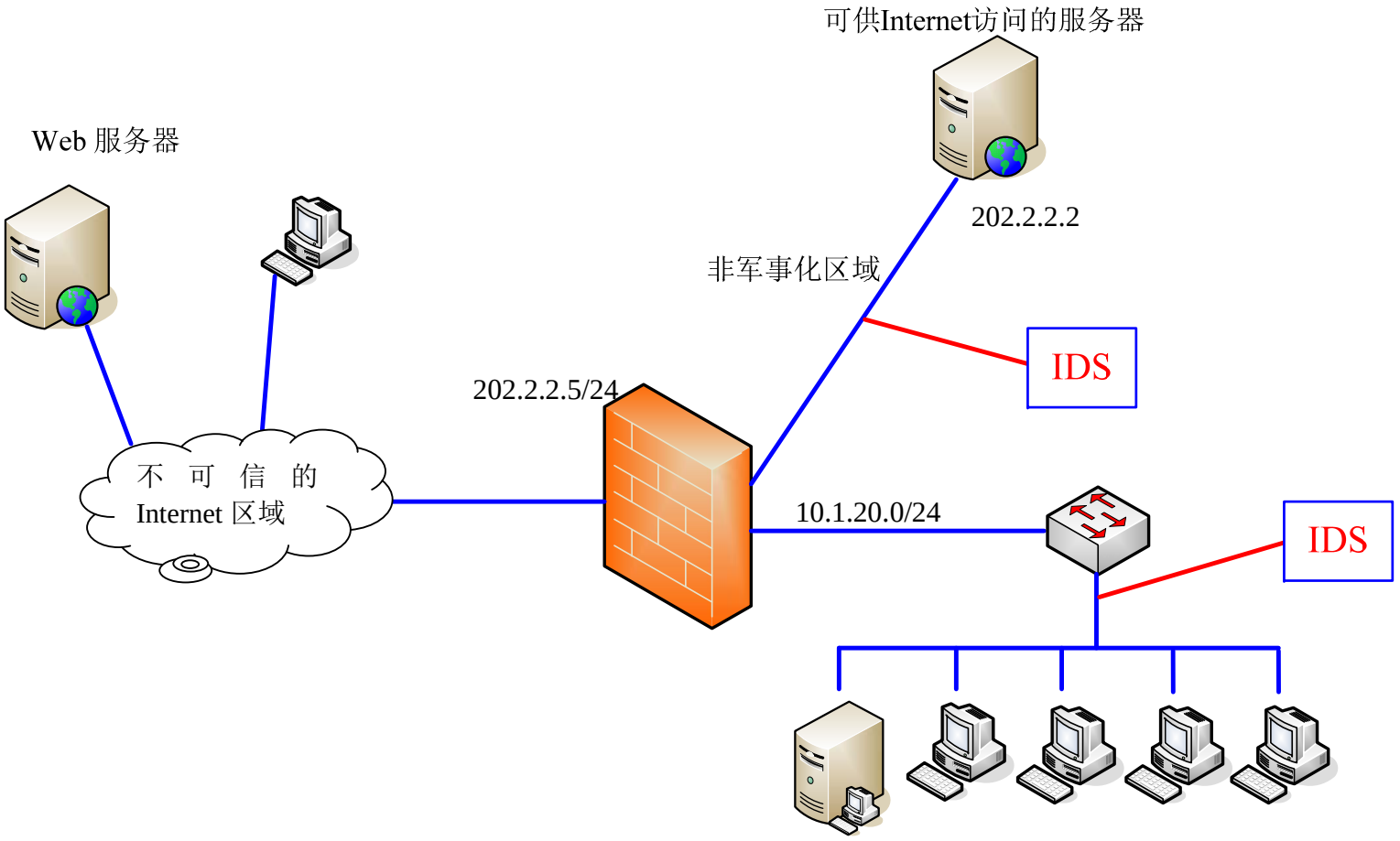


1防火墙

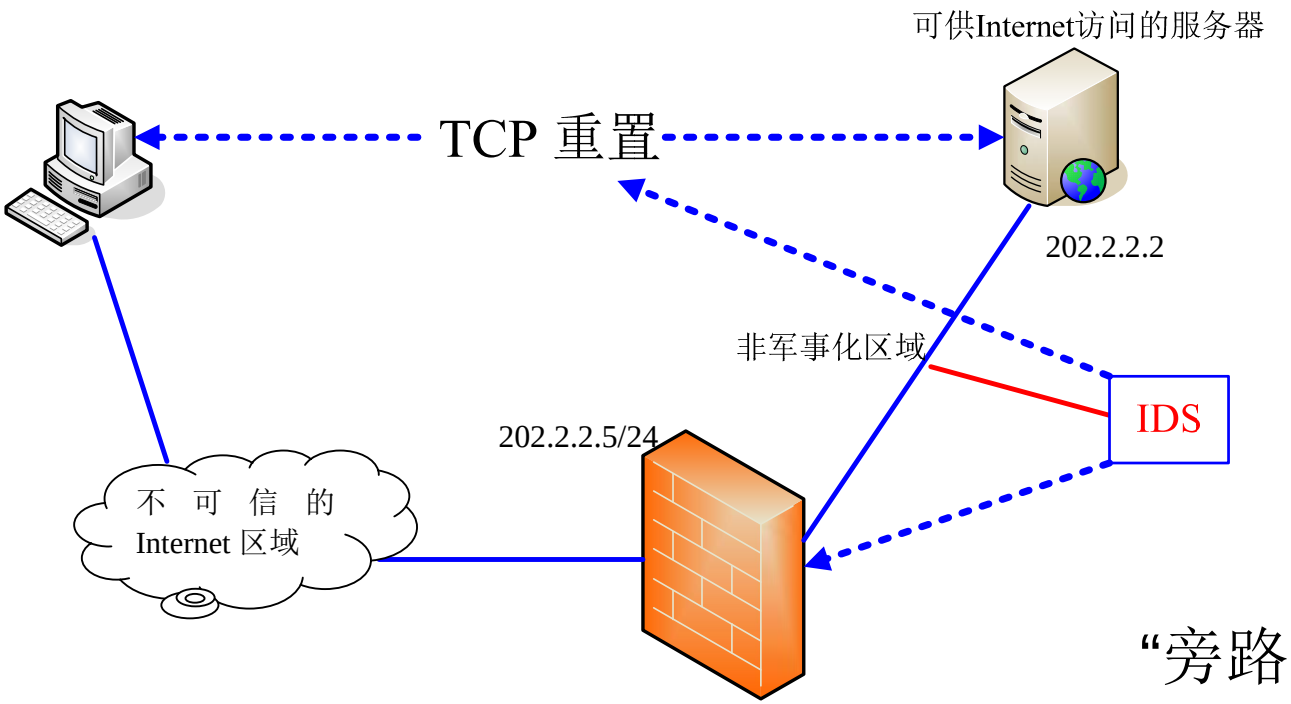




