X'CON 2003

企业级安全隔离技术

作者： 孤独剑客

日期： 2003.12.22

- 隔离技术概述
- 隔离产品分类
- 桌面级隔离技术
- 企业级隔离技术
- 网闸与防火墙

X'CON 2003

隔离技术概述

- 为什么隔离？
  - 历史原因：受技术和成本制约而被动隔离
  - 现实原因：互联后无法忍受侵害而主动隔离

隔离技术概述

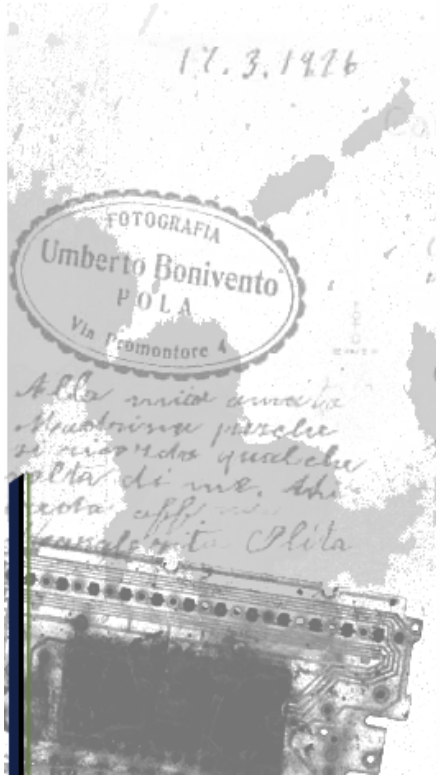
- 怎么算隔离？
  - 实体角度理解：在设备、线路、存储上是完全分离的
  - 过程角度理解：网络间不存在任何形式的自动信息交换

隔离技术概述

- 有哪些隔离方法？
  - 物理隔离：设备、线路、存储均独立
  - 网络隔离（协议隔离）：协议转换
  - 安全隔离：仅交换应用数据

隔离技术概述

- 国外认识之一
  - 1997年，安全专家Mark Joseph Edwards



Chapter Contents

- THE COST OF POOR SECURITY
- THE HISTORY OF TCP/IP SECURITY
  - Yesterday
  - Today' s Network Security
    - The Orange Book
  - The Security of Tomorrow
- SECURITY METHODS
  - Firewalls
  - Packet Filters
  - Proxy Servers and Application Gateways
  - Circuit-Level Gateways
  - Physical Isolation
  - Protocol Isolation
  - Monitoring and Auditing

隔离技术概述

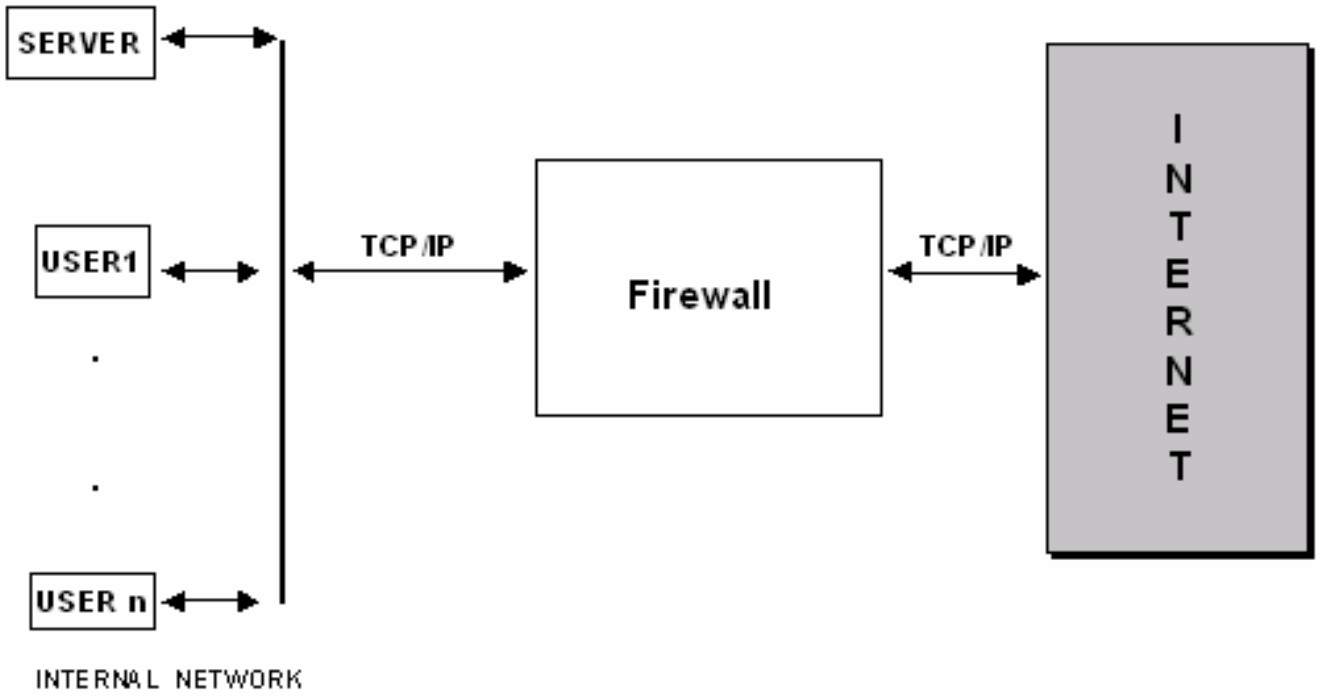
- 国外认识之二
  - 2000年，数据处理咨询专家E. NYONI

《TECHNICAL OPTIONS OF COMPUTERZED WORLD》

2.4 Internet Security 14
2.4.1 Cryptographic 14
2.4.2 Firewall 15
2.4.2.1 Proxy Servers 15
2.4.2.2 Routers 16
2.4.3 Physical Isolation 16
2.4.4 Protocol Isolation 16
2.4.5 Protocol Isolation with Server Replication 17
2.4.6 Multi-homed System with Routing Disabled 17
2.4.7 Tunnelling Through the Internet 18

