

网络物理隔离技术原理与应用

网络物理隔离概述
网络物理隔离系统与
类型
网络物理隔离机制与
实现技术
网络物理隔离产品与
技术指标
网络物理隔离应用

文老师软考教育

网络物理隔离概述

文老师软考教育

◆网络物理隔离概念：既能满足内外网信息及数据交换需求，又能防止网络安全事件出现的安全技术称为物理隔离技术。其基本原理是避免两台计算机之间直接的信息交换以及物理上的连通，以阻断两台计算机之间的直接在线网络攻击。隔离的目的是阻断直接网络攻击活动，避免敏感数据向外泄露，保障不同网络安全域之间进行信息及数据交换。

◆网络物理隔离安全风险：

- (1) 网络非法外联。处于隔离状态的网络用户私自连接互联网或第三方网络。
- (2) U盘摆渡攻击。网络攻击者利用U盘作为内外网络的摆渡工具，攻击程序将敏感数据拷贝到U盘中，然后由内部人员通过U盘泄露。如“U盘泄密者”病毒。
- (3) 网络物理隔离产品安全隐患。网络隔离产品的安全漏洞，导致DoS/DDoS攻击，使得网络物理隔离设备不可用。或者，网络攻击者通过构造恶意数据文档，绕过物理隔离措施，从而导致内部网络受到攻击。
- (4) 针对物理隔离的攻击新方法。利用各种手段，将被隔离计算机中的数据转换为声波、热量、电磁波等模拟信号后发射出去，在接收端通过模数转换复原数据，从而达到窃取信息的目的。如Bitwhisper窃密技术，是利用温度升降原理。

网络物理隔离系统与类型

- ◆网络物理隔离系统：是指通过物理隔离技术，在**不同的网络安全区域之间**建立一个能够实现物理隔离、信息交换和可信控制的系统，以满足不同安全域的信息或数据交换。
- ◆网络物理隔离类型：按照隔离的对象来分，网络物理隔离系统一般可以分为**单点隔离系统和区域隔离系统**。其中单点隔离系统主要是保护**单独的计算机系统**，防止外部直接攻击和干扰。区域隔离系统针对的是**网络环境**，防止外部攻击内部保护网络。
- ◆按照物理隔离的信息传递方向，网络物理隔离系统可分为**双向网络物理隔离系统与单向网络物理隔离系统**。

网络物理隔离机制与实现技术

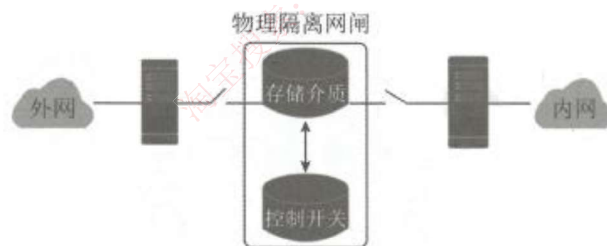
- ◆专用计算机上网：在内部网络中**指定一台计算机**，这台计算机只与外部网相连，不与内部网相连。用户**必须到指定的计算机才能上网**，并要求用户离开自己的工作环境。
- ◆多PC：内部网络中，在上外网的用户桌面上安放**两台PC**，分别连接两个分离的物理网络，一台用于连接外部网络，另一台用于连接内部网络。
- ◆外网代理服务：在内部网**指定一台或多台计算机充当服务器**，负责专门搜集外部网的制定信息，然后把**外网信息手工导入内部网**，供内部用户使用，从而实现内部用户“上网”，又切断内网与外网的物理连接，避免内网的计算机受到来自外网的攻击。
- ◆内外网线路切换器：在内部网中，**上外网的计算机上连接一个物理线路A/B交换盒**，通过交换盒的开关设置控制计算机的网络物理连接。
- ◆单硬盘内外分区：是**把单一硬盘分隔成不同的区域**，在IDE总线物理层上，通过一块IDE总线信号控制卡截取IDE总线信号，控制磁盘通道的访问，在任一时间内，仅允许操作系统访问指定的分区。这样，单硬盘内外分区技术将单台物理PC虚拟成逻辑上的两台PC，使得单台计算机在某一时刻只能连接到内部网或外部网。

网络物理隔离机制与实现技术

◆双硬盘：在一台机器上安装两个硬盘，通过硬盘控制卡对硬盘进行切换控制，用户在连接外网时，挂接外网硬盘，而当用内网办公时，重新启动系统，挂接内部网办公硬盘。在两个硬盘上实际上安装了两个操作系统。缺点是需要不断地重启系统，不易统一管理。

◆网闸：通过利用一种GAP技术，使两个或者两个以上的网络在不连通的情况下，实现它们之间的安全数据交换和共享。其技术原理是使用一个具有控制功能的开关读写存储安全设备，通过开关的设置来连接或切断两个独立主机系统的数据交换。

