ICS 35.030
CCS L 70

团　体　标　准

T/TAF 262—2025

基于大气激光通信的安全隔离设备技术要求

Technical requirements for safety isolation equipment based on atmospheric laser communication

2025-02-10 发布　　2025-02-10 实施

电信终端产业协会　发布

目　　次

前　　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由电信终端产业协会提出并归口

本文件起草单位：郑州信大捷安信息技术股份有限公司、中国信息通信研究院、博鼎实华（北京）技术有限公司、联想（北京）有限公司、国民认证科技（重庆）有限公司、成都泰瑞通信设备检测有限公司、深圳信息通信研究院。

本文件主要起草人：刘献伦、袁琦、王平、刘为华、康亮、李鑫、董霁、刘萧萧、廖正赟、李昭熹、彭金辉、韩秀德、梁松涛、李俊、冯志芳、靳涛、徐晓娜、李汝鑫、吴翔宇、王宇晓、邓佑军、王佳、吴建涛、曹帅、于跃、闫彦、王超、王鹏铖、张一驰、张永安、刘鑫、王爽、王威。

引　言

目前国内网络和终端隔离产品分为终端隔离产品和网络隔离产品两大类。终端隔离产品一般指隔离卡或者隔离计算机。网络隔离产品根据产品形态和功能上的不同，该类产品可以分为协议转换产品、网闸和网络单向导入产品三种。网络和终端隔离产品的功能目标是在不同的网络终端和网络安全域之间建立安全控制点，在不同的网络终端和网络安全域之间提供访问可控的服务，网络和终端隔离产品保护的资产是受安全策略保护的网络服务和资源等。此外，网络和终端隔离产品本身及其内部的重要信息也是受保护的对象。

基于大气激光通信的安全隔离设备是利用大气激光作为数据传输的载体，其原理是先将电信号转换成光信号，通过激光频率的调制实现信息的传输，激光用空气作为传输介质。由于光的传输具有不可逆特点，并且通过空气作为光的传输介质，没有任何有线连接或接触，可以很好的满足物理隔离和单向导入两个特点。

基于国家相关法律法规要求、结合行业特点和技术发展趋势，采用大气激光安全隔离设备可有效解决“物理隔离”和“单向导入”的业务需求，满足数据从低密级网络向高密级网络传递的需求，同时杜绝高密级网络数据的泄露风险。此技术方案可广泛应用于电力、医疗、工业互联网等重要行业，为保障重要行业的网络安全、数据安全和个人信息安全保驾护航。

基于大气激光通信的安全隔离设备技术要求

1　范围

本文件规定了基于大气激光通信的安全隔离设备技术要求，包括业务功能要求、自身安全要求、性能要求、运营管理要求等。

本文件主要适用于基于大气激光通信的安全隔离设备的设计、研发、运维管理等等。

2　规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 25069-2022　信息安全技术　术语

3　术语和定义

GB/T 25069-2022界定的以及下列术语和定义适用于本文件。

3.1

大气　atmosphere

包围地球的空气层。

[来源：《大气科学名词》，2009，科学出版社]

3.2

激光　laser

基于粒子(原子、分子)受激辐射放大原理而产生的一种相干性极强的光。

[来源：《光学名词》，2021，科学出版社]

3.3

大气激光通信　atmospheric laser communications

以大气作为信道的激光通信技术，主要用于完成点到点或点到多点的信息传输，主要采用半导体激光器为光源。

[来源：《电子学名词》]