隔离技术概述

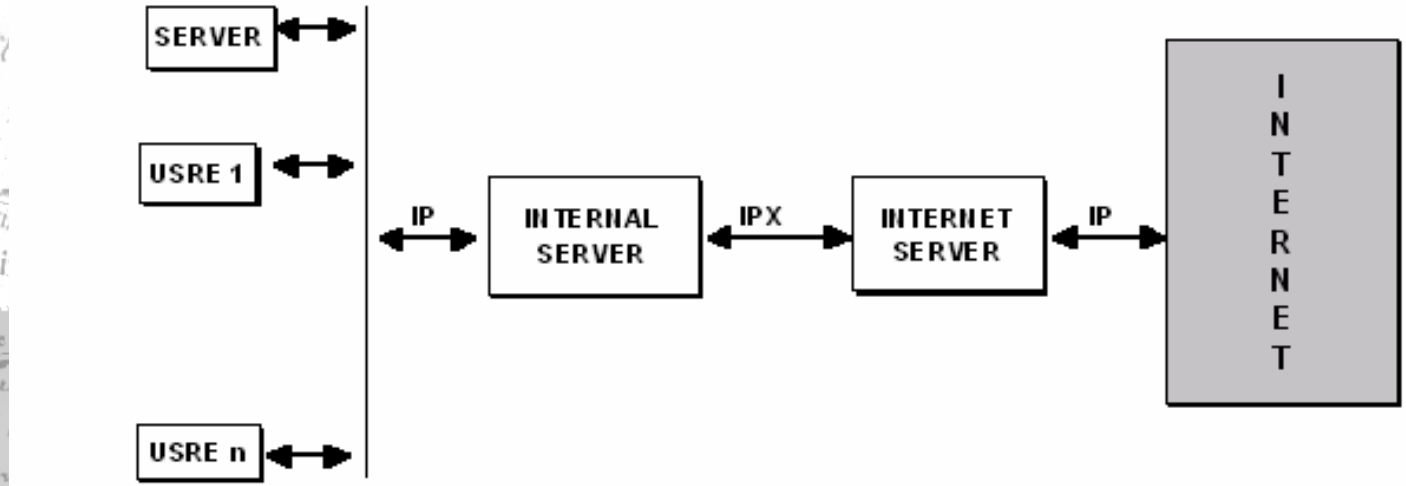
- 国外认识之二
  - 他还给出了防火墙的原理示意图：



隔离技术概述

- 国外认识之二
  - 在书中他也详细阐述了协议隔离：

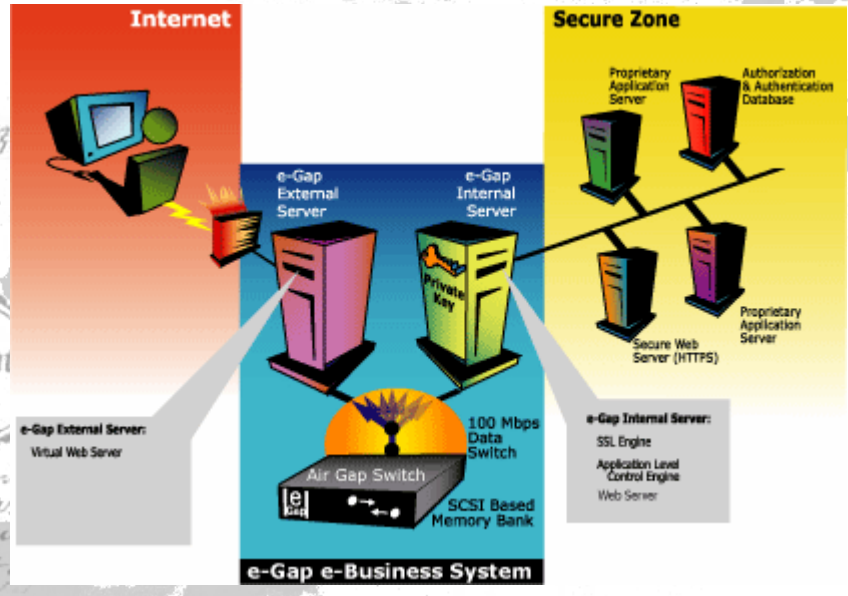
PROTOCOL ISOLATION WITH SERVER REPLICATION



This is a variation of (d) above with dual servers between which data is replicated. Protocol isolation is achieved by running IPX between the two servers, which individually each one of them runs TCP/IP. Because ALL information is replicated between the two servers both Internet users and internal users have access to the same and complete set of data.

国外公司

- 以色列的Whale公司
  - http://www.whalecommunications.com

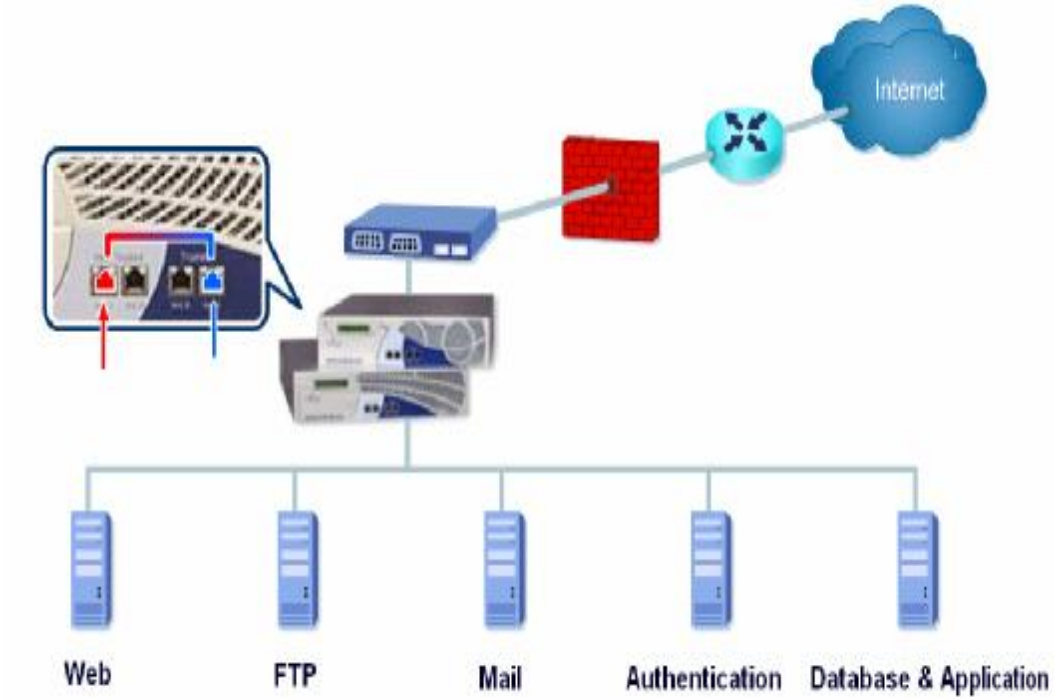


e-Gap Application Firewall

- **Application Filtering**
- **Authentication**
- **SSL Encryption/Decryption**
- **Network Isolation**