安全风险：入侵者可以利用恶意数据驱动攻击，将恶意代码隐藏在电子文档中，将其发送到目标网络中，通过具有恶意代码功能的电子文档触发，构成对内部网络的安全威胁。



网络物理隔离机制与实现技术

◆协议隔离技术：指处于不同安全域的网络在物理上是有连线的，通过协议转换的手段保证受保护信息在逻辑上是隔离的，只有被系统要求传输的、内容受限的信息可以通过。其中，协议转换的定义是协议的剥离和重建。把基于网络的公共协议中的应用数据剥离出来，封装为系统专用协议传递至所属其他安全域的隔离产品另一端，再将专用协议剥离，并封装成需要的格式。

◆单向传输部件：是指一对具有物理上单向传输特性的传输部件，该传输部件由一对独立的发送和接收部件构成，发送和接收部件只能以单工方式工作，发送部件仅具有单一的发送功能，接收部件仅具有单一的接收功能，两者构成可信的单向通道，该通道无任何反馈信息。

◆信息摆渡技术：是信息交换的一种方式，物理传输信道只在传输进行时存在。信息传输时，信息先由信息源所在安全域一端传输至中间缓存区域，同时物理断开中间缓存区域与信息目的所在安全域的连接；随后接通中间缓存区域与信息目的所在安全域的传输信道，将信息传输至信息目的所在安全域，同时在信道上物理断开信息源所在安全域与中间缓存区域的连接。在任何时刻，中间缓存区域只与一段安全域相连。

◆物理断开技术：是指处于不同安全域的网络之间不能以直接或间接的方式相连接。在一个物理网络环境中，实施不同安全域的网络物理断开，在技术上应确保信息在物理传导、物理存储上的断开。物理断开通常由电子开关实现。

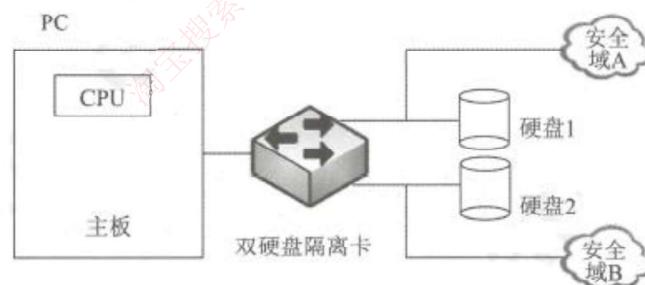
网络物理隔离产品与技术指标

◆网络物理隔离主要产品：

1. 终端隔离产品

终端隔离产品用于同时连接两个不同的安全域，采用物理断开技术在终端上实现安全域物理隔离的安全隔离卡或安全隔离计算机。

终端隔离产品一般以隔离卡的方式接入目标主机。隔离卡通过电子开关以互斥的形式同时连通安全域 A 所连硬盘、安全域 A 或安全域 B 所连硬盘、安全域 B，从而实现内外两个安全域的物理隔离。该类产品也可将隔离卡整合入主机，以整机的形式作为产品。终端隔离产品典型运行环境如图 11-7 所示。

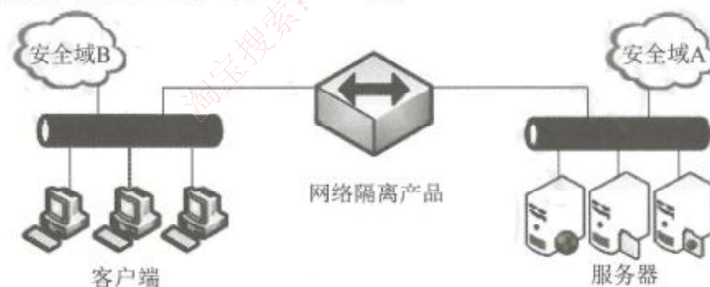


网络物理隔离产品与技术指标

◆网络物理隔离主要产品：

2. 网络隔离产品

网络隔离产品用于连接两个不同的安全域，实现两个安全域之间的应用代理服务、协议转换、信息流访问控制、内容过滤和信息摆渡等功能。产品技术原理采用“2+1”的架构，即以两台主机+专用隔离部件构成，采用协议隔离技术和信息摆渡技术在网络上实现安全域安全隔离与信息交换。其中，专用隔离部件一般采用包含电子开关并固化信息摆渡控制逻辑的专用隔离芯片构成的隔离交换板卡，或者是经过安全强化的运行专用信息传输逻辑控制程序的主机。网络隔离产品典型运行环境如图 11-8 所示。