2入侵检测系统



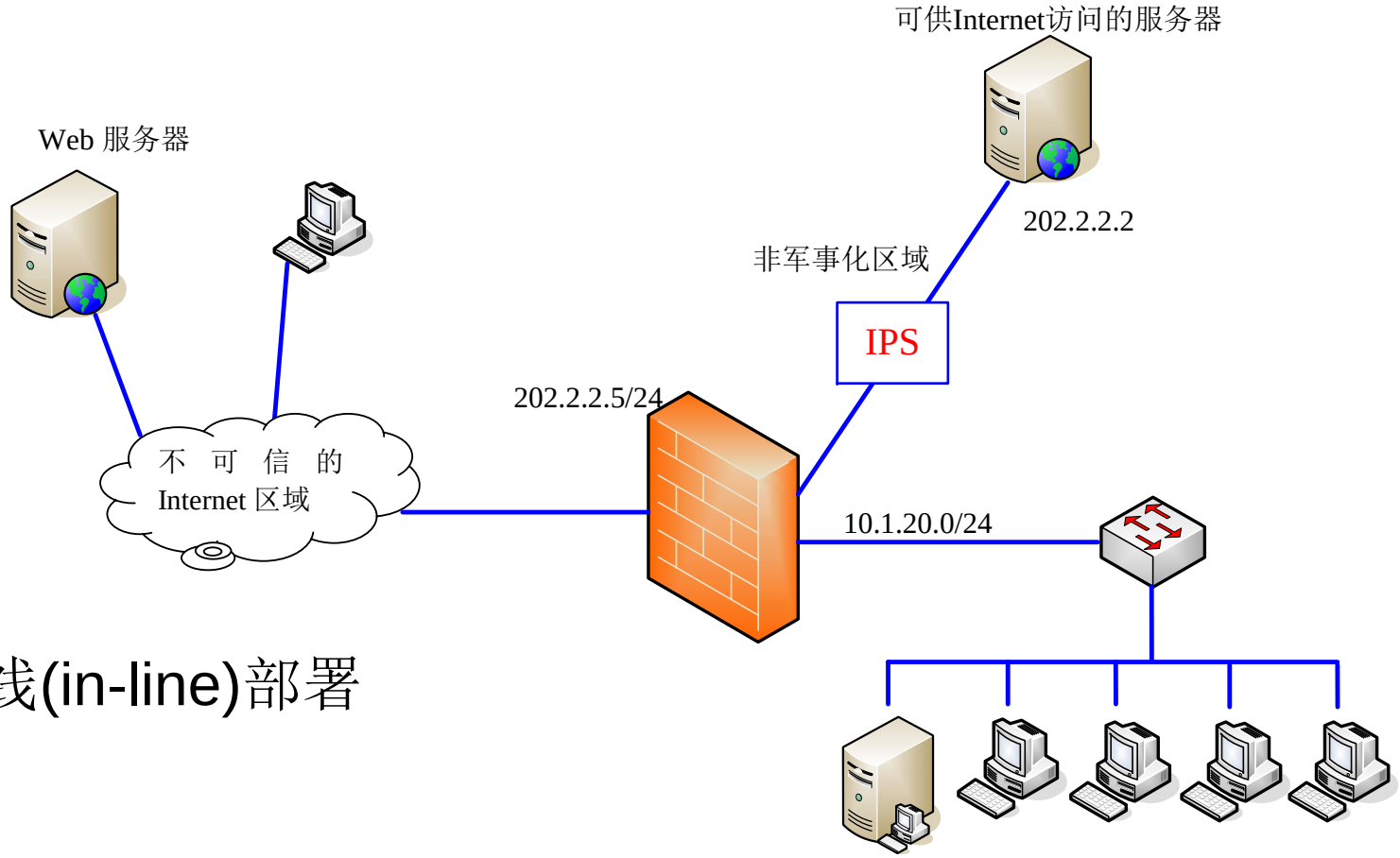
反应式入侵检测系统(IDS)部署



“旁路式”部署

3入侵防卫系统(IPS)