国外公司

- 以色列的Spearhead公司
  - http://www.spearheadsecurity.com



•Physical disconnection
•Protocol inspection
•Web application protection
•Authentication
•Central Policy, Distributed Control

隔离产品分类

- 网间安全威胁层次

威胁类别	风险等级	典型攻击
物理层次	低	超高电压、线路破坏等
协议层次	中	地址伪装、碎片攻击等
应用层次	高	恶意代码、垃圾邮件等

隔离产品分类

- 技术角度
  - 物理隔离：线路、设备、存储
  - 逻辑隔离：交换机、路由器、防火墙、网闸
- 应用角度
  - 桌面级隔离：
    - 部署位置：用户端
    - 产品形式：双机隔离、硬盘隔离、线路隔离
  - 企业级隔离：
    - 部署位置：网关处
    - 产品形式：交换机、路由器、防火墙、网闸

隔离技术发展与产品沿革

层次	隔离内容	产品
应用层	APPDATA	网闸
传输层	PORT	防火墙
网络层	IP	路由器
链路层	MAC	交换机
物理层	—	集线器

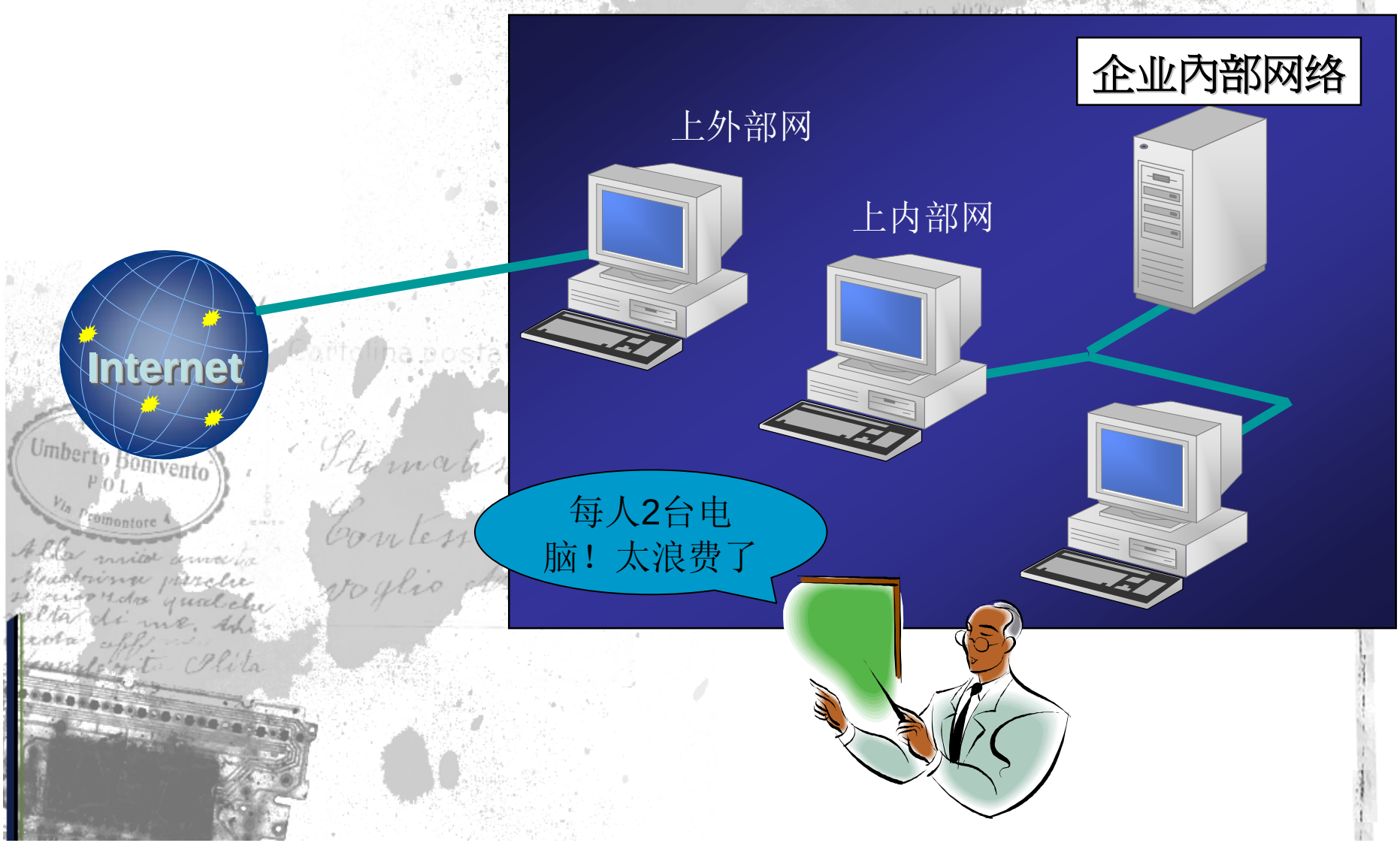
桌面级隔离技术

- 双机隔离
- 硬盘隔离
- 线路隔离

