9 网闸【安全隔离与信息交换系统】

0x01 实验环境

无，看看视频与 PPT,了解产品即可

0x02 原理介绍

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；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；内部用户通过严格的身份认证机制获取所需数据。

由于物理隔离网闸所连接的两个独立主机系统之间，不存在通信的物理连接、逻辑连接、信息传输命令、信息传输协议，不存在依据协议的信息包转发，只有数据文件的无协议”摆渡”,且对固态存储介质只有"读”和"写”两个命令。所以，物理隔离网闸从物理上隔离、阻断了具有潜在攻击可能的一切连接，使"黑客“无法入侵、无法攻击、无法破坏，实现了真正的安全。

第一代网闸的技术原理是利用单刀双掷开关使得内外网的处理单元分时存取共享存储设备来完成数据交换的，实现了在空气缝隙隔离(Air Gap)情况下的数据交换，安全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。

第二代网闸正是在吸取了第一代网闸优点的基础上，创造性地利用全新理念的专用交换通道 PET(PrivateExchange Tunnel)技术，通过专用硬件通信卡、私有通信协议和加密签名机制来实现的，虽然仍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效果的，但却提供了比第一代网闸更多的网络应用支持，并且由于其采用的是专用高速硬件通信卡，使得处理能力大大提高，达到第一代网闸的几十倍之多，而私有通信协议和加密签名机制保证了内外处理单元之间数据交换的机密性、完整性和可信性，从而在保证安全性的同时，提供更好的处理性能，能够适应复杂网络对隔离应用的需求。

安全隔离网闸是由软件和硬件组成。隔离网闸分为两种架构，一种为双主机的 2+1 结构，另一种为三主机的三系统结构。2+1 的安全隔离网闸的硬件设备由三部分组成：外部处理单元、内部处理单元、隔离安全数据交换单元。安全数据交换单元不同时与内外网处理单元连接。隔离网闸采用 SU-Gap 安全隔离技术，创建一个内、外网物理断开的环境。三系统的安全隔离网闸的硬件也由三部分组成：外部处理单元(外端机)、内部处理单元(内端机)、仲裁处理单元(仲裁机),各单元之间采用了隔离安全数据交换单元

光闸英文简称 FGAP,是一种由安全隔离网闸(GAP)基础上发展而成、基于光的单向性的单向隔离软硬件系统，用于对安全性要求极高的网络的数据交换场景，如涉密网络与非涉密网络之间，行业内网与公共只络之间

安全隔离网闸，它解决了电子政务兴起带来的政务内网和外网之间安全隔离、适度可控的数据交换的需求。

网闸技术是基于双向的，即通过配置，是允许高安全网络和低安全网络之间双向数据交换的。涉密网络与非涉密网络连接时，若非涉密网络与互联网物理隔离，则采用双向网闸隔离；若非涉密网络与互联网是逻辑隔离的，则采用单向网闸隔离，保证涉密数据不从高密级网络流向低密级网络。

单向隔离光闸由三部分组成：内网单元、外网单元、分光单向传输单元.

内网单元和外网单元所实现的安全功能是一致的，只是连接不同的网络，以内网单元为例，其包括内网接口单元与内网数据缓冲区。

接口部分负责与内网的连接，并终止内网用户的网络连接。对数据进行病毒检测、防火墙、入侵防护等安全检测后剥离出”纯数据”,作好交换的准备，也完成来自内网对用户身份的确认，确保数据的安全通道；数据缨冲区是存放并调度剥离后的数据，负责与隔离交换单元的数据交换，

单向隔离技术：物理单向技术：光盘，电气单向技术：程序控制，光的单向技术：光纤：单向隔离光闸根据业务场景需求，单向隔离光闸一般支持数据库传输、文件传输功能。高效率：光单向技术效率极高，延迟可控制在纳秒级。高可靠性：使用高可靠性硬件设计，数据传输模块内置差错校验机制

完善的业务功能：在单向文件传输基础上实现了数据库内容的单向同步，极大丰富单向光闸设备功能，具有更好的应用适应性。高安全性：网络间的单向隔离；设备不接受任何未知来源的主动请求；应用层数据获取后进行落地还原处理；通过可进行扩展定义的内容检查机制为白名单策略提供进一步的保障机制。