IPS可视为增加了阻截功能的IDS



在线(in-line)部署

4 防病毒网关

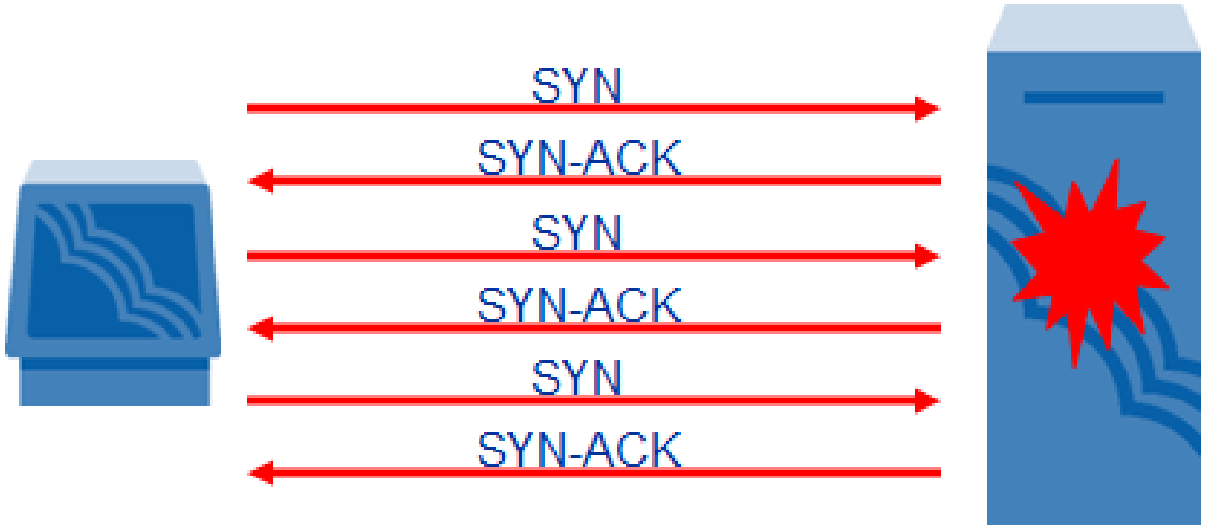
- 防病毒网关又称防毒墙。防毒墙是指位于网络入口处（网关），用于对网络传输中的病毒进行过滤的网络安全设备。
- 防毒墙与防火墙的最大区别在于，防毒墙主要工作在应用层，防毒墙扫描通过网关的数据包，然后对这些数据进行病毒扫描，如果是病毒，则将其清除。

5加密技术

- 加密，是指利用技术手段把重要的数据信息变为乱码（加密过程）后传送，到达目的地后再用相同或不同的手段还原成原来的信息（解密过程）。
- 加密技术包括两个元素：算法和密钥。

3、常见的分布式拒绝服务攻击

- 1 SYN Flood攻击

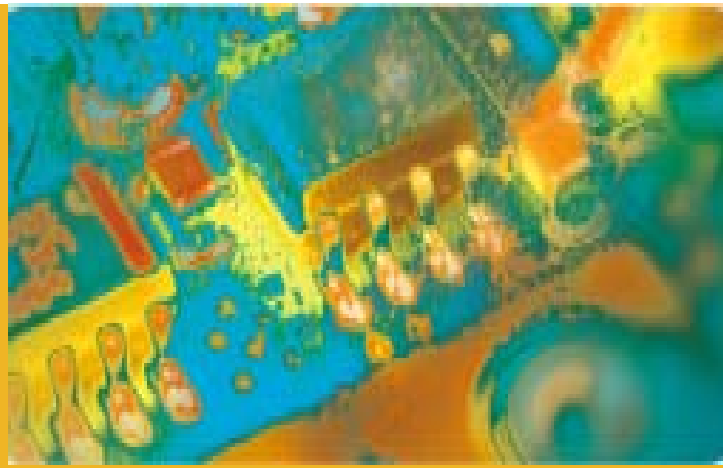


- 2 Land-based Attack
- 伪造一个源地址等于目的地址的IP数据包。当存在相应漏洞的被攻击主机收到这样的攻击包时，会向它自己的地址发送SYN-ACK消息，结果这个地址又发回ACK消息并创建一个空连接，被攻击的服务器每接收一个这样的连接都将保留，直到超时，如此不断地自我响应直到造成系统资源的过渡消耗而产生问题

- 3 Reset Flood攻击
- 利用TCP数据段中的RST位来实现。伪造合法用户的TCP RST包
- 4 ARP Flood攻击
- ARP攻击者利用伪造的IP地址，不断地向被攻击目标发出ARP请求，而被攻击者由于忙于响应这些假的ARP请求，无暇顾及其它正常的请求，因此造成“拒绝服务”。