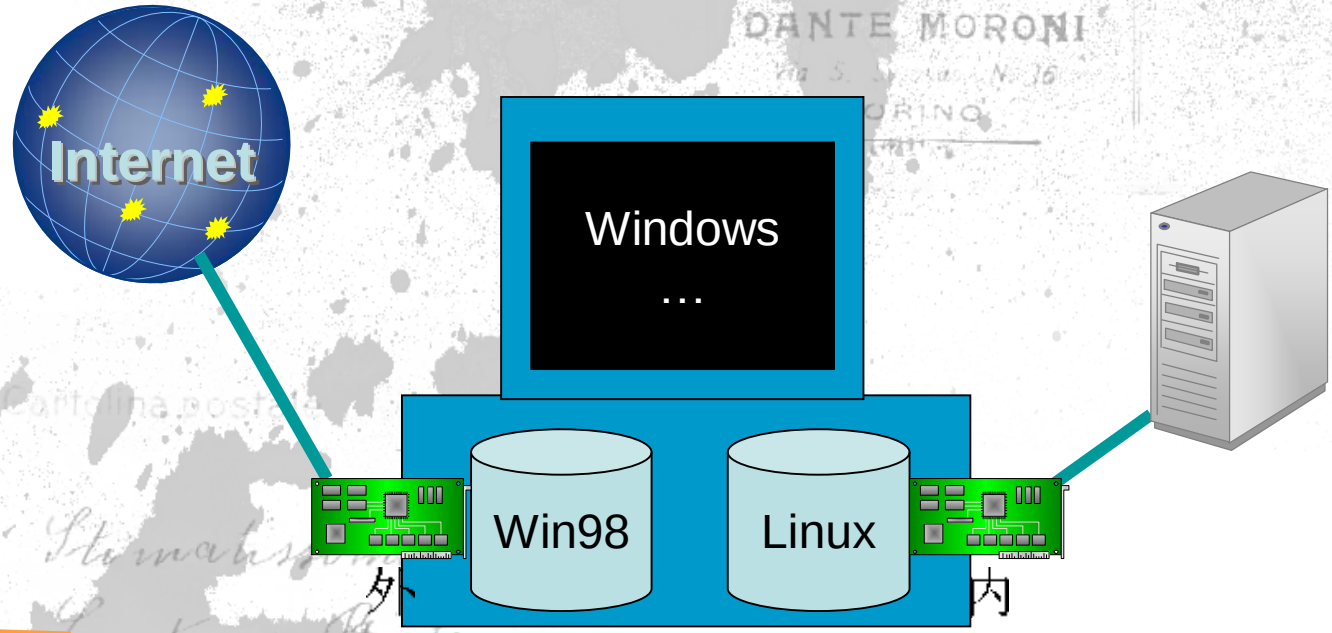
完全的物理隔离

上不了网L
我抗议…

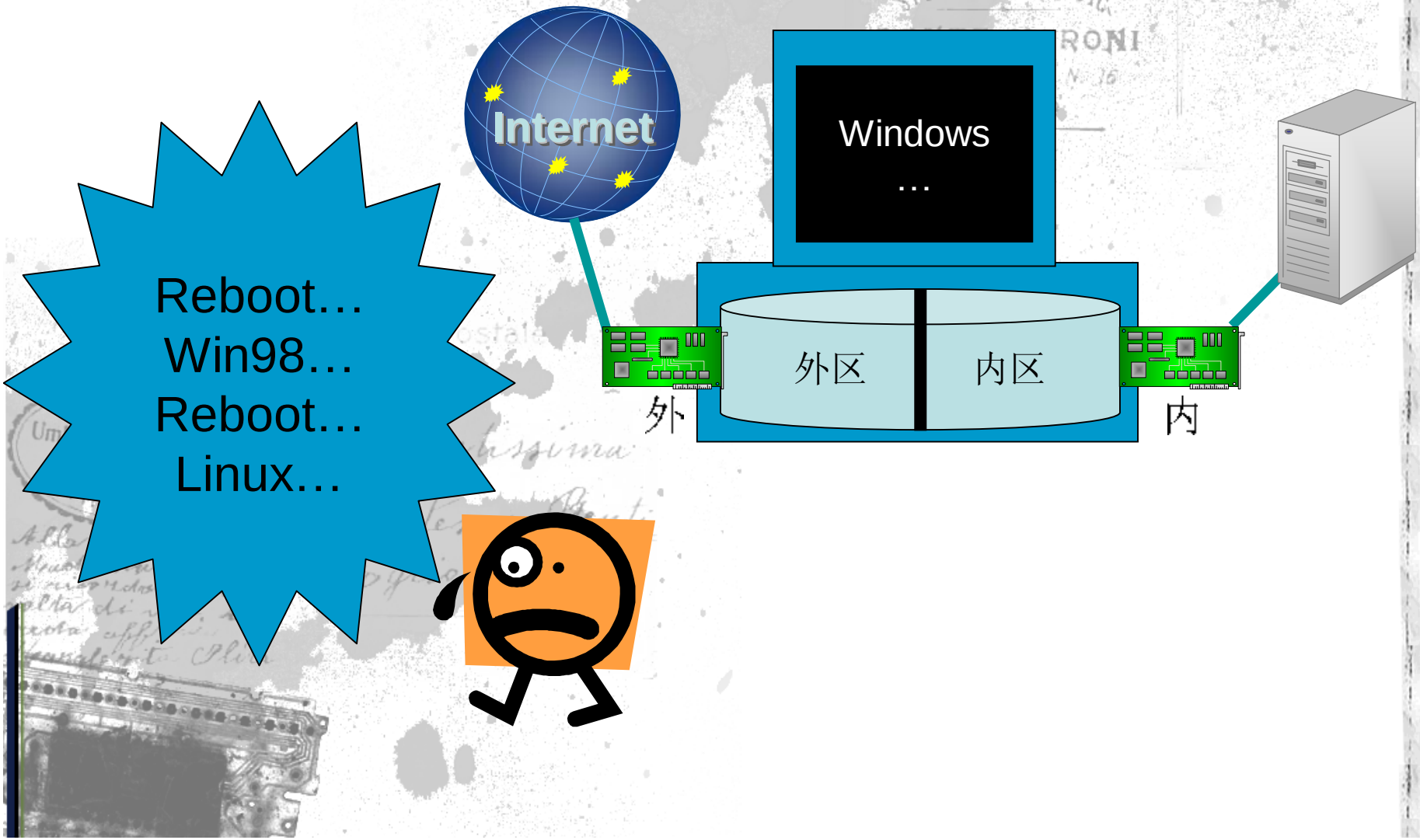
双机隔离



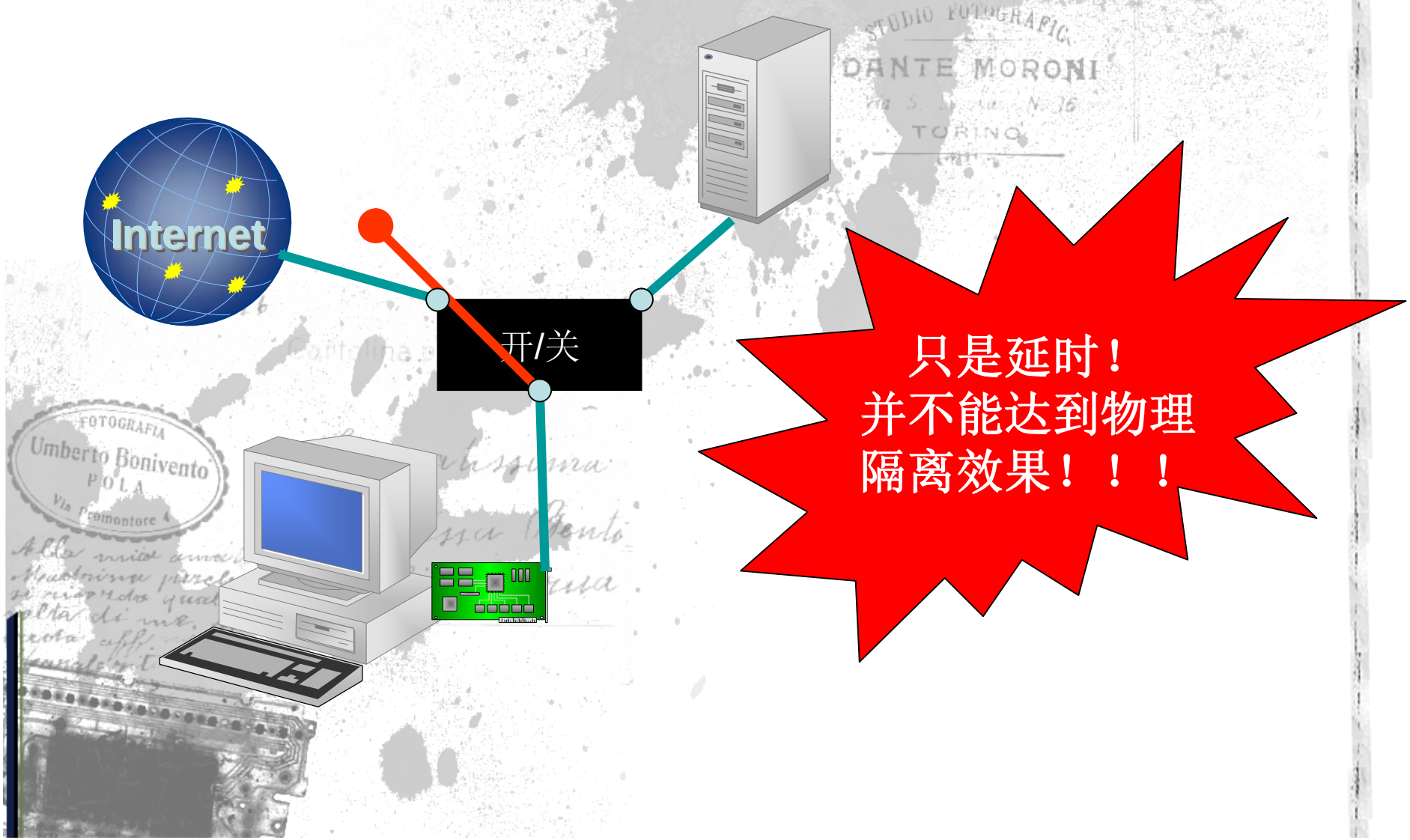
硬盘隔离（双硬盘）



硬盘隔离（单硬盘）



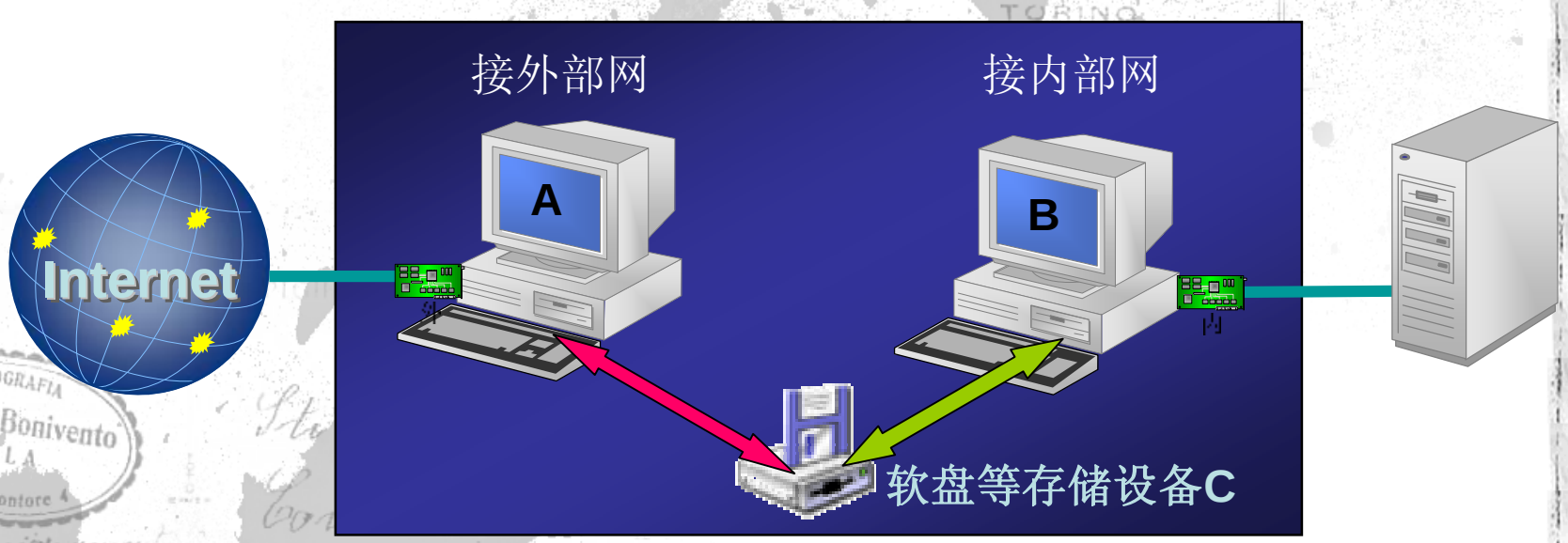
线路隔离



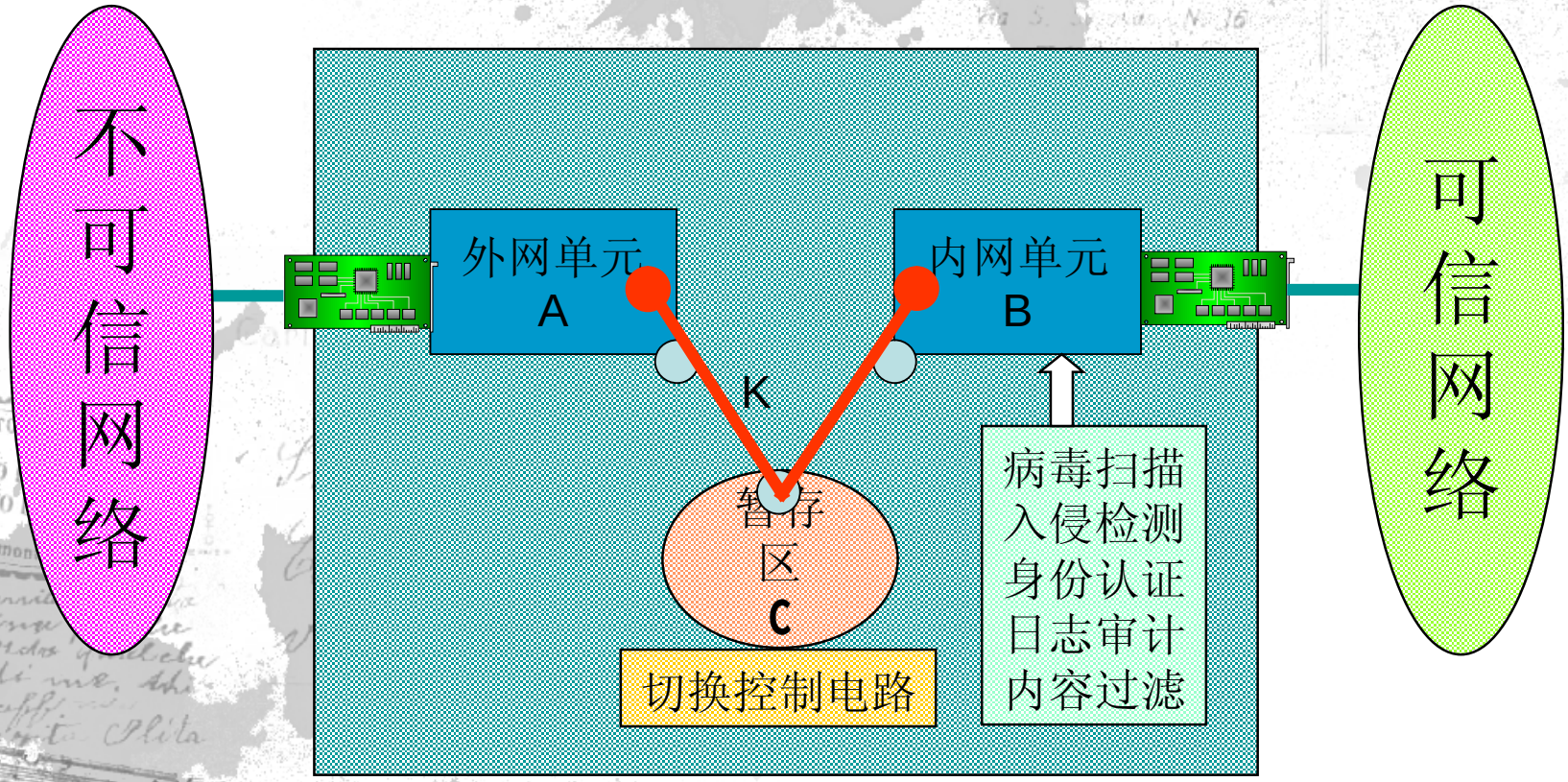
企业级隔离技术

- 第一代空气开关型隔离网闸
  - GAP：Air Gap
