(NAS)加密存储网关

摘要：综合应用 SM2、SM3、SM4 等国密标准算法，基于 SMB、CIFS、NFS 文件共享协议解析，封装，为原有 NAS 存储环境提供文件加解密，访问控制和审计日志，可有效降低非法访问、越权访问等带来的敏感数据泄露风险。以标准存储协议为技术核心能兼容复杂多变的存储环境，兼容主流存储设备。

关键词：加密存储、文件审计、大数据、国密应用

1. 概述

1.1 背景

(NAS)加密存储网关产品，专为数据高度敏感用户提供基于国密算法 SM2、SM3、SM4 的 NAS 存储文件加解密及审计功能，由管理中心、存储网关和密码模块组成。管理中心提供对多台存储网关管理的功能，所有的策略信息、日志信息及密钥信息由管理中心统一配置；网关负责真正核心业务数据的处理；密码模块负责国密标准算法，密钥管理。

管理中心是自主研发的管理程序，具备管理多台网关的处理能力；存储网关是自主研发的安全存储网关软件，具备对 NAS 存储协议解析，封装，和对文件加解密功能，审计功

能，支持的协议包括：SMB、CIFS、NFS。密码卡使用国密局认证的设备。

1.2 目标

安全存储网关产品适用于各类数据的安全加密存储，主要目标包括以下几点：

1. 数据私密性保障

文件采用明文的方式存储在硬盘上，存在安全隐患，需要加密存储。

2. 访问控制权限

对NAS的访问权限没有统一的控制或根本没有访问控制，非常容易造成越权访问或非法访问，需要有完善的访问控制管理；

3. 访问审计

对文件的访问没有留下记录，无法审计用户操作记录，需要提供文件访问日志记录。

2. 需求分析

随着信息时代得到来，人们对于数据安全和个人隐私越加重视。海量数据的存储为人工智能和大数据分析提供了基础，不断发展的存储技术为我们生活带来了极大便利，但安

全问题也在时时困扰着我们，病毒、黑客的猖獗，各种威胁之声不断传出。数据安全问题成为了各界关注的重点问题，很多机密文件一旦被黑客窃取或泄露，损失是不可想象的，重则可能威胁到国家的安全。数据安全在一定程度上依赖于数据的安全存储。党的十九大报告中，习近平总书记明确提出了建设网络强国、数字中国的战略目标，提出推动互联网、大数据、人工智能和实体经济深度融合，促进传统产业优化升级。在这种形势下，各类信息系统正在快速发展建设，信息系统产生的敏感业务数据也越来越多，信息系统面对的来自内部和外部的的安全风险也大大增加。威胁存储安全的根源在于存储介质中的数据是以明文方式保存的，这使得入侵者可以轻易地非法获取和篡改数据，应对这种威胁的有效方法就是使用密码技术对存储在介质中的数据进行加密保护。基于以上相关背景，我公司凭借扎实的技术积累，自主研制了安全存储网关产品，为数据安全存储提供密码保护和支撑。