温州大學
WENZHOU UNIVERSITY

第三节　网络安全性能的主要技术指标



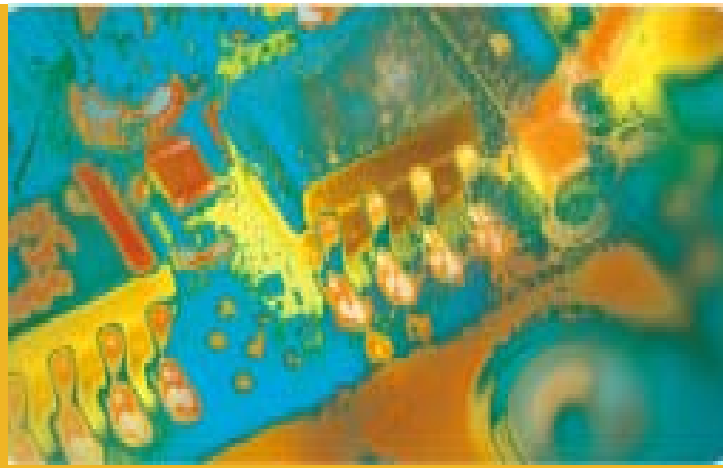
- 1. 防火墙

  防火墙的性能指标体现了防火墙能否满足特定环境的安全防范和处理能力需求，是否具备较好的可用性。通常遵从RFC2544、RFC2647和RFC3511标准，主要性能指标包括：吞吐量、丢包率、时延、背靠背、最大并发连接数、最大TCP连接建立速率等。

- 2. 入侵检测系统IDS
  - 1每秒数据流量（Mbps或Gbps）
  - 2每秒抓包数（pps）
  - 3每秒处理的事件数
  - 4每秒监控的网络连接数