- 第二代专用交换通道型隔离网闸
  - PET：Private Exchange Tunnel

回顾双机隔离



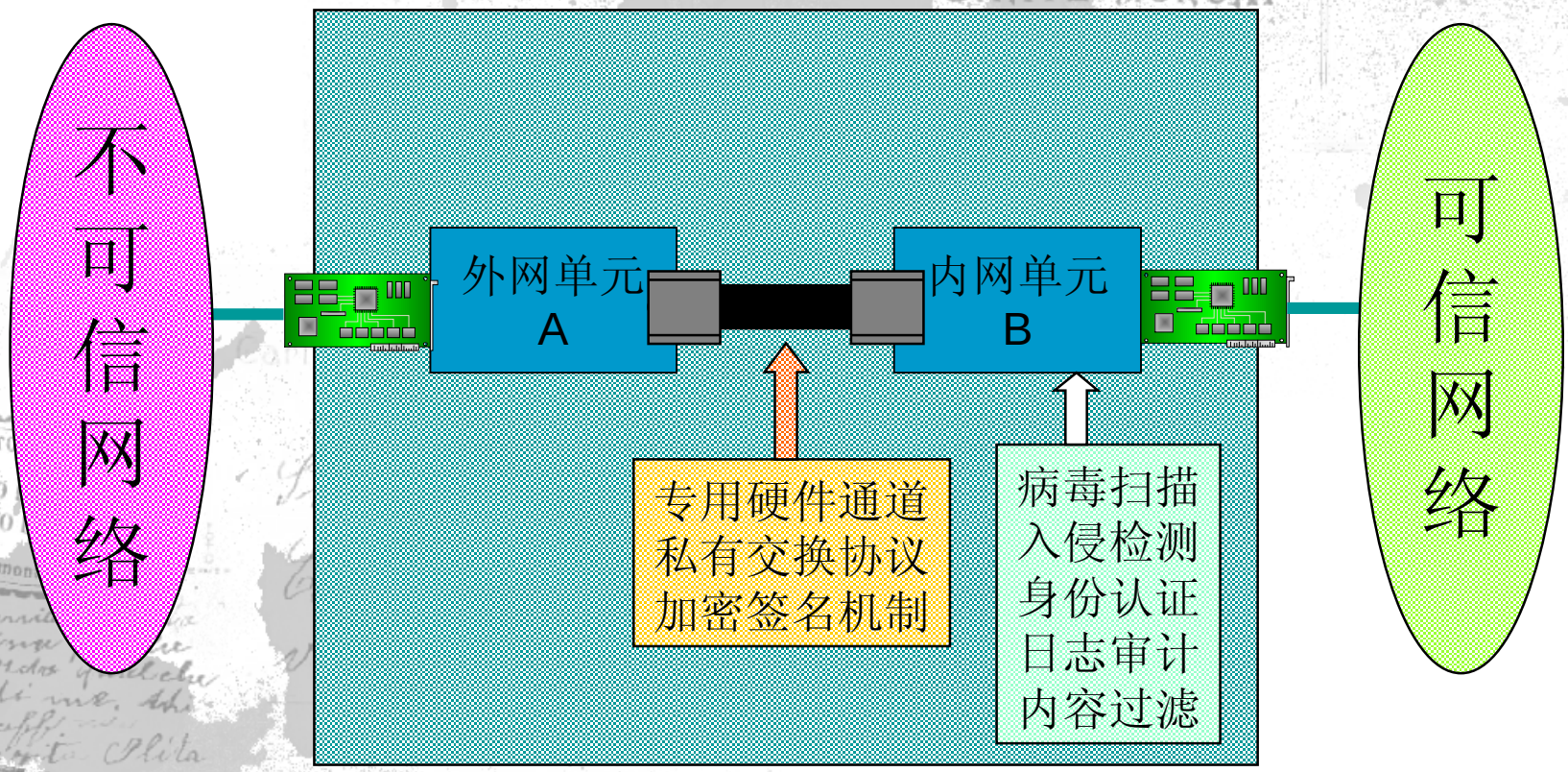
第一代空气开关型网闸


不可信网络
外网单元
A
内网单元
B
K
暂存区
C
切换控制电路
病毒扫描
入侵检测
身份认证
日志审计
内容过滤
可信网络

第一代空气开关型网闸

- 数据交换方式：是利用单刀双掷开关使得内外处理单元分时存取共享存储设备完成数据交换，实现了在空气缝隙隔离(Air Gap)情况下的数据交换。
- 安全功能原理：是通过应用层数据提取与安全审查达到杜绝基于协议层的攻击和增强应用层安全的效果。