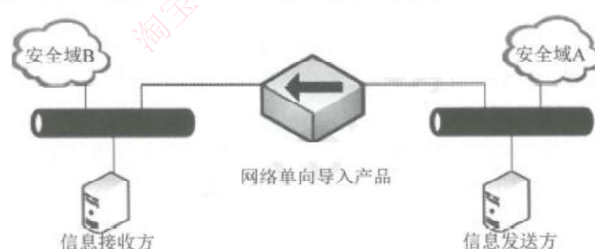


网络物理隔离产品与技术指标

◆网络物理隔离主要产品：

3. 网络单向导入产品

网络单向导入产品位于两个不同的安全域之间，通过物理方式（可基于电信号传输或光信号传输）构造信息单向传输的唯一通道，实现信息单向导入，并且保证只有安全策略允许传输的信息可以通过，同时反方向无任何信息传输或反馈。图 11-9 为网络单向导入产品的一个典型运行环境。网络单向导入产品一般以双机方式组成，即数据发送处理单元和数据接收处理单元，双机之间采用单向传输部件相连。网络单向导入产品部署在两个安全域之间，其中，数据发送处理单元网络接口连接信息发送方安全域 A，数据接收处理单元网络接口连接信息接收方安全域 B，信息流由发送数据的安全域 A 单向流入接收数据的安全域 B。单向传输部件利用单向传输的物理特性建立两个安全域之间唯一的单向传输通道，数据在这个通道中只能沿数据发送处理单元向数据接收处理单元方向的可信路径单向传输，无任何反馈信号。



网络物理隔离产品与技术指标

◆网络物理隔离技术指标：主要有安全功能指标、安全保障指标、性能指标。

◆安全功能指标：

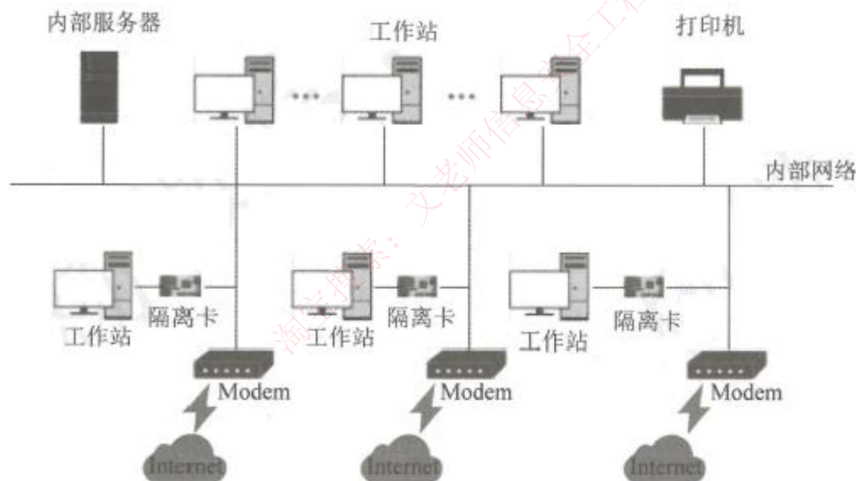
产品名称	功能要求
终端隔离产品	访问控制、不可旁路和客体重用
网络隔离产品	访问控制、抗攻击、安全管理、标识和鉴别、审计、域隔离、容错、数据完整性和密码支持
网络单向导入	访问控制、抗攻击、安全管理、标识和鉴别、审计、域隔离、配置数据保护和运行状态监测

◆安全保障指标主要是关于产品的质量和服务保障要求，如配置管理、交付和运行、开发和指导性文档、测试、脆弱性评定等。

◆性能要求则是对网络和终端隔离产品应达到的性能指标做出规定，包括交换速率和硬件切换时间。

网络物理隔离应用

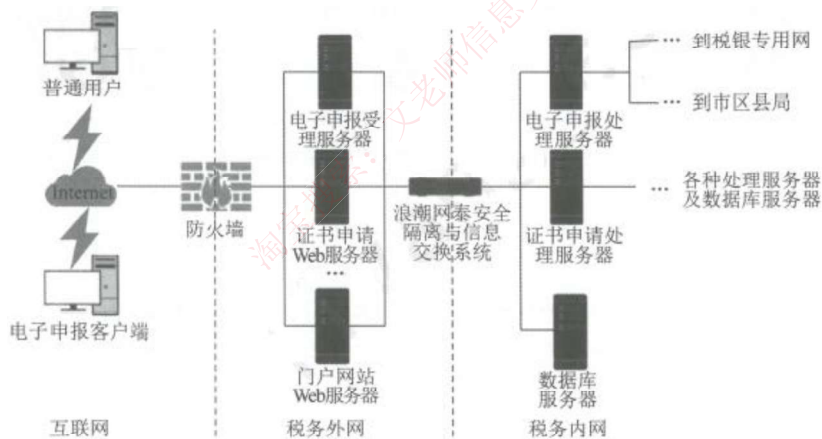
◆工作机安全上网实例：在需要上因特网的计算机中安装一块物理隔离卡，通过物理隔离卡，使一台工作机在上因特网时，从物理上断开与内部网的连接，因而减少内部网的安全威胁。



网络物理隔离应用

◆电子政务中网闸应用实例：电子政务网络由政务内网和政务外网构成，两网之间物理隔离，政务外网与互联网之间逻辑隔离。如下图：

◆税务外网和内网的数据交换只能通过安全隔离网闸，保证了内外网物理隔离并能进行实时的信息交换。该网闸技术原理是切断网络之间的通用协议连接，将数据包进行分解或重组为静态数据，然后对静态数据进行安全审查，包括网络协议检查和代码扫描等，确认后的安全数据流入内部单元。





谢谢！

文老师软考教育