3.4

大气激光安全隔离设备　atmospheric laser safety isolation equipment

一种由安全隔离网闸基础上发展而成、基于大气激光的单向性的单向隔离网络安全产品。

4　缩略语和符号

4.1　缩略语

下列缩略语适用于本文件。

CoAP：受限应用协议（Constrained Application Protocol）

CPU：中央处理器（Central Processing Unit）

FTP：文件传输协议（File Transfer Protocol）

HTTP：超文本传输安全协议（Hyper Text Transfer Protocol）

IC：集成电路（Integrated Circuit）

IMAP：交互式邮件存取协议（Internet Message Access Protocol）

IP：网际协议（Internet Protocol）

ICMP：互联网控制报文协议（Internet Control Message Protocol）

MAC：媒体存取控制位址（Media Access Control Address）

MAC：媒体访问控制（Media Access Control）

MQTT：消息队列遥测传输（Message Queuing Telemetry Transport）

NFS：网络文件系统（Net File System）

POP3：邮局协议第3版（Post Office Protocol - Version 3）

SMB：服务器信息块（Server Message Block）

SMTP：简单邮件传输协议（Simple Mail Transfer Protocol）

SNMP：简单网络管理协议（Simple Network Management Protocol）

SYN：同步报文（SYNchronous message）

TCP：传输控制协议（Transmission Control Protocol）

UDP：用户数据报协议（User Datagram Protocol）

4.2 符号

下列符号适用于本文件。

Gbps：吉波特每秒

Mbps：兆波特每秒

ms：毫秒

5 大气激光安全隔离设备概述

5.1 设备系统组成

大气激光安全隔离设备通常部署在不同安全等级网络边界，保护网络中的数据安全状态，不被传输出去，通过大气激光通信技术实现物理隔离和数据的绝对单向传输，切断了被保护区域数据泄露的风险。

大气激光安全隔离设备通常由数据发送处理单元、数据接收处理单元和大气激光单向传输模块组成。其中，两个处理单元分别连接不同的安全域，经大气激光单向传输模块实现数据单向传递。大气激光单向传输模块是两个安全域之间唯一的数据传输通道。大气激光安全隔离设备用于连接两个不同的安全域，实现网络的两个安全域之间的访问控制、数据传输等功能，其组成如图1所示。

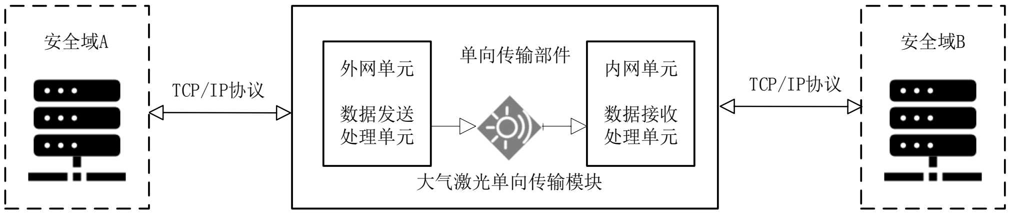

图1　大气激光安全隔离设备结构图

数据发送处理单元、大气激光单向传输模块、数据接收处理单元主要如下：

——数据发送处理单元：负责与安全域 A 的连接，并终止安全域 A 用户的网络连接，对数据进行病毒检测、格式检查、内容过滤等安全检测后剥离出“纯数据”，作好交换的准备，并对安全域 A 用户身份进行确认，确保数据来源安全；

——大气激光单向传输模块：包括光电发送端和光电接收端，光电发送模块将数据调制到光波中，通过空气介质传输，光电接收模块通过光电接收器接收光信号，并将光信号进行光电转换；

——数据接收处理单元：负责与安全域 B 的连接，并终止安全域 B 用户的网络连接。对从数据发送单元接收到的数据执行病毒检测、格式检查、内容过滤和加解密等安全能力，并对内网获取数据的用户身份进行确认，确保数据安全。

5.2　设备总体框架

大气激光安全隔离设备总体框架主要包含业务功能要求、自身安全要求和运营管理要求几大部分，总体框架如图2所示。

图2　大气激光安全隔离设备总体框架图

其中，业务功能主要是面向业务提供相应的功能，保证设备实现相应的功能；自身安全主要是设备本身需要具备的安全能力，保证设备整体运行期间安全管理、抗攻击等安全能力；运维管理主要是设备需要具备的运营能力，包括状态监测、备份恢复、系统诊断等能力，保证设备运营正常。