3. 方案架构

3.1 产品架构

安全存储网关产品由以下组件构成：

存储网关：提供万兆的加密性能，适应不同的NAS(存储系统)的文件加解密；

密码卡：提供标准的国密算法，密钥的生成，管理，为存储网关提供密码支撑。

管理中心：提供网关节点的策略设置，密钥管理，简化运维，可单独部署，也可以和网关部署在一起；

3.2 部署说明

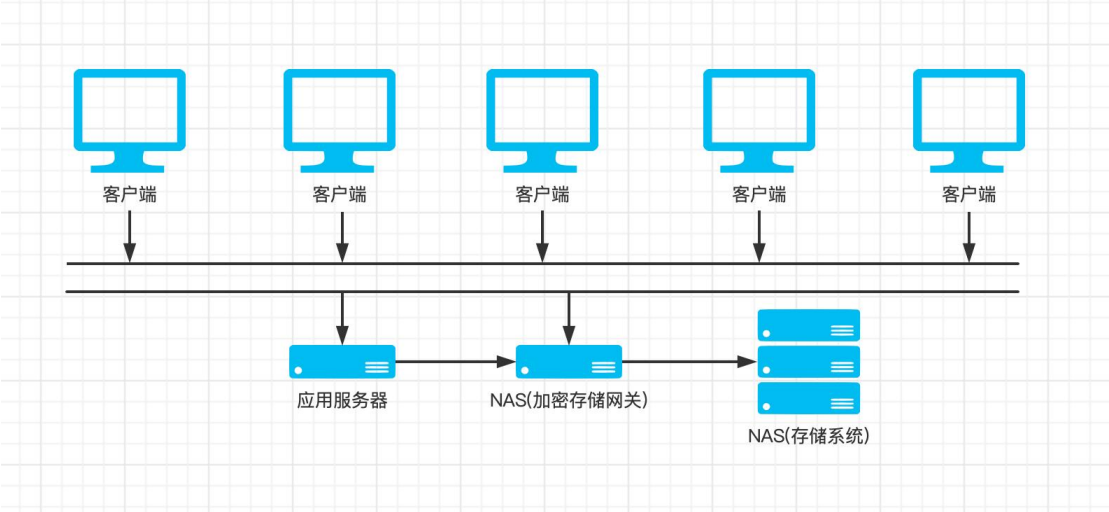

图 NAS 加密存储网关架构典型部署拓扑图

3.3 主要功能

1) 基于国密 SM2,SM3,SM4 算法的高性能数据加解密功能；

2) 支持 SMB,CIFS,NFS 协议,支持多用户,多路径；

3) 详细的文件访问控制和审计功能；

4) 图形化管理界面，支持网关节点集中化管理；

3.4 技术指标

1.存储网关

（1）外部接口指标

以太网口	2 个 10Gbps 全双工 SFP+光口
USB 口	2 个标准 USB2.0 接口
FC 口	2 个 16Gbps FC 口

（2）主要性能

1) 最大加解密带宽：20Gpbs；

2) 平均加解密时延：＜3ms。

（3）物理特性

1) 体积：宽 448mm×高 175.5mm×深 898.2mm；

2) 重量：61kg。

（4）电气特性

1) 控制电源：交流 100V～240V；

2) 功耗：200w。

（5）环境指标

1) 工作温度：5° C～+40° C；

2) 存储温度：-40° C～+55° C；

3) 湿　　度：10%～90%。

4. 方案特色

4.1 存储多样化支持

对已有存储系统的环境部署，无需改变现有的存储架构，可无缝接入现有环境；对没有存储系统的环境需先部署存储系统，NAS 系统。

多存储协议支持：SMB、CIFS、NFS。

存储网关核心架构主要实现对存储协议的数据解析,封装转发，在通过网关转发的过程中对文件数据加解密，无论是什么格式的文件数据或操作系统访问都能兼容，文件加解密的过程达到和应用、系统的无关性，透明化。

4.2 高适应性

安全存储网关采用密码卡加密，支持多种存储网络协议，在不改变现有业务和网络结构的基础之上，透明的解决了数据存储与访问的安全性问题，对保护企、事业单位的既有投资、快速解决信息系统合规性提供了灵活的解决方案与产品实现。

4.3 高灵活性

对已有存储系统的环境可直接部署安全存储网关，支持对文件的加解密，审计，一劳永逸解决数据存储、访问安全问题。

5.适用领域

该项目主要用于政府、部队、企事业部门和行业加密存储服务，适用范围包含但不局限于以下领域：

(一) 数据中心数据加密存储；

（二）具有重要核心业务数据和敏感数据单位的数据加密存储；

6.应用案例

实施单位：XX集团有限公司

需求：客户使用某磁盘集群构建的SAN环境和NAS（CIFS,NFS）环境，需要对存储系统中的的文件加密存储。

运行状况：安全存储网关部署后，能完全适配客户存储环境，系统运行稳定，NAS(CIFS,NFS)系统文件加解密，访问审计均工作正常。