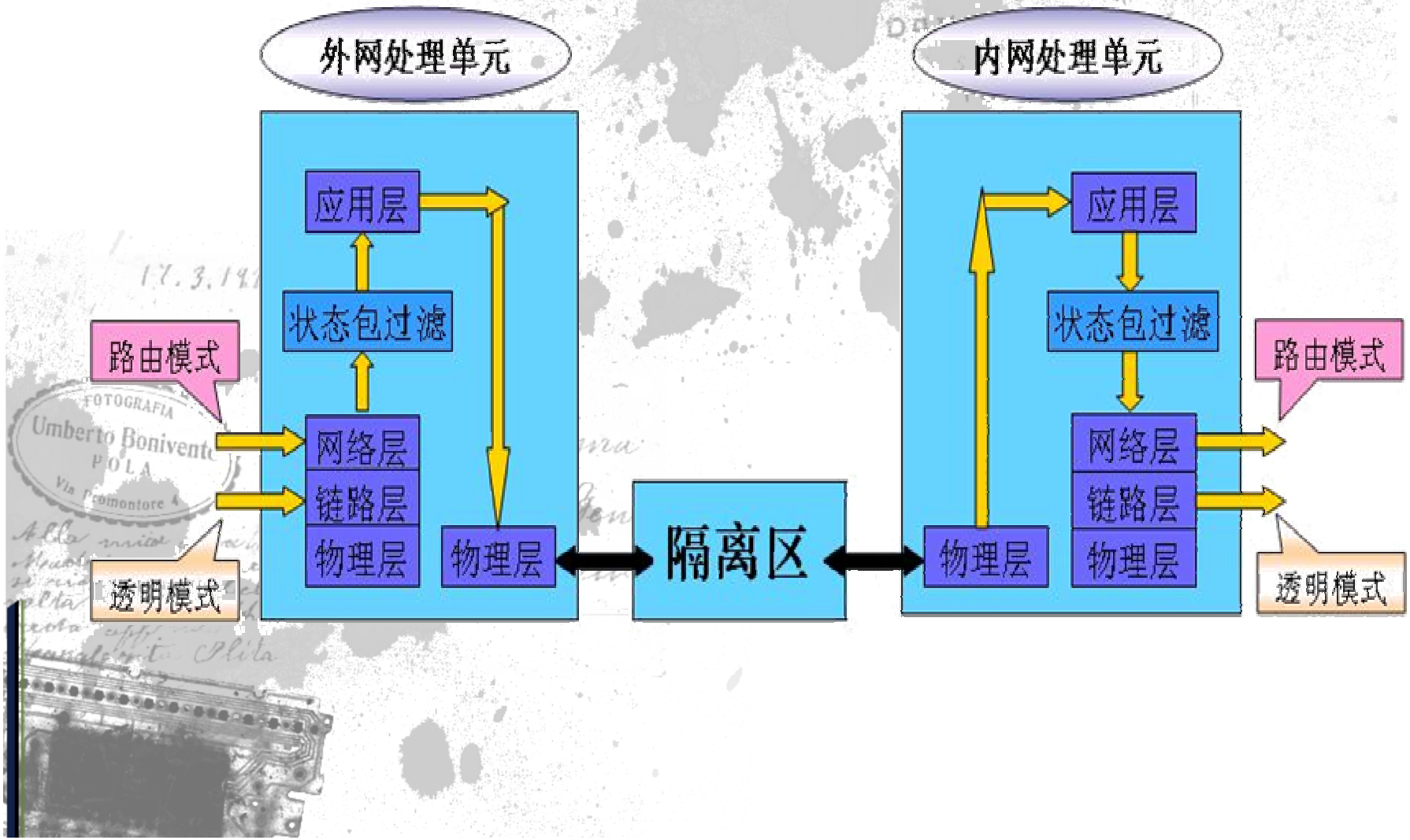
第二代专用交换通道型网闸



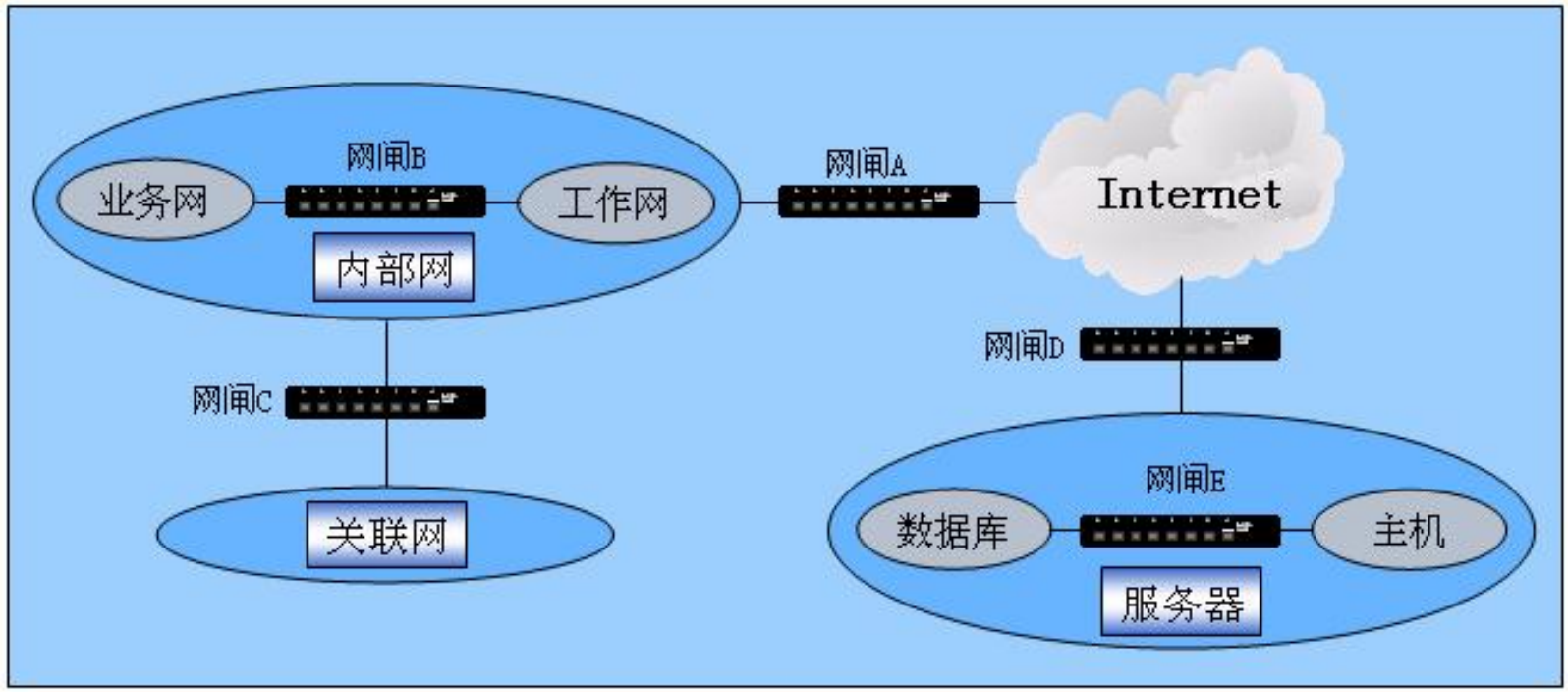
第二代专用交换通道型网闸

- 数据交换方式：利用专用高速通道、私有通信协议和加密签名机制实现了在网络隔离的情况下完成高速实时的数据交换。
- 安全功能原理：通过应用层数据提取与安全审查达到杜绝基于协议层的攻击和增强应用层安全的效果。

网闸的数据安全交换过程



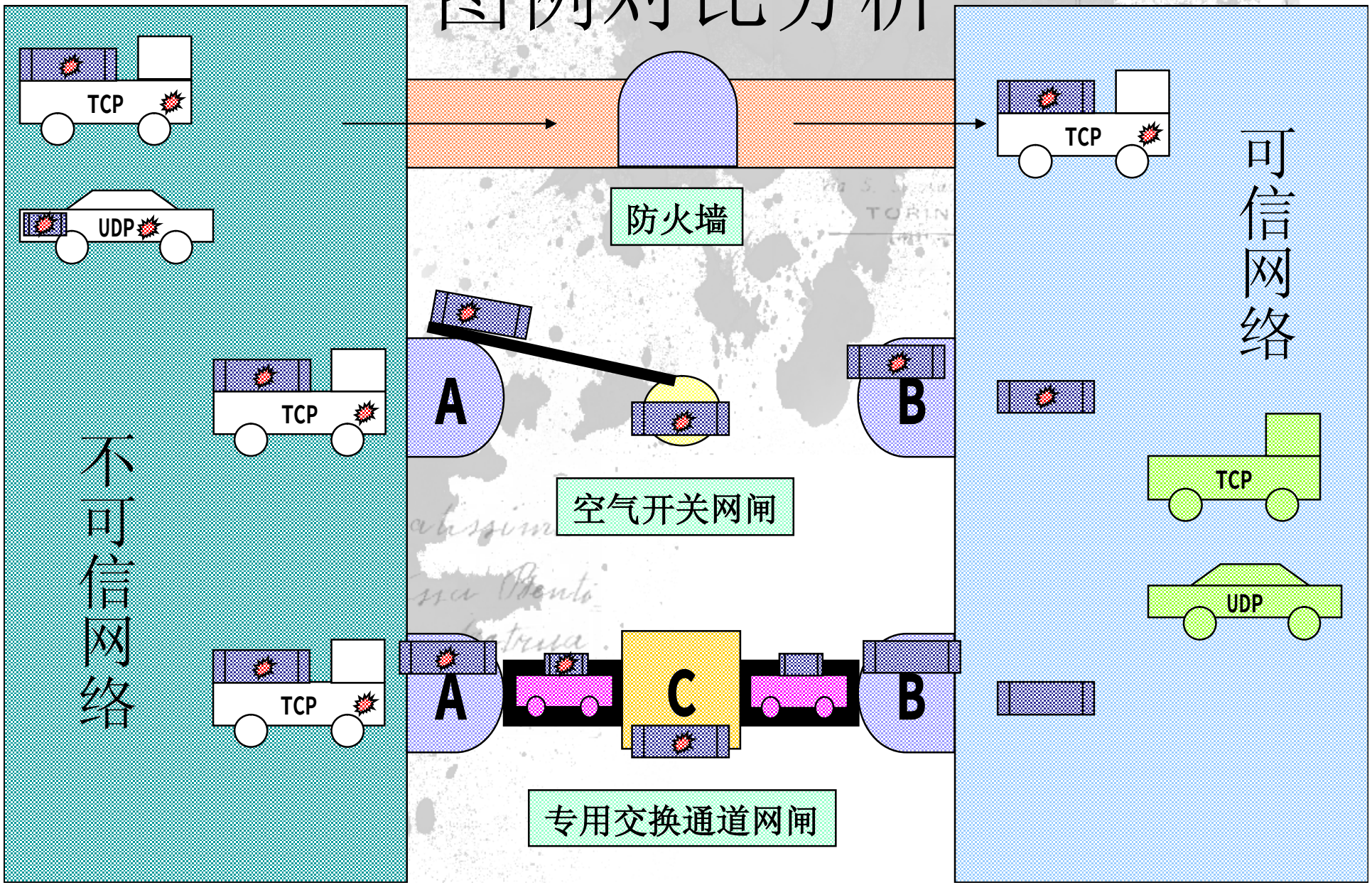
网闸的典型应用



网闸与防火墙

对比项目	网闸	防火墙
系统组成	2套以上主机	1套主机
专用交换硬件	有	无
通信协议	私有交换协议	TCP/IP
工作层次	应用层	网络层/链路层
自身安全性	高	低
网络隔离	是	否
应用层防护	强	弱

图例对比分析


TCP
UDP
防火墙
TCP
可信网络
TCP
A
B
空气开关网闸
TCP
TCP
UDP
不可信网络
TCP
A
C
B
专用交换通道网闸

Thanks !

Email: janker@janker.org

X'CON 2003