6 功能要求

6.1 单向传输链路

应保证大气激光安全隔离设备的两个处理单元之间采用大气激光单向传输模块进行数据传输，并且是唯一的数据传输通道。

6.2 访问控制

6.2.1 基于黑白名单的访问控制

应配置和应用基于账号口令的白名单、黑名单的访问控制策略，禁止白名单以外和黑名单以内的网络访问。

6.2.2 IP 地址/MAC 地址绑定

应支持自动或手工绑定通信接口对端设备的接口IP地址和MAC地址，当通信接口对端设备的IP地址和MAC地址与绑定列表不符时阻止通信。

6.2.3 链路和网络层访问控制

链路和网络层访问控制要求包括：

——应对发送数据的设备 MAC 地址、IP 地址进行访问控制；

——应对接收数据的设备 MAC 地址、IP 地址进行访问控制；

——应支持网络 MAC 地址或 IP 地址白名单或黑名单模式。

6.2.4 应用层访问控制

应用层访问控制要求包括：

——应支持 MQTT、CoAP 等常用的物联网协议；

——外网单元应仅通过系统允许的应用层协议进行数据接收，禁止未识别应用层协议的数据传输；

——内网单元应仅通过系统允许的应用层协议进行数据发送，禁止未识别应用层协议的数据传输。

6.2.5 强制访问控制

应根据业务要求构建的强制访问控制模型，识别用户和应用数据的敏感标记，根据标记执行强制访问控制策略。

6.2.6 安全功能策略检查

应通过安全功能策略检查后，才可执行安全相关操作。

6.3 应用和协议

6.3.1 基本要求

安全域两侧通过UDP/TCP协议进行数据传输过程中，应先将要传输的数据发送至外网单元所指定的数据接收服务，在外网单元剥离网络层、传输层协议，将传输层负载通过大气激光单向传输模块传输至内网单元。内网单元接收到负载数据后重新进行网络协议封装后发送至目标服务器。

数据单向传输要求包括：

——内网单元不宜从数据报文中获取到任何原数据报文的网络层信息；

——应采用一定方式处理数据传输过程中可能出现的粘包问题；

——宜支持应用层协议识别，防止非法应用数据传输。

6.3.2 文件单向同步要求

文件单向同步过程中，应先将要传输的文件传输至外网单元，在外网单元对文件进行安全检查之后，通过大气激光单向传输模块传输至内网单元，经由内网单元接收后发送至目标单元。

文件单向同步要求包括：

——外网单元应通过 FTP、SMB 或 NFS 协议接收文件数据；

——内网单元应通过 FTP、SMB 或 NFS 协议发送文件数据；

——外网单元接收数据使用的应用层协议可不同于内网单元发送数据使用的应用层协议；

——外网单元应对文件进行病毒查查杀，及时阻断病毒文件，支持常见的木马、蠕虫等病毒文件的识别与阻断；

——应对文件进行格式检查，及时阻断不明类型的文件，支持常见的文本、可执行程序、音视频等文件类型；

——应对文件内容进行检查，识别内容中的敏感词汇，及时阻断包含敏感数据的文件传输，或使用“*”等特殊字符对敏感内容进行替换处理；

——应采用商用密码算法对传输数据进行保护，通过 SM2 密码算法实现用户身份认证，通过 SM3 密码算法保证数据完整性，通过 SM4 算法保证数据机密性。

6.3.3 数据库单向同步要求

数据库数据单向同步过程中，应先将要传输的数据库表数据传输至外网单元，并落地为文件数据，在外网单元对文件内容进行安全检查之后，通过大气激光单向传输模块传输至内网单元，经由内外单元接收后还原成表数据发送至目标数据库。

数据库数据单向同步要求包括：

——应支持常见数据库类型的单向同步；

——应支持常见国产数据库类型的单向同步；

——应支持同构数据库之间的数据单向同步；

——应支持异构数据库之间的数据单向同步；

——应支持对数据库内容进行关键字过滤，及时阻断非法数据传输；

——宜支持数据库值转换功能，在同步过程中实现数据转换；

——宜支持选择特定表字段进行同步，防止冗余或无效数据对目标数据库造成数据污染。

6.3.4 邮件单向传输要求

支持外网单元接收邮件，对邮件及其附件进行安全检查后，通过大气激光单向传输模块发送至内网单元，由内网单元发送至目标邮箱。

邮件单向传输要求包括：

——应支持 SNMP、POP3 或 IMAP 中的一种；

——应对发件人、收件人进行黑、白名单访问控制；

——应对邮件内容进行敏感词过滤，及时阻断包含敏感数据的文件传输，或使用“*”等特殊字符对敏感内容进行替换处理；
——应对邮件附件进行病毒检查，及时阻断病毒文件，支持常见的木马、蠕虫等病毒文件的识别与阻断；
——应对接收邮件大小进行限制，定时清理历史邮件，保证系统正常运行。