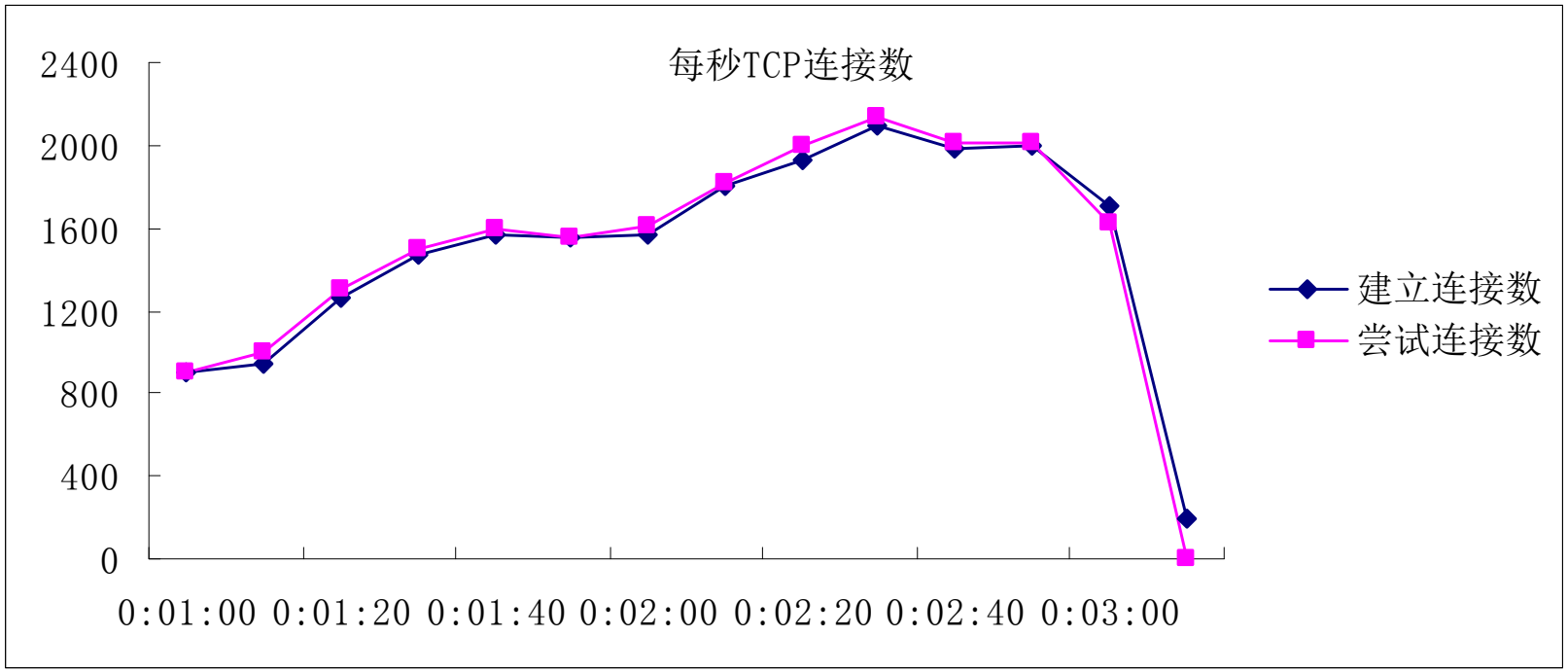
温州大學
WENZHOU UNIVERSITY

第四节 网络安全性能测试的基本方法