6.4 数据传输

6.4.1 被动接收数据

大气激光安全隔离设备外网单元被动从数据源接收数据。被动接收数据要求包括：
——应通过用户名、口令的形式对操作用户进行身份认证；
——应通过数字证书形式对操作用户的身份进行认证；
——应采用商用密码算法保证数据传输过程中的机密性、完整性；
——应支持视窗操作系统、Linux 等操作系统；
——应支持指定文件夹及其子文件夹文件监听，及时发送新增或被修改文件。

6.4.2 主动获取数据

大气激光安全隔离设备外网单元主动从数据源获取数据。主动获取数据要求包括：
——应能从文件服务器主动获取文件数据；
——应支持从数据库服务器主动获取数据库数据；
——应支持单次、周期性获取数据；
——应支持全量、增量方式获取数据。

6.5 冗余能力

应具有“主—备”模式的冗余能力，即当一台设备因电源、CPU等硬件出现故障或软件错误导致异常时，冗余功能将当前安全服务功能自动切换到另一台产品上继续运行，保证安全功能的可用性。

6.6 数据完整性

应具有完整性保护功能，包括：
——应保护储存于设备中的鉴别数据和信息传输策略不受未授权查阅、修改和破坏；
——应具备数据传输过程的完整性保护，保证传输的数据完整性。

7 自身安全要求

7.1 标识和鉴别

7.1.1 唯一性标识

应保证所有用户、设备、系统都具有唯一的标识。宜采用数字证书形式标识用户身份。

7.1.2 管理员属性定义

应为每个管理员规定与之相关的安全属性，如管理员标识、鉴别信息、权限等。

7.1.3 管理员角色

应为管理角色进行分级，使不同级别的管理角色具有不同的管理权限，且按照最小必要权限进行授权，各管理角色的权限应形成互相制约关系。

7.1.4 身份鉴别

7.1.4.1 基本鉴别

应保证任何用户在执行安全功能前都要进行身份鉴别。若其采用网络远程方式管理，还应对可管理的地址进行限制。

7.1.4.2 多鉴别

应能向管理角色提供除口令身份鉴别机制以外的其他身份鉴别机制（如证书、智能IC卡、指纹等鉴别机制）。

7.1.4.3 超时锁定或注销

当已通过身份鉴别的管理角色空闲操作的时间超过规定值，在该管理角色需要执行管理功能前，应对该管理角色的身份重新进行鉴别。

7.1.4.4 鉴别失败处理

应为管理员登录设定一个授权管理员可修改的鉴别尝试阈值，当管理员的不成功登录尝试超过阈值，系统应通过技术手段阻止管理员的进一步鉴别请求。

7.2 抗拒绝服务攻击

应支持拒绝服务攻击防护功能，包括：

——ICMP Flood 攻击防护；

——SYN Flood 攻击防护；

——UDP Flood 攻击防护；

——Ping 网络测试致死攻击防护。

7.3 安全管理

7.3.1 接口及管理安全

接口及管理安全要求包括：

——应支持业务接口和管理接口应采用不同的网络接口；

——管理接口及管理界面不应存在中高风险及以上的安全漏洞。

7.3.2 管理信息传输安全

当需要通过网络进行管理时，应能对管理信息进行保密传输。

7.4 日志审计管理

7.4.1 业务日志

业务日志内容要求包括：

——应访问控制策略匹配的访问请求，包括允许及禁止的访问请求；

——应识别及抵御的各类攻击行为；

——文件同步应记录日期、时间、文件信息、同步方式、同步结果等；
——数据库同步应记录日期、时间、数据库表信息、同步方式、同步结果等；
——UDP 数据单向同步应记录：源地址、源端口、目的地址、目的端口及协议、同步结果等；
——邮件同步应记录日期、时间、发件人、收件人、同步结果等信息；
——应包含攻击事件的类型及描述。

7.4.2 系统日志

系统日志内容应至少包括日期、时间、事件主体、事件客体、事件描述等，系统日志生成要求包括：
——应包含身份鉴别，包括成功和失败；
——应包含因鉴别失败次数超过阈值而采取的禁止进一步尝试的措施；
——应包含访问控制策略的增加、删除、修改；
——应包含管理员的增加、删除、修改；
——应包含时间同步；
——应包含超过保存时限的审计记录和自身审计日志的自动删除；
——应包含审计日志和审计记录的备份与恢复；
——应包含存储空间达到阈值报警；
——宜包含其他事件。

7.4.3 审计日志管理

审计日志管理要求包括：
——应只允许授权管理员能够对审计日志进行读取、存档、导出、删除和清空等操作；
——应提供能查阅日志的工具，支持多条件对审计日志进行组合查询；
——审计事件应存储于掉电非易失性存储介质中，且在存储空间临近和达到阈值时，通知授权审计员；
——应支持以标准格式将审计日志外发到专用的日志服务器；
——日志留存时间应不少于 6 个月。

8 性能要求

8.1 百兆网络性能要求

百兆网络性能要求包括：
——网络吞吐量应不小于 100Mbps；
——数据时延不应超过 10ms。

8.2 千兆网络性能要求

千兆网络性能要求包括：
——网络吞吐量应不小于 1Gbps；
——数据时延不应超过 5ms。

8.3 万兆网络性能要求

千兆网络性能要求包括：
——网络吞吐量应不小于 4Gbps；

——数据时延不应超过 5ms。

9　运维管理要求

9.1　运行状态监测

运行状态监测要求包括：

——应对系统中的 CPU、内存、存储空间等系统资源使用状态进行监测；

——应对系统的主要功能模块运行状态进行监测；

——宜在设备上通过小型液晶屏显示系统运行状态，在不登录设备管理网页页面的情况下获取系统、任务运行状态（设备的单向性特点）。

9.2　系统升级

系统升级要求包括：

——应支持管理页面一键升级系统补丁包或新软件版本；

——应支持病毒库在线或离线更新。

9.3　备份恢复

备份恢复要求包括：

——应对安全功能相关配置进行加密备份，应支持导出到本地进行存储；

——应通过导入备份的配置文件可恢复至某一时刻系统安全功能配置。

9.4　告警通知

应对系统运行异常、业务异常、攻击行为等通过短信、邮件或页面记录等方式进行告警，告警内容包括：

——事件主体；

——事件客体；

——事件描述；

——事件级别；

——事件发生的日期和时间。

9.5　第三方管理

应支持第三方管理平台管理能力，如SNMP探测设备信息、服务信息等。

9.6　系统诊断

应提供一定的诊断方式，用于在发生系统异常时快速、便捷地定位故障原因，包括：

——抓取网络报文的接口；

——网络状态测试工具。

9.7　存储管理

应提供存储管理功能，便于系统长时间稳定运行，要求包括：

——根据业务进行存储分配；

——根据业务数据大小或时间进行配额，超出阈值时进行自动清理或转储。

参 考 文 献

[1] GB/T 20279-2015 信息安全技术 网络和终端隔离产品安全技术要求
[2] GB/T 25069-2022 信息安全技术 术语
[3] GB/T 38832-2020 基于公用电信网的宽带客户网络联网技术要求 通照一体化高速可见光通信
[4] YD/T 3622-2019 低功耗短距离可见光通信技术要求
[5] YD/T 1766-2016 光通信用光收发合一模块的可靠性实验失效判据
[6] 《大气科学名词》，2009，科学出版社
[7] 《光学名词》，2021，科学出版社

电信终端产业协会团体标准

基于大气激光通信的安全隔离设备技术要求

T/TAF 262—2025

*

电信终端产业协会印发
地址：北京市西城区新街口外大街28号
电话：010-82052809
电子版发行网址：www.taf.org.cn