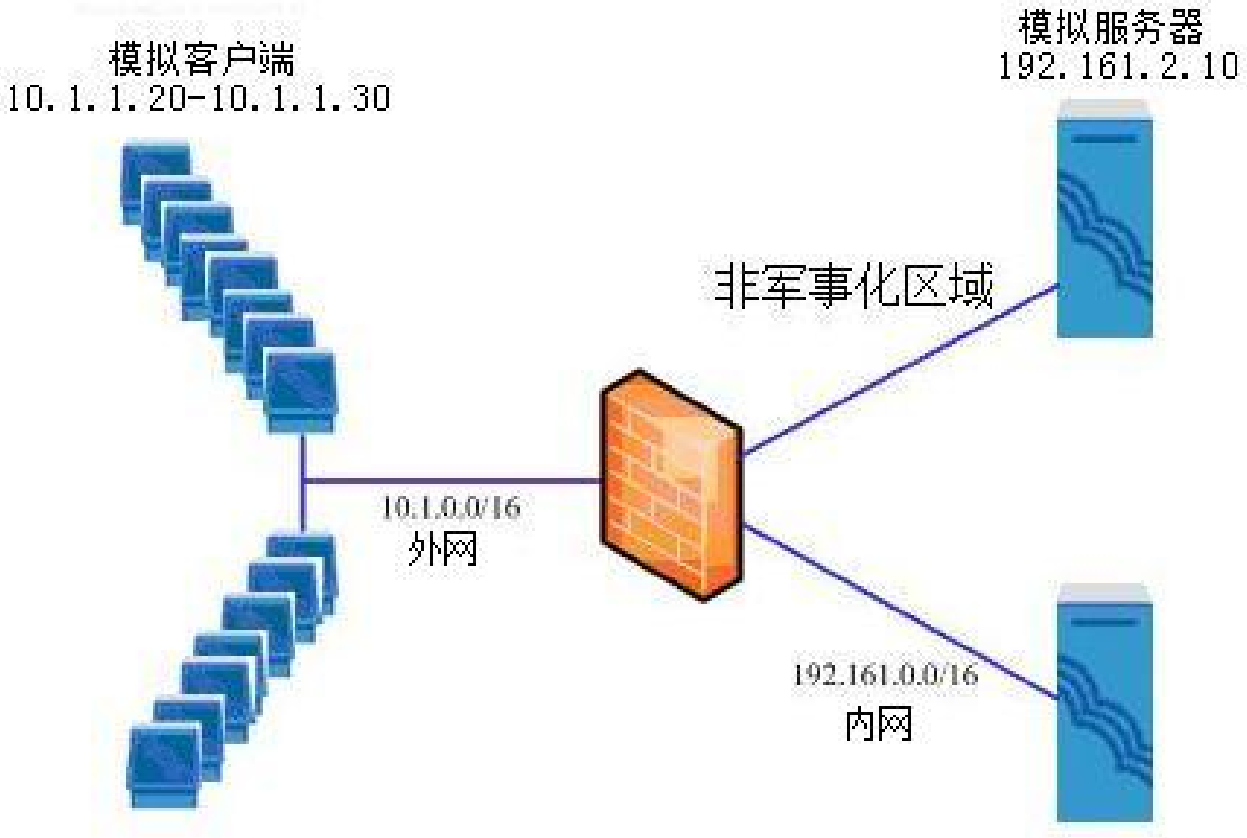
1、基础环境测试

基础环境测试拓扑图



测试环境新建TCP连接性能测试结果

2、防火墙压力测试



防火墙压力测试拓扑结构图